Microsoft

Microsoft Official Course

SC-100T00

Microsoft Cybersecurity Architect

SC-100T00

Microsoft Cybersecurity Architect

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The names of manufacturers, products, or URLs are provided for informational purposes only and Microsoft makes no representations and warranties, either expressed, implied, or statutory, regarding these manufacturers or the use of the products with any Microsoft technologies. The inclusion of a manufacturer or product does not imply endorsement of Microsoft of the manufacturer or product. Links may be provided to third party sites. Such sites are not under the control of Microsoft and Microsoft is not responsible for the contents of any linked site or any link contained in a linked site, or any changes or updates to such sites. Microsoft is not responsible for webcasting or any other form of transmission received from any linked site. Microsoft is providing these links to you only as a convenience, and the inclusion of any link does not imply endorsement of Microsoft of the site or the products contained therein.

Microsoft and the trademarks listed at **http://www.microsoft.com/trademarks** [1]are trademarks of the Microsoft group of companies. All other trademarks are property of their respective owners.

1 http://www.microsoft.com/trademarks

MICROSOFT LICENSE TERMS

MICROSOFT INSTRUCTOR-LED COURSEWARE

These license terms are an agreement between Microsoft Corporation (or based on where you live, one of its affiliates) and you. Please read them. They apply to your use of the content accompanying this agreement which includes the media on which you received it, if any. These license terms also apply to Trainer Content and any updates and supplements for the Licensed Content unless other terms accompany those items. If so, those terms apply.

BY ACCESSING, DOWNLOADING OR USING THE LICENSED CONTENT, YOU ACCEPT THESE TERMS. IF YOU DO NOT ACCEPT THEM, DO NOT ACCESS, DOWNLOAD OR USE THE LICENSED CONTENT.

If you comply with these license terms, you have the rights below for each license you acquire.

1. **DEFINITIONS.**
    1. "Authorized Learning Center" means a Microsoft Imagine Academy (MSIA) Program Member, Microsoft Learning Competency Member, or such other entity as Microsoft may designate from time to time.
    2. "Authorized Training Session" means the instructor-led training class using Microsoft Instructor-Led Courseware conducted by a Trainer at or through an Authorized Learning Center.
    3. "Classroom Device" means one (1) dedicated, secure computer that an Authorized Learning Center owns or controls that is located at an Authorized Learning Center's training facilities that meets or exceeds the hardware level specified for the particular Microsoft Instructor-Led Courseware.
    4. "End User" means an individual who is (i) duly enrolled in and attending an Authorized Training Session or Private Training Session, (ii) an employee of an MPN Member (defined below), or (iii) a Microsoft full-time employee, a Microsoft Imagine Academy (MSIA) Program Member, or a Microsoft Learn for Educators – Validated Educator.
    5. "Licensed Content" means the content accompanying this agreement which may include the Microsoft Instructor-Led Courseware or Trainer Content.
    6. "Microsoft Certified Trainer" or "MCT" means an individual who is (i) engaged to teach a training session to End Users on behalf of an Authorized Learning Center or MPN Member, and (ii) currently certified as a Microsoft Certified Trainer under the Microsoft Certification Program.
    7. "Microsoft Instructor-Led Courseware" means the Microsoft-branded instructor-led training course that educates IT professionals, developers, students at an academic institution, and other learners on Microsoft technologies. A Microsoft Instructor-Led Courseware title may be branded as MOC, Microsoft Dynamics, or Microsoft Business Group courseware.
    8. "Microsoft Imagine Academy (MSIA) Program Member" means an active member of the Microsoft Imagine Academy Program.
    9. "Microsoft Learn for Educators – Validated Educator" means an educator who has been validated through the Microsoft Learn for Educators program as an active educator at a college, university, community college, polytechnic or K-12 institution.
    10. "Microsoft Learning Competency Member" means an active member of the Microsoft Partner Network program in good standing that currently holds the Learning Competency status.
    11. "MOC" means the "Official Microsoft Learning Product" instructor-led courseware known as Microsoft Official Course that educates IT professionals, developers, students at an academic institution, and other learners on Microsoft technologies.
    12. "MPN Member" means an active Microsoft Partner Network program member in good standing.

13. "Personal Device" means one (1) personal computer, device, workstation or other digital electronic device that you personally own or control that meets or exceeds the hardware level specified for the particular Microsoft Instructor-Led Courseware.
14. "Private Training Session" means the instructor-led training classes provided by MPN Members for corporate customers to teach a predefined learning objective using Microsoft Instructor-Led Courseware. These classes are not advertised or promoted to the general public and class attendance is restricted to individuals employed by or contracted by the corporate customer.
15. "Trainer" means (i) an academically accredited educator engaged by a Microsoft Imagine Academy Program Member to teach an Authorized Training Session, (ii) an academically accredited educator validated as a Microsoft Learn for Educators – Validated Educator, and/or (iii) a MCT.
16. "Trainer Content" means the trainer version of the Microsoft Instructor-Led Courseware and additional supplemental content designated solely for Trainers' use to teach a training session using the Microsoft Instructor-Led Courseware. Trainer Content may include Microsoft PowerPoint presentations, trainer preparation guide, train the trainer materials, Microsoft One Note packs, classroom setup guide and Pre-release course feedback form. To clarify, Trainer Content does not include any software, virtual hard disks or virtual machines.

2. **USE RIGHTS.** The Licensed Content is licensed, not sold. The Licensed Content is licensed on a **one copy per user basis**, such that you must acquire a license for each individual that accesses or uses the Licensed Content.

- 2.1 Below are five separate sets of use rights. Only one set of rights apply to you.

1. **If you are a Microsoft Imagine Academy (MSIA) Program Member:**

1. Each license acquired on behalf of yourself may only be used to review one (1) copy of the Microsoft Instructor-Led Courseware in the form provided to you. If the Microsoft Instructor-Led Courseware is in digital format, you may install one (1) copy on up to three (3) Personal Devices. You may not install the Microsoft Instructor-Led Courseware on a device you do not own or control.
2. For each license you acquire on behalf of an End User or Trainer, you may either:

1. distribute one (1) hard copy version of the Microsoft Instructor-Led Courseware to one (1) End User who is enrolled in the Authorized Training Session, and only immediately prior to the commencement of the Authorized Training Session that is the subject matter of the Microsoft Instructor-Led Courseware being provided, **or**
2. provide one (1) End User with the unique redemption code and instructions on how they can access one (1) digital version of the Microsoft Instructor-Led Courseware, **or**
3. provide one (1) Trainer with the unique redemption code and instructions on how they can access one (1) Trainer Content.

3. For each license you acquire, you must comply with the following:

1. you will only provide access to the Licensed Content to those individuals who have acquired a valid license to the Licensed Content,
2. you will ensure each End User attending an Authorized Training Session has their own valid licensed copy of the Microsoft Instructor-Led Courseware that is the subject of the Authorized Training Session,
3. you will ensure that each End User provided with the hard-copy version of the Microsoft Instructor-Led Courseware will be presented with a copy of this agreement and each End

User will agree that their use of the Microsoft Instructor-Led Courseware will be subject to the terms in this agreement prior to providing them with the Microsoft Instructor-Led Courseware. Each individual will be required to denote their acceptance of this agreement in a manner that is enforceable under local law prior to their accessing the Microsoft Instructor-Led Courseware,

4. you will ensure that each Trainer teaching an Authorized Training Session has their own valid licensed copy of the Trainer Content that is the subject of the Authorized Training Session,
5. you will only use qualified Trainers who have in-depth knowledge of and experience with the Microsoft technology that is the subject of the Microsoft Instructor-Led Courseware being taught for all your Authorized Training Sessions,
6. you will only deliver a maximum of 15 hours of training per week for each Authorized Training Session that uses a MOC title, and
7. you acknowledge that Trainers that are not MCTs will not have access to all of the trainer resources for the Microsoft Instructor-Led Courseware.

2. **If you are a Microsoft Learning Competency Member:**

   1. Each license acquire may only be used to review one (1) copy of the Microsoft Instructor-Led Courseware in the form provided to you. If the Microsoft Instructor-Led Courseware is in digital format, you may install one (1) copy on up to three (3) Personal Devices. You may not install the Microsoft Instructor-Led Courseware on a device you do not own or control.
   2. For each license you acquire on behalf of an End User or MCT, you may either:
      1. distribute one (1) hard copy version of the Microsoft Instructor-Led Courseware to one (1) End User attending the Authorized Training Session and only immediately prior to the commencement of the Authorized Training Session that is the subject matter of the Microsoft Instructor-Led Courseware provided, **or**
      2. provide one (1) End User attending the Authorized Training Session with the unique redemption code and instructions on how they can access one (1) digital version of the Microsoft Instructor-Led Courseware, **or**
      3. you will provide one (1) MCT with the unique redemption code and instructions on how they can access one (1) Trainer Content.
   3. For each license you acquire, you must comply with the following:
      1. you will only provide access to the Licensed Content to those individuals who have acquired a valid license to the Licensed Content,
      2. you will ensure that each End User attending an Authorized Training Session has their own valid licensed copy of the Microsoft Instructor-Led Courseware that is the subject of the Authorized Training Session,
      3. you will ensure that each End User provided with a hard-copy version of the Microsoft Instructor-Led Courseware will be presented with a copy of this agreement and each End User will agree that their use of the Microsoft Instructor-Led Courseware will be subject to the terms in this agreement prior to providing them with the Microsoft Instructor-Led Courseware. Each individual will be required to denote their acceptance of this agreement in a manner that is enforceable under local law prior to their accessing the Microsoft Instructor-Led Courseware,

4. you will ensure that each MCT teaching an Authorized Training Session has their own valid licensed copy of the Trainer Content that is the subject of the Authorized Training Session,
5. you will only use qualified MCTs who also hold the applicable Microsoft Certification credential that is the subject of the MOC title being taught for all your Authorized Training Sessions using MOC,
6. you will only provide access to the Microsoft Instructor-Led Courseware to End Users, and
7. you will only provide access to the Trainer Content to MCTs.

3. **If you are a MPN Member:**
   1. Each license acquired on behalf of yourself may only be used to review one (1) copy of the Microsoft Instructor-Led Courseware in the form provided to you. If the Microsoft Instructor-Led Courseware is in digital format, you may install one (1) copy on up to three (3) Personal Devices. You may not install the Microsoft Instructor-Led Courseware on a device you do not own or control.
   2. For each license you acquire on behalf of an End User or Trainer, you may either:
      1. distribute one (1) hard copy version of the Microsoft Instructor-Led Courseware to one (1) End User attending the Private Training Session, and only immediately prior to the commencement of the Private Training Session that is the subject matter of the Microsoft Instructor-Led Courseware being provided, **or**
      2. provide one (1) End User who is attending the Private Training Session with the unique redemption code and instructions on how they can access one (1) digital version of the Microsoft Instructor-Led Courseware, **or**
      3. you will provide one (1) Trainer who is teaching the Private Training Session with the unique redemption code and instructions on how they can access one (1) Trainer Content.
   3. For each license you acquire, you must comply with the following:
      1. you will only provide access to the Licensed Content to those individuals who have acquired a valid license to the Licensed Content,
      2. you will ensure that each End User attending an Private Training Session has their own valid licensed copy of the Microsoft Instructor-Led Courseware that is the subject of the Private Training Session,
      3. you will ensure that each End User provided with a hard copy version of the Microsoft Instructor-Led Courseware will be presented with a copy of this agreement and each End User will agree that their use of the Microsoft Instructor-Led Courseware will be subject to the terms in this agreement prior to providing them with the Microsoft Instructor-Led Courseware. Each individual will be required to denote their acceptance of this agreement in a manner that is enforceable under local law prior to their accessing the Microsoft Instructor-Led Courseware,
      4. you will ensure that each Trainer teaching an Private Training Session has their own valid licensed copy of the Trainer Content that is the subject of the Private Training Session,

5. you will only use qualified Trainers who hold the applicable Microsoft Certification credential that is the subject of the Microsoft Instructor-Led Courseware being taught for all your Private Training Sessions,
6. you will only use qualified MCTs who hold the applicable Microsoft Certification credential that is the subject of the MOC title being taught for all your Private Training Sessions using MOC,
7. you will only provide access to the Microsoft Instructor-Led Courseware to End Users, and
8. you will only provide access to the Trainer Content to Trainers.

4. **If you are an End User:**
   For each license you acquire, you may use the Microsoft Instructor-Led Courseware solely for your personal training use. If the Microsoft Instructor-Led Courseware is in digital format, you may access the Microsoft Instructor-Led Courseware online using the unique redemption code provided to you by the training provider and install and use one (1) copy of the Microsoft Instructor-Led Courseware on up to three (3) Personal Devices. You may also print one (1) copy of the Microsoft Instructor-Led Courseware. You may not install the Microsoft Instructor-Led Courseware on a device you do not own or control.
5. **If you are a Trainer.**
   1. For each license you acquire, you may install and use one (1) copy of the Trainer Content in the form provided to you on one (1) Personal Device solely to prepare and deliver an Authorized Training Session or Private Training Session, and install one (1) additional copy on another Personal Device as a backup copy, which may be used only to reinstall the Trainer Content. You may not install or use a copy of the Trainer Content on a device you do not own or control. You may also print one (1) copy of the Trainer Content solely to prepare for and deliver an Authorized Training Session or Private Training Session.
   2. If you are an MCT, you may customize the written portions of the Trainer Content that are logically associated with instruction of a training session in accordance with the most recent version of the MCT agreement.
   3. If you elect to exercise the foregoing rights, you agree to comply with the following: (i) customizations may only be used for teaching Authorized Training Sessions and Private Training Sessions, and (ii) all customizations will comply with this agreement. For clarity, any use of "customize" refers only to changing the order of slides and content, and/or not using all the slides or content, it does not mean changing or modifying any slide or content.

- 2.2 **Separation of Components.** The Licensed Content is licensed as a single unit and you may not separate their components and install them on different devices.
- 2.3 **Redistribution of Licensed Content.** Except as expressly provided in the use rights above, you may not distribute any Licensed Content or any portion thereof (including any permitted modifications) to any third parties without the express written permission of Microsoft.
- 2.4 **Third Party Notices.** The Licensed Content may include third party code that Microsoft, not the third party, licenses to you under this agreement. Notices, if any, for the third party code are included for your information only.
- 2.5 **Additional Terms.** Some Licensed Content may contain components with additional terms, conditions, and licenses regarding its use. Any non-conflicting terms in those conditions and licenses also apply to your use of that respective component and supplements the terms described in this agreement.

3. **LICENSED CONTENT BASED ON PRE-RELEASE TECHNOLOGY.** If the Licensed Content's subject matter is based on a pre-release version of Microsoft technology ("**Pre-release**"), then in addition to the other provisions in this agreement, these terms also apply:

    1. **Pre-Release Licensed Content.** This Licensed Content subject matter is on the Pre-release version of the Microsoft technology. The technology may not work the way a final version of the technology will and we may change the technology for the final version. We also may not release a final version. Licensed Content based on the final version of the technology may not contain the same information as the Licensed Content based on the Pre-release version. Microsoft is under no obligation to provide you with any further content, including any Licensed Content based on the final version of the technology.

    2. **Feedback.** If you agree to give feedback about the Licensed Content to Microsoft, either directly or through its third party designee, you give to Microsoft without charge, the right to use, share and commercialize your feedback in any way and for any purpose. You also give to third parties, without charge, any patent rights needed for their products, technologies and services to use or interface with any specific parts of a Microsoft technology, Microsoft product, or service that includes the feedback. You will not give feedback that is subject to a license that requires Microsoft to license its technology, technologies, or products to third parties because we include your feedback in them. These rights survive this agreement.

    3. **Pre-release Term.** If you are an Microsoft Imagine Academy Program Member, Microsoft Learning Competency Member, MPN Member, Microsoft Learn for Educators – Validated Educator, or Trainer, you will cease using all copies of the Licensed Content on the Pre-release technology upon (i) the date which Microsoft informs you is the end date for using the Licensed Content on the Pre-release technology, or (ii) sixty (60) days after the commercial release of the technology that is the subject of the Licensed Content, whichever is earliest ("**Pre-release term**"). Upon expiration or termination of the Pre-release term, you will irretrievably delete and destroy all copies of the Licensed Content in your possession or under your control.

4. **SCOPE OF LICENSE.** The Licensed Content is licensed, not sold. This agreement only gives you some rights to use the Licensed Content. Microsoft reserves all other rights. Unless applicable law gives you more rights despite this limitation, you may use the Licensed Content only as expressly permitted in this agreement. In doing so, you must comply with any technical limitations in the Licensed Content that only allows you to use it in certain ways. Except as expressly permitted in this agreement, you may not:

    - access or allow any individual to access the Licensed Content if they have not acquired a valid license for the Licensed Content,
    - alter, remove or obscure any copyright or other protective notices (including watermarks), branding or identifications contained in the Licensed Content,
    - modify or create a derivative work of any Licensed Content,
    - publicly display, or make the Licensed Content available for others to access or use,
    - copy, print, install, sell, publish, transmit, lend, adapt, reuse, link to or post, make available or distribute the Licensed Content to any third party,
    - work around any technical limitations in the Licensed Content, or
    - reverse engineer, decompile, remove or otherwise thwart any protections or disassemble the Licensed Content except and only to the extent that applicable law expressly permits, despite this limitation.

5. **RESERVATION OF RIGHTS AND OWNERSHIP.** Microsoft reserves all rights not expressly granted to you in this agreement. The Licensed Content is protected by copyright and other intellectual property

laws and treaties. Microsoft or its suppliers own the title, copyright, and other intellectual property rights in the Licensed Content.

6. **EXPORT RESTRICTIONS.** The Licensed Content is subject to United States export laws and regulations. You must comply with all domestic and international export laws and regulations that apply to the Licensed Content. These laws include restrictions on destinations, end users and end use. For additional information, see www.microsoft.com/exporting.
7. **SUPPORT SERVICES.** Because the Licensed Content is provided "as is", we are not obligated to provide support services for it.
8. **TERMINATION.** Without prejudice to any other rights, Microsoft may terminate this agreement if you fail to comply with the terms and conditions of this agreement. Upon termination of this agreement for any reason, you will immediately stop all use of and delete and destroy all copies of the Licensed Content in your possession or under your control.
9. **LINKS TO THIRD PARTY SITES.** You may link to third party sites through the use of the Licensed Content. The third party sites are not under the control of Microsoft, and Microsoft is not responsible for the contents of any third party sites, any links contained in third party sites, or any changes or updates to third party sites. Microsoft is not responsible for webcasting or any other form of transmission received from any third party sites. Microsoft is providing these links to third party sites to you only as a convenience, and the inclusion of any link does not imply an endorsement by Microsoft of the third party site.
10. **ENTIRE AGREEMENT.** This agreement, and any additional terms for the Trainer Content, updates and supplements are the entire agreement for the Licensed Content, updates and supplements.
11. **APPLICABLE LAW.**
    1. United States. If you acquired the Licensed Content in the United States, Washington state law governs the interpretation of this agreement and applies to claims for breach of it, regardless of conflict of laws principles. The laws of the state where you live govern all other claims, including claims under state consumer protection laws, unfair competition laws, and in tort.
    2. Outside the United States. If you acquired the Licensed Content in any other country, the laws of that country apply.
12. **LEGAL EFFECT.** This agreement describes certain legal rights. You may have other rights under the laws of your country. You may also have rights with respect to the party from whom you acquired the Licensed Content. This agreement does not change your rights under the laws of your country if the laws of your country do not permit it to do so.
13. **DISCLAIMER OF WARRANTY. THE LICENSED CONTENT IS LICENSED "AS-IS" AND "AS AVAILABLE." YOU BEAR THE RISK OF USING IT. MICROSOFT AND ITS RESPECTIVE AFFILIATES GIVES NO EXPRESS WARRANTIES, GUARANTEES, OR CONDITIONS. YOU MAY HAVE ADDITIONAL CONSUMER RIGHTS UNDER YOUR LOCAL LAWS WHICH THIS AGREEMENT CANNOT CHANGE. TO THE EXTENT PERMITTED UNDER YOUR LOCAL LAWS, MICROSOFT AND ITS RESPECTIVE AFFILIATES EXCLUDES ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT.**
14. **LIMITATION ON AND EXCLUSION OF REMEDIES AND DAMAGES. YOU CAN RECOVER FROM MICROSOFT, ITS RESPECTIVE AFFILIATES AND ITS SUPPLIERS ONLY DIRECT DAMAGES UP TO US$5.00. YOU CANNOT RECOVER ANY OTHER DAMAGES, INCLUDING CONSEQUENTIAL, LOST PROFITS, SPECIAL, INDIRECT OR INCIDENTAL DAMAGES.**

This limitation applies to

- anything related to the Licensed Content, services, content (including code) on third party Internet sites or third-party programs; and
- claims for breach of contract, breach of warranty, guarantee or condition, strict liability, negligence, or other tort to the extent permitted by applicable law.

It also applies even if Microsoft knew or should have known about the possibility of the damages. The above limitation or exclusion may not apply to you because your country may not allow the exclusion or limitation of incidental, consequential, or other damages.

Please note: As this Licensed Content is distributed in Quebec, Canada, some of the clauses in this agreement are provided below in French.

Remarque : Ce le contenu sous licence étant distribué au Québec, Canada, certaines des clauses dans ce contrat sont fournies ci-dessous en français.

EXONÉRATION DE GARANTIE. Le contenu sous licence visé par une licence est offert « tel quel ». Toute utilisation de ce contenu sous licence est à votre seule risque et péril. Microsoft n'accorde aucune autre garantie expresse. Vous pouvez bénéficier de droits additionnels en vertu du droit local sur la protection dues consommateurs, que ce contrat ne peut modifier. La ou elles sont permises par le droit locale, les garanties implicites de qualité marchande, d'adéquation à un usage particulier et d'absence de contre-façon sont exclues.

LIMITATION DES DOMMAGES-INTÉRÊTS ET EXCLUSION DE RESPONSABILITÉ POUR LES DOMMAGES. Vous pouvez obtenir de Microsoft et de ses fournisseurs une indemnisation en cas de dommages directs uniquement à hauteur de 5,00 $ US. Vous ne pouvez prétendre à aucune indemnisation pour les autres dommages, y compris les dommages spéciaux, indirects ou accessoires et pertes de bénéfices.

Cette limitation concerne:

- tout ce qui est relié au le contenu sous licence, aux services ou au contenu (y compris le code) figurant sur des sites Internet tiers ou dans des programmes tiers; et.
- les réclamations au titre de violation de contrat ou de garantie, ou au titre de responsabilité stricte, de négligence ou d'une autre faute dans la limite autorisée par la loi en vigueur.

Elle s'applique également, même si Microsoft connaissait ou devrait connaître l'éventualité d'un tel dommage. Si votre pays n'autorise pas l'exclusion ou la limitation de responsabilité pour les dommages indirects, accessoires ou de quelque nature que ce soit, il se peut que la limitation ou l'exclusion ci-dessus ne s'appliquera pas à votre égard.

EFFET JURIDIQUE. Le présent contrat décrit certains droits juridiques. Vous pourriez avoir d'autres droits prévus par les lois de votre pays. Le présent contrat ne modifie pas les droits que vous confèrent les lois de votre pays si celles-ci ne le permettent pas.

Revised April 2019

Contents

Module 0 Introduction to Auto-assembly usage 1
Welcome to Microsoft Cybersecurity Architect 1

Module 1 Design a Zero Trust strategy and architecture 5
Build an overall security strategy and architecture 5
Design a security operations strategy 32
Design an identity security strategy 77
Knowledge check 112

Module 2 Evaluate Governance Risk Compliance (GRC)strategies 117
Evaluate a regulatory compliance strategy 117
Evaluate security posture 135
Knowledge check 162

Module 3 Design security for infrastructure 167
Understand architecture best practices and how they are changing with the Cloud 167
Design a strategy for securing server and client endpoints 183
Design a strategy for securing PaaS, IaaS, and SaaS services 207
Knowledge check 232

Module 4 Design a strategy for data and applications 241
Specify security requirements for applications 241
Design a strategy for securing data 256
Knowledge check 283

Module 0 Introduction to Auto-assembly usage

Welcome to Microsoft Cybersecurity Architect

About this course

Course Description

The Microsoft cybersecurity architect has subject matter expertise in designing and evolving the cybersecurity strategy to protect an organization's mission and business processes across all aspects of the enterprise architecture. The cybersecurity architect designs a Zero Trust strategy and architecture, including security strategies for data, applications, access management, identity, and infrastructure. The cybersecurity architect also evaluates Governance Risk Compliance (GRC) technical strategies and security operations strategies.

The cybersecurity architect continuously collaborates with leaders and practitioners in IT security, privacy, and other roles across an organization to plan and implement a cybersecurity strategy that meets the business needs of an organization.

Level

Advanced

Audience

A candidate for this certification should have advanced experience and knowledge in a wide range of security engineering areas including identity and access, platform protection, security operations, securing data and securing applications. They should also have experience with hybrid and cloud implementations.

To earn the Microsoft Cybersecurity Architect certification, candidates must also pass one of the following exams: SC-200, SC-300, AZ-500, or MS-500. We strongly recommend that you do this before taking this exam.

Prerequisites

- Basic understanding of Microsoft 365

- Fundamental understanding of Microsoft security, compliance, and identity products
- Intermediate understanding of Windows 10
- Familiarity with Azure services, specifically Azure SQL Database and Azure Storage
- Familiarity with Azure virtual machines and virtual networking
- Basic understanding of scripting concepts.

Expected learning

Module 1:

- Develop Integration points in an architecture
- Develop security requirements based on business goals
- Translate security requirements into technical capabilities
- Design security for a resiliency strategy
- Design security strategy for hybrid and multi-tenant environments
- Design technical and governance strategies for traffic filtering and segmentation
- Design a logging and auditing security strategy
- Develop security operations for hybrid and multi-cloud environments
- Design a strategy for Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR)
- Evaluate security workflows
- Review security strategies for incident management
- Evaluate security operations for technical threat intelligence
- Recommend an identity store for security
- Recommend secure authentication and security authorization strategies
- Secure conditional access
- Design a strategy for role assignment and delegation
- Define Identity governance for access reviews and entitlement management
- Design a security strategy for privileged role access to infrastructure
- Design a security strategy for privileged access
- Monitor sources for insights on threats and mitigations. Develop Integration points in an architecture.

Module 2:

- Interpret compliance requirements and their technical capabilities.
- Evaluate infrastructure compliance by using Microsoft Defender for Cloud.
- Interpret compliance scores and recommend actions to resolve issues or improve security.
- Design and validate implementation of Azure Policy.
- Design for data residency Requirements.
- Translate privacy requirements into requirements for security solutions.
- Evaluate security postures by using benchmarks

- Evaluate security postures by using Microsoft Defender for Cloud
- Evaluate security postures by using Secure Scores
- Evaluate security hygiene of Cloud Workloads
- Design security for an Azure Landing Zone
- Interpret technical threat intelligence and recommend risk mitigations
- Recommend security capabilities or controls to mitigate identified risks

Module 3:

- Plan and implement a security strategy across teams
- Establish a strategy and process for proactive and continuous evaluation of security strategy
- Specify security baselines for server and client endpoints
- Specify security requirements for servers
- Specify security requirements for mobile devices and clients
- Specify requirements for securing Active Directory Domain Services
- Design a strategy to manage secrets, keys, and certificates
- Design a strategy for secure remote access
- Understand security operations frameworks, processes, and procedures
- Understand deep forensics procedures by resource type
- Specify security baselines for PaaS services
- Specify security baselines for IaaS services
- Specify security baselines for SaaS services
- Specify security requirements for IoT workloads
- Specify security requirements for data workloads
- Specify security requirements for web workloads
- Specify security requirements for storage workloads
- Specify security requirements for containers
- Specify security requirements for container orchestration

Module 4:

- Specify a security strategy for applications and APIs
- Specify priorities for mitigating threats to applications
- Specify a security standard for onboarding a new application
- Prioritize mitigating threats to data
- Design a strategy to identify and protect sensitive data
- Specify an encryption standard for data at rest and in motion

Module 1 Design a Zero Trust strategy and architecture

Build an overall security strategy and architecture

Introduction

In this module, you'll learn how to:

- Develop Integration points in an architecture
- Develop security requirements based on business goals
- Translate security requirements into technical capabilities
- Design security for a resiliency strategy
- Design security strategy for hybrid and multi-tenant environments
- Design technical and governance strategies for traffic filtering and segmentation

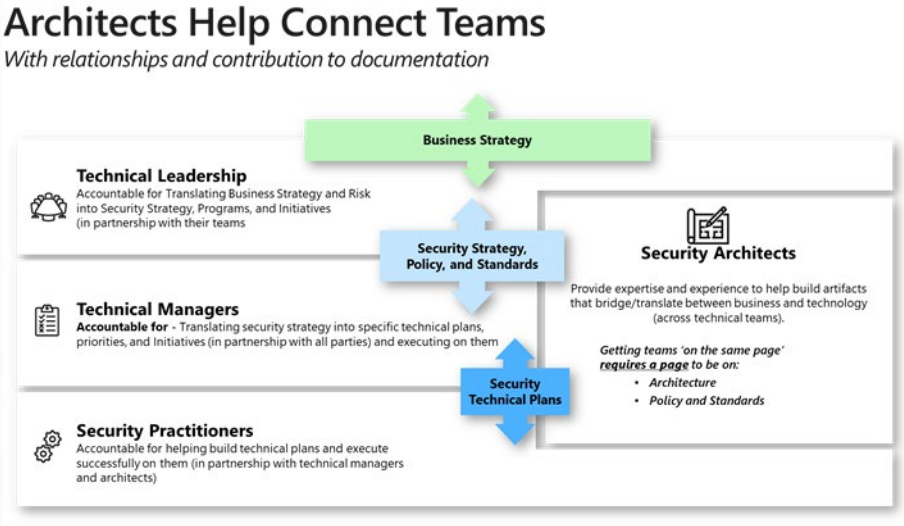
The content in the module will help you prepare for Exam SC-100: Cybersecurity Architecture. The module concepts are covered in:

- Design a Zero Trust Strategy and Architecture
- Build an Overall Security Strategy and Architecture

Prerequisites

- Conceptual knowledge of security policies, requirements, zero trust architecture, and management of hybrid environments
- Working experience with zero trust strategies, applying security policies, and developing security requirements based on business goals

Role of Security Architecture



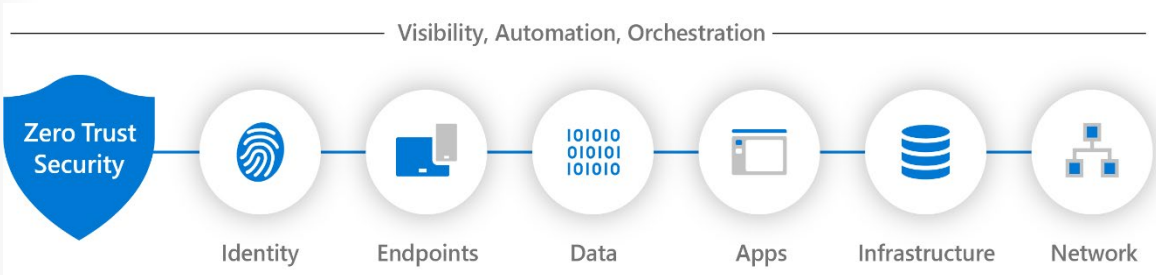
What is a Security Architect?

Security Architects are responsible for designing, building, and maintaining the security functions of an organization's IT environment. Security Architects help translate an organization's business and assurance goals into a security vision, providing documentation and diagrams to guide technical security decisions. They are responsible for ensuring that the information security requirements necessary to protect the organization's core missions and business processes are adequately addressed in all aspects of enterprise architecture, including reference models, segment and solution architectures, and the resulting information systems supporting those missions and business processes.

Zero Trust overview

Today, organizations need a new security model that effectively adapts to the complexity of the modern environment, embraces the mobile workforce, and protects people, devices, applications, and data wherever they're located.

This is the core of **Zero Trust**. Instead of believing everything behind the corporate firewall is safe, the Zero Trust model assumes breach, and verifies each request as though it originated from an uncontrolled network. Regardless of where the request originates or what resource it accesses, the Zero Trust model teaches us to "never trust, always verify."



Guiding principles of Zero Trust

Verify explicitly - Protect assets against attacker control by explicitly validating that all trust and security decisions use all relevant available information and telemetry. | Limit access of a potentially compromised asset with just-in-time and just-enough-access (JIT/JEA) and risk-based policies like adaptive access control. | Assume attackers can and will successfully attack anything in the system (identity, network, device, app, infrastructure, etc.) and plan accordingly. |

Use least privilege access - A Zero Trust approach should extend throughout the entire digital estate and serve as an integrated security philosophy and end-to-end strategy. This is done by implementing Zero Trust controls and technologies across six foundational elements. Each of these is a source of signal, a control plane for enforcement, and a critical resource to be defended.

Assume breach - Different organizational requirements, existing technology implementations, and security stages all affect how a Zero Trust security model implementation is planned. Using our experience in helping customers to secure their organizations, as well as in implementing our own Zero Trust model, we've developed the following guidance to assess your readiness and to help you build a plan to get to Zero Trust.

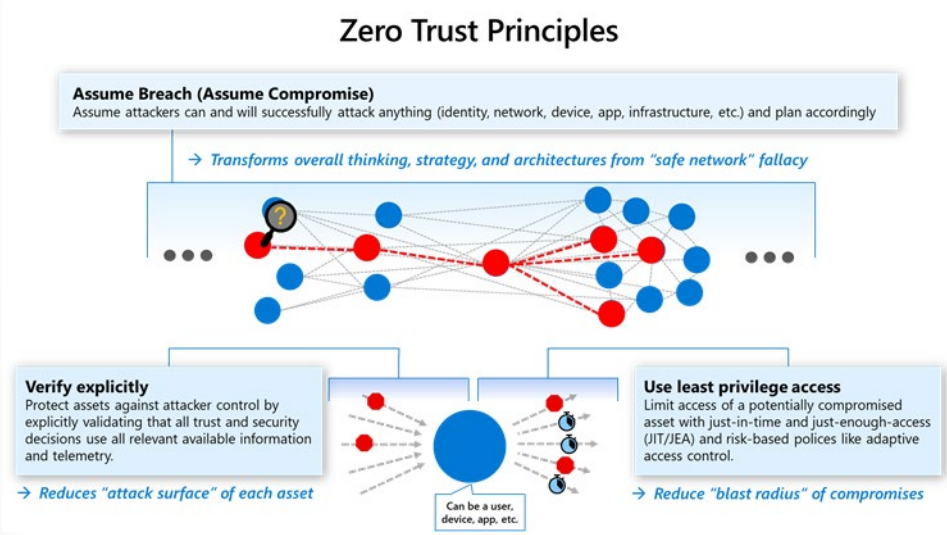
Technology pillars of Zero Trust

The Zero Trust approach can be organized around key technological pillars:

- **Secure identity with Zero Trust** - Identities, whether they represent people, services, or IoT devices—define the Zero Trust control plane. When an identity attempts to access a resource, verify that identity with strong authentication, and ensure access is compliant and typical for that identity. Follow least privilege access principles.
- **Secure endpoints with Zero Trust** - Once an identity has been granted access to a resource, data can flow to a variety of different endpoints—from IOT devices to smartphones, BYOD to partner-managed devices,
  and on-premises workloads to cloud-hosted servers. This diversity creates a massive attack surface area. Monitor and enforce device health and compliance for secure access.
- **Secure applications with Zero Trust** - Applications and APIs provide the interface by which data is consumed. They may be legacy on-premises, lifted-and-shifted to cloud workloads, or modern SaaS applications. Apply controls and technologies to discover shadow IT, ensure appropriate in-app permissions,
  ate access based on real-time analytics, monitor for abnormal behavior, control user actions, and validate secure configuration options.
- **Secure data with Zero Trust** - Ultimately, security teams are protecting data. Where possible, data should remain safe even if it leaves the devices, apps, infrastructure, and networks the organization controls. Classify, label, and encrypt data, and restrict access based on those attributes.
- **Secure infrastructure with Zero Trust** - Infrastructure—whether on-premises servers, cloud-based VMs, containers, or micro-services — represents a critical threat vector. Assess version, configuration, and JIT access to harden defense. Use telemetry to detect attacks and anomalies, and automatically block and flag risky behavior and take protective actions.
- **Secure networks with Zero Trust** - All data is ultimately accessed over network infrastructure. Networking controls can provide critical controls to enhance visibility and help prevent attackers from moving laterally across the network. Segment networks (and do deeper in-network micro-segmentation) and
  deploy real-time threat protection, end-to-end encryption, monitoring, and analytics.

- **Visibility, automation, and orchestration with Zero Trust** - In our Zero Trust guides, we define the approach to implement an end-to-end Zero Trust methodology across identities, endpoints and devices, data, apps, infrastructure, and network. These activities increase your visibility, which gives you better data for making trust decisions. With each Of these individual areas generating their own relevant alerts, we
  need an integrated capability to manage the resulting influx of data to better defend against threats and validate trust in a transaction.

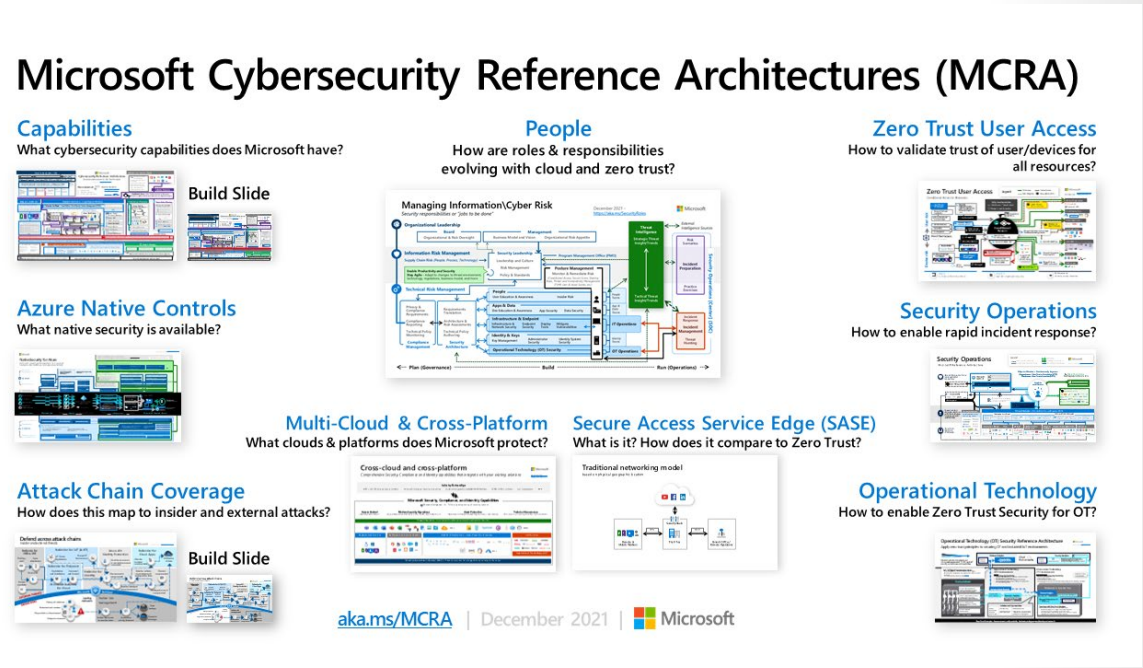
The following diagram visually illustrates the zero trust principles:



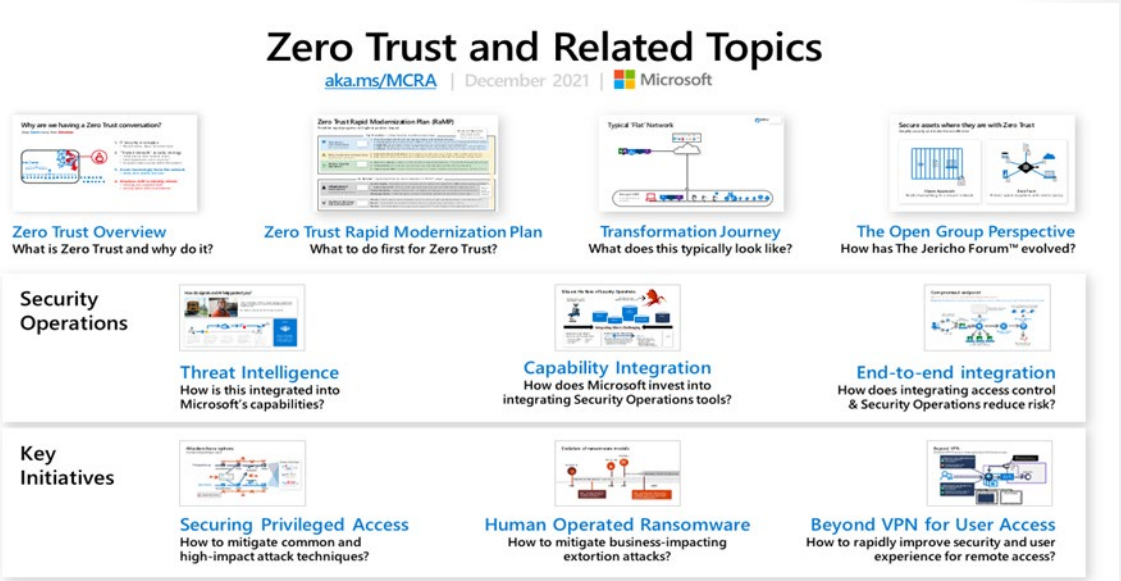
Develop integration points in an architecture

The Microsoft Cybersecurity Reference Architectures (MCRA) describe Microsoft's cybersecurity capabilities. The reference architectures describe how Microsoft security capabilities integrate with Microsoft services and applications, Microsoft cloud platforms such as Azure and Microsoft 365 third party apps such as ServiceNow and Salesforce, and third party platforms such as Amazon Web Services (AWS) and Google Cloud Platform (GCP).

The reference architectures are primarily composed of detailed technical diagrams on Microsoft cybersecurity capabilities, zero trust user access, security operations, operational technology (OT), multi-cloud and cross-platform capabilities, attack chain coverage, Azure native security controls, and security organizational functions.



The MCRA also includes an overview of Zero Trust and a Zero Trust rapid modernization plan (RaMP). Additionally, this includes other key information on security operations and key initiatives like protecting from human operated ransomware, securing privileged access, moving beyond VPN, and more.



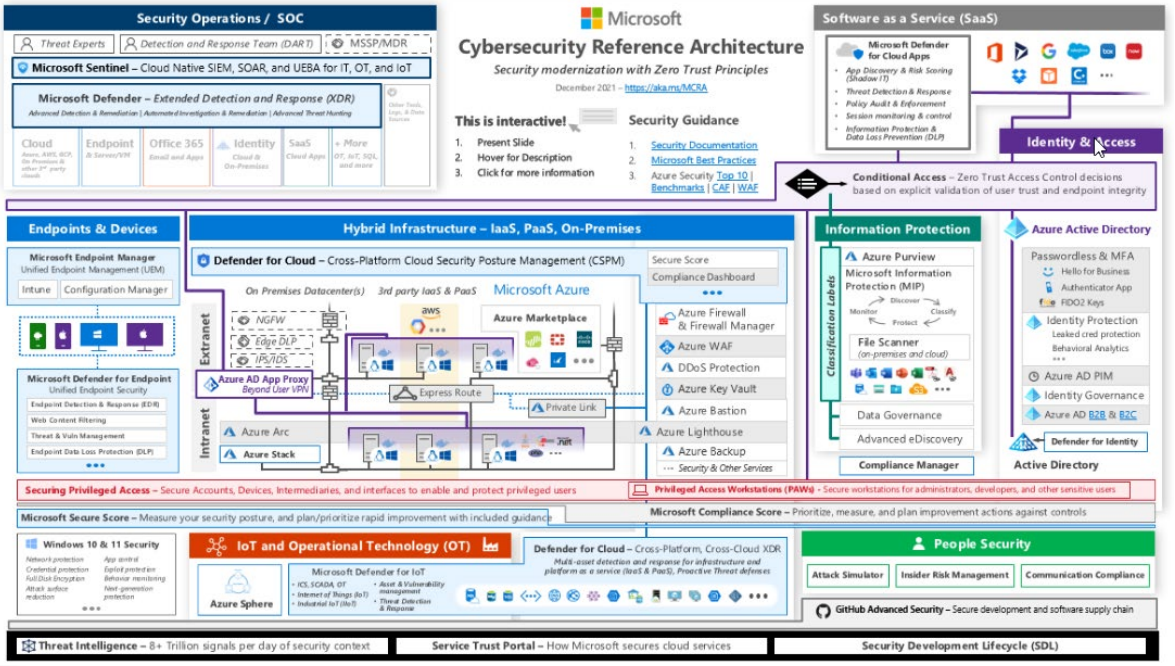
Using the MCRA

MCRA is used for several purposes, including:

- Starting template for a security architecture: The most common use case is to help organizations define a target state for cybersecurity capabilities. Organizations find this architecture useful because it covers capabilities across the modern enterprise estate that now spans on-premise, mobile devices, multiple clouds, and IoT / Operational Technology.

- Comparison reference of security capabilities: Some organizations use MCRA to compare Microsoft's architecture recommendations with what they already own and have implemented. Many organizations find that they weren't aware that they already own quite a bit of security architecture technology.
- Learn about Microsoft's integration investments: MCRA helps architects and technical teams identify how to take advantage of integration points within Microsoft capabilities and existing security capabilities.
- Learn about cybersecurity: Some architects, particularly those new to cybersecurity, use this as a learning tool to prepare for their first career or a career change.

The primary Cybersecurity Reference Architecture diagram represents the full organizational security landscape, demonstrating how key Microsoft technologies fit into that landscape.



The table below reproduces the information from the diagram showing each domain, the Microsoft products within it, a summary of the capability and some additional details.

Domain	Product	Capability	Details
Identity and Access			
	Azure Active Directory	Cloud-based Identity, Access Management Service	Password-less & MFA, Hello for Business, Authenticator App, RDO2 Keys, Azure AD PIM, B2B & B2C
	Identity Protection	Leaked Credential Protection	Behavioral Analytics

Domain	Product	Capability	Details
	Identity Governance	Identity, Access, and Privileged Access Lifecycle, Entitlement Management, Access Requests, Workflow, Policy and Role Management, Governance Enforcement	Azure AD User Provisioning, Azure AD PIM, Azure AD Reports, and Enterprise Mobility+Security
	Defender for Identity	User Behavior and Activities, Investigate Alerts, AD FS Protection, Lateral Movement Detection	AD, Azure AD, SecOps, ADFS,
Security Operations			
	Microsoft Defender	Extended Detection and Response (XDR)	Cloud, Endpoint, Office 365, Identity, SaaS
	Microsoft Sentinel	Cloud Native SIEM, SOAR, and UEBA for IT, OT and IoT	Same as Defender + other Tools, logs and data sources
Endpoint and Device Security			
	Microsoft Endpoint Manager	Unified Endpoint Management	Intune and Configuration Manager
	Microsoft Defender for Endpoint	Unified Endpoint Security	Endpoint Detection and Response (EDR), Web Content Filtering, Threat and Vulnerability management, Endpoint Data Loss protection (DLP)
Hybrid Infrastructure			
	Defender for Cloud	Security Posture Management, Threat Protection	Cross Platform, Cross Cloud XDR
	Azure AD App Proxy	Secure Remote Access	Azure AD, Web Applications, SSO
	Azure Arc	Hybrid and Multi-cloud Management	Azure Security, Cloud-Native Services, Windows, Linux, SQL Server, Kubernetes
	Azure Stack	Hybrid and Edge Computing	Edge, IoT, Network, Machine Learning, Datacenter

Domain	Product	Capability	Details
	Azure Firewall	Intelligent Network Firewall	Azure, Networking Services, Security, TLS Inspection, IDPS, URL Filtering, Web Categories
	Azure WAF	Intelligent Application Firewall	Azure AD, Web Applications
	DDoS Protection	DDoS Mitigation	Azure, Networking Services, Virtual Networks
	Azure Key Vault	Encryption, Authentication, Secrets Management,	Azure, Azure AD, Enterprise Application
	Azure Bastion	Separate Administration Workstation	PaaS, Secure RDP/SSH, Secure VM
	Azure Lighthouse	Azure Delegated Resource Management, Azure Resources Templates, Managed Service	Cross-Tenant Management, Azure Identity, Azure Resource Manager
	Azure Backup	On-Premises and Cloud Backup Solution	On-Premises, Azure VMs, Azure Managed Disks, Azure Files Shares, SQL Server in Azure VMs, SAP Hanna Databases, Azure Database for PostgreSQL Servers, Azure Blobs
	Express Route	On-Premises Network Extension	Layer 3 Connectivity, Connectivity to Microsoft Cloud Services, Global Connectivity to Microsoft Services, Dynamic Routing, Built-In Redundancy
	Private Link	Private Azure Access, On-Premises and Peered Networks, Data Leakage Protection	PaaS, Storage, SQL Databases, Network
Information Protection			
	Azure Purview	Unified Data Governance, Automated Data Discovery, Sensitive Data Classification	Microsoft Information Protection (MIP), File Scanner, Data Governance, eDiscovery (Premium)

Domain	Product	Capability	Details
	Compliance Manager	Pre-Built Assessments, Workflow, Risk-Based Compliance Score	Azure Controls, Assessments, Templates, Improvement Actions
People Security			
	Attack Simulator	Simulation Training Platform	Credential Harvest, Malware Attachment, Link in Attachment, Link to Malware, Drive-by-URL
	Insider Risk Management	Compliance Solution, Data Leak, Workflow	Policies, Alerts, Triage, Investigation, Action
	Communication Compliance	Insider Risk Solution, Flexible Remediation Workflows, Actionable Insights, Customizable Templates	Corporate Policies, Risk Management, Regulatory Compliance
IoT and Operational Technology			
	Azure Sphere	IoT and OT Security Services	Micro-controller Unit (MCU, Networking Services, Patch Management,
	Defender for Cloud	Security Posture Management, Threat Protection	Cross Platform, Cross Cloud XDR
	Defender for IoT	Asset Discovery, Vulnerability Management, Network Detection and Response (NDR)	IoT, SCADA, OT, Threat Detection & Response, Asset & Vulnerability Management

Develop security requirements based on business goals

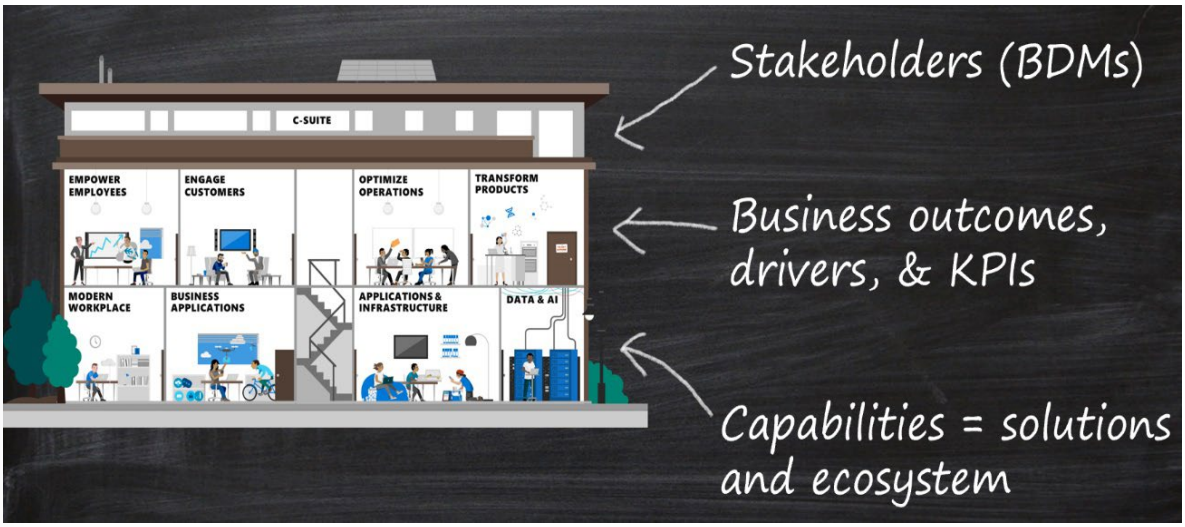
The most successful transformation journeys start with business goals. Cloud adoption can be a costly and time-consuming effort. Fostering the right level of support from IT and other areas of the business is crucial to success. This topic is designed to help customers identify business outcomes that are concise, defined, and drive observable results or change in business performance, supported by a specific measure.

During any cloud transformation, the ability to speak in terms of business outcomes supports transparency and cross-functional partnerships. The business outcome framework starts with a simple template to help technically minded individuals document and gain consensus. This template can be used with business stakeholders to collect a variety of business outcomes, which could each be influenced by a company's transformation journey.

In this template, business outcomes focus on three topics:

- Aligning to stakeholders or business decision makers

- Understanding business drivers and objectives
- Mapping outcomes to specific solutions and technical capabilities



The business outcome template focuses on simplified conversations that can quickly engage stakeholders without getting too deep into the technical solution. By rapidly understanding and aligning the key performance indicators (KPIs) and business drivers that are important to stakeholders, architects can consider about high-level approaches and transformations before implementing security solutions.

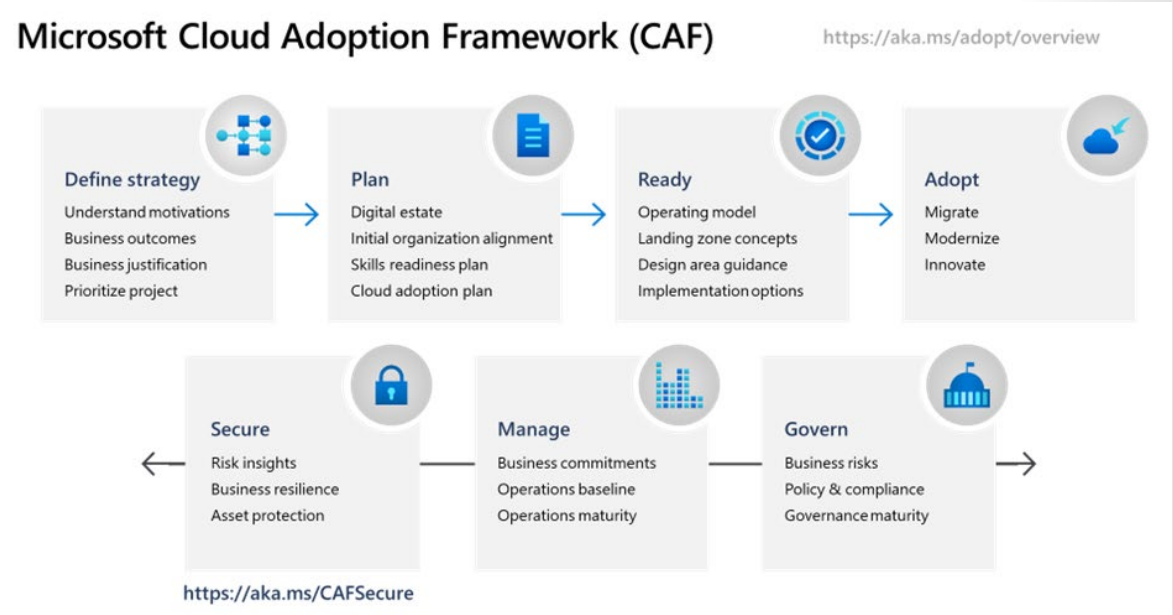
Cloud Adoption Framework

Media:Accelerate your cloud adoption journey by using the Cloud Adoption Framework for Azure - Learn[1]

As mentioned in the video, Cloud Adoption Framework consists of tools, documentation, and proven practices. The Cloud Adoption Framework includes these stages:

- Define your strategy
- Make a plan
- Ready your organization
- Adopt the cloud
- Govern and manage your cloud environments

1 https://docs.microsoft.com/learn/modules/build-cloud-governance-strategy-azure/9-accelerate-cloud-adoption-framework



The govern stage focuses on cloud governance. You can refer to the Cloud Adoption Framework for recommended guidance as you build your cloud governance strategy.

To help build your adoption strategy, the Cloud Adoption Framework breaks out each stage into further exercises and steps. Let's take a brief look at each stage.

Define your strategy

Here, you answer why you're moving to the cloud and what you want to get out of cloud migration. Do you need to scale to meet demand or reach new markets? Will it reduce costs or increase business agility? When defining your cloud business strategy, you should understand **cloud economics**[2] and consider the business impact, turnaround time, global reach, performance, and more. Here are the steps to define your cloud strategy:

1. **Define and document motivations**: Meeting with stakeholders and leadership can help you answer why you're moving to the cloud.
2. **Document business outcomes**: Meet with leadership from finance, marketing, sales, and human resource groups to help you document your goals.
3. **Evaluate financial considerations**: Measure objectives and identify the return expected from a specific investment.
4. **Understand technical considerations**: Evaluate technical considerations through the selection and completion of your first technical project.

Make a plan

Here, you build a plan that maps your aspirational goals to specific actions. A good plan helps ensure that your efforts map to the desired business outcomes. Here are steps to build a solid plan:

1. **Digital estate**: Create an inventory of the existing digital assets and workloads that you plan to migrate to the cloud.

2 https://azure.microsoft.com/overview/cloud-economics

2. **Initial organizational alignment**: Ensure the right people are involved in migration efforts, both from a technical standpoint as well as from a cloud governance standpoint.
3. **Skills readiness plan**: Build a plan that helps individuals build the skills they need to operate in the cloud.
4. **Cloud adoption plan**: Build a comprehensive plan that brings together the development, operations, and business teams toward a shared cloud adoption goal.

Ready your organization

Here, you create a *landing zone* or an environment in the cloud to begin hosting your workloads. Here are steps to ready your organization:

1. **Azure setup guide**: Review the Azure setup guide to become familiar with the tools and approaches you need to use to create a landing zone.
2. **Azure landing zone**: Begin to build out the Azure subscriptions that support each of the major areas of your business. A landing zone includes cloud infrastructure as well as governance, accounting, and security capabilities.
3. **Expand the landing zone**: Refine your landing zone to ensure that it meets your operations, governance, and security needs.
4. **Best practices**: Start with recommended and proven practices to help ensure that your cloud migration efforts are scalable and maintainable.

Adopt the cloud

Here, you begin to migrate your applications to the cloud. Along the way, you might find ways to modernize your applications and build innovative solutions that use cloud services. The Cloud Adoption Framework breaks this stage into two parts: migrate and innovate.

Migrate

Here are the steps in the migrate process of this stage:

1. **Migrate your first workload**: Use the Azure migration guide to deploy your first project to the cloud.
2. **Migration scenarios**: Use additional in-depth guides to explore more complex migration scenarios.
3. **Best practices**: Check in with the Azure cloud migration best practices checklist to verify that you're following recommended practices.
4. **Process improvements**: Identify ways to make the migration process scale while requiring less effort.

Innovate

Here are the steps in the innovate process of this stage:

1. **Business value consensus**: Verify that investments in new innovations add value to the business and meet customer needs.
2. **Azure innovation guide**: Use this guide to accelerate development and build a minimum viable product (MVP) for your idea.
3. **Best practices**: Verify that your progress maps to recommended practices before moving forward.

4. **Feedback loops**: Check in frequently with your customers to verify that you're building what they need.

Govern and manage your cloud environments

Here, you begin to form your cloud governance and cloud management strategies. As the cloud estate changes over time, so do cloud governance processes and policies. You need to create resilient solutions that are constantly optimized.

Govern

Here are the steps in the govern process of this stage:

1. **Methodology**: Consider your end state solution. Then define a methodology that incrementally takes you from your first steps all the way to full cloud governance.
2. **Benchmark**: Use the **governance benchmark tool**[3] to assess your current state and future state to establish a vision for applying the framework.
3. **Initial governance foundation**: Create a Minimum Viable Product (MVP) that captures the first steps of your governance plan.
4. **Improve the initial governance foundation**: Iteratively add governance controls that address tangible risks as you progress toward your end state solution.

Manage

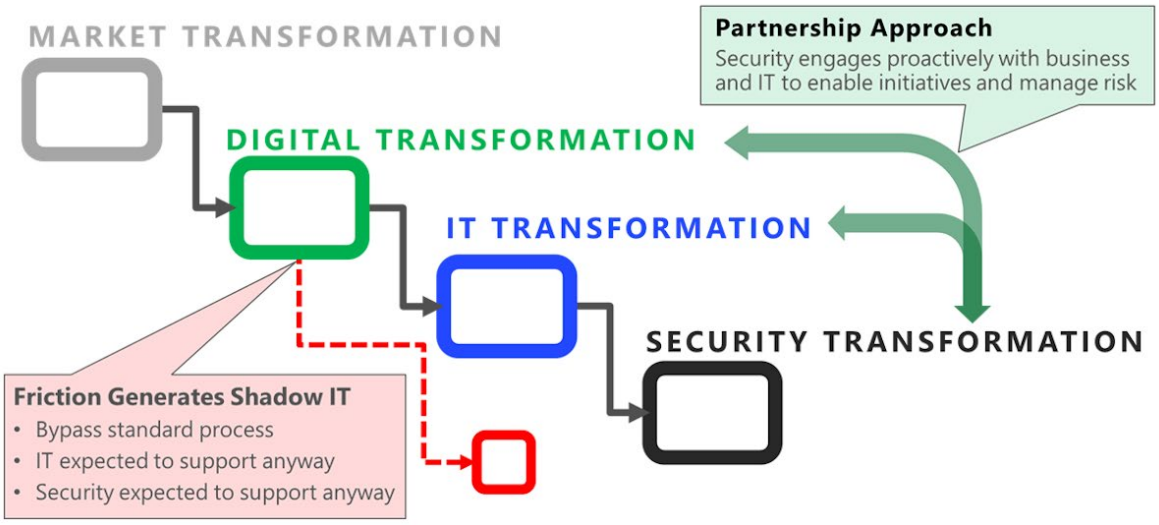
Here are the steps in the manage process of this stage:

1. **Establish a management baseline**: Define your minimum commitment to operations management. A management baseline is the minimum set of tools and processes that should be applied to every asset in an environment.
2. **Define business commitments**: Document supported workloads to establish operational commitments with the business and agree on cloud management investments for each workload.
3. **Expand the management baseline**: Apply recommended best practices to iterate on your initial management baseline.
4. **Advanced operations and design principles**: For workloads that require a higher level of business commitment, perform a deeper architecture review to deliver on your resiliency and reliability commitments.

Translate security requirements into technical capabilities

Many organizations are managing a chain of multiple simultaneous transformations in the organization. These internal transformations typically start because nearly all external markets are transforming to meet new customer preferences for mobile and cloud technologies. Organizations often face the competitive threat of new startups and the digital transformation of traditional competitors who can disrupt the market.

3 https://cafbaseline.com/



The internal transformation process typically includes:

- **Digital transformation** of the business to capture new opportunities and stay competitive against digital native startups
- **Technology transformation** of the IT organization to support the initiative with cloud services, modernized development practices, and related changes
- **Security transformation** to both adapt to the cloud and simultaneously address an increasingly sophisticated threat environment

Security design principles

Based on the organization's security transformation; enforcing security design principles is key to enforcing a Zero Trust architecture. Security design principles describe a securely architected system hosted on cloud or on-premises datacenters (or a combination of both). Application of these principles dramatically increases the likelihood your security architecture assures confidentiality, integrity, and availability.

To assess workloads using the tenets found in the Azure Well-Architected Framework, reference the **Microsoft Azure Well-Architected Review**[4].

The following design principles provide:

- Context for questions
- Why a certain aspect is important
- How an aspect is applicable to security

These critical design principles are used as lenses to assess the Security of an application deployed on Azure. These lenses provide a framework for the application assessment questions.

4 https://docs.microsoft.com/assessments/?id=azure-architecture-review&mode=pre-assessment

Plan resources and how to harden them

Recommendations:

- Consider security when planning workload resources
- Understand how individual cloud services are protected
- Use a service enablement framework to evaluate

Automate and use least privilege

Recommendations:

- Implement least privilege throughout the application and control plane to protect against data exfiltration and malicious actor scenarios
- Drive automation through DevSecOps to minimize the need for human interaction

Classify and encrypt data

Recommendations:

- Classify data according to risk
- Apply industry-standard encryption at rest and in transit, which ensures keys and certificates are stored securely and managed properly

Monitor system security, plan incident response

Recommendations:

- Correlate security and audit events to model application health
- Correlate security and audit events to identify active threats
- Establish automated and manual procedures to respond to incidents
- Use security information and event management (SIEM) tooling for tracking

Identify and protect endpoints

Recommendations:

- Monitor and protect the network integrity of internal and external endpoints through security appliances or Azure services, such a firewalls and web application firewalls
- Use industry standard approaches to protect against common attack vectors, such as distributed denial of service (DDoS) attacks like SlowLoris.

Protect against code-level vulnerabilities

Recommendations:

- Identify and mitigate code-level vulnerabilities, such as cross-site scripting and structured query language (SQL) injection.
- In the operational lifecycle, regularly incorporate:
    - Security fixes

- Codebase and dependency patching

Model and test against potential threats

Recommendations:

- Establish procedures to identify and mitigate known threats
- Use penetration testing to verify threat mitigation
- Use static code analysis to detect and prevent future vulnerabilities
- Use code scanning to detect and prevent future vulnerabilities

Design security for a resiliency strategy

Organization and enterprise application workloads have recovery time objective (RTO) and recovery point objective (RPO) requirements. Effective business continuity and disaster recovery (BCDR) design provides platform-level capabilities that meet these requirements. To design BCDR capabilities, capture platform disaster recovery (DR) requirements.

Design considerations

Consider the following factors when designing BCDR for application workloads:

- Application and data availability requirements:
  - RTO and RPO requirements for each workload
  - Support for active-active and active-passive availability patterns
- BCDR as a service for platform-as-a-service (PaaS) services:
  - Native DR and high-availability (HA) feature support
  - Geo-replication and DR capabilities for PaaS services
  - Support for multi-region deployments for failover, with component proximity for performance
  - Application operations with reduced functionality or degraded performance during an outage
  - Workload suitability for Availability Zones or availability sets
  - Data sharing and dependencies between zones
  - Availability Zones compared to availability sets impact on update domains
  - Percentage of workloads that can be under maintenance simultaneously
  - Availability Zones support for specific virtual machine (VM) stock-keeping units (SKUs); for example, Azure Ultra Disk Storage requires using Availability Zones
- Consistent backups for applications and data:
  - VM snapshots
  - Azure Backup Recovery Services vaults
  - Subscription limits restricting the number of Recovery Services vaults and the size of each vault

- Network connectivity if a failover occurs:
  - Bandwidth capacity planning for Azure ExpressRoute
  - Traffic routing during a regional, zonal, or network outage
- Planned and unplanned fail-overs:
  - IP address consistency requirements, and the potential need to maintain IP addresses after failover and failback
  - Maintaining engineering DevOps capabilities
  - Azure Key Vault DR for application keys, certificates, and secrets

Design recommendations

The following design practices support BCDR for application workloads:

- **Employ Azure Site Recovery for Azure-to-Azure VM DR scenarios** - Site Recovery uses real-time replication and recovery automation to replicate workloads across regions. Built-in platform capabilities for VM workloads meet low RPO and RTO requirements. You can use Site Recovery to run recovery drills without affecting production workloads. You can also use Azure Policy to enable replication and to audit VM protection.
- **Use native PaaS DR capabilities** - Built-in PaaS features simplify both design and deployment automation for replication and failover in workload architectures. Organizations that define service standards can also audit and enforce the service configuration through Azure Policy.
- **Use Azure-native backup capabilities** - Azure Backup and PaaS-native backup features remove the need for third-party backup software and infrastructure. As with other native features, you can set, audit, and enforce backup configurations with Azure Policy to ensure compliance with organization requirements.
- **Use multiple regions and peering locations for ExpressRoute connectivity** - A redundant hybrid network architecture can help ensure uninterrupted cross-premises connectivity if an outage affects an Azure region or peering provider location.
- **Avoid using overlapping IP address ranges for production and DR sites.** - Production DR networks that use the same classless interdomain routing blocks require a failover process that can complicate and delay application failover. When possible, plan for a BCDR network architecture that provides concurrent connectivity to all sites.

Overview of the reliability pillar

Reliability ensures applications can meet the commitments made to customers. Architecting resiliency into an application framework ensures workloads are available and can recover from failures at any scale.

Building for reliability includes ensuring a highly available architecture and recovering from failures such as data loss, major downtime, or ransomware incidents

To assess the reliability of a workload using the tenets found in the **Microsoft Azure Well-Architected Framework**[5], reference the **Microsoft Azure Well-Architected Review**[6].

5 https://docs.microsoft.com/azure/architecture/framework/
6 https://docs.microsoft.com/assessments/?id=azure-architecture-review&mode=pre-assessment

In traditional application development, there has been a focus on increasing the mean time between failures (MTBF). This effort was spent trying to prevent the system from failing. In cloud computing, a different mindset is required because of several factors:

- Distributed systems are complex, and a failure at one point can potentially cascade throughout the system
- Costs for cloud environments are kept low through commodity hardware, so occasional hardware failures should be expected
- Applications often depend on external services, which may become temporarily unavailable or throttle high-volume users
- Today's users expect an application to be available 24/7 without ever going offline

These factors mean that cloud applications must be designed to expect occasional failures and recover from them. Azure has many resiliency features already built into the platform. For example:

- Azure Storage, SQL Database, and Cosmos DB provide built-in data replication across availability zones and regions
- Azure managed disks are automatically placed in different storage scale units to limit the effects of hardware failures
- Virtual machines (VMs) are spread across several fault domains in an availability set. A *fault domain* is a group of VMs that share a common power source and network switch. Spreading VMs across fault domains limits the impact of physical hardware failures, network outages, or power interruptions
- Availability Zones are physically separate locations within each Azure region. Each zone comprises one or more data centers equipped with independent power, cooling, and networking infrastructure. With availability zones, one can design and operate applications and databases that automatically transition between zones without interruption, ensuring resiliency if one zone is affected. For more information, go to **Regions and Availability Zones in Azure**[7].

Design a security strategy for hybrid and multi-tenant environments

A hybrid deployment offers organizations the ability to extend the feature-rich experience and administrative control with their existing on-premises environment to the cloud. A hybrid deployment provides a single organization's seamless look and feel between an on-premises and cloud environment. A hybrid deployment can also serve as an intermediate step to moving completely to a cloud environment.

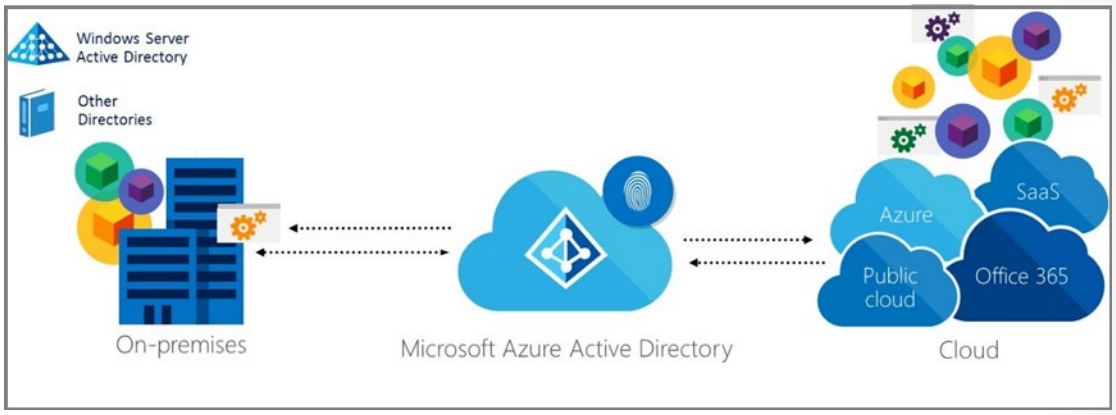
Implement a secure hybrid identity environment

Microsoft's identity solutions span on-premises and cloud-based capabilities, creating a single user identity for authentication and authorization to all resources, regardless of location. This concept is known as Hybrid Identity. There are different design and configuration options for hybrid identity using Microsoft solutions. In some cases, it might be difficult to determine which combination will best meet the needs of an organization.

The following graphic shows an example of a hybrid identity solution that enables IT Admins to integrate their current Windows Server Active

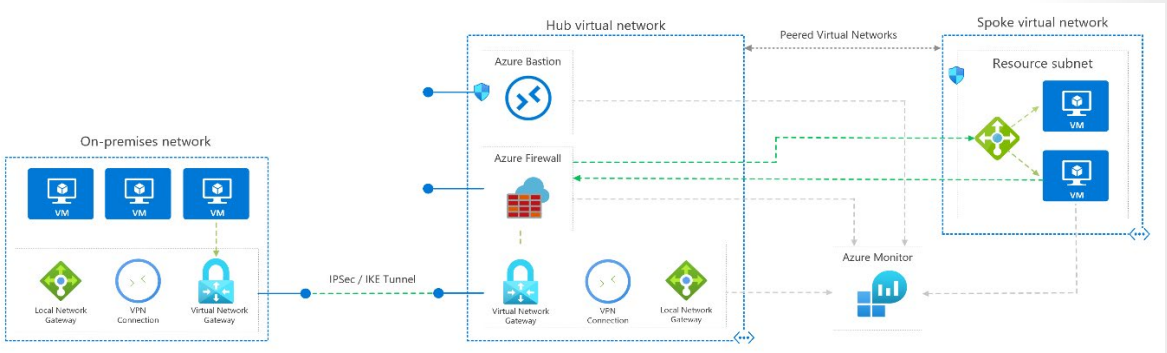
7 https://docs.microsoft.com/azure/availability-zones/az-overview

Directory solution located on-premises with Microsoft Azure Active Directory to enable users to use Single Sign-on (SSO) across applications located in the cloud and on-premises.



Implement a secure hybrid network

This reference architecture shows a secure hybrid network that extends an on-premises network to Azure. The architecture implements a DMZ, also called a *perimeter network*, between the on-premises network and an Azure virtual network. All inbound and outbound traffic passes through Azure Firewall.



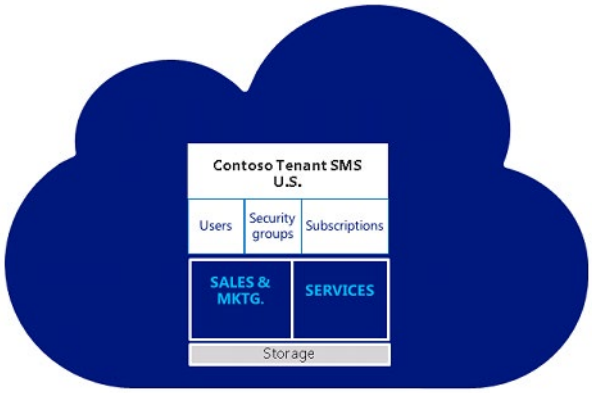
Use multiple online environments or tenants

The customer engagement apps (Dynamics 365 Sales, Dynamics 365 Customer Service, Dynamics 365 Field Service, Dynamics 365 Marketing, and Dynamics 365 Project Service Automation) provide options for segregating data and user access. For most companies, adding and using multiple environments in a subscription provides the right mix of functionality and ease of management. Enterprises with separate geographic locations might consider using multiple tenants to separate licenses. Multiple environments can share users among environments; multiple tenants can't.

Uses for multiple environments

A typical deployment includes one tenant only. A tenant can include one or more environments; however, an environment is always associated with a single tenant.

This example uses two environments for three teams: Sales, Marketing, and Services:



Sales and marketing share an environment so lead information can be easily accessed by both. Services has their own environment, so tickets and warranties can be managed separately from marketing campaigns and other related sales events.

Access to one or both environments can be provided easily. Sales and marketing users could be limited to their environment, while service users with extended access could update support escalations records related to accounts in both environments.

About single tenants with multiple environments:

- Each environment within a tenant receives its own SQL database
- Data isn't shared across environments
- Go to **Microsoft Dataverse storage capacity**[8] for help understanding how storage is shared across environments
- All environments for a single customer tenant will be set up in the geography where they initially signed up for their account. Storage consumption is totaled and tracked across all the environments attached to a customer tenant
- Separate security groups can be set up for all environments
- A licensed user can potentially access all the environments associated with the tenant. Access is controlled by environment security group membership
- Additional environments may be purchased through the Additional environment Add-On. Additional environments can only be added to "paid" subscriptions, and not trials or Internal Use Rights (IUR). If subscriptions are purchased through Volume Licensing, additional environments need to be purchased through a Large Account Reseller (LAR)

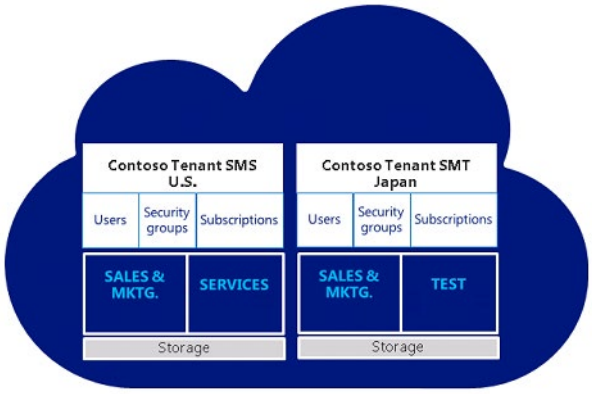
8 https://docs.microsoft.com/power-platform/admin/capacity-storage

- Existing trials or subscriptions can't be merged onto another environment; instead, data and customizations needed to move over

Uses for multi-tenants

Global businesses with different regional or country models can use tenants to account for variations in approach, market size, or
compliance with legal and regulatory constraints.

This example includes a second tenant for Contoso Japan:



User accounts, identities, security groups, subscriptions, licenses, and storage can't be shared among tenants. All tenants can have multiple environments associated with each specific tenant. Data isn't shared across environments or tenants.

In a **multi-tenant scenario**, a licensed user associated with a tenant can only access one or more environments mapped to the same tenant. To access another tenant, a user would need a separate license and a unique set of sign-in credentials for that tenant.

For example, suppose User A has an account to access Tenant A. In that case, their license allows them to access any and all environments created within Tenant A – if allowed by their administrator. If User A needs to access environments within Tenant B, they will need an additional license.

- Each tenant requires Microsoft Power Platform admin(s) with unique sign-in credentials, and each tenant affiliate will manage its tenant separately in the administrator console
- Multiple environments within a tenant are visible from the interface if the administrator has access
- Licenses can't be reassigned between tenant enrollments. An enrolled affiliate can use license reduction under one enrollment and add licenses to another enrollment to facilitate this
- On-premises Active Directory federation can't be established with more than one tenant unless there are top-level domains that need to be federated with different tenants (for example, contoso.com and fabricam.com)

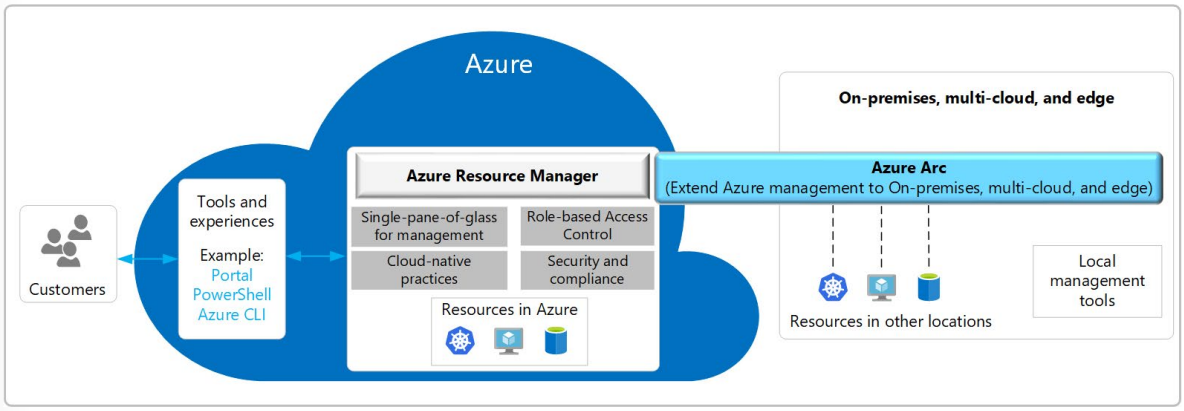
Manage hybrid environments at scale with Azure Arc

Today, companies struggle to control and govern increasingly complex environments that extend across data centers, multiple clouds, and edge of a network boundary. Each environment and cloud possess its own set of management tools, and new DevOps and ITOps operational models can be hard to implement across resources.

Azure Arc simplifies governance and management by delivering a consistent multi-cloud and on-premises management platform.

Azure Arc provides a centralized, unified way to:

- Manage an entire environment by projecting existing non-Azure and/or on-premises resources into Azure Resource Manager
- Manage virtual machines, Kubernetes clusters, and databases as if they're running in Azure
- Use familiar Azure services and management capabilities, regardless of where they live
- Continue using traditional ITOps while introducing DevOps practices to support new cloud native patterns in an environment
- Configure custom locations as an abstraction layer on top of Azure Arc-enabled Kubernetes clusters and cluster extensions



Manage hybrid environments at scale with Azure Policy

Azure Policy helps to enforce organizational standards and to assess compliance at-scale. Through its compliance dashboard, it provides an aggregated view to evaluate the overall state of the environment, with the ability to drill down to the per-resource, per-policy granularity. It also helps to bring resources to compliance through bulk remediation for existing resources and automatic remediation for new resources.

Common use cases for Azure Policy include implementing governance for resource consistency, regulatory compliance, security, cost, and management. Policy definitions for these common use cases are already available in Azure environments as built-ins to help architects get started.

Azure Policy uses a JavaScript Object Notation (JSON) format to form the logic the evaluation uses to determine whether a resource is compliant or not. Definitions include metadata and the policy rule. The defined rule can use functions, parameters, logical operators, conditions, and property aliases to match exactly specific scenarios. The policy rule determines which resources in the scope of the assignment get evaluated.

Resources are evaluated at specific times during the resource lifecycle, the policy assignment lifecycle, and for regular ongoing compliance evaluation.

The following are the times or events that cause a resource to be evaluated:

- A resource is created or updated in a scope with a policy assignment
- A policy or initiative is newly assigned to a scope
- A policy or initiative already assigned to a scope is updated
- During the standard compliance evaluation cycle, which occurs once every 24 hours

Design technical and governance strategies for traffic filtering and segmentation

Perimeter-based networks operate on the assumption that all systems within a network can be trusted. But today's employees access their organization's resources from anywhere on a variety of devices and apps, which makes perimeter security controls irrelevant. Access control policies that focus only on who can access a resource are not enough. To master the balance between security and productivity, security admins also need to factor in how a resource is being accessed.

Adopt a Zero Trust approach

Networks need to evolve from traditional defenses because networks might be vulnerable to breaches: an attacker can compromise a single endpoint within the trusted boundary and then quickly expand a foothold across the entire network. Zero Trust networks eliminate the concept of trust based on network location within a perimeter. Instead, Zero Trust architectures use the device, and user trust claims to gate access to organizational data and resources. For new initiatives, adopt Zero Trust approaches that validate trust at the time of access.

Logically segment subnets

Azure virtual networks are similar to Local Area Networks (LANs) on an on-premises network. The idea behind an Azure virtual network is to create a network based on a single private IP address space, on which all Azure virtual machines can be placed. The private IP address spaces available are in the Class A (10.0.0.0/8), Class B (172.16.0.0/12), and Class C (192.168.0.0/16) ranges.

Deploy perimeter networks for security zones

A **perimeter network**[9] (also known as a DMZ) is a physical or logical network segment that provides another layer of security between assets and the internet. Specialized network access control devices on the edge of a perimeter network allow only desired traffic into a virtual network.
Perimeter networks are useful to help focus network access control management, monitoring, logging, and reporting on the devices at the edge of an Azure virtual network. A perimeter network is where distributed denial of service (DDoS) prevention i, intrusion detection/intrusion prevention systems (IDS/IPS), firewall rules and policies, web filtering, network antimalware, and more are typically enabled. The

9 https://docs.microsoft.com/azure/architecture/vdc/networking-virtual-datacenter

network security devices sit between the internet and an Azure virtual network and have an interface on both networks.

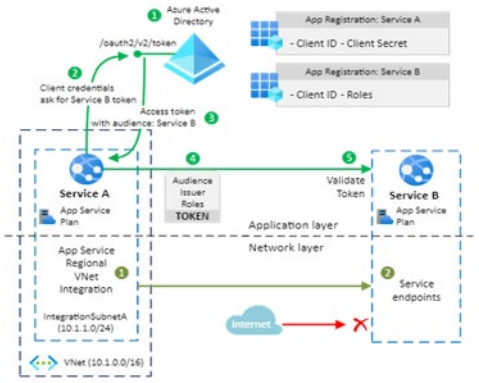
Based on the Zero Trust concept, consider using a perimeter network for all high security deployments in order to enhance the level of network security and access control for Azure resources. Azure or a third party solution can be used to provide another layer of security between assets and the internet.

Avoid exposure to the internet with dedicated WAN links

Many organizations have chosen the hybrid IT route. With hybrid IT, some of the company's information assets are in Azure, and others remain on-premises. In many cases, some components of a service are running in Azure while other components remain on-premises.
In a hybrid IT scenario, there's usually some type of cross-premises connectivity. Cross-premises connectivity allows the company to connect its on-premises networks to Azure virtual networks.

Use virtual network appliances

Network security groups and user-defined routing can provide a certain measure of network security at the network and transport layers of the OSI model. But in some situations, security needs to be enabled at high levels of the stack. In such situations, it is recommended to deploy virtual network security appliances provided by Azure partners. Azure network security appliances can deliver better security than what network-level controls provide.



Exercise

Tailwind Trader is a fictitious home improvement retailer. It operates retail hardware stores across the globe and online.

Case study: Design a Zero Trust Solution

Meet Tailwind Traders

The Tailwind Traders CISO is aware of the opportunities offered by Azure, but also understands the need for strong security and solid cloud architecture. Without strong security and a great point of reference architecture, the company may have difficulty managing the Azure environment and costs, which are hard to track and control. The CISO is interested in understanding how Azure manages and enforces security standards.

Requirements

Tailwind Traders is planning significant changes to their Azure Architecture. They have asked for your assistance with recommendations and questions. Here are the specific requirements.

- **User Access and Productivity.** The company has a new security optimization project for customer environments. The CISO wants to ensure all Azure resources are highly secured. For the architecture review phase, user accounts should require:
  - Passwordless or MFA for all users and be able to measure risk with threat intelligence & behavior analytics
  - Endpoints should require device integrity for access
  - Network should be able to establish basic traffic filtering and segmentation to isolate business-critical or highly vulnerable resources

Tasks

User Access and Productivity

- **Question 1:** What are different ways Tailwind Traders could use the MCRA to require Passwordless or MFA for all users and be able to measure risk with threat intelligence & behavior analytics?
- **Task 1:** Design an architecture and explain your decision-making process.
- **Question 2:** What are the different ways Tailwind Traders could require integrity for access for end-points using the MCRA?
- **Task 2:** Design a architecture and explain your decision-making process.
- **Question 3:** What are the different ways Tailwind Traders could establish basic network traffic filtering and segmentation to isolate business-critical or highly vulnerable resources using the MCRA?
- **Task 3:** Propose at least two ways of meeting the requirements. Explain your final decision.

How are you incorporating the Microsoft Cybersecurity Reference Architectures (MCRA) to produce a secured, high available, and efficient cloud architecture?

Summary

In this module, you've learned how to build an overall security strategy and architecture with zero trust in mind. You have learned different strategies for designing, defining, and recommending an organizational security strategy and architecture. You should now be able to:

- Develop integration points in an architecture
- Develop security requirements based on business goals
- Translate security requirements into technical capabilities
- Design security for a resiliency strategy
- Design a security strategy for hybrid and multi-tenant environments
- Design technical and governance strategies for traffic filtering and segmentation

Learn more with Azure documentation

- **Microsoft Cybersecurity Reference Architectures - Security documentation**[10]
- **Governance in the Microsoft Cloud Adoption Framework for Azure - Cloud Adoption Framework**[11]
- **Balance competing priorities - Cloud Adoption Framework**[12]
- **Resiliency and continuity - Microsoft Service Assurance**[13]

10 https://docs.microsoft.com/security/cybersecurity-reference-architecture/mcra
11 https://docs.microsoft.com/azure/cloud-adoption-framework/govern/
12 https://docs.microsoft.com/azure/cloud-adoption-framework/strategy/balance-competing-priorities
13 https://docs.microsoft.com/compliance/assurance/assurance-resiliency-and-continuity

- **Organize and manage multiple Azure subscriptions - Cloud Adoption Framework**[14]
- **Recommended policies for Azure services - Azure Policy**[15]

Learn more with self-paced training

- **Build a cloud governance strategy on Azure - Learn**[16]
- **Describe core Azure architectural components - Learn**[17]
- **Microsoft Cloud Adoption Framework for Azure - Learn**[18]

14 https://docs.microsoft.com/azure/cloud-adoption-framework/ready/azure-best-practices/organize-subscriptions
15 https://docs.microsoft.com/azure/governance/policy/concepts/recommended-policies
16 https://docs.microsoft.com/learn/modules/build-cloud-governance-strategy-azure/
17 https://docs.microsoft.com/learn/modules/azure-architecture-fundamentals/
18 https://docs.microsoft.com/learn/modules/microsoft-cloud-adoption-framework-for-azure/

Design a security operations strategy

Introduction

In this module, you'll learn how to:

- Design a logging and auditing security strategy
- Develop security operations for hybrid and multi-cloud environments
- Design a strategy for Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR)
- Evaluate security workflows
- Review security strategies for incident management
- Evaluate security operations for technical threat intelligence
- Monitor sources for insights on threats and mitigations. Develop Integration points in an architecture.

The content in the module will help you prepare for Exam SC-100: Cybersecurity Architecture. The module concepts are covered in:

- Design a Zero Trust Strategy and Architecture
- Design a Security Operations Strategy

Prerequisites

Conceptual knowledge of security policies, requirements, zero trust architecture, and management of hybrid environments

Working experience with zero trust strategies, applying security policies, and developing security requirements based on business goals

Security Operations Strategy Overview

One of the significant changes in perspectives that are a hallmark of a Zero Trust security framework is moving away from trust-by-default toward trust-by-exception. However, a reliable way to establish trust once trust is needed. Since you no longer assume that requests are trustworthy, establishing a means to attest to the trustworthiness of the request is critical to proving its point-in-time trustworthiness. This attestation requires gaining visibility into the activities on and around the request.

Our other Zero Trust guides defined the approach to implementing an end-to-end Zero Trust approach across **identities**[19], **endpoints**[20] and devices, **data**[21], **apps**[22], **infrastructure**[23], and **networks**[24].
All these investments increase your visibility, which gives you better data for making trust decisions. However, adopting a Zero Trust approach in other areas like identities, endpoints, infrastructure and networks, increases the number of incidents Security Operation Center (SOC) analysts need to mitigate.

19 https://aka.ms/ZTIdentity
20 https://aka.ms/ZTEndpoints
21 https://aka.ms/ZTData
22 https://aka.ms/ZTApplications
23 https://aka.ms/ZTInfrastructure
24 https://aka.ms/ZTNetwork

With each of these individual areas generating its relevant alerts, an integrated capability is needed to manage the resulting influx of data to better defend against threats and validate trust in a transaction. The following abilities are needed:

- Detect threats and vulnerabilities.
- Investigate.
- Respond.
- Hunt.
- Provide additional context through threat analytics.
- Assess vulnerabilities.
- Get help from world class experts
- Prevent or block events from happening across the pillars.

Managing threats includes reactive and proactive detection and requires tools that support both.

- **Reactive detection:** Incidents are triggered from one of the six pillars that can be investigated. Additionally, a management product like a SIEM will likely support another layer of analytics that will enrich and correlate data, resulting in flagging an incident as bad. The next step would then be to investigate to get the full narrative of the attack.
- **Proactive detection:** Hunting to the data is applied to prove a compromised hypothesis. Threat hunting starts with the assumption there has been a breach, hence hunt for proof that there's indeed a breach.

Each minute that an attacker has in the environment allows them to continue to conduct attack operations and access sensitive or valuable systems. Maintaining control over environment ensures that compliancy with industry standards, such as information security management and corporate or organizational standards, such as ensuring that network data is encrypted.

An efficient Security Operations Strategy is most beneficial when there are:

- Multiple engineering teams working in Azure.

- Multiple subscriptions to manage.
- Regulatory requirements that must be enforced.
- Standards that must be followed for all cloud resources.
- Defined logging and auditing security process.

Understand security operations frameworks, processes, and procedures

The responsibility of the security operation team (also known as Security Operations Center (SOC), or SecOps) is to rapidly detect, prioritize, and triage potential attacks. These operations help eliminate false positives and focus on real attacks, reducing the mean time to remediate real incidents.

Watch the video below for an overview about Security Operations:

[!VIDEO https://www.microsoft.com/videoplayer/embed/RWVECU]

The central SecOps team monitors security-related telemetry data and investigates security breaches. It's important that any communication, investigation, and hunting activities are aligned with the application team. Here are some general best practices for conducting security operations:

- Follow the NIST Cybersecurity Framework functions as part of operations:
  - **Detect** the presence of adversaries in the system.
  - **Respond** by quickly investigating whether it's an actual attack or a false alarm.
  - **Recover** and restore the confidentiality, integrity, and availability of the workload during and after an attack.
- Acknowledge an alert quickly. A detected adversary must not be ignored while defenders are triaging false positives.
- Reduce the time to remediate a detected adversary. Reduce their opportunity time to conduct and attack and reach sensitive systems.
- Prioritize security investments into systems that have high intrinsic value. For example, administrator accounts.
- Proactively hunt for adversaries as your system matures. This effort will reduce the time that a higher skilled adversary can operate in the environment. For example, skilled enough to evade reactive alerts.

SecOps has multiple potential interactions with business leadership, which includes:

- **Business context to SecOps**: SecOps must understand what is most important to the organization so that the team can apply that context to fluid real-time security situations. What would have the most negative impact on the business? Downtime of critical systems? A loss of reputation and customer trust? Disclosure of sensitive data? Tampering with critical data or systems? We've learned it's critical that key leaders and staff in the SOC understand this context. They'll wade through the continuous flood of information and triage incidents and prioritize their time, attention, and effort.
- **Joint practice exercises with SecOps**: Business leaders should regularly join SecOps in practicing response to major incidents. This training builds the muscle memory and relationships that are critical to fast and effective decision making in the high pressure of real incidents, reducing organizational risk. This practice also reduces risk by exposing gaps and assumptions in the process that can be fixed before a real incident occurs.
- **Major incidents updates from SecOps**: SecOps should provide updates to business stakeholders for major incidents as they happen. This information allows business leaders to understand their risk and take both proactive and reactive steps to manage that risk.
- **Business intelligence from the SOC**: Sometimes SecOps finds that adversaries are targeting a system or data set that isn't expected. As these discoveries are made, the threat intelligence team should share these signals with business leaders as they might trigger insight for business leaders. For example, someone outside the company is aware of a secret project or unexpected attacker targets highlight the value of an otherwise overlooked dataset.

People and process

Security operations can be highly technical, but more importantly, it's a human discipline. People are the most valuable asset in security

operations. Their experience, skill, insight, creativity, and resourcefulness are what make the discipline effective.

Attacks on your organization are also planned and conducted by people like criminals, spies, and hacktivists. While some commodity attacks are fully automated, the most damaging ones are often done by live human attack operators.

Focus on empowering people

Your goal shouldn't be to replace people with automation. Empower your people with tools that simplify their daily workflows. These tools enable them to keep up with or get ahead of the human adversaries they face.

Rapidly sorting out signal (real detections) from the noise (false positives) requires investing in both humans and automation. Automation and technology can reduce human work, but attackers are human and human judgment is critical in defeating them.

Diversify your thinking portfolio

Security operations can be highly technical, but it's also just another new version of forensic investigation that shows up in many career fields like criminal justice. Don't be afraid to hire people with a strong competency in investigation or deductive or inductive reasons and train them on technology.

Metrics

Metrics drive behavior, so measuring success is a critical element to get right. Metrics translate culture into clear measurable goals that drive outcomes.

We've learned that it's critical to consider what you measure, and the ways that you focus on and enforce those metrics. Recognize that security operations must manage significant variables that are out of their direct control, like attacks and attackers. Any deviations from targets should be viewed primarily as a learning opportunity for process or tool improvement, rather than assumed to be a failure by the SOC to meet a goal.

The main metrics to focus on that have a direct influence on organizational risk are:

- **Mean time to acknowledge (MTTA)**: Responsiveness is one of the few elements SecOps has more direct control over. Measure the time between an alert, like when the light starts to blink, and when an analyst sees that alert and begins the investigation. Improving this responsiveness requires that analysts don't waste time investigating false positives. It can be achieved with ruthless prioritization, ensuring that any alert feed that requires an analyst response must have a track record of 90 percent true positive detections.

- **Mean time to remediate (MTTR)**: Effectiveness of reducing risk measures the next period of time. That period is the time the analyst begins the investigation to when the incident is remediated. MTTR identifies how long it takes SecOps to remove the attacker's access from the environment. This information helps identify where to invest in processes and tools to help analysts reduce risk.
- **Incidents remediated (manually or with automation)**: Measuring how many incidents are remediated manually and how many are resolved with automation is another key way to inform staffing and tool decisions.
- **Escalations between each tier**: Track how many incidents escalated between tiers. It helps ensure accurate tracking of the workload to inform staffing and other decisions. For example, so that work done on escalated incidents isn't attributed to the wrong team.

Design a logging and auditing security strategy

The cloud has dramatically changed the role of the operations team. They are no longer responsible for managing the hardware and infrastructure that hosts the application. Operations are still a critical part of running a successful cloud application. Some of the important functions of the operations team include:

- Deployment
- Monitoring
- Escalation
- Incident response
- Security auditing

Robust logging and tracing are particularly important in cloud applications. Involve the operations team in design and planning to ensure the application gives them the data and insight they need to be successful.

Recommendations

- **Make all things observable.** Once a solution is deployed and running, logs and traces are your primary insight into the system. *Tracing* records a path through the system and is useful to pinpoint bottlenecks, performance issues, and failure points. *Logging* captures individual events such as application state changes, errors, and exceptions. Log in production, or else you lose insight at the very times when you need it the most.
- **Instrument for monitoring.** Monitoring gives insight into how well (or poorly) an application performs in terms of availability, performance, and system health. For example, monitoring indefinite if SLAs are being met. Monitoring happens during the normal operation of the system. It should be as close to real-time as

possible so that the operations staff can react to issues quickly. Ideally, monitoring can help avert problems before a critical failure. For more information, see **Monitoring and diagnostics**[25].

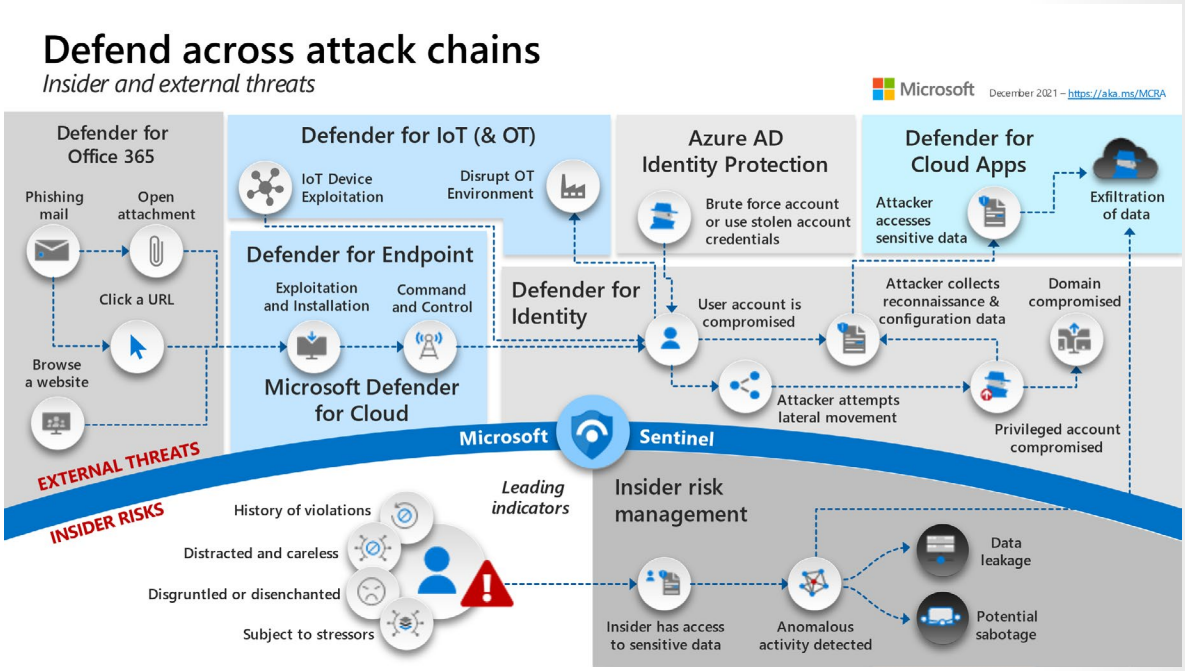
- **Instrument for root cause analysis.** Root cause analysis is the process of finding underlying causes of failures. It occurs after a failure has already happened.
- **Use distributed tracing.** Use a distributed tracing system designed for concurrency, asynchrony, and cloud scale. Traces should include a correlation ID that flows across service boundaries. A single operation may involve calls to multiple application services. If an operation fails, the correlation ID helps pinpoint the failure's cause.
- **Standardize logs and metrics.** The operations team will need to aggregate logs from across various services in your solution. If every service uses its logging format, it becomes difficult or impossible to get useful information from them. Define a common schema that includes fields such as correlation ID, event name, IP address of the sender, and so forth. Individual services can derive custom schemas that inherit the base schema and contain additional fields.
- **Automate management tasks**. This includes provisioning, deployment, and monitoring. Automating a task makes it repeatable and less prone to human errors.
- **Treat configuration as code.** Check configuration files into a version control system so that you can track and version your changes and roll back if needed.

Review the cyber kill chain

In the information security lexicon, a kill chain describes the structure of an attack against an objective. The series of steps describe a cyberattacks progression from reconnaissance to data exfiltration.

Understanding the intention of an attack can help you investigate and report the event more easily. Microsoft Defender for Cloud alerts includes the 'intent' field to help with these efforts.

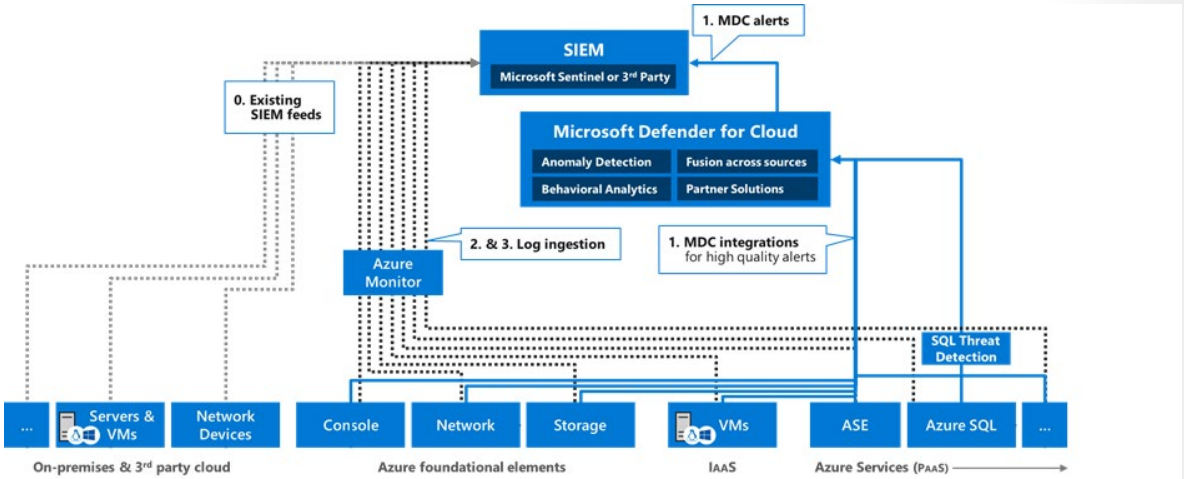
25 https://docs.microsoft.com/azure/architecture/best-practices/monitoring



Types of logs in Azure

Cloud applications are complex, with many moving parts. Logging data can provide insights about your applications and help you:

- Troubleshoot past problems or prevent potential ones
- Improve application performance or maintainability
- Automate actions that would otherwise require manual intervention



Azure logs are categorized into the following types:

- **Control/management logs** provide information about Azure Resource Manager CREATE, UPDATE, and DELETE operations. For more information, see **Azure activity logs**[26].
- **Data plane logs** provide information about events raised as part of Azure resource usage. Examples of this type of log are the Windows event system, security and application logs in a virtual machine (VM), and the **diagnostics logs**[27] configured through Azure Monitor.
- **Processed events** provide information about analyzed events/alerts. Examples of this type are **Microsoft Defender for Cloud alerts**[28], where **Microsoft Defender for Cloud**[29] has processed and analyzed subscriptions and provides concise security alerts.

The following table lists the most important types of logs available in Azure:

Log category	Log type	Usage	Integration
Activity logs *(https://docs.microsoft.com/azure/azure-monitor/essentials/platform-logs-overview)*	Control-plane events on Azure Resource Manager resources	Provides insight into the operations that were performed on resources in your subscription.	REST API, **Azure Monitor** *(https://docs.microsoft.com/azure/azure-monitor/essentials/platform-logs-overview)*
Azure Resource logs *(https://docs.microsoft.com/azure/azure-monitor/essentials/platform-logs-overview)*	Frequent data about the operation of Azure Resource Manager resources in the subscription	Provides insight into operations that your resource itself performed.	**Azure Monitor** *(https://docs.microsoft.com/azure/azure-monitor/essentials/platform-logs-overview)*
Azure Active Directory reporting *(https://docs.microsoft.com/azure/active-directory/reports-monitoring/overview-reports)*	Logs and reports	Reports user sign-in activities and system activity information about users and group management.	**Graph API** *(https://docs.microsoft.com/azure/active-directory/develop/microsoft-graph-intro)*
Virtual machines and cloud services *(https://docs.microsoft.com/azure/azure-monitor/vm/monitor-virtual-machine)*	Windows Event Log service and Linux Syslog	Captures system data and logging data on the virtual machines and transfers that data into a storage account of your choice.	Windows (using Windows Azure Diagnostics **WAD** *(https://docs.microsoft.com/azure/azure-monitor/agents/diagnostics-extension-overview)* storage) and Linux in Azure Monitor

26 https://docs.microsoft.com/azure/azure-monitor/essentials/platform-logs-overview
27 https://docs.microsoft.com/azure/azure-monitor/essentials/platform-logs-overview
28 https://docs.microsoft.com/azure/security-center/security-center-managing-and-responding-alerts
29 https://docs.microsoft.com/azure/security-center/security-center-introduction

Log category	Log type	Usage	Integration
Azure Storage Analytics *(https://docs.microsoft.com/rest/api/storageservices/fileservices/storage-analytics)*	Storage logging, provides metrics data for a storage account	Provides insight into trace requests, analyzes usage trends, and diagnoses issues with your storage account.	REST API or the **client library** *(https://docs.microsoft.com/dotnet/api/overview/azure/storage)*
Network security group (NSG) flow logs *(https://docs.microsoft.com/azure/network-watcher/network-watcher-nsg-flow-logging-overview)*	JSON format, shows outbound and inbound flows on a per-rule basis	Displays information about ingress and egress IP traffic through a Network Security Group.	**Azure Network Watcher** *(https://docs.microsoft.com/azure/network-watcher/network-watcher-monitoring-overview)*
Application insight *(https://docs.microsoft.com/azure/azure-monitor/app/app-insights-overview)*	Logs, exceptions, and custom diagnostics	Provides an application performance monitoring (APM) service for web developers on multiple platforms.	REST API, **Power BI** *(https://powerbi.microsoft.com/documentation/powerbi-azure-and-power-bi/)*
Process data / security alerts *(https://docs.microsoft.com/azure/security-center/security-center-introduction)*	Microsoft Defender for Cloud alerts, Azure Monitor logs alerts	Provides security information and alerts.	REST APIs, JSON

Using the Security Operations Frame

Azure provides a wide array of configurable security auditing and logging options to help you identify gaps in your security policies and mechanisms. The tables below discuss generating, collecting, and analyzing security logs from services hosted on Azure using the Security Operations Frame for the following items:

Product/Service	Article
Dynamics CRM	**Identify sensitive entities in your solution and implement change auditing** *(https://docs.microsoft.com/azure/security/develop/threat-modeling-tool-auditing-and-logging#sensitive-entities)*
Web Application	**Ensure that auditing and logging is enforced on the application** *(https://docs.microsoft.com/azure/security/develop/threat-modeling-tool-auditing-and-logging#auditing)*
	Ensure that log rotation and separation are in place *(https://docs.microsoft.com/azure/security/develop/threat-modeling-tool-auditing-and-logging#log-rotation)*
	Ensure that the application does not log sensitive user data *(https://docs.microsoft.com/azure/security/develop/threat-modeling-tool-auditing-and-logging#log-sensitive-data)*

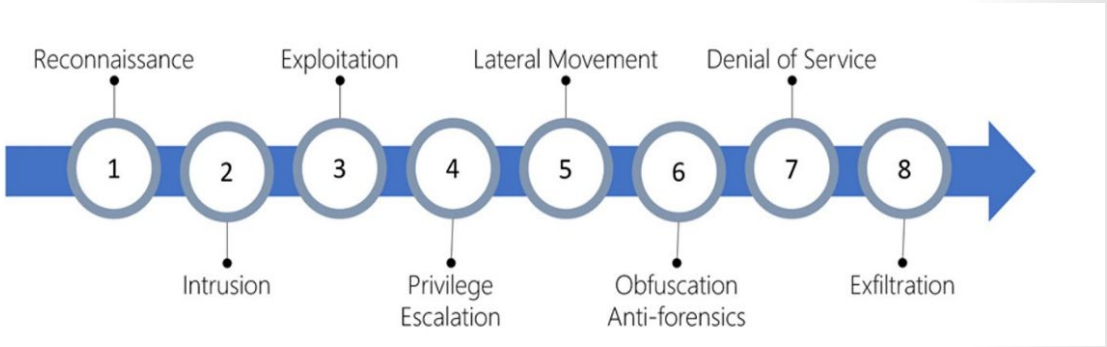
Product/Service	Article
	Ensure that Audit and Log Files have Restricted Access *(https://docs.microsoft.com/azure/security/develop/threat-modeling-tool-auditing-and-logging#log-restricted-access)*
	Ensure that User Management Events are Logged *(https://docs.microsoft.com/azure/security/develop/threat-modeling-tool-auditing-and-logging#user-management)*
	Ensure that the system has inbuilt defenses against misuse *(https://docs.microsoft.com/azure/security/develop/threat-modeling-tool-auditing-and-logging#inbuilt-defenses)*
	Enable diagnostics logging for web apps in Azure App Service *(https://docs.microsoft.com/azure/security/develop/threat-modeling-tool-auditing-and-logging#diagnostics-logging)*
Database	**Ensure that login auditing is enabled on SQL Server** *(https://docs.microsoft.com/azure/security/develop/threat-modeling-tool-auditing-and-logging#identify-sensitive-entities)*
	Enable Threat detection on Azure SQL *(https://docs.microsoft.com/azure/security/develop/threat-modeling-tool-auditing-and-logging#-threat-detection)*
Azure Storage	**Use Azure Storage Analytics to audit access of Azure Storage** *(https://docs.microsoft.com/azure/security/develop/threat-modeling-tool-auditing-and-logging#analytics)*
WCF	**Implement sufficient Logging** *(https://docs.microsoft.com/azure/security/develop/threat-modeling-tool-auditing-and-logging#sufficient-logging)*
	Implement sufficient Audit Failure Handling *(https://docs.microsoft.com/azure/security/develop/threat-modeling-tool-auditing-and-logging#audit-failure-handling)*
Web API	**Ensure that auditing and logging is enforced on Web API** *(https://docs.microsoft.com/azure/security/develop/threat-modeling-tool-auditing-and-logging#logging-web-api)*
IoT Field Gateway	**Ensure that appropriate auditing and logging is enforced on Field Gateway** *(https://docs.microsoft.com/azure/security/develop/threat-modeling-tool-auditing-and-logging#logging-field-gateway)*

Product/Service	Article
IoT Cloud Gateway	**Ensure that appropriate auditing and logging is enforced on Cloud Gateway** *(https://docs.microsoft.com/azure/security/develop/threat-modeling-tool-auditing-and-logging#logging-cloud-gateway)*

Protect against threats

Security Center's threat protection enables you to detect and prevent threats at the Infrastructure as a Service (IaaS) layer, non-Azure servers, and Platforms as a Service (PaaS) in Azure.

Security Center's threat protection includes fusion kill-chain analysis, which automatically correlates alerts in your environment based on cyber kill-chain analysis to help you better understand the full story of an attack campaign, where it started, and what kind of impact it had on your resources. Security Center's supported kill chain intents are based on the MITRE ATT&CK™ framework. As illustrated below, the typical steps that trace the stages of a cyberattack.



- **Reconnaissance:** The observation stage where attackers assess networks and services to identify possible targets and techniques to gain entry.
- **Intrusion:** Attackers use the knowledge gained in the reconnaissance phase to get access to a part of a network. This often involves exploring a flaw or security hole.
- **Exploitation:** This phase involves exploiting vulnerabilities and inserting malicious code onto the system to get more access.
- **Privilege Escalation:** Attackers often try to gain administrative access to compromised systems to get access to more critical data and move into other connected systems.
- **Lateral Movement:** This is the act of moving laterally to connected servers and gaining greater access to potential data.
- **Obfuscation / Anti-forensics:** Attackers need to cover their entry to successfully pull off a cyberattack. They will often compromise data and clear audit logs to prevent detection by any security team.
- **Denial of Service:** This phase involves disrupting normal access for users and systems to keep the attack from being monitored, tracked, or blocked.
- **Exfiltration:** The final extraction stage: getting valuable data out of the compromised systems.

Different types of attacks are associated with each stage, targeting various subsystems.

Develop Security Operations for Hybrid and Multi-cloud Environments

A hybrid cloud combines a private cloud (on-premises infrastructure) with a public cloud (computing services offered by third-party providers over the public internet). Hybrid clouds allow data and applications to consistently move between the two cloud environments. Many organizations choose a hybrid cloud strategy because of business requirements, such as meeting regulatory and data sovereignty requirements, maximizing on-premises technology investments, or addressing latency issues.

The hybrid cloud is evolving to include edge workloads. Cloud-managed edge computing devices bring the computing power of the public cloud to the private cloud, closer to where the IoT devices reside, including data residing in applications, connected devices, and mobile consumer services. Reducing latency by moving workloads to the edge, devices spend less time communicating with the cloud and can operate reliably in extended offline periods.

Multi-cloud computing uses multiple cloud computing services from more than one cloud provider (including private and public clouds) in a heterogeneous environment. A multi-cloud strategy provides greater flexibility and mitigates risk. Choose services from different cloud providers best suited for a specific task or take advantage of services offered by a particular cloud provider in a specific location.

Unified Operations

The primary objective of unified operations is to create as much process consistency as possible across deployments. No cloud service provider will be able to reach 100% feature parity across all hybrid, multi-cloud, and edge deployments. However, the provider should be able to deliver baseline feature sets common across all deployments so that your **governance**[30] and **operations management**[31] processes remain consistent.

Most commonly, customers require the ability to deliver consistency within their defined governance and operations management processes. To meet long-term requirements, your unified operations solution will need to be able to scale to meet these common processes specified below.

30 https://docs.microsoft.com/azure/cloud-adoption-framework/scenarios/hybrid/govern
31 https://docs.microsoft.com/azure/cloud-adoption-framework/scenarios/hybrid/manage

Common governance processes (tasks)

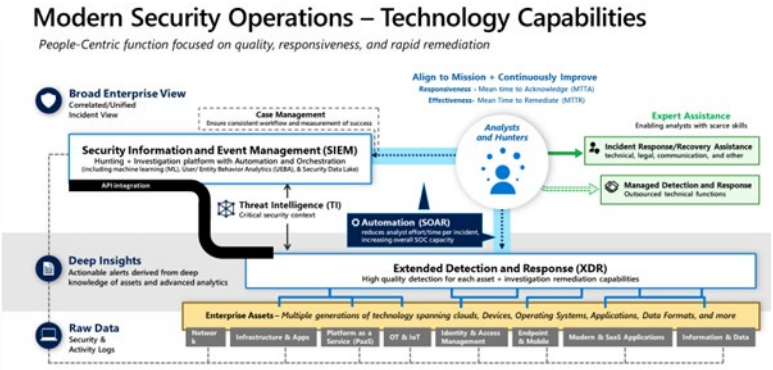
- **Cost management:** View, manage, or optimize costs and **identify and provide mitigation guidance for cloud-related IT spend risk**.
- **Security baseline:** Audit, apply, or automate requirements from recommended security controls and **identify and provide mitigation guidance for security-related business risks**.
- **Resource consistency:** Onboard, organize, configure resources and services, and **identify and provide risk mitigation guidance for potential business risks**.
- **Identity baseline:** Enforce authentication and authorization across user identity and access and **identify and provide risk-mitigation guidance for potential identity-related business risks**.
- **Deployment acceleration:** Drive consistency using templates, automation, and pipelines (for deployments, configuration alignment, and reusable assets), **establishing policies to ensure compliant, consistent, and repeatable resource deployment and configuration**.

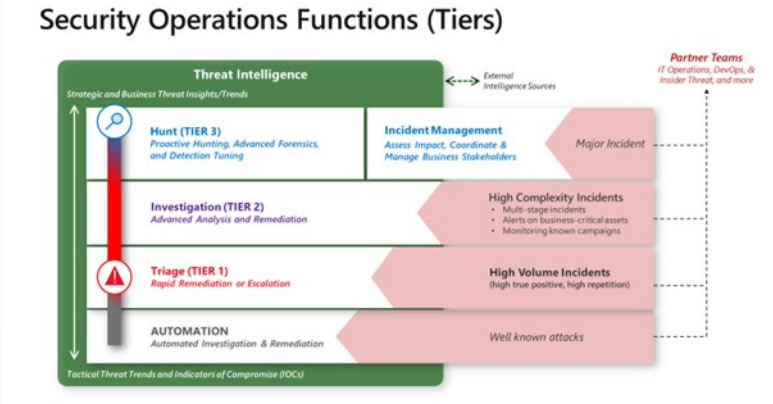
Common operations management processes (tasks)

- **Inventory and visibility:** Account for, and ensure reporting for all assets, and **collect and monitor your inventory's run state in enterprise-grade environments**.
- **Optimized operations:** Track, patch, and optimize supported resources and **minimize business interruption risks from configuration drift or vulnerabilities from inconsistent patch management**.
- **Protection and recovery:** Backup, business continuity, and disaster recovery best practices and **reduce the duration and impact of unpreventable outages**.
- **Platform operations[32]:**
  Specialized operations for common technology platforms such as SQL databases, virtual desktops, and SAP (for medium to high criticality workloads).
- **Workload operations[33]:**
  Specialized operations (for high priority/mission-critical workloads) with greater operations requirements.

Your primary cloud platform should be able to provide the required technical capabilities and tools to automate processes and reach the goals above for governance and operations management. Your unified operations solution should enable you to extend these processes across all hybrid, multi-cloud, and edge deployments.

32 https://docs.microsoft.com/azure/cloud-adoption-framework/manage/azure-management-guide/platform-specialization
33 https://docs.microsoft.com/azure/cloud-adoption-framework/manage/azure-management-guide/workload-specialization





Azure Security Operation services

Azure security operations[34] refer to the services, controls, and features available to users to protect their data, applications, and other assets in Microsoft Azure. It is a framework that incorporates the knowledge gained through various capabilities that are unique to Microsoft. These capabilities include the Microsoft Security Development Lifecycle (SDL), the Microsoft Security Response Center program, and deep awareness of the cybersecurity threat landscape.

Azure management services

An IT operations team is responsible for managing hybrid and multi-cloud environments, such as data center infrastructure, applications, and data, including the stability and security of these systems. However, gaining security insights across increasingly complex IT environments often requires organizations to cobble together data from multiple security and management systems.

34 https://docs.microsoft.com/azure/security/fundamentals/operational-security

Microsoft Azure Monitor logs[35] is a cloud-based IT management solution that helps you manage and protect your on-premises and cloud infrastructure. Its core functionality is provided by the following services that run in Azure. Azure includes multiple services that help you manage and protect on-premises and cloud infrastructures. Each service provides a specific management function. Services can be combined to achieve different management scenarios.

Azure Monitor

Azure Monitor[36] collects data from managed sources into central data stores. This data can include events, performance data, or custom data provided through the API. After the data is collected, it is available for alerting, analysis, and export.

Data can be consolidated from various sources and combined from Azure services with existing on-premises environments. Azure Monitor logs also clearly separate the data collection from the action taken on that data so that all actions are available to all kinds of data.

Automation

Azure Automation[37] provides a way to automate the manual, long-running, error-prone, and frequently repeated tasks commonly performed in a cloud and enterprise environment. It saves time and increases the reliability of administrative tasks. It even schedules these tasks to be automatically performed at regular intervals. Processes can be automated using runbooks or configuration management using Desired State Configuration.

Backup

Azure Backup[38] is the Azure-based service that you can use to back up (or protect) and restore your data in the Microsoft Cloud. Azure Backup replaces existing on-premises or off-site backup solutions with a cloud-based solution that's reliable, secure, and cost-competitive.

Azure Backup offers components to download and deploy on the appropriate computer or server or in the cloud. The component or agent deployed depends on what needs to be protected. All Azure Backup components (whether protecting data on-premises or in the cloud) can be used to back up data to an Azure Recovery Services vault in Azure.

For more information, see the **Azure Backup components table**[39].

35 https://docs.microsoft.com/azure/azure-monitor/overview
36 https://docs.microsoft.com/azure/azure-monitor/overview
37 https://docs.microsoft.com/azure/automation/automation-intro
38 https://docs.microsoft.com/azure/backup/backup-overview
39 https://docs.microsoft.com/azure/backup/backup-overview#what-can-i-back-up

Site Recovery

Azure Site Recovery[40] provides business continuity by orchestrating the replication of on-premises virtual and physical machines to Azure or a secondary site. If primary sites are unavailable, failover to the secondary location so that users can keep working. Fail back when systems return to working order. Use Microsoft Defender for Cloud to perform more intelligent and effective threat detection.

Azure Active Directory

Azure Active Directory (Azure AD)[41] is a comprehensive identity service that:

- Enables identity and access management (IAM) as a cloud service.
- Provides central access management, single sign-on (SSO), and reporting.
- Supports integrated access management for **thousands of applications**[42] in the Azure Marketplace, including Salesforce, Google Apps, Box, and Concur.

Azure AD also includes a full suite of **identity management capabilities**[43], including these:

- **Multi-factor authentication**[44]
- **Self-service password management**[45]
- **Self-service group management**[46]
- **Privileged account management**[47]
- **Azure role-based access control (Azure RBAC)**[48]
- **Application usage monitoring**[49]
- **Rich auditing**[50]
- **Security monitoring and alerting**[51]

With Azure Active Directory, all applications published for partners and customers (business or consumer) have the same identity and access management capabilities. This enables significant reduction in operational costs.

40 https://azure.microsoft.com/documentation/services/site-recovery
41 https://docs.microsoft.com/azure/active-directory/manage-apps/what-is-application-management
42 https://azuremarketplace.microsoft.com/marketplace/apps/Microsoft.AzureActiveDirectory
43 https://docs.microsoft.com/azure/security/fundamentals/identity-management-overview#security-monitoring-alerts-and-machine-learning-based-reports
44 https://docs.microsoft.com/azure/active-directory/authentication/concept-mfa-howitworks
45 https://azure.microsoft.com/resources/videos/self-service-password-reset-azure-ad/
46 https://support.microsoft.com/account-billing/reset-your-work-or-school-password-using-security-info-23dde81f-08bb-4776-ba72-e6b72b9dda9e
47 https://docs.microsoft.com/azure/active-directory/privileged-identity-management/pim-configure
48 https://docs.microsoft.com/azure/role-based-access-control/overview
49 https://docs.microsoft.com/azure/active-directory/hybrid/whatis-hybrid-identity
50 https://docs.microsoft.com/azure/active-directory/reports-monitoring/concept-audit-logs
51 https://docs.microsoft.com/azure/security-center/security-center-managing-and-responding-alerts

Microsoft Defender for Cloud

Microsoft Defender for Cloud[52] helps prevent, detect, and respond to threats with increased visibility into (and control over) the security of your Azure resources. It provides integrated security monitoring and policy management across subscriptions. It helps detect threats that might otherwise go unnoticed, and it works with a broad ecosystem of security solutions.

Safeguard virtual machine (VM) data[53] in Azure by providing visibility into virtual machines' security settings and monitoring for threats. Defender for Cloud can monitor your virtual machines for:

- Operating system security settings with the recommended configuration rules.
- System security and critical updates that are missing.
- Endpoint protection recommendations.
- Disk encryption validation.
- Network-based attacks.

Defender for Cloud uses **Azure role-based access control (Azure RBAC)**[54]. Azure RBAC provides **built-in roles**[55] that can be assigned to Azure users, groups, and services.

Defender for Cloud assesses the configuration resources to identify security issues and vulnerabilities. In Defender for Cloud, information related to a resource is seen only when by assigned the role of owner, contributor, or reader for the subscription or resource group that a resource belongs to.

Design a strategy for Security Information and Event Management (SIEM)

Organizations today must contend with an increasingly complex threat landscape. A key tenant of Zero Trust is assuming breach. An effective approach to "assume breach" means having a threat detection approach that provides visibility across the entire estate, with the depth of information that security teams need to investigate individual threats.

Visibility, automation, and orchestration integrations build robust solutions for monitoring security signals. They are key to ensuring the ongoing security of an environment by detecting suspicious behavior and enabling proactive hunting for threats. They allow customers to scan for unexpected behavior and access and proactively search for bad actors already in the network.

This guidance is for software providers and technology partners who want to enhance their visibility, automation, and orchestration security solutions by integrating with Microsoft products.

52 https://docs.microsoft.com/azure/security-center/security-center-introduction
53 https://docs.microsoft.com/azure/security-center/security-center-introduction
54 https://docs.microsoft.com/azure/role-based-access-control/role-assignments-portal
55 https://docs.microsoft.com/azure/role-based-access-control/built-in-roles

Visibility, automation, and orchestration Zero Trust integration guide

This integration guide includes instructions for integrating with **Microsoft Sentinel**[56]. Microsoft Sentinel is Microsoft's cloud-native Security Information and Event Management (SIEM) service. Independent software vendors (ISVs) can integrate with Microsoft Sentinel to enable new use-cases for customers with data connectors, analytics rules, interactive workbooks, and automation playbooks to deliver end-to-end product or domain or industry vertical value for customers.

Azure operational security refers to the services, controls, and features available to users for protecting their data, applications, and other assets in Azure. Azure operational security is built on a framework that incorporates the knowledge gained through capabilities that are unique to Microsoft, including the Security Development Lifecycle (SDL), the Microsoft Security Response Center program, and deep awareness of the cybersecurity threat landscape.

Security Operations Tools

The following table contains Azure tools that a SOC team can use to investigate and remediate incidents.

Tools	Purpose
Azure Monitor *(https://docs.microsoft.com/azure/azure-monitor/overview)*	Event logs from application and Azure services.
Log Analytics *(https://docs.microsoft.com/azure/azure-monitor/logs/log-analytics-workspace-overview)*	A unique environment for log data from Azure Monitor and other Azure services such as Microsoft Sentinel and Microsoft Defender for Cloud.
Azure Network Security Group (NSG) *(https://docs.microsoft.com/azure/virtual-network/network-security-groups-overview)*	Visibility into network activities.
Azure Information Protection *(https://docs.microsoft.com/azure/information-protection/what-is-information-protection)*	You share secure email, documents, and sensitive data outside your company.
Microsoft Sentinel *(https://docs.microsoft.com/azure/sentinel/overview)*	Centralized Security Information and Event Management (SIEM) to get enterprise-wide visibility into logs.
Microsoft Defender for Cloud *(https://docs.microsoft.com/azure/security-center/security-center-intro)*	Alert generation. Use a security playbook in response to an alert.

Security operations best practices for SIEM and SOAR

Below are operational best practices for protecting your data, applications, and other assets in Azure. The best practices are based on a consensus, and they work with current Azure platform capabilities and feature sets.

Receive incident notifications from Microsoft

Be sure security operations teams receive Azure incident notifications from Microsoft. An incident notification lets a security team know when there are compromised Azure resources so they can quickly respond to and remediate potential security risks.

56 https://docs.microsoft.com/azure/sentinel

The Azure enrollment portal admin contact information includes details that notify security operations. Contact information is an email address and phone number.

Monitor storage services for unexpected changes in behavior

Diagnosing and troubleshooting issues in a distributed application hosted in a cloud environment can be more complex than in traditional environments. Applications can be deployed in a PaaS or IaaS infrastructure, on-premises, on a mobile device, or some combination of these environments. An application's network traffic might traverse public and private networks using multiple storage technologies.

Continuously monitor the storage services of application uses for any unexpected changes in behavior (such as slower response times). Use logging to collect more detailed data and analyze a problem in depth. The diagnostics information obtained from monitoring and logging helps determine the root cause of the issue that an application encountered. From there, troubleshoot the issue and determine the appropriate steps to remediate it.

Azure Storage Analytics[57] performs logging and provides metrics data for an Azure storage account. We recommend using this data to trace requests, analyze usage trends, and diagnose issues with storage accounts.

Prevent, detect, and respond to threats

Here are best practices for preventing, detecting, and responding to threats:

Best practice: Increase the speed and scalability of your SIEM solution by using a cloud-based SIEM.

Detail: Investigate the features and capabilities of **Microsoft Sentinel**[58] and compare them with the capabilities of what you're currently using on-premises. Consider adopting Microsoft Sentinel if it meets your organization's SIEM requirements.

Best practice: Find the most serious security vulnerabilities to prioritize investigating.

Detail: Review **Azure secure score**[59] to see the recommendations from the Azure policies and initiatives built into Microsoft Defender for Cloud. These recommendations help address top risks like security updates, endpoint protection, encryption, security configurations, missing WAF, internet-connected VMs, and many more.

The secure score, based on Center for Internet Security (CIS) controls, lets one benchmark an organization's Azure security against external sources. External validation helps validate and enrich a security strategy.

Best practice: Monitor the security posture of machines, networks, storage and data services, and applications to discover and prioritize potential security issues.

Detail: Follow the **security recommendations**[60] in Defender for Cloud starting with the highest priority items.

Best practice: Integrate Defender for Cloud alerts into a security information and event management (SIEM) solution.

Detail: Most organizations with a SIEM use it as a central clearinghouse for security alerts that require an analyst response. Processed events produced by Defender for Cloud are published to the Azure Activity

57 https://docs.microsoft.com/azure/storage/common/storage-analytics
58 https://docs.microsoft.com/azure/sentinel/overview
59 https://docs.microsoft.com/azure/security-center/secure-score-security-controls
60 https://docs.microsoft.com/azure/security-center/security-center-recommendations

Log, one of the logs available through Azure Monitor. Azure Monitor offers a consolidated pipeline for routing any of your monitoring data into a SIEM tool. See **Stream alerts to a SIEM, SOAR, or IT Service Management solution**[61] for instructions. If using Microsoft Sentinel, see **Connect Microsoft Defender for Cloud**[62].

Best practice: Integrate Azure logs with your SIEM.

Detail:Use Azure Monitor to gather and export data[63]. This practice is critical for enabling security incident investigation, and online log retention is limited. If using Microsoft Sentinel, see **Connect data sources**[64].

Best practice: Speed up investigation and hunting processes and reduce false positives by integrating Endpoint Detection and Response (EDR) capabilities into an attack investigation.

Detail: Enable the Microsoft Defender for Endpoint integration[65] via a Defender for Cloud security policy. Consider using Microsoft Sentinel for threat hunting and incident response.

Monitor end-to-end scenario-based network monitoring

Customers build an end-to-end network in Azure by combining network resources like a virtual network, ExpressRoute, Application Gateway, and load balancers. Monitoring is available on each of the network resources.

Azure Network Watcher[66] is a regional service. Use its diagnostic and visualization tools to monitor and diagnose conditions at a network scenario level in, to, and from Azure.

The following are best practices for network monitoring and available tools.

Best practice: Automate remote network monitoring with packet capture.

Detail: Monitor and diagnose networking issues without logging in to your VMs using Network Watcher. Trigger **packet capture**[67] by setting alerts and gaining access to real-time performance information at the packet level. Better diagnoses can be investigated in detail when issues are seen.

Best practice: Gain insight into network traffic by using flow logs.

Detail: Build a deeper understanding of network traffic patterns **using network security group flow logs**[68]. Information in flow logs helps gather data for compliance, auditing, and monitoring a network security profile.

Best practice: Diagnose VPN connectivity issues.

Detail: Use Network Watcher to **diagnose your most common VPN Gateway and connection issues**[69]. You can not only identify the issue but also use detailed logs to further investigate.

Monitor Azure AD risk reports

Most security breaches occur when attackers gain access to an environment by stealing a user's identity. Discovering compromised identities is no easy task. Azure AD uses adaptive machine learning algorithms and heuristics to detect suspicious actions related to user accounts. Each detected suspicious action is

61 https://docs.microsoft.com/azure/security-center/export-to-siem
62 https://docs.microsoft.com/azure/sentinel/connect-azure-security-center
63 https://docs.microsoft.com/azure/azure-monitor/overview#integrate-and-export-data
64 https://docs.microsoft.com/azure/sentinel/connect-data-sources
65 https://docs.microsoft.com/azure/security-center/security-center-wdatp#enable-the-microsoft-defender-for-endpoint-integration
66 https://docs.microsoft.com/azure/network-watcher/network-watcher-monitoring-overview
67 https://docs.microsoft.com/azure/network-watcher/network-watcher-alert-triggered-packet-capture
68 https://docs.microsoft.com/azure/network-watcher/network-watcher-nsg-flow-logging-overview
69 https://docs.microsoft.com/azure/network-watcher/network-watcher-diagnose-on-premises-connectivity

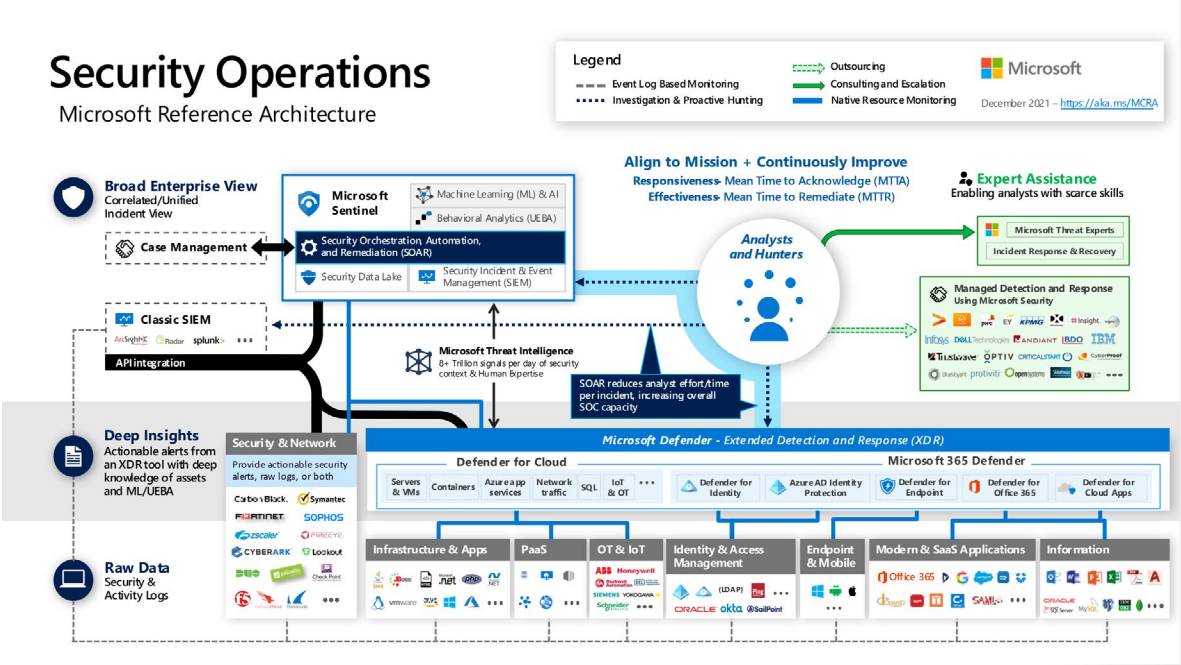
stored in a record called risk detection. Risk detections are recorded in Azure AD security reports. For more information, read about the users at risk security report and the risky sign-ins security report.

Best practice: Monitor for suspicious actions related to your user accounts.

Detail: Monitor for **users at risk**[70] and **risky sign-ins**[71] by using Azure AD security reports.

Architecture for Security Operations

The Security Operations Microsoft Reference Architecture describes how Microsoft's security capabilities integrate with Microsoft services and applications for Microsoft's Security Operations functions.



Evaluate security workflows

Every security program includes multiple workflows for incident response. These processes might include notifying relevant stakeholders, launching a change management process, and applying specific remediation steps. Security experts recommend that you automate as many steps of those procedures as possible. Automation reduces overhead. It can also improve your security by ensuring the process steps are done quickly, consistently, and according to your predefined requirements.

General incident response workflow

Consider these steps for your incident response workflow:

1. For each incident, begin an **attack and alert investigation and analysis**[72]
2. Perform containment to reduce any additional impact of the attack and eradication the security threat.
3. Recover from the attack by restoring your tenant resources to the state they were in before the incident.

70 https://docs.microsoft.com/azure/active-directory/identity-protection/overview-identity-protection
71 https://docs.microsoft.com/azure/active-directory/identity-protection/overview-identity-protection
72 https://docs.microsoft.com/microsoft-365/security/defender/investigate-incidents?view=o365-worldwide&preserve-view=true

4. Resolve the incident or escalate to a triage team member if the situation requires some human judgment.

Incident response best practices

With these recommendations, responding to incidents can be done effectively from technical and operations perspectives.

For the technical aspects of incident response, here are some goals to consider:

- Try to identify the scope of the attack operation - Most adversaries use multiple persistence mechanisms.
- Identify the objective of the attack, if possible - Persistent attackers will frequently return for their objective (data/systems) in a future attack.

For security operations (SecOps) aspects of incident response, here are some goals to consider:

- Staying focused - Confirm you keep the focus on business-critical data, customer impact, and getting ready for remediation.
- Providing coordination and role clarity - Establish distinct roles for operations in support of the crisis team and confirm that technical, legal, and communications teams are keeping each other informed.
- Keeping your business perspective - You should always consider the impact on business operations by both adversary actions and your response actions.

Recovery best practices

Recovering from incidents can be done effectively from both technical and operations perspectives with these recommendations.

For the technical aspects of recovering from an incident, here are some goals to consider:

- Don't boil the ocean - Limit your response scope so that recovery operation can be executed within 24 hours or less. Plan a weekend to account for contingencies and corrective actions.
- Avoid distractions - Defer long-term security investments like implementing large and complex new security systems or replacing anti-malware solutions until after the recovery operation. Anything that does not have a direct and immediate impact on the current recovery operation is a distraction.

For the operations aspects of recovering from an incident, here are some goals to consider:

- Have a clear plan and limited scope - Work closely with your technical teams to build a clear plan with limited scope. While plans may change based on adversary activity or new information, you should work diligently to limit scope expansion and take on additional tasks.
- Have clear plan ownership - Recovery operations involve many people doing many different tasks at once, so designate a project lead for the operation for clear decision-making and definitive information to flow among the crisis team.
- Maintain stakeholder communications - Work with communication teams to provide timely updates and active expectation management for organizational stakeholders.

Workflow Automation

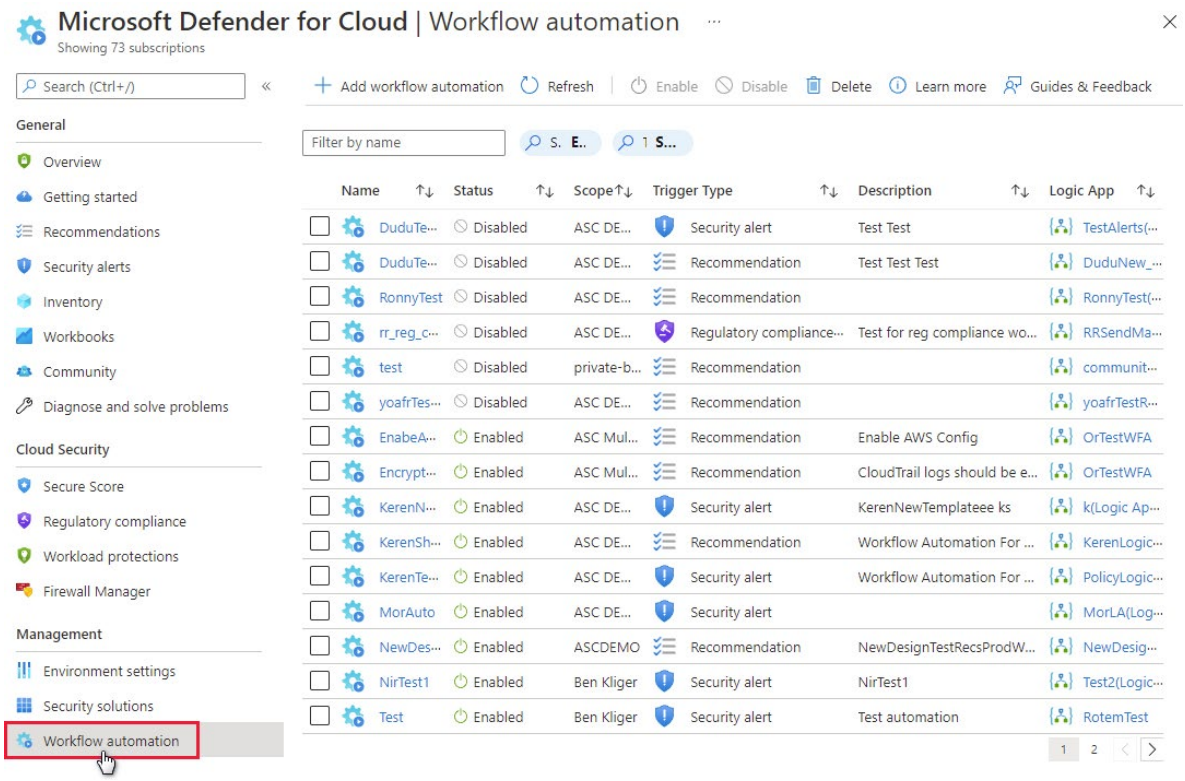
There are a few key technologies to be used for workflow automation in Azure:

- **Azure Logic Apps** - Azure Logic Apps is a cloud-based platform for creating and running automated *workflows* that integrate your apps, data, services, and systems. With this platform, you can quickly develop highly scalable integration solutions for your enterprise and business-to-business (B2B) scenarios. As a member of Azure Integration Services, Azure Logic Apps simplifies the way that you connect legacy, modern, and cutting-edge systems across cloud, on premises, and hybrid environments. For more information on Azure Logic Apps, see **Overview for Azure Logic Apps**[73].
- **Microsoft Defender for cloud** - the workflow automation feature of Microsoft Defender for Cloud can trigger Logic Apps on security alerts, recommendations, and changes to regulatory compliance. For more information on creating workflow automation with Defender for Cloud, see **Automate responses to Defender for cloud triggers**[74]
- **Microsoft Graph security** - With Azure Logic Apps and the Microsoft Graph Security connector, you can improve how your app detects, protects, and responds to threats by creating automated workflows for integrating Microsoft security products, services, and partners. For example, you can create Microsoft Defender for Cloud playbooks that monitor and manage Microsoft Graph Security entities, such as alerts. For more information on the integration, see **Improve threat protection by integrating security operations with Microsoft Graph Security & Azure Logic Apps**[75].
- **Microsoft Sentinel** – Sentinel provides both automation rules and playbooks. Automation rules help you triage incidents by changing incident attributes or running playbooks. Playbooks are collections of procedures that can be run from Microsoft Sentinel in response to an alert or incident.

Creating a workflow using Defender for Cloud and Azure Logic Apps

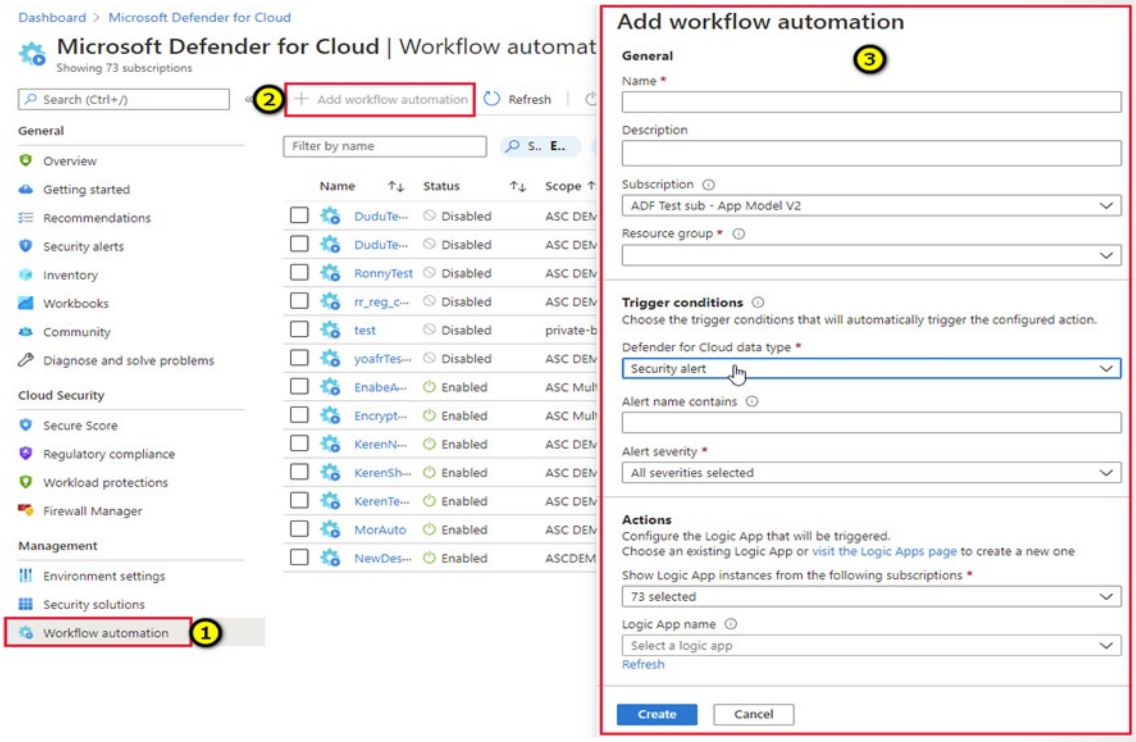
1. From Defender for Cloud's sidebar, select **Workflow automation**. From this page you can create new automation rules, as well as enable, disable, or delete existing ones.

73 https://docs.microsoft.com/azure/logic-apps/logic-apps-overview
74 https://docs.microsoft.com/azure/defender-for-cloud/workflow-automation
75 https://docs.microsoft.com/azure/connectors/connectors-integrate-security-operations-create-api-microsoft-graph-security



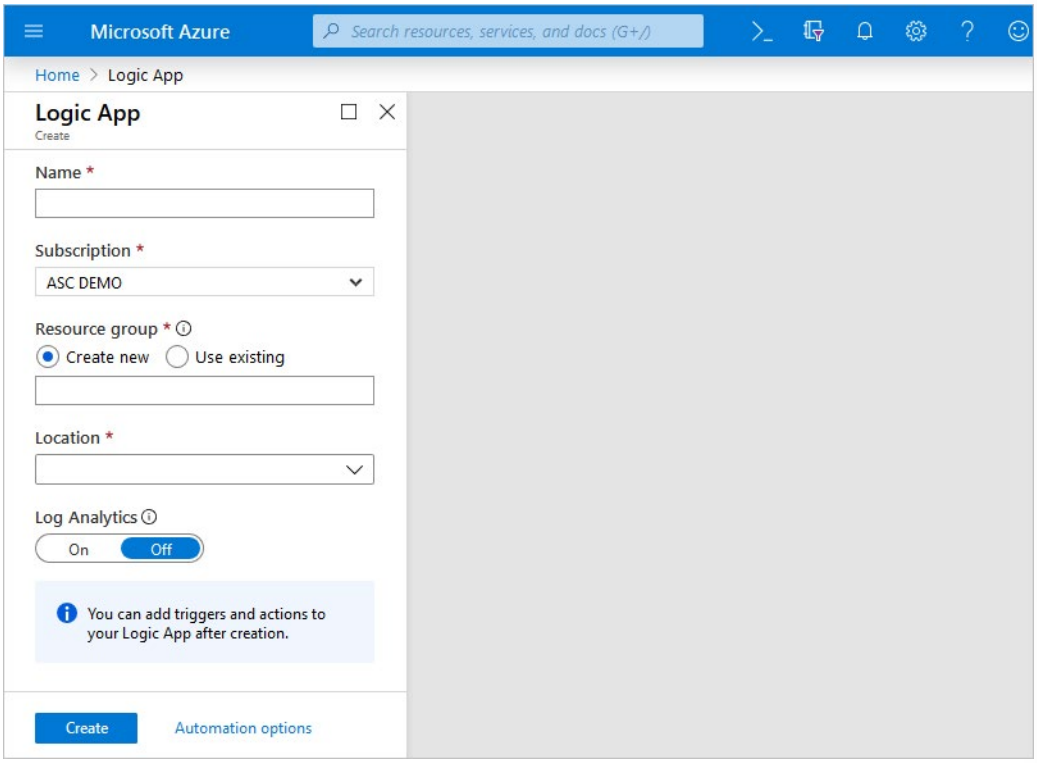
2. To define a new workflow, click **Add workflow automation**. The options pane for your new automation opens. Here you can enter:

    1. A name and description for the automation.
    2. The triggers that will initiate this automatic workflow. For example, you might want your Logic App to run when a security alert that contains “SQL” is generated.
    3. The Logic App that will run when your trigger conditions are met.

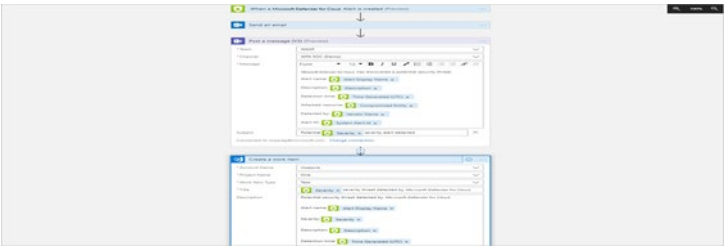


3. From the Actions section, select **visit the Logic Apps page** to begin the Logic App creation process. You'll be taken to Azure Logic Apps.

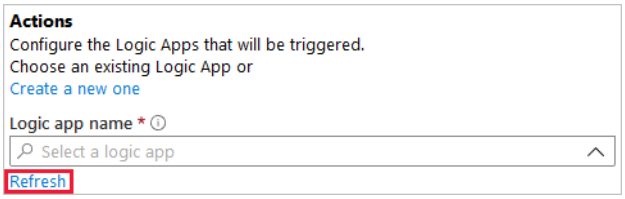
4. Select **Add**.



5. Enter a name, resource group, and location, and select **Review and create** > **Create**. The message **Deployment is in progress** appears. Wait for the deployment complete notification to appear and select **Go to resource** from the notification.
6. In your new logic app, you can choose from built-in, predefined templates from the security category. Or you can define a custom flow of events to occur when this process is triggered. The logic app designer supports these triggers from Defender for Cloud:
   - **When a Microsoft Defender for Cloud Recommendation is created or triggered** - If your logic app relies on a recommendation that gets deprecated or replaced, your automation will stop working, and you'll need to update the trigger. To track changes to recommendations, use the **release notes**[76].
   - **When a Defender for Cloud Alert is created or triggered** - You can customize the trigger so that it relates only to alerts with the severity levels that interest you.
   - **When a Defender for Cloud regulatory compliance assessment is created or triggered** - Trigger automations based on updates to regulatory compliance assessments.



7. After you've defined your logic app, return to the workflow automation definition pane ("Add workflow automation"). Click **Refresh** to ensure your new Logic App is available for selection.



8. Select your logic app and save the automation. Note that the Logic App dropdown only shows Logic Apps with supporting Defender for Cloud connectors mentioned above.

Creating a workflow using Microsoft Security Graph and Azure Logic Apps

Add triggers

In Azure Logic Apps, every logic app must start with a **trigger**[77], which fires when a specific event happens or when a specific condition is met. Each time that the trigger fires, the Logic Apps engine creates a logic app instance and starts running your app's workflow.

When a trigger fires, the trigger processes all the new alerts. If no alerts are received, the trigger run is skipped. The next trigger poll

76 https://docs.microsoft.com/azure/defender-for-cloud/release-notes
77 https://docs.microsoft.com/azure/logic-apps/logic-apps-overview#logic-app-concepts

happens based on the recurrence interval that you specify in the trigger's properties.

This example shows how you can start a logic app workflow when new alerts are sent to your app.

1. In the Azure portal or Visual Studio, create a blank logic app, which opens the Logic App Designer. This example uses the Azure portal.
2. On the designer, in the search box, enter "microsoft graph security" as your filter. From the triggers list, select this trigger: **On all new alerts**.
3. In the trigger, provide information about the alerts that you want to monitor. For more properties, open the **Add new parameter** list, and select a parameter to add that property to the trigger. For a more detailed list of possible properties, see **Add triggers**[78].
4. When you're done, on the designer toolbar, select **Save**.
5. Now continue adding one or more actions to your logic app for the tasks you want to perform with the trigger results.

Manage alerts

To filter, sort, or get the most recent results, provide *only* the **ODATA query parameters supported by Microsoft Graph**[79]. *Don't specify* the complete base URL or the HTTP action, for example, `<https://graph.microsoft.com/v1.0/security/alerts>`, or the `GET` or `PATCH` operation.

For more information about the queries you can use with this connector, see the **Microsoft Graph Security alerts reference documentation**[80].
To build enhanced experiences with this connector, learn more about the **schema properties alerts**[81] that the connector supports.

Action	Description
Get alerts	Get alerts filtered based on one or more alert properties, for example, Provider eq 'Azure Security Center' or 'Palo Alto Networks'.
Get alert by ID	Get a specific alert based on the alert ID.
Update alert	Update a specific alert based on the alert ID. To make sure you pass the required and editable properties in your request, see the editable properties for alerts. For example, to assign an alert to a security analyst so they can investigate, you can update the alert's Assigned to property.

Manage alert subscriptions

Microsoft Graph supports ***subscriptions***[82], or ***webhooks***[83]. To get, update, or delete subscriptions, provide the **ODATA query parameters support-**

78 https://docs.microsoft.com/azure/connectors/connectors-integrate-security-operations-create-api-microsoft-graph-security#add-triggers
79 https://docs.microsoft.com/graph/query-parameters
80 https://docs.microsoft.com/graph/api/alert-list
81 https://docs.microsoft.com/graph/api/resources/alert
82 https://docs.microsoft.com/graph/api/resources/subscription
83 https://docs.microsoft.com/graph/api/resources/webhooks

ed by Microsoft Graph[84] to the Microsoft Graph entity construct and include security/alerts followed by the ODATA query. *Don't include* the base URL, for example, **https://graph.microsoft.com/v1.0**. Instead, use the format in this example:

```
security/alerts?\$filter=status eq 'NewAlert'
```

Action	Description
Create subscriptions	Create a subscription that notifies you about any changes. You can filter this subscription for the specific alert types you want. For example, you can create a subscription that notifies you about high severity alerts.
Get active subscriptions	Get unexpired subscriptions.
Update subscription	Update a subscription by providing the subscription ID. For example, to extend your subscription, you can update the subscription's expirationDateTime property.
Delete subscription	Delete a subscription by providing the subscription ID.

Manage threat intelligence indicators

To filter, sort, or get the most recent results, provide *only* the **ODATA query parameters supported by Microsoft Graph**[85]. *Don't specify* the complete base URL or the HTTP action, for example, **https://graph.microsoft.com/beta/security/tiIndicators**, or the GET or PATCH operation.

For more information about the queries that you can use with this connector, see **"Optional Query Parameters" in the Microsoft Graph Security threat intelligence indicator reference documentation**[86]. To build enhanced experiences with this connector, learn more about the **schema properties threat intelligence indicator**[87] that the connector supports. For more information on possible threat intelligence actions, see **Manage threat indicators**[88].

Creating a playbook with Microsoft Sentinel and Logic Apps

1. Create a new playbook from the Microsoft Sentinel navigation under **Automation**. Decide whether you will use an **incident trigger** or an **alert trigger**.
2. Complete the required fields on the **Create playbook** window.
3. Add actions to define what happens when you call the playbook. These could be actions, logical conditions, loops, or switch case conditions.
4. Create an automation rule from the Microsoft Sentinel navigation under Automation.

    1. You can specify analytics rules or conditions for the automation rule to take effect.

84 https://docs.microsoft.com/graph/query-parameters
85 https://docs.microsoft.com/graph/query-parameters
86 https://docs.microsoft.com/graph/api/tiindicators-list
87 https://docs.microsoft.com/graph/api/resources/tiindicator
88 https://docs.microsoft.com/azure/connectors/connectors-integrate-security-operations-create-api-microsoft-graph-security#manage-threat-intelligence-indicators

2. You can also specify what actions you want the automation rule to take – such as assigning an owner or running a playbook.
3. You can also create an analytics rule in response to alerts.

For more detailed instructions on creating playbooks, see **Use playbooks with automation rules in Microsoft Sentinel**[89].

Review Security Strategies for Incident Management

A security incident is a confirmed breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to customer data or personal data. For example, unauthorized access to infrastructure and exfiltration of customer data would constitute a security incident, while compliance events that don't affect the confidentiality, integrity, or availability of services or customer data aren't considered security incidents.

Responding to Security Incidents

Whenever there's a security incident, an organization should respond quickly and effectively to protect its services and customer data. An incident response strategy should be designed to investigate, contain, and remove security threats quickly and efficiently.

In addition to automated security monitoring and alerting, all employees should receive annual training to recognize and report signs of potential security incidents. Any suspicious activity detected by employees, customers, or security monitoring tools should be escalated to Service-specific Security Response teams for investigation. Organizations should strive to have service operations teams, including Service-specific Security Response teams, maintain a deep on-call rotation to ensure resources are available for incident response 24x7x365. Many companies are now also outsourcing the function of providing Managed Service-specific Response capabilities.

When suspicious activity is detected and escalated, Security Response teams should be able to initiate a process of analysis, containment, eradication, and recovery. These teams should be able to coordinate analysis of the potential incident to determine its scope, including any impact on customers or customer data. Based on this analysis, Security Response teams should be able to work with impacted service teams to develop a plan to contain the threat and minimize the impact of the incident, eradicate the threat from the environment, and have the ability to fully recover systems to a known secure state.

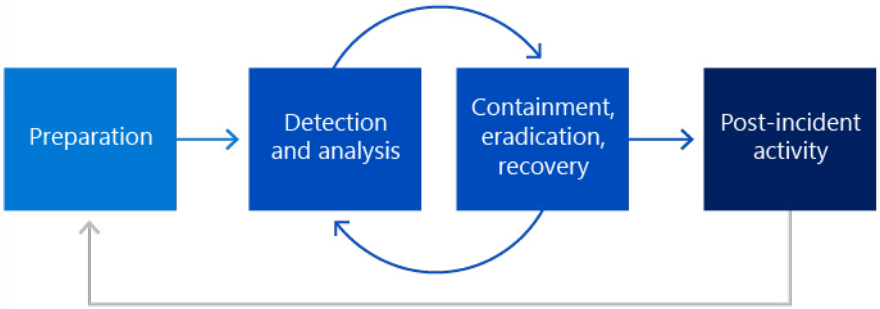
After an incident is resolved, service teams should strive to implement any lessons learned from the incident to better prevent, detect, and respond to similar incidents in the future. Security incidents, especially those incidents that are customer-impacting or result in a data breach, should undergo a full incident post-mortem. The post-mortem process should be designed to identify technical lapses, procedural failures, manual errors, and other process flaws that might have contributed to the incident or been identified during the incident response process. Improvements identified during the post-mortem should be implemented with coordination from Security Response teams to help prevent future incidents and improve detection and response capabilities.

89 https://docs.microsoft.com/azure/sentinel/tutorial-respond-threats-playbook?tabs=LAC

Incident Management Process

Security Response teams and the various service teams should work jointly and take the same approach to security incidents:

- **Preparation:** Refers to the organizational preparation needed to be able to respond, including tools, processes, competencies, and readiness.
- **Detection & analysis:** Refers to the activity to detect a security incident in a production environment and to analyze all events to confirm the authenticity of the security incident.
- **Containment, eradication, recovery:** Refers to the required and appropriate actions taken to contain the security incident based on the analysis done in the previous phase. More analysis may also be necessary for this phase to fully recover from the security incident.
- **Post-incident activity:** Refers to the post-mortem analysis performed after the recovery of a security incident. The operational actions performed during the process are reviewed to determine if any changes need to be made in the preparation or detection and analysis phases.



Preparation

Preparation enables rapid response when an incident occurs and may even prevent incidents in the first place. Azure dedicates significant resources to preparing for security incidents.

Organizations using Azure services should provide employees with training regarding security incidents and response procedures appropriate to their role. Every employee should be receiving training upon joining and annual refresher training every year thereafter. The training should be designed to provide the employee with a basic understanding of the Organization's approach to security so that upon completion of training, all employees understand:

- The definition of a security incident
- The responsibility of all employees to report security incidents
- How to escalate a potential security incident
- How security incident response teams respond to security incidents
- Special concerns regarding privacy, particularly customer privacy
- Where to find more information about security and privacy and escalation contacts
- Any other relevant security areas (as needed)

The appropriate employees should receive refresher training on security annually. The annual refresher training focuses on:

- Any changes made to the standard operating procedures in the preceding year

- The responsibility of everyone to report security incidents, and how to do so
- Where to find more information about security and privacy, and escalation contacts
- Any other security focus areas that may be relevant each year

Detection and Analysis

Organizations should use a centralized audit logging and analysis to detect anomalous or suspicious activity. Log files from Azure services should be collected and stored in a central, consolidated database. Centralized log analysis will allow the Security Response teams to comprehensively monitor the environment and correlate log entries from different services.

There should be centrally managed detection tools in place, including anti-virus and anti-malware suites, network-based and host-based intrusion detection systems, manual detection methods, and such as observations from engineers and end users.

When a potential incident is detected, a process should be escalated with a preliminary severity rating to a Security Response team, which serves as a key orchestrator of the security incident response process. The Security Response team should be responsible for analyzing the detection indicators to determine whether a security incident has occurred and to adjust its severity level if needed. If at any point the Security Response team discovers if data has been disclosed, modified, or destroyed, the team should initiate a security notification process.

At the beginning of the investigation, the Security Response team should record all information relevant to the incident. Continuous Improvement. Relevant information may include:

- A summary of the incident
- The incident's severity and priority based on its potential impact
- A list of all indicators that led to the detection of the incident
- A list of any related incidents
- A list of all actions taken by the Security Response team and any associated service teams
- Any evidence gathered during the incident response process
- Recommended next steps and actions

Containment, Eradication, and Recovery

Based on the analysis coordinated by the Security Response team, an appropriate containment and recovery plan should be developed to minimize the impact of the security incident and remove the threat from the environment. Relevant service teams should implement the plan with support from the Security Response team to ensure the threat is successfully eliminated and the impacted services undergo a complete recovery.

Containment

The primary goal of containment is to limit harm to systems, applications, customers, and customer data. During this phase, the Security Response team should work with affected service teams to limit the impact of the security incident and prevent further damage. All automated response solutions within Azure should help the team contain the incident.

The data collection and analysis should continue through the containment phase to ensure that the incident's root cause has been correctly identified and that all impacted services and tenants are included

in the eradication and recovery plan. Successfully tracing all impacted services makes full eradication and recovery possible.

Eradication

Eradication is the process of eliminating the root cause of the security incident with a high degree of confidence. The goal of eradication is twofold: to evict the adversary completely from the environment and mitigate any vulnerabilities that contributed to the incident or could enable the adversary to reenter the environment.

Eradication steps to evict the adversary and mitigate vulnerabilities are based on the analysis performed in the previous incident response phases. The Security Response team should coordinate with affected service teams to ensure the threat is successfully removed from the environment. Recovery isn't possible until the threat has been removed and its underlying causes have been resolved.

Recovery

When the Security Response team is confident the adversary has been evicted from the environment, and known vulnerabilities have been remediated, the team should work with affected service teams to initiate recovery. Recovery brings affected services to a known secure configuration. The recovery process includes identifying the last known good state of the service, restoring from backups to this state, and confirming the restored state mitigates the vulnerabilities that contributed to the incident.

A key aspect of the recovery process is enhanced detection controls to validate that the recovery plan has been successfully executed and that no signs of breach remain within the environment. Examples of additional detection controls include increased network-level monitoring, targeted alerting for attack vectors identified during the incident response process, and additional security team vigilance for critical resources. Enhanced monitoring helps to ensure that eradication was successful and that the adversary is unable to reenter the environment.

Post-Incident Activity

After the incident has been resolved, select security incidents, especially customer-impacting or resulting in a data breach, undergo a full incident post-mortem. The post-mortem process should be designed to identify technical lapses, procedural failures, manual errors, and other process flaws that might have contributed to the incident or been identified during the incident response process. The process should include the following:

A deep analysis of the root cause and investigation to identify any opportunities to improve system security or the security incident response process.

Discussion with Product Group Subject Matter Experts along with Security and Privacy Experts to identify opportunities for improvements in process, training, or technology.

Implementation of new automated monitoring and detection mechanisms to discover similar issues in the future.

Recording any findings as ticketed work items or bugs to be addressed by product teams as part of our normal Security Development Lifecycle and assigning these items to appropriate owning teams for follow-up.

Discussing the results of the completed post-mortem in monthly security incident review meetings conducted by senior management.

Continuous Improvement

Lessons learned from the security incident should be implemented with coordination from the Security Response team to help prevent future incidents and improve detection and response capabilities. Continuous improvement is paramount for effective and efficient incident response. Post-incident activities ensure that lessons learned from the security incident are successfully implemented across the enterprise to defend organizations and their customers against evolving threats.

Evaluate Security Operations strategy for sharing Technical Threat Intelligence

Organizations use Cyber Threat Intelligence to collect information gained from access to various signals across the Microsoft network. Cyber Threat Intelligence can be sourced from many places. These include, open-source data feeds, threat intelligence-sharing communities, commercial intelligence feeds, and local intelligence gathered during security investigations within an organization. Every second, hundreds of GB's worth of data is added to the Microsoft Intelligent Security Graph. This anonymized data comes from:

- Over a hundred Microsoft data centers across the globe.
- Threats faced by over 1 billion PCs updated by Windows Update each month.
- External data points are collected through extensive research and partnership with industry and law enforcement. This research is accomplished through Microsoft's Digital Crime Unit and Cybersecurity Defense Operations Center.

Threat intelligence in Azure:

- Consumes billions of signals (“signals” is a term meaning information traffic) across the Microsoft network.
- Uses artificial intelligence and machine learning capabilities.
- Integrates this data across different security products to address different attack scenarios.

The signals obtained from the Intelligent Security Graph, plus other third-party feeds, are fed into Microsoft's three major platforms: Windows, Azure, and Microsoft 365. Microsoft then integrates these signals so that security services on one platform can communicate with security services on one of the other platforms. As a result, any threat seen in Windows is automatically and quickly added to the set of threats that Azure views. This design provides deep insight into the evolving cyber threat landscape.

Threat Intelligence in Microsoft Sentinel

Within a Security Information and Event Management (SIEM) solution like Microsoft Sentinel, the most commonly used form of CTI is threat indicators, also known as Indicators of Compromise or IoCs. Threat indicators are data that associate observed artifacts such as URLs, file

hashes, or IP addresses with known threat activity such as phishing, botnets, or malware. Using Microsoft Sentinel, you can evaluate threat indicators to help detect malicious activity observed in your environment and provide context to security investigators to help inform response decisions.

Integrate threat intelligence (TI) into Microsoft Sentinel through the following activities:

- Import threat intelligence into Microsoft Sentinel by enabling data connectors to various TI platforms and feeds.
- View and manage the imported threat intelligence in Logs and the Microsoft Sentinel Threat Intelligence page.
- Detect threats and generate security alerts and incidents using the built-in Analytics rule templates based on your imported threat intelligence.
- Visualize key information about your imported threat intelligence in Microsoft Sentinel with the Threat Intelligence workbook.

Threat Intelligence in Defender for Endpoint

With Microsoft 365 Defender, you can create custom threat alerts that help you keep track of possible attack activities in your organization. You can flag suspicious events to gather clues and possibly stop an attack chain. These custom threat alerts will only appear in your organization and will flag events that you set it to track.

Before creating custom threat alerts, it's important to know the concepts behind alert definitions and indicators of compromise (IOCs) and their relationship.

Alert definitions

Alert definitions are contextual attributes that can be used collectively to identify early clues on a possible cybersecurity attack. These indicators are typically a combination of activities, characteristics, and actions taken by an attacker to successfully achieve the objective of an attack. Monitoring these combinations of attributes is critical in gaining a vantage point against attacks. These possibly interfere with the chain of events before an attacker's objective is reached.

Indicators of compromise (IOC)

IOCs are individually known malicious events that indicate that a network or device has already been breached. Unlike alert definitions, these indicators are considered evidence of a breach. They're often seen after an attack has already been carried out, and the objective has been reached, such as exfiltration. Keeping track of IOCs is also important during forensic investigations. Although it might not be able

to intervene with an attack chain, gathering these indicators can be useful in creating better defenses for possible future attacks.

Relationship between alert definitions and IOCs

In Microsoft 365 Defender and Microsoft Defender for Endpoint, alert definitions are containers for IOCs and define the alert, including the metadata raised for a specific IOC match. Various metadata is provided as part of the alert definitions. Metadata such as alert definition, attack name, severity, and description is provided along with other options.

Each IOC defines the concrete detection logic based on its type, value, and action, determining how it's matched. It's bound to a specific alert definition that defines how detection is displayed as an alert on the Microsoft 365 Defender console.

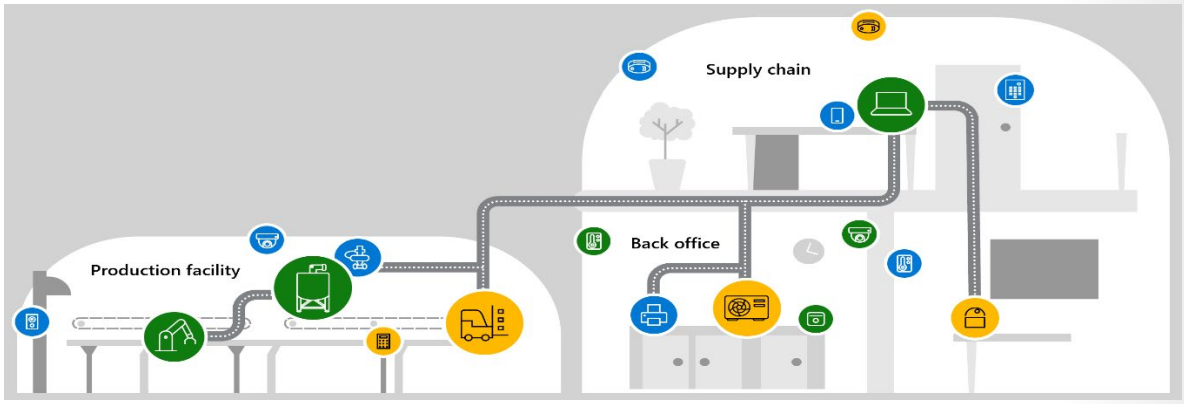
Here's an example of an IOC:

- Type: Sha1
- Value: 92cfceb39d57d914ed8b14d0e37643de0797ae56
- Action: Equals

Threat Intelligence in Defender for IoT

Microsoft Defender for IoT is a unified security solution for identifying IoT and OT devices, vulnerabilities, and threats and managing them through a central interface.

Defender for IoT has **native threat intelligence capabilities**[90] using threat intelligence packages. You can deploy Microsoft Defender for IoT in Azure-connected and hybrid environments or completely on-premises. If you choose to integrate Defender for IoT with Microsoft Sentinel, you'll get threat intelligence from Defender for IoT and the enriched threat intelligence from Sentinel.



90 https://docs.microsoft.com/azure/sentinel/iot-solution?tabs=use-out-of-the-box-analytics-rules-recommended

Defender for IoT has both agent-based and agentless monitoring solutions:

- **For end-user organizations**, Microsoft Defender for IoT provides agentless, network-layer monitoring that integrates smoothly with industrial equipment and SOC tools. You can deploy Microsoft Defender for IoT in Azure-connected and hybrid environments or completely on-premises.
- **For IoT device builders**, Microsoft Defender for IoT also offers a lightweight micro-agent that supports standard IoT operating systems, such as Linux and RTOS. The Microsoft Defender device builder agent helps you ensure that security is built into your IoT/OT projects from the cloud. For more information, see **Microsoft Defender for IoT for device builders documentation**[91].

Threat Intelligence in Defender for Cloud

Defender for Cloud's threat protection works by monitoring security information from your Azure resources, the network, and connected partner solutions. It analyzes this information, often correlating information from multiple sources, to identify threats. For more information, see **How Microsoft Defender for Cloud detects and responds to threats**[92].

When Defender for Cloud identifies a threat, it triggers a **security alert**[93], containing detailed information regarding the event, including suggestions for remediation. To help incident response teams investigate and remediate threats, Defender for Cloud provides threat intelligence reports containing information about detected threats. The report includes information such as:

- Attacker's identity or associations (if this information is available)
- Attackers' objectives
- Current and historical attack campaigns (if this information is available)
- Attackers' tactics, tools, and procedures
- Associated indicators of compromise (IoC) such as URLs and file hashes
- Victimology, which is the industry and geographic prevalence to assist you in determining if your Azure resources are at risk
- Mitigation and remediation information

91 https://docs.microsoft.com/device-builders/index.md
92 https://docs.microsoft.com/azure/defender-for-cloud/alerts-overview#detect-threats
93 https://docs.microsoft.com/azure/defender-for-cloud/managing-and-responding-alerts

Threat Intelligence in Microsoft 365 Defender

Threat investigation and response capabilities provide insights into threats and related response actions available in the Microsoft 365 Defender. These insights can help your organization's security team protect users from email- or file-based attacks. The capabilities help monitor signals and gather data from multiple sources, such as user activity, authentication, email, compromised PCs, and security incidents. Business decision makers and your security operations team can use this information to understand and respond to threats against your organization and protect your intellectual property.

Threat investigation and response capabilities in the Microsoft 365 Defender portal at **https://security.microsoft.com**[94] are a set of tools and response workflows that include:

- **Explorer**[95]
- **Incidents**[96]
- **Attack simulation training**[97]
- **Automated investigation and response**[98]

Best Practices

Microsoft recommends different ways to use threat intelligence feeds to enhance your security analysts' ability to detect and prioritize known threats.

- You can use one of many available integrated threat intelligence platform (TIP) products, you can connect to TAXII servers to take advantage of any STIX-compatible threat intelligence source, and you can also make use of any custom solutions that can communicate directly with the **Microsoft Graph Security tiIndicators API**[99].
- You can also connect to threat intelligence sources from playbooks to enrich incidents with TI information to help direct investigation and response actions.

Additional information on Sharing Technical Threat Intelligence

For more information on Threat Intelligence, see the following:

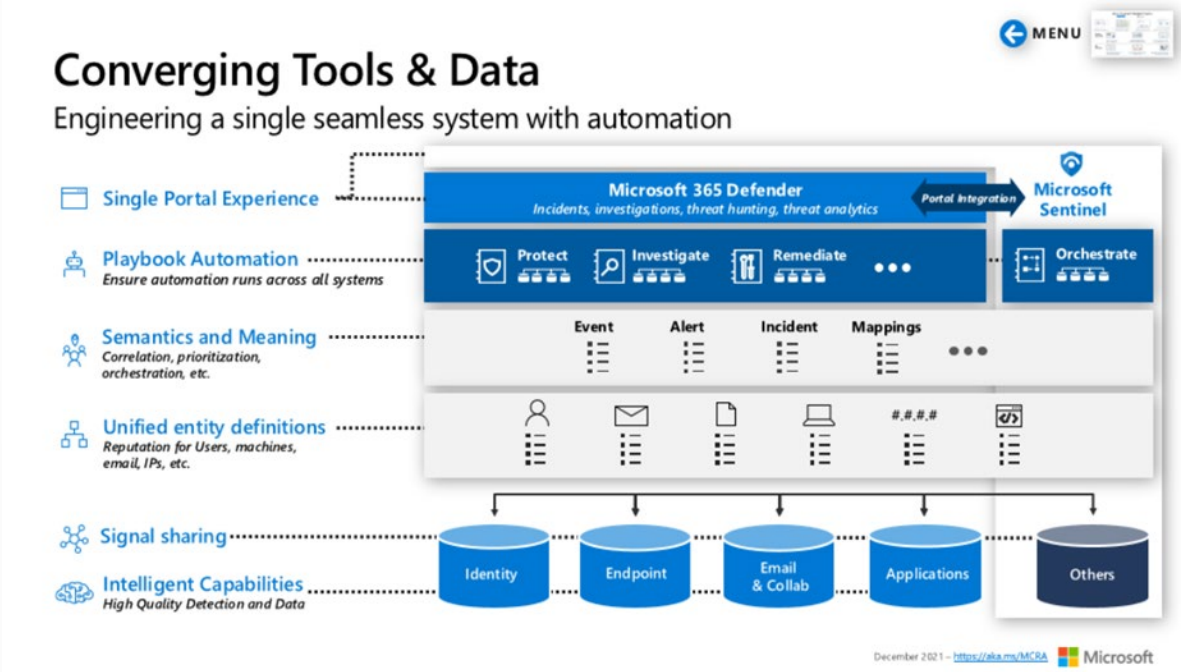
- **TAXII threat intelligence feeds**[100]

94 https://security.microsoft.com/
95 https://docs.microsoft.com/microsoft-365/security/office-365-security/office-365-ti?view=o365-worldwide&preserve-view=true#explorer
96 https://docs.microsoft.com/microsoft-365/security/office-365-security/office-365-ti?view=o365-worldwide&preserve-view=true#incidents
97 https://docs.microsoft.com/microsoft-365/security/office-365-security/attack-simulation-training?view=o365-worldwide&preserve-view=true
98 https://docs.microsoft.com/microsoft-365/security/office-365-security/automated-investigation-response-office?view=o365-worldwide&preserve-view=true
99 https://docs.microsoft.com/graph/api/resources/tiindicator
100 https://steyer.sharepoint.com/sites/MSLearnSC_100/Learning%20Paths%20and%20Modules/LP1%20Design%20a%20Zero%20Trust%20strategy%20and%20architecture/docs.microsoft/com/azure/sentinel/threat-intelligence-integration

- **Best Practices for Security Operations**[101]
- **Integrated threat intelligence platform products**[102]

Monitor sources for insights on threats and mitigations

Advanced cybersecurity attacks comprise multiple complex malicious events, attributes, and contextual information. Identifying and deciding which of these activities qualify as suspicious can be challenging. Your knowledge of known attributes and abnormal activities specific to your industry is fundamental in knowing when to call an observed behavior suspicious.



Threat Intelligence in Microsoft Sentinel

Within a Security Information and Event Management (SIEM) solution like Microsoft Sentinel, the most commonly used form of CTI is threat indicators, also known as Indicators of Compromise or IoCs. Threat indicators are data that associate observed artifacts such as URLs, file hashes, or IP addresses with known threat activity such as phishing, botnets, or malware. Using Microsoft Sentinel, you can evaluate threat indicators to help detect malicious activity observed in your environment and provide context to security investigators to help inform response decisions.
Integrate threat intelligence (TI) into Microsoft Sentinel through the following activities:

- Import threat intelligence into Microsoft Sentinel by enabling data connectors to various TI platforms and feeds.
- View and manage the imported threat intelligence in Logs and the Microsoft Sentinel Threat Intelligence page.

101 https://docs.microsoft.com/security/compass/security-operations-videos-and-decks
102 https://docs.microsoft.com/azure/sentinel/threat-intelligence-integration#integrated-threat-intelligence-platform-products

- Detect threats and generate security alerts and incidents using the built-in Analytics rule templates based on your imported threat intelligence.
- Visualize key information about your imported threat intelligence in Microsoft Sentinel with the Threat Intelligence workbook.

Threat Intelligence in Defender for Endpoint

With Microsoft 365 Defender, you can create custom threat alerts that help you keep track of possible attack activities in your organization. You can flag suspicious events to gather clues and possibly stop an attack chain. These custom threat alerts will only appear in your organization and will flag events that you set it to track.

Before creating custom threat alerts, it's important to know the concepts behind alert definitions and indicators of compromise (IOCs) and their relationship.

Alert definitions

Alert definitions are contextual attributes that can be used collectively to identify early clues on a possible cybersecurity attack. These indicators are typically a combination of activities, characteristics, and actions taken by an attacker to successfully achieve the objective of an attack. Monitoring these combinations of attributes is critical in gaining a vantage point against attacks and possibly interfering with the chain of events before an attacker's objective is reached.

Indicators of compromise (IOC)

IOCs are individually known malicious events that indicate that a network or device has already been breached. Unlike alert definitions, these indicators are considered evidence of a breach. They are often seen after an attack has already been carried out, and the objective has been reached, such as exfiltration. Keeping track of IOCs is also important during forensic investigations. Although it might not be able to intervene with an attack chain, gathering these indicators can be useful in creating better defenses for possible future attacks.

Relationship between alert definitions and IOCs

In Microsoft 365 Defender and Microsoft Defender for Endpoint, alert definitions are containers for IOCs and define the alert, including the metadata raised for a specific IOC match. Various metadata is provided as part of the alert definitions. Metadata such as alert definition, attack name, severity, and description is provided along with other options.

Each IOC defines the concrete detection logic based on its type, value, and action, determining how it is matched. It is bound to a specific alert definition that defines how detection is displayed as an alert on the Microsoft 365 Defender console.

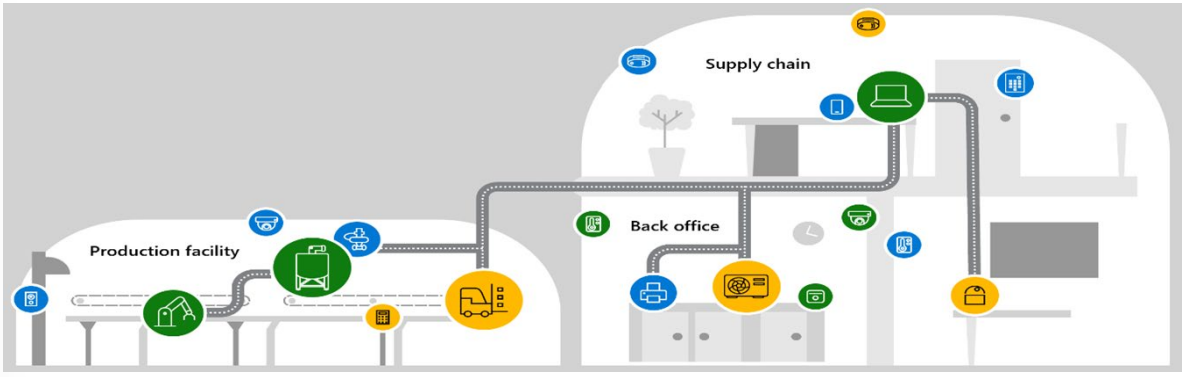
Here is an example of an IOC:

```
Type: Sha1
Value: 92cfceb39d57d914ed8b14d0e37643de0797ae56
Action: Equals
```

Threat Intelligence in Defender for IoT

Microsoft Defender for IoT is a unified security solution for identifying IoT and OT devices, vulnerabilities, and threats and managing them through a central interface.

Defender for IoT has **native threat intelligence capabilities**[103] using threat intelligence packages. You also have the option to **integrate Defender for IoT with Microsoft Sentinel**[104]. If you integrate Defender for IoT with Microsoft Sentinel, you'll get threat intelligence from Defender for IoT as well as the enriched threat intelligence from Sentinel.



Defender for IoT has both agent-based and agentless monitoring solutions:

- For end-user organizations, Microsoft Defender for IoT provides agentless, network-layer monitoring that integrates smoothly with industrial equipment and SOC tools. You can deploy Microsoft Defender for IoT in Azure-connected and hybrid environments or completely on-premises.
- For IoT device builders, Microsoft Defender for IoT also offers a lightweight micro-agent that supports standard IoT operating systems, such as Linux and RTOS. The Microsoft Defender device builder agent helps you ensure that security is built into your IoT/OT projects from the cloud. For more information, see **Microsoft Defender for IoT for device builders documentation**[105]

Threat Intelligence in Defender for Cloud

Defender for Cloud's threat protection works by monitoring security information from your Azure resources, the network, and connected partner solutions. It analyzes this information, often correlating information from multiple sources, to identify threats. For more information, see **How Microsoft Defender for Cloud detects and responds to threats**[106].

When Defender for Cloud identifies a threat, it triggers a **security alert**[107], containing detailed information regarding the event, including suggestions for remediation. To help incident response teams investigate and remediate threats, Defender for Cloud provides threat intelligence reports containing information about detected threats. The report includes information such as:

- Attackers' identities or associations (if this information is available)
- Attackers' objectives
- Current and historical attack campaigns (if this information is available)

103 https://docs.microsoft.com/azure/sentinel/iot-solution?tabs=use-out-of-the-box-analytics-rules-recommended
104 https://docs.microsoft.com/azure/sentinel/iot-solution
105 https://docs.microsoft.com/device-builders/index.md
106 https://docs.microsoft.com/azure/defender-for-cloud/alerts-overview#detect-threats
107 https://docs.microsoft.com/azure/defender-for-cloud/managing-and-responding-alerts

- Attackers' tactics, tools, and procedures
- Associated indicators of compromise (IoC) such as URLs and file hashes
- Victimology, which is the industry and geographic prevalence to assist you in determining if your Azure resources are at risk
- Mitigation and remediation information

Threat Intelligence in Microsoft 365 Defender

Threat investigation and response capabilities provide insights into threats and related response actions available in the Microsoft 365 Defender. These insights can help your organization's security team protect users from email- or file-based attacks. The capabilities help monitor signals and gather data from multiple sources, such as user activity, authentication, email, compromised PCs, and security incidents. Business decision makers and your security operations team can use this information to understand and respond to threats against your organization and protect your intellectual property.

Threat investigation and response capabilities in the Microsoft 365 Defender portal at **https://security.microsoft.com**[108] are a set of tools and response workflows that include:

- **Explorer**[109]
- **Incidents**[110]
- **Attack simulation training**[111]
- **Automated investigation and response**[112]

Best Practices

Microsoft recommends different ways to use threat intelligence feeds to enhance your security analysts' ability to detect and prioritize known threats.

- You can use one of many available integrated threat intelligence platform (TIP) products, you can connect to TAXII servers to take advantage of any STIX-compatible threat intelligence source, and you can also make use of any custom solutions that can communicate directly with the **Microsoft Graph Security tiIndicators API**[113].
- You can also connect to threat intelligence sources from playbooks to enrich incidents with TI information to help direct investigation and response actions.

Additional information on Sharing Technical Threat Intelligence

For more information on Threat Intelligence, see the following:

- TAXII threat intelligence feeds
- Best Practices for Security Operations

108 https://security.microsoft.com/
109 https://docs.microsoft.com/microsoft-365/security/office-365-security/office-365-ti?view=o365-worldwide&preserve-view=true#explorer
110 https://docs.microsoft.com/microsoft-365/security/office-365-security/office-365-ti?view=o365-worldwide&preserve-view=true#incidents
111 https://docs.microsoft.com/microsoft-365/security/office-365-security/attack-simulation-training?view=o365-worldwide&preserve-view=true
112 https://docs.microsoft.com/microsoft-365/security/office-365-security/automated-investigation-response-office?view=o365-worldwide&preserve-view=true
113 https://docs.microsoft.com/graph/api/resources/tiindicator

- Integrated threat intelligence platform products

Exercise

Case Study: Design a Security Operations Solution

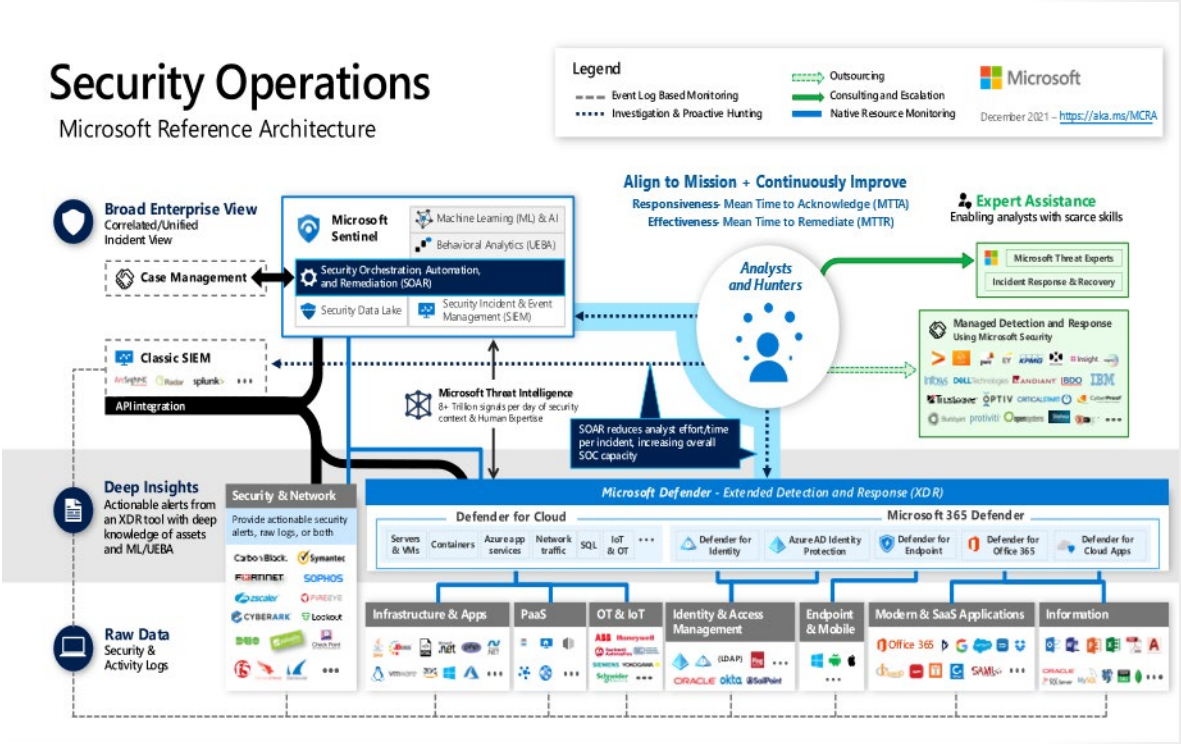
Meet Tailwind Traders

Tailwind Trader is a fictitious home improvement retailer. It operates retail hardware stores across the globe and online. The Tailwind Traders CISO is aware of the opportunities offered by Azure but also understands the need for strong security and solid cloud architecture. Without strong security and a great point of reference architecture, the company may have difficulty managing the Azure environment and costs, which are hard to track and control. The CISO is interested in understanding how Azure manages and enforces security standards.

Requirements

Tailwind Traders is planning to make some significant changes to their Security Operations. They have asked for your assistance with recommendations and questions. Here are the specific requirements.

- **Security and Activity logs** The company has a new security optimization project for customer environments. The CISO wants to ensure that all available Azure logs are sourced and correlated within Microsoft Sentinel.



Tasks

Security and Activity Logs

- **Question** What are different ways Tailwind Traders could collect events, performance data, or custom data provided through the API?
- **Task** Evaluate a solution and explain your decision-making process.
- **Question** What are the different ways Tailwind Traders could prevent, detect, and respond to threats with increased visibility into (and control over) the security of your Azure resources?
- **Task** Evaluate a solution and explain your decision-making process.
- **Question** How are you incorporating Azure Security Operations services available to users to protect their data, applications, and other assets in Microsoft Azure?

Summary

In this module, you've learned how to build an overall security operations strategy with zero trust in mind. You have learned different strategies for designing, defining, and recommending an organizational security strategy and architecture. You should now be able to:

- Design a logging and auditing security strategy
- Develop security operations for hybrid and multi-cloud environments
- Design a strategy for Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR)
- Evaluate security workflows

- Review security strategies for incident management
- Evaluate security operations for technical threat intelligence

Learn more with Azure documentation

- **Security operations in Azure**[114]
- **Azure security logging and auditing**[115]
- **Integrate your SIEM tools with Microsoft Defender for Endpoint**[116]
- **Improve security with Azure Sentinel, a cloud-native SIEM and SOAR solution**[117]
- **Microsoft security incident management - Microsoft Service Assurance**[118]
- **Cyber threat intelligence in Microsoft Sentinel - Azure Example Scenarios**[119]
- **Visualize collected data**[120]
- **Overview - Microsoft Defender for IoT for organizations - Microsoft Defender for IoT**[121]
- **Understand threat intelligence concepts in Microsoft Defender for Endpoint**[122]

Learn more with self-paced training

- **Plan for threat intelligence connectors - Learn**[123]
- **When to use Microsoft Sentinel - Learn**[124]
- **Connect logs to Microsoft Sentinel - Learn**[125]

114 https://docs.microsoft.com/security/compass/security-operations
115 https://docs.microsoft.com/azure/security/fundamentals/log-audit
116 https://docs.microsoft.com/microsoft-365/security/defender-endpoint/configure-siem?view=o365-worldwide&preserve-view=true
117 https://docs.microsoft.com/shows/azure-friday/improve-security-with-azure-sentinel-a-cloud-native-siem-and-soar-solution
118 https://docs.microsoft.com/compliance/assurance/assurance-security-incident-management
119 https://docs.microsoft.com/azure/architecture/example-scenario/data/sentinel-threat-intelligence
120 https://docs.microsoft.com/azure/sentinel/get-visibility
121 https://docs.microsoft.com/azure/defender-for-iot/organizations/overview
122 https://docs.microsoft.com/microsoft-365/security/defender-endpoint/threat-indicator-concepts?view=o365-worldwide&preserve-view=true
123 https://docs.microsoft.com/learn/modules/connect-threat-indicators-to-azure-sentinel/2-plan-for-threat-intelligence-connectors
124 https://docs.microsoft.com/learn/modules/intro-to-azure-sentinel/4-when-to-use-azure-sentinel
125 https://docs.microsoft.com/learn/paths/sc-200-connect-logs-to-azure-sentinel/

Design an identity security strategy

Introduction

In this module, you'll learn how to:

- Recommend an identity store for security
- Recommend secure authentication and security authorization strategies
- Secure conditional access
- Design a strategy for role assignment and delegation
- Define Identity governance for access reviews and entitlement management
- Design a security strategy for privileged role access to infrastructure
- Design a security strategy for privileged access

The content in the module will help you prepare for Exam SC-100: Cybersecurity Architecture. The module concepts are covered in:

- Design a Zero Trust Strategy and Architecture
- Design an Identity Security Strategy

Prerequisites

- Conceptual knowledge of security policies, requirements, zero trust architecture, and management of hybrid environments.
- Working experience with zero trust strategies, applying security policies, and developing security requirements based on business goals.

Identity Security Strategy Overview

The term Identity Security Strategy defines the general process of authenticating and authorizing security principals for an organization. It also involves controlling information about those principals (identities). Security principals (identities) may include services, applications, users, groups, etc. Microsoft identity and access management solutions help IT protect access to applications and resources across the corporate datacenter and into the cloud. Such protection enables additional levels of validation, such as Multi-Factor Authentication and Conditional Access policies.

A good Identity Security Strategy helps maintain control over the applications and resources that are managed in the cloud. Maintaining control over your environment ensures compliancy with:

- Industry standards, such as information security management.
- Corporate or organizational standards, such as ensuring that network data is encrypted.

An efficient Security Strategy and Architecture is most beneficial when there are:

- Multiple engineering teams working in Azure.

- Multiple subscriptions to manage.
- Regulatory requirements that must be enforced.
- Standards that must be followed for all cloud resources.
- Defined secure authentication and authorization strategy.

Secure access to cloud resources

Cloud applications and the mobile workforce have redefined the security perimeter. Employees are bringing their own devices and working remotely. Data is accessed outside the corporate network and shared with external collaborators such as partners and vendors. Corporate applications and data are moving from on-premises to hybrid and cloud environments. Organizations can no longer rely on traditional network controls for security. Controls need to move to where the data is: on devices, inside apps, and with partners.

Identities representing people, services, or IoT devices, are the common dominator across today's many **networks**[126], **endpoints**[127], and **applications**[128]. In the Zero Trust security model, they function as a powerful, flexible, and granular way to control access to **data**[129].

Before an identity attempts to access a resource, organizations must:

- Verify the identity with strong authentication.
- Ensure access is compliant and typical for that identity.
- Follows least privilege access principles.

Once the identity has been verified, we can control that identity's access to resources based on organization policies, ongoing risk
analysis, and other tools.

Identity Zero Trust deployment objectives

Before most organizations start the Zero Trust journey, their approach to identity is problematic in that the on-premises identity provider is
in use, no SSO is present between cloud and on-premises apps, and **visibility**[130] into identity risk is very limited.

When implementing an end-to-end Zero Trust framework for identity, we recommend focusing first on these initial deployment objectives:

- **I. Cloud identity federates with on-premises identity systems**[131]
- **II. Conditional Access policies gate access and provide remediation activities**[132]
- **III. Analytics improve visibility**[133]

126 https://aka.ms/ZTNetwork
127 https://aka.ms/ZTDevices
128 https://aka.ms/ZTApplications
129 https://aka.ms/ZTData
130 https://aka.ms/ZTCrossPillars
131 https://docs.microsoft.com/security/zero-trust/deploy/identity#i-cloud-identity-federates-with-on-premises-identity-systems
132 https://docs.microsoft.com/security/zero-trust/deploy/identity#ii-conditional-access-policies-gate-access-and-provide-remediation-activities
133 https://docs.microsoft.com/security/zero-trust/deploy/identity#iii-analytics-improve-visibility

After these are completed, focus on these additional deployment objectives:

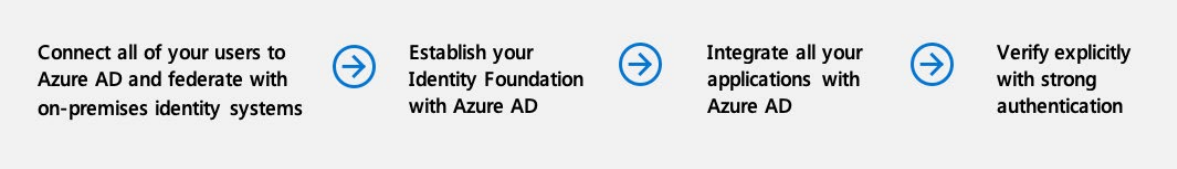
- **IV. Identities and access privileges are managed with identity governance**[134]
- **V. User, device, location, and behavior are analyzed in real time to determine risk and deliver ongoing protection**[135].
- **VI. Integrate threat signals from other security solutions to improve detection, protection, and response**[136].

Identity Zero Trust deployment guide

This guide walks through the steps required to manage identities following the principles of a Zero Trust security framework.

I. Cloud identity federates with on-premises identity systems

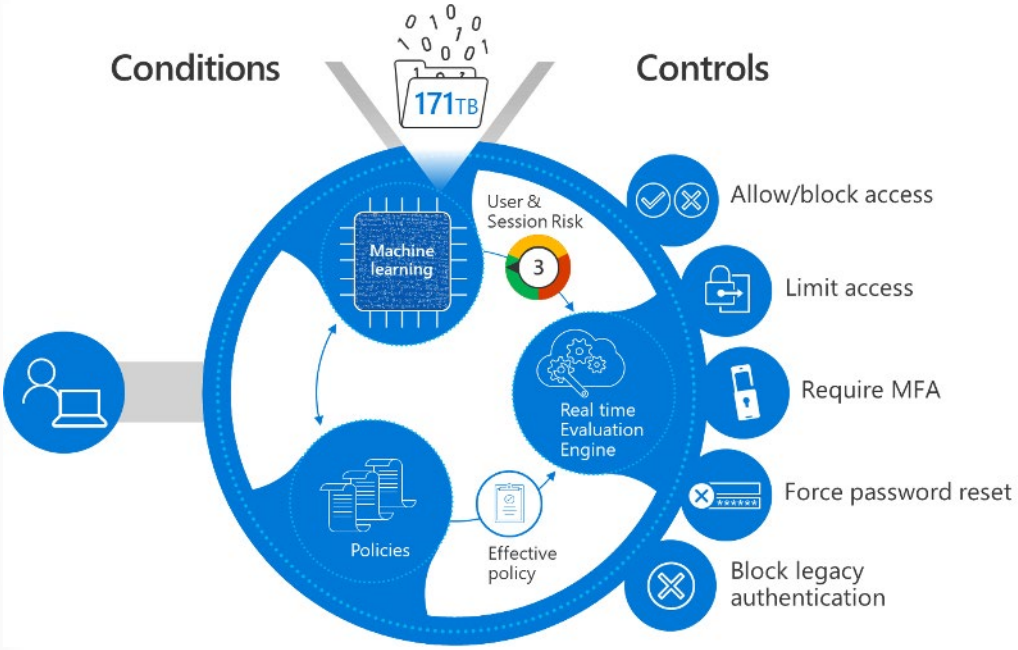
Azure Active Directory (AD) enables strong authentication, a point of integration for endpoint security, and the core of your user-centric policies to guarantee least-privileged access. Azure AD's Conditional Access capabilities are the policy decision point for access to resources based on user identity, environment, device health, and risk—verified explicitly at the point of access. We will show how to implement a Zero Trust identity strategy with Azure AD.



II. Conditional Access policies gate access and provide remediation activities

Azure AD Conditional Access (CA) analyzes signals such as user, device, and location to automate decisions and enforce organizational access policies for the resource. Use CA policies to apply access controls like multifactor authentication (MFA). CA policies allow for prompting users for MFA when needed for security and stay out of users way when not needed.

134 https://docs.microsoft.com/security/zero-trust/deploy/identity#iv-identities-and-access-privileges-are-managed-with-identity-governance
135 https://docs.microsoft.com/security/zero-trust/deploy/identity#v-user-device-location-and-behavior-is-analyzed-in-real-time-to-determine-risk-and-deliver-ongoing-protection
136 https://docs.microsoft.com/security/zero-trust/deploy/identity#vi-integrate-threat-signals-from-other-security-solutions-to-improve-detection-protection-and-response



Planning your Conditional Access policies in advance and having a set of active and fallback policies is a foundational pillar of your Access
Policy enforcement in a Zero Trust deployment. Take the time to configure your trusted IP locations in your environment. Even if they
are not used in a Conditional Access policy, configuring these IPs informs the risk of Identity Protection mentioned above.

III. Analytics improve visibility

As you build your estate in Azure AD with authentication, authorization, and provisioning, it's important to have strong operational insights
into what is happening in the directory.

To configure your logging and reporting to improve visibility, take this step: **Plan an Azure AD reporting and monitoring deployment**[137] to be able to persist and analyze logs from Azure AD, either in Azure or using a SIEM system of choice.

IV. Identities and access privileges are managed with identity governance

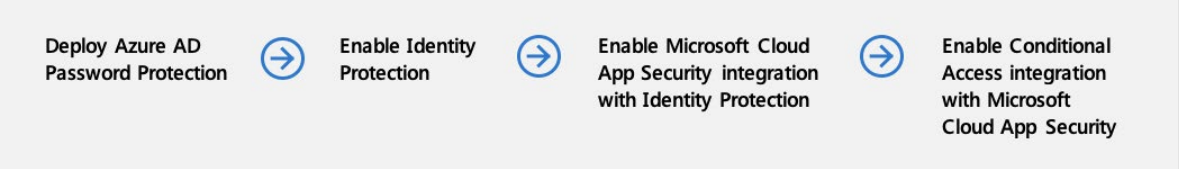
Once the initial three objectives are accomplished, focus on additional objectives such as more robust identity governance.

Secure privileged access with Privileged Identity Management → **Restrict user consent to applications** → **Manage entitlement** → **Use passwordless authentication to reduce the risk of phishing and password attacks**

137 https://docs.microsoft.com/azure/active-directory/reports-monitoring/plan-monitoring-and-reporting

V. User, device, location, and behavior are analyzed in real time to determine risk and deliver ongoing protection

Real-time analysis is critical for determining risk and protection.



VI. Integrate threat signals from other security solutions to improve detection, protection, and response

Finally, other security solutions can be integrated for greater effectiveness.

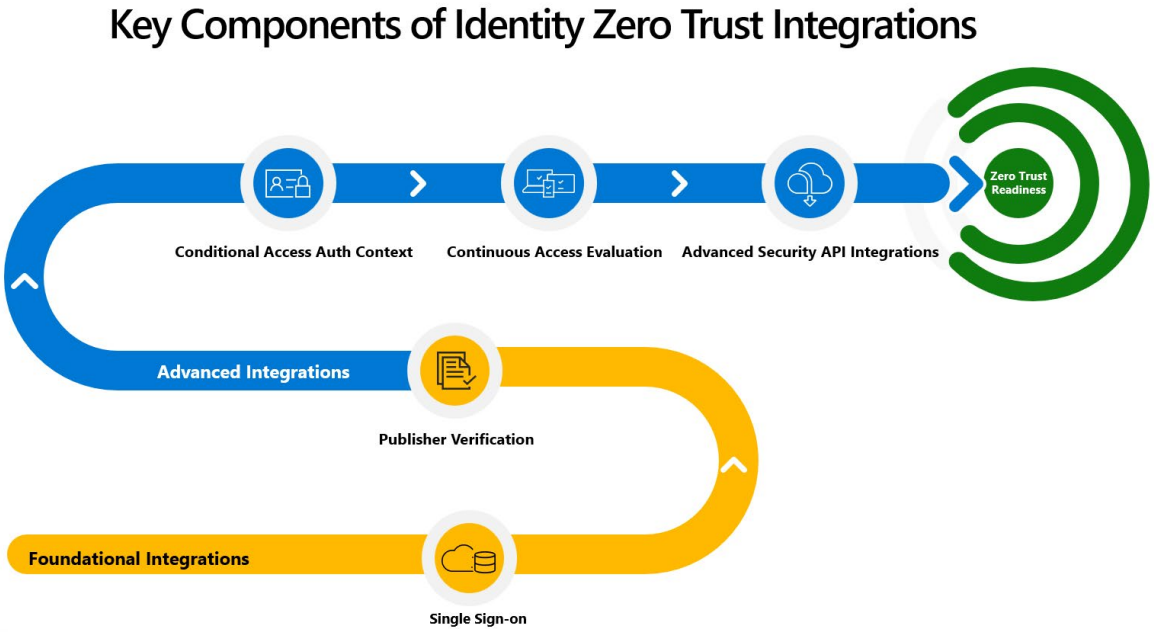
Integration with Microsoft Defender for Identity enables Azure AD to know that a user is indulging in risky behavior while accessing on-premises, non-modern resources (like file shares). This can then be factored into overall user risk. High user risk might lead to blocking further access in the cloud.

Recommend an identity store for security

Azure Active Directory is Microsoft's cloud-based identity and access management service. It provides single sign-on authentication, conditional access, password-less and multifactor authentication, automated user provisioning, and many more features that enable enterprises to protect and automate identity processes at scale.

Azure Active Directory

There are many ways to integrate your solution with Azure Active Directory. Foundational integrations are about protecting your customers using Azure Active Directory's built-in security capabilities. Advanced integrations will take your solution one step further with enhanced security capabilities.



Foundational integrations

Foundational integrations protect your customers with Azure Active Directory's built-in security capabilities.

Enable single sign-on and publisher verification

To enable single sign-on, we recommend publishing your app in **the app gallery**[138].
This will increase customer trust because they know that your application has been validated as compatible with Azure Active Directory, and you can become a **verified publisher**[139] so that customers are certain you're the publisher of the app they're adding to their tenant.

Publishing the app gallery will make it easy for IT admins to integrate the solution into their tenant with automated app registration. Manual registrations are a common cause of support issues with applications. Adding your app to the gallery will avoid these issues with your app.

Integrate user provisioning

Managing identities and access for organizations with thousands of users are challenging. If large organizations use your solution, consider synchronizing information about users and access between your application and Azure Active Directory. This helps keep user access consistent when changes occur.

SCIM (System for Cross-Domain Identity Management) is an open standard for exchanging user identity information. Use the SCIM user management

138 https://www.microsoft.com/security/business/identity-access-management/integrated-apps-azure-ad
139 https://docs.microsoft.com/azure/active-directory/develop/publisher-verification-overview

API to automatically provision users and groups between your application and Azure Active Directory.

Azure Active Directory B2C

Azure Active Directory B2C is a customer identity and access management (CIAM) solution capable of supporting millions of users and billions of authentications per day. It is a white-label authentication solution that enables user experiences that blend with branded web and mobile applications.

As with Azure Active Directory, partners can integrate with Azure Active Directory B2C by using **Microsoft Graph**[140] and key security APIs such as Conditional Access, confirm compromise, and risky user APIs. Read more about those integrations in the Azure AD section above.

Integrate with RESTful endpoints

Independent software vendors can integrate their solutions via RESTful endpoints to enable multifactor authentication (MFA) and role-based access control (RBAC), enable identity verification and proofing, improve security with bot detection and fraud protection, and meet Payment Services Directive 2 (PSD2) Secure Customer Authentication (SCA) requirements.

We have **guidance on how to use our RESTful endpoints**[141] as well as detailed sample walk-throughs of partners who have integrated using the RESTful APIs:

- **Identity verification and proofing**[142], which enables customers to verify the identity of their end users
- **Role-based access control**[143], which enables granular access control to end users
- **Secure hybrid access to the on-premises application**[144], which enables end users to access on-premises and legacy applications with modern authentication protocols
- **Fraud protection**[145], which enables customers to protect their applications and end users from fraudulent login attempts and bot attacks

Recommend secure authentication and security authorization strategies

Choosing the correct authentication method is the first concern for organizations wanting to move their apps to the cloud. Don't take this decision lightly for the following reasons:

- It's the first decision for an organization that wants to move to the cloud.

140 https://docs.microsoft.com/azure/active-directory-b2c/microsoft-graph-operations
141 https://docs.microsoft.com/azure/active-directory-b2c/api-connectors-overview?pivots=b2c-user-flow
142 https://docs.microsoft.com/azure/active-directory-b2c/partner-gallery#identity-verification-and-proofing
143 https://docs.microsoft.com/azure/active-directory-b2c/partner-gallery#role-based-access-control
144 https://docs.microsoft.com/azure/active-directory-b2c/partner-gallery#role-based-access-control
145 https://docs.microsoft.com/azure/active-directory-b2c/partner-gallery#fraud-protection

- The authentication method is a critical component of an organization's presence in the cloud. It controls access to all cloud data and resources.
- It's the foundation of all the other advanced security and user experience features in Azure AD.

Identity is the new control plane of IT security, so authentication is an organization's access to the new cloud world. Organizations need an identity control plane that strengthens their security and keeps their cloud apps safe from intruders.

Secure Authentication methods

When the Azure AD hybrid identity solution is your new control plane, authentication is the foundation of cloud access. Choosing the correct authentication method is a crucial first decision in setting up an Azure AD hybrid identity solution. Implement the authentication method configured by using Azure AD Connect, which also provisions users in the cloud.

To choose an authentication method, consider the time, existing infrastructure, complexity, and cost of implementing your choice. These factors are different for every organization and might change over time.

Azure AD supports the following authentication methods for hybrid identity solutions.

Cloud authentication

When choosing this authentication method, Azure AD handles users' sign-in process. Cloud authentication includes single sign-on (SSO), so that users can sign into cloud apps without re-entering their credentials. With cloud authentication, there are two options:

Azure AD password hash synchronization

The simplest way to enable authentication for on-premises directory objects in Azure AD. Users can use the same username and password that they use on-premises without deploying any additional infrastructure. Some premium features of Azure AD, like Identity Protection and **Azure AD Domain Services**[146], require password hash synchronization, no matter which authentication method is chosen.

Azure AD Pass-through Authentication

Azure AD Pass-through Authentication provides a simple password validation for Azure AD authentication services by using a software
agent that runs on one or more on-premises servers. The servers validate the users directly with your on-premises Active Directory, ensuring that the password validation doesn't happen in the cloud.

Companies with a security requirement to immediately enforce on-premises user account states, password policies, and sign-in hours might use this authentication method. For more information on the actual pass-through

146 https://docs.microsoft.com/azure/active-directory-domain-services/tutorial-create-instance

authentication process, see **User sign-in with Azure AD pass-through authentication**[147].

Federated authentication

Azure AD hands off the authentication process to a separate trusted authentication system when you choose this authentication method. An example is on-premises Active Directory Federation Services (AD FS) to validate the user's password.

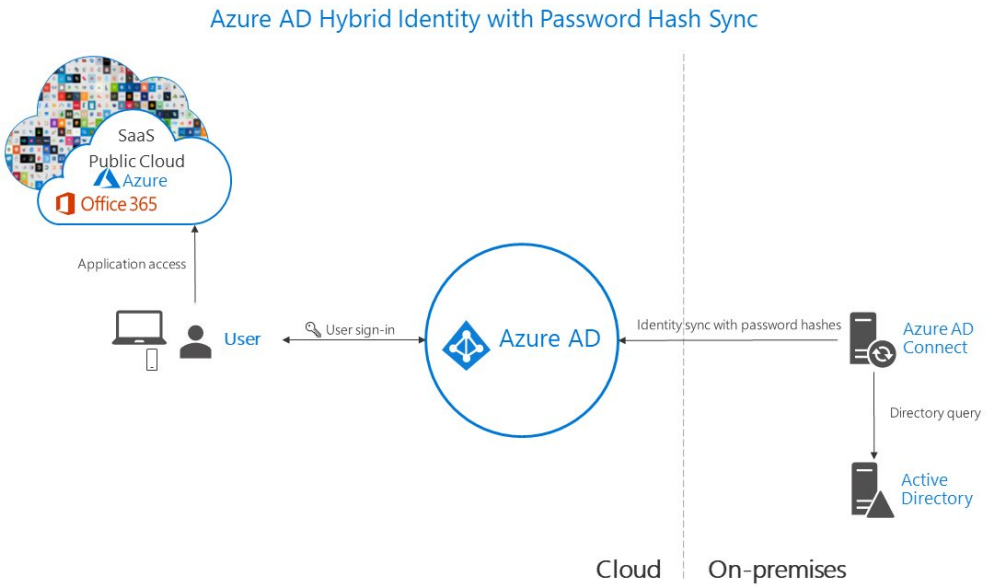
The authentication system can provide additional advanced authentication requirements. Examples are smartcard-based authentication or third-party multifactor authentication. For more information, see **Deploying Active Directory Federation Services**[148].

The following section helps determine which authentication method is right using a decision tree. It helps determine whether to deploy a cloud or federated authentication for an Azure AD hybrid identity solution.

Architecture diagrams

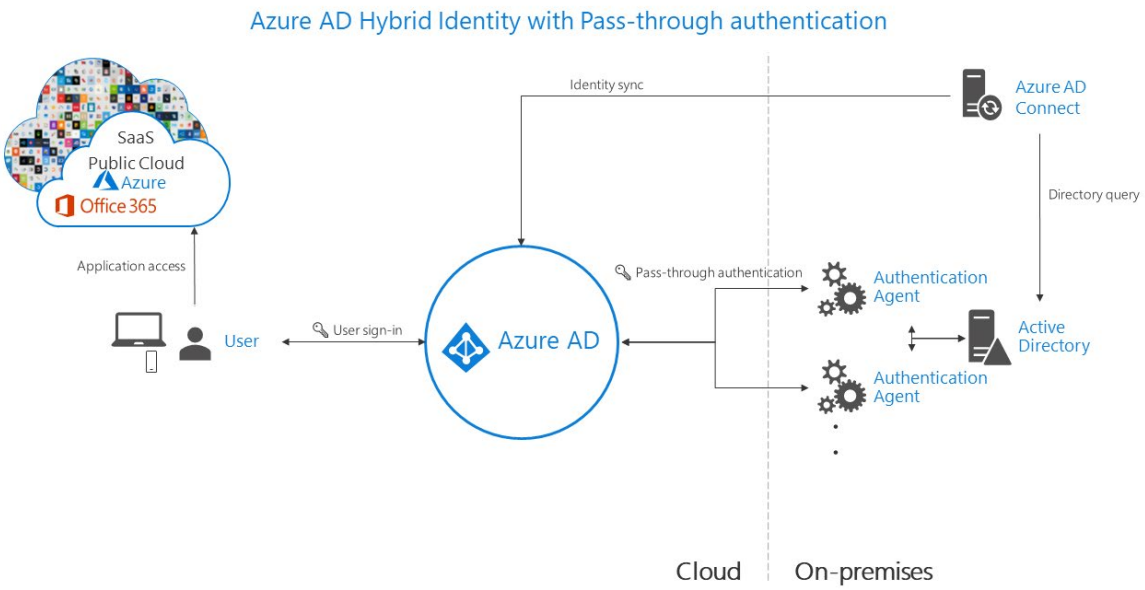
The following diagrams outline the high-level architecture components required for each authentication method that can be used with an Azure AD hybrid identity solution.

The simplicity of a password hash synchronization solution:

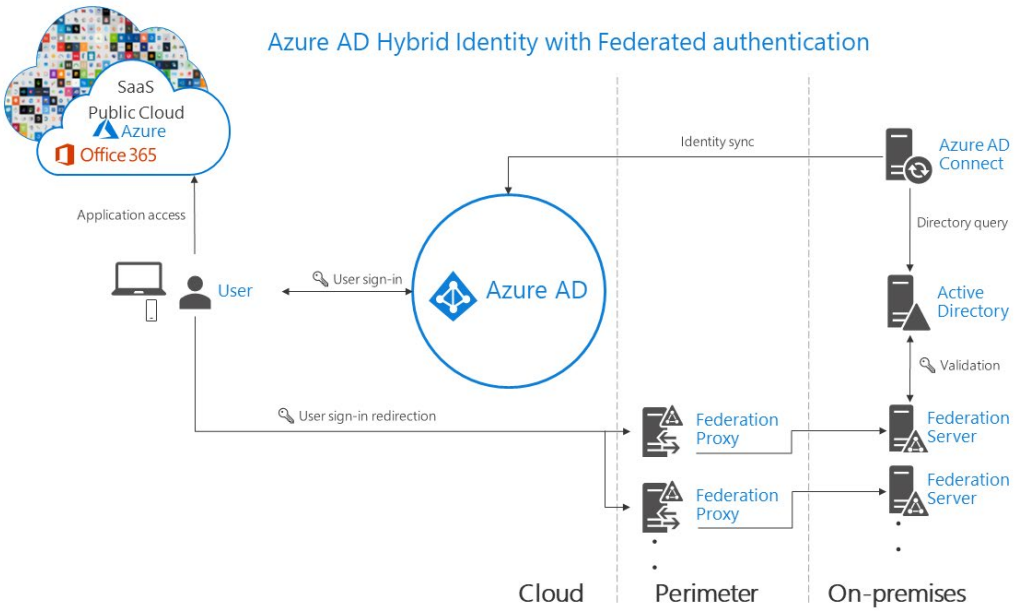


Agent requirements of pass-through authentication, using two agents for redundancy:

147 https://docs.microsoft.com/azure/active-directory/hybrid/how-to-connect-pta
148 https://docs.microsoft.com/windows-server/identity/ad-fs/deployment/windows-server-2012-r2-ad-fs-deployment-guide



Components required for federation in your perimeter and internal network of your organization:



Comparing Authentication Methods

The following table offers a detailed comparison of the various authentication methods available and their respective features.

Consideration	Password hash synchronization + Seamless SSO	Pass-through Authentication + Seamless SSO	Federation with AD FS
Where does authentication happen?	In the cloud	In the cloud, after a secure password verification exchange with the on-premises authentication agent	On-premises
What are the on-premises server requirements beyond the provisioning system: Azure AD Connect?	None	One server for each additional authentication agent	Two or more AD FS servers
			Two or more WAP servers in the perimeter/DMZ network
What are the requirements for on-premises Internet and networking beyond the provisioning system?	None	Outbound Internet access from the servers running authentication agents	Inbound Internet access to WAP servers in the perimeter
			Inbound network access to AD FS servers from WAP servers in the perimeter
			Network load balancing
Is there a TLS/SSL certificate requirement?	No	No	Yes
Is there a health monitoring solution?	Not required	Agent status provided by Azure Active Directory admin center	Azure AD Connect Health
Do users get single sign-on to cloud resources from domain-joined devices within the company network?	Yes with Seamless SSO	Yes with Seamless SSO	Yes
What sign-in types are supported?	UserPrincipalName + password	UserPrincipalName + password	UserPrincipalName + password
	Windows-Integrated Authentication by using Seamless SSO	Windows-Integrated Authentication by using Seamless SSO	sAMAccountName + password
	Alternate login ID	Alternate login ID	Windows-Integrated Authentication
			Certificate and smart card authentication
			Alternate login ID

Consideration	Password hash synchronization + Seamless SSO	Pass-through Authentication + Seamless SSO	Federation with AD FS
Is Windows Hello for Business supported?	Key trust model	Key trust model	Key trust model
		Requires Windows Server 2016 Domain functional level	
			Certificate trust model
What are the multifactor authentication options?	Azure AD MFA	Azure AD MFA	Azure AD MFA
	Custom Controls with Conditional Access*	Custom Controls with Conditional Access*	Azure Multi-Factor Authentication server
			Third-party MFA
			Custom Controls with Conditional Access*
What user account states are supported?	Disabled accounts	Disabled accounts	Disabled accounts
		Account locked out	Account locked out
		Account expired	Account expired
		Password expired	Password expired
		Sign-in hours	Sign-in hours
What are the Conditional Access options?	Azure AD Conditional Access, with Azure AD Premium	Azure AD Conditional Access, with Azure AD Premium	Azure AD Conditional Access, with Azure AD Premium
			AD FS claim rules
Is blocking legacy protocols supported?	Yes	Yes	Yes
Can logo, image, and description be customized on the sign-in pages?	Yes, with Azure AD Premium	Yes, with Azure AD Premium	Yes
What advanced scenarios are supported?	Smart password lockout	Smart password lockout	Multisite low-latency authentication system
	Leaked credentials reports, with Azure AD Premium P2		AD FS extranet lockout
			Integration with third-party identity systems

Secure Authorization Methods

Authorization verifies that the identity attempting to connect has the necessary permissions to access a service, feature, function, object, or method. Authorization always occurs after successful authentication. If a connection isn't authenticated, it fails before any authorization checking is performed. If authentication of a connection succeeds, a

specific action might still be disallowed because the user or group did not have the authorization to perform that action.

Administrators benefit from understanding the following authorization methods to enforce Zero Trust. To learn more about these authorization methods, see **Get started with permissions, access, and security groups**[149].

Authorization Methods

- Security group membership
- Role-based access control
- Access levels
- Feature flags
- Security namespaces & permissions

Secure conditional access

Conditional access[150] is a key part of Zero Trust because it helps to ensure the right user has the right access to the right resources. Enabling Conditional Access allows Azure Active Directory to make access decisions based on computed risk and pre-configured policies. Independent software vendors can take advantage of conditional access by surfacing the option to apply conditional access policies when relevant.

Requirements

Every company has different requirements and security policies. When you create an architecture and follow this suggested framework for Conditional Access, consider the company's requirements. The guidance includes principles related to Zero Trust that can be used as input when you create an architecture. Then, address specific company requirements and policies and adjust the architecture accordingly.

For example, a company might have these requirements:

- At least two factors must protect all access.
- No data on unmanaged devices.
- No guest access is allowed.
- Access to cloud services must be based on password-less authentication.

Conditional Access guidance

This section includes the following articles:

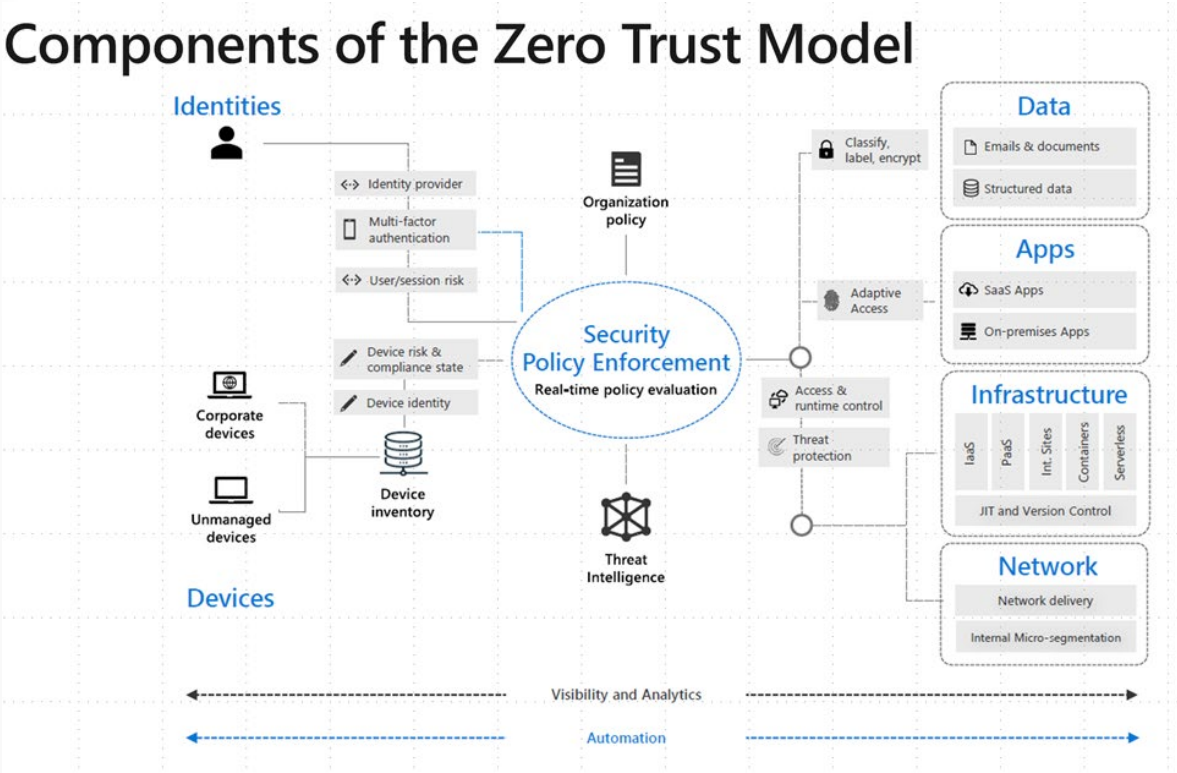
- **Conditional Access design principles and dependencies**[151] provide recommended principles that, together with your company's requirements, serve as input to the suggested persona-based architecture.

149 https://docs.microsoft.com/azure/devops/organizations/security/about-permissions?view=azure-devops&preserve-view=true
150 https://docs.microsoft.com/azure/active-directory/conditional-access/overview
151 https://docs.microsoft.com/azure/architecture/guide/security/conditional-access-design

- **Conditional Access architecture and personas**[152] introduce the persona-based approach for structuring Conditional Access policies. It also provides suggested personas to use as a starting point.
- **Conditional Access framework and policies**[153] provide specific details on how to structure and name Conditional Access policies based on the personas.

Conditional Access as a Zero Trust policy engine

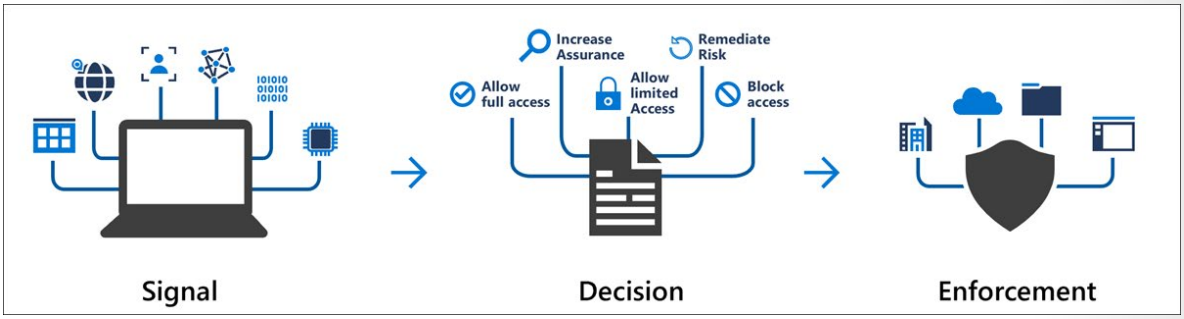
The Microsoft approach to Zero Trust includes Conditional Access as the main policy engine. Here's an overview of that approach:



Download an **SVG file**[154] of this architecture.

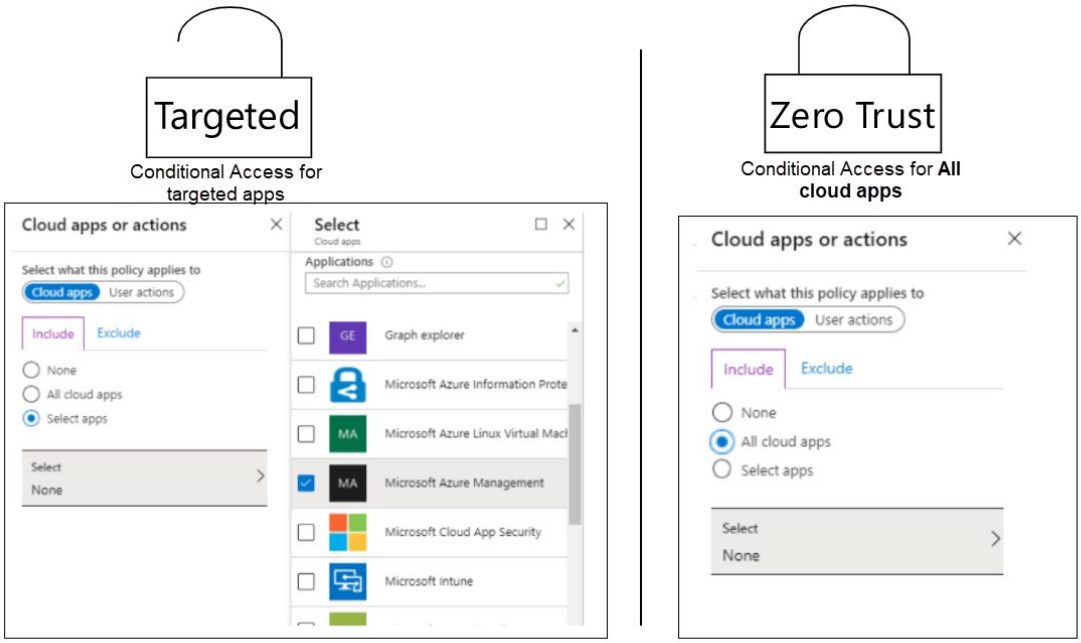
Conditional Access is used as the policy engine for a Zero Trust architecture that covers both policy definition and policy enforcement. Based on various signals or conditions, Conditional Access can block or give limited access to resources, as shown here:

152 https://docs.microsoft.com/azure/architecture/guide/security/conditional-access-architecture
153 https://docs.microsoft.com/azure/architecture/guide/security/conditional-access-framework
154 https://arch-center.azureedge.net/zero-trust-model.svg



Conditional Access Zero Trust architecture

You first need to choose an architecture. We recommend that considering either a Targeted or a Zero Trust Conditional Access architecture. This diagram shows the corresponding settings:



The **Zero Trust Conditional Access architecture** is the one that best fits the principles of Zero Trust. If the **All cloud apps** option in a Conditional Access policy is selected, all endpoints are protected by the provided grant controls, like known users and known or compliant devices. But the policy doesn't just apply to the endpoints and apps that support Conditional Access. It applies to any endpoint that the user interacts with.

The challenge with this sign-in is that it doesn't support device-based Conditional Access. This means that nobody can use the tools and commands if you apply a baseline policy requiring known users and known devices for all cloud apps. Other applications have the same problem with device-based Conditional Access.

The **other architecture, the Targeted one**, is built on the principle that you target only individual apps you want to protect in Conditional Access policies. In this case, endpoints like device-login endpoints aren't protected by the Conditional Access policies, so they continue to work.

The challenge with this architecture is that you might forget to protect all your cloud apps. The number of Office 365 and Azure Active Directory (Azure AD) apps increases as Microsoft and partners release new features, and your IT admins integrate various applications with Azure AD.

Design Conditional Access personas

There are many ways to structure Conditional Access policies. One approach is to structure policies based on the sensitivity of the resource being accessed. In practice, this approach can be difficult to implement in a way that still protects access to resources for various users.

Another approach is defining access policies based on where a user is in the organization. This approach might result in many Conditional Access policies and might be unmanageable.

A better approach is to structure policies related to common access needs and bundle a set of access needs in a persona for a group of users who have the same needs. Personas are identity types that share common enterprise attributes, responsibilities, experiences, objectives, and access. Understanding how enterprise assets and resources are accessed by various personas is integral to developing a comprehensive Zero Trust strategy.

Suggested Conditional Access personas from Microsoft

Microsoft also recommends defining a separate persona for identities that aren't part of any other persona group. This is called the Global persona. Global is meant to enforce policies for identities that aren't in a persona group and policies that should be enforced for all personas.

The following list describes some recommended personas.

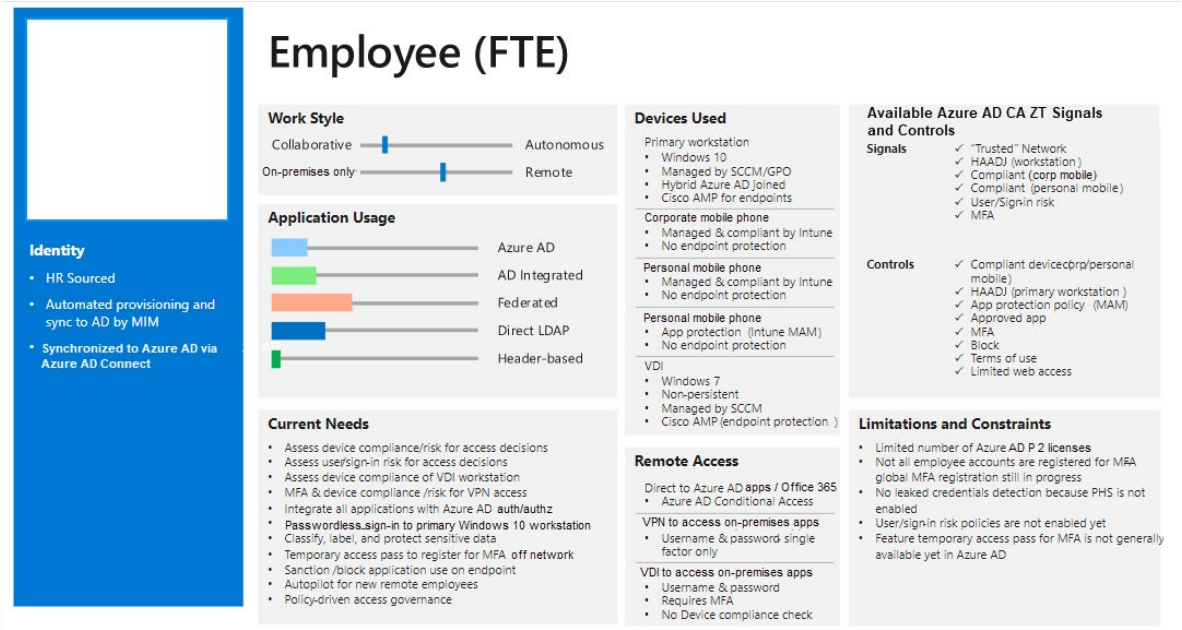
- `Global` - Global is a persona/placeholder for policies that are general. It's used to define policies that apply to all personas or that don't apply to one specific persona. Use it for policies that aren't covered by other personas. You need this persona to protect all relevant scenarios.
- `Admins` - In this context, an admin is any non-guest identity, cloud or synced, that has any Azure AD or other Microsoft 365 admin role (for example, in Microsoft Defender for Cloud Apps, Exchange, Defender for Endpoint, or Compliance Manager). Because guests who have these roles are covered in a different persona, guests are excluded from this persona.
- `Developers` - The Developers persona contains users who have unique needs. They're based on Active Directory accounts synced to Azure AD, but they need special access to services like Azure DevOps, CI/CD pipelines, device code flow, and GitHub. The Developers persona can include users considered internal and others considered external, but a person should be in only one of the personas.

- `Internals` - Internals contains all users who have an Active Directory account synced to Azure AD, are employees of the company and work in a standard end-user role. We recommend that you add internal users who are developers to the Developers persona.
- `Externals` - This persona holds all external consultants who have an Active Directory account synced to Azure AD. We recommend that you add external users who are developers to the Developers persona.
- `Guests` - Guests hold all users who have an Azure AD guest account invited to the customer tenant.
- `GuestAdmins` - The GuestAdmins persona holds all users who have an Azure AD guest account assigned any of the previously mentioned admin roles.
- `Microsoft365ServiceAccounts` - This persona contains cloud (Azure AD) user-based service accounts used to access Microsoft 365 services when no other solution meets the need, like using a managed service identity.
- `AzureServiceAccounts` - This persona contains cloud (Azure AD) user-based service accounts that are used to access Azure (IaaS/PaaS) services when no other solution meets the need, like using a managed service identity.
- `CorpServiceAccounts` - This persona contains user-based service accounts that have all of these characteristics:

  - Originate from on-premises Active Directory. Originate from on-premises Active Directory
  - They are used from on-premises or an IaaS-based virtual machine in another (cloud) datacenter, like Azure.
  - Are synced to an Azure AD instance that accesses any Azure or Microsoft 365 service. Note that this scenario should be avoided.
- `WorkloadIdentities` - This persona contains machine identities, like Azure AD service principals and managed identities. Conditional Access now supports protecting access to resources from these

Access template cards

We recommend that you use access template cards to define the characteristics of each persona. Here's an example:



The template card for each persona provides input for creating the specific Conditional Access policies for each persona.

Conditional Access framework and policies

Important factors to remember in the creation of conditional access policies include:

- Naming conventions - A properly defined naming convention helps you and your colleagues understand the purpose of a policy, which enables easier policy management and troubleshooting. Your naming convention should fit the framework you use to structure your policies.
- Numbering Scheme - use a standard and predictable numbering scheme
- Policy types - recommended types include `BaseProtection`, `IdentityProtection`, `DataProtection`, `AppProtection`, `AttackSurfaceReduction` and `Compliance`
- Standard policy components - Apps, platform types, grant control types, named locations should all be defined in advanced to ensure consistency across all policies

For more details on the recommended framework for conditional access policies, see **Conditional Access framework and policies**[155].

Design a strategy for role assignment and delegation

Azure Active Directory (Azure AD) lets you target Azure AD groups for role assignments. Assigning roles to groups can simplify the management of role assignments in Azure AD with minimal effort from your Global Administrators and Privileged Role Administrators.

155 https://docs.microsoft.com/azure/architecture/guide/security/conditional-access-framework

Why assign roles to groups?

Consider the example where the Contoso company has hired people across geographies to manage and reset passwords for employees in its Azure AD organization. Instead of asking a Privileged Role Administrator or Global Administrator to assign the Helpdesk Administrator role to each person individually, they can create a Contoso_Helpdesk_Administrators group and assign the role to the group. When people join the group, they are assigned the role indirectly. Your existing governance workflow can then take care of the approval process and auditing of the group's membership to ensure that only legitimate users are members of the group and are thus assigned the Helpdesk Administrator role.

Use PIM to make a group eligible for a role assignment

If you do not want members of the group to have standing access to a role, you can use **Azure AD Privileged Identity Management (PIM)**[156] to make a group eligible for a role assignment. Each member of the group is then eligible to activate the role assignment for a fixed time duration.

Best practices for Azure AD roles

This section describes some of the best practices for using Azure Active Directory role-based access control (Azure AD RBAC). These best practices are derived from our experience with Azure AD RBAC and the experiences of customers like yourself.

Manage to least privilege

When planning your access control strategy, it's a best practice to manage to least privilege. Least privilege means you grant your administrators exactly the permission they need to do their job. There are three aspects to consider when you assign a role to your administrators: a specific set of permissions, over a specific scope, for a specific period of time. Avoid assigning broader roles at broader scopes even if it initially seems more convenient to do so. By limiting roles and scopes, you limit what resources are at risk if the security principal is ever compromised. Azure AD RBAC supports over 65 **built-in roles**[157].

There are Azure AD roles to manage directory objects like users, groups, and applications, and also to manage Microsoft 365 services like Exchange, SharePoint, and Intune.

Use Privileged Identity Management to grant just-in-time access

One of the principles of least privilege is that access should be granted only for a specific period of time. **Azure AD Privileged Identity Management (PIM)**[158] lets you grant just-in-time access to your administrators. Microsoft recommends that you enable PIM in Azure AD. Using PIM, a user can be

156 https://docs.microsoft.com/azure/active-directory/privileged-identity-management/pim-configure
157 https://docs.microsoft.com/azure/active-directory/roles/permissions-reference
158 https://docs.microsoft.com/azure/active-directory/privileged-identity-management/pim-configure

made an eligible member of an Azure AD role where they can then activate the role for a limited time when needed. Privileged access is automatically removed when the timeframe expires. You can also **configure PIM settings**[159] to require approval or receive notification emails when someone activates their role assignment. Notifications provide an alert when new users are added to highly privileged roles.

Turn on multifactor authentication (MFA) for all your administrator accounts

Based on our studies[160], your account is 99.9% less likely to be compromised if you use multifactor authentication (MFA).

You can enable MFA on Azure AD roles using two methods:

- **Role settings**[161] in Privileged Identity Management
- **Conditional Access**[162]

Configure recurring access reviews to revoke unneeded permissions over time

Access reviews enable organizations to review administrators' access regularly to make sure only the right people have continued access. Regular auditing of your administrators is crucial because of the following reasons:

- A malicious actor can compromise an account.
- People move teams within a company. If there's no auditing, they can amass unnecessary access over time.

For information about access reviews for roles, see **Create an access review of Azure AD roles in PIM**[163]. For information about access reviews of groups that are assigned roles, see **Create an access review of groups and applications in Azure AD access reviews**[164].

Limit the number of Global Administrators to less than 5

As a best practice, Microsoft recommends that you assign the Global Administrator role to **fewer than five** people in your organization. Global Administrators hold keys to the kingdom, and it is in your best interest to keep the attack surface low. As stated previously, all of these accounts should be protected with multifactor authentication.

Microsoft recommends that you keep two break glass accounts that are permanently assigned to the Global Administrator role. Make sure that

159 https://docs.microsoft.com/azure/active-directory/privileged-identity-management/pim-how-to-change-default-settings
160 https://techcommunity.microsoft.com/t5/azure-active-directory-identity/your-pa-word-doesn-t-matter/ba-p/731984
161 https://docs.microsoft.com/azure/active-directory/privileged-identity-management/pim-how-to-change-default-settings
162 https://docs.microsoft.com/azure/active-directory/conditional-access/howto-conditional-access-policy-admin-mfa
163 https://docs.microsoft.com/azure/active-directory/privileged-identity-management/pim-create-azure-ad-roles-and-resource-roles-review
164 https://docs.microsoft.com/azure/active-directory/governance/create-access-review

these accounts don't require the same multifactor authentication mechanism as your normal administrative accounts to sign in, as described in **Manage emergency access accounts in Azure AD**[165].

Use groups for Azure AD role assignments and delegate the role assignment

If you have an external governance system that takes advantage of groups, then you should consider assigning roles to Azure AD groups instead of individual users. You can also manage role-assignable groups in PIM to ensure that there are no standing owners or members in these privileged groups. For more information, see **Management capabilities for privileged access Azure AD groups**[166].

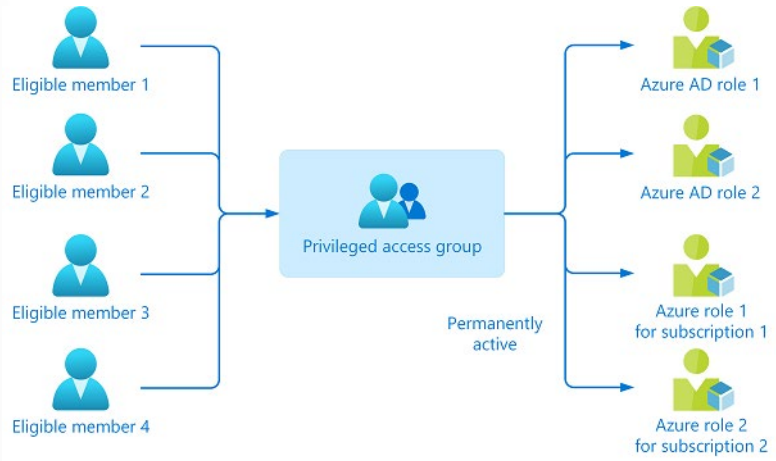
You can assign an owner to role-assignable groups. That owner decides who is added to or removed from the group, so indirectly, decides who gets the role assignment. A Global Administrator or Privileged Role Administrator can delegate role management on a per-role basis by using groups. For more information, see **Use Azure AD groups to manage role assignments**[167].

Activate multiple roles at once using privileged access groups

It may be the case that an individual has five or six eligible assignments to Azure AD roles through PIM. They will have to activate each role individually, which can reduce productivity. Worse still, they can also have tens or hundreds of Azure resources assigned to them, which aggravates the problem.

In this case, you should use **privileged access groups**[168]. Create a privileged access group and grant it permanent access to multiple roles (Azure AD and/or Azure). Make that user an eligible member or owner of this group. With just one activation, they will have access to all the linked resources.

165 https://docs.microsoft.com/azure/active-directory/roles/security-emergency-access
166 https://docs.microsoft.com/azure/active-directory/privileged-identity-management/groups-features
167 https://docs.microsoft.com/azure/active-directory/roles/groups-concept
168 https://docs.microsoft.com/azure/active-directory/privileged-identity-management/groups-features



Use cloud native accounts for Azure AD roles

Avoid using on-premises synced accounts for Azure AD role assignments. If your on-premises account is compromised, it can compromise your Azure AD resources as well.

Why enforce delegation?

To understand how to delegate access governance in entitlement management, it helps to consider an example. Suppose an organization has the following administrator and managers.

Hana is the IT administrator. She has contacts in each department who are responsible for their department's resources and business critical content: Mamta in Marketing, Mark in Finance, and Joe in Legal.

With entitlement management, access governance can be delegated to these non-administrators because they're the ones who know which users need access, for how long, and to which resources. Delegating to non-administrators ensures the right people are managing access for their departments.

Define Identity governance for access reviews and entitlement management

By default, Global administrators and Identity governance administrators can create and manage all aspects of Azure AD entitlement management and easily ensure that users or guests have the appropriate access. You can ask the users themselves or a decision maker to participate in an access review and re-certify (or attest) to users' access. However, the users in these roles may not know all the situations where access packages are required. The reviewers can give their input on each user's need for continued access based on suggestions from Azure AD. When an access review is finished, you can make changes and remove access from users who no longer need it.

Create and perform an access review for users

To perform an access review, you must be assigned one of the following roles:

- Global administrator
- User administrator
- Identity Governance Administrator
- Privileged Role Administrator (for reviews of role-assignable groups only)
- (Preview) Microsoft 365 or Azure Active Directory Security Group owner of the group to be reviewed

If you have the required permissions, go to the **Identity Governance page**[169] to ensure that access reviews are ready for your organization.

You can have one or more users as reviewers in an access review.

Next, do the following:

1. Select a group in Azure AD that has one or more members. Or select an application connected to Azure AD that has one or more users assigned to it.
2. Decide whether to have each user review their own access or to have one or more users review everyone's access.
3. In one of the roles listed above, go to the **Identity Governance page**[170].
4. Create the access review. For more information, see **Create an access review of groups or applications**[171].
5. When the access review starts, ask the reviewers to give input. By default, they each receive an email from Azure AD with a link to the access panel, where they **review access to groups or applications**[172].
6. If the reviewers haven't given input, you can ask Azure AD to send them a reminder. By default, Azure AD automatically sends a reminder halfway to the end date to all reviewers.
7. After the reviewers give input, stop the access review and apply the changes. For more information, see **Complete an access review of groups or applications**[173].

Manage guest access with Azure AD access reviews

With Azure Active Directory (Azure AD), you can easily enable collaboration across organizational boundaries by using the **Azure AD B2B feature**[174].

Guest users from other tenants can be **invited by administrators**[175] or by **other users**[176].

This capability also applies to social identities such as Microsoft accounts.

169 https://portal.azure.com/#blade/Microsoft_AAD_ERM/DashboardBlade/
170 https://portal.azure.com/#blade/Microsoft_AAD_ERM/DashboardBlade/
171 https://docs.microsoft.com/azure/active-directory/governance/create-access-review
172 https://docs.microsoft.com/azure/active-directory/governance/self-access-review
173 https://docs.microsoft.com/azure/active-directory/governance/complete-access-review
174 https://docs.microsoft.com/azure/active-directory/external-identities/what-is-b2b
175 https://docs.microsoft.com/azure/active-directory/external-identities/add-users-administrator
176 https://docs.microsoft.com/azure/active-directory/external-identities/what-is-b2b

You can then decide whether to ask each guest to review their own access or to ask one or more users to review every guest's access.

Create and perform an access review for guests

The same roles required to create an access review for users are also required to create an access review for guests. For more information, see **Create and perform an access review for users**[177].

Azure AD enables several scenarios for reviewing guest users.

You can review either:

- A group in Azure AD that has one or more guests as members.
- An application connected to Azure AD that has one or more guest users assigned to it.

When reviewing guest user access to Microsoft 365 groups, you can either create a review for each group individually or turn on automatic, recurring access reviews of guest users across all Microsoft 365 groups.

Typically it's users within the respective departments, teams, or projects who know who they're collaborating with, using what resources, and for how long. Instead of granting unrestricted permissions to non-administrators, you can grant users the least permissions they need to do their job and avoid creating conflicting or inappropriate access rights.

There are a few main scenarios for delegating access governance from IT administrators to users who aren't administrators:

- Ask guests to review their own membership in a group - You can use access reviews to ensure that users who were invited and added to a group continue to need access. You can easily ask guests to review their own membership in that group. |
- Ask a sponsor to review a guest's membership in a group - You can ask a sponsor, such as the owner of a group, to review a guest's need for continued membership in a group.
- Ask guests to review their own access to an application - You can use access reviews to ensure that users who were invited for a particular application continue to need access. You can easily ask the guests themselves to review their own need for access.
- Ask a sponsor to review a guest's access to an application - You can ask a sponsor, such as the owner of an application, to review the guest's need for continued access to the application.
- Ask guests to review their need for access, in general - In some organizations, guests might not be aware of their group memberships.

Manage entitlement

With applications centrally authenticating and driven from Azure AD, you can now streamline your access request, approval, and re-certification process to make sure that the right people have the right access and
that you have a trail of why users in your organization have the access they have.

Follow these steps:

1. Use Entitlement Management to **create access packages**[178] that users can request as they join different teams/projects and that assign them access to the associated resources (such as applications, SharePoint sites, group memberships).

177 https://docs.microsoft.com/azure/active-directory/governance/manage-access-review#create-and-perform-an-access-review-for-users
178 https://docs.microsoft.com/azure/active-directory/governance/entitlement-management-access-package-create

2. If deploying Entitlement Management isn't possible for your organization at this time, at least enable self-service paradigms in your organization by deploying **self-service group management**[179] and **self-service application access**[180].

Additional information on entitlement

For more information on entitlement, see the following:

- **Entitlement management roles**[181]
- **Required roles to add resources to a catalog**[182]

Design a security strategy for privileged role access to infrastructure

The security of business assets depends on the integrity of the privileged accounts that administer your IT systems. Cyber-attackers use credential theft attacks to target administrator accounts and other privileged access to try to gain access to sensitive data.

For cloud services, prevention and response are the joint responsibilities of the cloud service provider and the customer. For more information about the latest threats to endpoints and the cloud, see the **Microsoft Security Intelligence Report**[183].
This section can help you develop a roadmap toward closing the gaps between your current plans and the guidelines described here.

Traditionally, organizational security was focused on the entry and exit points of a network as the security perimeter. However, SaaS apps and personal devices on the Internet have made this approach less effective. In Azure AD, we replace the network security perimeter with authentication in your organization's identity layer, with users assigned to privileged administrative roles in control. Their access must be protected, whether the environment is on-premises, cloud, or a hybrid.

Securing privileged access requires changes to:

- Processes, administrative practices, and knowledge management
- Technical components such as host defenses, account protections, and identity management

Secure your privileged access in a managed and reported way in the Microsoft services you care about. If you have on-premises administrator accounts, see the guidance for on-premises and hybrid privileged access in Active Directory at **Securing Privileged Access**[184].

179 https://docs.microsoft.com/azure/active-directory/users-groups-roles/groups-self-service-management
180 https://docs.microsoft.com/azure/active-directory/manage-apps/manage-self-service-access
181 https://docs.microsoft.com/azure/active-directory/governance/entitlement-management-delegate#entitlement-management-roles
182 https://docs.microsoft.com/azure/active-directory/governance/entitlement-management-delegate#required-roles-to-add-resources-to-a-catalog
183 https://www.microsoft.com/security/operations/security-intelligence-report
184 https://docs.microsoft.com/windows-server/identity/securing-privileged-access/securing-privileged-access

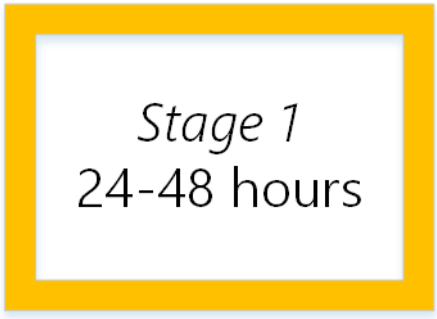
Develop a roadmap

Microsoft recommends that you develop and follow a roadmap to secure privileged access against cyber attackers. You can always adjust your roadmap to accommodate your existing capabilities and specific requirements within your organization. Each stage of the roadmap should raise the cost and difficulty for adversaries to attack privileged access for your on-premises, cloud, and hybrid assets. Microsoft recommends the following four roadmap stages. Schedule the most effective and the quickest implementations first. This article can be your guide based on Microsoft's experiences with cyber-attack incidents and response implementation. The timelines for this roadmap are approximations.

- **Stage 1 (24-48 hours):** Critical items that we recommend you do right away
- **Stage 2 (2-4 weeks):** Mitigate the most frequently used attack techniques
- **Stage 3 (1-3 months):** Build visibility and build full control of administrator activity
- **Stage 4 (six months and beyond):** Continue building defenses to further harden your security platform

This roadmap framework is designed to maximize the use of Microsoft technologies that you may have already deployed. Consider tying into any security tools from other vendors that you have already deployed or are considering deploying.

Stage 1: Critical items to do right now



Stage 1 of the roadmap is focused on critical tasks that are fast and easy to implement. We recommend that you do these few items right away

within the first 24-48 hours to ensure a basic level of secure privileged access. This stage of the Secured Privileged Access roadmap includes the following actions:

- Use Azure AD Privileged Identity Management
- Identify and categorize accounts that are in highly privileged roles
- Define at least two emergency access accounts

Stage 2: Mitigate frequently used attacks

Stage 2 of the roadmap focuses on mitigating the most frequently used attack techniques of credential theft and abuse and can be implemented in approximately 2-4 weeks. This stage of the Secured Privileged Access roadmap includes the following actions:

- Conduct an inventory of services, owners, and administrators
- Identify Microsoft accounts in administrative roles that need to be switched to work or school accounts
- Ensure separate user accounts and mail forwarding for Global Administrator accounts
- Ensure the passwords of administrative accounts have recently changed
- Turn on password hash synchronization
- Require multifactor authentication for users in privileged roles and exposed users
- Configure Identity Protection
- Establish incident/emergency response plan owners
- Secure on-premises privileged administrative accounts

Stage 3: Take control of administrator activity

Stage 3 builds on the mitigations from Stage 2 and should be implemented in approximately 1-3 months. This stage of the Secured Privileged Access roadmap includes the following components.

- Complete an access review of users in administrator roles
- Continue rollout of stronger authentication for all users
- Use dedicated workstations for administration for Azure AD
- Review National Institute of Standards and Technology recommendations for handling incidents
- Implement Privileged Identity Management (PIM) for JIT in additional administrative roles
- Determine exposure to password-based sign-in protocols (if using Exchange Online)
- Inventory your privileged accounts within hosted Virtual Machines
- Implement PIM for Azure AD administrator roles

Use Privileged identity Management with Azure AD administrator roles to manage, control, and monitor access to Azure resources. Using PIM protects by lowering the exposure time of privileges and increasing your visibility into their use through reports and alerts. For more information, see **What is Azure AD Privileged Identity Management**[185].

185 https://docs.microsoft.com/azure/active-directory/privileged-identity-management/pim-configure

Stage 4: Continue building defenses

Stage 4 of the roadmap should be implemented within six months and beyond. Complete your roadmap to strengthen your privileged access protections from potential attacks that are known today. For tomorrow's security threats, we recommend viewing security as an ongoing process to raise the costs and reduce the success rate of adversaries targeting your environment. This stage of the Secured Privileged Access roadmap includes the following components:

- Review administrator roles in Azure AD
- Review users who have the administration of Azure AD joined devices
- Validate incident response plan

Additional information on roadmap framework

For more information on entitlement, see **Secure Access Practices for Administrators in Azure AD**[186].

Design a security strategy for privileged activities

Organizations should make securing privileged access the top security priority because of the significant potential business impact (and high likelihood) of attackers compromising this level of access. Privileged access includes IT administrators controlling large portions of the enterprise estate and other users with access to business-critical assets.

Attackers frequently exploit weaknesses in privileged access security during **human operated ransomware attacks**[187] and targeted data theft. Privileged access accounts and workstations are so attractive to attackers because these targets allow them to rapidly gain broad access to the business assets in the enterprise, often resulting in a rapid and significant business impact.

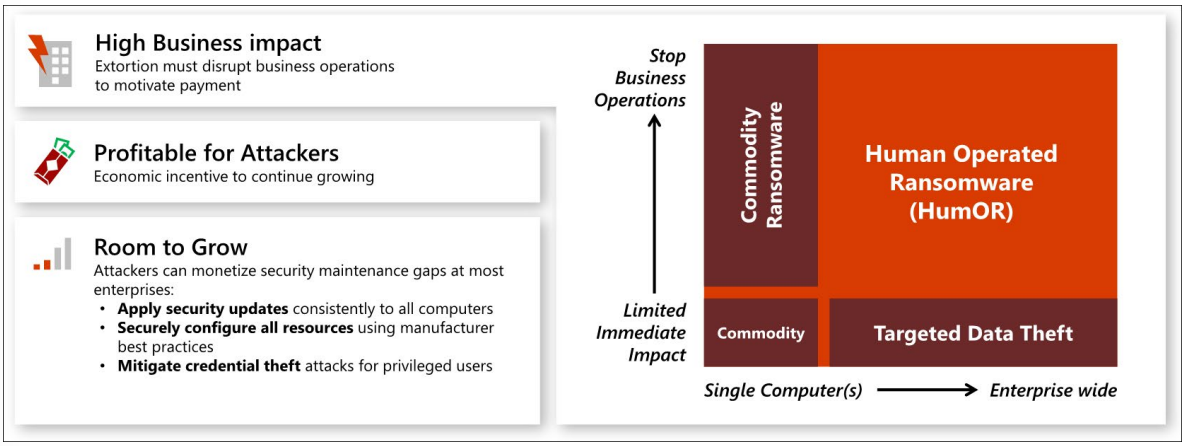
186 https://docs.microsoft.com/azure/active-directory/roles/security-planning
187 https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/

Privileged Access should be the Top Security Priority

Any compromise of these users has a high likelihood of a significant negative impact to the organization. Privileged users have access to business-critical assets in an organization, nearly always causing a major impact when attackers compromise their accounts.

This strategy is built on Zero Trust principles of explicit validation, least privilege, and assumption of breach. Microsoft has provided **implementation guidance**[188] to help you rapidly deploy protections based on this strategy.

This graphic describes how this extortion-based attack is growing in impact and likelihood using privileged access:



- **High business impact:** It is difficult to overstate the potential business impact and damage of a loss of privileged access. Attackers with privileged access effectively have full control of all enterprise assets and resources, allowing them to disclose any confidential data, stop all business processes, or subvert business processes and machines to damage property, hurt people, or worse.
- **High likelihood of occurrence:** The prevalence of privileged access attacks has grown since the advent of modern credential theft attacks starting with **pass the hash techniques**[189]. These techniques first jumped in popularity with criminals starting with the 2008 release of the attack tool "Pass-the-Hash Toolkit" and have grown into a suite of reliable attack techniques (mostly based on the **Mimikatz**[190] toolkit).
  This weaponization and automation of techniques allowed the attacks (and their subsequent impact) to grow rapidly, limited only by the target organization's vulnerability to the attacks and the attacker's monetization/incentive models.

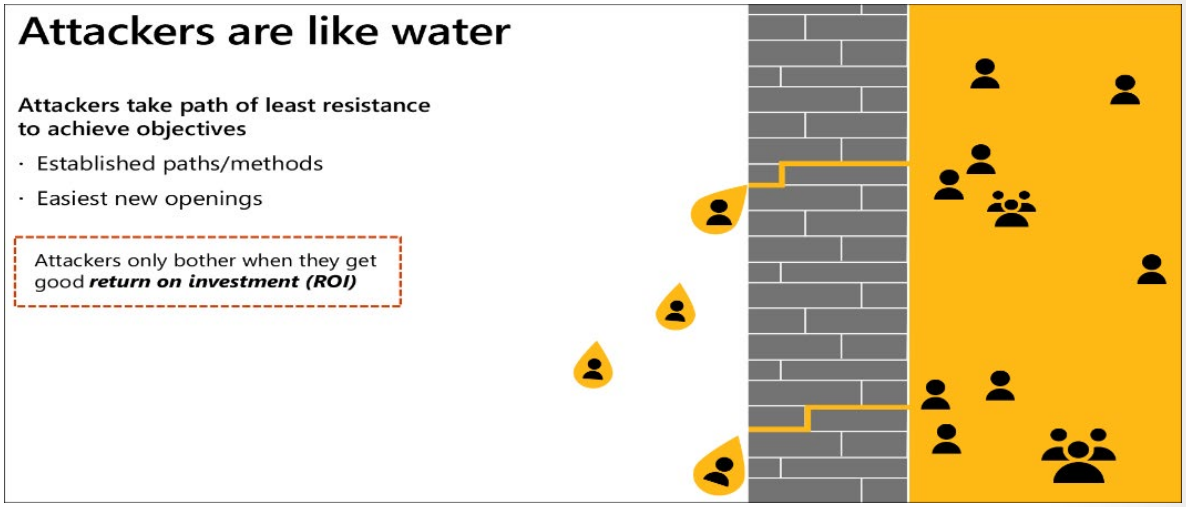
188 https://docs.microsoft.com/security/compass/security-rapid-modernization-plan
189 https://en.wikipedia.org/wiki/Pass_the_hash
190 https://github.com/gentilkiwi/mimikatz

Building your privileged access strategy

A privileged access strategy is a journey that must be composed of quick wins and incremental progress. Each step in a privileged access strategy must take you closer to "seal" out persistent and flexible attackers from privileged access, who are like water trying to seep into environments through any available weakness.

Holistic practical strategy

Reducing the risk from privileged access requires a thoughtful, holistic, and prioritized combination of risk mitigations spanning multiple technologies. Building this strategy requires recognition that attackers are like water as they have numerous options they can exploit (some of which can appear insignificant at first), attackers are flexible in which ones they use, and they generally take the path of least resistance to achieving their objectives.



Building the recommended strategy

Understand strategic goals

Microsoft's recommended strategy is to incrementally build a 'closed loop' system for privileged access that ensures only trustworthy **'clean'**[191] devices, accounts, and intermediary systems can be used for privileged access to business sensitive systems.

Securing Privileged Access has two simple goals:

- Strictly limit the ability to perform privileged actions to a few authorized pathways
- Protect and closely monitor those pathways

191 https://docs.microsoft.com/security/compass/privileged-access-success-criteria#clean-source-principle

There are two types of pathways to accessing the systems, **user access** (to use the capability) and **privileged access** (to manage the capability or access a sensitive capability):

- **User Access** - the lighter blue path on the bottom of the diagram depicts a standard user account performing general productivity tasks like email, collaboration, web browsing, and line-of-business applications or websites. This path includes an account logging on to a device or workstations, sometimes passing through an intermediary like a remote access solution, and interacting with enterprise systems.
- **Privileged Access** - the darker blue path on the top of the diagram depicts privileged access, where privileged accounts like IT Administrators or other sensitive accounts access business critical systems and data or perform administrative tasks on enterprise systems. While the technical components may be similar in nature, the damage an adversary can inflict with privileged access is much higher.

These components collectively comprise the privileged access attack surface that an adversary may target to attempt to gain elevated access to your enterprise.

Lay foundations for successful privileged identity strategy

This strategy requires a combination of:

- **Zero Trust access control** is described throughout this guidance, including the rapid modernization plan (RAMP).
- **Asset protection** protects against direct asset attacks by applying good security hygiene practices to these systems. Asset protection for resources (beyond access control components) is out of the scope of this guidance but typically includes rapid application of security updates/patches, configuring operating systems using manufacturer/industry security baselines, protecting data at rest and in transit, and integrating security best practices to development / DevOps processes.

Security rapid modernization plan

The privileged identity strategy is enabled by the Rapid modernization plan (RAMP). At a high level, RAMP contains the following steps:

1. **Separate and manage privileged accounts**
    1. Emergency access accounts ensure that organizations are not accidentally locked out of their Azure Active Directory (Azure AD) in an emergency. These accounts should be rarely used due to the possibility of risk due to a compromise.
    2. Enable Azure AD Privileged Identity Management (PIM) to discover and secure privileged accounts. PIM provides time-based and approval-based role activation to mitigate the risks of excessive, unnecessary, or misused access permissions.
    3. Identify and categorize privileged accounts (Azure AD) with a high business impact requiring a privileged security level (immediately or over time). The process identifies and minimizes the number of people that require separate accounts and privileged access protection.

4. Use separate accounts (On-premises AD accounts) to ensure administrative functions are isolated from user account activities. All administrator accounts should have mail disabled, and no personal Microsoft accounts should be allowed.
5. Deploy Microsoft Defender for Identity and review any open alerts. All open alerts should be reviewed and mitigated by the appropriate teams.

2. **Improve credential management experience**
    1. Implement and document self-service password reset and combined security information registration by enforcing self-service password reset (SSPR) in your organization.
    2. Protect admin accounts by enforcing MFA / Passwordless for Azure AD privileged users. Require Azure Active Directory Multi-Factor Authentication at sign-in for all individual users who are permanently assigned to one or more of the Azure AD admin roles.
    3. Block legacy authentication protocols for privileged user accounts. Leaving legacy authentication protocols enabled can create an entry point for attackers.
    4. Ensure the application consent process disables the end user's consent to Azure AD applications. Enforcing the process establishes a centralized consent process to maintain centralized visibility and control of the applications that have access to data.
    5. Clean up accounts and sign-in risks by utilizing Azure AD Identity Protection and remediate any discovered risks. Ensure to create a process that monitors and manages user and sign-in risk.

Execute critical strategic initiatives for privileged activity management

The final step of building the recommended strategy for privileged activities is to execute strategic initiatives, such as:

- **End-to-end Session Security** establishes explicit Zero Trust validation for privileged sessions, user sessions, and authorized elevation paths. **Success Criteria** Each session will validate that users' accounts and devices are trusted at a sufficient level before allowing access.
- **Protect & Monitor Identity Systems**, including Directories, Identity Management, Admin Accounts, Consent grants, etc. **Success Criteria:** Each of these systems will be protected at a level appropriate for the potential business impact of accounts hosted in it.
- **Mitigate Lateral Traversal** to protect against lateral traversal with local account passwords, service account passwords, or other secrets. **Success Criteria**: Compromising a single device will not immediately lead to controlling many or all other devices in the environment.
- **Rapid Threat Response** to limit adversary access and time in the environment. **Success Criteria** Incident response processes impede adversaries from reliably conducting a multi-stage attack in the environment that would result in loss of privileged access.

Exercise

Case Study: Design an identity security solution

Tailwind Traders is a fictitious home improvement retailer. It operates retail hardware stores across the globe and online. The Tailwind Traders CISO is aware of the opportunities offered by Azure but also understands the need for strong security and solid cloud architecture. Without strong security and a great point of reference architecture, the company may have difficulty managing the Azure environment and costs, which are hard to track and control. The CISO is interested in understanding how Azure manages and enforces security standards.

Requirements

Tailwind Traders is planning on making some significant changes to their Identity Security Strategy. They have asked for your assistance with recommendations and questions. Here are the specific requirements.

Conditional Access. The company has a new security optimization project for customer environments. The CISO wants to ensure that all available Privileged Users are controlled in the cloud.

Tasks

Question: Conditional Access - What could Tailwind Traders do to enforce Privileged Users to require MFA for all cloud access?

1. Evaluate a solution and explain your decision-making process.
2. Create a Conditional Access Policy that enforces all Global Administrators to require MFA.

3. What could Tailwind Traders do to review administrators' access regularly to ensure only the right people have continued access to Azure resources?
4. Configure recurring access reviews to revoke unneeded permissions over time.

Question: How are you enforcing Identity Security for all users to protect their data, applications, and other assets in Microsoft Azure?

Summary

In this module, you've learned how to build an overall identity security strategy with zero trust in mind. You have learned different strategies for designing, defining, and recommending an organizational security strategy and architecture. You should now be able to:

- Secure access to cloud resources
- Recommend an identity store for security
- Recommend a secure authentication and authorization strategy
- Secure conditional access
- Design a strategy for role assignment and delegation
- Define Identity governance for access reviews and entitlement management
- Design a security strategy for privileged role access to infrastructure
- Design a security strategy for privileged activities

Learn more with Azure documentation

- **Securing identity with Zero Trust**[192]
- **Conditional Access for Zero Trust - Azure Architecture Center**[193]
- **Delegation and roles in entitlement management - Azure AD**[194]
- **Identity Zero Trust integration overview**[195]
- **Use Azure AD groups to manage role assignments - Azure Active Directory**[196]

Learn more with self-paced training

- **Investigate roles in Azure AD - Learn**[197]
- **Explore authentication options - Learn**[198]
- **Explore the zero trust model - Learn**[199]

192 https://docs.microsoft.com/security/zero-trust/deploy/identity
193 https://docs.microsoft.com/azure/architecture/guide/security/conditional-access-zero-trust
194 https://docs.microsoft.com/azure/active-directory/governance/entitlement-management-delegate
195 https://docs.microsoft.com/security/zero-trust/integrate/identity
196 https://docs.microsoft.com/azure/active-directory/roles/groups-concept
197 https://docs.microsoft.com/learn/modules/azure-active-directory/4-roles-azure-active-directory
198 https://docs.microsoft.com/learn/modules/hybrid-identity/3-authentication-options
199 https://docs.microsoft.com/learn/modules/azure-ad-privileged-identity-management/2-microsofts-zero-trust-model

Knowledge check

Check your knowledge

Multiple choice

Item 1. How can Tailwind Traders reference Microsoft Zero Trust Architecture?

- ☐ Develop security requirements based on the organizational financial goals.
- ☐ Identify the integration points for architecture using Microsoft Cybersecurity Reference Architecture (MCRA).
- ☐ Provide familiar security tools and significantly enhanced levels of network security.

Multiple choice

Item 2. How can Tailwind Traders enable IT Admins to integrate their current Windows Server Active Directory solution located on-premises with Microsoft Azure Active Directory?

- ☐ Design and implement a secure hybrid identity environment.
- ☐ Use familiar Azure services and management capabilities, regardless of where they live.
- ☐ Use Azure Policy to define common use cases by using built-ins available in the Azure environment.

Multiple choice

Item 3. How can Tailwind Traders enforce organizational standards and assess compliance at-scale?

- ☐ Use Azure Policy to enable replication and to audit VM protection.
- ☐ Give Conditional Access to resources based on device, identity, assurance, network location, and more.
- ☐ Use Azure Policy to implement governance for resource consistency.

Multiple choice

Item 4. What solution can Tailwind Traders use to evaluate security workflows in their Azure environment?

- ☐ Azure Logic Apps could be used to evaluate and run automated workflows that integrate apps, data, services, and systems.
- ☐ Azure Arc could be used to evaluate and run automated workflows that integrate apps, data, services, and systems.
- ☐ Azure BluePrint could be used to evaluate and run automated workflows that integrate apps, data, services, and systems.

Multiple choice

Item 5. How can Tailwind Traders evaluate and use Threat Intelligence to secure their Azure environment?

- ☐ Using Microsoft Sentinel, you can evaluate threat indicators to help detect malicious activity observed in an Azure environment and provide context to security investigators to help inform response decisions.
- ☐ Using standardized logs, you can monitor for threat indicators in an Azure environment.
- ☐ Using Unified Operations, you can evaluate threat indicators in an Azure environment.

Multiple choice

Item 6. What are some Azure logs Tailwind Traders can monitor for a security incident?

- ☐ You can use Activity Logs, Azure AD Reporting, and Network Security Group flow logs to monitor security incidents.
- ☐ You can monitor storage services for performance metrics.
- ☐ You can monitor Azure Network watcher to monitor diagnostics conditions.

Multiple choice

Item 7. What can Tailwind Traders do to enforce strong authentication?

- ☐ Roll out Azure AD MFA for all users and block legacy authentication using conditional access policies.
- ☐ Use Azure AD MFA for only administrators.
- ☐ Use Application Proxy to restrict access to applications.

Multiple choice

Item 8. How can Tailwind Traders reduce the risk of phishing and password attacks to secure their Azure environment?

- ☐ Enforce Azure AD to deploy FIDO 2.0 or password-less phone sign-in to reduce the risk of phishing and password attacks.
- ☐ Use ADFS to enforce authentication for legacy applications.
- ☐ Enable Azure AD Hybrid Join to block access from clients.

Multiple choice

Item 9. What solution can Tailwind Traders use to monitor for user behavior inside SaaS and modern applications?

- ☐ Enable Microsoft Defender for Cloud Apps integration with Identity Protection.
- ☐ Use Intune to monitor for abnormal behavior with applications.
- ☐ Enforce Azure Active Directory B2C to implement secure white-label authentication.

Answers

Multiple choice

Item 1. How can Tailwind Traders reference Microsoft Zero Trust Architecture?

- ☐ Develop security requirements based on the organizational financial goals.
- ■ Identify the integration points for architecture using Microsoft Cybersecurity Reference Architecture (MCRA).
- ☐ Provide familiar security tools and significantly enhanced levels of network security.

Explanation
Identify the integration points for architecture using Microsoft Cybersecurity Reference Architecture (MCRA).

Multiple choice

Item 2. How can Tailwind Traders enable IT Admins to integrate their current Windows Server Active Directory solution located on-premises with Microsoft Azure Active Directory?

- ■ Design and implement a secure hybrid identity environment.
- ☐ Use familiar Azure services and management capabilities, regardless of where they live.
- ☐ Use Azure Policy to define common use cases by using built-ins available in the Azure environment.

Explanation
Design and implement a secure hybrid identity environment.

Multiple choice

Item 3. How can Tailwind Traders enforce organizational standards and assess compliance at-scale?

- ☐ Use Azure Policy to enable replication and to audit VM protection.
- ☐ Give Conditional Access to resources based on device, identity, assurance, network location, and more.
- ■ Use Azure Policy to implement governance for resource consistency.

Explanation
Use Azure Policy to implement governance for resource consistency.

Multiple choice

Item 4. What solution can Tailwind Traders use to evaluate security workflows in their Azure environment?

- ■ Azure Logic Apps could be used to evaluate and run automated workflows that integrate apps, data, services, and systems.
- ☐ Azure Arc could be used to evaluate and run automated workflows that integrate apps, data, services, and systems.
- ☐ Azure BluePrint could be used to evaluate and run automated workflows that integrate apps, data, services, and systems.

Explanation
Azure Logic Apps could be used to evaluate and run automated workflows that integrate apps, data, services, and systems.

Multiple choice

Item 5. How can Tailwind Traders evaluate and use Threat Intelligence to secure their Azure environment?

- ■ Using Microsoft Sentinel, you can evaluate threat indicators to help detect malicious activity observed in an Azure environment and provide context to security investigators to help inform response decisions.
- ☐ Using standardized logs, you can monitor for threat indicators in an Azure environment.
- ☐ Using Unified Operations, you can evaluate threat indicators in an Azure environment.

Explanation
Using Microsoft Sentinel, you can evaluate threat indicators to help detect malicious activity observed in an Azure environment and provide context to security investigators to help inform response decisions.

Multiple choice

Item 6. What are some Azure logs Tailwind Traders can monitor for a security incident?

- ■ You can use Activity Logs, Azure AD Reporting, and Network Security Group flow logs to monitor security incidents.
- ☐ You can monitor storage services for performance metrics.
- ☐ You can monitor Azure Network watcher to monitor diagnostics conditions.

Explanation
You can use Activity Logs, Azure AD Reporting, and Network Security Group flow logs to monitor security incidents.

Multiple choice

Item 7. What can Tailwind Traders do to enforce strong authentication?

- ■ Roll out Azure AD MFA for all users and block legacy authentication using conditional access policies.
- ☐ Use Azure AD MFA for only administrators.
- ☐ Use Application Proxy to restrict access to applications.

Explanation
MFA has to be deployed for all users.

Multiple choice

Item 8. How can Tailwind Traders reduce the risk of phishing and password attacks to secure their Azure environment?

- ■ Enforce Azure AD to deploy FIDO 2.0 or password-less phone sign-in to reduce the risk of phishing and password attacks.
- ☐ Use ADFS to enforce authentication for legacy applications.
- ☐ Enable Azure AD Hybrid Join to block access from clients.

Explanation
Reducing risk of phishing and password attacks isn't achieved by ADFS or Azure AD Hybrid Join.

Multiple choice

Item 9. What solution can Tailwind Traders use to monitor for user behavior inside SaaS and modern applications?

■ Enable Microsoft Defender for Cloud Apps integration with Identity Protection.

☐ Use Intune to monitor for abnormal behavior with applications.

☐ Enforce Azure Active Directory B2C to implement secure white-label authentication.

Explanation
Microsoft Defender for Cloud Apps with Identity Protection is the only of the three solutions that provides user behavior monitoring.

Module 2 Evaluate Governance Risk Compliance (GRC)strategies

Evaluate a regulatory compliance strategy

Introduction

Learn how to evaluate a regulatory compliance strategy for your organization and use the right set of tools to measure progress.

Learning Objectives

In this module, you'll learn how to:

- Interpret compliance requirements and their technical capabilities.
- Evaluate infrastructure compliance by using Microsoft Defender for Cloud.
- Interpret compliance scores and recommend actions to resolve issues or improve security.
- Design and validate implementation of Azure Policy.
- Design for data residency Requirements.
- Translate privacy requirements into requirements for security solutions.

Interpret compliance requirements and their technical capabilities

Cloud governance is the product of an ongoing adoption effort over time, as a true lasting transformation doesn't happen overnight. It becomes critical to evaluate risk tolerance to inform minimally invasive policies that govern cloud adoption and manage risks. In some industries, third-party compliance affects initial policy creation.

Regulatory organizations frequently publish standards and updates to help define good security practices so that organizations can avoid negligence. The purpose and scope of these standards, and regulations

vary. The security requirements, however, can influence the design for data protection and retention, network access, and system security.

Once the business risks are mapped and converted into decisions to policy statements, the cybersecurity architect will be able to establish the regulatory compliance strategy. This strategy also takes into consideration the industry in which the organization belongs or the type of transactions that the organization performs. A good compliance strategy needs to ensure that security controls are implemented to directly map regulatory compliance requirements, that's why is important to have full visibility of the type of business, transactions, and overall business requirements before establishing a regulatory compliance strategy.

Noncompliance can lead to fines or other business impact. Work with your regulators and carefully review the standard to understand both the intent and the literal wording of each requirement. Here are some questions that may help you understand each requirement.

- How is compliance measured?
- Who approves if the workload meets the requirements?
- Are there processes for obtaining attestations?
- What are the documentation requirements?

In traditional governance and incremental governance, corporate policy creates the working definition of governance. Most IT governance actions seek to implement technology to monitor, enforce, operate, and automate those corporate policies. Cloud governance is built on similar concepts.

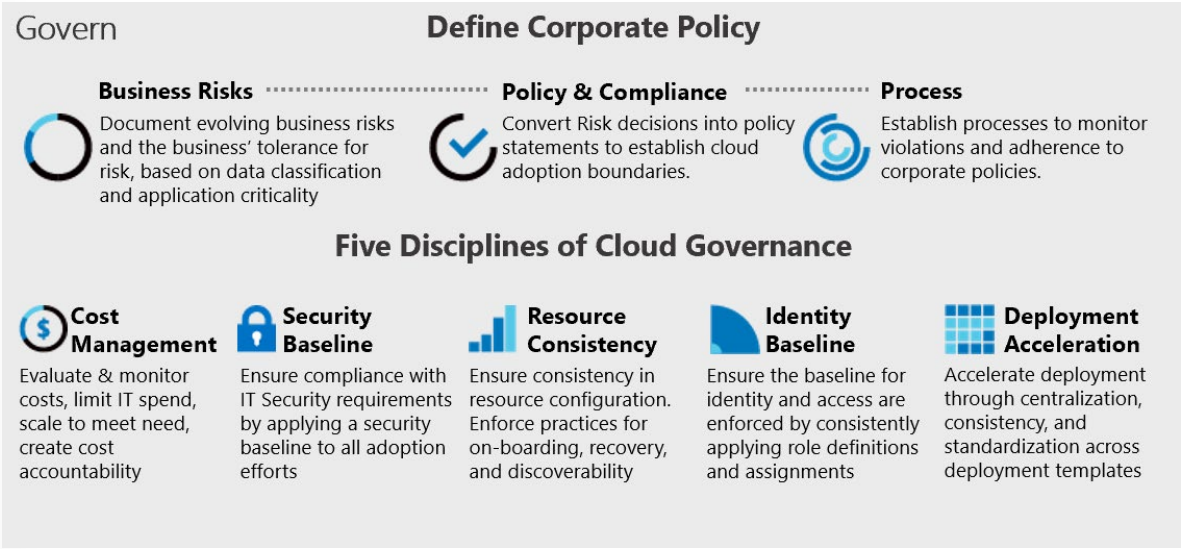


Figure 1: Corporate governance and governance disciplines.

The image above demonstrates the interactions between business risk, policy and compliance, and monitoring and enforcement to create a governance strategy. During the corporate policy definition you'll need to first evaluate the business risk, which includes the investigation of current cloud adoption plans and data classification. In this phase you'll work with the business to balance risk tolerance and mitigation costs.

Once you establish the business risk, you'll evaluate risk tolerance to inform minimally invasive policies that govern cloud adoption and manage risks. Keep in mind that in some industries, third-party compliance affects initial policy creation. The final stage is comprised by the pace of adoption and innovation activities that will naturally create policy violations. Executing relevant processes will aid in monitoring and enforcing adherence to policies.

After defining your corporate policy strategy, which includes regulatory compliance requirements, you'll need to ensure that you have proper governance in place to stay compliant over time as new workloads are provisioned. You can use the five disciplines of cloud governance shown in the diagram as the main pillars for your cloud governance strategy.

Compliance considerations

Organizations may need to be compliant with one or more industry standards. Compliance is based on various types of assurances, including formal certifications, attestations, validations, authorizations, and assessments produced by independent third-party auditing firms, as well as contractual amendments, self-assessments, and customer guidance documents.

Compliance can also be distinguished according to the type of risk, regulatory or operational. According to Federal US regulators, *Operational Risk* is the failure to establish a system of internal controls and an independent assurance function and exposes the organization to the risk of signification fraud, defalcation, and other operational losses. While *Compliance Risk* is the risk of legal or regulatory sanctions, financial loss, or damage to reputation resulting from failure to comply with laws, regulations, rules, other regulatory requirements, or codes of conduct. When planning your compliance strategy, you should take into consideration operational compliance that will support your regulatory compliance.

If your organization uses vendors or other trusted business partners, one of the biggest business risks to consider may be a lack of adherence to **regulatory compliance** by these external organizations. This risk often can't be remediated, and instead may require a strict adherence to requirements by all parties. Make sure you've identified and understand any third-party compliance requirements before beginning a policy review.

Improving **operational compliance** reduces the likelihood of an outage related to configuration drift or vulnerabilities related to systems being improperly patched. The following table gives some examples of operational compliance processes along with the tools that can perform them and their purpose.

Process	Tool	Purpose
Patch Management	Azure Automation Update Management	Management and scheduling of updates
Policy enforcement	Azure Policy	Policy enforcement to ensure environment and guest compliance
Environment configuration	Azure Blueprints	Automated compliance for core services
Resource configuration	Desired State Configuration	Automated configuration on guest OS and some aspects of the environment

The compliance requirements that an organization must follow will vary according to the organization's industry and type of service. Consider a health organization, which could be a doctors' offices, hospitals, health insurers, and other healthcare companies—that create, receive, maintain, transmit, or access protected health information (PHI)—this organization will need to be compliant with the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The regulations issued under HIPAA are a set of US healthcare laws that, among other provisions, establish requirements for the use, disclosure, and safeguarding of PHI. Azure Policy Regulatory Compliance built-in initiative definition maps to compliance domains and controls in HIPAA HITRUST 9.2.

Azure Policy Regulatory Compliance built-in initiative definition maps to compliance domains and controls in Azure Security Benchmark. Each control is associated with one or more Azure Policy defini-

tions. These policies may help you assess compliance with the control; however, there often isn't a one-to-one or complete match between a control and one or more policies. As such, Compliant in Azure Policy refers only to the policy definitions themselves; this doesn't ensure you're fully compliant with all requirements of a control. In addition, the compliance standard includes controls that aren't addressed by any Azure Policy definitions at this time. Therefore, compliance in Azure Policy is only a partial view of your overall compliance status. The associations between compliance domains, controls, and Azure Policy definitions for this compliance standard may change over time.

By default, every subscription has the Azure Security Benchmark assigned. This is the Microsoft-authored, Azure-specific guidelines for security and compliance best practices based on common compliance frameworks. Learn more about Azure Security Benchmark. Available regulatory standards:

- PCI-DSS v3.2.1:2018
- SOC TSP
- NIST SP 800-53 R4
- NIST SP 800 171 R2
- UK OFFICIAL and UK NHS
- Canada Federal PBMM
- Azure CIS 1.1.0
- HIPAA/HITRUST
- SWIFT CSP CSCF v2020
- ISO 27001:2013
- New Zealand ISM Restricted
- CMMC Level 3
- Azure CIS 1.3.0
- NIST SP 800-53 R5
- FedRAMP H
- FedRAMP M

Evaluate infrastructure compliance by using Microsoft Defender for Cloud

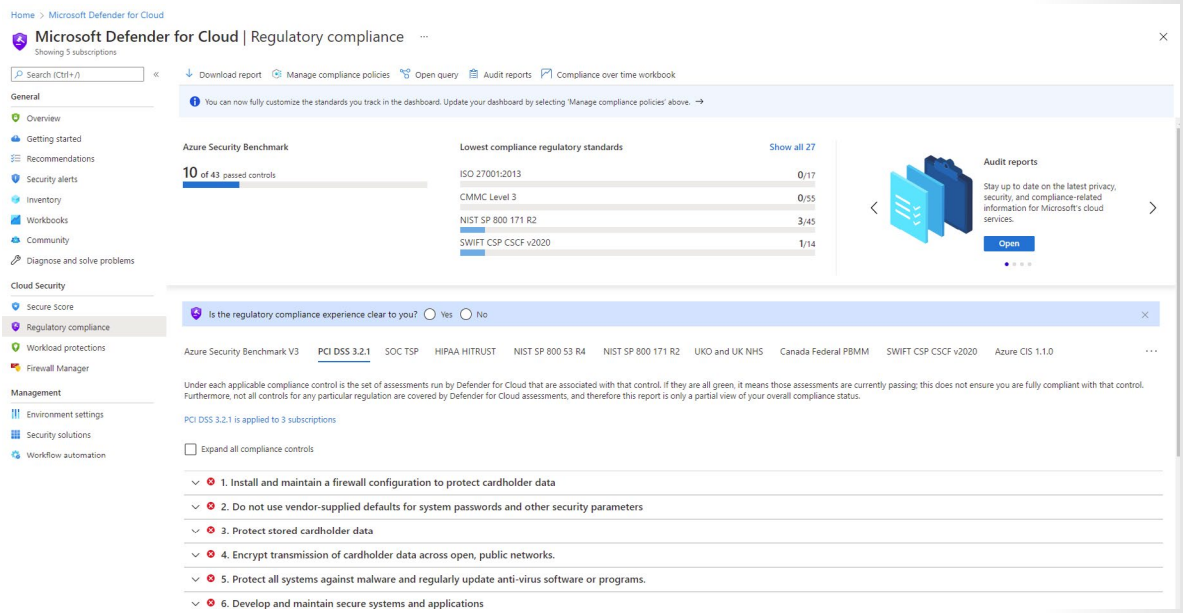
As you establish corporate policy and plan your governance strategies, you can use tools and services like Azure Policy, Azure Blueprints, and Microsoft Defender for Cloud to enforce and automate your organization's governance decisions.

Microsoft Defender for Cloud plays an important part in your governance strategy. It helps you stay on top of security because it:

- Provides a unified view of security across your workloads.
- Collects, searches, and analyzes security data from a variety of sources, which includes firewalls and other partner solutions.
- Provides actionable security recommendations to fix issues before they can be exploited.
- Can be used to apply security policies across your hybrid cloud workloads to ensure compliance with security standards.

Many security features, like security policy and recommendations, are available for free. Some of the more advanced features, like just-in-time VM access and hybrid workload support, are available under the Defender for Cloud Standard tier. Just-in-time VM access can help reduce the network attack surface by controlling access to management ports on Azure VMs.

The regulatory compliance dashboard in Microsoft Defender for Cloud shows your selected compliance standards with all their requirements, where supported requirements are mapped to applicable security assessments. The status of these assessments reflects your compliance with the standard. Below you have an example of the Regulatory Compliance Dashboard in Microsoft Defender for Cloud:

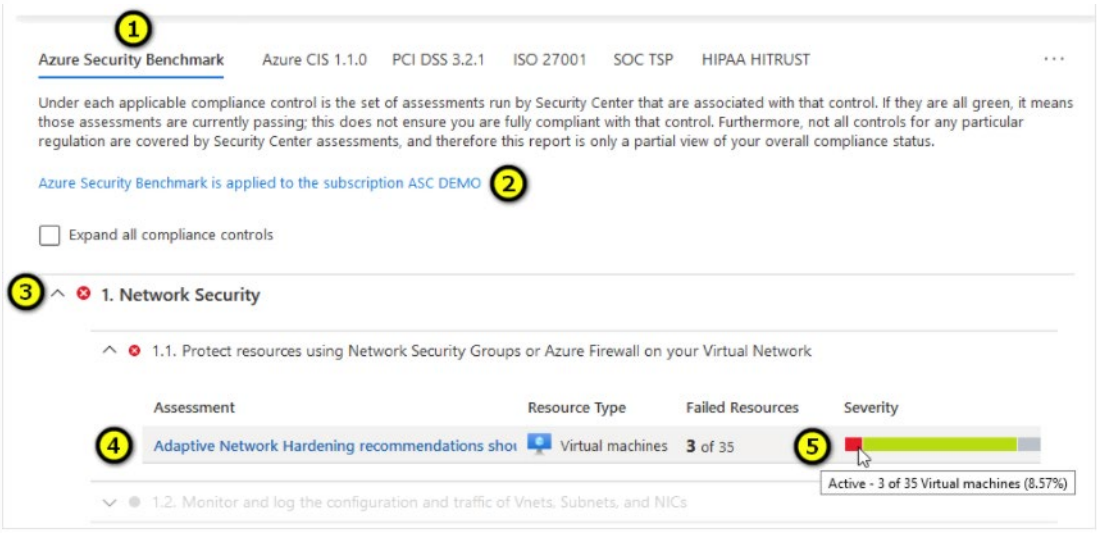


The regulatory compliance dashboard shows the status of all the assessments within your environment for your chosen standards and regulations. As you act on the recommendations and reduce risk factors in your environment, your compliance posture improves.

Using the information in the regulatory compliance dashboard, you can improve your compliance posture by resolving recommendations directly within the dashboard. You can select any of the failing assessments that appear in the dashboard to view the details for that recommendation. Each recommendation includes a set of remediation steps to resolve the issue. From there you can select any of the failing assessments that appear in the dashboard to view the details for that recommendation. Each recommendation includes a set of remediation steps to resolve the issue.

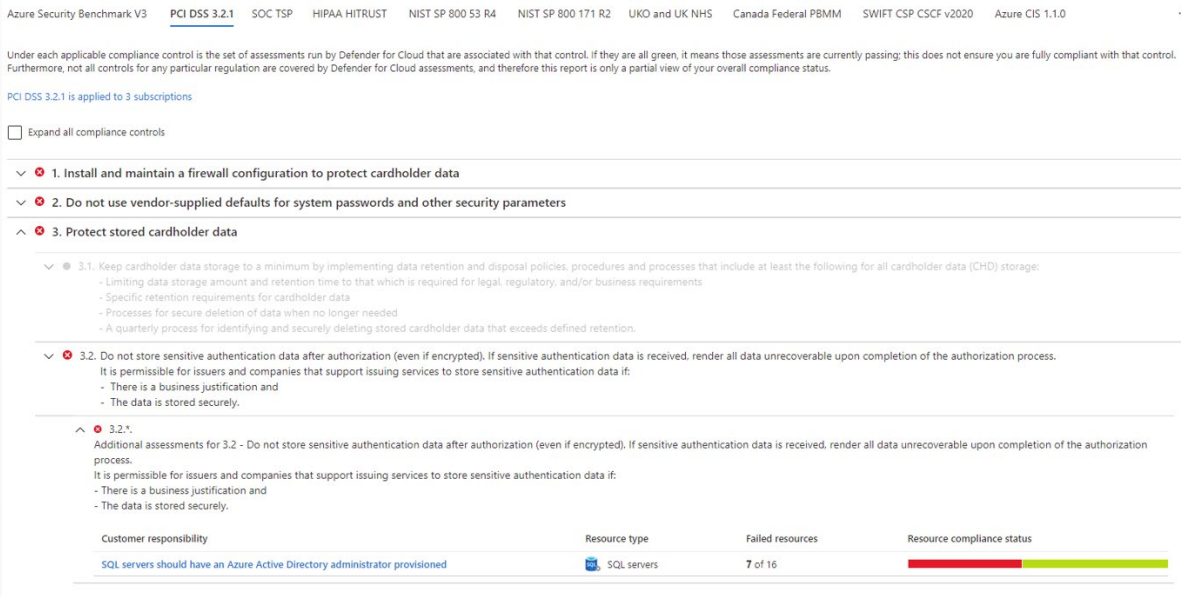
Interpret compliance scores and recommend actions to resolve issues or improve security

When reviewing the assessments, you can select a tab for a compliance standard that is relevant to you (1). You'll see which subscriptions the standard is applied on (2), and the list of all controls for that standard (3). For the applicable controls, you can view the details of passing and failing assessments associated with that control (4), and the number of affected resources (5). Some controls are greyed out. These controls don't have any Defender for Cloud assessments associated with them. Check their requirements and assess them in your environment. Some of these might be process-related and not technical.



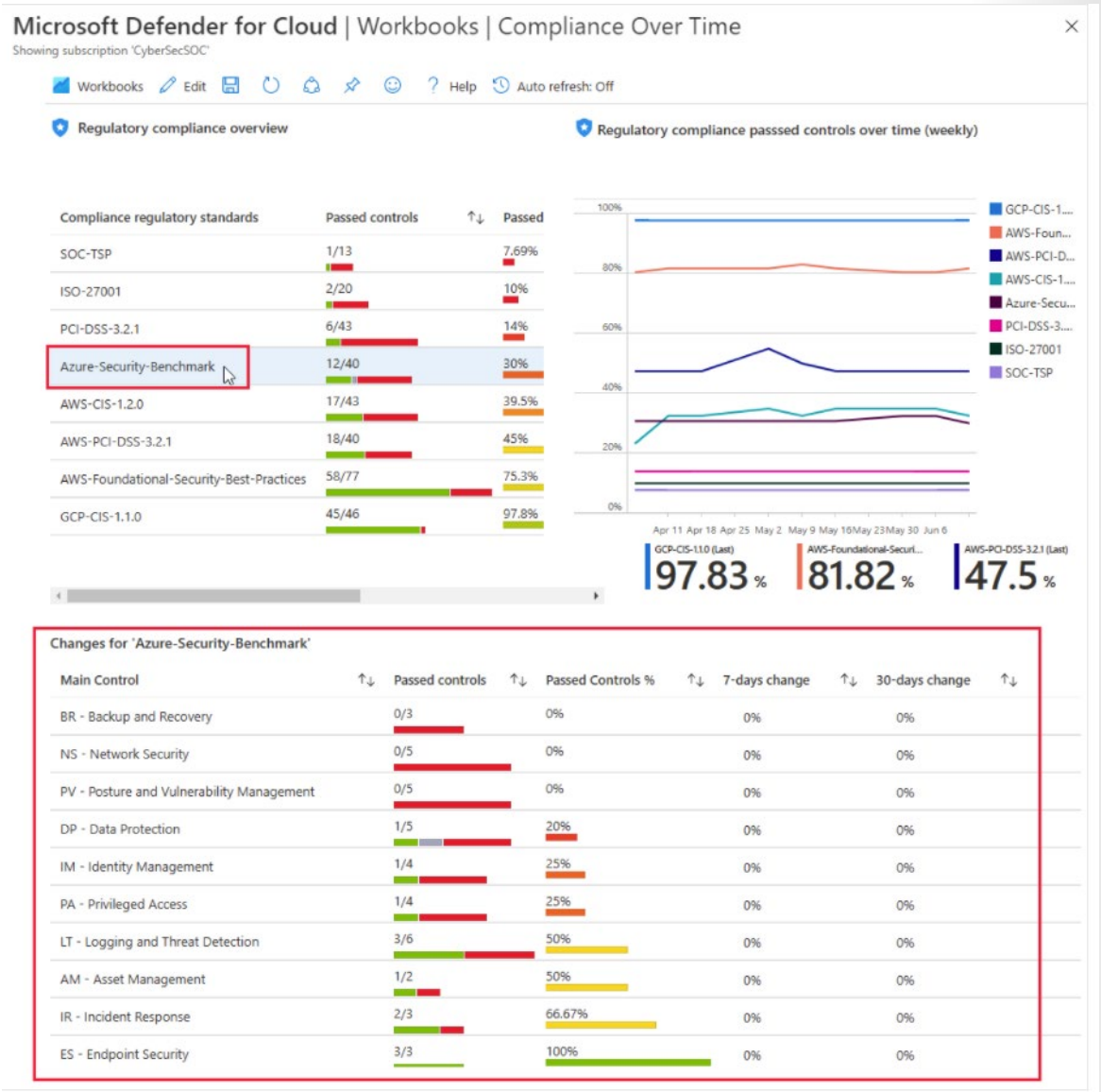
Use the regulatory compliance dashboard to help focus your attention on the gaps in compliance with your chosen standards and regulations.

Let's consider a scenario where Contoso Security Admin needs to ensure their SQL Databases workloads are compliant with PCI DSS 3.2.1. When reviewing the dashboard, he noticed the following item was not compliant:



To address this issue, the Security Admin needs to click on the *SQL servers should have an Azure Active Directory administrator provisioned* recommendation and remediate it.

To track your progress over time you can use the *Compliance Over Time Workbook*. This workbook tracks your compliance status over time with the various standards you've added to your dashboard.



Design and validate implementation of Azure Policy

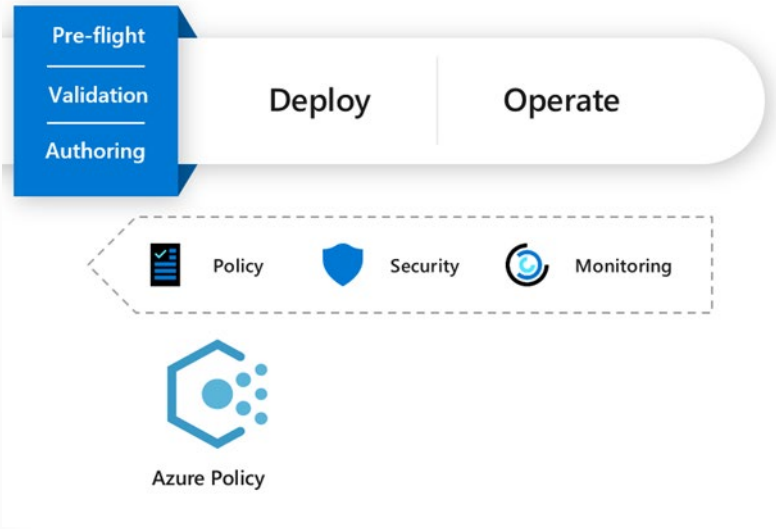
Continuous monitoring is imperative for organizations that are adopting cloud computing since the nature of the workloads is very dynamic. New workloads are provisioned on a daily basis, and it becomes critical to ensure that these workloads are secure by default. In other words, it is necessary to implement guardrails at the beginning of the pipeline to ensure that users are not able to provision unsecure workloads.

Without this continuous monitoring and policy enforcement your environment will be exposed to more risks as the workloads won't be secure by default.

When designing your Azure Policy, you need to take into consideration the organization's needs from the infrastructure perspective as well as compliance. By designing a tailored policy, you can help to reduce the time necessary to audit your environment by having all your compliance data in a single place.

Set Guardrails

Azure Policy can also help to set guardrails throughout your resources to help ensure cloud compliance, avoid misconfigurations, and practice consistent resource governance. Consider also using Azure Policy to reduce the number of external approval processes by implementing policies at the core of the Azure platform for increased developer productivity and control optimization of your cloud spend. Azure Policy will help you govern your Azure resources with simplicity, enforce policies and audit compliance, and monitor compliance continuously. Azure Policy establishes conventions for resources. Policy definitions describe resource compliance conditions and the effect to take if a condition is met. A condition compares a resource property field or a value to a required value. Resource property fields are accessed by using aliases. When a resource property field is an array, a special array alias can be used to select values from all array members and apply a condition to each one. The diagram below shows an example of how Azure Policy can be used in the beginning of the pipeline to ensure that policies are enforced upon the creation of the resources.



Control Costs

By defining conventions, you can control costs and more easily manage your resources. For example, you can specify that only certain types of virtual machines are allowed. Or, you can require that resources have a particular tag. Policy assignments are inherited by child resources. If a policy assignment is applied to a resource group, it's applicable to all the resources in that resource group.

Azure Policy and Azure Resources

When designing your Azure Policy, you need to take into account how the policies will affect your Azure resources to business standards and meet compliance needs. When people, processes, or pipelines create or update resources, Azure Policy reviews the request. When the policy definition effect is *Modify*, *Append*, or *DeployIfNotExists*, Policy alters the request or adds to it. When the policy definition effect is *Audit* or *AuditIfNotExists*, Policy causes an activity log entry to be created for new and updated resources. And when the policy definition effect is *Deny*, Policy stops the creation or alteration of the request.

Validating New Policy

The recommended approach to validating a new policy definition is by following these steps:

- Tightly define your policy.
- Audit your existing resources.
- Audit new or updated resource requests.
- Deploy your policy to resources.
- Continuously monitor.

Tightly define your policy

It's important to understand how the business policy is implemented as a policy definition and the relationship of Azure resources with other Azure services. This step is accomplished by identifying the requirements and determining the resource properties. But it's also important to see beyond the narrow definition of your business policy. Does your policy state for example "All Virtual Machines must..."? What about other Azure services that make use of VMs, such as HDInsight or AKS? When defining a policy, we must consider how this policy impacts resources that are used by other services.

For this reason, your policy definitions should be as tightly defined and focused on the resources and the properties you need to evaluate for compliance as possible.

Audit existing resources

Before looking to manage new or updated resources with your new policy definition, it's best to see how it evaluates a limited subset of existing resources, such as a test resource group. Use the enforcement mode Disabled (*DoNotEnforce*) on your policy assignment to prevent the effect from triggering or activity log entries from being created.

This step gives you a chance to evaluate the compliance results of the new policy on existing resources without impacting workflow. Check that no compliant resources are marked as non-compliant (false positive) and that all the resources you expect to be non-compliant are marked correctly. After the initial subset of resources validates as expected, slowly expand the evaluation to all existing resources.

Evaluating existing resources in this way also provides an opportunity to remediate non-compliant resources before full implementation of the new policy. This cleanup can be done manually or through a remediation task if the policy definition effect is *DeployIfNotExists*.

Audit new or updated resources

Once you've validated your new policy definition is reporting correctly on existing resources, it's time to look at the impact of the policy when resources get created or updated. If the policy definition supports effect parameterization, use Audit. This configuration allows you to monitor the creation and updating of resources to see whether the new policy definition triggers an entry in Azure Activity log for a resource that is non-compliant without impacting existing work or requests.

It's recommended to both update and create new resources that match your policy definition to see that the Audit effect is correctly being triggered when expected. Be on the lookout for resource requests that shouldn't be affected by the new policy definition that trigger the Audit effect. These affected resources are another example of false positives and must be fixed in the policy definition before full implementation.

In the event the policy definition is changed at this stage of testing, it's recommended to begin the validation process over with the auditing of existing resources. A change to the policy definition for a false positive on new or updated resources is likely to also have an impact on existing resources.

Deploy your policy to resources

After completing validation of your new policy definition with both existing resources and new or updated resource requests, you begin the process of implementing the policy. It's recommended to create the policy assignment for the new policy definition to a subset of all resources first, such as a resource group. After validating initial deployment, extend the scope of the policy to broader and broader levels, such as subscriptions and management groups. This expansion is achieved by removing the assignment and creating a new one at the target scopes until it's assigned to the full scope of resources intended to be covered by your new policy definition.

During rollout, if resources are located that should be exempt from your new policy definition, address them in one of the following ways:

- Update the policy definition to be more explicit to reduce unintended impact.
- Change the scope of the policy assignment (by removing and creating a new assignment).
- Add the group of resources to the exclusion list for the policy assignment.

Any changes to the scope (level or exclusions) should be fully validated and communicated with your security and compliance organizations to ensure there are no gaps in coverage.

Monitor your policy and compliance

Implementing and assigning your policy definition isn't the final step. Continuously monitor the compliance level of resources to your new policy definition and set up appropriate Azure Monitor alerts and notifications for when non-compliant devices are identified. It's also recommended to evaluate the policy definition and related assignments on a scheduled basis to validate the policy definition is meeting business policy and compliance needs. Policies should be removed if no longer needed. Policies also need updating from time to time as the underlying Azure resources evolve and add new properties and capabilities.

Design for data residency Requirements

Data sovereignty implies data residency; however, it also introduces rules and requirements that define who has control over and access to customer data stored in the cloud. In many cases, data sovereignty mandates that customer data be subject to the laws and legal jurisdiction of the country or region in which data resides. These laws can have direct implications on data access even for platform maintenance or customer-initiated support requests.

When it comes to compliance, data residency regulations govern the physical locations where data can be stored and how and when it can be transferred, processed, or accessed internationally. These regulations can differ significantly depending on jurisdiction.

For regulatory compliance considerations, data residency considerations may support or even mandate the physical locations where data can be stored, and how and when it can be transferred internationally. These regulations can differ significantly depending on jurisdiction. Azure's regions and service features provide customers with different avenues so they can select and limit data residency and data access. This enables customers in regulated industries to successfully run mission-critical workloads in the cloud and use all the advantages of the Microsoft hyperscale cloud.

Data Sovereignty

When designing your data residency solution, one common requirement is regarding data sovereignty. While it implies data residency; it also introduces rules and requirements that define who has control over and access the data stored in the cloud. In many cases, data sovereignty mandates that customer data be subject to the laws and legal jurisdiction of the country or region in which data resides. These laws can have direct implications on data access even for platform maintenance or customer-initiated support requests. You can use Azure public multi-tenant cloud in combination with Azure Stack products for on-premises and edge solutions to meet your data sovereignty requirements, as described later in this article. These other products can be deployed to put you solely in control of your data, including storage, processing, transmission, and remote access.

Personal Data

As a customer, you retain all rights, titles, and interest in and to customer data—personal data and other content—that you provide for storing and hosting in Azure services. Microsoft will not store or process customer data outside the geography you specify, except for certain services and scenarios. You are also in control of any additional geographies where you decide to deploy your solutions or replicate your data. In addition, you and your users may move, copy, or access your customer data from any location globally. Most Azure services are deployed regionally and enable you to specify where your customer data will be stored and processed. Examples of such regional services include VMs, storage, and SQL Database. To maintain resiliency, Microsoft uses variable network paths that sometimes cross geo boundaries; however, replication of customer data between regions is always transmitted over encrypted network connections.

Consider Azure Policy

When designing your data resident solution, take into consideration the use of Azure Policy. You can use Azure Policy to implement governance over cloud infrastructure and data, including but not limited to regions in which resources can be deployed, which services can be deployed, and resource monitoring requirements. To restrict the data and resources to certain Azure regions, such as for data residency, customers can use the *Allowed Locations* policy. Once policies are established, not only will new resources that are deployed be checked against the policies, but all resources will be periodically scanned to help ensure ongoing compliance.

Consider Azure Blueprints

Another option to take into consideration is the use of Azure Blueprints. Blueprints can be used to help manage data residency for specific compliance needs by specifying both allowed locations and allowed locations for resource groups. The typical scenario to use Azure Blueprints is when you need to create scale deployments by supplying templates to create, deploy, and update fully governed cloud environments to consistent standards, which helps customers comply with regulatory requirements. It differs from Azure Resource Manager (ARM) and Azure Policy in that Blueprints is a package that contains different types of artifacts—including ARM templates, resource groups, policy assignments, and role assignments—all in one container, so you can quickly and easily deploy all these components in a repeatable configuration. Blueprints help to simplify large-scale Azure deployments by packaging policies in a single blueprint definition.

If you want to ensure your data is stored only in your chosen Geography, you should select from the options below:

- Data storage for regional services: Most Azure services are deployed regionally and enable you to specify the region into which the service will be deployed. Microsoft won't store your data outside the Geography you specified except for a few regional services and Preview services as described on the Azure data location page. This commitment helps ensure that your data stored in a given region will remain in the corresponding Geography, and won't be moved to another Geography for most regional services. For service availability, see Products available by region.
- Data storage for non-regional services: Certain Azure services don't enable you to specify the region where the services will be deployed as described on the data location page. For a complete list of non-regional services, see Products available by region.

Your data in an Azure Storage account is always replicated to help ensure durability and high availability. Azure Storage copies your data to protect it from transient hardware failures, network or power outages, and even massive natural disasters. You can typically choose to replicate your data within the same data center, across availability zones within the same region, or across geographically separated regions.

One example of a non-regional service is Azure Active Directory (Azure AD). In other words, Azure AD may store identity data globally, except for Azure AD deployments in:

- The United States, where identity data is stored solely in the United States.
- Europe, where Azure AD keeps most of the identity data within European datacenters except as noted in Identity data storage for European customers in Azure Active Directory.
- Australia and New Zealand, where identity data is stored in Australia except as noted in Customer data storage for Australian and New Zealand customers in Azure Active Directory.

Customers can configure certain Azure services, tiers, or plans to store customer data only in a single region, with certain exceptions. These include Azure Backup, Azure Data Factory, Azure Site Recovery, Azure Stream Analytics, and locally redundant storage (LRS).

Translate privacy requirements into requirements for security solutions

Microsoft has an enduring commitment to protect data privacy, not as an afterthought, but built into Microsoft Azure from the ground up. Microsoft designed Azure with industry-leading security controls, compliance tools, and privacy policies to safeguard your data in the cloud, including the categories of personal data identified by certain security or privacy regulations. These also help you comply with other important global and regional privacy standards such as ISO/IEC 27018, EU-U.S. Privacy Shield, EU Model Clauses, HIPAA/HITECH, and HITRUST.

Leverage Azure Policy

Consider also using Azure Policy to enforce your privacy requirements. Azure Policy is deeply integrated into Azure Resource Manager, which helps your organization to enforce policy across resources. With Azure Policy you can define policies at an organizational level to manage resources and prevent developers from accidentally allocating resources in violation of those policies. You can use Azure Policy in a wide range of compliance scenarios, such as ensuring that your data is encrypted or remains in a specific region to comply with specific security regulations.

Azure's Secure Foundation

When you build on Azure's secure foundation, you accelerate your move to the cloud by achieving compliance more readily, allowing you to enable privacy-sensitive cloud scenarios, such as financial and health service, with confidence. Different organizations will need different levels of privacy requirements based on the industry and compliance standards that are required to follow. Azure provides customers with strong data security, both by default on its own infrastructure, as well as for customer-enabled services.

State of the Data

When designing your solution to fulfill the privacy requirements, take into consideration the state of the data at a certain point of time. For example, for some scenarios it may not be enough to protect the data only when the data is at rest, you may also need to protect it while in-transit. For example, the PCI DSS requirement 4 is about *Encrypt transmission of cardholder data across open, public networks.* To fulfill this requirement your solution must encrypt data in-transit. Below you have some examples of ta protection according to the data stage:

- **At-rest data protection:** Encryption at rest provides data protection for stored data (at rest). Attacks against data at-rest include attempts to obtain physical access to the hardware on which the data is stored, and then compromise the contained data. In such an attack, a server's hard drive may have been mishandled during maintenance allowing an attacker to remove the hard drive. Later the attacker would put the hard drive into a computer under their control to attempt to access the data. Customers are responsible for ensuring that data stored in Azure is encrypted in accordance with their standards. Azure offers a wide range of encryption capabilities, giving customers the flexibility to choose the solution that best meets their needs. Azure Key Vault helps customers easily maintain control of keys that are used by cloud applications and services to encrypt data. Azure Disk Encryption enables customers to encrypt VMs. Azure Storage Service Encryption makes it possible to encrypt all data placed into a customer's storage account.
- **In-transit data protection:** Protecting data in transit should be an essential part of your data protection strategy. Because data is moving back and forth from many locations, we generally recommend that you always use SSL/TLS protocols to exchange data across different locations. In some circumstances, you might want to isolate the entire communication channel between your on-premises and cloud infrastructures by using a VPN. Microsoft provides a number of options that can be utilized by customers for securing data in transit internally within the Azure network and externally across the Internet to the end user. These include communication through Virtual Private Networks (utilizing IPsec/IKE encryption), Transport Layer Security (TLS) 1.2 or later (via Azure components such as Application Gateway or Azure Front Door), protocols directly on the Azure virtual machines (such as Windows IPsec or SMB), and more.

Azure resource providers encryption model support

Microsoft Azure Services each support one or more of the encryptions at rest models. For some services, however, one or more of the encryption models may not be applicable. For services that support customer-managed key scenarios, they may support only a subset of the key types that Azure Key Vault supports for key encryption keys. Additionally, services may release support for these scenarios and key types at different schedules. This section describes the encryption at rest support at the time of this writing for each of the major Azure data storage services.

Azure disk encryption

Any customer using Azure Infrastructure as a Service (IaaS) features can achieve encryption at rest for their IaaS VMs and disks through Azure Disk Encryption. For more information on Azure Disk encryption, see the Azure Disk Encryption documentation.

Azure storage

All Azure Storage services (Blob storage, Queue storage, Table storage, and Azure Files) support server-side encryption at rest; some services additionally support customer-managed keys and client-side encryption.

Azure SQL Database

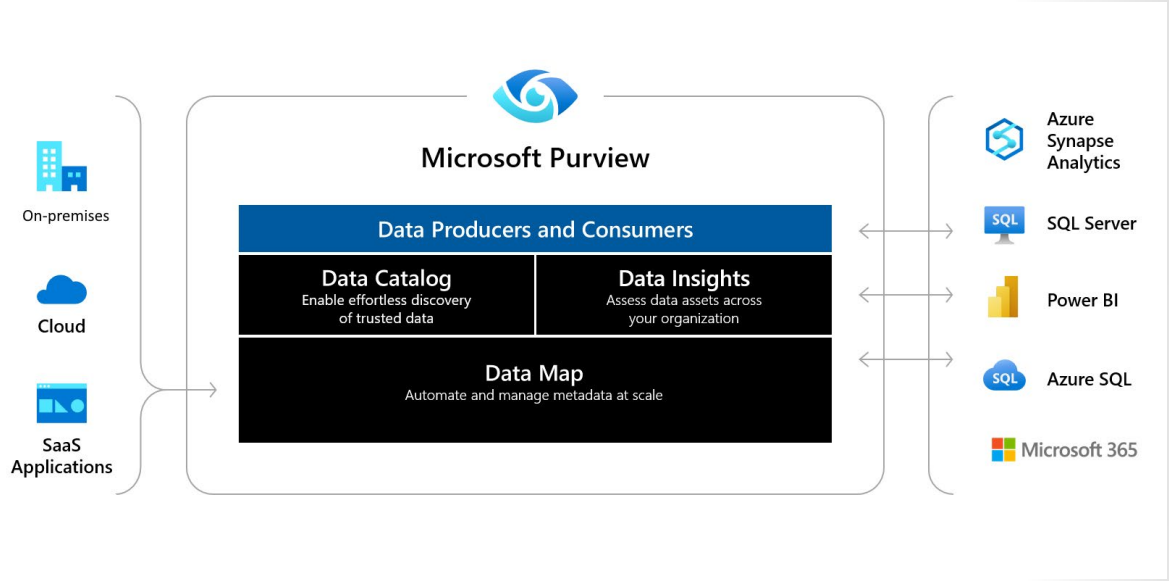
Azure SQL Database currently supports encryption at rest for Microsoft-managed service side and client-side encryption scenarios. Support for server encryption is currently provided through the SQL feature called Transparent Data Encryption. Once an Azure SQL Database customer enables TDE key are automatically created and managed for them. Encryption at rest can be enabled at the database and server levels. As of June 2017, Transparent Data Encryption (TDE) is enabled by default on newly created databases. Azure SQL Database supports RSA 2048-bit customer-managed keys in Azure Key Vault. For more information, see Transparent Data Encryption with Bring Your Own Key support for Azure SQL Database and Data Warehouse.

Client-side encryption of Azure SQL Database data is supported through the Always Encrypted feature. Always Encrypted uses a key that is created and stored by the client. Customers can store the master key in a Windows certificate store, Azure Key Vault, or a local Hardware Security Module. Using SQL Server Management Studio, SQL users choose what key they'd like to use to encrypt which column.

Data classification

The security controls that will be applied to the data will vary also according to the level of privacy required by the data and to ensure that you're prioritizing the data that it is important to be secure you'll need to classify your data. Data classification is a way of categorizing data assets by assigning unique logical labels or classes to the data assets. Classification is based on the business context of the data. For example, you might classify assets by Passport Number, Driver's License Number, Credit Card Number, SWIFT Code, Person's Name, and so on.

One solution for data classification in Azure is Microsoft Purview. Microsoft Purview is a unified data governance service that helps you manage and govern your on-premises, multi-cloud, and Software as a Service (SaaS) data. Create a holistic, up-to-date map of your data landscape with automated data discovery, sensitive data classification, and end-to-end data lineage. Enable data curators to manage and secure your data estate. Empower data consumers to find valuable, trustworthy data. Microsoft Purview provides a common platform for data producers and consumers to access common data management functions like a data catalog, data insights, and a data map. This common platform integrates with on-premises, the cloud as well as software-as-a-service applications. It also integrates with cloud data services such as Azure Synapse Analytics, SQL Server, Power BI, Azure SQL and Microsoft 365.



Identity Protection

One important aspect of privacy is to ensure that you have a system to protect the user's identity. A compromised identity could lead to data compromise and directly affect the privacy requirements for your project. Consider using Azure AD Identity Protection to enhance your identity protection strategy to ensure you're fulfilling the privacy requirements.

Identity Protection uses the learnings Microsoft has acquired from their position in organizations with Azure AD, the consumer space with Microsoft Accounts, and in gaming with Xbox to protect your users. Microsoft analyzes 6.5 trillion signals per day to identify and protect customers from threats. The signals generated by and fed to Identity Protection, can be further fed into tools like Conditional Access to make access decisions, or fed back to a security information and event management (SIEM) tool for further investigation based on your organization's enforced policies.

Exercise

Contoso Pharma is an international pharmaceutical industry with a presence in North America and Europe. Contoso Pharma has workloads on-premises and in Azure. The goal is that in the next two years, all workloads will be fully in Azure and there will be minimum workloads on-premises. Below is a list of their major workloads:

- VMs (Windows and Linux)
- Storage accounts
- Key Vault
- SQL PaaS and SQL on VMs

Contoso Pharma also has a Site-to-Site VPN between the headquarters in Redmond and the main office in London. This VPN is used to allow resources on-premises to communicate.

Contoso Pharma has a legacy environment in Redmond composed by a couple of Windows Server 2012 running a Web Server that is used by the application that queries the database to check for customer's information. Upon investigation it was noted that the communication of the legacy web server with the database is done via HTTP.

Design Requirements

Contoso Pharma has different compliance needs according to their workloads, as shown in the table below:

Workload	Type of Data	Compliance Standard
Windows VMs	Credit card holder information	PCI DSS
SQL PaaS	Patient health information	HIPAA
Storage Accounts	Credit card holder information	PCI DSS accounts

To be compliant with these standards, Contoso Pharma must be able to:

- Monitor compliance progress over time
- Prohibit workload owners to provision resources that are not compliant with those standards
- Ensure that new subscriptions that are deployed in the environment are using required standards by default
- Ensure resources that are provisioned on each geo-location keep the data in the source region for data sovereignty purposes

Questions

- To ensure that Contoso Pharma can analyze their compliance status over time, which tool should be utilized? Select the most appropriate option.
- Which service in Azure should be used to enforce workload owners to create only resources that are following the required standards?
- Which option should be utilized to ensure that when workload owners create resources, they're keeping the data in the correct geo-location?
- How can Contoso Pharma validate if the VMs that were provisioned are compliant with PCI DSS and if they're not what needs to be done to remediate?
- Data encryption is an imperative component to address your privacy requirements. What are the data stages that you must apply encryption?
- Which Azure service can you use to enforce data encryption across workloads?

Summary

In this module you learned that business risk is the starting point to establishing a compliance strategy, since it is during the business's risk assessment that you'll identify the regulatory compliance needs based on the industry's requirements. You learned that operational compliance should be in place to support the regulatory compliance needs and the options available in Azure to help you be compliant with the major regulatory standards. You also learned how to interpret compliance scores using Microsoft Defender for cloud and how to recommend actions to improve your compliance over time.

In addition, you learned how to design and validate your Azure Policy to enforce compliance requirements and continuously monitor your environment. As part of the compliance strategy, you also learned to design data residency requirements and translate privacy requirements

into security solutions with proper data classification and identity protection.

More information

Visit the links below for more information about the topics covered in this module:

- **Define cloud governance corporate policy - Cloud Adoption Framework**[1]
- **Operational compliance in Azure - Cloud Adoption Framework**[2]
- **Azure and other Microsoft cloud services compliance offerings - Azure Compliance**[3]
- **Operational compliance in Azure - Cloud Adoption Framework**[4]
- **Evaluate and define corporate policy - Cloud Adoption Framework**[5]
- **Regulatory compliance - Microsoft Azure Well-Architected Framework**[6]
- **HIPAA HITRUST 9.2**[7]
- Visit Azure Compliance offerings to learn more about the industries that are covered by Azure from the compliance perspective: **Azure and other Microsoft cloud services compliance offerings - Azure Compliance**[8]
- Watch **this webinar**[9] for more information on how to track your regulatory compliance. Although this webinar was delivered when Microsoft Defender for Cloud was called Azure Security Center, the content and rationale are still applicable for this topic.
- Watch **this video**[10] more information on how to use the Compliance Over Time Workbook workbook. Although this video was recorded when Microsoft Defender for Cloud was called Azure Security Center, the content and rationale are still applicable for this topic.
- Watch **this video**[11] for a quick demo on Allowed Locations policy
- For more information, visit **Data Residency in Azure**[12]

1 https://docs.microsoft.com/azure/cloud-adoption-framework/govern/policy-compliance/policy-definition
2 https://docs.microsoft.com/azure/cloud-adoption-framework/manage/azure-management-guide/operational-compliance?tabs=UpdateManagement%2CAzurePolicy%2CAzureBlueprints
3 https://docs.microsoft.com/azure/compliance/offerings/
4 https://docs.microsoft.com/azure/cloud-adoption-framework/manage/azure-management-guide/operational-compliance?tabs=UpdateManagement%2CAzurePolicy%2CAzureBlueprints
5 https://docs.microsoft.com/azure/cloud-adoption-framework/govern/corporate-policy
6 https://docs.microsoft.com/azure/architecture/framework/security/design-regulatory-compliance
7 https://docs.microsoft.com/azure/governance/policy/samples/hipaa-hitrust-9-2
8 https://docs.microsoft.com/azure/compliance/offerings/
9 https://youtu.be/tD8JnqzNOPc
10 https://youtu.be/S_zJ2QBkk-0
11 https://youtu.be/n469bC2V2Wo
12 https://azure.microsoft.com/global-infrastructure/data-residency/

- Watch **this video**[13] for more information about Azure Purview.
- Watch **this video**[14] for more information on Azure AD Identity Protection.

13 https://youtu.be/W2bsj3ULw0Y
14 https://youtu.be/1REQYdZ6364

Evaluate security posture

Introduction

Learn how to evaluate your organization's security posture and recommend the technical strategies to manage risk.

Learning Objectives

In this module, you'll learn how to:

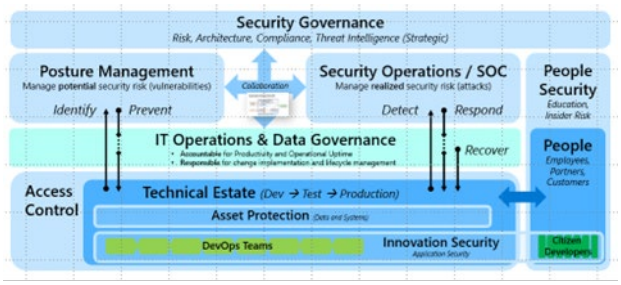
- Evaluate security postures by using benchmarks
- Evaluate security postures by using Microsoft Defender for Cloud
- Evaluate security postures by using Secure Scores
- Evaluate security hygiene of Cloud Workloads
- Design security for an Azure Landing Zone
- Interpret technical threat intelligence and recommend risk mitigations
- Recommend security capabilities or controls to mitigate identified risks

Evaluate security postures by using benchmarks

Posture management and the Security operating model

Governance in the cloud age must have an active component that continuously engages with other teams. Security posture management is an emerging function. It represents a step forward in the long-term convergence of security functions. These functions answer the question "how secure is the environment?", including vulnerability management and security compliance reporting.

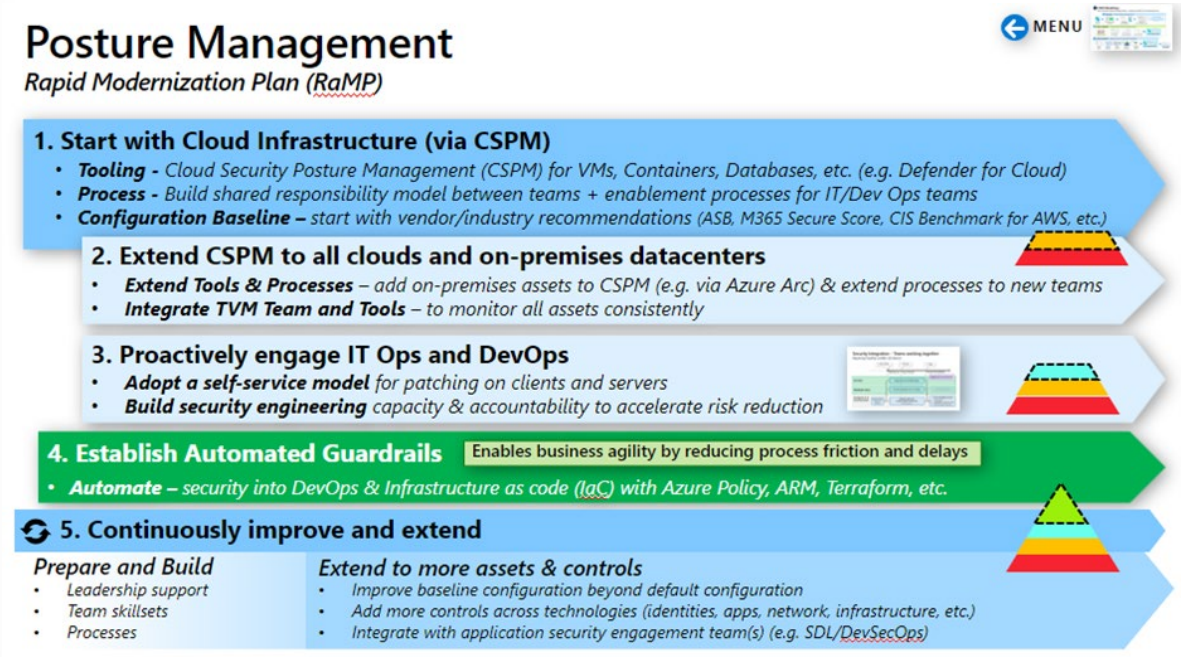
In the on-premises world, security governance followed the cadence of data it could get about the environment. This way of getting data might take time and be constantly out of date. Cloud technology now provides on-demand visibility into the current security posture and asset coverage. This visibility drives a major transformation of governance into a more dynamic organization. This organization provides a closer relationship to other security teams to monitor security standards, provide guidance, and improve processes. In its ideal state, governance is the heart of continuous improvement. This improvement engages across your organization to constantly improve security posture, which is called Posture Management and it fits in the overall security governance as shown in the diagram below:



Continuous improvement of asset security posture means that governance teams should focus on improving standards, and enforcement of those standards, to keep up with the cloud and attackers.

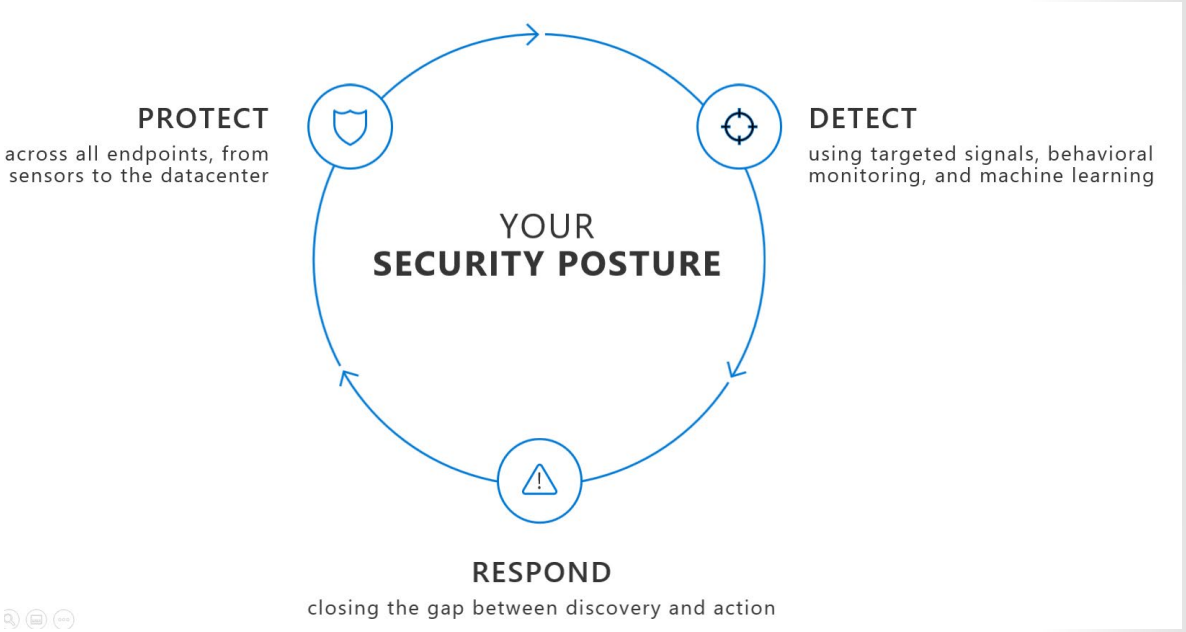
Information technology (IT) organizations must react quickly to new threats and adapt accordingly. Attackers are continuously evolving their techniques, and defenses are continuously improving and might need to be enabled. You can't always get all the security you need into the initial configuration.

This Rapid Modernization Plan (RaMP) shown in the diagram below will enable you to quickly improve your security posture with the least number of challenges.



The posture management function will need to grow and continuously improve to tackle the full set of technical debt that the organization has accrued from over 30+ years of security being a low priority. Posture management will need to secure all the technologies and teams in the organization plus meet the needs of the organization as it changes (new platforms are adopted, new security tools become available to monitor and reduce risk, etc.). Any expansions in scope will take preparation to build leadership support, relationships across technical teams, posture management team skillsets, and processes.

Security posture refers to the current state of an organization's security—that is, its overall state of protection to its identities, endpoints, user data, apps and infrastructure.. The diagram below shows the three major pillars of security posture management.



These three pillars are:

- Protect: An organization's security posture is not static, it changes constantly in response to emerging new threats and variabilities in the environment. Enabling protections, like multifactor authentication (MFA) for administrators, strengthens a company's posture. A lack of vigilance, such as failing to update endpoints or use available protections can weaken an organizations security posture. The security hygiene of your environment helps to reduce the likelihood that threat actors will successfully compromise your workloads.
- Detect: After mitigating all security recommendations, you also must ensure that you have threat detection in place to quickly identify suspicious activities in your workloads and trigger an alert to bring awareness about it.
- Respond: Finally, ensure that you have automation in place to take immediate action on the alerts that you receive by appropriately responding to it with actions that can contain and mitigate the attack.

The use of benchmarks to evaluate your current environment, understand the current gaps and provide guidance on how to improve, is a very common practice in the IT industry. When it comes to security posture enhancement, benchmarks can give you tangible actions based on industry standards, such as ISO 2701 or by using cloud provider's benchmark, such as Azure Security Benchmark for Azure workloads, or Center for Internet Security (CIS) AWS Foundations Benchmark which is crafted for AWS workloads. Benchmarks will also help you to accelerate the identification of security gaps by providing remediation steps to harden your workloads. As you remediate these security recommendations, your workloads will get more secure, and your overall cloud security posture is enhanced. As an architect, you'll look to benchmarks as a tool to guide your efforts to improve the cloud security posture while follow industry standards.

When evaluating your security hygiene for cloud workloads, consider all available options. Take into account that every security program may include multiple workflows. These processes might include notifying

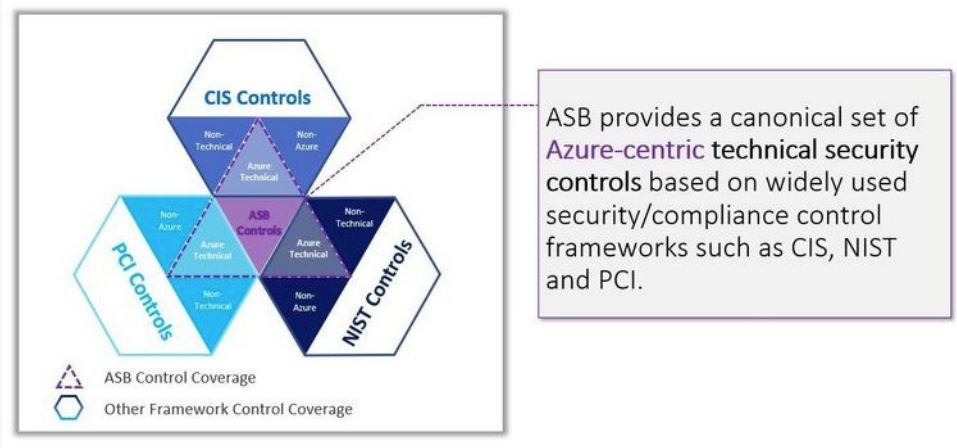
relevant stakeholders, launching a change management process, and applying specific remediation steps. Consider automating as many steps of those procedures as you can, since automation reduces overhead. It can also improve your security by ensuring the process steps are done quickly, consistently, and according to your predefined requirements.

To improve the security hygiene of the cloud workloads, you also need to ensure that you're using security best practices to harden these workloads. Each workload has a different set of security best practices that must be in place to improve its security hygiene. Make sure to visit **https://aka.ms/MyASIS** for more information about security best practices for Azure workloads.

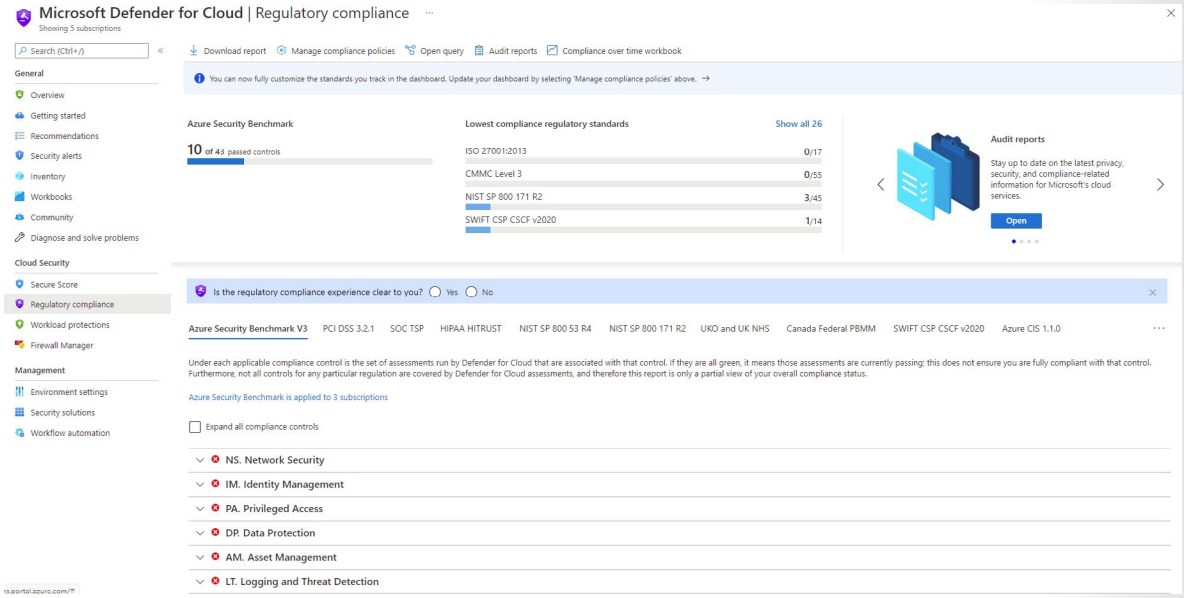
Evaluating security posture in Azure workloads

One option to evaluate the security posture of your workloads is by using Azure Security Benchmark (ASB), which is widely used by organizations to meet security control requirements in Azure. ASB provides clear and concrete guidance on how to securely configure Azure resources to meet both security and compliance requirements. ASB often plays a key role in Azure onboarding, enabling organizations to accelerate both initial Azure onboarding as well as ongoing onboarding/assessment of Azure Cloud Services.

Customers often have to reconcile and harmonize multiple control frameworks when planning and evaluating their Azure environments to meet security and compliance requirements. This often requires security teams to repeat the same evaluation process for the various control frameworks, creating unnecessary overhead, cost, and effort. To address this concern, Microsoft developed ASB to function as a harmonizing control framework to help you quickly work with established standards in the context of a cloud environment—standards such as CIS Controls v8 and v7, NIST SP800-53 Rev4, and PCI-DSS v3.2.1. Organizations can use ASB to evaluate their Azure deployment's security posture consistently and easily against these industry standards with minimal repeated work.



Azure Security Benchmark is surfaced in Microsoft Defender for Cloud regulatory compliance dashboard as shown in the following image:



This benchmark gives you visibility of which security recommendations are open per compliance control. Under each applicable compliance control, you have a set of assessments run by Defender for Cloud that are associated with that control. If they're all green, it means those assessments are currently passing; this does not ensure you're fully compliant with that control. Furthermore, not all controls for any particular regulation are covered by Defender for Cloud assessments, and therefore this report is only a partial view of your overall compliance status.

While this is the preferred benchmark for Azure, you may need to use a different benchmark according to your organization's needs. You can navigate through different tabs that have assigned regulatory standards to visualize the applicable compliance controls that were assessed and the current status of each item.

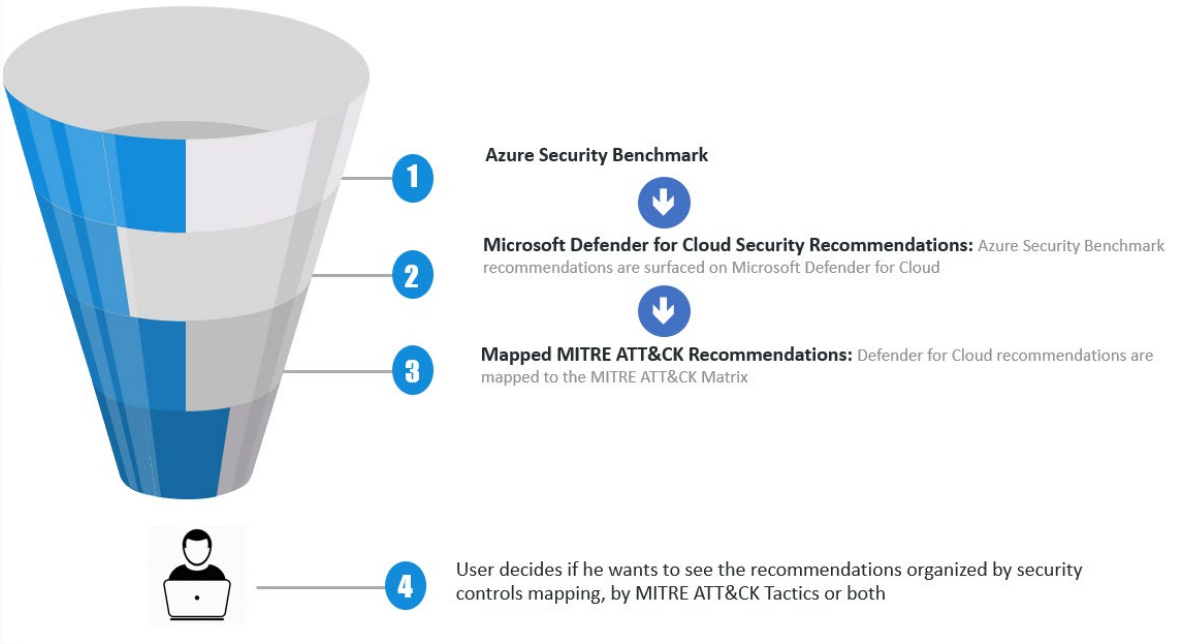
Evaluate security postures by using Microsoft Defender for Cloud

Defender for Cloud continually assesses your resources, subscriptions, and organization for security issues. It then aggregates all the findings into a single score so that you can tell, at a glance, your current security situation: the higher the score, the lower the identified risk level.

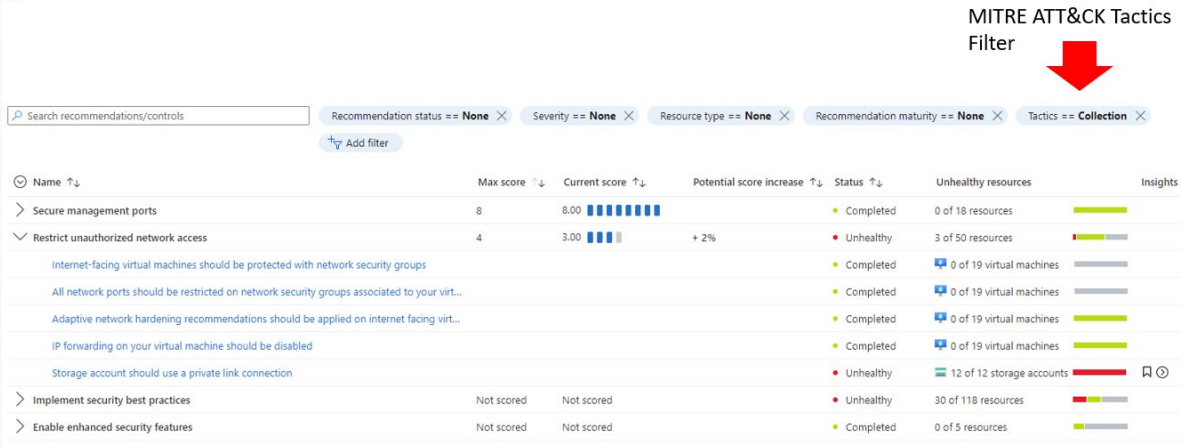
For security analysts, it's essential to identify the potential risks associated with security recommendations and understand the attack vectors, so they can prioritize more effectively. To make prioritization easier, Microsoft Defender for Cloud maps its security recommendations against the **MITRE ATTACK framework**[15], a globally accessible knowledge base of adversary tactics and techniques

15 https://attack.mitre.org/

based on real-world observations. Using this capability, customers can strengthen the security posture of their environment with recommendations that are mapped to the MITRE ATTACK framework and prioritize based on the potential risk across the cyber kill chain.

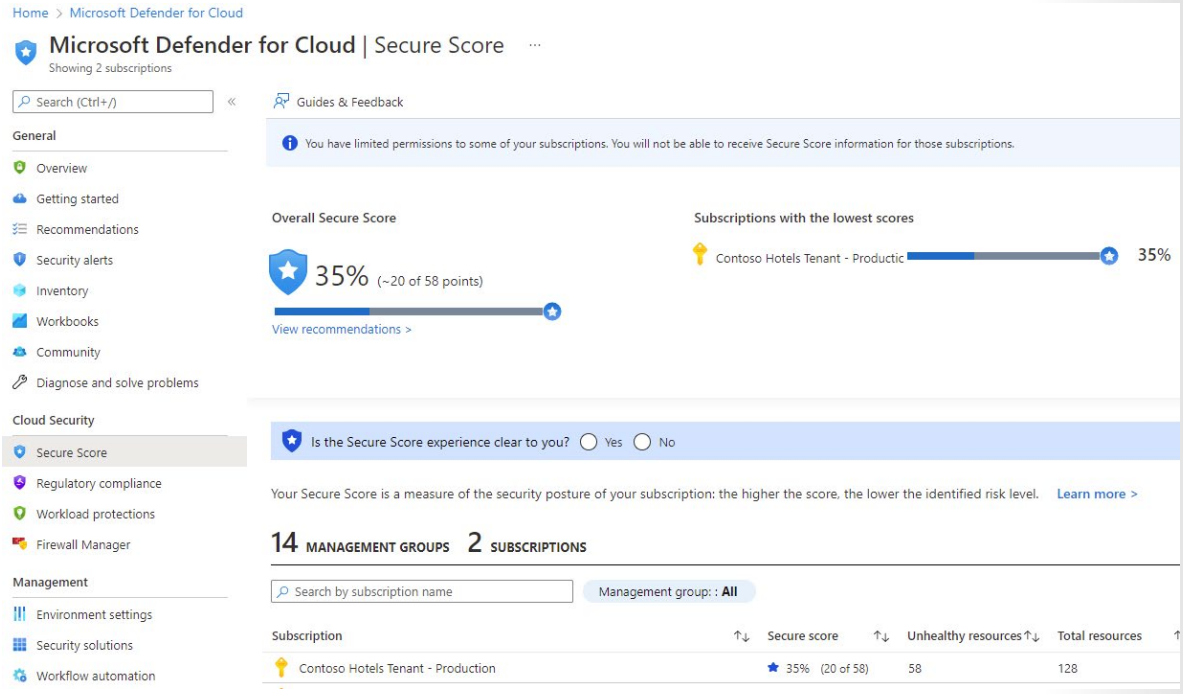


The advantage of using MITRE ATTACK when evaluating your security posture is that you can create campaigns to remediate recommendations based on the different phases of the MITRE ATTACK framework. The rationale is that if you remediate recommendations that are mapped to early stages of the MITRE ATTACK framework, you can prevent a threat actor from gaining further access to your workloads. Defender for Cloud has a filter that enables you to create this visualization as shown in the image below:



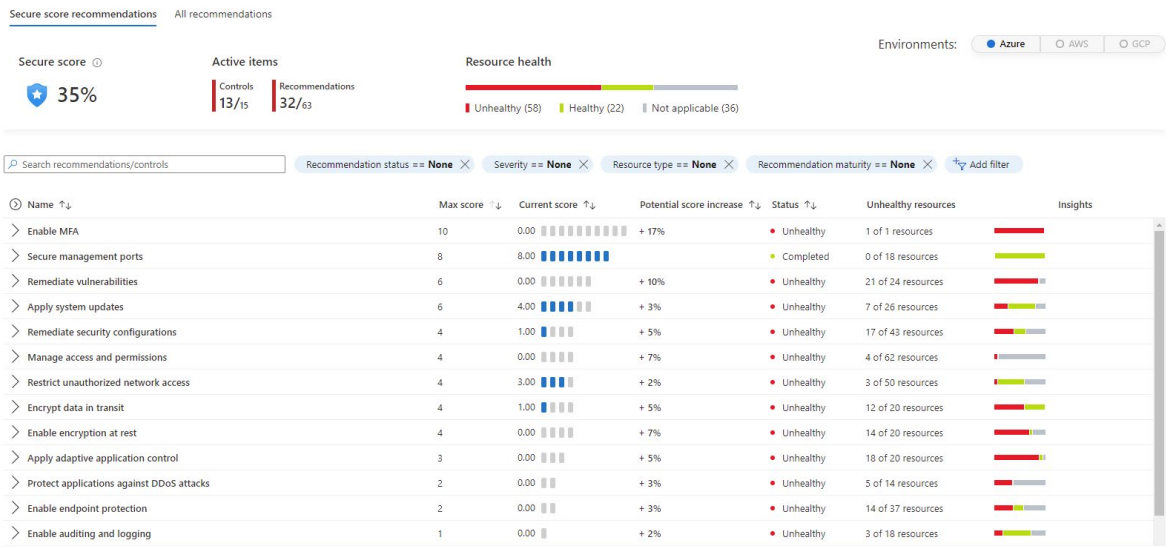
Evaluate security postures by using Secure Scores

The secure score dashboard in Defender for Cloud shows the secure score on the subscription level for one or more subscriptions (depending on how many subscriptions are selected in the Azure portal).



To increase your security, review Defender for Cloud's recommendations page and remediate the recommendation by implementing the remediation instructions for each issue. Recommendations are grouped into security controls. Each control is a logical group of related security recommendations and reflects your vulnerable attack surfaces. Your score only improves when you remediate all the recommendations for a single resource within a control. To see how well your organization is securing each individual attack surface, review the scores for each security control.

The example below shows the Recommendations dashboard with all security controls organized in a top-down list, where the controls on top will have a higher impact on the secure score improvement.

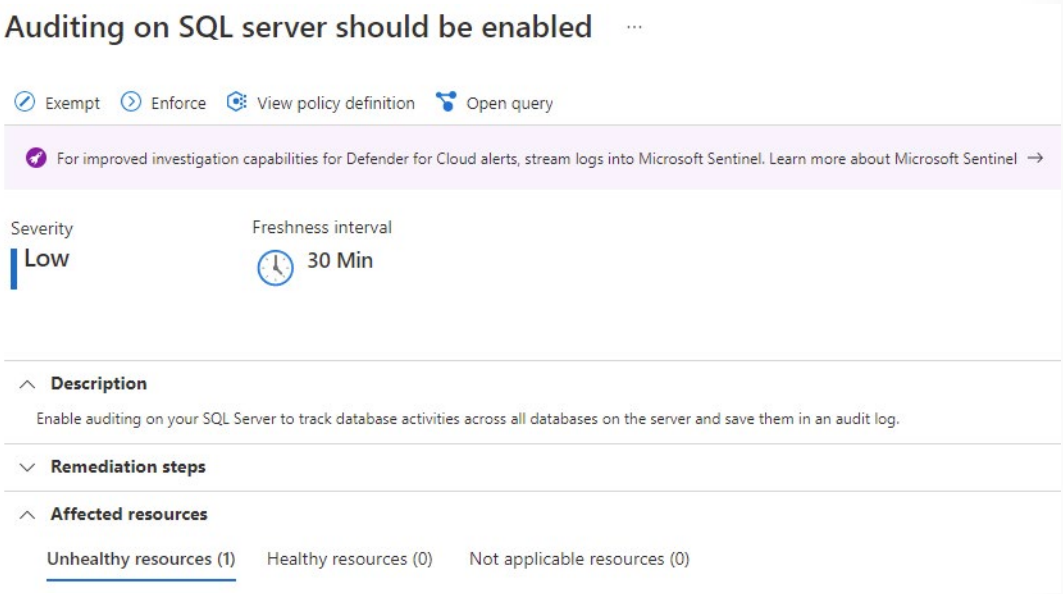


When you use Secure Score as your Key Performance Indicators (KPI), you can track progress as you continuously remediate security recommendations to drive your secure score up.

While driving security posture enhancement by remediating security recommendations triggered by Microsoft Defender for Cloud and using Secure Score to track your progress is the recommended choice, more can be done to keep positively progressing towards a better security posture. When a company doesn't have a very mature Azure Governance, chances are that they will experience a fluctuation in the secure score (ups and downs), and this can happen if you continue provisioning new resources that are not secure by default.

Having a solid Azure Governance enables you to ensure that new resources that are deployed, are going to have certain standards, patterns, and configurations. To ensure proper governance you can use Azure Policy and Azure Blueprints. This will allow you to enforce policies and reject deployment of resources that are not following certain standards.

Defender for Cloud can help the governance of those workloads by using Azure Policy to enforce secure configuration, based on a specific recommendation. Some recommendations will be based on policies that can use the *Deny* effect, which in this case can stop unhealthy resources from being created. Some other recommendations are based on the *DeployIfNotExist* effect, which can automatically remediate non-compliant resources upon creation. Below you have an example of a recommendation that has the *Enforce* button, which behind the scene is implementing the *DeployIfNotExist* effect.



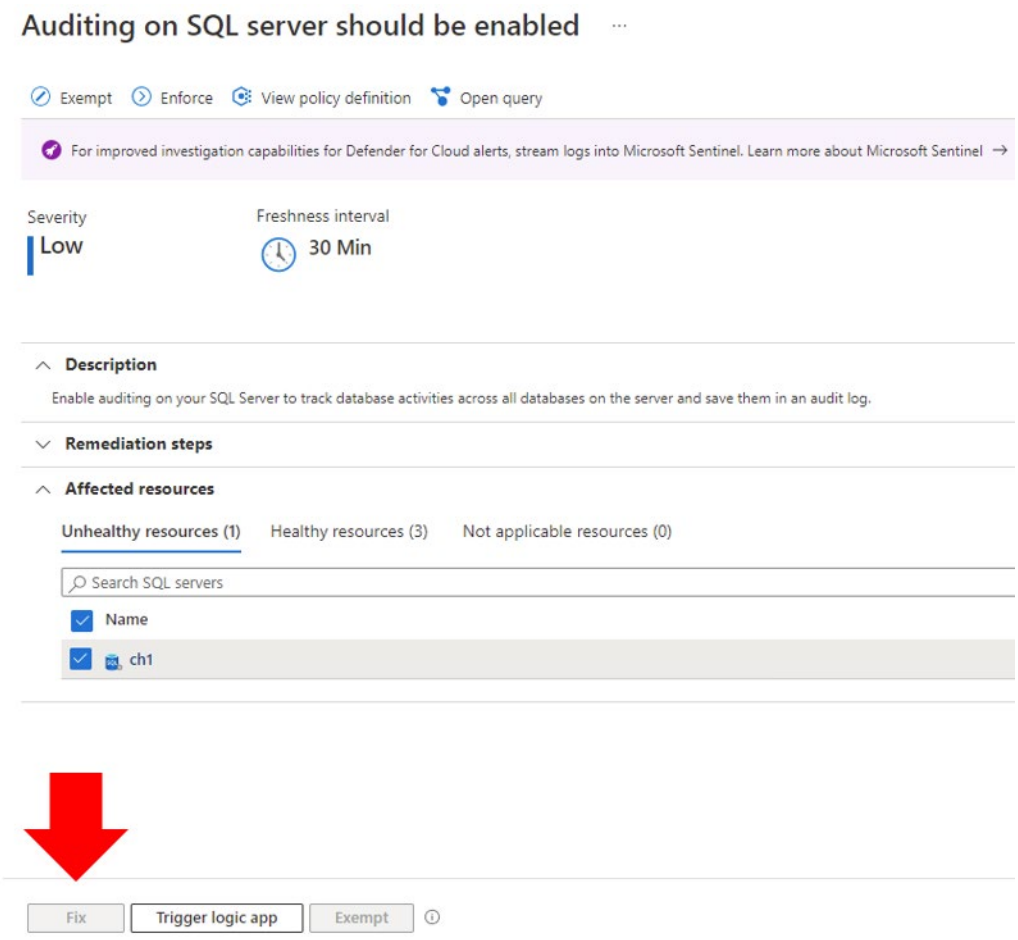
Evaluate security hygiene of Cloud Workloads

Depending on the size and structure of your organization, multiple individuals and teams may use Defender for Cloud to perform different security-related tasks. In the following diagram, you have an example of fictitious personas and their respective roles and security responsibilities:

Defender for Cloud enables these individuals to meet these various responsibilities. For example:

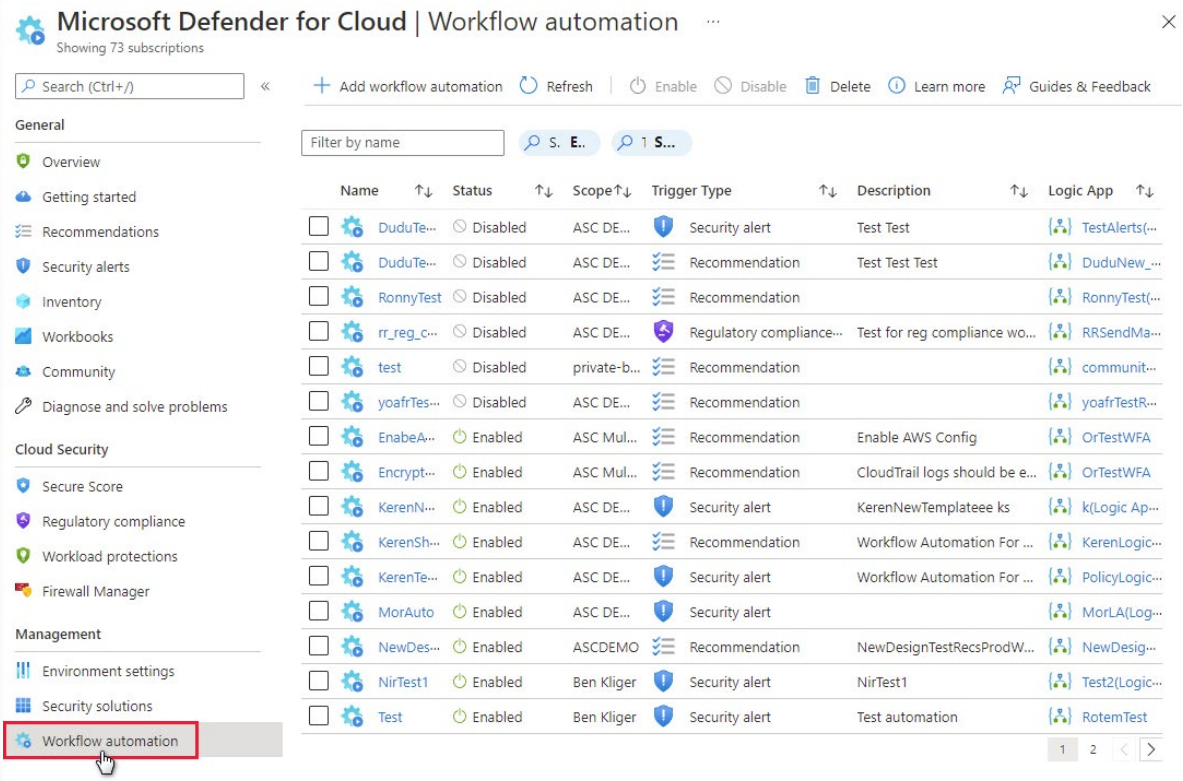
- Jeff (Workload Owner)
    - Manage a cloud workload and its related resources
    - Responsible for implementing and maintaining protections in accordance with company security policy
- Ellen (CISO/CIO)
    - Responsible for all aspects of security for the company
    - Wants to understand the company's security posture across cloud workloads
    - Needs to be informed of major attacks and risks
- David (IT Security)
    - Sets company security policies to ensure the appropriate protections are in place
    - Monitors compliance with policies
    - Generates reports for leadership or auditors
- Judy (Security Operations)
    - Monitors and responds to security alerts 24/7
    - Escalates to cloud workload Owner or IT Security Analyst
- Sam (Security Analyst)
    - Investigate attacks
    - Work with cloud workload Owner to apply remediation

In many scenarios the IT Security Admin does not have the right level of privileges in the workload to expedite the remediation of recommendations. When a user doesn't have the right level of privilege in the workload and tries to remediate a recommendation by using the *Fix* button, they will have the experience shown in the image below, where the Fix button is grey out.



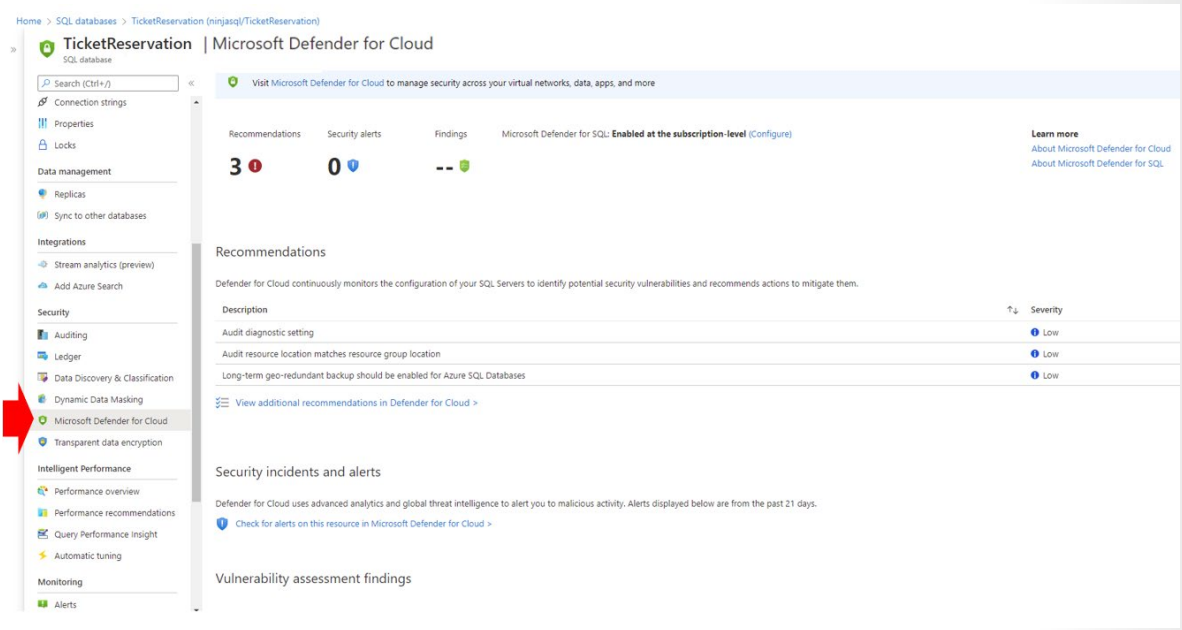
For this reason, workload owners must be able to receive notifications when there are open security recommendations for them to remediate. In Defender for Cloud you can use the **Workflow Automation**[16] capability to activate actions such as sending an email to the resource owner, when a recommendation is triggered. An example of this workflow is shown below:

16 https://docs.microsoft.com/azure/defender-for-cloud/workflow-automation



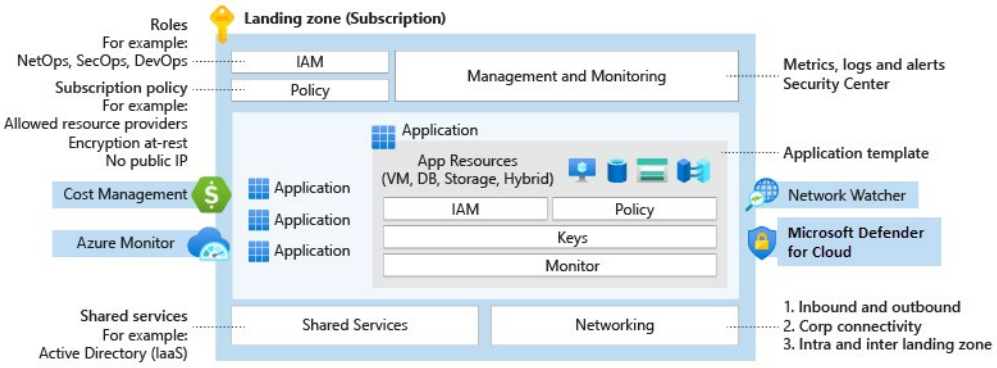
1. The team that is responsible for Microsoft Defender for Cloud identifies that there's a security recommendation that needs to be addressed and which resources are affected.
2. A ticket is open and assigned to the workload owner. In this ticket they have details about the security recommendation and the suggested steps to remediate.
3. The workload owner reviews the ticket and identifies that there's a quick fix for this recommendation. They can use the View remediation logic button to understand what changes will be made to the system.
4. Once they few comfortable with the changes, they start a change management process to schedule the remediation.
5. The remediation is applied on the day that was scheduled.

Workload owners can also use the built-in integration with Defender for Cloud available in the workload's proprieties. For example, a Database Administrator that manages multiple databases can see security recommendations that will improve the security hygiene of its workloads by visiting the Microsoft Defender for Cloud option as shown in the example below:



Design security for an Azure Landing Zone

Azure landing zones are the output of a multi-subscription Azure environment that accounts for scale, security governance, networking, and identity. Azure landing zones enable application migration, modernization, and innovation at enterprise-scale in Azure. These zones consider all platform resources that are required to support the customer's application portfolio and don't differentiate between infrastructure as a service or platform as a service.



A landing zone is an environment for hosting your workloads, pre-provisioned through code. Watch the following video to learn more.

[!VIDEO https://www.microsoft.com/videoplayer/embed/RE4xdvm]

Security, governance, and compliance are key topics when designing and building an Azure environment. These topics help you start from strong foundations and ensure that solid ongoing processes and controls are in place.

The tools and processes you implement for managing environments play an important role in detecting and responding to issues. These tools work alongside the controls that help maintain and demonstrate compliance. As the organization's cloud environment develops, these compliance design areas will be the focus for iterative refinement. This refinement might be because of new applications that introduce specific new requirements, or the business requirements changing. For example, in response to a new compliance standard.

Design Area	Objective	Relevant methodology
Security	Implement controls and processes to protect your cloud environments.	Secure
Management	For stable, ongoing operations in the cloud, a management baseline is required to provide visibility, operations compliance, and protect and recover capabilities.	Manage
Governance	Automate auditing and enforcement of governance policies.	Govern
Platform automation and DevOps	Align the best tools and templates to deploy your landing zones and supporting resources.	Ready

Design security review

Security is a core consideration for all customers, in every environment. When designing and implementing an Azure landing zone, security should be a consideration throughout the process.

The security design area focuses on considerations and recommendations for landing zone decisions. The Secure methodology in the Cloud Adoption Framework also provides further in-depth guidance for holistic security processes and tools. This design area creates a foundation for security across your Azure, hybrid, and multi-cloud environments. You can enhance this foundation later with security guidance outlined in the Cloud Adoption Framework's Secure methodology.

When it comes to design area review, ensure that you establish the involved roles and functions, what is in scope and what is out of scope as per the guidelines below:

- **Involved roles or functions:** This design area is led by cloud security, specifically the security architects within that team. The cloud platform and cloud center of excellence are required to review networking and identity decisions. The collective roles might be required to define and implement the technical requirements coming from this exercise. More advanced security guardrails might also need support from cloud governance.
- **Scope:** The goal of this exercise is to understand security requirements and implement them consistently across all workloads in

your cloud platform. The primary scope of this exercise focuses on security operations tooling and access control. This scope includes zero trust and advanced network security.

- **Out of scope:** This exercise focuses on the foundation for a modern security operations center in the cloud. To streamline the conversation, this exercise doesn't address some of the disciplines in the CAF Secure methodology. Security operations, asset protection, and innovation security will build on your Azure landing zone deployment. However, they're out of scope for this design area discussion.

Security design considerations

An organization must have visibility into what's happening within their technical cloud estate. Security monitoring and audit logging of Azure platform services is a key component of a scalable framework. When it comes to security operations design, make sure to review the following guidelines:

- **Security alerts**:
    - Which teams require notifications for security alerts?
    - Are there groups of services that alerts require routing to different teams?
    - Business requirements for real-time monitoring and alerting.
    - Security information and event management integration with Microsoft Defender for Cloud and Microsoft Sentinel.
- **Security logs**:
    - Data retention periods for audit data. Azure Active Directory (Azure AD) Premium reports have a 30-day retention period.
    - Long-term archiving of logs like Azure activity logs, virtual machine (VM) logs, and platform as a service (PaaS) logs.
- **Security controls**:
    - Baseline security configuration via Azure in-guest VM policy.
    - Consider how your security controls will align with governance guardrails.
- **Vulnerability management**:
    - Emergency patching for critical vulnerabilities.
    - Patching for VMs that are offline for extended periods of time.
    - Vulnerability assessment of VMs.
- **Shared responsibility**:
    - Where are the handoffs for team responsibilities? These responsibilities need consideration when monitoring or responding to security events.
    - Consider the guidance in the Secure methodology for security operations.

- **Encryption and keys**:
  - Who requires access to keys in the environment?
  - Who will be responsible for managing the keys?

Security in the Azure landing zone accelerator

Security is at the core of the Azure landing zone accelerator. As part of the implementation, many tools and controls are deployed to help organizations quickly achieve a security baseline.

For example, the following are included:

Tools:

- Microsoft Defender for Cloud, standard or free tier
- Microsoft Sentinel
- Azure DDoS standard protection plan (optional)
- Azure Firewall
- Web Application Firewall (WAF)
- Privileged Identity Management (PIM)

Policies for online and corporate-connected landing zones:

- Enforce secure access, like HTTPS, to storage accounts
- Enforce auditing for Azure SQL Database
- Enforce encryption for Azure SQL Database
- Prevent IP forwarding
- Prevent inbound RDP from internet
- Ensure subnets are associated with NSG

Interpret technical threat intelligence and recommend risk mitigations

Threat intelligence at Microsoft includes signals inside and outside the company, related to areas shown in the figure below, like denial of service, malware, or unauthorized data access. With the right context, this intelligence leads to targeted actions—for example, releasing system updates, enforcing security policies like multi-factor authentication, or applying other security measures.

Threat intelligence is used as a tool to learn about threat and help mitigate risks. This is because threat intelligence gives context, relevance, and priority. Threat intelligence goes beyond the lists of bad domains or bad hashes. It provides the necessary context, relevance, and priority—sometimes called enrichment. This helps people to make faster, better, and more proactive cybersecurity decisions. Below you have examples of scenarios where threat intelligence can be used:

- A security analyst who uses threat intelligence to analyze the highest priority signals and takes action.
- An information worker who knows to watch for emails with links that appear suspicious and could be a phishing campaign targeting the company. This awareness could, for example, influence the email recipient to be vigilant, avoid opening files or clicking questionable links, and report the email as suspicious.
- An organization that uses threat intelligence to alert employees that a particular email attachment is associated with ransomware that has affected other companies in the same sector.

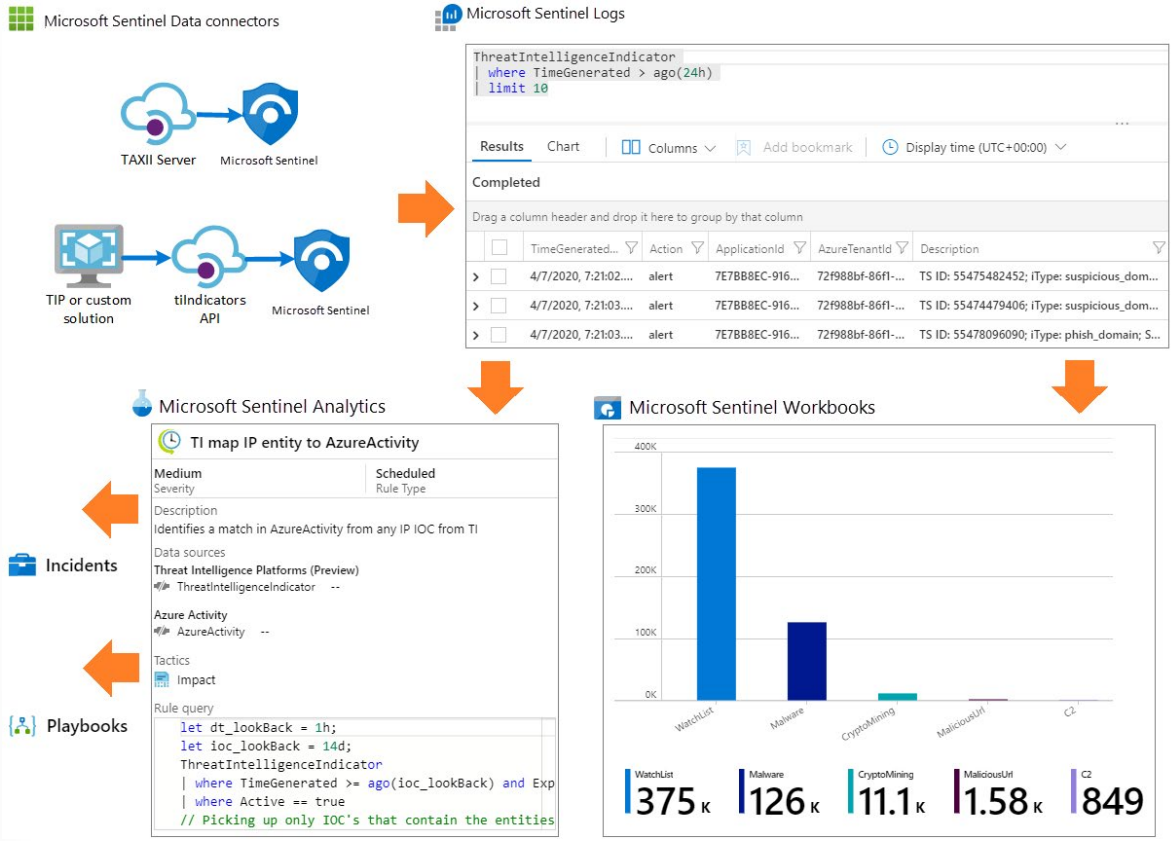
Security concerns aren't limited to any sector. All organizations need to defend themselves against cyberthreats, making it a core part of their strategies and operations. Visibility and intelligence into threats are crucial for preparedness—for example, knowing the type of attack, who's being targeted, how often, and the source of attacks. Through threat intelligence, organizations can gain visibility, context, and relevance of security events. Having access to—and sharing this knowledge—helps decision makers both inside and outside security teams prioritize actions and reduce risk.

Identify technical threat intelligence

Cyber threat intelligence (CTI) can come from many sources, such as open-source data feeds, threat intelligence sharing communities, paid intelligence feeds, and security investigations within organizations. CTI can range from written reports on a threat actor's motivations, infrastructure, and techniques, to specific observations of IP addresses, domains, and file hashes. CTI provides essential context for unusual activity, so security personnel can act quickly to protect people and assets.

The most utilized CTI in SIEM solutions like Microsoft Sentinel is threat indicator data, sometimes called Indicators of Compromise (IoCs).

Threat indicators associate URLs, file hashes, IP addresses, and other data with known threat activity like phishing, botnets, or malware. This form of threat intelligence is often called tactical threat intelligence, because security products and automation can use it in large scale to protect and detect potential threats. The diagram below shows the core architecture of this solution:



Microsoft Sentinel can help detect, respond to, and provide CTI context for malicious cyber activity. You can also use Microsoft Sentinel to:

- Import threat indicators from Structured Threat Information Expression (STIX) and Trusted Automated Exchange of Intelligence Information (TAXII) servers, or from any threat intelligence platform (TIP) solution
- View and query threat indicator data
- Create analytics rules to generate security alerts, incidents, and automated responses from CTI data
- Visualize key CTI information in workbooks

Another product that also uses threat intelligence is Microsoft Defender for Cloud. Defender for Cloud's threat protection works by monitoring security information from your Azure resources, the network, and connected partner solutions. It analyzes this information, often correlating information from multiple sources, to identify threats. When Defender for Cloud identifies a threat, it triggers a security alert, which contains detailed information regarding the event, including suggestions for remediation. To help incident response teams investigate and remediate threats, Defender for Cloud provides threat intelligence

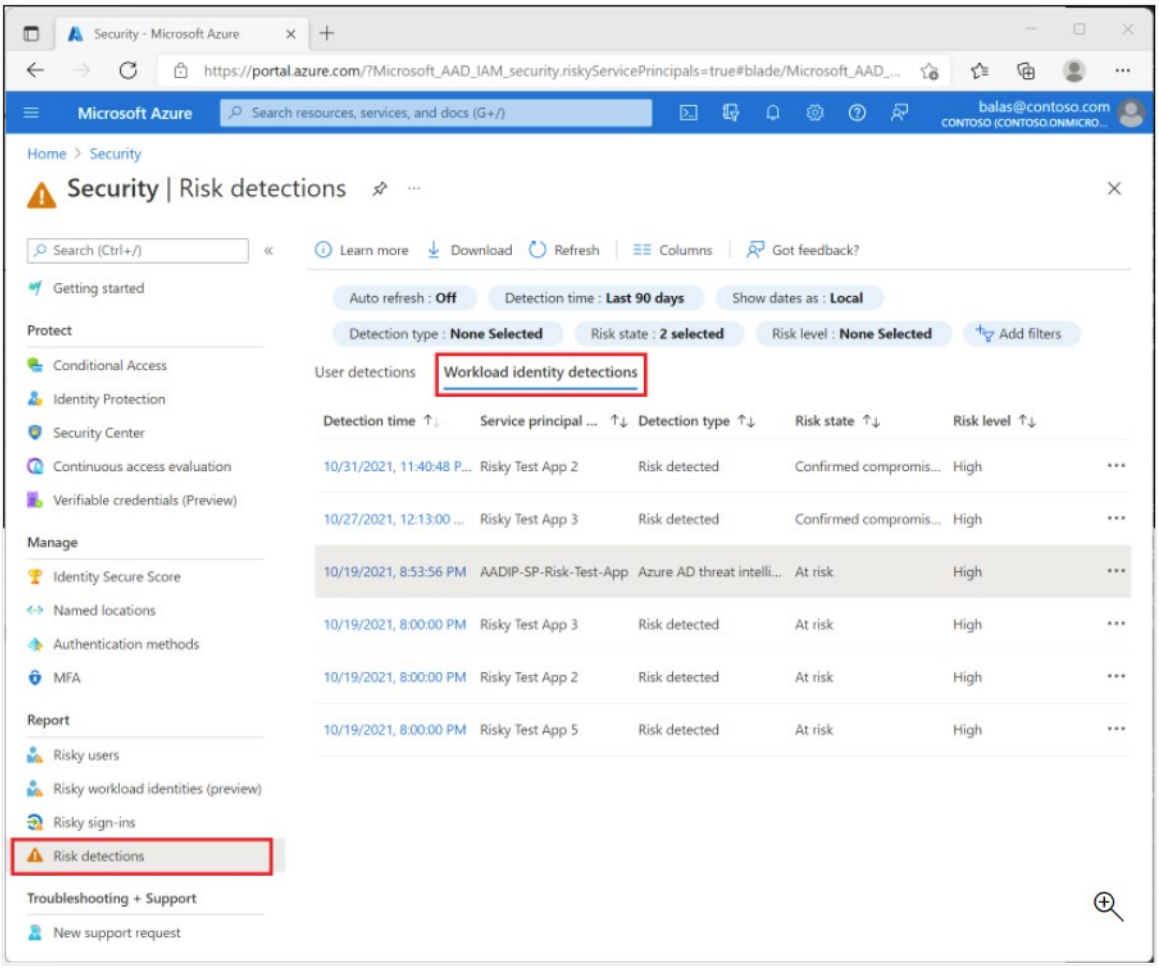
reports containing information about detected threats. The report includes information such as:

- Attacker's identity or associations (if this information is available)
- Attackers' objectives
- Current and historical attack campaigns (if this information is available)
- Attackers' tactics, tools, and procedures
- Associated indicators of compromise (IoC) such as URLs and file hashes
- Victimology, which is the industry and geographic prevalence to assist you in determining if your Azure resources are at risk
- Mitigation and remediation information Defender for Cloud has three types of threat reports, which can vary according to the attack. The reports available are:

    - Activity Group Report: provides deep dives into attackers, their objectives, and tactics.
    - Campaign Report: focuses on details of specific attack campaigns.
    - Threat Summary Report: covers all of the items in the previous two reports.

This type of information is useful during the incident response process, where there's an ongoing investigation to understand the source of the attack, the attacker's motivations, and what to do to mitigate this issue in the future.

Threat intelligence is also used in other Microsoft Security solutions, such as Azure AD Identity Protection, which has a featured called Risk Detection. Risk detections (both user and sign-in linked) contribute to the overall user risk score that is found in the Risky Users report. These risks are calculated offline using Microsoft's internal and external threat intelligence sources including security researchers, law enforcement professionals, security teams at Microsoft, and other trusted sources. The image below has an example of the risk detection capability in Azure AD Identity Protection:



Risk mitigations

Thinking of risks in this manner is sometimes referred to as the event-driven risk model. This term implies that a list of risks is a list of potential future events. Each risk describes some event that could occur in the future. The risk might include some information about the probability of occurrence. It should include a description of the impact that such an occurrence would have on the project plan. It may also include a description of ways to reduce the probability of occurrence and ways to mitigate the impact of occurrence.

Risk management activities fall into four phases: identification, assessment, response, and monitoring and reporting. In the list below you have more details about each phase:

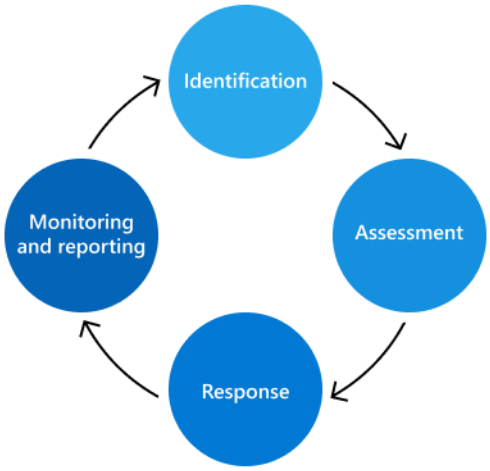
- Identification: The risk management process starts with identifying all possible risks to all key control areas, internal and external threats, and vulnerabilities in the environment. The identification phase is also when decision logs, active security and compliance exceptions, and mitigation work from previous risk assessments are reviewed

- Assessment: Each identified risk is assessed using three metrics: impact, likelihood, and control deficiency. Impact refers to the damage that would occur to the service or business. Likelihood defines the probability of the potential risk being realized and control deficiency measures the effectiveness of implemented mitigation controls.
- Response: How you'll respond to the risk that was identified, which could be based on the following options:
  - Tolerate: Areas of low-risk exposure with a low level of control.
  - Operate: Areas of low-risk exposure where controls are deemed adequate.
  - Monitor: Areas of high-risk exposure where controls are deemed adequate and should be monitored for effectiveness.
  - Improve: Areas of high-risk exposure with a low level of control that are top priorities in addressing.
- Monitoring and reporting: Risks identified as part of the risk assessment are monitored and reported to relevant stakeholders. Monitoring strategies include security monitoring, periodic risk reviews, penetration testing, and vulnerability scanning.

Recommend security capabilities or controls to mitigate identified risks

Increasingly, employees have more access to create, manage, and share data across a broad spectrum of platforms and services. In most cases, organizations have limited resources and tools to identify and mitigate organization-wide risks while also meeting compliance requirements and employee privacy standards. These risks may include data theft by departing employees and data leaks of information outside your organization by accidental oversharing or malicious intent.

The top priority should be to proactively identify and address risks that could impact your organization's service infrastructure and their data. In addition, a robust risk management program is necessary to meet contractual obligations. Each risk management activity will have outputs that will feed the next phase, as shown in the diagram below:



Let's use as an example a scenario where you're the Cybersecurity Architect that is recommending security capabilities and controls to mitigate the identified risks.

- During the *Identification* of the risks, you found a production subscription that has ten Azure Storage accounts
  that are widely open to the Internet.
- During the *Assessment* phase, you determined that five of these storage accounts have low impact in case of compromise. The low impact was because they do not contain important information. However, you found five other storage accounts that could have a high impact in case of compromise.
- The *Response* for the first five is to tolerate the risk while the other five will need to be improved by adding technical controls to mitigate the risk.

In this case technical controls include:

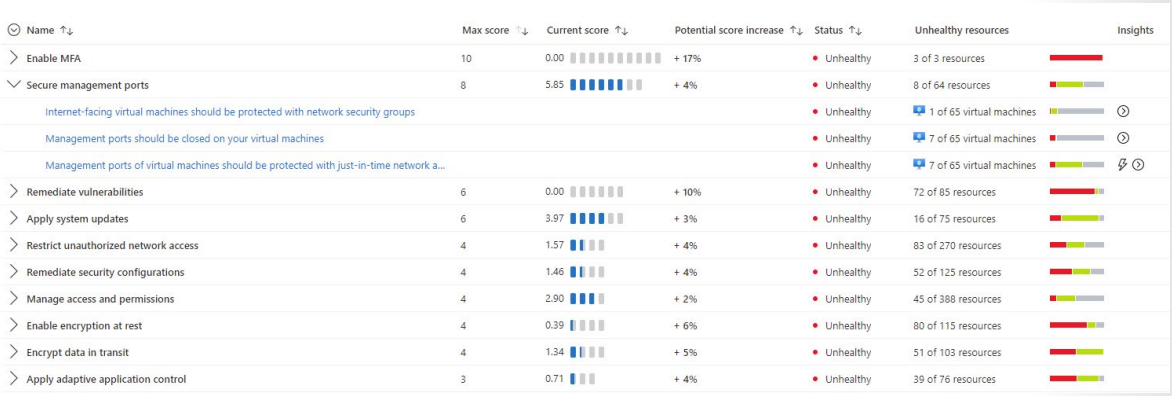
- Require secure transfer (HTTPS) to the storage account
- Lock storage account to prevent accidental or malicious deletion or configuration changes
- Use Azure Active Directory (Azure AD) to authorize access to blob data
- Disable anonymous public read access to containers and blobs
- Configure the minimum required version of Transport Layer Security (TLS) for a storage account.
- Enable firewall rules
- Enable Defender for Storage

As part of the *Monitoring and Reporting* phase, ensure that the storage account has diagnostic logging enabled. Also ensure that Microsoft Defender for Cloud is enabled on the subscription level for continuous assessment of storage accounts as well as security recommendations.

Risk mitigations should be evaluated case-by-case based on those parameters mentioned above, which also includes the type of threat. If during the Identification it was established that there's a high probably that Windows VMs with management port open could be compromised

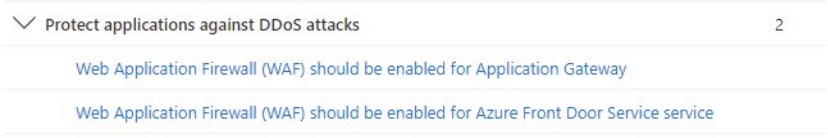
by RDP Brute Force Attack, then you need to mitigate this risk, and one technical control that can reduce the attack vector is Defender for Servers feature called Just-in-Time VM access.

Defender for Cloud provides a list of security controls organized in a top-down approach that can help you to use a priority list to address security recommendations. As you remediate all security recommendations that belong to a security control, you'll see an increase in your overall security score, which means you're improving your security posture. The example below shows the *Secure management ports* security control expanded with three recommendations that needs to be addressed.



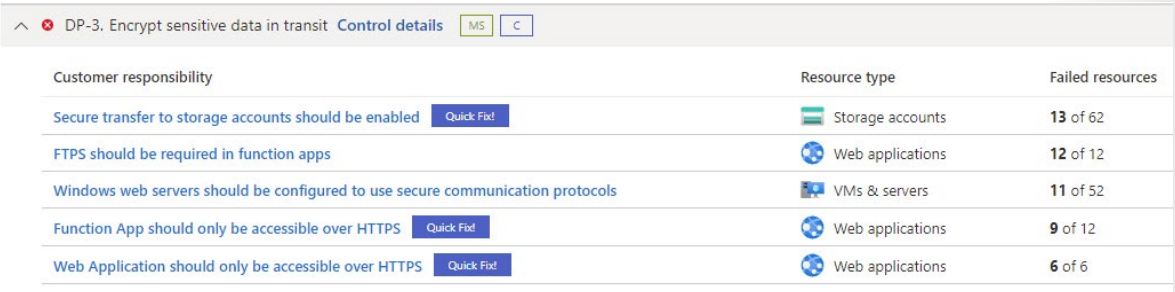
Name	Max score	Current score	Potential score increase	Status	Unhealthy resources	Insights
Enable MFA	10	0.00	+ 17%	Unhealthy	3 of 3 resources	
Secure management ports	8	5.85	+ 4%	Unhealthy	8 of 64 resources	
Internet-facing virtual machines should be protected with network security groups				Unhealthy	1 of 65 virtual machines	
Management ports should be closed on your virtual machines				Unhealthy	7 of 65 virtual machines	
Management ports of virtual machines should be protected with just-in-time network a...				Unhealthy	7 of 65 virtual machines	
Remediate vulnerabilities	6	0.00	+ 10%	Unhealthy	72 of 85 resources	
Apply system updates	6	3.97	+ 3%	Unhealthy	16 of 75 resources	
Restrict unauthorized network access	4	1.57	+ 4%	Unhealthy	83 of 270 resources	
Remediate security configurations	4	1.46	+ 4%	Unhealthy	52 of 125 resources	
Manage access and permissions	4	2.90	+ 2%	Unhealthy	45 of 388 resources	
Enable encryption at rest	4	0.39	+ 6%	Unhealthy	80 of 115 resources	
Encrypt data in transit	4	1.34	+ 5%	Unhealthy	51 of 103 resources	
Apply adaptive application control	3	0.71	+ 4%	Unhealthy	39 of 76 resources	

Once all three are remediated, you'll receive eight points in your secure score, as shown in the Max score column. There are also security controls that will suggest the implementation of a security capability, for example the security control *Protect applications against DDoS attacks* shown below, suggests the enablement of WAF to mitigate this risk.



Protect applications against DDoS attacks	2
Web Application Firewall (WAF) should be enabled for Application Gateway	
Web Application Firewall (WAF) should be enabled for Azure Front Door Service service	

You can also use Azure Security Benchmark to identify the resources that are in risk enable security capabilities to mitigate these risks based on the remediation steps suggested by the benchmark, as shown in the example below:



DP-3. Encrypt sensitive data in transit **Control details** MS C

Customer responsibility	Resource type	Failed resources
Secure transfer to storage accounts should be enabled Quick Fix!	Storage accounts	**13** of 62
FTPS should be required in function apps	Web applications	**12** of 12
Windows web servers should be configured to use secure communication protocols	VMs & servers	**11** of 52
Function App should only be accessible over HTTPS Quick Fix!	Web applications	**9** of 12
Web Application should only be accessible over HTTPS Quick Fix!	Web applications	**6** of 6

Notice that in this scenario, you have a security control called *DP-3 Encrypt sensitive data in transit*, and within this control, you have a series of security recommendations for different workloads (storage account, web applications, VMs and servers). The advantage of this approach is that you're mitigating a specific scenario, which is the encryption of sensitive data in transit, and you're looking at this scenario across different workloads.

As a cybersecurity architect, you need to select the appropriate security capability for a given risk. For certain scenarios that may mean the addition of a new service.

Let's use as an example of a scenario where a company needs to provide customized remote access to employees based on a series of conditions, including limiting access upon an abnormal behavior. Although most users have a normal behavior that can be tracked, when they fall outside of this norm it could be risky to allow them to just sign in.

In scenarios like this, you may want to block that user or maybe just ask them to perform multifactor authentication to prove that they really are who they say they are. To address this risk, you can use Azure AD Conditional Access and use the *Sign-in risk-based Conditional Access* policy.

There are also the scenarios that you'll need to select the appropriate security control for a given risk and in this case the security control may be just hardening the current resource. An example could be to reduce the risk on of an attacker compromise a database by hardening the database and enabling security controls such as Transparent Data Encryption (TDE). This enables you to encrypt data at rest without changing existing applications.

Exercise

Scenario

Tailwind Traders is a modern commerce company. For more than 30 years, the company has been a popular retail destination. It has grown to more than 50 physical stores. Several years ago, its chief executive officer (CEO) anticipated changes in retail and bought a competing e-commerce start-up that was growing aggressively in niche markets. Today, the company is seen as an innovative leader with customer-focused local storefronts.

The retail innovation team reports to the company's chief technology officer (CTO), who was the CEO of the acquired e-commerce start-up. Those technology solutions are the main hub for interactions with customers. Those solutions affect 60 percent of global revenue and produce 30 percent of annual gross sales.

Examples of those innovations include:

- Boundless commerce: Originally a simple e-commerce solution, this custom-built platform now provides online and offline experiences for customers. Customers can make purchases from the platform. The mobile app gathers information from customers' viewing history to customize the retail experience with in-store ads, shopping lists, and other interactions.
- Analytics, AI, and robotics innovation: The team is experimenting with drone delivery, autonomous warehousing, and other AI-led approaches to reduce costs, scale through automation, and improve customer experiences. These experiments are built on big data, analytics, and AI solutions.

The new CIO is focused on improving technical operations in multiple areas to fuel greater innovation throughout the company while limiting disruptions to core business operations. The cloud will play an important role in this transition. One of the key requirements for this

transformation is to empower remote workers in a secure manner. The new CIO wants to ensure remote workers are using multifactor authentication and if they're traveling to visit customers, the access should be restricted based on their geo-location. The CIO also wants to ensure that all incubation projects led by the AI/Robotics Team are tested in an isolated environment to avoid disruption in the production environment.

The new CIO is concerned with the rise of high-profile companies getting compromised and asked the CSO to perform a risk assessment to identify the companies' high assets and ensure they're secure. In addition, the CIO wants the CSO to track security posture enhancement overtime and use cyber-threat intelligence to improve their defenses against threats. The CIO wants to have a monthly meeting to track this progress and the CSO should present a sort of KPI to show how the company is progressing. This is the first transformation effort to start since the new CIO accepted the role. The CIO will closely monitor the project and will examine how IT operates in the cloud.

Questions

1. Evaluate security posture
   - In this scenario, should the company track progress using Azure Security Benchmark or Secure Score? Justify your answer.
   - What tool should the CISO adopt to track progress overtime?
2. Threat intelligence
   - Which tool should be utilized to aggregate CTI feeds and present in a meaningful dashboard?
   - Which tool provides built-in threat intelligence report that can be used to improve the companies' defenses?
3. Which security capability will enable Tailwind Traders to implement the CIO's vision of empowering the remote users while enforcing security and restrictions based on the user's geo-location?

   a. Defender for Cloud

   b. Microsoft Sentinel

   c. Azure AD Identity Protection

   d. Azure WAF

   Answer: C
4. Which cloud security capability should be used to enable the AI/Robotics Team test their apps without disrupting the production environment?

   a. SDL

   b. Azure Landing Zone

   c. Azure Policy

   d. On-premises sandbox

   Answer: B

Summary

In this module you learned how to evaluate your organization's security posture by using different benchmarks, including Azure Security Benchmark. You learned how to use Microsoft Defender for Cloud as a cloud security posture management platform and improved your security hygiene. You also learned to use Secure Score to drive security posture enhancements and track progress overtime. As part of this continuous improvement process, you also learned how to evaluate the security hygiene of cloud workloads and how to design security for Azure Landing Zone.

In addition, you learned how to interpret threat intelligence and used this insight to recommend mitigations when appropriated. Lastly, you learned how to recommend security capabilities or controls to mitigate the risks that were identified.

Visit the links below for more information about the topics covered in this module:

- **Microsoft uses threat intelligence to protect, detect, and respond to threats**[17]
- **What is risk? Azure AD Identity Protection**[18]
- **Sign-in risk-based Conditional Access - Azure Active Directory**[19]
- **Cyber threat intelligence in Microsoft Sentinel - Azure Example Scenarios**[20]
- **Tracking your secure score in Microsoft Defender for Cloud**[21]
- **Security recommendations in Microsoft Defender for Cloud**[22]
- **Microsoft Defender for Cloud threat intelligence report**[23]

17 https://www.microsoft.com/en-us/insidetrack/microsoft-uses-threat-intelligence-to-protect-detect-and-respond-to-threats
18 https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks
19 https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-risk
20 https://docs.microsoft.com/en-us/azure/architecture/example-scenario/data/sentinel-threat-intelligence
21 https://docs.microsoft.com/en-us/azure/defender-for-cloud/secure-score-access-and-track
22 https://docs.microsoft.com/en-us/azure/defender-for-cloud/review-security-recommendations
23 https://docs.microsoft.com/en-us/azure/defender-for-cloud/threat-intelligence-reports

Knowledge check

Check your knowledge

Multiple choice

Item 1. Which tool should you use to automate compliance for core Azure Services and set a standard in the environment's settings?

- ☐ Azure Automation Update Management
- ☐ Azure Policy
- ☐ Azure Blueprints

Multiple choice

Item 2. Which solution should you utilize if the requirements for your project include cloud security posture management from a centralized location?

- ☐ Microsoft Defender for Cloud
- ☐ Azure Purview
- ☐ Azure AD

Multiple choice

Item 3. Which steps below are not part of the recommended approach to validate a new Azure Policy that was customized for your organization's compliance requirements?

- ☐ Audit new or updated resource requests
- ☐ Deploy your policy to resources
- ☐ Duplicate your Azure Policy

Multiple choice

Item 4. When you design your data residency strategy, which tool should you use to ensure you're controlling which regions different resource types can be deployed to?

- ☐ Azure Policy
- ☐ Azure AD
- ☐ Azure Identity Protection

Multiple choice

Item 5. To which scenario is the use of SSL/TLS protocols to exchange data across different locations relevant?

- ☐ Data at-rest in the datacenter
- ☐ Data in-transit
- ☐ Data at-rest in the user's device

Multiple choice

Item 6. When evaluating your organization's security posture, which pillar represents proactive measures that need to be done to enhance the security hygiene of your workloads?

- ☐ Detect
- ☐ Protect
- ☐ Respond

Multiple choice

Item 7. Which capability in Defender for Cloud can be used to expedite notifications to workload owners when new security recommendations are available?

- ☐ Workflow Automation
- ☐ Secure Score
- ☐ Playbook

Multiple choice

Item 8. Risk detection is a capability that belongs to which product?

- ☐ Defender for Cloud
- ☐ Microsoft Sentinel
- ☐ Azure ID Identity Protection

Answers

Multiple choice

Item 1. Which tool should you use to automate compliance for core Azure Services and set a standard in the environment's settings?

- ☐ Azure Automation Update Management
- ☐ Azure Policy
- ■ Azure Blueprints

Explanation
Azure Blueprints can be used to automate compliance for Azure Services.

Multiple choice

Item 2. Which solution should you utilize if the requirements for your project include cloud security posture management from a centralized location?

- ■ Microsoft Defender for Cloud
- ☐ Azure Purview
- ☐ Azure AD

Explanation
Security posture management from a centralized location is one of the main capabilities in Defender for Cloud.

Multiple choice

Item 3. Which steps below are not part of the recommended approach to validate a new Azure Policy that was customized for your organization's compliance requirements?

- ☐ Audit new or updated resource requests
- ☐ Deploy your policy to resources
- ■ Duplicate your Azure Policy

Explanation
The duplication of Azure Policy is not part of the validation process.

Multiple choice

Item 4. When you design your data residency strategy, which tool should you use to ensure you're controlling which regions different resource types can be deployed to?

- ■ Azure Policy
- ☐ Azure AD
- ☐ Azure Identity Protection

Explanation
Azure Policy has features that enable admins to enforce the deployment per region.

Multiple choice

Item 5. To which scenario is the use of SSL/TLS protocols to exchange data across different locations relevant?

☐ Data at-rest in the datacenter

■ Data in-transit

☐ Data at-rest in the user's device

Explanation
SSL/TLS are relevant for data-in-transit.

Multiple choice

Item 6. When evaluating your organization's security posture, which pillar represents proactive measures that need to be done to enhance the security hygiene of your workloads?

☐ Detect

■ Protect

☐ Respond

Explanation
Protect is the only pillar that includes proactive measures. Detect and Respond are both reactive.

Multiple choice

Item 7. Which capability in Defender for Cloud can be used to expedite notifications to workload owners when new security recommendations are available?

■ Workflow Automation

☐ Secure Score

☐ Playbook

Explanation
Workflow Automation is the best choice for automating notifications.

Multiple choice

Item 8. Risk detection is a capability that belongs to which product?

☐ Defender for Cloud

☐ Microsoft Sentinel

■ Azure ID Identity Protection

Explanation
Azure AD Identity Protection is the only one of the three choices that includes Risk detection.

Module 3 Design security for infrastructure

Understand architecture best practices and how they are changing with the Cloud

Introduction

Security teams must still focus on reducing business risk from attacks and work to get confidentiality, integrity, and availability assurances built into all information systems and data. In this module you'll learn how architecture best practices help to design a more secure environment and how Cloud computing is changing the architect thought process.

Learning Objectives

In this module, you'll learn how to:

- Plan and implement a security strategy across teams
- Establish a strategy and process for proactive and continuous evaluation of security strategy

Plan and implement a security strategy across teams

Shifting to the cloud for security is more than a simple technology change, it's a generational shift in technology akin to moving from mainframes to desktops and onto enterprise servers. Successfully navigating this change requires fundamental shifts in expectations and mindset by security teams. Adopting the right mindsets and expectations reduces conflict within your organization and increases the effectiveness of security teams.

While these could be part of any security modernization plan, the rapid pace of change in the cloud makes adopting them an urgent priority.

- Partnership with shared goals. In this age of fast paced decisions and constant process evolution, security can no longer adopt an "arms-length" approach to approving or denying changes to the environment. Security teams must partner closely with business and IT teams to establish shared goals around productivity, reliability, and security and work collectively with those partners to achieve them.
- This partnership is the ultimate form of "shift left"—the principle of integrating security earlier in the processes to make fixing security issues easier and more effective. This requires a culture change by all involved (security, business, and IT), requiring each to learn the culture and norms of other groups while simultaneously teaching others about their own. Security teams must:
    - Learn the business and IT objectives and why each is important and how they're thinking about achieving them as they transform.
    - Share why security is important in the context of those business goals and risks, what other teams can do to meet security goals, and how they should do it.
- Security is an ongoing risk, not a problem. You can't "solve" crime. At its core, security is just a risk management discipline, which happens to be focused on malicious actions by humans rather than natural events. Like all risks, security isn't a problem that can be fixed by a solution, it's a combination of the likelihood and impact of damage from a negative event, an attack. It's most comparable to traditional corporate espionage and criminal activities where organizations face motivated human attackers who have financial incentive to successfully attack the organization.
- Success in either productivity or security requires both. An organization must focus on both security and productivity in today's "innovation or become irrelevant" environment. If the organization isn't productive and driving new innovation, it could lose competitiveness in the marketplace that causes it to weaken financially or eventually fail. If the organization isn't secure and loses control of assets to attackers, it could lose competitiveness in the marketplace that causes it to weaken financially and eventually fail.
- No organization is perfect at adopting the cloud, not even Microsoft. Microsoft's IT and security teams grapple with many of the same challenges that our customers do such as figuring out how to structure programs well, balancing supporting legacy software with supporting cutting-edge innovation, and even technology gaps in cloud services. As these teams learn how to better operate and secure the cloud, they're actively sharing their lessons learned via documents like this along with others on the IT showcase site,

while continuously providing feedback to our engineering teams and third-party vendors to improve their offerings.

- Opportunity in transformation. It's important to view digital transformation as a positive opportunity for security. While it's easy to see the potential downsides and risk of this change, it's easy to miss the massive opportunity to reinvent the role of security and earn a seat at the table where decisions are made. Partnering with the business can result in increased security funding, reduce wasteful repetitive efforts in security, and make working in security more enjoyable as they will be more connected to the organization's mission.

As an architect you need to ensure all teams are aligned to a single strategy that both enables and secures enterprise systems and data.

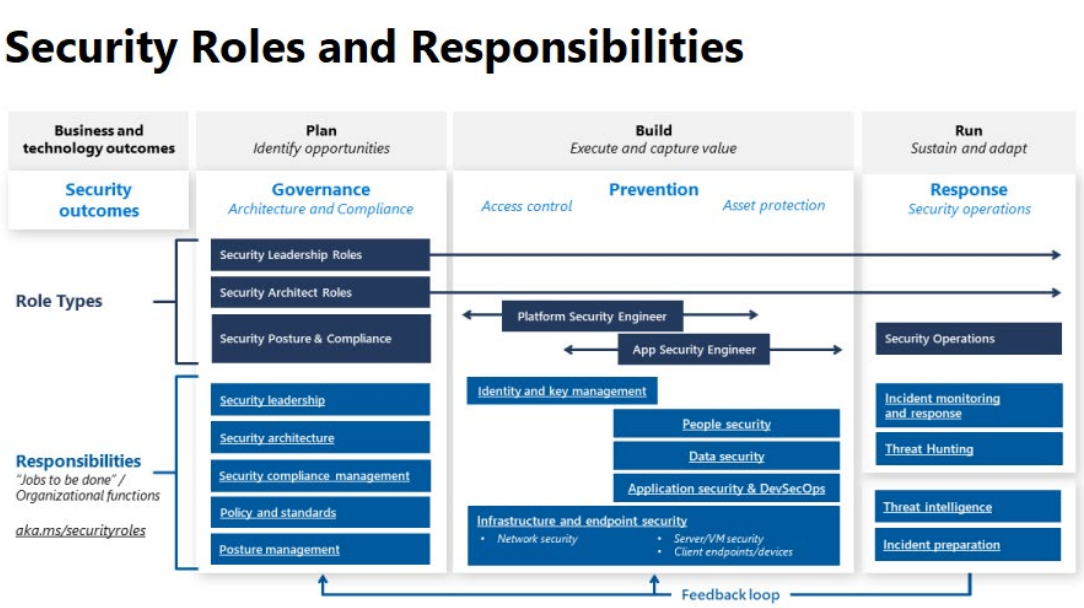
Security strategy principles

Watch the video below for an overview about the Security Strategy principles:

[!VIDEO https://www.microsoft.com/videoplayer/embed/RWtT8S]

Security roles and responsibilities

Business and technology outcomes are traditionally driven using a plan/build/run framework (which is becoming increasingly agile for digital transformation with rapid iteration through all stages). Security Outcomes are driven through a similar framework of governance, prevention and response that maps to that framework. This also maps to the NIST Cybersecurity framework of identify, protect, detect, respond, and recover functions. The diagram below shows how security roles map to business outcome enablement:



Security Leadership Roles and Security Architect Roles provide vision, guidance, and coordination across the organization and technical estate.

Security Posture and Compliance Roles focus on identifying security risks across the enterprise and work with subject matter experts to ensure the top risks are mitigated. The responsibility of these roles typically includes Security Compliance Management, Policy and Standards, and Posture management.

Platform Security Engineers are security subject matter experts (SMEs) that focus on enterprise-wide systems like identity and key management, and various infrastructure and endpoint disciplines like Network security, Server/VM security, and Client endpoints/devices.

Application Security Engineers are security SMEs that focus on securing individual workload and applications, often as they're developed. These responsibilities include per-workload application of infrastructure and endpoint skills as well as application security & DevSecOps and Data security. We expect that demand will continue to increase for these skillsets as digital transformation increases adoption of Cloud technology, DevOps/DevSecOps models, and Infrastructure as Code approaches.

People Security is an emerging discipline that focuses on educating people, protecting them, and protecting the organization against insider risks.

The operational phase is executed by a combination of operations teams who are responsible for the production environments (IT & OT Operations, DevOps) + Security Operations teams.

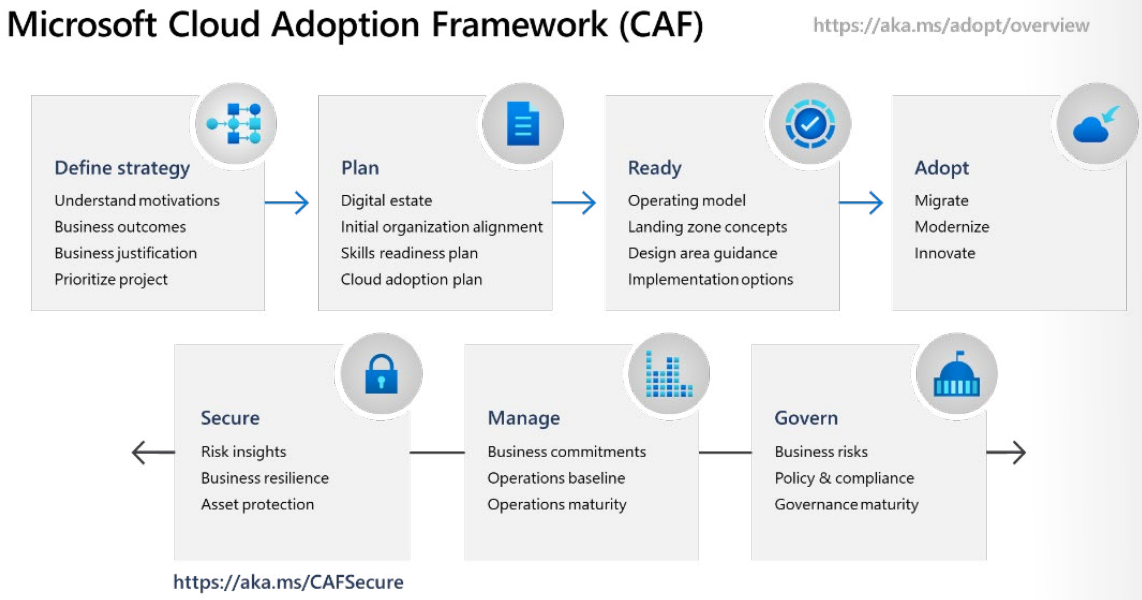
Security Operations typically focuses on reactive Incident monitoring & response and proactive Threat Hunting for adversaries that slipped past

detections. Threat Intelligence and Incident preparation functions are often incubated in security operations, but then shift to a broader scope as they mature and become integrated into technology and organizational processes.

Creating a healthy Feedback loop is critical to effectiveness in all parts of security (and in maturing security processes). We expect the relationship between prevention and response to continue to get closer as teams increasingly automate technical processes and adopt DevOps style processes focused on rapid agile iteration.

Security strategy considerations

Security helps create assurances of confidentiality, integrity, safety, and availability for a business. Security efforts have a critical focus on protecting against the potential impact to operations caused by both internal and external malicious and unintentional acts. The diagram below shows that security is integrated as part of the cloud adoption process and from the beginning (defining the strategy), security is taking into consideration.



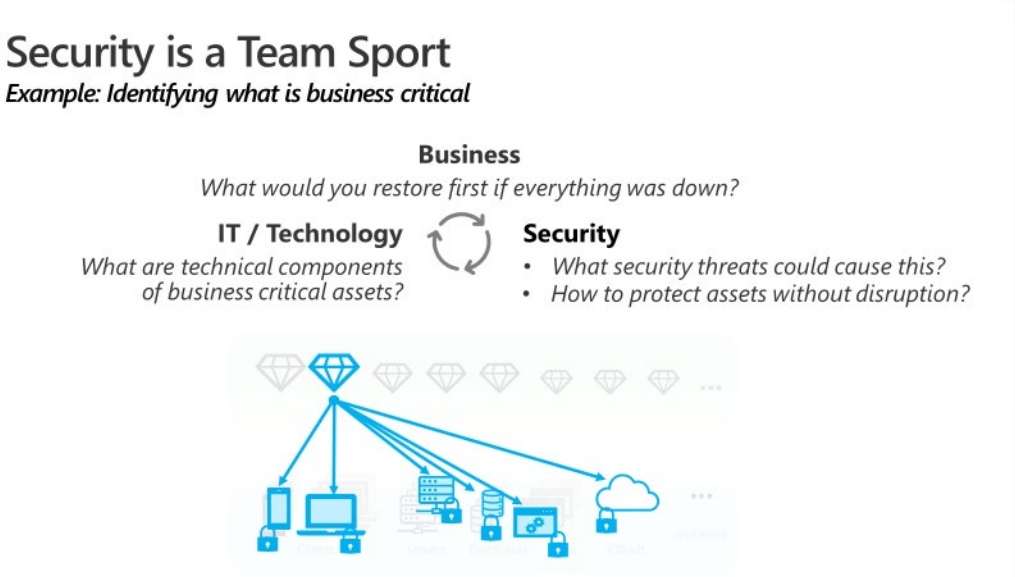
Adhering to these steps will help you integrate security at critical points in the process. The goal is to avoid obstacles in cloud adoption and reduce unnecessary business or operational disruption.

Effective security in the cloud requires a strategy that reflects the current threat environment and the nature of the cloud platform that's hosting the enterprise assets. A clear strategy improves the effort of all teams to provide a secure and sustainable enterprise cloud environment. The security strategy must enable defined business outcomes, reduce risk to an acceptable level, and enable employees to be productive.

A cloud security strategy provides guidance to all teams working on the technology, processes, and people readiness for this adoption. The strategy should inform the cloud architecture and technical capabilities, guide the security architecture and capabilities, and influence the training and education of teams.

Build and implement a security strategy for cloud that includes the input and active participation of all teams. While the process documentation format can vary, it always includes:

- **Active input from teams:** Strategies typically fail if people in the organization don't buy into them. Ideally, get all teams in the same room to collaboratively build the strategy. In the workshops we conduct with customers, we often find organizations have been operating in de facto silos and these meetings often result in people meeting each other for the first time. We find that inclusiveness is a requirement. If some teams aren't invited, this meeting typically has to be repeated until all participants join it. If they don't join, then the project doesn't move forward.
- **Documented and communicated clearly:** All teams must have awareness of the security strategy. Ideally, the security strategy is a security component of the overall technology strategy. This strategy includes why to integrate security, what is important in security, and what security success looks like. This strategy includes specific guidance for application and development teams so they can get clear, organized guidance without having to read through non-relevant information.
- **Stable, but flexible:** Keep strategies relatively consistent and stable, but the architectures and the documentation might need to add clarity and accommodate the dynamic nature of cloud. For example, filtering out malicious external traffic would stay consistent as a strategic imperative even if you shift from the use of a third-party next generation firewall to Azure Firewall and adjust diagrams and guidance on how to do it.
- **Start with business alignment:** Security teams will address many strategy issues large and small, but you need to start somewhere. We recommend establishing alignment to business goals and risk as the north star and starting point for the security strategy. This may be challenging at first, but by starting with concrete questions like "what would you restore first if all business systems were down?" you can start building relationships while establishing quick wins.



Deliverables

The strategy step should result in a document that can easily be communicated to many stakeholders within the organization. The stakeholders can potentially include executives on the organization's leadership team.

We recommended capturing the strategy in a presentation to facilitate easy discussion and updating. This presentation can be supported with a document, depending on the culture and preferences.

- Strategy presentation: You might have a single strategy presentation, or you might choose to also create summary versions for leadership audiences.
  - Full presentation: This should include the full set of elements for the security strategy in the main presentation or in optional reference slides.
  - Executive summaries: Versions to use with senior executives and board members might contain only critical elements relevant to their role, such as risk appetite, top priorities, or accepted risks.
- You can also record motivations, outcomes, and business justifications in the **strategy and plan template**[1].

Best practices for building security strategy

Successful programs incorporate these elements into their security strategy process:

- Align closely to business strategy: Security's charter is to protect business value. It's critical to align all security efforts to that purpose and minimize internal conflict.
  - Build a shared understanding of business, IT, and security requirements.
  - Integrate security early into cloud adoption to avoid last-minute crises from avoidable risks.

1 https://raw.githubusercontent.com/microsoft/CloudAdoptionFramework/master/plan/cloud-adoption-framework-strategy-and-plan-template.docx

- Use an agile approach to immediately establish minimum security requirements and continuously improve security assurances over time.
- Encourage security culture change through intentional proactive leadership actions.

- Modernize security strategy: The security strategy should include considerations for all aspects of modern technology environment, current threat landscape, and security community resources.
  - Adapt to the shared responsibility model of the cloud.
  - Include all cloud types and multi-cloud deployments.
  - Prefer native cloud controls to avoid unnecessary and harmful friction.
  - Integrate the security community to keep up with the pace of attacker evolution.

Accountable team	Responsible and supporting teams
Security leadership team (chief information security officer (CISO) or equivalent)	Cloud strategy team
	Cloud security team
	Cloud adoption team
	Cloud center of excellence or central IT team

Strategy approval

Executives and business leaders with accountability for outcomes or risks of business lines within the organization should approve this strategy. This group might include the board of directors, depending on the organization.

Establish a strategy and process for proactive and continuous evolution of a security strategy

Planning puts the security strategy into action by defining outcomes, milestones, timelines, and task owners. Security planning and cloud adoption planning should not be done in isolation. It's critical to invite the cloud security team into the planning cycles early, to avoid work stoppage or increased risk from security issues being discovered too late.

Security planning considerations

Security planning works best with in-depth knowledge and awareness of the digital estate and existing IT portfolio that comes from being fully integrated into the cloud planning process.

Deliverables:

- Security plan: A security plan should be part of the main planning documentation for the cloud. It might be a document that uses the **strategy and plan template**[2], a detailed slide deck, or a project

2 https://raw.githubusercontent.com/microsoft/CloudAdoptionFramework/master/plan/cloud-adoption-framework-strategy-and-plan-template.docx

file. Or it might be a combination of these formats, depending on the organization's size, culture, and standard practices. The security plan should include all of these elements:

  - Organizational functions plan, so teams know how current security roles and responsibilities will change with the move to the cloud.
  - Security skills plan to support team members as they navigate the significant changes in technology, roles, and responsibilities.
  - Technical security architecture and capabilities roadmap to guide technical teams.
- Security awareness and education plan, so all teams have basic critical security knowledge.
- Asset sensitivity marking to designate sensitive assets by using a taxonomy aligned to business impact. The taxonomy is built jointly by business stakeholders, security teams, and other interested parties.
- Security changes to the cloud plan: Update other sections of the cloud adoption plan to reflect changes triggered by the security plan.

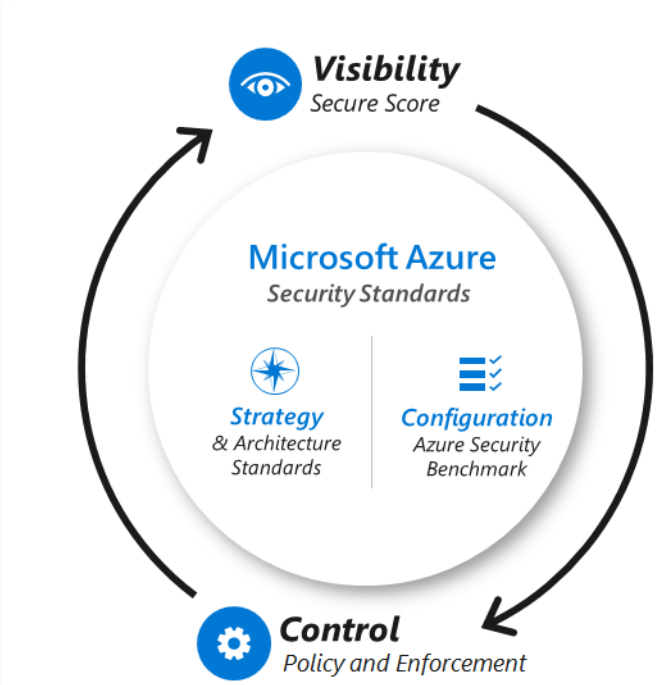
Best practices for security planning:

Your security plan is likely to be more successful if your planning takes the approach of:

- Assume a hybrid environment: That includes software as a service (SaaS) applications and on-premises environments. It also includes multiple cloud infrastructure as a service (IaaS) and platform as a service (PaaS) providers, if applicable.
- Adopt agile security: Establish minimum security requirements first and move all noncritical items to a prioritized list of next steps. This should not be a traditional, detailed plan of 3-5 years. The cloud and threat environment changes too fast to make that type of plan useful. Your plan should focus on developing the beginning steps and end state:
  - Quick wins for the immediate future that will deliver a high impact before longer-term initiatives begin. The time frame can be 3-12 months, depending on organizational culture, standard practices, and other factors.
  - Clear vision of the desired end state to guide each team's planning process (which might take multiple years to achieve).
- Share the plan broadly: Increase awareness of, feedback from, and buy-in by stakeholders.
- Meet the strategic outcomes: Ensure that your plan aligns to and accomplishes the strategic outcomes described in the security strategy.
- Set ownership, accountability, and deadlines: Ensure that the owners for each task are identified and are committed to completing that task in a specific time frame.
- Connect with the human side of security: Engage people during this period of transformation and new expectations by:
  - Actively supporting team member transformation with clear communication and coaching on:
    - What skills they need to learn.
    - Why they need to learn the skills (and the benefits of doing so).
    - How to get this knowledge (and provide resources to help them learn).
  - Making security awareness engaging to help people genuinely connect with their part of keeping the organization safe.

- Review Microsoft learnings and guidance: Microsoft has published insights and perspectives to help your organization plan its transformation to the cloud and a modern security strategy. The material includes recorded training, documentation, and security best practices and recommended standards.

Microsoft has built capabilities and resources to help accelerate your implementation of this security guidance on Microsoft Azure. The following diagram shows a holistic approach for using security guidance and platform tooling to establish security visibility and control over your cloud assets in Azure.



You can use this model to proactively and continuously monitor the evolution of a security strategy, which includes evaluating new security capabilities that may be added over time. The arrows represent the continuous assessment of workloads to bring visibility, in this case using Secure Score from Defender for Cloud and enforcing controls using policies.

Establish essential security practices

Security in the cloud starts with applying the most important security practices to the people, process, and technology elements of your system. Additionally, some architectural decisions are foundational and are very difficult to change later so should be carefully applied.

Whether you're already operating in the cloud or you're planning for future adoption, we recommend that you follow these 11 essential security practices (in addition to meeting any explicit regulatory compliance requirements).

People:

- Educate teams about the cloud security journey
- Educate teams on cloud security technology

Process:

- Assign accountability for cloud security decisions
- Update incident response processes for cloud
- Establish security posture management

Technology:

- Require passwordless or multifactor authentication
- Integrate native firewall and network security
- Integrate native threat detection

Foundational architecture decisions:

- Standardize on a single directory and identity
- Use identity-based access control (instead of keys)
- Establish a single unified security strategy

Each organization should define its own minimum standards. Risk posture and subsequent tolerance to that risk can vary widely based on industry, culture, and other factors. For example, a bank might not tolerate any potential damage to its reputation from even a minor attack on a test system. Some organizations would gladly accept that same risk if it accelerated their digital transformation by three to six months.

Security management strategy

The ultimate objectives for a security organization don't change with adoption of cloud services, but how those objectives are achieved will change. Security teams must still focus on reducing business risk from attacks and work to get confidentiality, integrity, and availability assurances built into all information systems and data.

Security teams need to modernize strategies, architectures, and technology as the organization adopts cloud and operates it over time. While the size and number of changes can initially seem daunting, the modernization of the security program allows security to shed some painful burdens associated with legacy approaches. An organization can temporarily operate with legacy strategy and tooling, but this approach is difficult to sustain with the pace of change in cloud and the threat environment:

Security teams are likely to be left out of cloud adoption decision making if they take a legacy mindset of “arms-length” security where the answer always starts with "no" (instead of working together with IT and business teams to reduce risk while enabling the business).

Security teams will have a difficult time detecting and defending against cloud attacks if they use only legacy on-premises tooling and exclusively adhere to network perimeter-only doctrine for all defenses and monitoring.

Continuous assessment

Continuous assessment and validation of these systems is essential to ensure secure configurations remain intact and previously unknown vulnerabilities are identified. Continuous assessment is imperative to monitor the security posture of your workloads, which can include virtual machines, networks, storage, and applications. Since Cloud Computing by nature is very dynamic, new workloads will be constantly provisioned and if your cloud adoption isn't mature, you may not have all the guardrails in place to enforce security by default, which means that continuous assessment of your workloads become even more critical.

In an IaaS and PaaS environment you can use Defender for Cloud capabilities for continuous security assessment of your workloads. Defender for Cloud fills three vital needs as you manage the security of your resources and workloads in the cloud and on-premises:

Security requirement	Defender for Cloud solution
Continuous assessment - Understand your current security posture.	Secure score - A single score so that you can tell, at a glance, your current security situation: the higher the score, the lower the identified risk level.
Secure - Harden all connected resources and services.	Security recommendations - Customized and prioritized hardening tasks to improve your posture. You implement a recommendation by following the detailed remediation steps provided in the recommendation. For many recommendations, Defender for Cloud offers a "Fix" button for automated implementation!
Defend - Detect and resolve threats to those resources and services.	Security alerts - With the enhanced security features enabled, Defender for Cloud detects threats to your resources and workloads. These alerts appear in the Azure portal and Defender for Cloud can also send them by email to the relevant personnel in your organization. Alerts can also be streamed to SIEM, SOAR, or IT Service Management solutions as required.

The central feature in Defender for Cloud that enables you to achieve those goals is secure score. Defender for Cloud continually assesses your resources, subscriptions, and organization for security issues. It then aggregates all the findings into a single score so that you can tell, at a glance, your current security situation: the higher the score, the lower the identified risk level.

Defender for Cloud continuously discovers new resources that are being deployed across your workloads and assesses whether they're configured according to security best practices. If not, they're flagged and you get a prioritized list of recommendations for what you need to fix. Recommendations help you reduce the attack surface across each of your resources.

Deploying Microsoft Defender for Cloud enables the continuous assessment of your organization's security posture and controls. It strengthens the security posture of your cloud resources, and with its integrated Microsoft Defender plans, Defender for Cloud protects workloads running in Azure, hybrid, and other cloud platforms. Learn more about Microsoft Defender for Cloud.

In a SaaS environment with Microsoft 365, you can use Compliance Manager for continuous assessment. Compliance Manager automatically identifies settings in your Microsoft 365 environment that help determine when certain configurations meet improvement action implementation requirements. Compliance Manager detects signals from other compliance solutions you may have deployed, including data lifecycle management, information protection, communication compliance, and insider risk management, and also uses Microsoft Secure Score monitoring of complementary improvement actions.

Your action status is updated on your dashboard within 24 hours of a change being made. Once you follow a recommendation to implement a control, you'll typically see the control status updated the next day. For example, if you turn on Azure Active Directory Multi-Factor Authentication in the Azure AD portal, Compliance Manager detects the setting and reflects it in the control access solution details. Conversely, if you didn't turn on MFA, Compliance Manager flags that as a recommended action for you to take.

Continuous strategy evolution

The evolution of your security strategy over time requires you to set high-level goals and continually assess progress towards those goals. One method for doing this is to establish and monitor security metrics.

Microsoft recommends scorecard metrics in four main areas:

- Business enablement – How much security friction is in user experience and business processes?
- Security Improvement – Are we getting better every month?
- Security Posture - How good are we at preventing damage?
- Security Response – How good are we at responding to and recovering from attacks?

Sample metrics in each of these categories are summarized in the following table. These performance measurements can help get the discussion started on how to measure success for a security program.

Ultimately these measures and the targets/thresholds/weightings will be customized by each organization based on their business goals, risk appetite, and technical portfolio, and more.

Security Area	Metric
Business Enablement	Mean Time for security review
	# days for application security review
	Average boot/logon time for managed devices
	Number of security interruptions in user workflow
	% of IT help desk time spent on low-value security activities
Security Posture	% of new apps reviewed
	Secure score
	% compliant apps
	# of privileged accounts meeting 100% of requirements
	# pf accounts meeting 100% of requirements
Security Response	Mean Time to Recover (MTTR)
	Mean Time to Acknowledge (MTTA)
	Time to Restore Critical Systems
	# of high severity incidents
	Incident growth rate (overall)
Security Improvement	# of modernization projects open
	# modernization project milestones achieved in last 60 days
	Number of repetitive manual steps removed from workflows
	# of Lessons learned from internal/external incidents

Exercise

Tailwind Traders is a modern commerce company. For more than 30 years, the company has been a popular retail destination. It has grown to more than 50 physical stores. Several years ago, its chief executive officer (CEO) anticipated changes in retail and bought a competing e-commerce startup that was growing aggressively in niche markets. Today, the company is seen as an innovative leader with customer-focused local storefronts.

The retail innovation team reports to the company's chief technology officer (CTO), who was the CEO of the acquired e-commerce start-up. Those technology solutions are the main hub for interactions with customers. Those solutions affect 60 percent of global revenue and produce 30 percent of annual gross sales.

The new CIO is focused on improving technical operations in multiple areas to fuel greater innovation throughout the company while limiting

disruptions to core business operations. The cloud will play an important role in this transition. One of the key requirements for this transformation is to empower remote workers in a secure manner. The new CIO wants to ensure remote workers are using multifactor authentication and if they're traveling to visit customers, the access should be restricted based on their geo-location. The CIO also wants to ensure that all incubation project led by the AI/Robotics Team is tested in an isolated environment to avoid disruption in the production environment.

To accomplish this vision the CIO hired a new Chief Information Security Officer (CISO) and made a reorganization to assign the following teams under this new CISO:

- Cloud strategy team
- Cloud security team
- Cloud adoption team
- Cloud center of excellence or central IT team

To accomplish this vision, the new CISO needs to modernize the company's security strategy. The security strategy should include considerations for all aspects of modern technology environment, current threat landscape, and security community resources.

Questions

1. Security Strategy
    - What are the security strategy principles that should be used in this project?
    - Who needs to approve the security strategy before it goes live?
2. Validating the solution
    - Which solution should Tailwind Traders utilize to understand the security state and risk across resources in Azure?
    - Which product should Tailwind Traders utilize to define consistent security policies and enable controls?

Summary

In this module you learned that as an architect you need to ensure all teams are aligned to a single strategy that both enables and secures enterprise systems and data. You learned about the security strategy principles and key aspects that need to be taken into consideration when planning your security strategy. You learned that a security strategy provides not only guidance to all teams working on the technology, but also influences processes, and people readiness for this adoption.

In addition, you learned about key deliverables and best practices for security that need to be part of your adoption plan. You learned about essential security practices, security management and the importance of using a Proof of Concept (PoC) as an opportunity to deliver evidence that the proposed solution solves business problems.

Visit the links below for more information about the topics covered in this module:

- **Define a security strategy - Cloud Adoption Framework**[3]
- **Get started: Secure the enterprise environment - Cloud Adoption Framework**[4]
- **Cloud security architecture functions - Cloud Adoption Framework**[5]
- **Chief Information Security Officer (CISO) Workshop, Module 2: Security Management - Security documentation**[6]
- **What's inside Microsoft Security Best Practices?**[7]

3 https://docs.microsoft.com/azure/cloud-adoption-framework/strategy/define-security-strategy
4 https://docs.microsoft.com/azure/cloud-adoption-framework/get-started/security
5 https://docs.microsoft.com/azure/cloud-adoption-framework/organize/cloud-security-architecture
6 https://docs.microsoft.com/security/ciso-workshop/ciso-workshop-module-2
7 https://docs.microsoft.com/security/compass/microsoft-security-compass-introduction

Design a strategy for securing server and client endpoints

Introduction

A security strategy needs to be established to ensure servers and client endpoints are protected and that there are continuously assessed to ensure their security posture is up to date while ensuring that there are tools in places to obtain enterprise-wide visibility into attack dynamics.

Learning Objectives

In this module, you'll learn how to:

- Specify security baselines for server and client endpoints
- Specify security requirements for servers
- Specify security requirements for mobile devices and clients
- Specify requirements for securing Active Directory Domain Services
- Design a strategy to manage secrets, keys, and certificates
- Design a strategy for secure remote access
- Understand security operations frameworks, processes, and procedures
- Understand deep forensics procedures by resource type

Specify security baselines for server and client endpoints

Even though Windows Client and Windows Server are designed to be secure out-of-the-box, many organizations still want more granular control over their security configurations. To navigate the large number of controls, organizations often seek guidance on configuring various security features. Microsoft provides this guidance in the form of security baselines.

Security baselines are groups of pre-configured Windows settings that help you apply and enforce granular security settings that are recommended by the relevant security teams. You can also customize each baseline you deploy to enforce only those settings and values you require. When you create a security baseline profile in Intune, you're creating a template that consists of multiple device *configuration* profiles.

We recommend that you implement an industry-standard configuration that is broadly known and well-tested, such as Microsoft security baselines, as opposed to creating a baseline yourself. This helps increase flexibility and reduce costs.

What are security baselines?

Every organization faces security threats. However, the types of security threats that are of most concern to one organization can be completely different from another organization. For example, an e-commerce company may focus on protecting its Internet-facing web apps, while a hospital may focus on protecting

confidential patient information. The one thing that all organizations have in common is a need to keep their apps and devices secure. These devices must be compliant with the security standards (or security baselines) defined by the organization.

A security baseline is a group of Microsoft-recommended configuration settings that explains their security impact. These settings are based on feedback from Microsoft security engineering teams, product groups, partners, and customers.

Security baselines are an essential benefit to customers because they bring together expert knowledge from Microsoft, partners, and customers.

In modern organizations, the security threat landscape is constantly evolving, and IT pros and policymakers must keep up with security threats and make required changes to security settings to help mitigate these threats. To enable faster deployments and make managing Microsoft products easier, Microsoft provides customers with security baselines that are available in consumable formats, such as Group Policy Objects Backups.

Baselines principles

Our recommendations follow a streamlined and efficient approach to baseline definitions. The foundation of that approach is essentially:

- The baselines are designed for well-managed, security-conscious organizations in which standard end users do not have administrative rights.
- A baseline enforces a setting only if it mitigates a contemporary security threat and does not cause operational issues that are worse than the risks they mitigate.
- A baseline enforces a default only if it's otherwise likely to be set to an insecure state by an authorized user:
  - If a non-administrator can set an insecure state, enforce the default.
  - If setting an insecure state requires administrative rights, enforce the default only if it's likely that a misinformed administrator will otherwise choose poorly.

Selecting the appropriate baseline

The selection of the appropriate security baseline starts with the understanding of which operating system the security baseline needs to be applied to. There are many versions of Windows Client and Windows Servers, and in a heterogeneous environment, you may need to have multiple baselines that address the requirements of each operating system. Once you have an inventory of the operating systems and its versions, you can decide which tool you'll utilize to deploy these baselines.

One option is to utilize the **Security Compliance Toolkit (SCT)**, which is a set of tools that allows enterprise security administrators to download, analyze, test, edit, and store Microsoft-recommended security configuration baselines for Windows and other Microsoft products. The SCT enables administrators to effectively manage their enterprise's Group Policy Objects (GPOs). Using the toolkit, administrators can compare their current GPOs with Microsoft-recommended GPO baselines or other baselines, edit them, store them in GPO backup file format, and apply them broadly through Active Directory or individually through local policy.

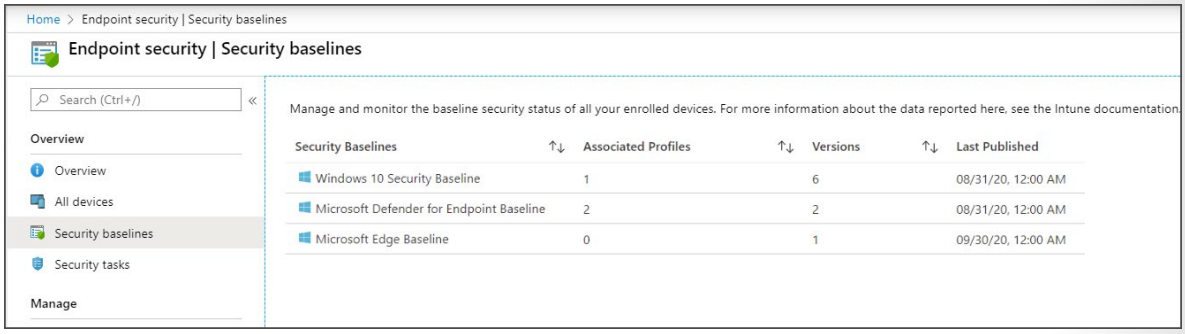
Another option available for Servers is to use Azure security baselines to machines through **Azure Security Benchmark (ASB)**. The ASB has guidance for OS hardening which has led to security baseline documents for Windows and Linux.

However, if the focus of your security baseline is to configure endpoint (Windows Client), you can use **Intune** to automate the deployment and configuration. By using Intune capabilities, you can easily deploy Windows security baselines to help you secure and protect your users and devices. You can deploy security baselines to groups of users or devices in Intune, and the settings apply to devices that run Windows 10/11. For example, the MDM Security Baseline automatically enables BitLocker for removable drives, automatically requires a password to unlock a device, automatically disables basic authentication, and more. When a default value doesn't work for your environment, customize the baseline to apply the settings you need.

Separate baseline types can include the same settings but use different default values for those settings. It's important to understand the defaults in the baselines you choose to use, and to then modify each baseline to fit your organizational needs.

Is very important to emphasize that Intune security baselines are not CIS or NIST compliant. While Microsoft security team consults organizations, such as CIS, to compile its recommendations, there's no one-to-one mapping between "CIS-compliant" and Microsoft baselines.

The recommendations in these baselines are from the Microsoft security team's engagement with enterprise customers and external agencies, including the Department of Defense (DoD), National Institute of Standards and Technology (NIST), and more. Microsoft shares recommendations and baselines with these organizations. These organizations also have their own recommendations that closely mirror Microsoft's recommendations. As mobile device management (MDM) continues to grow into the cloud, Microsoft created equivalent MDM recommendations of these group policy baselines. These additional baselines are built into Microsoft Intune, and include compliance reports on users, groups, and devices that follow (or don't follow) the baseline. Security baselines can be found in the Endpoint security configuration as shown below:



Specify security requirements for servers

An integral part of securing your Windows Server environment is making sure the servers and client computers are configured in as secure a manner as possible, also known as "hardening" the operating system. To define the security requirements for servers you first need to understand the server's role, since the server role will dictate the hardening settings that should be applied.

While most Servers will have a core foundational security requirement, some servers in a unique role may need more configuration. For example, if your Server is a Domain Controller (DC), you'll have extra steps to harden the Directory Services that are peculiar to this scenario. In general you should start by understanding the current state of the server, and for that you can use the Microsoft Security Compliance Toolkit (SCT).

Analyze security configuration

The Microsoft Security Compliance Toolkit (SCT) is a set of tools provided by Microsoft that you can use to download and implement security configuration baselines, typically referred to as simply security baselines, for Windows Server and other Microsoft products, including Windows 10, Microsoft 365 Apps for enterprise, and Microsoft Edge. You implement the security configuration baselines by using the toolkit to manage your Group Policy Objects (GPOs).

You can also use the SCT to compare your current GPOs to the recommended GPO security baselines. You can then edit the recommended GPOs and apply them to devices in your organization.

In addition to security baselines for Windows Server, the SCT also includes the Policy Analyzer and Local Group Policy Object (LGPO) tools, which also help you manage your GPO settings.

Secure Servers (Domain Members)

Each computer that is member of a domain keeps a local Administrator account. This is the account that you configure when you first deploy the computer manually, or which is configured automatically when you use software deployment tools such as Microsoft Endpoint Configuration Manager. The local Administrator account allows IT staff to sign in to the computer if they can't establish connectivity to the domain.

Managing passwords for the local Administrator account for every computer in the organization can be extremely complicated. An organization with 5,000 computers has 5,000 separate local Administrator accounts to manage. What often happens is that organizations assign a single, common local Administrator account password to all local Administrator accounts. The drawback to this approach is that people beyond the IT operations team often figure out this password, and then use it to gain unauthorized local Administrator access to computers in their organization.

The "Local Administrator Password Solution" (LAPS) provides management of local account passwords of domain joined computers. LAPS is available for all currently supported Windows Server and client operating system versions. To get LAPS to function, you must update the AD DS schema. You perform this update by running the *Update-AdmPwdADSchema* cmdlet, which is included in a Windows PowerShell module that's made available when you install LAPS on a computer.

Another important part of server's protection is to ensure that you disable legacy protocols and enforce a more secure communication method. Server Message Block (SMB) protocol is a network protocol primarily used for file sharing. Along with its common file-sharing use, it's also frequently used by printers, scanners, and email servers. The original version of SMB, SMB 1.0 does not support encryption. SMB encryption was introduced with version 3.0.

Encryption is important whenever sensitive data is moved by using the SMB protocol. SMB encryption also lets file services provide secure storage for server applications such as Microsoft SQL Server and is generally simpler to use than dedicated hardware-based encryption.

SMB 3.0 introduced end-to-end encryption to the SMB (Server Message Block) protocol. SMB encryption provides for data packet confidentiality and helps prevent a malicious hacker from tampering with or eavesdropping on any data packet.

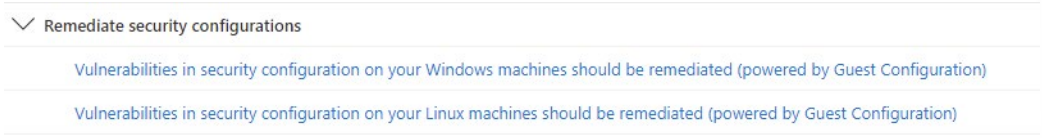
SMB 3.1.1, introduced in Windows Server 2016, provides several enhancements to SMB 3.0 security, including pre-authentication integrity checks and encryption improvements. The version of SMB included with Windows Server 2019 is SMB 3.1.1.c.

Windows Server systems support multiple versions of SMB (Server Message Block). This enables them to communicate with servers and clients running other operating systems and other Windows versions. To use SMB 3.1.1, both your host server and the system it communicates with must support SMB 3.1.1.

Pre-authentication with SMB 3.1.1 isn't compatible with devices that modify SMB packets, such as some wide area network (WAN) accelerators. Therefore, you might need to replace some network equipment to use SMB 3.1.1.

Azure Security Benchmark

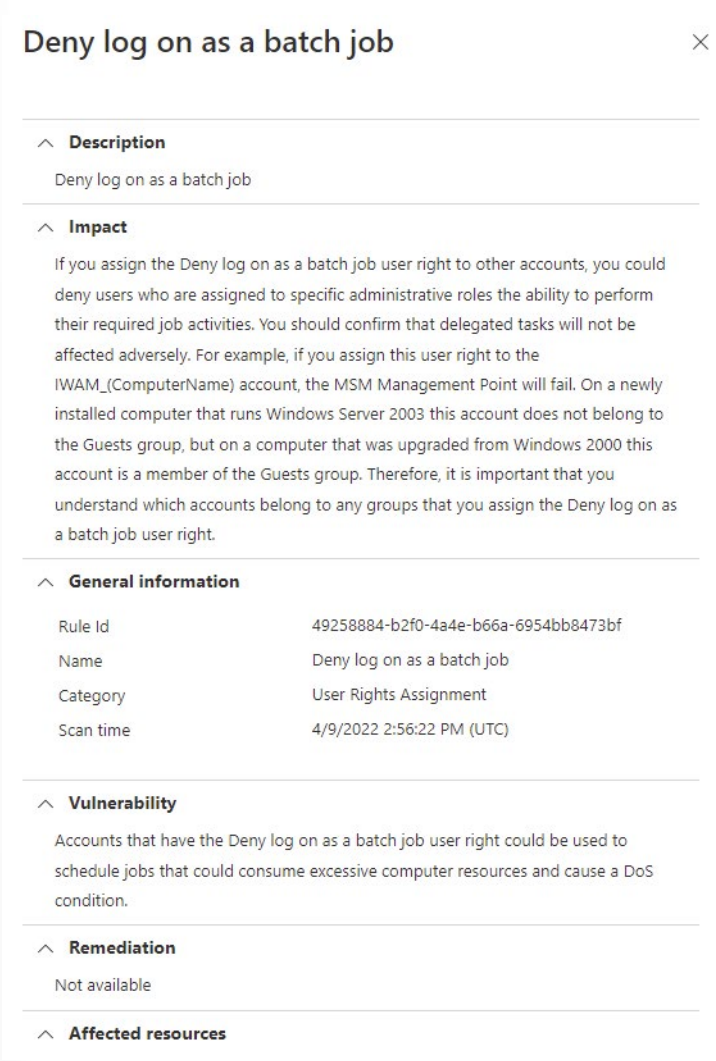
Another approach to specify server requirements is to ensure all servers are compliant with **Azure Security Benchmark (ASB)** OS baseline. The ASB OS baseline is available through Microsoft Defender for Cloud in the format of security recommendations for **Windows**[8] or **Linux**[9], as shown below:



Once you access one of those recommendations, you'll see a set of rules that are using the Azure Guest Configuration capability to run security checks to verify if the operating system is using the most secure configurations.

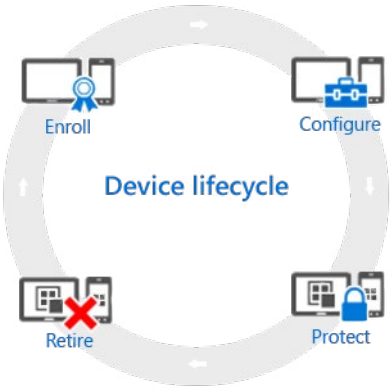
Once you click on each rule, you'll have more details about the security check and the affected resources, as shown in the image below:

8 https://docs.microsoft.com/azure/governance/policy/samples/guest-configuration-baseline-windows
9 https://docs.microsoft.com/azure/governance/policy/samples/guest-configuration-baseline-linux



Specify security requirements for mobile devices and clients

All devices that you manage have a lifecycle. Intune can help you manage this lifecycle: from enrollment, through configuration and protection, to retiring the device when it's no longer required. The mobile device management (MDM) lifecycle is shown below:



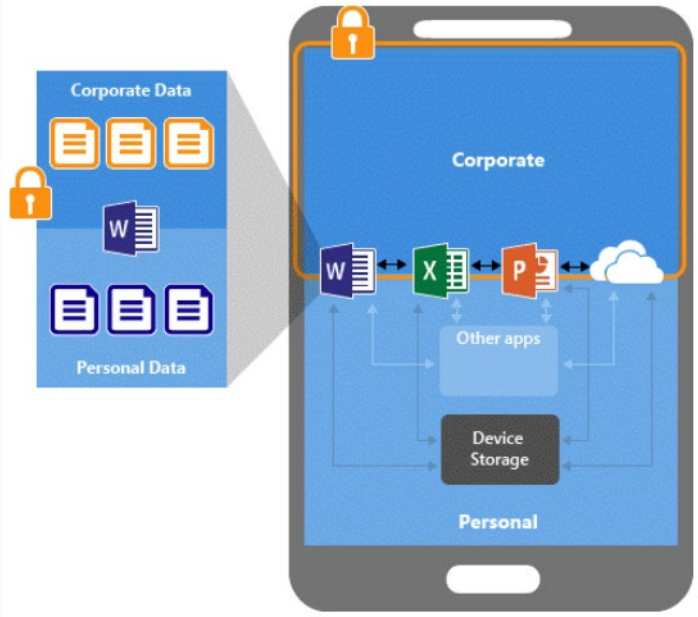
When you specify security requirements for mobile devices, most of your focus will be on the *Configure* and *Protect* stages, but you should also have general considerations on each one of the other phases:

- **Enroll**: evaluate the types of devices you have in your organization and verify the **enrollment options**[10] available.
- **Configure**: to ensure that your devices are secure and compliant with company standards, you can choose from a wide range of policies during the initial **configuration**[11] of the device.
- **Protect**: protecting devices from unauthorized access is one of the most important tasks that you perform. In addition to the items that were established in the initial configuration, you have addition settings to protect your devices from unauthorized access or malicious attack.
- **Retire**: When a device gets lost or stolen, when it needs to be replaced, or when users move to another position, it's usually time to retire or wipe the device. There are many ways you can do this—including resetting the device, removing it from management, and wiping the corporate data on it.

App isolation and control

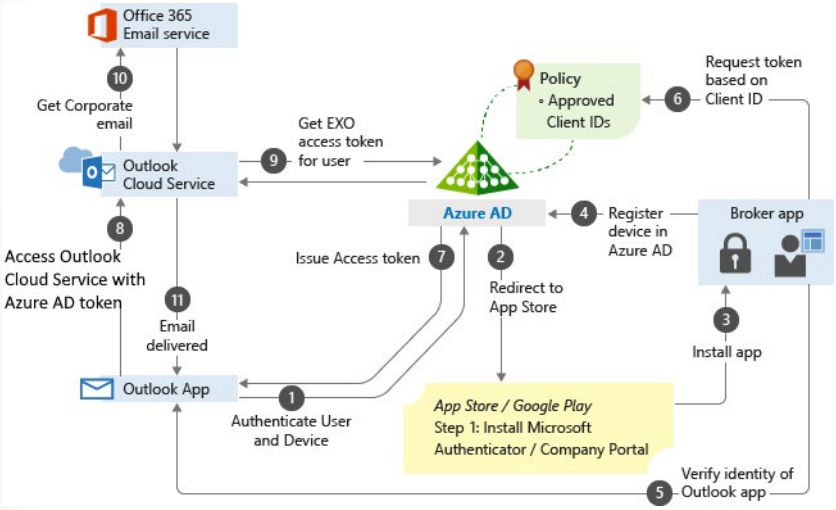
When dealing with mobile devices that will also have corporate date, you need to ensure that corporate data and apps are isolated and can be managed separately from the user's owned apps.

10 https://docs.microsoft.com/mem/intune/enrollment/device-enrollment
11 https://docs.microsoft.com/mem/intune/configuration/device-profiles



Intune app protection policies help protect your work files on devices that are enrolled into Intune. You can also use app protection policies on employee-owned devices that are not enrolled for management in Intune. In this case, even though your company doesn't manage the device, you still need to make sure that work files and resources are protected.

In the example below, the admin has applied app protection policies to the Outlook app. This is followed by a conditional access rule that adds the Outlook app to an approved list of apps. This list can be used when accessing corporate e-mail.



In a scenario like this, you could use the app protection to enforce the security requirements for your mobile devices, which could include:

- Encrypt work files.
- Require a PIN to access work files.
- Require the PIN to be reset after five failed attempts.

- Block work files from being backed up in iTunes, iCloud, or Android backup services.
- Require work files to only be saved to OneDrive or SharePoint.
- Prevent protected apps from loading work files on jailbroken or rooted devices.
- Block access to work files if the device is offline for 720 minutes.
- Remove work files if device is offline for 90 days.

Device settings

Besides the app isolation and protection on the device, you also need to ensure that the device's settings are securely configured. With the Mobility and Security feature, you can manage and secure mobile devices when they're connected to your Microsoft 365 organization. Mobile devices like smartphones and tablets that are used to access work email, calendar, contacts, and documents play a big part in making sure that employees get their work done anytime, from anywhere. So, it's critical that you help protect your organization's information when people use devices. You can use Basic Mobility and Security to set device security policies and access rules. You can also use it to wipe mobile devices if they're lost or stolen.

Basic Mobility and Security can help you secure and manage mobile devices like iPhones, iPads, Androids, and Windows Phones used by licensed Microsoft 365 users in your organization. You can create mobile device management policies with settings that can help control access to your organization's Microsoft 365 email and documents for supported mobile devices and apps. If a device is lost or stolen, you can remotely wipe the device to remove sensitive organizational information.

Hardening options for mobile devices must include the following requirements:

- Require a password
- Prevent simple password
- Require an alphanumeric password
- Minimum password length
- Number of sign-in failures before device is wiped
- Minutes of inactivity before device is locked
- Password expiration (days)
- Remember password history and prevent reuse
- Require data encryption on devices
- Device can't be jail broken or rooted
- Block screen capture
- Require password when accessing application store

When establishing your security requirement for mobile devices, make sure that the security setting that you want to manage is available for the type of device that your organization utilizes. For more information about how to manage mobile devices that connect to your Microsoft 365 organization according to each type of device, visit **this article**[12].

12 https://docs.microsoft.com/microsoft-365/admin/basic-mobility-security/capabilities

Client requirements

One important consideration to take is if your client workstation is domain joined. Many environments use on-premises Active Directory (AD). When AD domain-joined devices are also joined to Azure AD, they're called hybrid Azure AD joined devices. Using Windows Autopilot, you can enroll hybrid Azure AD joined devices in Intune. To enroll, you also need a Domain Join configuration profile.

Once you determine if the client is domain joined or not, you can start planning the security requirements for the operating system configuration. The requirements can also be part of the security baseline that was initially selected. You can deploy security baselines to groups of users or devices in Intune, and the settings apply to devices that run Windows 10/11. For example, the *MDM Security Baseline* automatically enables BitLocker for removable drives, automatically requires a password to unlock a device, automatically disables basic authentication, and more. When a default value doesn't work for your environment, customize the baseline to apply the settings you need.

Client security requirements should include security policies that can manage the following settings:

- **Antivirus**[13]
- **Disk encryption**[14]
- **Windows firewall**[15]
- **Endpoint Detection and Response (EDR)**[16]
- **Attack surface reduction**[17]
- **Account protection**[18]

Specify requirements for securing Active Directory Domain Services

Organizations can use Active Directory Domain Services (AD DS) in Windows Server to simplify user and resource management while creating scalable, secure, and manageable infrastructures. You can use AD DS to manage your network infrastructure, including branch office, Microsoft Exchange Server, and multiple forest environments.

Performing a high-level assessment of your current environment and correctly identifying your Active Directory Domain Services (AD DS) deployment tasks is essential for the success of your AD DS deployment strategy. Your AD DS deployment strategy depends on your existing network configuration.

When it comes to specifying the requirements to secure your Active Director Domain Services, you must start by understanding that threat actors tend to perform credential theft and that they target some specific accounts. Credential theft attacks are those in which an attacker initially gains highest-privilege (root, Administrator, or SYSTEM, depending on the operating system in use) access to a computer on a network and then uses freely available tooling to extract credentials from the sessions of other logged-on accounts. Depending on the system configuration, these credentials can be extracted in the form of hashes, tickets, or even plaintext passwords.

Because the target of credential theft is usually highly privileged domain accounts and VIP accounts, it's important for administrators to be conscious of activities that increase the likelihood of success of a

13 https://docs.microsoft.com/mem/intune/protect/endpoint-security-antivirus-policy
14 https://docs.microsoft.com/mem/intune/protect/endpoint-security-disk-encryption-policy
15 https://docs.microsoft.com/mem/intune/protect/endpoint-security-firewall-policy
16 https://docs.microsoft.com/mem/intune/protect/endpoint-security-edr-policy
17 https://docs.microsoft.com/mem/intune/protect/endpoint-security-asr-policy
18 https://docs.microsoft.com/mem/intune/protect/endpoint-security-account-protection-policy

credential-theft attack. Although attackers also target VIP accounts, if VIPs are not given high levels of privilege on systems or in the domain, theft of their credentials requires other types of attacks, such as socially engineering the VIP to provide secret information.

The core vulnerability that allows credential theft attacks to succeed is the act of logging on to computers that are not secure with accounts that are broadly and deeply privileged throughout the environment. Which means that among the requirements to secure AD DS you need to ensure that you're reducing the attack surface, which includes the following tasks:

- **Implementing Least-Privilege Administrative Models**: focuses on identifying the risk that the use of highly privileged accounts for day-to-day administration presents, in addition to providing recommendations to implement to reduce the risk that privileged accounts present.
- **Implementing Secure Administrative Hosts**: describes principles for deployment of dedicated, secure administrative systems, in addition to some sample approaches to a secure administrative host deployment.
- **Securing Domain Controllers Against Attack**: discusses policies and settings that, although similar to the recommendations for the implementation of secure administrative hosts, contain some domain controller-specific recommendations to help ensure that the domain controllers and the systems used to manage them are well-secured.

In addition, you should never administer a trusted system (that is, a secure server such as a domain controller) from a less-trusted host (that is, a workstation that isn't secured to the same degree as the systems it manages). Also, do not rely on a single authentication factor when performing privileged activities; that is, username and password combinations should not be considered acceptable authentication because only a single factor (something you know) is represented. You should consider where credentials are generated and cached or stored in administrative scenarios.

Securing Domain Controllers Against Attack

In datacenters, physical domain controllers should be installed in dedicated secure racks or cages that are separate from the general server population. When possible, domain controllers should be configured with Trusted Platform Module (TPM) chips and all volumes in the domain controller servers should be protected via BitLocker Drive Encryption. BitLocker generally adds performance overhead in single digit percentages but protects the directory against compromise even if disks are removed from the server. BitLocker can also help protect systems against attacks such as rootkits because the modification of boot files will cause the server to boot into recovery mode so that the original binaries can be loaded. If a domain controller is configured to use software RAID, serial-attached SCSI, SAN/NAS storage, or dynamic volumes, BitLocker can't be implemented, so locally attached storage (with or without hardware RAID) should be used in domain controllers whenever possible.

Group Policy Objects that link to all domain controllers OUs in a forest should be configured to allow RDP connections only from authorized users and systems (for example, jump servers). This can be achieved through a combination of user rights settings and WFAS configuration and should be implemented in GPOs so that the policy is consistently applied. If it's bypassed, the next Group Policy refresh returns the system to its proper configuration.

You should run all domain controllers on the newest version of Windows Server that is supported within your organization and prioritize decommissioning of legacy operating systems in the domain controller population. By keeping your domain controllers current and eliminating legacy domain controllers, you can often take advantage of new functionality and security that may not be available in domains or forests with domain controllers running legacy operating system.

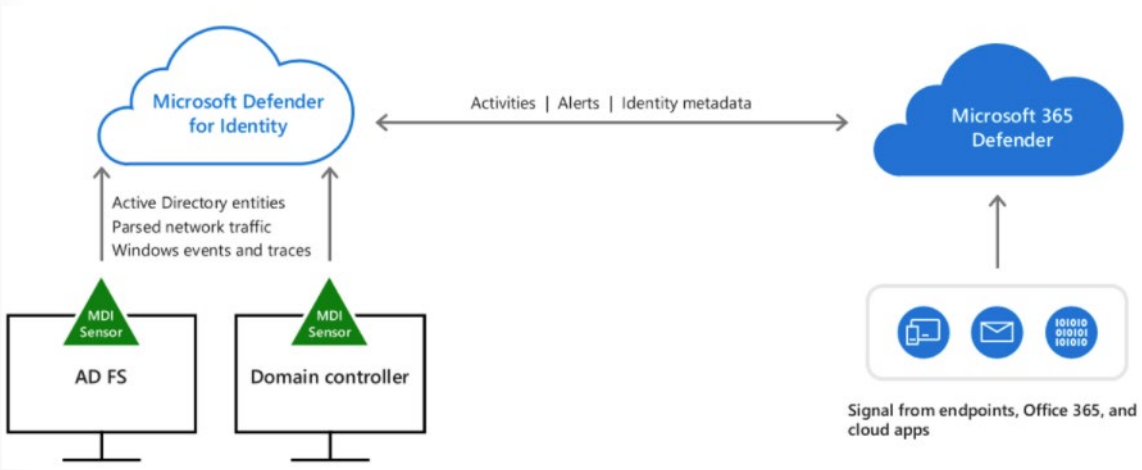
Although it may seem counterintuitive, you should consider patching domain controllers and other critical infrastructure components separately from your general Windows infrastructure. If you use enterprise configuration management software for all computers in your infrastructure, compromise of the systems management software can be used to compromise or destroy all infrastructure components managed by that software. By separating patch and systems management for domain controllers from the general population, you can reduce the amount of software installed on domain controllers, in addition to tightly controlling their management.

In addition, make sure to:

- Continuously monitor Active Directory for **signs of compromise**[19] using tools such as **Microsoft Defender for Identity**[20]
- Enable and review **audit policy**[21]

Microsoft Defender for Identity

Microsoft Defender for Identity (MDI) monitors your domain controllers by capturing and parsing network traffic and using Windows events directly from your domain controllers, then analyzes the data for attacks and threats. Utilizing profiling, deterministic detection, machine learning, and behavioral algorithms Defender for Identity learns about your network, enables detection of anomalies, and warns you of suspicious activities. The image below shows the core architecture of Defender for Identity:



Once you install the Defender for Identity sensor directly on your domain controller or AD FS server, it accesses the event logs it requires directly from each server. After the logs and network traffic are parsed by the sensor, Defender for Identity sends only the parsed information to the Defender for Identity cloud service (only a percentage of the logs are sent).

Design a strategy to manage secrets, keys, and certificates

Azure Key Vault is a centralized cloud service for storing application secrets such as encryption keys, certificates, and server-side tokens. Key Vault helps you control your applications' secrets by keeping

19 https://docs.microsoft.com/windows-server/identity/ad-ds/plan/security-best-practices/monitoring-active-directory-for-signs-of-compromise
20 https://docs.microsoft.com/defender-for-identity/sensor-monitoring
21 https://docs.microsoft.com/windows-server/identity/ad-ds/plan/security-best-practices/audit-policy-recommendations

them in a single central location and providing secure access, permissions control, and access logging. There are three primary concepts used in an Azure Key Vault: vaults, keys, and secrets.

You use Azure Key Vault to create multiple secure containers, called *vaults*. Vaults help reduce the chances of accidental loss of security information by centralizing application secrets storage. Organizations will have several key vaults. Each key vault is a collection of cryptographic keys and cryptographically protected data (call them "secrets") managed by one or more responsible individuals within your organization. These key vaults represent the logical groups of keys and secrets for your organization; those that you want to manage together. They are like folders in the file system. Key vaults also control and log the access to anything stored in them.

Keys are the central actor in the Azure Key Vault service. A given key in a key vault is a cryptographic asset destined for a particular use such as the asymmetric master key of Microsoft Azure RMS, or the asymmetric keys used for SQL Server TDE (Transparent Data Encryption), CLE (Column Level Encryption) and Encrypted backup.

Secrets are small (less than 10K) data blobs protected by a HSM-generated key created with the Key Vault. Secrets exist to simplify the process of persisting sensitive settings that almost every application has: storage account keys, .PFX files, SQL connection strings, data encryption keys, etc.

Azure Key Vault enables Microsoft Azure applications and users to store and use certificates, which are built on top of keys and secrets and add an automated renewal feature.

When designing your strategy to maintain Key Vault, make sure to include the following security best practices:

Best practice	Solution
Grant access to users, groups, and applications at a specific scope.	Use RBAC's predefined roles. For example, to grant access to a user to manage key vaults, you would assign the predefined role Key Vault Contributor to this user at a specific scope. The scope, in this case, would be a subscription, a resource group, or just a specific key vault. If the predefined roles don't fit your needs, you can define your own roles.
Control what users have access to.	Access to a key vault is controlled through two separate interfaces: management plane, and data plane. The management plane and data plane access controls work independently. Use RBAC to control what users have access to. For example, if you want to grant an application the rights to use keys in a key vault, you only need to grant data plane access permissions using key vault access policies. No management plane access is needed for this application. Conversely, if you want a user to be able to read vault properties and tags but not have any access to keys, secrets, or certificates, by using RBAC, you can grant read access to the management plane. No access to the data plane is required.

Best practice	Solution
Store certificates in your key vault.	Azure Resource Manager can securely deploy certificates stored in Azure Key Vault to Azure VMs when the VMs are deployed. By setting appropriate access policies for the key vault, you also control who gets access to your certificate. Another benefit's that you manage all your certificates in one place in Azure Key Vault.
Ensure that you can recover a deletion of key vaults or key vault objects.	Deletion of key vaults or key vault objects can be either inadvertent or malicious. Enable the soft delete and purge protection features of Key Vault, particularly for keys that are used to encrypt data at rest. Deletion of these keys is equivalent to data loss, so you can recover deleted vaults and vault objects if needed. Practice Key Vault recovery operations regularly.

Manage access to secrets, certificates, and keys

Key Vault access has two facets: the management of the Key Vault itself, and accessing the data contained in the Key Vault. Documentation refers to these facets as the management plane and the data plane.

These two areas are separated because the creation of the Key Vault (a management operation) is a different role than storing and retrieving a secret stored in the Key Vault. To access a key vault, all users or apps must have proper authentication to identify the caller, and authorization to determine the operations the caller can perform.

Authentication

Azure Key Vault uses Azure Active Directory (Azure AD) to authenticate users and apps that try to access a vault. Authentication is always performed by associating the authenticated identity of any user or app making a request with the Azure AD tenant of the subscription where the Key Vault resides. There is no support for anonymous access to a Key Vault.

Authorization

Management operations (creating a new Azure Key Vault) use role-based access control (RBAC). There is a built-in role Key Vault Contributor that provides access to management features of key vaults, but doesn't allow access to the key vault data. This is the recommended role to use. There's also a Contributor role that includes full administration rights - including the ability to grant access to the data plane.

Reading and writing data in the Key Vault uses a separate Key Vault access policy. A Key Vault access policy is a permission set assigned to a user or managed identity to read, write, and/or delete secrets and keys. You can create an access policy using the CLI, REST API, or Azure portal.

Restrict network access

Another point to consider with Azure Key Vault is what services in your network can access the vault. In most cases, the network endpoints don't need to be open to the Internet. You should determine the minimum network access required - for example you can restrict Key Vault endpoints to specific Azure

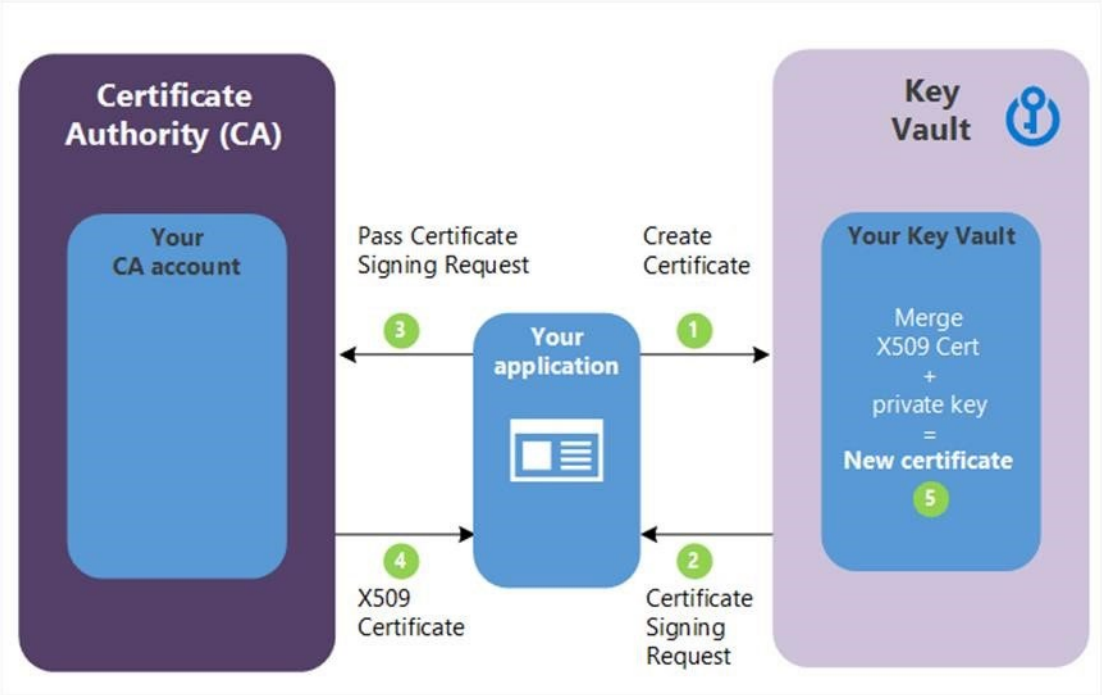
Virtual Network subnets, specific IP addresses, or trusted Microsoft services including Azure SQL, Azure App Service, and various data and storage services that use encryption keys.

Manage certificate

Securely managing certificates is a challenge for every organization. You must ensure that the private key is kept safe, and certificates have an expiration date, which means you need to renew periodically to ensure your website traffic is secure.

Azure Key Vault manages X.509 based certificates that can come from several sources. One strategy is to create self-signed certificates directly in the Azure portal. This process creates a public/private key pair and signs the certificate with its own key. These certificates can be used for testing and development.

Another strategy is to create an X.509 certificate signing request (CSR). This creates a public/private key pair in Key Vault along with a CSR you can pass over to your certification authority (CA). The signed X.509 certificate can then be merged with the held key pair to finalize the certificate in Key Vault as shown in the following diagram.

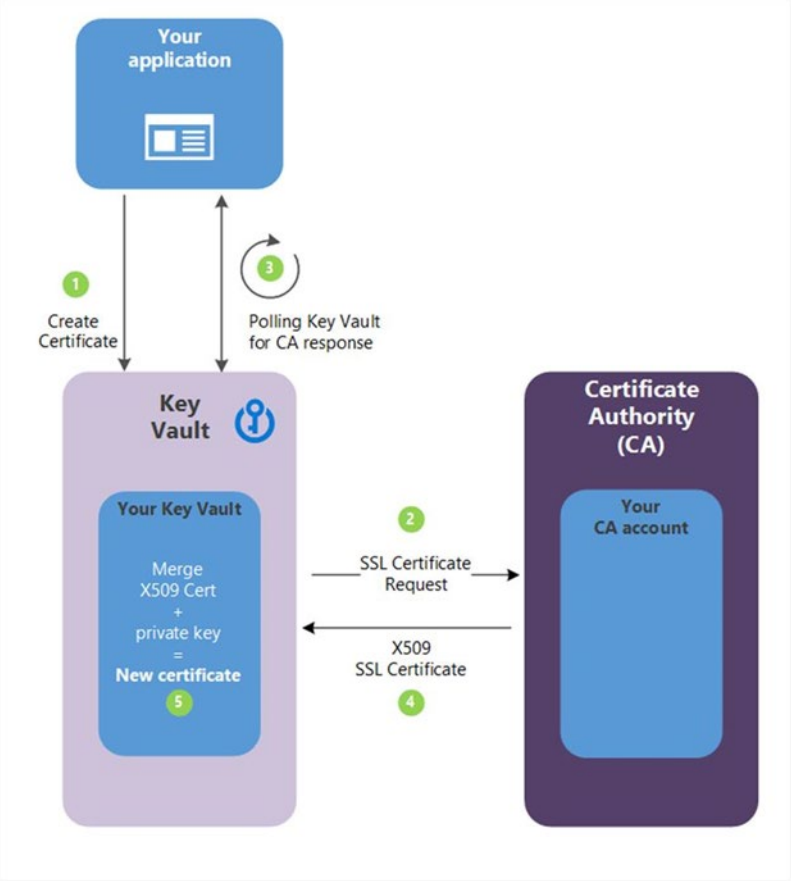


In the previous diagram, your application is creating a certificate which internally begins by creating a key in your Azure Key Vault.

1. Key Vault returns a Certificate Signing Request (CSR) to your application.
2. Your application passes the CSR to your chosen CA.
3. Your chosen CA responds with an X.509 Certificate.
4. Your application completes the new certificate creation with a merger of the X.509 Certificate from your CA.

This strategy works with any certificate issuer and provides better security than handling the CSR directly because the private key is created and secured in Azure Key Vault and never revealed.

Lastly, you can also connect your Key Vault with a trusted certificate issuer (referred to as an integrated CA) and create the certificate directly in Azure Key Vault. This approach requires a one-time setup to connect the certificate authority. You can then request to create a certificate and the Key Vault will interact directly with the CA to fulfill the request in a similar process to the manual CSR creation process shown above. The full details of this process are presented in the following diagram.



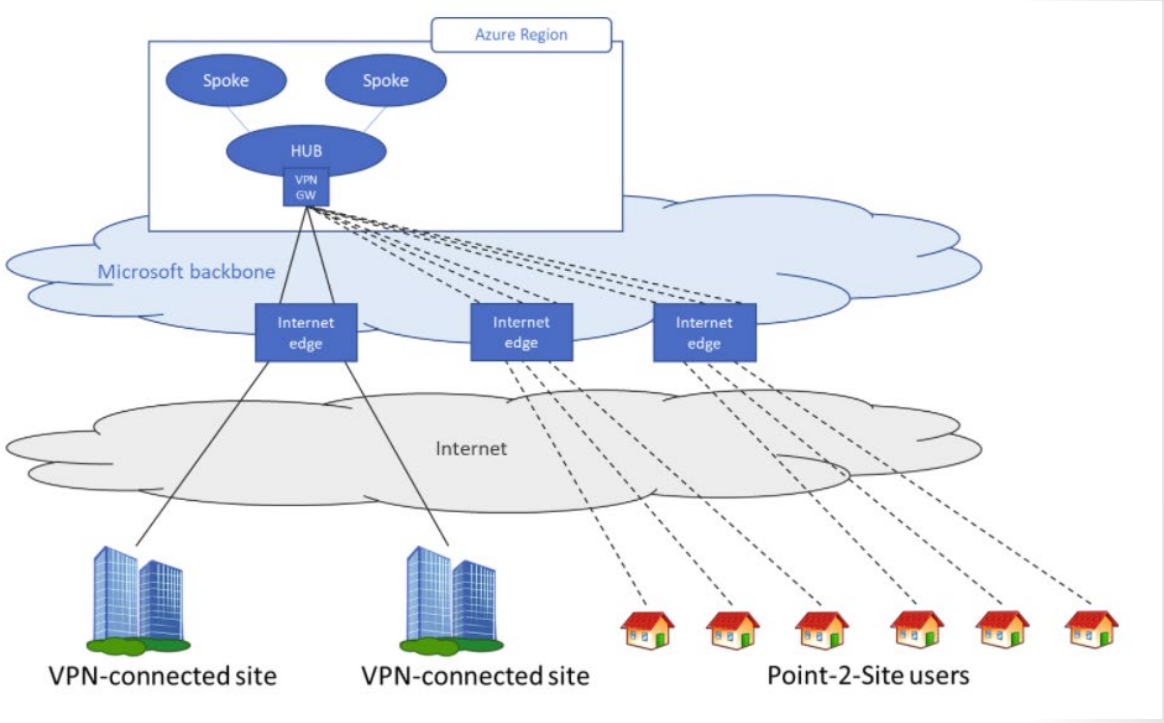
1. In the previous diagram, your application is creating a certificate which internally begins by creating a key in your key vault.
2. Key Vault sends an SSL Certificate Request to the CA.
3. Your application polls, in a loop and wait process, for your Key Vault for certificate completion. The certificate creation is complete when Key Vault receives the CA's response with x509 certificate.
4. The CA responds to Key Vault's SSL Certificate Request with an X509 SSL Certificate.
5. Your new certificate creation completes with the merger of the X509 Certificate for the CA.

This approach has several distinct advantages. Because the Key Vault is connected to the issuing CA, it can manage and monitor the lifecycle of the certificate. That means it can automatically renew the certificate, notify you about expiration, and monitor events such as whether the certificate has been revoked.

Design a strategy for secure remote access

When designing your remote access strategy, you need to take into consideration the different options available and which option is more suitable for the design requirements.

The Azure point-to-site solution is cloud-based and can be provisioned quickly to cater for the increased demand of users to work from home. It can scale up easily and turned off just as easily and quickly when the increased capacity isn't needed anymore. A Point-to-Site (P2S) VPN gateway connection lets you create a secure connection to your virtual network from an individual client computer. A P2S connection is established by starting it from the client computer. This solution is useful for telecommuters who want to connect to Azure VNets or on-premises datacenters from a remote location, such as from home or a conference. You could use this solution if of your design requirements states that remote users need to access to resources that are in Azure and in the on-premises datacenters as shown in the image below:

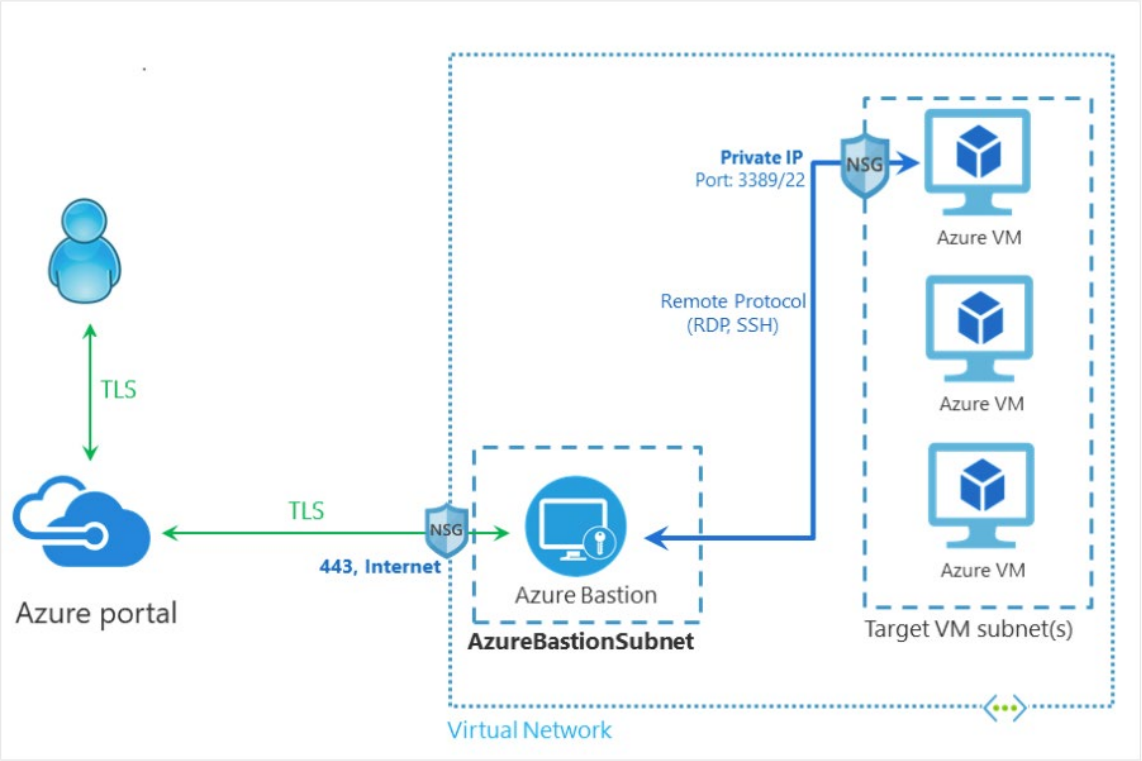


At a high level, the following steps are needed to enable users to connect to Azure resources securely:

1. Create a virtual network gateway (if one does not exist).
2. Configure point-to-site VPN on the gateway
3. Configure a site-to-site tunnel on the Azure virtual network gateway with BGP enabled.
4. Configure the on-premises device to connect to Azure virtual network gateway.
5. Download the point-to-site profile from the Azure portal and distribute to clients

If your design requirements states that you need to connect two sites, for example headquarter and branch office, you could use Site-to-Site VPN. A Site-to-Site (S2S) VPN gateway connection is a connection over IPsec/IKE (IKEv1 or IKEv2) VPN tunnel. S2S connections can be used for cross-premises and hybrid configurations. A S2S connection requires a VPN device located on-premises that has a public IP address assigned to it.

In some scenarios, the remote worker may just need access to resources deployed in Azure, for this scenario the remote worker could use Azure Bastion solution, instead of VPN connection to get secure shell access using Remote Desktop Protocol (RDP) or Secure Shell Protocol (SSH) without requiring public IPs on the VMs being accessed, as shown in the example below:



Below you have some benefits of using this solution:

Benefit	Description
RDP and SSH through the Azure portal	You can get to the RDP and SSH session directly in the Azure portal using a single-click seamless experience.
Remote Session over TLS and firewall traversal for RDP/SSH	Azure Bastion uses an HTML5 based web client that is automatically streamed to your local device. Your RDP/SSH session is over TLS on port 443. This enables the traffic to traverse firewalls more securely.
No Public IP address required on the Azure VM	Azure Bastion opens the RDP/SSH connection to your Azure VM by using the private IP address on your VM. You don't need a public IP address on your virtual machine.
No hassle of managing Network Security Groups (NSGs)	You don't need to apply any NSGs to the Azure Bastion subnet. Because Azure Bastion connects to your virtual machines over private IP, you can configure your NSGs to allow RDP/SSH from Azure Bastion only. This removes the hassle of managing NSGs each time you need to securely connect to your virtual machines.
No need to manage a separate bastion host on a VM	Azure Bastion is a fully managed platform PaaS service from Azure that is hardened internally to provide you secure RDP/SSH connectivity.

Benefit	Description
Protection against port scanning	Your VMs are protected against port scanning by rogue and malicious users because you don't need to expose the VMs to the internet.
Hardening in one place only	Azure Bastion sits at the perimeter of your virtual network, so you don€™t need to worry about hardening each of the VMs in your virtual network.
Protection against zero-day exploits	The Azure platform protects against zero-day exploits by keeping the Azure Bastion hardened and always up to date for you.

Work from home policies requires many IT organizations to address fundamental changes in capacity, network, security, and governance. Employees aren't protected by the layered security policies associated with on-premises services while working from home. This type of scenario could lead you to choose a solution where you can respond faster to changes in the environment, and that€™s where the use of Virtual Desktop Infrastructure (VDI) becomes appropriate. VDI deployments on Azure can help organizations rapidly respond to this changing environment. However, you need a way to protect inbound/outbound Internet access to and from these VDI deployments. You can use Azure Firewall DNAT rules along with its threat intelligence-based filtering capabilities to protect your VDI deployments.

Azure Virtual Desktop is a comprehensive desktop and app virtualization service running in Azure. It's the only virtual desktop infrastructure (VDI) that delivers simplified management, multi-session Windows 10/11, optimizations for Microsoft 365 apps for enterprise, and support for Remote Desktop Services (RDS) environments. You can deploy and scale your Windows desktops and apps on Azure in minutes, and get built-in security and compliance features. Azure Virtual Desktop doesn't require you to open any inbound access to your virtual network. However, you must allow a set of outbound network connections for the Azure Virtual Desktop virtual machines that run in your virtual network.

Understand security operations frameworks, processes, and procedures

The responsibility of the security operation team (also known as Security Operations Center (SOC), or SecOps) is to rapidly detect, prioritize, and triage potential attacks. These operations help eliminate false positives and focus on real attacks, reducing the mean time to remediate real incidents.

Watch the video below for an overview about Security Operations:

[!VIDEO https://www.microsoft.com/videoplayer/embed/RWVECU]

Central SecOps team monitors security-related telemetry data and investigates security breaches. It's important that any communication, investigation, and hunting activities are aligned with the application team. Here are some general best practices for conducting security operations:

- Follow the NIST Cybersecurity Framework functions as part of operations:
  - **Detect** the presence of adversaries in the system.
  - **Respond** by quickly investigating whether it's an actual attack or a false alarm.
  - **Recover** and restore the confidentiality, integrity, and availability of the workload during and after an attack.
- Acknowledge an alert quickly. A detected adversary must not be ignored while defenders are triaging false positives.

- Reduce the time to remediate a detected adversary. Reduce their opportunity time to conduct and attack and reach sensitive systems.
- Prioritize security investments into systems that have high intrinsic value. For example, administrator accounts.
- Proactively hunt for adversaries as your system matures. This effort will reduce the time that a higher skilled adversary can operate in the environment. For example, skilled enough to evade reactive alerts.

SecOps has multiple potential interactions with business leadership, which includes:

- **Business context to SecOps**: SecOps must understand what is most important to the organization so that the team can apply that context to fluid real-time security situations. What would have the most negative impact on the business? Downtime of critical systems? A loss of reputation and customer trust? Disclosure of sensitive data? Tampering with critical data or systems? We've learned it's critical that key leaders and staff in the SOC understand this context. They'll wade through the continuous flood of information and triage incidents and prioritize their time, attention, and effort.
- **Joint practice exercises with SecOps**: Business leaders should regularly join SecOps in practicing response to major incidents. This training builds the muscle memory and relationships that are critical to fast and effective decision making in the high pressure of real incidents, reducing organizational risk. This practice also reduces risk by exposing gaps and assumptions in the process that can be fixed before a real incident occurs.
- **Major incidents updates from SecOps**: SecOps should provide updates to business stakeholders for major incidents as they happen. This information allows business leaders to understand their risk and take both proactive and reactive steps to manage that risk.
- **Business intelligence from the SOC**: Sometimes SecOps finds that adversaries are targeting a system or data set that isn't expected. As these discoveries are made, the threat intelligence team should share these signals with business leaders as they might trigger insight for business leaders. For example, someone outside the company is aware of a secret project or unexpected attacker targets highlight the value of an otherwise overlooked dataset.

People and process

Security operations can be highly technical, but more importantly, it's a human discipline. People are the most valuable asset in security operations. Their experience, skill, insight, creativity, and resourcefulness are what make the discipline effective.

Attacks on your organization are also planned and conducted by people like criminals, spies, and hacktivists. While some commodity attacks are fully automated, the most damaging ones are often done by live human attack operators.

- **Focus on empowering people**: your goal shouldn't be to replace people with automation. Empower your people with tools that simplify their daily workflows. These tools enable them to keep up with or get ahead of the human adversaries they face.
  Rapidly sorting out signal (real detections) from the noise (false positives) requires investing in both humans and automation. Automation and technology can reduce human work, but attackers are human and human judgment is critical in defeating them.
- **Diversify your thinking portfolio**: security operations can be highly technical, but it's also just another new version of forensic investigation that shows up in many career fields like criminal justice. Don't be afraid to hire people with a strong competency in investigation or deductive or inductive reasons and train them on technology.

Metrics

Metrics drive behavior, so measuring success is a critical element to get right. Metrics translate culture into clear measurable goals that drive outcomes.

We've learned that it's critical to consider what you measure, and the ways that you focus on and enforce those metrics. Recognize that security operations must manage significant variables that are out of their direct control, like attacks and attackers. Any deviations from targets should be viewed primarily as a learning opportunity for process or tool improvement, rather than assumed to be a failure by the SOC to meet a goal.

The main metrics to focus on that have a direct influence on organizational risk are:

- **Mean time to acknowledge (MTTA)**: Responsiveness is one of the few elements SecOps has more direct control over. Measure the time between an alert, like when the light starts to blink, and when an analyst sees that alert and begins the investigation. Improving this responsiveness requires that analysts don't waste time investigating false positives. It can be achieved with ruthless prioritization, ensuring that any alert feed that requires an analyst response must have a track record of 90 percent true positive detections.
- **Mean time to remediate (MTTR)**: Effectiveness of reducing risk measures the next period of time. That period is the time the analyst begins the investigation to when the incident is remediated. MTTR identifies how long it takes SecOps to remove the attacker's access from the environment. This information helps identify where to invest in processes and tools to help analysts reduce risk.
- **Incidents remediated (manually or with automation)**: Measuring how many incidents are remediated manually and how many are resolved with automation is another key way to inform staffing and tool decisions.
- **Escalations between each tier**: Track how many incidents escalated between tiers. It helps ensure accurate tracking of the workload to inform staffing and other decisions. For example, so that work done on escalated incidents isn't attributed to the wrong team.

Understand deep forensics procedures by resource type

Digital forensics is a science that addresses the recovery and investigation of digital data to support criminal investigations or civil proceedings. Computer forensics is a branch of digital forensics that captures and analyzes data from computers, virtual machines (VMs), and digital storage media.

Companies must guarantee that digital evidence they provide in response to legal requests demonstrates a valid Chain of Custody (CoC) throughout the evidence acquisition, preservation, and access process. To ensure a valid CoC, digital evidence storage must demonstrate adequate access control, data protection and integrity, monitoring and alerting, and logging and auditing. The main use cases are:

- A company's Security Operation Center (SOC) team can implement this technical solution to support a valid CoC for digital evidence
- Investigators can attach disk copies obtained with this technique on a computer dedicated to forensic analysis, without re-creating, powering on, or accessing the original source VM

Only two individuals within the SOC team should have rights to modify the controls governing access to the subscription and its data. Grant other individuals only bare minimum access to data subsets they need to perform their work. Configure and enforce access through Azure role-based access control (Azure RBAC). Only the virtual network in the SOC subscription has access to the Storage account. Azure Audit Logs can show evidence acquisition by recording the action of taking a VM disk snapshot, with elements like who took the snapshot, how, and where.

Endpoint forensics

Microsoft Defender for Endpoint provides detailed device information, including forensics information. You are a Security Operations Analyst working at a company that has implemented Microsoft Defender for Endpoint, and your primary job is to remediate incidents.

Live response gives security operations teams instantaneous access to a device (also referred to as a machine) using a remote shell connection. This forensics information gives you the power to do in-depth investigative work and take immediate response actions to promptly contain identified threats in real time. Live response is designed to enhance investigations by enabling your security operations team to collect forensic data, run scripts, send suspicious entities for analysis, remediate threats, and proactively hunt for emerging threats.

Watch the video below for a demonstration on live response feature.

[!VIDEO https://www.microsoft.com/videoplayer/embed/RE4qLUW]

With live response, analysts can do all of the following tasks:

- Run basic and advanced commands to do investigative work on a device.
- Download files such as malware samples and outcomes of PowerShell scripts.
- Download files in the background (new!).
- Upload a PowerShell script or executable to the library and run it on a device from a tenant level.
- Take or undo remediation actions.

Depending on the role that's been granted to you, you can run basic or advanced live response commands. User permissions are controlled by RBAC custom roles. Live response is a cloud-based interactive shell. Specific command experience may vary in response time depending on network quality and system load between the end user and the target device.

As part of the investigation or response process, you can collect an investigation package from a device. By collecting the investigation package, you can identify the current state of the device and further understand the tools and techniques used by the attacker. This data collection includes the following artifacts:

- Autoruns
- Installed programs

- Network connections
- Windows Prefetch files
- Processes
- Scheduled tasks
- Security event log
- List of services
- Windows Server Message Block (SMB) sessions
- System information
- Temp directories
- User and groups

Exercise

Tailwind Traders is a modern commerce company. For more than 30 years, the company has been a popular retail destination. It has grown to more than 50 physical stores. Several years ago, its chief executive officer (CEO) anticipated changes in retail and bought a competing e-commerce start-up that was growing aggressively in niche markets. Today, the company is seen as an innovative leader with customer-focused local storefronts.

The retail innovation team reports to the company's chief technology officer (CTO), who was the CEO of the acquired e-commerce start-up. Those technology solutions are the main hub for interactions with customers. Those solutions affect 60 percent of global revenue and produce 30 percent of annual gross sales.

The new CIO is focused on improving technical operations in multiple areas to fuel greater innovation throughout the company while limiting disruptions to core business operations. The cloud will play an important role in this transition. One of the key requirements for this transformation is to empower remote workers in a secure manner. The new CIO wants to ensure remote workers can connect to cloud resources without having to expose management ports on their cloud workloads and that remote branch offices can stay always connected with company's headquarter.

The CISO understands that in the current threat landscape, most of the attacks are targeting the end-points. He needs to establish a new security baseline to harden all endpoints and provide a seamless experience to deploy these baselines across the clients. The CISO also wants to empower the SOC Team to perform investigations on the endpoints to better understand the root cause of an attack.

Questions

1. **Remote access**:

    - Which solution should you use to enable the CIO vision regarding the connectivity for remote workers?
    - Which solution should you use for the remote branches?

2. **Endpoint strategy**:

   - Which tool should you use to deploy the security baseline?
   - How can you enable the SOC Team to perform investigation of the endpoints?

Summary

In this module you learned how to specify security baseline for clients' endpoints based on the different options that are available. You learned that the selection of the appropriate security baseline starts with the understanding of which operating system the security baseline needs to be applied to. You learned how to define the security requirements for servers and the importance of understanding the server's role as the server's role will dictate the hardening settings that should be applied.

You learned how to specify security requirements for mobile devices and clients. The considerations regarding application isolation and operating system hardening. In addition, you learned more how to specify requirements for securing Active Directory Domain Services, and how to design a strategy to manage secrets, keys, and certificates.

In addition, you learned the options available for remote access and the security operations frameworks, processes, and procedures. Lastly, you learned about some capabilities available in Windows 10/11 that can help you during forensics investigation.

Visit the links below for more information about the topics covered in this module:

- **Working remotely using Azure networking services**[22]
- **Azure Bastion**[23]
- **Best Practices for Securing Active Directory**[24]
- **Azure Key Vault security overview**[25]
- **Security Operations Center (SOC or SecOps) monitoring in Azure - Microsoft Azure Well-Architected Framework**[26]
- **Security operations - Cloud Adoption Framework**[27]
- **Investigate entities on devices using live response in Microsoft Defender for Endpoint**[28]
- **Computer forensics chain of custody in Azure - Azure Example Scenarios**[29]

22 https://docs.microsoft.com/azure/networking/working-remotely-support
23 https://docs.microsoft.com/azure/bastion/bastion-overview
24 https://docs.microsoft.com/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-for-securing-active-directory
25 https://docs.microsoft.com/azure/key-vault/general/security-features
26 https://docs.microsoft.com/azure/architecture/framework/security/monitor-security-operations
27 https://docs.microsoft.com/azure/cloud-adoption-framework/secure/security-operations
28 https://docs.microsoft.com/microsoft-365/security/defender-endpoint/live-response
29 https://docs.microsoft.com/azure/architecture/example-scenario/forensics/

Design a strategy for securing PaaS, IaaS, and SaaS services

Introduction

When designing the security strategy for your cloud workloads, you need to take into considerations that different cloud services will have different security requirements. In this module you'll learn how to design a strategy for security PaaS, IaaS and SaaS services.

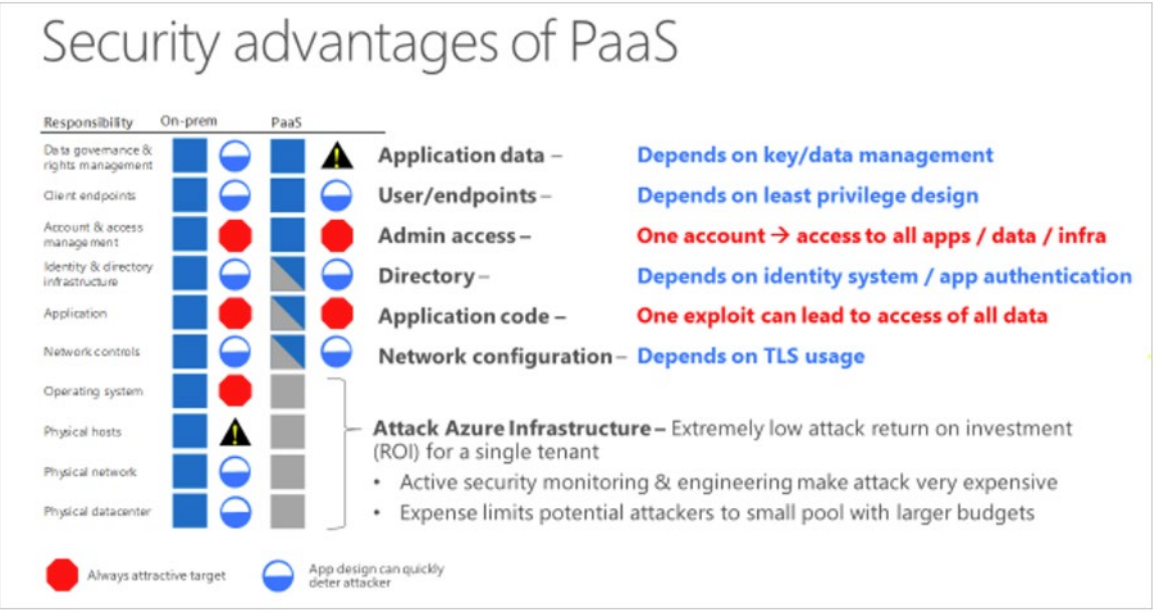
Learning Objectives

In this module, you'll learn how to:

- Specify security baselines for PaaS services
- Specify security baselines for IaaS services
- Specify security baselines for SaaS services
- Specify security requirements for IoT workloads
- Specify security requirements for data workloads
- Specify security requirements for web workloads
- Specify security requirements for storage workloads
- Specify security requirements for containers
- Specify security requirements for container orchestration

Specify security baselines for PaaS services

Let's look at the security advantages of an Azure PaaS deployment versus on-premises.



Microsoft mitigates common risks and responsibilities starting at the bottom of the stack: the physical infrastructure. Because the Microsoft cloud is continually monitored by Microsoft, it's hard to attack. It doesn't make sense for an attacker to pursue the Microsoft cloud as a target. Unless the attacker has lots of money and resources, the attacker is likely to move on to another target.

In the middle of the stack, there's no difference between a PaaS deployment and on-premises. At the application layer and the account and access management layer, you have similar risks. In the next steps section of this article, we will guide you to best practices for eliminating or minimizing these risks.

At the top of the stack, data governance and rights management, you take on one risk that can be mitigated by key management. (Key management is covered in best practices.) While key management is an additional responsibility, you have areas in a PaaS deployment that you no longer have to manage so you can shift resources to key management.

The Azure platform also provides you strong DDoS protection by using various network-based technologies. However, all types of network-based DDoS protection methods have their limits on a per-link and per-datacenter basis. To help avoid the impact of large DDoS attacks, you can take advantage of Azure's core cloud capability of enabling you to quickly and automatically scale out to defend against DDoS attacks.

With PaaS deployments come a shift in your overall approach to security. You shift from needing to control everything yourself to sharing responsibility with Microsoft. Another significant difference between PaaS and traditional on-premises deployments is a new view of what defines the primary security perimeter. Historically, the primary on-premises security perimeter was your network, and most on-premises security designs use the network as its primary security pivot. For PaaS deployments, you're better served by considering identity to be the primary security perimeter.

Microsoft Defender for Cloud has security recommendations that are based on Azure Security Benchmark for all supported PaaS services. The list of supported PaaS services can be found below:

Service	Recommendations (Free)	Security alerts	Vulnerability assessment
Azure App Service	X	X	-
Azure Automation account	X	-	-
Azure Batch account	X	-	-
Azure Blob Storage	X	X	-
Azure Cache for Redis	X	-	-
Azure Cloud Services	X	-	-
Azure Cognitive Search	X	-	-
Azure Container Registry	X	X	X
Azure Cosmos DB	X	X	-

Service	Recommendations (Free)	Security alerts	Vulnerability assessment
Azure Data Lake Analytics	X	-	-
Azure Data Lake Storage	X	X	-
Azure Database for MySQL	-	X	-
Azure Database for PostgreSQL	-	X	-
Azure Event Hubs namespace	X	-	-
Azure Functions app	X	-	-
Azure Key Vault	X	X	-
Azure Kubernetes Service	X	X	-
Azure Load Balancer	X	-	-
Azure Logic Apps	X	-	-
Azure SQL Database	X	X	X
Azure SQL Managed Instance	X	X	X
Azure Service Bus namespace	X	-	-
Azure Service Fabric account	X	-	-
Azure Storage accounts	X	X	-
Azure Stream Analytics	X	-	-
Azure Subscription	X	X	-
Azure Virtual Network	X	-	-
(incl. subnets, NICs, and network security groups)			

The recommendations column represents the security recommendations that are coming from Azure Security Benchmark and are part of the Defender for Cloud free tier. The security alerts column represents the alerts that are coming from each individual threat detection plan. The vulnerability assessment column represents the services that have this capability available.

Security baseline for PaaS

Security baselines for Azure PaaS help you strengthen security through improved tooling, tracking, and security features. They also provide you with consistent experience when securing your environment. Security baselines for Azure focus on cloud-centric control areas. These controls are consistent with well-known security benchmarks, such as those described by the Center for Internet Security (CIS). These baselines provide guidance for the control areas listed in the Azure Security Benchmark.

Each recommendation includes the following information:

- **Azure ID**: The Azure Security Benchmark ID that corresponds to the recommendation.
- **Recommendation**: Following directly after the Azure ID, the recommendation provides a high-level description of the control.
- **Guidance**: The rationale for the recommendation and links to guidance on how to implement it. If the recommendation is supported by Microsoft Defender for Cloud, that information will also be listed.
- **Responsibility**: Who is responsible for implementing the control. Possible scenarios are customer responsibility, Microsoft responsibility, or shared responsibility.
- **Microsoft Defender for Cloud monitoring**: Whether the control is monitored by Microsoft Defender for Cloud, with link to reference.

All recommendations, including recommendations that are not applicable to this specific service, are included in the baseline to provide you a complete picture of how the Azure Security Benchmark relates to each service. There may occasionally be controls that are not applicable for various reasons—for example, IaaS/compute-centric controls (such as controls specific to OS configuration management) may not be applicable to PaaS services.

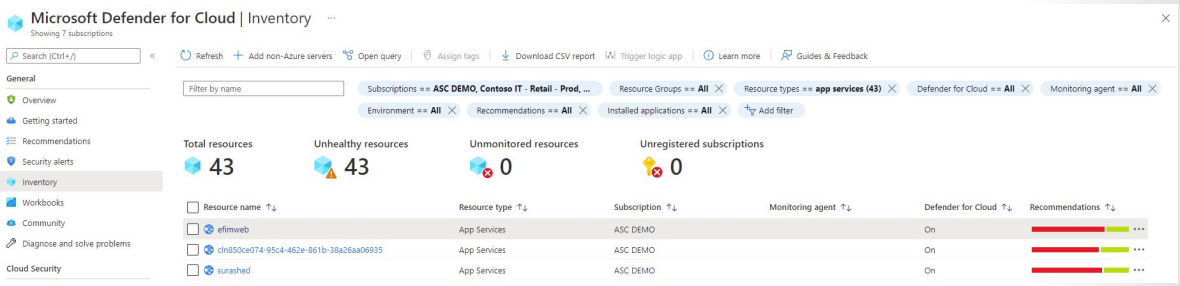
The PaaS baseline will vary according to the service, so it's important for you to familiarize yourself with the PaaS service that you want to protect, and then apply the appropriate baseline. For example, for App Service, the security baseline establishes security recommendations in the following areas:

- Network security
- Logging and Monitoring
- Identity and Access Control
- Data Protection
- Vulnerability Management
- Inventory and Asset Management
- Secure Configuration
- Data Recovery
- Incident Response

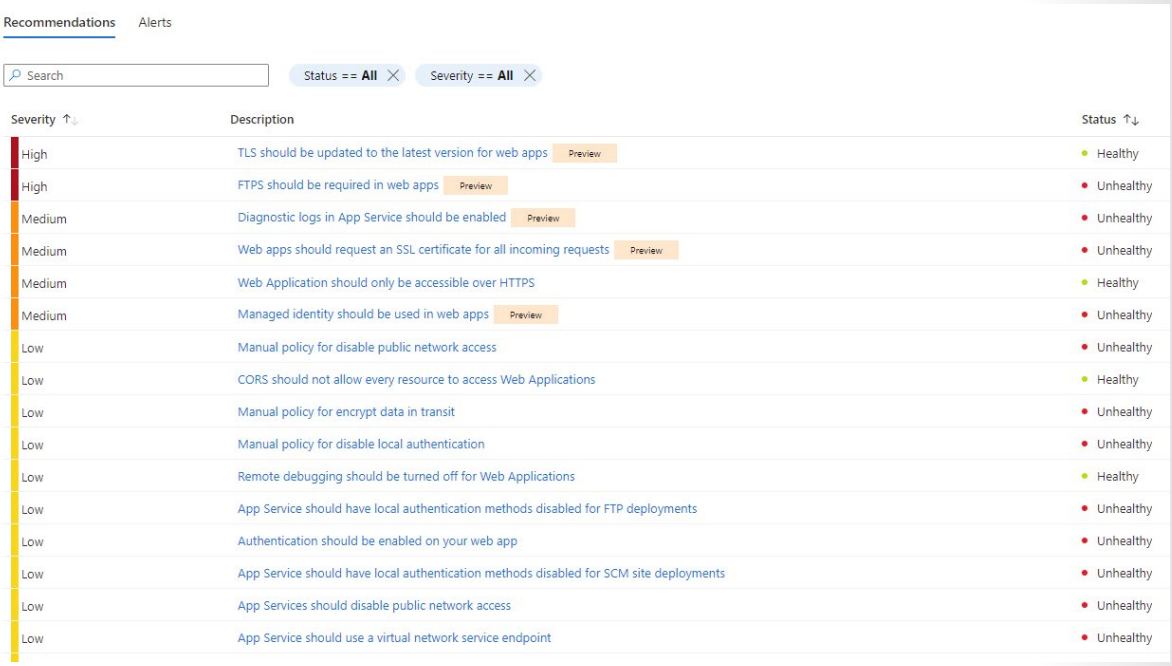
For more information about App Service security baseline, visit **Azure security baseline for App Service**[30].

One strategy to The Inventory dashboard in Defender for Cloud allows you to identify all your PaaS resources and verify the open issues. You can create a filter by resource type and see only the PaaS resources that you want to evaluate. The example below shows only the resource type that is equal to App Service.

30 https://docs.microsoft.com/security/benchmark/azure/baselines/app-service-security-baseline



Once you identify the resource, you can click on it and see the open security recommendations as shown below:



This list provides the list of recommendations, which are derived from Azure Security Benchmark, organized by priority and showing the current status (healthy or unhealthy).

Specify security baselines for IaaS services

In most infrastructure as a service (IaaS) scenarios, Azure virtual machines (VMs) are the main workload for organizations that use cloud computing. This fact is evident in hybrid scenarios where organizations want to slowly migrate workloads to the cloud. In such scenarios, follow the general security considerations for IaaS, and apply security best practices to all your VMs.

The first step in protecting your VMs is to ensure that only authorized users can set up new VMs and access VMs. To improve the security of Linux VMs on Azure, you can integrate with Azure AD authentication. When

you use Azure AD authentication for Linux VMs, you centrally control and enforce policies that allow or deny access to the VMs.

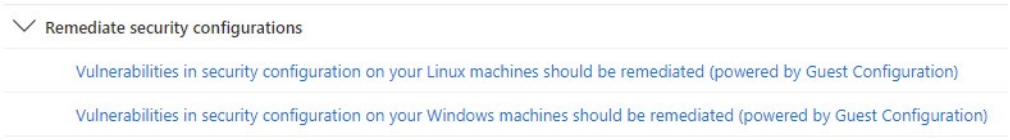
Security baseline for IaaS VMs

Security baselines for IaaS VMs are available for
Windows[31]
and
Linux[32].
While each operating system will have its own security settings, there are some general guidelines that you can ensure are in place regardless of the operating system, such as:

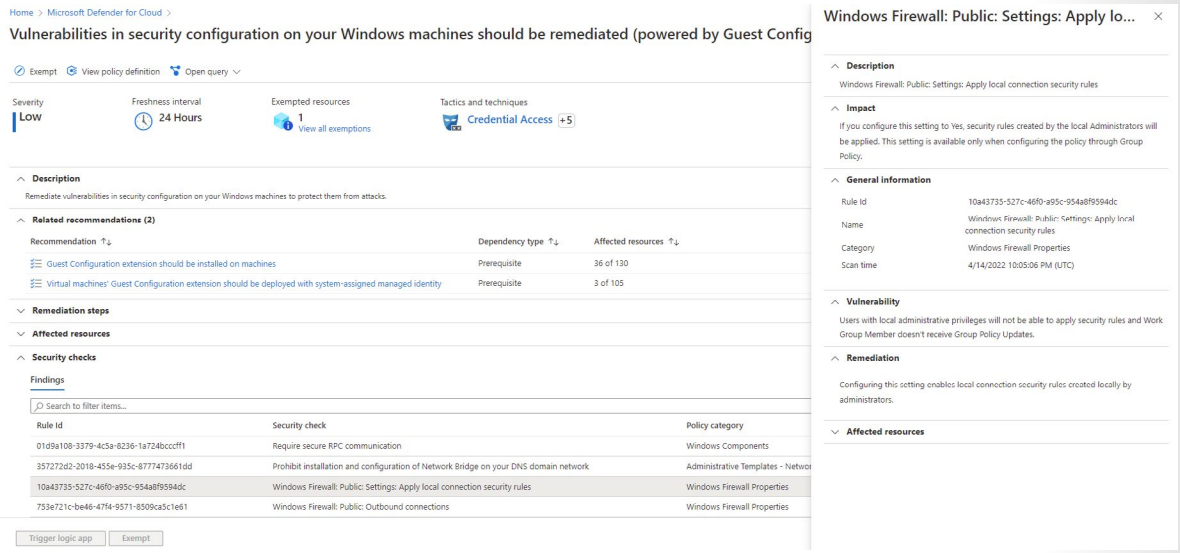
- **Protect your virtual machines from viruses and malware:** if you are using Windows, you can use the Microsoft Antimalware for Azure, which is a single-agent solution for applications and tenant environments. It's designed to run in the background without human intervention. You can deploy protection based on the needs of your application workloads, with either basic secure-by-default or advanced custom configuration, including antimalware monitoring. For Linux you can use Microsoft Defender for Endpoint (MDE) for Linux.
- **Encrypt your sensitive data:** you can use Azure Disk Encryption for encrypting your Windows and Linux virtual machine disks. Azure Disk Encryption uses the industry-standard BitLocker feature of Windows and the dm-crypt feature of Linux to provide volume encryption for the OS and the data disks. The solution is integrated with Azure Key Vault to help you control and manage the disk encryption keys and secrets in your key vault subscription. It ensures that all data in the virtual machine disks are encrypted at rest in Azure Storage.
- **Secure network traffic:** use Azure virtual network to control traffic. An Azure virtual network is a logical construct built on top of the physical Azure network fabric. Each logical Azure virtual network is isolated from all other Azure virtual networks. This isolation helps ensure that network traffic in your deployments is not accessible to other Microsoft Azure customers.
- **Identify and detect threats:** you can use Microsoft Defender for Servers threat detection which is available for Windows and Linux. This plan offers threat detection and it integrates with MDE (for Windows and Linux).

Security baselines for VMs are accessible via Defender for Cloud recommendations. Each operating system has its own recommendation as shown below:

31 https://docs.microsoft.com/azure/governance/policy/samples/guest-configuration-baseline-windows
32 https://docs.microsoft.com/azure/governance/policy/samples/guest-configuration-baseline-linux



As you open each recommendation, you'll see the security checks that were performed, and when you select a security check, you'll see more details about the impact, the vulnerability and remediation as shown below:



Specify security baselines for SaaS services

With Software as a Service (SaaS) solutions, the security options that you can control may be only at the application level. In a Public Cloud scenario, this requires a high degree of trust in the cloud vendor because they have complete control of the infrastructure and platform layers. As well as their reputation and track record, you should assess the processes they have in place to provide security. When performing due diligence, you should also assess whether they can provide network security in addition to application and data security.

Just like Microsoft Defender for Cloud has its Secure Score to assist you improving the security posture of Azure workloads, Microsoft 365 has the Microsoft Secure Score that helps with the security posture of your SaaS environment. Following the Secure Score recommendations can protect your organization from threats. From a centralized dashboard in the Microsoft 365 Defender portal, organizations can monitor and work on the security of their Microsoft 365 identities, apps, and devices. Secure Score helps organizations to:

- Report on the current state of the organization's security posture.
- Improve their security posture by providing discoverability, visibility, guidance, and control.

- Compare with benchmarks and establish key performance indicators (KPIs).

The recommendations won't cover all the attack surfaces associated with each product, but they're a good baseline. You can also mark the improvement actions as covered by a third party or alternate mitigation. Currently there are recommendations for the following products:

- Microsoft 365 (including Exchange Online)
- Azure Active Directory
- Microsoft Defender for Endpoint
- Microsoft Defender for Identity
- Defender for Cloud Apps
- Microsoft Teams

Watch this video for a quick overview of Secure score.

[!VIDEO https://www.microsoft.com/videoplayer/embed/RWUPrP]

Security baseline for SaaS

The Office cloud policy service lets you enforce policy settings for Microsoft 365 Apps for enterprise on a user's device, even if the device isn't domain joined or otherwise managed. When a user signs into Microsoft 365 Apps for enterprise on a device, the policy settings roam to that device. Policy settings are available for devices running Windows, macOS, iOS, and Android, although not all policy settings are available for all operating systems.

When you create policy configurations, you can review and apply policies that are recommended by Microsoft as security baseline policies. These recommendations are marked as “Security Baseline” when selecting policies. If the policy is recommended as a Security Baseline you'll see the policy tagged as such in this column. You can also use the column filter to limit the view to only policies that are tagged as *Security Baseline*.

Policy	Platform	Application	Recommendation
Disable Smart Document's use of manifests	Windows	Office	Security Baseline
Disable all Trust Bar notifications for security issues	Windows	Office	Security Baseline
Turn off Protected View for attachments opened fro...	Windows	Excel	Security Baseline
Turn off file validation	Windows	Excel	Security Baseline
Load pictures from Web pages not created in Excel	Windows	Excel	Security Baseline

Specify security requirements for IoT workloads

The Internet of Things (IoT) supports billions of connected devices that use operational technology (OT) networks. IoT/OT devices and networks are often designed without security in priority, and therefore can't be protected by traditional systems. With each new wave of innovation, the risk to IoT devices and OT networks increases the possible attack surfaces.

Securing an Internet of Things (IoT) infrastructure requires a rigorous security-in-depth strategy. This strategy requires you to secure data in the cloud, protect data integrity while in transit over the public internet, and securely provision devices. Each layer builds greater security assurance in the overall infrastructure.

This security-in-depth strategy can be developed and executed with active participation of various players involved with the manufacturing, development, and deployment of IoT devices and infrastructure. Here is a high-level description of these roles and security requirements:

Role	Role Description	Security Requirements
IoT hardware manufacturer/ integrator	Typically, these players are the manufacturers of IoT hardware being deployed, integrators assembling hardware from various manufacturers, or suppliers providing hardware for an IoT deployment manufac-tured or integrated by other suppliers.	Scope hardware to minimum requirements:
		Make hardware tamper proof
		Make hardware tamper proof
		Make upgrades secure
IoT solution developer	The development of an IoT solution is typically done by a solution developer. This devel-oper may part of an in-house team or a system integrator (SI) specializing in this activity. The IoT solution developer can develop various components of the IoT solution from scratch or integrate various off-the-shelf or open-source components.	Follow secure software develop-ment methodology
		Choose open-source software with care
		Integrate to avoid security flows

Role	Role Description	Security Requirements
IoT solution deployer	After an IoT solution is developed, it needs to be deployed in the field. This process involves deployment of hardware, interconnection of devices, and deployment of solutions in hardware devices or the cloud.	Deploy hardware securely
		Keep authentication keys safe
IoT solution operator	After the IoT solution is deployed, it requires long-term operations, monitoring, upgrades, and maintenance. These tasks can be done by an in-house team that comprises information technology specialists, hardware operations and maintenance teams, and domain specialists who monitor the correct behavior of overall IoT infrastructure.	Keep the system up-to-date
		Protect against malicious activity
		Audit frequently
		Audit frequently
		Protect cloud credentials

Connected special-purpose devices have a significant number of potential interaction surface areas and interaction patterns, all of which must be considered to provide a framework for securing digital access to those devices. The term “digital access” is used here to distinguish from any operations that are carried out through direct device interaction where access security is provided through physical access control. For example, putting the device into a room with a lock on the door. While physical access can't be denied using software and hardware, measures can be taken to prevent physical access from leading to system interference.

As you explore the interaction patterns, look at “device control” and "device data" with the same level of attention. “Device control” can be classified as any information that is provided to a device by any party with the goal of changing or influencing its behavior towards its state or the state of its environment. "Device data" can be classified as any information that a device emits to any other party about its state and the observed state of its environment.

In order to optimize security best practices, it's recommended that a typical IoT architecture is divided into several component/zones as part of the threat modeling exercise. These zones are:

- Device
- Field Gateway

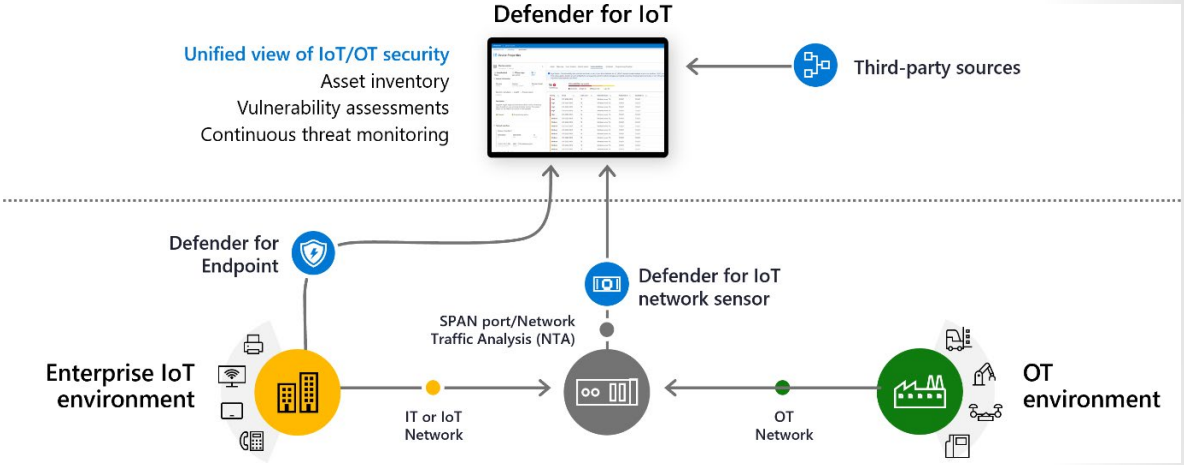
- Cloud gateways
- Services

Zones are a broad way to segment a solution; each zone often has its own data and authentication and authorization requirements. Zones can also be used to isolation damage and restrict the impact of low trust zones on higher trust zones. Each zone is separated by a Trust Boundary, and it represents a transition of data/information from one source to another. During this transition, the data/information could be subject to Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service and Elevation of Privilege (STRIDE).

Security posture management and threat detection

Just like any other cloud workload, IoT workloads need to have an ongoing security assessment to improve the overall security posture. In addition, you need threat detection in place to better understand current attack vectors and how to respond. An important part of the security requirements for IoT is to adopt a solution that can provide both: security posture management and threat detection.

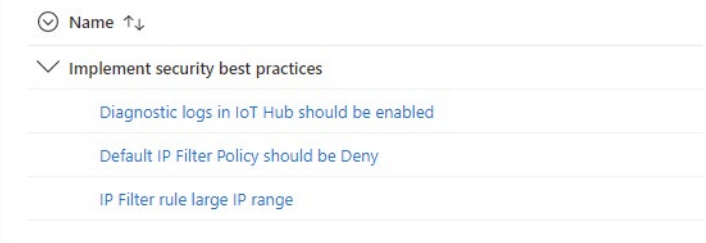
Microsoft Defender for IoT is a unified security solution for identifying IoT devices, vulnerabilities, and threats and managing them through a central interface.



Defender for IoT connects to both cloud and on-premises components and is built for scalability in large and geographically distributed environments. Defender for IoT systems includes the following components:

- The Azure portal, for cloud management and integration to other Microsoft services, such as Microsoft Sentinel
- Network sensors, deployed on either a virtual machine or a physical appliance. You can configure your OT sensors as cloud-connected sensors, or fully on-premises sensors.
- An on-premises management console for cloud-connected or local, air-gapped site management.
- An embedded security agent (optional).

Security recommendations triggered by Defender for IoT will be surfaced in Defender for Cloud dashboard, as shown in the example below:



It's also important that you can integrate the threat detection generated by your security IoT solution with your SIEM solution. Microsoft Sentinel and Microsoft Defender for IoT help to bridge the gap between IT and OT security challenges, and to empower SOC teams with out-of-the-box capabilities to detect and respond to OT threats efficiently and effectively. The integration between Microsoft Defender for IoT and Microsoft Sentinel helps organizations to quickly detect multistage attacks, which often cross IT and OT boundaries.

Specify security requirements for data workloads

Your on-premises and cloud data must be protected from both inadvertent and malicious access. *Inadvertent access* occurs when a user gains access to data that, based on their roles and responsibilities, they should not have. The result can be unintended data leakage, data destruction, or violations of data security and privacy regulations. *Malicious access* occurs when an external attacker or a malicious insider intentionally tries to access data. Malicious insiders can use your data for profit or to harm your organization. External attackers can delete, alter, exfiltrate, and encrypt your most sensitive data, leaving you open to a ransomware attack.

For both types of attacks, you must take the necessary steps to identify your data, protect it, prevent its destruction or exfiltration, and ensure that only users with a business purpose have access to it. Protecting your data is part of the “assume breach” Zero Trust principle. Even with all the user account and device protections in place, you must assume that an attacker could find their way in and begin traversing your environment, searching for the most valuable data for your organization.

Before establishing the security requirements for data workloads, you must first know your data. In other words, understand your data landscape and identify important information across your cloud and on-premises environment. During this process of better understanding your data, you can execute the following steps:

Task	Owner
1. Determine data classification levels.	Data Security Architect

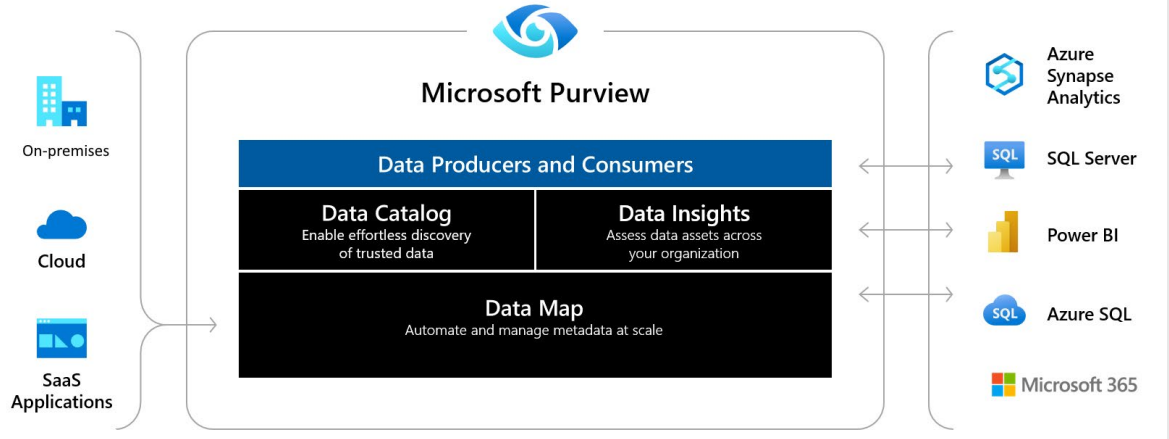
Task	Owner
2. Determine built-in and custom sensitive information types.	Data Security Architect
3. Determine the use of pre-trained and custom trainable classifiers.	Data Security Architect
4. Discover and classify sensitive data.	Data Security Architect and/or Data Security Engineer

Once you know your data, you can establish key requirements such as:

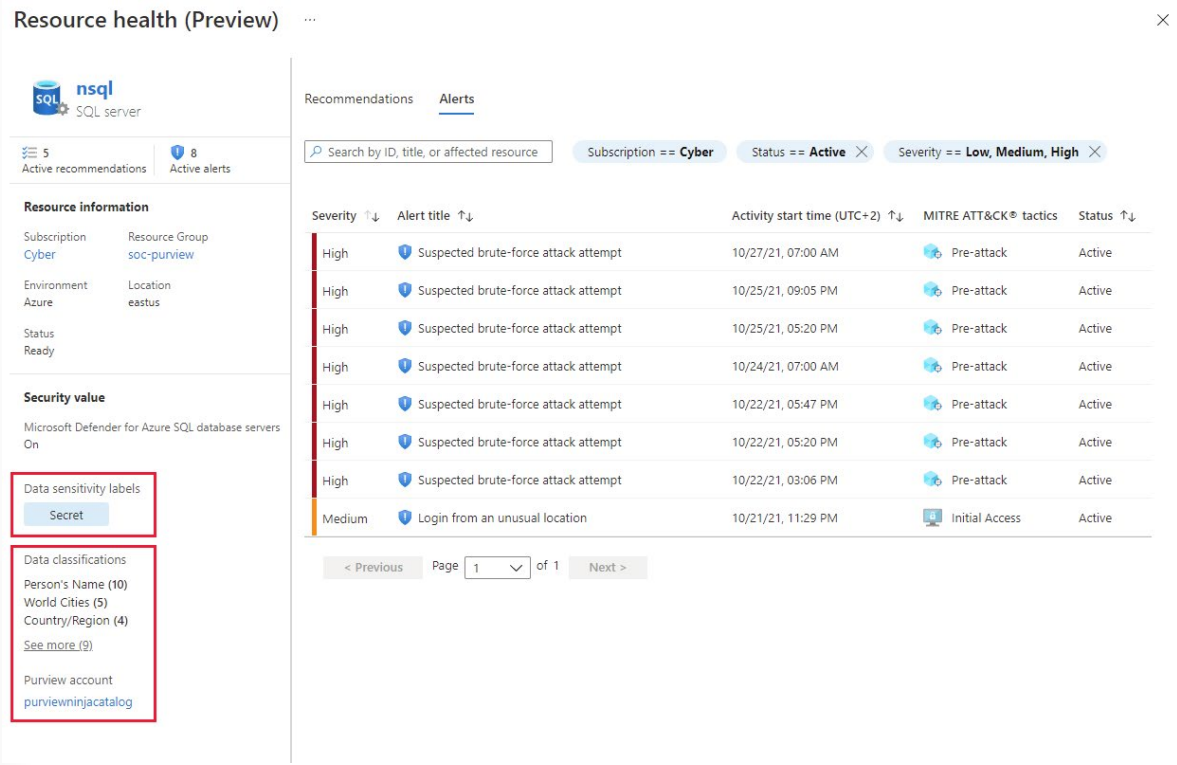
- **Data protection across all data workloads**: protect your sensitive data throughout its lifecycle by applying sensitivity labels linked to protection actions like encryption, access restrictions, visual markings, and more.
- **Prevent data loss**: apply a consistent set of data loss prevention policies across the cloud, on-premises environments, and endpoints to monitor, prevent, and remediate risky activities with sensitive data.
- **Use least privilege access**: apply minimal permissions consisting of who is allowed to access and what they're allowed to do with data to meet business and productivity requirements.

Security posture management for data

Just like any other cloud workload, data workloads need to have an ongoing security assessment to improve the overall security posture. Azure Purview is a unified data governance service that helps you manage and govern your on-premises, multi-cloud, and software-as-a-service (SaaS) data. Create a holistic, up-to-date map of your data landscape with automated data discovery, sensitive data classification, and end-to-end data lineage. Enable data curators to manage and secure your data estate. Empower data consumers to find valuable, trustworthy data.

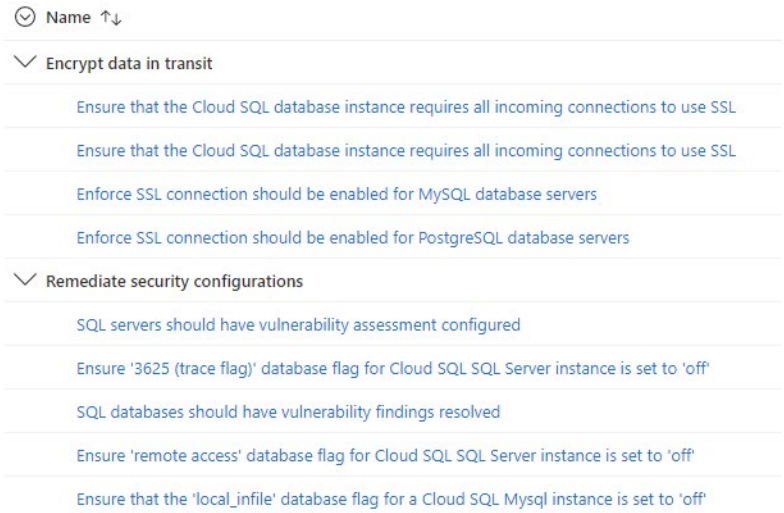


Microsoft Defender for Cloud integration with Azure Purview allows you to obtain vital layer of metadata from Azure Purview and use in alerts and recommendations: information about any potentially sensitive data involved. This knowledge helps solve the triage challenge and ensures security professionals can focus their attention on threats to sensitive data. The example below shows a SQL database status in Defender for Cloud, with the data enrichment coming from Azure Purview in the low left corner:



Databases

Data workloads include databases, and to provide security posture management for databases you can use Microsoft Defender for SQL. Microsoft Defender for Cloud is available for Azure SQL Database, Azure SQL Managed Instance, and Azure Synapse Analytics. It includes functionality for surfacing and mitigating potential database vulnerabilities and detecting anomalous activities that could indicate a threat to your database. It provides a single go-to location for enabling and managing these capabilities. Security recommendations for SQL database will be surfaced in Defender for Cloud as shown the screen below:



An advanced threat protection service continuously monitors your SQL servers for threats such as SQL injection, brute-force attacks, and privilege abuse. This service provides action-oriented security alerts in Microsoft Defender for Cloud with details of the suspicious activity, guidance on how to mitigate to the threats, and options for continuing your investigations with Microsoft Sentinel. Learn more about advanced threat protection.

In addition to SQL, you need to also take in considerations cloud-native database such as Azure Cosmos DB. Microsoft Defender for Azure Cosmos DB detects potential SQL injections, known bad actors based on Microsoft Threat Intelligence, suspicious access patterns, and potential exploitation of your database through compromised identities, or malicious insiders. Defender for Azure Cosmos DB uses advanced threat detection capabilities, and Microsoft Threat Intelligence data to provide contextual security alerts. Those alerts also include steps to mitigate the detected threats and prevent future attacks.

Specify security requirements for web workloads

When taking into consideration the security requirements for your web workloads, you need to include Azure App Service. Azure App Service is an HTTP-based service for hosting web applications, REST APIs, and mobile back ends. Applications run and scale with ease on both Windows and Linux-based environments.

The platform components of App Service, including Azure VMs, storage, network connections, web frameworks, management, and integration features, are actively secured and hardened. Security requirements for Azure App Service includes:

- **Ensure that you secure your apps with HTTPS:** When your app is created, its default domain name ({{app_name}}.azurewebsites.net) is already accessible using HTTPS. If you configure a custom domain for your app, you should also secure it with a TLS/SSL certificate so

that client browsers can make secured HTTPS connections to your custom domain.

- **Disable insecure protocols:** To secure your app against all unencrypted (HTTP) connections, App Service provides one-click configuration to enforce HTTPS. Unsecured requests are turned away before they even reach your application code. For more information, see Enforce HTTPS.
- **Create static IP restrictions:** by default, your App Service app accepts requests from all IP addresses from the internet, but you can limit that access to a small subset of IP addresses. App Service on Windows lets you define a list of IP addresses that are allowed to access your app.
- **Enable client authentication and authorization:** Azure App Service provides turn-key authentication and authorization of users or client apps. When enabled, it can sign in users and client apps with little or no application code. You may implement your own authentication and authorization solution or allow App Service to handle it for you instead.
- **Don't store application secrets:** application secrets, such as database credentials, API tokens, and private keys in your code or configuration files. The commonly accepted approach is to access them as environment variables using the standard pattern in your language of choice.
- **Implement network isolation:** the isolated tier gives you complete network isolation by running your apps inside a dedicated App Service environment. An App Service environment runs in your own instance of Azure Virtual Network.

Security posture management for App Service

Just like any other cloud workload, web workloads need to have an ongoing security assessment to improve the overall security posture. Microsoft Defender for App Service uses the scale of the cloud to identify attacks targeting applications running over App Service. Attackers probe web applications to find and exploit weaknesses. Before being routed to specific environments, requests to applications running in Azure go through several gateways, where they're inspected and logged. This data is then used to identify exploits and attackers, and to learn new patterns that will be used later.

When you enable Microsoft Defender for App Service, you immediately benefit from the following services offered by this Defender plan:

- Security assessment: Defender for App Service assesses the resources covered by your App Service plan and generates security recommendations based on its findings. Use the detailed instructions in these recommendations to harden your App Service resources.

- Threat Detection: Defender for App Service detects a multitude of threats to your App Service resources by monitoring:
  - the VM instance in which your App Service is running, and its management interface
  - the requests and responses sent to and from your App Service apps
  - the underlying sandboxes and VMs
  - App Service internal logs - available thanks to the visibility that Azure has as a cloud provider

As a cloud-native solution, Defender for App Service can identify attack methodologies applying to multiple targets. For example, from a single host it would be difficult to identify a distributed attack from a small subset of IPs, crawling to similar endpoints on multiple hosts.

Specify security requirements for storage workloads

Azure Storage Accounts are ideal for workloads that require fast and consistent response times, or that have a high number of input output (IOP) operations per second. Storage accounts contain all your Azure Storage data objects, which include:

- Blobs
- File shares
- Queues
- Tables
- Disks

Consider the following recommendations to optimize security when configuring your Azure Storage Account:

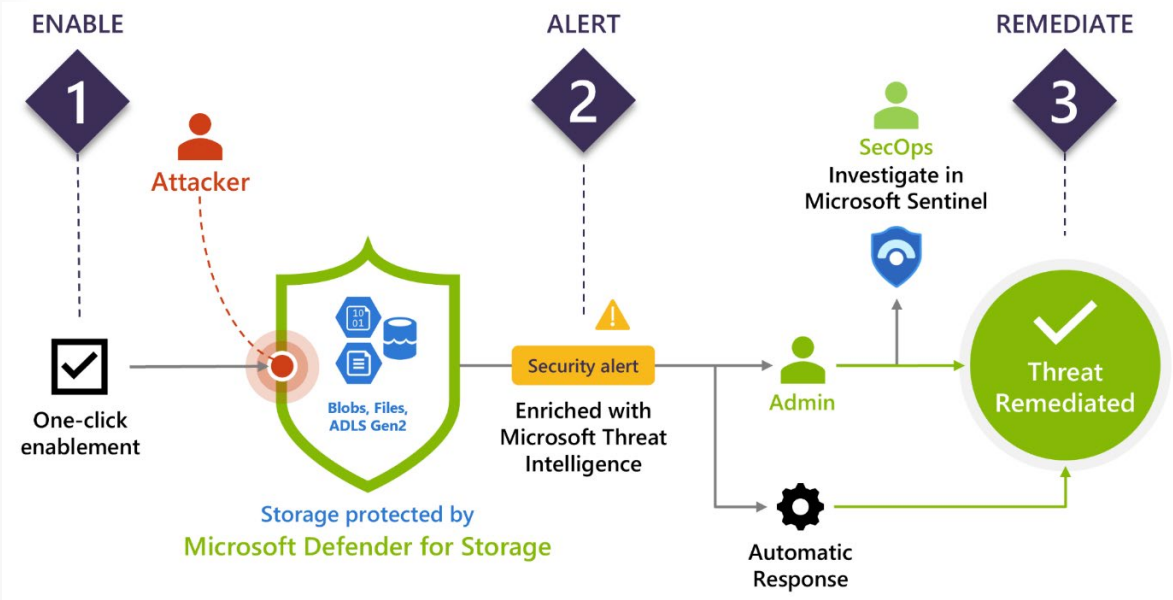
- Turn on soft delete for blob data
- Use Azure AD to authorize access to blob data.
- Consider the principle of least privilege when you assign permissions to an Azure AD security principal through Azure RBAC.
- Consider the principle of least privilege when you assign permissions to an Azure AD security principal through Azure RBAC.
- Use blob versioning or immutable blobs to store business-critical data.
- Restrict default internet access for storage accounts.
- Configure firewall rules to limit access to your storage account
- Limit network access to specific networks.
- Allow trusted Microsoft services to access the storage account.

- Enable the Secure transfer required option on all your storage accounts.
- Limit shared access signature (SAS) tokens to HTTPS connections only.
- Avoid and prevent using Shared Key authorization to access storage accounts.
- Regenerate your account keys periodically.
- Create a revocation plan and have it in place for any SAS that you issue to clients.

Security posture management for storage

Just like any other cloud workload, web workloads need to have an ongoing security assessment to improve the overall security posture. Microsoft Defender for Storage is an Azure-native layer of security intelligence that detects unusual and potentially harmful attempts to access or exploit your storage accounts. It uses advanced threat detection capabilities and Microsoft Threat Intelligence data to provide contextual security alerts. Those alerts also include steps to mitigate the detected threats and prevent future attacks.

You can enable Microsoft Defender for Storage at either the subscription level (recommended) or the resource level. Defender for Storage continually analyzes the telemetry stream generated by the Azure Blob Storage and Azure Files services. When potentially malicious activities are detected, security alerts are generated. These alerts are displayed in Microsoft Defender for Cloud together with the details of the suspicious activity along with the relevant investigation steps, remediation actions, and security recommendations. The diagram below shows the three major actions performed by Defender for Storage:



1. One-click enablement via Defender for Cloud dashboard

2. Once enabled, Defender for cloud will be monitoring the storage account, generating security recommendations and in case of a suspicious activity, it will trigger an alert
3. The alert can be handled in the Defender for Cloud dashboard, or if the company is using Microsoft Sentinel, they can perform the investigation there.

Specify security requirements for containers

A container is an isolated, lightweight silo for running an application on the host operating system. Containers build on top of the host operating system's kernel (which can be thought of as the buried plumbing of the operating system), and contain only apps and some lightweight operating system APIs and services that run in user mode. While a container shares the host operating system's kernel, the container doesn't get unfettered access to it. Instead, the container gets an isolated–and in some cases virtualized–view of the system. For example, a container can access a virtualized version of the file system and registry, but any changes affect only the container and are discarded when it stops. To save data, the container can mount persistent storage such as an Azure Disk or a file share (including Azure Files).

Containers are built from images that are stored in one or more repositories. These repositories can belong to a public registry, like Docker Hub, or to a private registry. An example of a private registry is the Docker Trusted Registry, which can be installed on-premises or in a virtual private cloud. You can also use cloud-based private container registry services, including Azure Container Registry.

A publicly available container image does not guarantee security. Container images consist of multiple software layers, and each software layer might have vulnerabilities. To help reduce the threat of attacks, you should store and retrieve images from a private registry, such as Azure Container Registry or Docker Trusted Registry. In addition to providing a managed private registry, Azure Container Registry supports service principal-based authentication through Azure Active Directory for basic authentication flows. This authentication includes role-based access for read-only (pull), write (push), and other permissions.

Take advantage of solutions to scan container images in a private registry and identify potential vulnerabilities. It's important to understand the depth of threat detection that the different solutions provide. For example, Azure Container Registry optionally integrates with Microsoft Defender for Cloud to automatically scan all Linux images pushed to a registry. Microsoft Defender for Cloud integrated Qualys scanner detects image vulnerabilities, classifies them, and provides remediation guidance.

Containers can spread across several clusters and Azure regions. So, you must secure credentials required for logins or API access, such as passwords or tokens. Ensure that only privileged users can access those containers in transit and at rest. Inventory all credential secrets, and

then require developers to use emerging secrets-management tools that are designed for container platforms. Make sure that your solution includes encrypted databases, TLS encryption for secrets data in transit, and least-privilege role-based access control. Azure Key Vault is a cloud service that safeguards encryption keys and secrets (such as certificates, connection strings, and passwords) for containerized applications. Because this data is sensitive and business critical, secure access to your key vaults so that only authorized applications and users can access them.

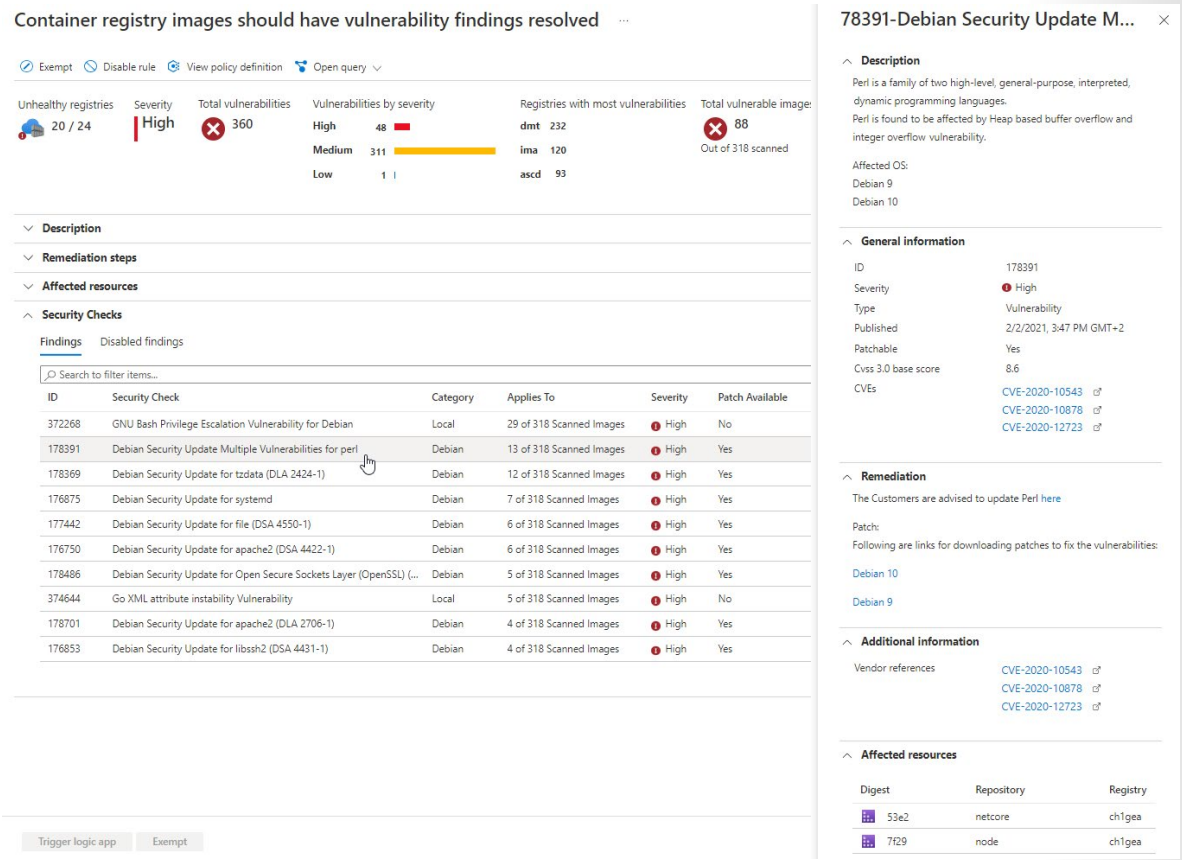
There's enough change and volatility in a container ecosystem without allowing unknown containers as well. Allow only approved container images. Have tools and processes in place to monitor for and prevent the use of unapproved container images. An effective way of reducing the attack surface and preventing developers from making critical security mistakes is to control the flow of container images into your development environment. For example, you might sanction a single Linux distribution as a base image, preferably one that is lean (Alpine or CoreOS rather than Ubuntu), to minimize the surface for potential attacks.

Security posture management for containers

Just like any other cloud workload, web workloads need to have an ongoing security assessment to improve the overall security posture. Defender for Containers helps with the core aspects of container security, including:

- **Environment hardening:** Defender for Containers protects your Kubernetes clusters whether they're running on Azure Kubernetes Service, Kubernetes on-premises / IaaS, or Amazon EKS. By continuously assessing clusters, Defender for Containers provides visibility into misconfigurations and guidelines to help mitigate identified threats. Learn more in Hardening.
- **Vulnerability assessment:** Vulnerability assessment and management tools for images stored in ACR registries and running in Azure Kubernetes Service. Learn more in Vulnerability assessment.
- **Run-time threat protection for nodes and clusters:** Threat protection for clusters and Linux nodes generates security alerts for suspicious activities. Learn more in Run-time protection for Kubernetes nodes, clusters, and hosts.

Defender for Cloud continuously assesses the configurations of your clusters and compares them with the initiatives applied to your subscriptions. When it finds misconfigurations, Defender for Cloud generates security recommendations. Use Defender for Cloud's recommendations page to view recommendations and remediate issues, as you can see the example below:



Specify security requirements for container orchestration

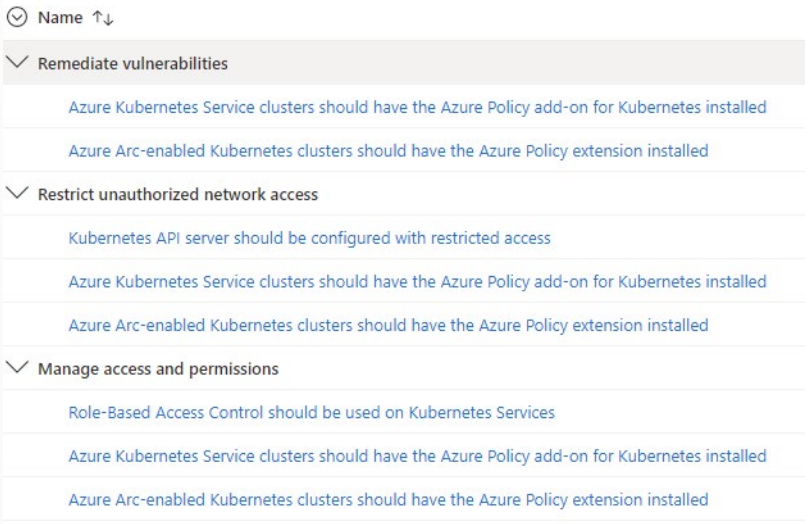
The application that manages the containers is called a container orchestrator. The process of orchestration typically involves tooling that can automate all aspects of application management from initial placement, scheduling, and deployment to steady-state activities, such as deployment, update, and health monitoring functions that support scaling and failover.

Kubernetes, the most popular container orchestration system and one of the fastest-growing projects in the history of open source, has become a significant part of many companies' compute stack. The Azure platform has three services that make it easy to deploy and manage Kubernetes clusters. The services are Azure Kubernetes managed Service (AKS), Azure Container Service Engine (ACS-engine), and Azure Container Instance. Kubernetes is a popular solution and has a strong developer community. The application has been proven at scale and is evolving constantly. It is the only orchestrator that has cloud-provider concept natively, which allows seamless integration into public clouds, such as Microsoft Azure, Amazon Web Services, and Google Cloud Platform.

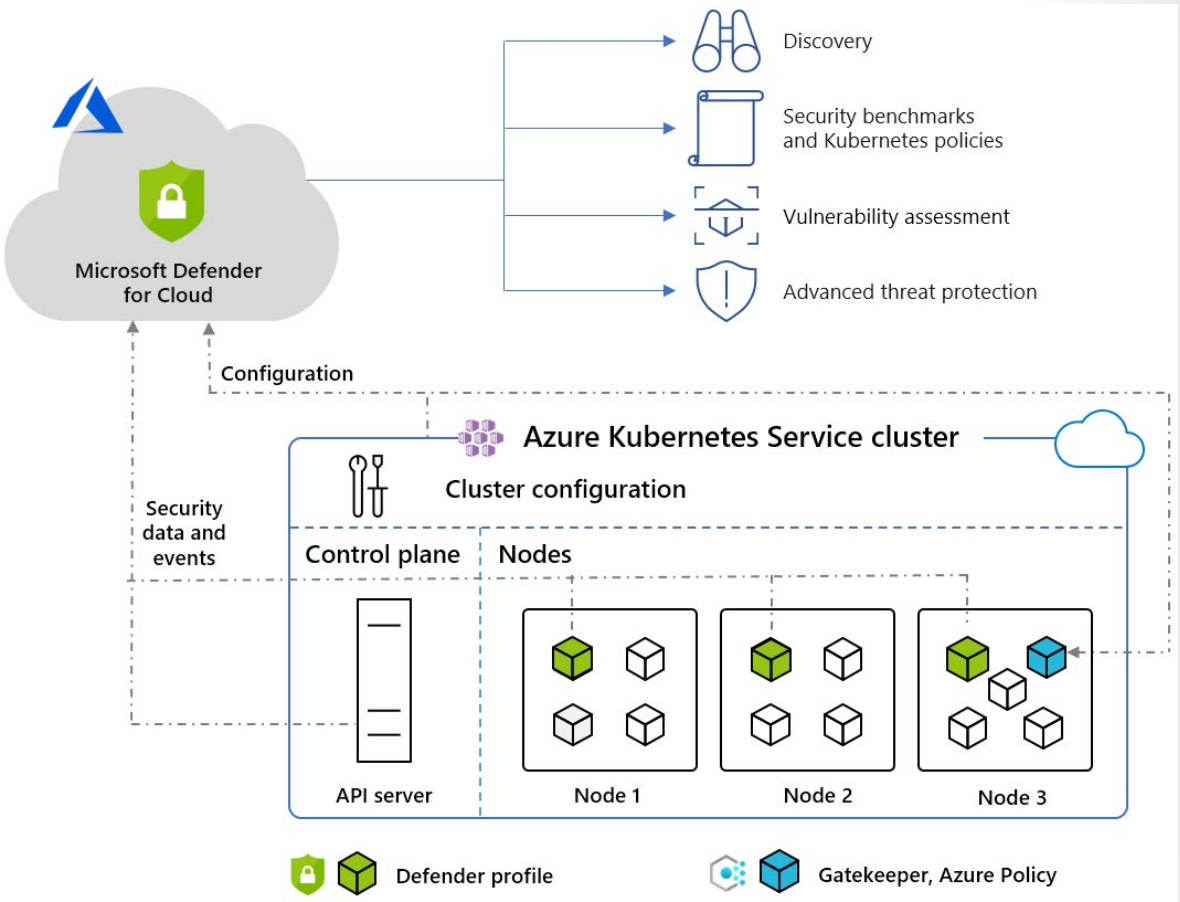
While Kubernetes has many advantages, it also brings new security challenges that should be considered. Therefore, it's crucial to

understand the various security risks that exist in containerized environments, and specifically in Kubernetes.

When you enable Microsoft Defender for Containers, Azure Kubernetes Service clusters, and Azure Arc enabled Kubernetes clusters (Preview) protection are both enabled by default. You can configure your Kubernetes data plane hardening when you enable Microsoft Defender for Containers. The security recommendations will appear in Defender for Cloud dashboard as shown below:



When Defender for Cloud protects a cluster hosted in Azure Kubernetes Service, the collection of audit log data is agentless and frictionless. The Defender profile deployed to each node provides the runtime protections and collects signals from nodes. The Azure Policy add-on for Kubernetes collects cluster and workload configuration for admission control policies as explained in Protect your Kubernetes workloads. The diagram below provides an overview of this solution:



- Defender profile includes a *DaemonSet*, which is a set of containers that focus on collecting inventory and security events from the Kubernetes environment.
- Gatekeeper, Azure Policy, which is the admission controller webhook for Open Policy Agent (OPA), to apply at-scale enforcements and safeguards on your clusters in a centralized, consistent manner.

Exercise

TAILWIND TRADERS

Tailwind Traders is a modern commerce company. For more than 30 years, the company has been a popular retail destination. It has grown to more than 50 physical stores. Several years ago, its chief executive officer (CEO) anticipated changes in retail and bought a competing e-commerce startup that was growing aggressively in niche markets. Today, the company is seen as an innovative leader with customer-focused local storefronts.

The retail innovation team reports to the company's chief technology officer (CTO), who was the CEO of the acquired e-commerce start-up.

Those technology solutions are the main hub for interactions with customers. Those solutions affect 60 percent of global revenue and produce 30 percent of annual gross sales.

The new CIO is focused on improving technical operations in multiple areas to fuel greater innovation throughout the company while limiting disruptions to core business operations. The cloud will play an important role in this transition. To accomplish this vision the CIO hired a new Chief Information Security Officer (CISO). The new CISO started planning his strategy to secure PaaS, IaaS and SaaS workloads, and as part of this strategy he established that the company needs to:

- Implement a cloud security posture management platform that can offer native vulnerability assessment for VMs and Containers, and support threat detection for Cosmos DB
- Implement a data classification system for their Azure workloads that is able to classify and label data in SQL databases and storage accounts
- Implement a security baseline for SaaS workloads in Microsoft 365
- Support security posture management and threat detection for IoT workloads

Questions

1. Which solution should be utilized to:
   - Provide data classification and labeling in Azure?
   - Provide cloud security posture management and threat detection for VM, Containers and Cosmos DB?
2. Which solution should be used to provide cloud security posture management and threat detection for IoT?

Summary

In this module you learned how to specify security baselines for PaaS workloads, and which Azure PaaS workloads are supported by Microsoft Defender for Cloud. You also learned how to specify a security baseline for IaaS VMs, and the general guidelines that you can enforce regardless of the operating system. You learned about the use of Microsoft Secure Score to track security posture enhancement over time in a SaaS environment and the security requirements for IoT workloads.

You also learned the security requirements for Azure App Service and how to use Microsoft Defender for App Service to provide posture management and threat detection for this type of workload. You learned about the requirements for data and storage workloads, and how Azure Purview can help with data classification and labeling. Lastly, you learned about the security requirements for containers and container orchestration.

Visit the links below for more information about the topics covered in this module:

- **Best practices for secure PaaS deployments - Microsoft Azure**[33]

33 https://docs.microsoft.com/azure/security/fundamentals/paas-deployments

- **Overview of the Office cloud policy service for Microsoft 365 Apps for enterprise - Deploy Office**[34]
- **Security recommendations for Azure IoT**[35]
- **Microsoft Defender for IoT for organizations documentation**[36]
- **Data**[37]
- **Introduction to Azure Purview - Azure Purview**[38]
- **Security - Azure App Service**[39]
- **Microsoft Defender for Storage - the benefits and features**[40]
- **Container security with Microsoft Defender for Cloud**[41]

34 https://docs.microsoft.com/deployoffice/admincenter/overview-office-cloud-policy-service
35 https://docs.microsoft.com/azure/iot-fundamentals/security-recommendations
36 https://docs.microsoft.com/azure/defender-for-iot/organizations/
37 https://docs.microsoft.com/security/zero-trust/data-compliance-gov-data
38 https://docs.microsoft.com/azure/purview/overview
39 https://docs.microsoft.com/azure/app-service/overview-security
40 https://docs.microsoft.com/azure/defender-for-cloud/defender-for-storage-introduction
41 https://docs.microsoft.com/azure/defender-for-cloud/defender-for-containers-introduction?tabs=defender-for-container-arch-aks

Knowledge check

Check your Knowledge

Multiple choice

Item 1. How can Tailwind Traders reference Microsoft Zero Trust Architecture?

- ☐ Develop security requirements based on the organizational financial goals.
- ☐ Identify the integration points for architecture using Microsoft Cybersecurity Reference Architecture (MCRA).
- ☐ Provide familiar security tools and significantly enhanced levels of network security.

Multiple choice

Item 2. Security helps create assurances for a business based on three major elements. Which one isn't part of this list?

- ☐ Confidentiality
- ☐ Availability
- ☐ Redundancy

Multiple choice

Item 3. A security strategy must enable defined business outcomes while:

- ☐ Reducing risk to an acceptable level and enable employees to be productive.
- ☐ Reducing risk to zero and enable employees to be productive.
- ☐ Reducing risk to an acceptable level and enable partners.

Multiple choice

Item 4. Which one of the options below isn't a key security strategy principle?

- ☐ Productivity and security
- ☐ Shared responsibility
- ☐ Reduce compromise

Multiple choice

Item 5. Microsoft has built capabilities and resources to help accelerate your implementation of this security guidance on Microsoft Azure. Which tool is responsible for continuous assessment of the workloads and provides security visibility via Secure Score?

- ☐ Azure Security Benchmark
- ☐ Microsoft Defender for Cloud
- ☐ Microsoft Sentinel

Multiple choice

Item 6. Security management strategy is composed by some imperative principles. Given the following definition, which principle does it relate to? "Elevate security through built-in intelligence and recommendations".

- ☐ Visibility
- ☐ Control
- ☐ Guidance

Multiple choice

Item 7. When selecting the appropriate baseline to use, which tool should you use to analyze, test, edit, and store Microsoft-recommended security configuration baselines for Windows?

- ☐ Group Policy
- ☐ Security Compliance Toolkit (SCT)
- ☐ Azure Security Benchmark (ASB)

Multiple choice

Item 8. Which tool should you use if you need to provide guidance for OS hardening and security baseline for Windows and Linux?

- ☐ Group Policy
- ☐ Security Compliance Toolkit (SCT)
- ☐ Azure Security Benchmark (ASB)

Multiple choice

Item 9. Hardening options for mobile devices must include the following requirements except?

- ☐ Establish minimum password length
- ☐ Require data encryption on devices
- ☐ Safely enable jail broken devices

Multiple choice

Item 10. Which solution should be used to capture and parse network traffic by using Windows events directly from your Domain Controllers?

- ☐ Microsoft Defender for Cloud
- ☐ Microsoft Defender for Identity (MDI)
- ☐ Microsoft Sentinel

Multiple choice

Item 11. You are planning a remote access strategy that needs to allow remote workers to connect via RDP and SSH directly from the Azure portal. Which solution should you use?

- ☐ Azure Bastion
- ☐ Point-to-Site (P2S) VPN
- ☐ Site-to-Site (S2S) VPN

Multiple choice

Item 12. Security baselines for Azure focus on cloud-centric control areas. Each recommendation includes a series of information organized in different fields. Which field provides the rationale for the recommendation and links to show how to implement it?

- ☐ Responsibility
- ☐ Azure ID
- ☐ Guidance

Multiple choice

Item 13. Which capability helps to track the security posture progress overtime in a Microsoft 365 environment?

- ☐ Baseline
- ☐ Compliance report
- ☐ Microsoft Secure Score

Multiple choice

Item 14. Which role is responsible for establishing the following security requirements for an IoT environment? 1) Scope hardware to minimum requirements, 2) Make hardware tamper proof, 3) Make upgrades secure.

- ☐ IoT hardware manufacturer/integrator
- ☐ IoT solution operator
- ☐ IoT solution deployer

Multiple choice

Item 15. During this process of better understanding your data, you need to execute a series of tasks that are assigned to different owners. Who owns the task to determine data classification levels?

- ☐ Data security architect
- ☐ Data security engineer
- ☐ System administrator
  [explanation]
  The data security architect is responsible for determining data classification levels. The data security

engineer is responsible for discovering and classifying sensitive data.
[explanation]

Multiple choice

Item 16. Which tool should be used to manage the security posture of Azure App Service workloads?

- ☐ Microsoft Sentinel
- ☐ Microsoft 365
- ☐ Microsoft Defender for Cloud

Answers

Multiple choice

Item 1. How can Tailwind Traders reference Microsoft Zero Trust Architecture?

- ☐ Develop security requirements based on the organizational financial goals.
- ■ Identify the integration points for architecture using Microsoft Cybersecurity Reference Architecture (MCRA).
- ☐ Provide familiar security tools and significantly enhanced levels of network security.

Explanation
Using the Microsoft Cybersecurity Reference Architecture (MCRA) is key to implementing a Zero Trust architecture.

Multiple choice

Item 2. Security helps create assurances for a business based on three major elements. Which one isn't part of this list?

- ☐ Confidentiality
- ☐ Availability
- ■ Redundancy

Explanation
Redundancy isn't a separate element, is actually part of availability.

Multiple choice

Item 3. A security strategy must enable defined business outcomes while:

- ■ Reducing risk to an acceptable level and enable employees to be productive.
- ☐ Reducing risk to zero and enable employees to be productive.
- ☐ Reducing risk to an acceptable level and enable partners.

Explanation
The security strategy must enable defined business outcomes, reduce risk to an acceptable level, and enable employees to be productive.

Multiple choice

Item 4. Which one of the options below isn't a key security strategy principle?

- ☐ Productivity and security
- ☐ Shared responsibility
- ■ Reduce compromise

Explanation
Reduce compromise isn't a key security strategy principle. Shared responsibility as well as Productivity and security are actually key security strategy principles.

Multiple choice

Item 5. Microsoft has built capabilities and resources to help accelerate your implementation of this security guidance on Microsoft Azure. Which tool is responsible for continuous assessment of the workloads and provides security visibility via Secure Score?

☐ Azure Security Benchmark

■ Microsoft Defender for Cloud

☐ Microsoft Sentinel

Explanation
Defender for Cloud performs continuous assessment, and it has the Secure Score capability built-in.

Multiple choice

Item 6. Security management strategy is composed by some imperative principles. Given the following definition, which principle does it relate to? "Elevate security through built-in intelligence and recommendations".

☐ Visibility

☐ Control

■ Guidance

Explanation
Guidance is used to elevate security through built-in intelligence and recommendations.

Multiple choice

Item 7. When selecting the appropriate baseline to use, which tool should you use to analyze, test, edit, and store Microsoft-recommended security configuration baselines for Windows?

☐ Group Policy

■ Security Compliance Toolkit (SCT)

☐ Azure Security Benchmark (ASB)

Explanation
SCT is used to analyze, test, edit, and store Microsoft-recommended security configuration baselines for Windows.

Multiple choice

Item 8. Which tool should you use if you need to provide guidance for OS hardening and security baseline for Windows and Linux?

☐ Group Policy

☐ Security Compliance Toolkit (SCT)

■ Azure Security Benchmark (ASB)

Explanation
ASB can be used to provide guidance for OS hardening and security baseline for Windows and Linux.

Multiple choice

Item 9. Hardening options for mobile devices must include the following requirements except?

☐ Establish minimum password length

☐ Require data encryption on devices

■ Safely enable jail broken devices

Explanation
Jail broken devices should be prohibited.

Multiple choice

Item 10. Which solution should be used to capture and parse network traffic by using Windows events directly from your Domain Controllers?

☐ Microsoft Defender for Cloud

■ Microsoft Defender for Identity (MDI)

☐ Microsoft Sentinel

Explanation
MDI captures and parses network traffic by using Windows events directly from your Domain Controllers.

Multiple choice

Item 11. You are planning a remote access strategy that needs to allow remote workers to connect via RDP and SSH directly from the Azure portal. Which solution should you use?

■ Azure Bastion

☐ Point-to-Site (P2S) VPN

☐ Site-to-Site (S2S) VPN

Explanation
Azure Bastion allows remote workers to connect via RDP and SSH directly from the Azure portal.

Multiple choice

Item 12. Security baselines for Azure focus on cloud-centric control areas. Each recommendation includes a series of information organized in different fields. Which field provides the rationale for the recommendation and links to show how to implement it?

☐ Responsibility

☐ Azure ID

■ Guidance

Explanation
Guidance contains the rationale for the recommendation. Responsibility describes who is responsible for implementing the control and Azure ID describes the Azure Security Benchmark ID that corresponds to the recommendation.

Multiple choice

Item 13. Which capability helps to track the security posture progress overtime in a Microsoft 365 environment?

- ☐ Baseline
- ☐ Compliance report
- ■ Microsoft Secure Score

Explanation
Secure Score helps to track the security posture progress of your SaaS environment.

Multiple choice

Item 14. Which role is responsible for establishing the following security requirements for an IoT environment? 1) Scope hardware to minimum requirements, 2) Make hardware tamper proof, 3) Make upgrades secure.

- ■ IoT hardware manufacturer/integrator
- ☐ IoT solution operator
- ☐ IoT solution deployer

Explanation
IoT hardware manufacturer/integration is responsible for these tasks. The IoT solution operator is responsible for keeping the system up-to-date. The IoT solution deployer is responsible for deploying hardware securely.

Multiple choice

Item 15. During this process of better understanding your data, you need to execute a series of tasks that are assigned to different owners. Who owns the task to determine data classification levels?

- ■ Data security architect
- ☐ Data security engineer
- ☐ System administrator
  [explanation]
  The data security architect is responsible for determining data classification levels. The data security engineer is responsible for discovering and classifying sensitive data.
  [explanation]

Multiple choice

Item 16. Which tool should be used to manage the security posture of Azure App Service workloads?

- ☐ Microsoft Sentinel
- ☐ Microsoft 365
- ■ Microsoft Defender for Cloud

Explanation
Microsoft Defender for Cloud is a cloud security posture management solution. Microsoft Sentinel is a SIEM Solution. Microsoft 365 is a SaaS productivity solution.

Module 4 Design a strategy for data and applications

Specify security requirements for applications

Introduction

In this module, you'll learn how to:

- Specify a security strategy for applications and APIs
- Specify priorities for mitigating threats to applications
- Specify a security standard for onboarding a new application

The content in the module will help you prepare for Exam SC-100: Cybersecurity Architecture. The module concepts are covered in:

- Design a Strategy for Data and Applications
- Specify Security Requirements for Applications

Prerequisites

- Conceptual knowledge of application threat modeling, requirements, zero trust architecture, and management of hybrid environments.
- Working experience with application security strategies and developing security requirements based on business goals.

Understand application threat modeling

Do a comprehensive analysis to identify threats, attacks, vulnerabilities, and countermeasures. Having this information can protect the application and its threats to the system. Start with simple questions to gain insight into potential risks. Then, progress to advanced techniques using threat modeling.

1- Gather information about the basic security controls

A threat modeling tool will produce a report of all threats identified. This report is typically uploaded into a tracking tool or converted to work items that can be validated and addressed by the developers. The threat model should be updated and integrated into the code management process as new features are added to the solution. If a security issue is found, there should be a process to triage issue severity and determine when and how to remediate (such as in the next release cycle or a faster release).

Start by gathering information about each component of the application. The answers to these questions will identify gaps in basic protection and clarify the attack vectors.

2- Evaluate the application design progressively

Analyze application components and connections and their relationships. Threat modeling is a crucial engineering exercise that includes defining security requirements, identifying and mitigating threats, and validating those mitigations. This technique can be used at any application development or production stage, but it's most effective during the design stages of new functionality.

Popular methodologies include:

STRIDE[1]:

Category	Description
Spoofing	Involves illegally accessing and then using another user's authentication information, such as user-name and password
Tampering	Involves the malicious modification of data. Examples include unauthorized changes made to persistent data, such as that held in a database and the alteration of data as it flows between two computers over an open network, such as the Internet
Repudiation	Associated with users who deny performing an action without other parties having any way to prove otherwise for example, a user performs an illegal operation in a system that lacks the ability to trace the prohibited operations. Non-Repudia-tion refers to the ability of a system to counter repudiation threats. For example, a user who purchases an item might have to sign for the item upon receipt. The vendor can then use the signed receipt as evidence that the user did receive the package

1 https://docs.microsoft.com/azure/security/develop/threat-modeling-tool-threats

Category	Description
Information Disclosure	Involves the exposure of information to individuals who are not supposed to have access to it for example, the ability of users to read a file that they were not granted access to, or the ability of an intruder to read data in transit between two computers
Denial of Service	Denial of service (DoS) attacks deny service to valid users for example, by making a Web server temporarily unavailable or unusable. You must protect against certain types of DoS threats simply to improve system availability and reliability
Elevation of Privilege	An unprivileged user gains privileged access and thereby has sufficient access to compromise or destroy the entire system. Elevation of privilege threats include those situations in which an attacker has effectively penetrated all system defenses and become part of the trusted system itself, a dangerous situation indeed

Microsoft Security Development Lifecycle uses STRIDE and provides a tool to assist with this process. This tool is available at no additional cost. For more information, see **Microsoft Threat Modeling Tool**[2].

- **Open Web Application Security Project (OWASP)**[3] has documented a threat modeling approach for applications.

Integrate threat modeling through automation using secure operations. Here are some resources:

- Toolkit for **Secure DevOps on Azure**[4].
- **Guidance on DevOps pipeline security**[5] by OWASP.

3- Mitigate the identified threats

The threat modeling tool produces a report of all the threats identified. After identifying a potential threat, determine how it can be detected and respond to that attack. Define a process and timeline which minimizes exposure to any identified vulnerabilities in the workload so that those vulnerabilities can't be left unaddressed.

Use the *Defense-in-Depth* approach. This can help identify controls needed in the design to mitigate risk if a primary security control fails. Evaluate how likely it is for the primary control to fail. If it

2 https://www.microsoft.com/securityengineering/sdl/threatmodeling
3 https://owasp.org/www-community/Threat_Modeling_Process
4 https://azsk.azurewebsites.net/
5 https://www.owasp.org/index.php/OWASP_AppSec_Pipeline#tab=Main

does, what is the extent of the potential organizational risk? Also, what is the effectiveness of the additional control (especially in cases that would cause the primary control to fail)? Based on the evaluation, apply Defense-in-Depth measures to address potential failures of security controls.

The principle of *least privilege* is one way of implementing Defense-in-Depth. It limits the damage that a single account can do. Grant the least number of privileges to accounts that allows them to accomplish the required permissions within a time period. This helps mitigate the damage of an attacker who gains access to the account to compromise security assurances.

Microsoft Threat Modeling Tool mitigations

The Threat Modeling Tool is a core element of the Microsoft Security Development Lifecycle (SDL). It allows software architects to identify and mitigate potential security issues early when they're relatively easy and cost-effective to resolve. As a result, it greatly reduces the total cost of development. Also, we designed the tool with non-security experts in mind, making threat modeling easier for all developers by providing clear guidance on creating and analyzing threat models.

Mitigation categories

The Threat Modeling Tool mitigations are categorized according to the Web Application Security Frame, which consists of the following:

Category	Description
Auditing and Logging	Who did what and when? Auditing and logging refer to how your application records security-related events
Authentication	Who are you? Authentication is the process where an entity proves the identity of another entity, typically through credentials, such as a user name and password
Authorization	What can you do? Authorization is how your application provides access controls for resources and operations
Communication Security	Who are you talking to? Communication Security ensures all communication done is as secure as possible
Configuration Management	Who does your application run as? Which databases does it connect to? How is your application administered? How are these settings secured? Configuration management refers to how your application handles these operational issues

Category	Description
Cryptography	How are you keeping secrets (confidentiality)? How are you tamper-proofing your data or libraries (integrity)? How are you providing seeds for random values that must be cryptographically strong? Cryptography refers to how your application enforces confidentiality and integrity
Exception Management	When a method call in your application fails, what does your application do? How much do you reveal? Do you return friendly error information to end users? Do you pass valuable exception information back to the caller? Does your application fail gracefully?
Input Validation	How do you know that the input your application receives is valid and safe? Input validation refers to how your application filters, scrubs, or rejects input before additional processing. Consider constraining input through entry points and encoding output through exit points. Do you trust data from sources such as databases and file shares?
Sensitive Data	How does your application handle sensitive data? Sensitive data refers to how your application handles any data that must be protected either in memory, over the network, or in persistent stores
Session Management	How does your application handle and protect user sessions? A session refers to a series of related interactions between a user and your Web application

Specify priorities for mitigating threats to applications

Enterprise organizations typically have a large application portfolio, but not all applications have equal importance. Applications containing business-critical data regulated data and high business value, visibility, or criticality should be prioritized based on identification and classification to appropriately direct monitoring, time, and resources. You should also identify applications or systems with significant access, which might grant control over other critical systems or data.

Identify and classify applications

Ensure you have identified and classified the applications in your portfolio that are critical to business functions. Enterprise organizations typically have a large application portfolio, so prioritizing where to invest time and effort into manual and resource-intensive tasks like threat modeling can increase the effectiveness of your security program.

Identify applications with a high potential impact and, or a high potential exposure to threats.

Risk	Mitigation	Examples
High Potential Impact	Identify applications that would have a significant impact on the business if compromised.	Business critical data: Applications that process or store information, which would cause significant negative business or mission impact if assurance of confidentiality, integrity, or availability is lost.
		Regulated data: Applications that handle monetary instruments and sensitive personal information are regulated by standards. For example, the payment card industry (PCI) and Health Information Portability and Accountability Act (HIPAA).
		Business critical availability: Applications whose functionality is critical to the organization's business mission, such as production lines generating revenue, devices or services critical to life and safety, and other critical functions.
		Significant Access: Applications that have access to systems with a high potential impact through technical means such as Stored Credentials or Permissions granted via access control lists or other means.
High exposure to attacks	Applications that are easily accessible to attackers, such as web applications on the open Internet.	

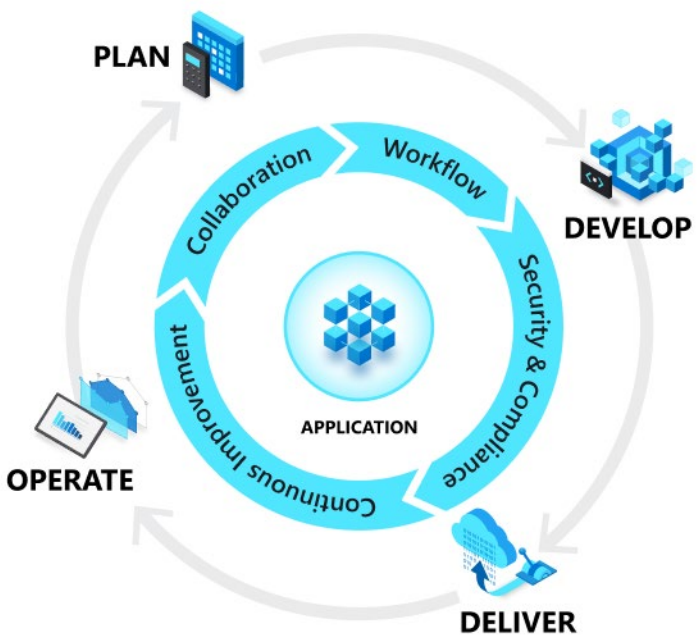
Specify a security standard for onboarding a new application

Specify a security strategy for applications and APIs

Organizations should shift from a 'Waterfall' development cycle to the DevOps lifecycle of continuous integration, continuous delivery (CI/CD) for applications, and API development as quickly as possible. DevOps is the union of people, processes, and tools that enable continuous delivery of value to end users. The contraction of Dev and Ops refers to combining the development and operations disciplines into multidisciplinary teams that work together with shared and efficient practices and tools.

The DevOps model increases the organization's ability to rapidly address security concerns without waiting for a waterfall model's longer planning and testing cycle.

Deploy the DevOps and the application lifecycle



DevOps influences the application and API lifecycle throughout its plan, develop, deliver, and operate phases. Each phase relies on the others, and the phases are not role-specific. In a true DevOps culture, each role is involved in each phase to some extent.

Phase	Activities
Plan	DevOps teams ideate, define and describe features and capabilities of the applications and systems they're building. They track progress at low and high levels of granularity from single-product tasks to tasks that span portfolios of multiple products. Some of the ways DevOps teams plan with agility and visibility are creating backlogs, tracking bugs, managing agile software development with Scrum, using Kanban boards, and visualizing progress with dashboards.

Phase	Activities
Develop	Includes all aspects of coding writing, testing, reviewing, and integrating code by team members as well as building that code into build artifacts that can be deployed into various environments. Teams use version control, usually Git, to collaborate on code and work in parallel. They also seek to innovate rapidly without sacrificing quality, stability, and productivity. To do that, they use highly productive tools, automate mundane and manual steps, and iterate in small increments through automated testing and continuous integration
Deliver	The process of deploying applications into production environments consistently and reliably, ideally via continuous delivery. The deliver phase also includes deploying and configuring the fully governed foundational Infrastructure that makes up those environments. These environments often use technologies like Infrastructure as Code (IaC), containers, and microservices.
Operate	Involves maintaining, monitoring, and troubleshooting applications in production environments, usually hosted in public and hybrid clouds. In adopting DevOps practices, teams work to ensure system reliability, high availability and aim for zero downtime while reinforcing security and governance.

Enforcing Security for DevOps

Teams that don't have a formal DevSecOps strategy are encouraged to begin the planning as soon as possible. At first, there may be some resistance from team members who don't fully appreciate the existing threats. Others may not feel that the team is equipped to face the problem and that any special investment would be a wasteful distraction from shipping features. However, it's necessary to begin the conversation to build consensus on the nature of the risks, how the team can mitigate them, and whether the team needs resources, they don't currently have.

Expect skeptics to bring some common arguments, such as:

- **How real is the threat?** Teams often don't appreciate the potential value of the services and data they're charged with protecting.
- **Our team is good, right?** A security discussion may be perceived as doubt about the team's ability to build a secure system.
- **I don't think that's possible.** This is a common argument from junior engineers. Those with experience usually know better.
- **We've never been breached.** But how do you know? How *would* you know?

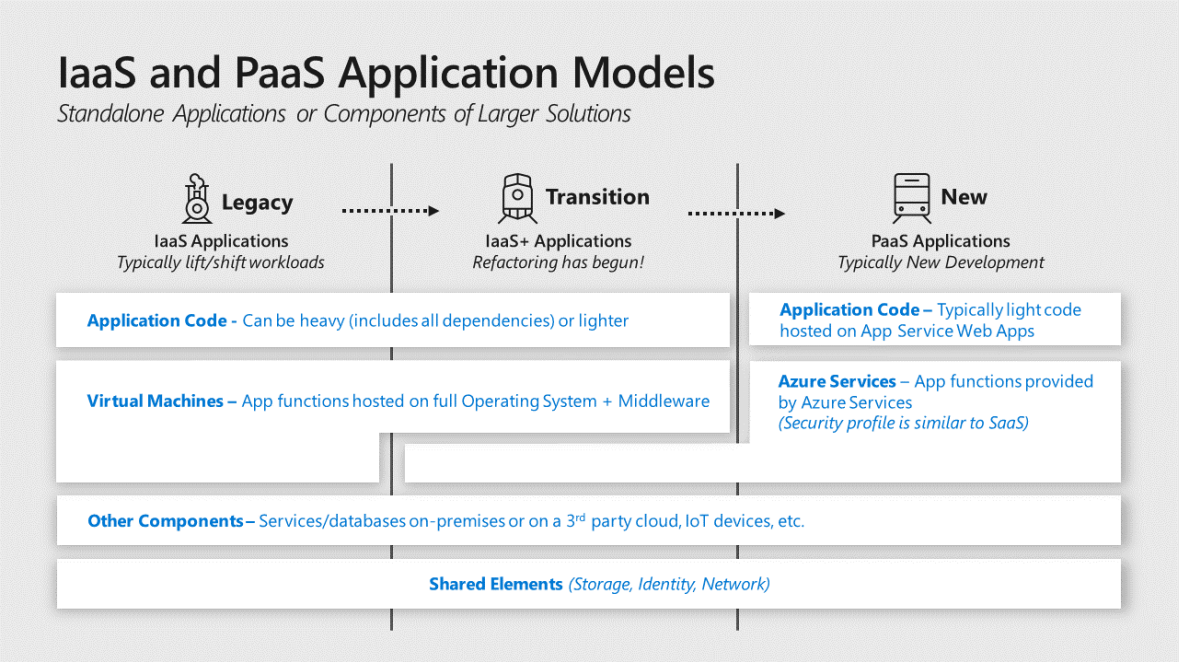
- **Endless debates about value.** DevSecOps is a serious commitment that may be perceived as a distraction from core feature work. While the security investment should be balanced with other needs, it can't be ignored.

Specify a security strategy for applications and APIs

Applications and their data ultimately act as the primary store of business value on a cloud platform. While the platform components like identity and storage are critical elements of the security environment, applications play an outsize role in risks to the business because:

- **Business Processes** are encapsulated and executed by applications, and services need to be available and provided with high integrity
- **Business Data** is stored and processed by application workloads and requires high assurances of confidentiality, integrity, and availability.

This section focuses on applications written by your organization or by others on behalf of your organization vs. SaaS or commercially available applications installed on IaaS VMs.



Modern cloud platforms like Azure can host both legacy and modern generations of applications

- **Legacy**–applications are hosted on Infrastructure as a Service (IaaS) virtual machines that typically include all dependencies, including OS, middleware, and other components.

- **Modern**–Platform as a Service (PaaS) applications don't require the application owner to manage and secure the underlying server operating systems (OSes) and are sometimes fully "Serverless" and built primarily using functions as a service.
- **Hybrid**–While hybrid applications can take many forms, the most common is an "IaaS plus" state where legacy applications are transitioning to modern architecture with modern services replacing legacy components or being added to a legacy application.

Securing an application requires security assurances for three different component types:

- **Application Code**–Application Code is the logic that defines the custom application that you write. The security of this code is the application owners' responsibility in all generations of application architecture, including any open-source snippets or components included in the code. Securing the code requires identifying and mitigating risks from the design and implementation of the application. It also requires assessing the supply chain risk of included components.
- **Application Services**–Application Services are the various standardized components that the application uses, such as databases, identity providers, event hubs, IoT device management, and so on.
- **Application Hosting Platform**–This is the computing environment where the application actually executes and runs. In an enterprise with applications hosted on premises, in Azure, and in third-party clouds like Amazon Web Services (AWS), this (Application Hosting Platform) could take many forms with significant variations on who is responsible for security:

Onboarding New Applications

An Azure Active Directory (Azure AD) application registration is a critical part of your business application. Any misconfiguration or lapse in the hygiene of your application can result in downtime or compromise.

This article describes security best practices for the following application registration properties.

Redirect URI	It's important to keep Redirect URIs of your application up to date. A lapse in the ownership of one of the redirect URIs can lead to an application compromise. Ensure that all DNS records are updated and monitored periodically for changes. Along with maintaining ownership of all URIs, don't use wildcard reply URLs or insecure URI schemes such as http or URN.
Implicit grant flow for an access token	Scenarios that require implicit flow can now use Auth code flow to reduce the risk of compromise associated with implicit grant flow misuse. If you configured your application registration to get Access tokens using implicit flow but don't actively use it, we recommend you turn off the setting to protect it from misuse.
Credential	Credentials are a vital part of an application registration when your application is used as a confidential client. If your app registration is used only as a Public Client App (which allows users to sign in using a public endpoint), ensure that you don't have any credentials on your application object.
AppId URI	Certain applications can expose resources (via WebAPI) and, as such, need to define an AppId URI that uniquely identifies the resource in a tenant. We recommend using either of the following URI schemes: API or HTTPS, and set the AppId URI in the following formats to avoid URI collisions in your organization. The AppId URI acts as the prefix for the scopes referenced in the API's code, and it must use a verified customer owned domain. For multi-tenant applications, the value must also be globally unique.
Application ownership	Ensure app ownership is kept to a minimal set of people within the organization. It's recommended to run through the owner's list once every few months to ensure owners are still part of the organization and their charter accounts for ownership of the application registration.
Checklist	App developers can use the Checklist available in the Azure portal to ensure their app registration meets a high quality bar and provides guidance to integrate securely. The integration assistant highlights best practices and recommendations that help avoid common oversights when integrating with the Microsoft identity platform.

Security Standards for Onboarding applications

Organizations should use guidance and automation for securing applications in the cloud rather than starting from zero.

- Using resources and lessons learned by external organizations that are early adopters of these models can accelerate the improvement of an organization's security posture with less effort and resources.
- Developers should use services available from your cloud provider for well-established functions like databases, encryption, identity directory, and authentication instead of writing custom versions of them.
- Use native security capabilities built into cloud services instead of adding external security components (data encryption, network traffic filtering, threat detection, and other functions).
- Always authenticate with identity services rather than cryptographic keys when available.
- Deploy web application firewalls (WAFs) to mitigate the risk of an attacker being able to exploit commonly seen security vulnerabilities for applications.
- Enforce security for applications hosted in containers, general application best practices, and some specific guidelines to manage this new application architecture type.
- Enforce a more comprehensive threat model standard that can identify more potential risks; two popular standards are STRIDE and OWASP.

Several capabilities should be prioritized first because of potential security impact:

- **Identity** - User directories and other authentication functions are complex to develop and critically important to security assurances. Avoid using homegrown authentication solutions and favor mature capabilities like:
  - Azure Active Directory (**Azure AD**[6])
  - **Azure AD B2B**[7]
  - **Azure AD B2C**[8]
  - Third-party solutions to authenticate and grant permission to users, partners, and customers, applications, services, and other entities.
- **Data Protection** - Developers, should use established capabilities from cloud providers such as native encryption in cloud services to encrypt and protect data. The security world is littered with examples of failed attempts to protect data or passwords that didn't stand up to real world attacks. If direct use of cryptography is required, developers should call well-established cryptographic algorithms and not attempt to invent their own.

6 https://docs.microsoft.com/azure/active-directory/
7 https://docs.microsoft.com/azure/active-directory/b2b/
8 https://docs.microsoft.com/azure/active-directory-b2c/

- **Key management**–Ideally, use identity for authentication rather than directly handling keys (see **Prefer Identity Authentication over Keys**[9]). For situations where accessing services that require access to keys, use a key management service like **Azure Key Vault**[10] or AWS **Key Management Service**[11]. This will help you manage and secure these keys rather than attempting to safely handle keys in application code. You can use **CredScan**[12] to discover potentially exposed keys in your application code.
- **Application Configurations** - Inconsistent configurations for applications can create security Risks. Azure App Configuration provides a service to centrally manage application settings and feature flags, which helps mitigate this risk.

Additional information

For additional information on Security Standards for applications, see the following:

- **Best Practices for Application Registration**[13]
- **Threat Modeling**[14]
- **OWASP ASVS**[15]
- **STRIDE**[16]
- **NIST SSDF**[17]
- **Microsoft Secure DevOps using Azure**[18]

Exercise

Meet Tailwind Traders

Tailwind Trader is a fictitious home improvement retailer. It operates retail hardware stores across the globe and online. The Tailwind Traders CISO is aware of the opportunities offered by Azure but also understands the need for strong security and solid cloud architecture. Without strong security and a great point of reference architecture, the company may have difficulty managing the Azure environment and costs, which are hard to track and control. The CISO is interested in understanding how Azure manages and enforces security standards.

9 https://docs.microsoft.com/security/compass/applications-services#prefer-identity-authentication-over-keys
10 https://docs.microsoft.com/azure/key-vault/
11 https://aws.amazon.com/kms/
12 https://secdevtools.azurewebsites.net/helpcredscan.html
13 https://docs.microsoft.com/azure/active-directory/develop/security-best-practices-for-app-registration
14 https://docs.microsoft.com/azure/security/develop/threat-modeling-tool
15 https://owasp.org/www-project-application-security-verification-standard/
16 https://docs.microsoft.com/azure/security/develop/threat-modeling-tool-threats
17 https://csrc.nist.gov/publications/detail/sp/800-218/final
18 https://azsk.azurewebsites.net/

Requirements

Tailwind Traders is planning on making some significant changes to their Application Security Strategy. Currently, they're using the Waterfall development cycle to manage all applications. They have asked for your assistance with recommendations and questions. Here are the specific requirements.

- **Security in DevOps.** The company has a new security optimization project for customer environments. The CISO wants to ensure that all available Applications are secured and controlled in the cloud.

Tasks

Evaluate an Application Security Standard

- What could Tailwind Traders do to increase the organization's ability to rapidly address security concerns without waiting for a longer planning and testing cycle of a waterfall model?
- Evaluate a standard and explain your decision-making process.
- Tailwind Traders should shift from a 'Waterfall' development cycle to a DevOps lifecycle of continuous integration, continuous delivery (CI/CD) for applications, and API development as quickly as possible.
- What security strategy components could Tailwind Traders use to mitigate breaches for new applications deployed in Azure?
- Tailwind Traders should enforce Threat Modeling, Code Reviews, Security Testing and optimize their Security
  Development Lifecycle (SDL) for new applications.

How are you enforcing Application Security for all users to protect their identity, data, and other assets in Microsoft Azure?

Summary

In this module, you've learned how to build an overall application security strategy. You have learned different strategies for designing, defining, and recommending an organizational application security strategy and architecture. You should now be able to:

- Specify a security strategy for applications and APIs
- Specify priorities for mitigating threats to applications
- Specify a security standard for onboarding a new application

Learn more with Azure documentation

- **Threats - Microsoft Threat Modeling Tool - Azure**[19]
- **Mitigations - Microsoft Threat Modeling Tool**[20]

19 https://docs.microsoft.com/azure/security/develop/threat-modeling-tool-threats
20 https://docs.microsoft.com/azure/security/develop/threat-modeling-tool-mitigations

- **Application threat analysis - Microsoft Azure Well-Architected Framework**[21]
- **Azure security baseline for App Service**[22]
- **Application security in Azure**[23]
- **Security in DevOps**[24]

21 https://docs.microsoft.com/azure/architecture/framework/security/design-threat-model
22 https://docs.microsoft.com/security/benchmark/azure/baselines/app-service-security-baseline
23 https://docs.microsoft.com/security/compass/applications-services
24 https://docs.microsoft.com/devops/operate/security-in-devops

Design a strategy for securing data

Introduction

In this module, you'll learn how to:

- Prioritize mitigating threats to data
- Design a strategy to identify and protect sensitive data
- Specify an encryption standard for data at rest and in motion

The content in the module will help you prepare for Exam SC-100: Cybersecurity Architecture. The module concepts are covered in:

Design a Strategy for Data and Applications

- Design a Strategy for Securing Data

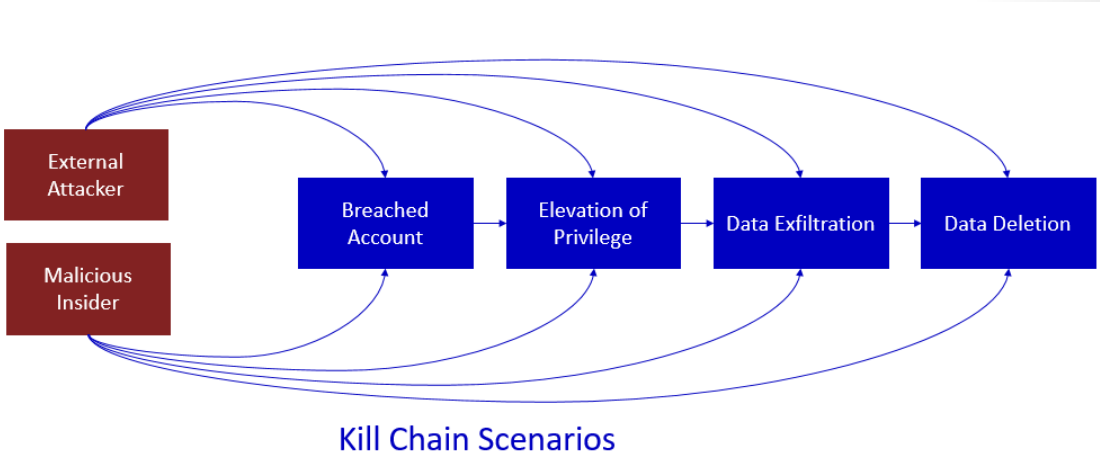
Prerequisites

- Conceptual knowledge of application threat modeling, requirements, zero trust architecture, and management of hybrid environments.
- Working experience with application security strategies and developing security requirements based on business goals.

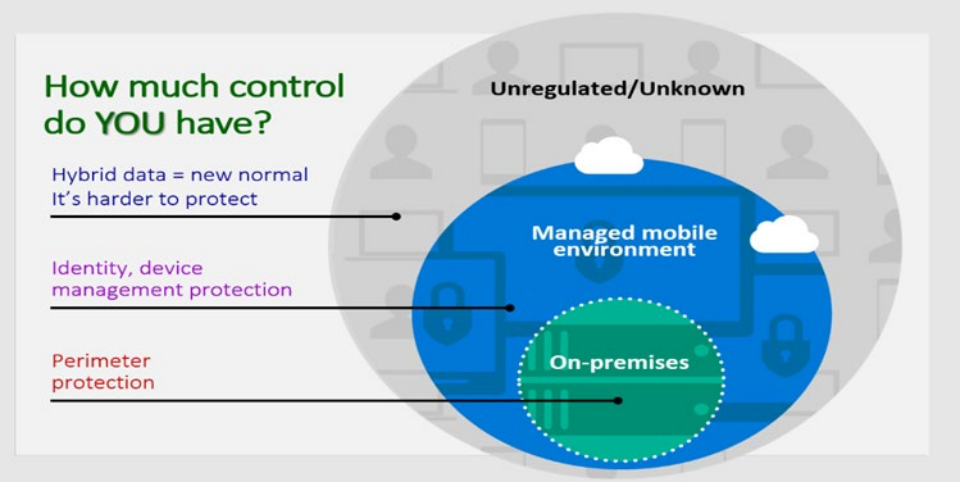
Prioritize mitigating threats to data

Cybersecurity weaknesses identified in your organization are mapped to actionable security recommendations and prioritized by their impact. Prioritized recommendations help shorten the time to mitigate or remediate vulnerabilities and drive compliance.

Most attacks follow a common process referred to within the security industry as the “Kill Chain.” An attack follows a basic pattern and proceeds from one step to the next to achieve the wanted outcomes. This step-wise process can be defended against by implementing security measures on choke points in the chain. Since any step can be bypassed through various exploitation techniques, the best strategies apply defenses at every step along the chain.



How much control do companies have?



In an on-premises environment, you have firewalls, email gateways, and proxies that can conduct a content inspection. That protection boundary has now expanded to include mobile devices, tablets, and cloud assets. Often the devices that have access to a company's data are either lightly managed or not managed at all. Some companies may use Mobile Device Management (MDM) solutions to help enforce some level of security, such as encrypting the device or configuring it for remote wipe in the event the device gets stolen. However, they still don't have any control when data on those devices moves outside their controlled environment.

In today's cloud-centric world, organizations are faced with the unregulated (such as files on cloud storage services) and the unknown (such as advanced threats targeting users' email). This situation is more difficult to protect because data is now stored everywhere - it's on-premises, on PCs, on phones, and in the cloud.

Security recommendations to mitigate threats to data

Product/Service	Article	
Machine Trust Boundary	Ensure that binaries are obfuscated if they contain sensitive information	
	Consider using an Encrypted File System (EFS) is used to protect confidential user-specific data	
	Ensure that sensitive data stored by the application on the file system is encrypted	
Web Application	Ensure that sensitive content isn't cached on the browser	
	Encrypt sections of Web App's configuration files that contain sensitive data	
	Explicitly disable the autocomplete HTML attribute in sensitive forms and inputs	
	Ensure that sensitive data displayed on the user screen is masked	
Database	Implement dynamic data masking to limit sensitive data exposure non privileged users	
	Ensure that passwords are stored in salted hash format	
	Ensure that sensitive data in database columns are encrypted	
	Ensure that database-level encryption (TDE) is enabled	
	Ensure that database backups are encrypted	
Web API	Ensure that sensitive data relevant to Web API isn't stored in the browser's storage	
Azure Document DB	Encrypt sensitive data stored in Azure Cosmos DB	
Azure IaaS VM Trust Boundary	Use Azure Disk Encryption to encrypt disks used by Virtual Machines	
Service Fabric Trust Boundary	Encrypt secrets in Service Fabric applications	
Dynamics CRM	Perform security modeling and use Business Units/Teams where required	

Product/Service	Article	
	Minimize access to share feature on critical entities	
	Train users on the risks associated with the Dynamics CRM Share feature and good security practices	
	Include a development standards rule proscribing showing config details in exception management	
Azure Storage	Use Azure Storage Service Encryption (SSE) for Data at Rest (Preview)	
	Use Client-Side Encryption to store sensitive data in Azure Storage	
Mobile Client	Encrypt sensitive or PII data written to phones local storage	
	Obfuscate generated binaries before distributing to end users	
WCF	Set clientCredentialType to Certificate or Windows	
	WCF-Security Mode isn't enabled	————————+

Ransomware Protection

Mitigating ransomware and extortion attacks is an urgent priority for organizations because of the high impact of these attacks and high likelihood an organization will experience one.

Ransomware is a type of extortion attack that encrypts files and folders, preventing access to important data. Criminals use ransomware to extort money from victims by demanding money, usually in form of cryptocurrency, in exchange for a decryption key. Criminals also often use ransomware to extort money from victims in exchange for not releasing sensitive data to the dark web or the public internet.

These attacks can be catastrophic to business operations and are difficult to clean up, requiring complete adversary eviction to protect against future attacks. Unlike early forms of ransomware that only required malware remediation, human-operated ransomware can continue to threaten your business operations after the initial encounter.

Prevent and Recover from Ransomware

Phase 1. Prepare your recovery plan

This phase is designed to **minimize the monetary incentive from ransomware**

attackers[25] by making it:

- Much harder to access and disrupt systems or encrypt or damage key organization data.
- Easier for your organization to recover from an attack without paying the ransom.

Phase 2. Limit the scope of damage

Make the attackers work a lot harder to **gain access to multiple business critical systems through privileged access roles**[26]. Limiting the attacker's ability to get privileged access makes it much harder to profit off of an attack on your organization, making it more likely they will give up and go elsewhere.

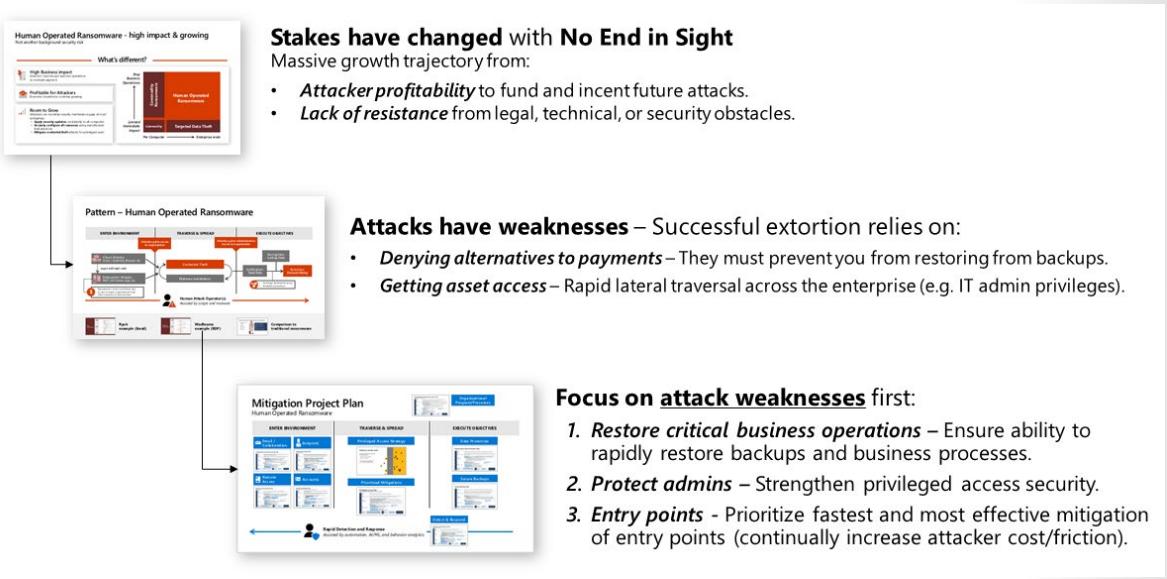
Phase 3. Make it harder to get in

This last set of tasks is important to raise friction for entry but will take time to complete as part of a larger security journey. The goal of this phase is for attackers to have to work a lot harder to **obtain access to your on-premises or cloud infrastructures**[27] at the various common points of entry. There are a lot of these tasks, so it's important to prioritize your work here based on how fast you can accomplish these with your current resources.

For a comprehensive view of ransomware and extortion and how to protect your organization, use the information in the **Human-Operated Ransomware Mitigation Project Plan**[28] PowerPoint presentation.

Here's a summary of the guidance:

25 https://docs.microsoft.com/security/compass/protect-against-ransomware-phase1
26 https://docs.microsoft.com/security/compass/protect-against-ransomware-phase2
27 https://docs.microsoft.com/security/compass/protect-against-ransomware-phase3
28 https://download.microsoft.com/download/7/5/1/751682ca-5aae-405b-afa0-e4832138e436/RansomwareRecommendations.pptx



- The stakes of ransomware and extortion-based attacks are high.
- However, the attacks have weaknesses that can mitigate your likelihood of being attacked.
- There are three phases to configure your infrastructure to exploit attack weaknesses.

For additional information on Mitigating Threats to Data, see the following:

- **Defender for Cloud App Best Practices**[29]
- **Threat Remediation**[30]
- **Manage Multi-Cloud Environment**[31]
- **Ransomware Protection**[32]

Design a strategy to identify and protect sensitive data

In a perfect world, all your employees understand the importance of information protection and work within your policies. In the real world, it's likely that a busy partner who frequently works with accounting information will inadvertently upload a sensitive document to your Box repository with incorrect permissions. A week later, you realize your enterprise's confidential information was leaked to your competition.

29 https://docs.microsoft.com/defender-cloud-apps/best-practices
30 https://docs.microsoft.com/defender-cloud-apps/tutorial-flow
31 https://docs.microsoft.com/defender-cloud-apps/tutorial-cloud-platform-security
32 https://docs.microsoft.com/security/compass/protect-against-ransomware

The basic strategy for data identification and protection relies on the following elements - depending on which product you use, there may be a greater emphasis on certain concepts:

1. Data discovery - create an inventory of all of the data stores and knowledge bases within your organization.
2. Data classification - define what counts as sensitive for your organization.
3. Data protection – define policies to control access to and sharing of data. To apply flexible protection actions that include encryption, access restrictions, and visual markings
4. Usage monitoring – reporting and auditing on data access activity and policy violations.
5. Data loss prevention - To help prevent accidental oversharing of sensitive information

Data discovery - know your data

It's vital for organizations to identify what kind of, and how much, data exists in their environment. You need a deep understanding of how much sensitive data exists and where it is stored before it can be protected and governed. This information is critical to assess your overall risk, which helps you define your strategy for protecting and governing the data. Start your journey by discovering and classifying important data across your environment. Here are some of the types of questions you'll answer during this process:

- Who owns my data?
- What types of data do I have?
- Where is my data?
- Why is it a risk?
- What methods can I use to classify my data?
- Where can I classify my data?
- How can I see what happens to my data over its lifecycle?

Data classification

Classification is the process of identifying and labeling content in your organization to get a better understanding of your data landscape. This is accomplished by applying one or more of the following to your data:

Capability	What problems does it solve?
Sensitive information types	Identifies sensitive data by using built-in or custom regular expressions or a function. Corroborative evidence includes keywords, confidence levels, and proximity.

Capability	What problems does it solve?
Trainable classifiers	Identifies sensitive data by using examples of the data you're interested in rather than identifying elements in the item (pattern matching). You can use built-in classifiers or train a classifier with your own content.
Data classification	A graphical identification of items in your organization that have a sensitivity label, a retention label, or have been classified. You can also use this information to gain insights into the actions that your users are taking on these items.
Polices	Sensitive information types, trainable classifiers, sensitivity labels, and retention labels act as inputs into policies. Policies define behaviors, like if there will be a default label, if labeling is mandatory, what locations the label will be applied to, and under what conditions.

What is a data classification framework?

Often codified in a formal, enterprise-wide policy, a data classification framework (sometimes called a 'data classification policy') is typically comprised of 3-5 classification levels. These usually include three elements: a name, description, and real-world examples.

Microsoft recommends no more than five top-level parent labels, each with five sub-labels (25 total) to keep the user interface (UI) manageable. Levels are typically arranged from least to most sensitive:

- Public
- Internal
- Confidential
- Highly Confidential

Other level name variations you may encounter include *Restricted*, *Unrestricted*, and *Consumer Protected*. Microsoft recommends label names that are self-descriptive and that highlight their relative sensitivity clearly. For example, *Confidential* and *Restricted* may leave users guessing which label is appropriate, while *Confidential* and *Highly Confidential* are clearer on which is more sensitive.

Another important component of a data classification framework is the controls associated with each level. Data classification levels by themselves are simply labels (or tags) that indicate the value or sensitivity of the content. To *protect* that content, data classification frameworks define the controls that should be in place for each of your data classification levels. These controls may include requirements related to:

- Storage type and location

- Encryption
- Access control
- Data destruction
- Data loss prevention
- Public disclosure
- Logging and tracking access
- Other control objectives, as needed

Custom sensitive data types

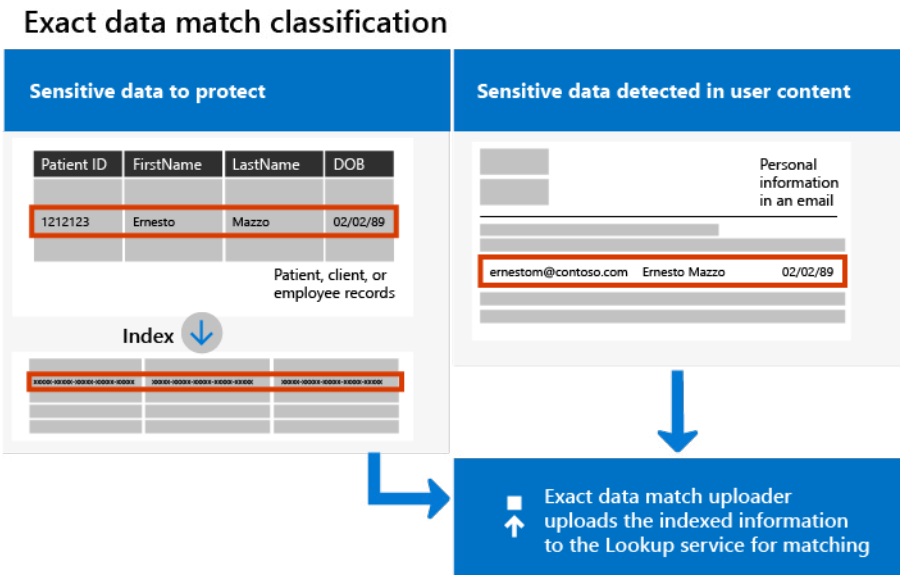
Sensitive information types are used to help identify sensitive items so that you can prevent them from being inadvertently or inappropriately shared, to help in locating relevant data in eDiscovery (Premium), and to apply governance actions to certain types of information. You define a custom sensitive information type (SIT) based on:

- patterns
- keyword evidence such as *employee*, *social security number*, or *ID*
- character proximity to evidence in a particular pattern
- confidence levels

But what if you wanted a custom sensitive information type (SIT) that uses exact or nearly exact data values, instead of one that found matches based on generic patterns? With Exact Data Match (EDM) based classification, you can create a custom sensitive information type that is designed to:

- be dynamic and easily refreshed
- be more scalable
- result in fewer false-positives
- work with structured sensitive data
- handle sensitive information more securely, not sharing it with anyone, including Microsoft
- be used with several Microsoft cloud services

It can include Exact Data Match (EDM) where a customer can take millions of pieces of data like SSNs or Credit Card numbers and use them to inform DLP or MCAS policies. The database can be updated dynamically. The database for this exact match can have up to 100 MM rows of data. This is really good for say if a retailer wants to put rules around sensitive information like Credit Card numbers with strict rules around the specific numbers it has for its customers and perhaps less strict rules for Credit Card numbers identified from the out of the box classifiers.



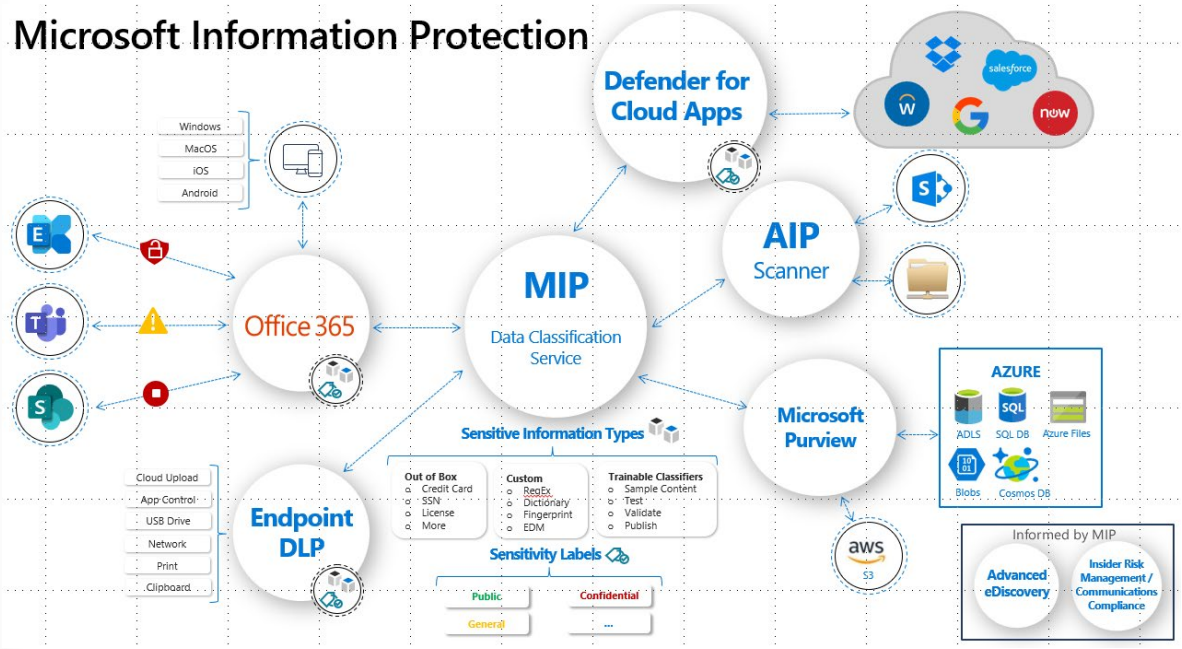
Data Protection

The data protection component essentially acts as an enforcement point where the policies regarding access to and sharing of different types of sensitive information are applied to the data that has been discovered across the data estate.

Microsoft Information Protection: Process and Capabilities

Information protection can be split into different phases depending on the product which is being used:

- Defender for Cloud Apps: Discover, Classify, Protect, Monitor. Microsoft Defender for Cloud Apps provides you with an expansive suite of DLP capabilities that cover the various data leak points that exist in organizations.
- Microsoft Purview: Know your data, Protect your data, Prevent Data loss, Govern your data. Microsoft Purview is a unified data governance service that helps you manage and govern your on-premises, multi-cloud, and software-as-a-service (SaaS) data. Create a holistic, up-to-date map of your data landscape with automated data discovery, sensitive data classification, and end-to-end data lineage. Enable data curators to manage and secure your data estate. Empower data consumers to find valuable, trustworthy data.



Purview Phase 1: Know your data

Automated data discovery and classification with Microsoft Purview

Microsoft Purview merges the phases of data discovery and classification under the pillar of “Know your data”.

To understand your data landscape and identify sensitive data across your hybrid environment, use the following capabilities:

Capability	What problems does it solve?	Get started
Sensitive information types	Identifies sensitive data by using built-in or custom regular expressions or a function. Corroborative evidence includes keywords, confidence levels, and proximity.	Customize a built-in sensitive information type
Trainable classifiers	Identifies sensitive data by using examples of the data you're interested in rather than identifying elements in the item (pattern matching). You can use built-in classifiers or train a classifier with your own content.	Get started with trainable classifiers

Capability	What problems does it solve?	Get started
Data classification	A graphical identification of items in your organization that have a sensitivity label, a retention label, or have been classified. You can also use this information to gain insights into the actions that your users are taking on these items.	Get started with content explorer
		Get started with activity explorer

Defender Phase 1: Discover your data

Automated data discovery with Defender for Cloud Apps:

1. **Connect apps:** The first step in discovering which data is being used in your organization is to connect cloud apps used in your organization to Defender for Cloud Apps. Once connected, Defender for Cloud Apps can scan data, add classifications, and enforce policies and controls. Depending on how apps are connected affects how and when scans and controls are applied. You can connect your apps in one of the following ways:
2. **Investigate**: After you connect an app to Defender for Cloud Apps using its API connector, Defender for Cloud Apps scans all the files it uses. You can then go to the file investigation page by clicking **Investigate** > **Files** to get an overview of the files shared by your cloud apps, their accessibility, and their status. For more information, see **Investigate files**[33].

33 https://docs.microsoft.com/defender-cloud-apps/file-filters

Use an app connector	Microsoft app connectors use the APIs supplied by app providers. They provide greater visibility into and control over the apps used in your organization. Scans are performed periodically (every 12 hours) and in real time (triggered each time a change is detected). For more information and instructions on how to add apps, see Connecting apps.
Use Conditional Access App Control	Conditional Access App Control solution uses a reverse proxy architecture that is uniquely integrated with Azure Active Directory (AD) Conditional Access. Once configured in Azure AD, users will be routed to Defender for Cloud Apps where access and session policies are enforced to protect the data apps attempt to use. This connection method allows you to apply controls to any app. For more information, see Protect apps with Defender for Cloud Apps Conditional Access App Control.

Defender Phase 2: Classify sensitive information

Data Classification with Defender for Cloud Apps is natively integrated with Microsoft Information Protection, which is part of Microsoft Purview.

Purview Phase 2: Protect your data (Phase 3 Defender)

Data protection with Microsoft Purview (including Defender for Cloud Apps as a capability):

Capability	What problems does it solve?	Get started
Sensitivity labels	A single solution across apps, services, and devices to label and protect your data as it travels inside and outside your organization.	Get started with sensitivity labels
	Example scenarios:	
	- Manage sensitivity labels for Office apps	
	- Encrypt documents and emails	
	- Apply and view labels in Power BI	
	For a comprehensive list of scenarios for sensitivity labels, see the Get started documentation.	

Capability	What problems does it solve?	Get started
Azure Information Protection unified labeling client	For Windows computers, extends labeling to File Explorer and PowerShell, with additional features for Office apps if needed	Azure Information Protection unified labeling client administrator guide
Double Key Encryption	Under all circumstances, only your organization can ever decrypt protected content or for regulatory requirements, you must hold encryption keys within a geographical boundary.	Deploy Double Key Encryption
Office 365 Message Encryption (OME)	Encrypts email messages and attached documents that are sent to any user on any device, so only authorized recipients can read emailed information.	Set up new Message Encryption capabilities
	Example scenario: Revoke email encrypted by Advanced Message Encryption	
Service encryption with Customer Key	Protects against viewing of data by unauthorized systems or personnel, and complements BitLocker disk encryption in Microsoft datacenters.	Set up Customer Key for Office 365
SharePoint Information Rights Management (IRM)	Protects SharePoint lists and libraries so that when a user checks out a document, the downloaded file is protected so that only authorized people can view and use the file according to policies that you specify.	Set up Information Rights Management (IRM) in SharePoint admin center
Rights Management connector	Protection-only for existing on-premises deployments that use Exchange or SharePoint Server, or file servers that run Windows Server and File Classification Infrastructure (FCI).	Steps to deploy the RMS connector
Azure Information Protection unified labeling scanner	Discovers, labels, and protects sensitive information that resides in data stores that are on premises.	Configuring and installing the Azure Information Protection unified labeling scanner
Microsoft Defender for Cloud Apps	Discovers, labels, and protects sensitive information that resides in data stores that are in the cloud.	Discover, classify, label, and protect regulated and sensitive data stored in the cloud

Capability	What problems does it solve?	Get started
Microsoft Purview Data Map	Identifies sensitive data and applies automatic labeling to content in Microsoft Purview Data Map assets. These include files in storage such as Azure Data Lake and Azure Files, and schematized data such as columns in Azure SQL DB, and Cosmos DB.	Labeling in Microsoft Purview Data Map
Microsoft Information Protection SDK	Extends sensitivity labels to third-party apps and services.	Microsoft Information Protection (MIP) SDK setup and configuration
	Example scenario: Set and get a sensitivity label (C++)	

Defender Phase 4: Monitor and report on your data

Monitoring and reporting is a greater emphasis in the data protection story with Defender for Cloud Apps.

Your policies are all in place to inspect and protect your data. Now, you'll want to **check your dashboard**[34] daily to see what new alerts have been triggered. It's a good place to keep an eye on the health of your cloud environment. Your dashboard helps you get a sense of what's happening and, if necessary, launch an **investigation**[35].

One of the most effective ways of monitoring sensitive file incidents is to head over to the **Policies** page and review the matches for policies you have configured. Additionally, if you configured alerts, you should also consider regularly monitoring file alerts by heading over to the **Alerts** page, specifying the category as **DLP**, and reviewing which file-related policies are being triggered. Reviewing these incidents can help you fine-tune your policies to focus on threats that are of interest to your organization.

In conclusion, managing sensitive information in this way ensures that data saved to the cloud has maximal protection from malicious exfiltration and infiltration. Also, if a file is shared or lost, authorized users can only access it.

34 https://docs.microsoft.com/defender-cloud-apps/daily-activities-to-protect-your-cloud-environment#check-the-dashboard
35 https://docs.microsoft.com/defender-cloud-apps/investigate

Purview Phase 4: Govern your data

In Microsoft Purview, governance consists of:

- Data Lifecycle Management
  - Retention policies for workloads
  - Inactive and archive mailboxes
- Records Management
  - Retention labels for items
  - Disposition review

Microsoft Purview Data Lifecycle Management

To keep what you need and delete what you don't:

Capability	What problems does it solve?
Retention policies for Microsoft 365 workloads, with retention labels for exceptions	Lets you retain or delete content with policy management for email, documents, Teams and Yammer messages.
Inactive mailboxes	Lets you retain mailbox content after employees leave the organization so that this content remains accessible to administrators, compliance officers, and records managers.
Archive mailboxes	Provides additional mailbox storage space for users.
Import service for PST files	Supports bulk-importing PST files to Exchange Online mailboxes to retain and search email messages for compliance or regulatory requirements.

Microsoft Purview Records Management

Manage high-value items for business, legal, or regulatory record-keeping requirements:

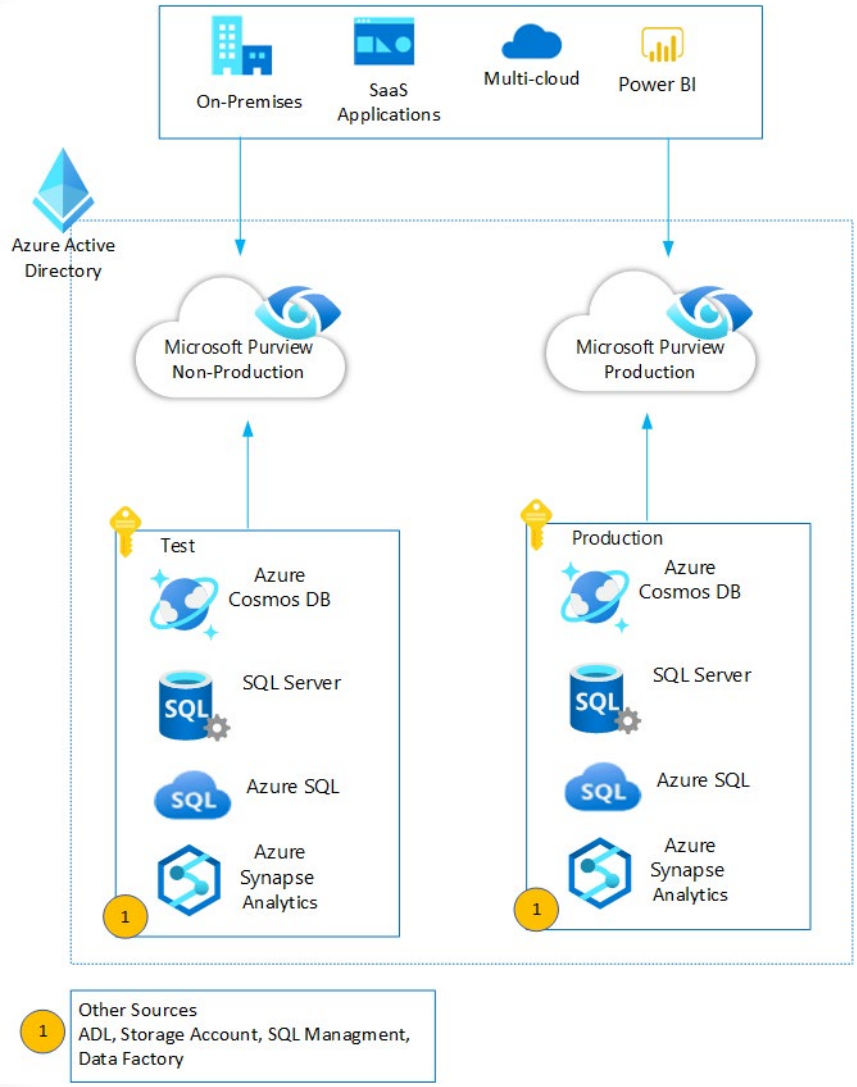
Capability	What problems does it solve?
File plan	Lets you create retention labels interactively or import in bulk, and export for analysis. Labels support additional administrative information (optional) to help you identify and track business or regulatory requirements.
Retention labels for individual items, retention policies if needed for baseline retention	Labels support flexible retention and deletion schedules that can be applied manually or automatically, with records declaration when needed.
Disposition review and proof of disposition	Manual review of content before it's permanently deleted, with proof of disposition of records.

Best Practices

Isolating production and non-production environments

Consider deploying separate instances of Microsoft Purview accounts for development, testing, and production environments, especially when you have separate instances of data for each environment.

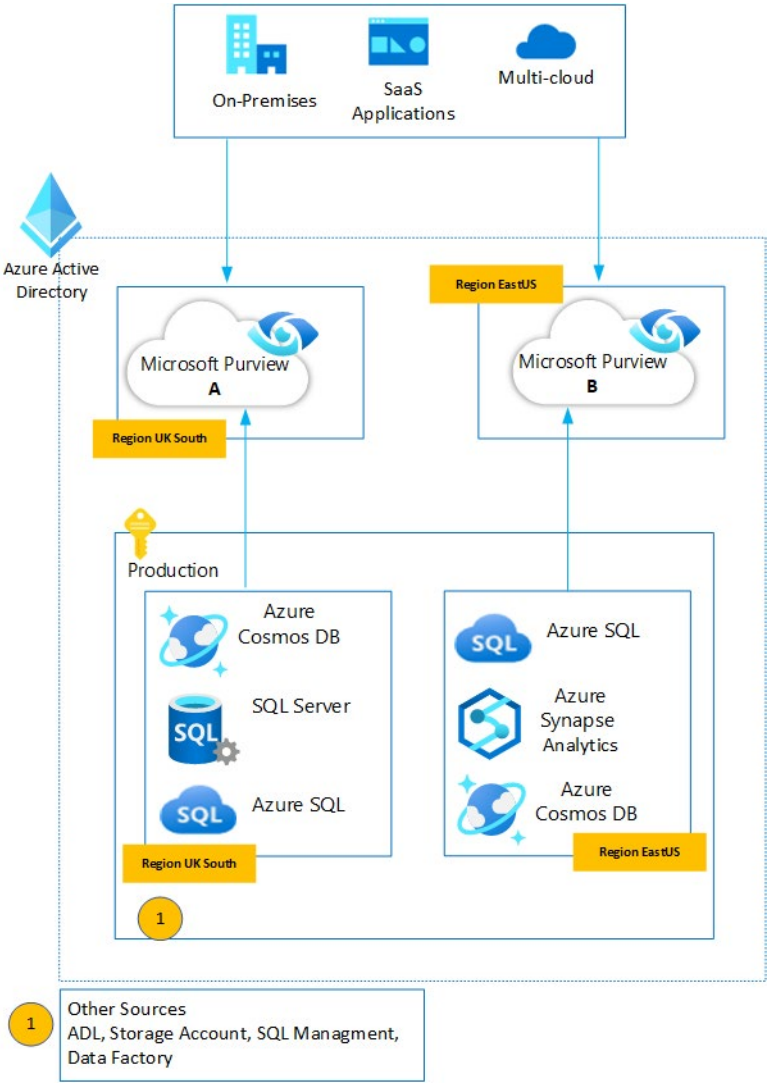
In this scenario, production and non-production data sources can be registered and scanned inside their corresponding Microsoft Purview instances. Optionally, you can register a data source in more than one Microsoft Purview instance, if needed.



Enforcing compliance Requirements

If your organization has data in multiple geographies and you must keep metadata in the same region as the actual data, you must deploy multiple Microsoft Purview instances, one for each geography. In this case, data

sources from each region should be registered and scanned in the Microsoft Purview account that corresponds to the data source region or geography.



More information about alert policies and searching the audit log:

- **Turn audit log search on or off**[36]
- **Search the audit log**[37]
- **Search-UnifiedAuditLog**[38] (cmdlet)
- **Detailed properties in the audit log**[39]

36 https://docs.microsoft.com/microsoft-365/compliance/turn-audit-log-search-on-or-off?view=o365-worldwide&preserve-view=true
37 https://docs.microsoft.com/microsoft-365/compliance/search-the-audit-log-in-security-and-compliance?view=o365-worldwide&preserve-view=true
38 https://docs.microsoft.com/powershell/module/exchange/search-unifiedauditlog
39 https://docs.microsoft.com/microsoft-365/compliance/detailed-properties-in-the-office-365-audit-log?view=o365-worldwide&preserve-view=true

Data Protection Best Practices

DP-1: Discover, classify and label sensitive data

Guidance: Microsoft Defender for Cloud Apps manages sensitive data; all data flow is covered by the Microsoft privacy review and SDL process. Customers have no ability to control the data,

DP-2: Protect sensitive data

Guidance: Microsoft Defender for Cloud Apps manages sensitive data and uses Azure Active Directory (Azure AD) roles to control permissions for different types of data.

- **Azure AD roles with access to Microsoft Defender for Cloud Apps**[40]

DP-3: Monitor for unauthorized transfer of sensitive data

Guidance: Monitor for unauthorized transfer of data to locations outside of enterprise visibility and control. This typically involves monitoring for abnormal activities (large or unusual transfers) that could indicate unauthorized data exfiltration.

DP-4: Encrypt sensitive information in transit

Microsoft Defender for Cloud Apps supports data encryption in transit with TLS v1.2 or greater. While this is optional for traffic on private networks, this is critical for traffic on external and public networks. Ensure that any clients connecting to your Azure resources can negotiate TLS v1.2 or greater for HTTP traffic. For remote management, use SSH (for Linux) or RDP/TLS (for Windows) instead of an unencrypted protocol. Obsolete SSL, TLS, SSH versions and protocols, and weak ciphers should be disabled.

By default, Azure provides encryption for data in transit between Azure data centers.

- **Microsoft Defender for Cloud Apps data security and privacy**[41]
- **Understand encryption in transit with Azure**[42]
- **Information on TLS Security**[43]
- **Double encryption for Azure data in transit**[44]

40 https://docs.microsoft.com/cloud-app-security/manage-admins#office-365-and-azure-ad-roles-with-access-to-cloud-app-security
41 https://docs.microsoft.com/cloud-app-security/cas-compliance-trust#encryption
42 https://docs.microsoft.com/azure/security/fundamentals/encryption-overview#encryption-of-data-in-transit
43 https://docs.microsoft.com/security/engineering/solving-tls1-problem
44 https://docs.microsoft.com/azure/security/fundamentals/double-encryption#data-in-transit

Specify an encryption standard for data at rest and in motion

Microsoft Defender for Cloud Apps encrypts data at rest to protect against 'out-of-band' attacks (such as accessing underlying storage) using encryption. This helps ensure that attackers can't easily read or modify the data.

- **Microsoft Defender for Cloud Apps data security and privacy**[45]
- **Understand encryption at rest in Azure**[46]
- **Data at rest double encryption in Azure**[47]

For additional information on Identifying and Protecting Sensitive Data, see the following:

- **Discover and Protect Sensitive Information**[48]
- **Sensitivity Labels**[49]
- **Information Protection**[50]
- **Microsoft Purview**[51]
- **Sensitive Information Types**[52]

To help protect data in the cloud, you need to account for the possible states in which your data can occur and what controls are available for that state. Best practices for Azure data security and encryption related to the following data states:

- **At rest:** This includes all information storage objects, containers, and types that exist statically on physical media, whether magnetic or optical disk.
- **In transit:** When data is being transferred between components, locations, or programs, it's in transit. Examples are transferred over the network, across a service bus (from on-premises to cloud and vice-versa, including hybrid connections such as ExpressRoute), or during an input/output process.

Azure provides double encryption for data at rest and data in transit. Double encryption is where two or more independent layers of encryption are enabled to protect against compromises of any one layer of encryption. Using two layers of encryption mitigates threats that come with encrypting data.

45 https://docs.microsoft.com/cloud-app-security/cas-compliance-trust#encryption
46 https://docs.microsoft.com/azure/security/fundamentals/encryption-atrest#encryption-at-rest-in-microsoft-cloud-services
47 https://docs.microsoft.com/azure/security/fundamentals/encryption-atrest
48 https://docs.microsoft.com/defender-cloud-apps/tutorial-dlp
49 https://docs.microsoft.com/defender-cloud-apps/use-case-information-protection
50 https://docs.microsoft.com/defender-cloud-apps/use-case-admin-quarantine
51 https://docs.microsoft.com/azure/purview/overview
52 https://docs.microsoft.com/microsoft-365/compliance/sensitive-information-type-entity-definitions?view=o365-worldwide&preserve-view=true

Encryption of data at rest

Data at rest includes information that resides in persistent storage on physical media, in any digital format. The media can include magnetic or optical media files, archived data, and data backups. Microsoft Azure offers a variety of data storage solutions to meet different needs, including file, disk, blob, and table storage. Microsoft also provides encryption to protect **Azure SQL Database**[53], **Azure Cosmos DB**[54], and Azure Data Lake.

Data encryption at rest is available for services across the software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS) cloud models. This article summarizes and provides resources to help you use the Azure encryption options.

Azure encryption of data at rest models

Azure supports various encryption models, including server-side encryption that uses service-managed keys, customer-managed keys in Key Vault, or customer-managed keys on customer-controlled hardware. You can manage and store keys on-premises or in another secure location with client-side encryption.

Client-side encryption	Client-side encryption is performed outside of Azure. It includes:
	Data is encrypted by an application running in the customer's datacenter or by a service application.
	Data that is already encrypted when Azure receives it.
	With client-side encryption, cloud service providers don't have access to the encryption keys and can't decrypt this data. You maintain complete control of the keys.
Server-side encryption	The three server-side encryption models offer different key management characteristics, which you can choose according to your requirements:
	Service-managed keys: Provides a combination of control and convenience with low overhead.
	Customer-managed keys: Gives you control over the keys, including Bring Your Own Keys (BYOK) support, or allows you to generate new ones.
	Service-managed keys in customer-controlled hardware: Enables you to manage keys in your proprietary repository, outside of Microsoft control. This characteristic is called Host Your Own Key (HYOK). However, the configuration is complex, and most Azure services don't support this model.

53 https://docs.microsoft.com/azure/azure-sql/database/sql-database-paas-overview
54 https://docs.microsoft.com/azure/cosmos-db/database-encryption-at-rest

Encryption of data in transit

Azure offers many mechanisms for keeping data private as it moves from one location to another.

- **Data-link Layer encryption in Azure** - Whenever Azure Customer traffic moves between data-centers– outside physical boundaries not controlled by Microsoft (or on behalf of Microsoft)– a data-link layer encryption method using the IEEE 802.1AE MAC Security Standards (also known as MACsec) is applied from point-to-point across the underlying network hardware. The packets are encrypted and decrypted on the devices before being sent, preventing physical man-in-the-middle or snooping/wiretapping attacks. Because this technology is integrated on the network hardware itself, it provides line rate encryption on the network hardware with no measurable link latency increase. This MACsec encryption is on by default for all Azure traffic traveling within a region or between regions, and no action is required on customers' part to enable.
- **TLS encryption in Azure** - Microsoft gives customers the ability to use Transport Layer Security (TLS) protocol to protect data when it's traveling between the cloud services and customers. Microsoft datacenters negotiate a TLS connection with client systems that connect to Azure services. TLS provides strong authentication, message privacy, and integrity (enabling detection of message tampering, interception, and forgery), interoperability, algorithm flexibility, and ease of deployment and use.
- **Perfect Forward Secrecy (PFS)** - protects connections between customers' client systems and Microsoft cloud services by unique keys. Connections also use RSA-based 2,048-bit encryption key lengths. This combination makes it difficult for someone to intercept and access data that is in transit.
- **Azure Storage transactions** - When you interact with Azure Storage through the Azure portal, all transactions take place over HTTPS. You can also use the Storage REST API over HTTPS to interact with Azure Storage. You can enforce the use of HTTPS when you call the REST APIs to access objects in storage accounts by enabling the secure transfer that's required for the storage account.
- **Shared Access Signatures (SAS)** - can be used to delegate access to Azure Storage objects, include an option to specify that only the HTTPS protocol can be used when you use Shared Access Signatures. This approach ensures that anybody who sends links with SAS tokens uses the proper protocol.

    - SMB 3.0, which used to access Azure Files shares, supports encryption, and it's available in Windows Server 2012 R2, Windows 8, Windows 8.1, and Windows 10. It allows cross-region access and even access on the desktop.
    - Client-side encryption encrypts the data before it's sent to your Azure Storage instance, so that it's encrypted as it travels across the network.
- **SMB encryption over Azure virtual networks** - By using SMB 3.0 in VMs that are running Windows Server 2012 or later, you can make data transfers secure by encrypting data in transit over Azure Virtual Networks. By encrypting data, you help protect against tampering and eavesdropping attacks. Administrators can enable SMB encryption for the entire server, or just specific shares.

    - By default, after SMB encryption is turned on for a share or server, only SMB 3.0 clients are allowed to access the encrypted shares.
- **Point-to-site VPNs** - Point-to-site VPNs allow individual client computers access to an Azure virtual network. The Secure Socket Tunneling Protocol (SSTP) is used to create the VPN tunnel. It can traverse firewalls (the tunnel appears as an HTTPS connection). You can use your own internal public key infrastructure (PKI) root certificate authority (CA) for point-to-site connectivity.

- **Site-to-site VPNs** -You can use a site-to-site VPN gateway connection to connect your on-premises network to an Azure virtual network over an IPsec/IKE (IKEv1 or IKEv2) VPN tunnel. This type of connection requires an on-premises VPN device that has an external-facing public IP address assigned to it.

Azure data security and encryption best practices

Choose a key management solution

You can use Key Vault to create multiple secure containers, called vaults. These vaults are backed by HSMs. Vaults help reduce the chances of accidental loss of security information by centralizing the storage of application secrets. Key vaults also control and log the access to anything stored in them. Azure Key Vault can handle requesting and renewing Transport Layer Security (TLS) certificates. It provides features for a robust solution for certificate lifecycle management.

Best practice: Grant access to users, groups, and applications at a specific scope.
Detail: Use Azure RBAC predefined roles. For example, to grant access to a user to manage key vaults, you would assign the predefined role **Key Vault Contributor**[55] to this user at a specific scope. The scope in this case would be a subscription, a resource group, or just a specific key vault. If the predefined roles don't fit your needs, you can **define your own roles**[56].

Best practice: Control what users have access to.
Detail: Access to a key vault is controlled through two separate interfaces: the management and data plane. The management plane and data plane access controls work independently.

Best practice: Store certificates in your key vault. Your certificates are of high value. In the wrong hands, your application's security or the security of your data can be compromised.
Detail: Azure Resource Manager can securely deploy certificates stored in Azure Key Vault to Azure VMs when the VMs are deployed. By setting appropriate access policies for the key vault, you also control who gets access to your certificate. Another benefit is that you manage all your certificates in one place in Azure Key Vault. See **Deploy Certificates to VMs from customer-managed Key Vault**[57] for more information.

Best practice: Ensure that you can recover a deletion of key vaults or key vault objects.
Detail: Deletion of key vaults or key vault objects can be inadvertent or malicious. Enable the soft delete and purge protection

55 https://docs.microsoft.com/azure/role-based-access-control/built-in-roles
56 https://docs.microsoft.com/azure/role-based-access-control/custom-roles
57 https://docs.microsoft.com/archive/blogs/kv/updated-deploy-certificates-to-vms-from-customer-managed-key-vault

features of Key Vault, particularly for keys used to encrypt data at rest. Deleting these keys is equivalent to data loss, so you can recover deleted vaults and vault objects if needed. Practice Key Vault recovery operations regularly.

Manage with secure workstations

Because the vast majority of attacks target the end user, the endpoint becomes one of the primary points of attack. An attacker who compromises the endpoint can use the user's credentials to gain access to the organization's data. Most endpoint attacks take advantage of users' administrators in their local workstations.

Best practice: Use a secure management workstation to protect sensitive accounts, tasks, and data.
Detail: Use a **privileged access workstation**[58] to reduce the attack surface in workstations. These secure management workstations can help you mitigate some of these attacks and ensure that your data is safer.

Best practice: Ensure endpoint protection.
Detail: Enforce security policies across all devices used to consume data, regardless of the data location (cloud or on-premises).

Protect data at rest

Organizations that don't enforce data encryption are more exposed to data-confidentiality issues. For example, unauthorized or rogue users might steal data in compromised accounts or gain unauthorized access to data coded in Clear Format. Companies also must prove that they're diligent and using correct security controls to enhance their data security to comply with industry regulations.

Best practice: Apply disk encryption to help safeguard your data.
Detail: Use **Azure Disk Encryption**[59].
It enables IT administrators to encrypt Windows and Linux IaaS VM disks. Disk Encryption combines the industry-standard Windows BitLocker feature and the Linux dm-crypt feature to provide volume encryption for the OS and the data disks.

Azure Storage and Azure SQL Database encrypt data at rest by default, and many services offer encryption as an option. You can use Azure Key Vault to maintain control of keys that access and encrypt your data.
See **Azure resource providers encryption model support to learn more**[60].

Best practices: Use encryption to help mitigate risks related to unauthorized data access.
Detail: Encrypt your drives before you write sensitive data to them.

58 https://4sysops.com/archives/understand-the-microsoft-privileged-access-workstation-paw-security-model/
59 https://docs.microsoft.com/azure/security/fundamentals/azure-disk-encryption-vms-vmss
60 https://docs.microsoft.com/azure/security/fundamentals/encryption-atrest#azure-resource-providers-encryption-model-support

Protect data in transit

Protecting data in transit should be essential for your data protection strategy. Because data is moving back and forth from many locations, we generally recommend that you always use SSL/TLS protocols to exchange data across different locations. In some circumstances, you might want to isolate the entire communication channel between your on-premises and cloud infrastructures by using a VPN.

Best practice: Secure access from multiple workstations located on-premises to an Azure virtual network.
Detail: Use a **site-to-site VPN**[61].

Best practice: Secure access from an individual workstation located on-premises to an Azure virtual network.
Detail: Use a **point-to-site VPN**[62].

Best practice: Move larger data sets over a dedicated high-speed WAN link.
Detail:
Use **ExpressRoute**[63].
If you choose to use ExpressRoute, you can also encrypt the data at the application level by using SSL/TLS or other protocols for added protection.

Best practice: Interact with Azure Storage through the Azure portal.
Detail: All transactions occur via HTTPS. You can also use **Storage REST API**[64] over HTTPS to interact with **Azure Storage**[65].

Key management with Key Vault

Without proper protection and management of the keys, encryption is rendered useless. Key Vault is the Microsoft-recommended solution for managing and controlling access to encryption keys used by cloud services. Permissions to access keys can be assigned to services or users through Azure Active Directory accounts. Key Vault relieves organizations of configuring, patching, and maintaining hardware security modules (HSMs) and key management software.

Azure Key Vault helps solve the following problems:

- **Secrets Management** - Azure Key Vault can be used to Securely store and tightly control access to tokens, passwords, certificates, API keys, and other secrets

61 https://docs.microsoft.com/azure/vpn-gateway/tutorial-site-to-site-portal
62 https://docs.microsoft.com/azure/vpn-gateway/vpn-gateway-howto-point-to-site-classic-azure-portal
63 https://docs.microsoft.com/azure/expressroute/expressroute-introduction
64 https://docs.microsoft.com/rest/api/storageservices/
65 https://azure.microsoft.com/services/storage/

- **Key Management** - Azure Key Vault can be used as a Key Management solution. Azure Key Vault makes it easy to create and control the encryption keys used to encrypt your data.
- **Certificate Management** - Azure Key Vault lets you easily provision, manage, and deploy public and private Transport Layer Security/Secure Sockets Layer (TLS/SSL) certificates for use with Azure and your internal connected resources.

For additional information on Encryption Standards, see the following:

- **Azure Encryption Overview**[66]
- **Data Encryption Best Practices**[67]
- **Protect Sensitive Information**[68]

Exercise

Meet Tailwind Traders

Tailwind Trader is a fictitious home improvement retailer. It operates retail hardware stores across the globe and online. The Tailwind Traders CISO is aware of the opportunities offered by Azure but also understands the need for strong security and solid cloud architecture. Without strong security and a great point of reference architecture, the company may have difficulty managing the Azure environment and costs, which are hard to track and control. The CISO is interested in understanding how Azure manages and enforces security standards.

Requirements

Tailwind Traders plans to make some significant changes to their Data Security Strategy. Currently, they're using the Waterfall development cycle to manage all applications. They have asked for your assistance with recommendations and questions. Here are the specific requirements.

- **Data Security.** The company has a new security optimization project for customer environments. The CISO wants to ensure that all data in rest and transit are secured and controlled in the cloud.

Tasks

Evaluate a Data Security Strategy

- What could Tailwind Traders evaluate to design a Data Security Strategy?

66 https://docs.microsoft.com/azure/security/fundamentals/encryption-overview
67 https://docs.microsoft.com/azure/security/fundamentals/data-encryption-best-practices
68 https://docs.microsoft.com/defender-cloud-apps/use-case-proxy-block-session-aad

- Evaluate a standard and explain your decision-making process.
- Tailwind Traders should evaluate the Data Protection Best Practices to Discover, Protect, Monitor, and Encrypt Sensitive Data.
- What security strategy could be used to Protect Data in Transit?
- Tailwind Traders should secure access from individual and multiple workstations located on-premises to an Azure virtual network by using Point-to-Site VPN or Site-to-Site VPN.

How are you enforcing Data Security for all users to protect their identity, data, and other assets in Microsoft Azure?

Summary

In this module, you've learned how to build an overall data security strategy. You have learned different strategies for designing, defining, and recommending an organizational application security strategy and architecture. You should now be able to:

- Prioritize mitigating threats to data
- Design a strategy to identify and protect sensitive data
- Specify an encryption standard for data at rest and in motion

Learn more with Azure documentation

- **Best practices for protecting your organization**[69]
- **Discover and protect sensitive information in your organization tutorial**[70]
- **Protect any apps in use in your organization in real time tutorial**[71]
- **Data security and encryption best practices - Microsoft Azure**[72]

69 https://docs.microsoft.com/defender-cloud-apps/best-practices
70 https://docs.microsoft.com/defender-cloud-apps/tutorial-dlp
71 https://docs.microsoft.com/defender-cloud-apps/tutorial-proxy
72 https://docs.microsoft.com/azure/security/fundamentals/data-encryption-best-practices

Knowledge check

Check your knowledge

Multiple choice

Item 1. How can Tailwind Traders enforce security assurance for new applications in their Azure environment?

- ☐ Securing an application requires security assurances for three different component types: application code, application services, and application hosting platform.
- ☐ Use identity for authentication rather than directly handling keys.
- ☐ Always authenticate with identity services rather than cryptographic keys when available.

Multiple choice

Item 2. What security standard or model can Tailwind Traders use to secure modern applications?

- ☐ STRIDE
- ☐ NIST SP 800-63-1
- ☐ ISO 27001

Multiple choice

Item 3. What can Tailwind Traders do to ensure the organization's data is encrypted to protect against compromises of any layer of encryption?

- ☐ Use Azure encryption services to enforce double encryption to provide two or more independent layers of encryption to protect against compromises.
- ☐ Detect activity from unexpected locations or countries.
- ☐ Identify and control sensitive information (DLP); respond to sensitivity labels on content.

Multiple choice

Item 4. How can Tailwind Traders discover and manage Shadow IT in their network?

- ☐ Monitor user activities for anomalies, protect data when it is exfiltrated, and prevent unprotected data from uploading to apps.
- ☐ Encrypt sensitive information in transit.
- ☐ Create a block download policy for unmanaged devices.

Multiple choice

Item 5. What can Tailwind Traders do to classify sensitive information in the Azure environment?

- ☐ Define which information is sensitive by using Microsoft Information Protection.
- ☐ Tune anomaly policies set IP ranges, and send feedback for alerts.
- ☐ Ensure that sensitive data relevant to Web APIs isn't stored in the browser's storage.

Answers

Multiple choice

Item 1. How can Tailwind Traders enforce security assurance for new applications in their Azure environment?

- ■ Securing an application requires security assurances for three different component types: application code, application services, and application hosting platform.
- ☐ Use identity for authentication rather than directly handling keys.
- ☐ Always authenticate with identity services rather than cryptographic keys when available.

Explanation
Application security assurance includes code, services and the hosting platform. The decision about how to do authentication is a more fundamental decision that should be prioritized before onboarding new applications.

Multiple choice

Item 2. What security standard or model can Tailwind Traders use to secure modern applications?

- ■ STRIDE
- ☐ NIST SP 800-63-1
- ☐ ISO 27001

Explanation
STRIDE is a model for identifying computer security threats in six different categories. NIST SP 800-63-1 offers general guidelines on electronic authentication, but doesn't specifically address securing modern applications. ISO 27001 provides general guidance on securing information systems, but is not the best choice for specific guidance on securing modern applications.

Multiple choice

Item 3. What can Tailwind Traders do to ensure the organization's data is encrypted to protect against compromises of any layer of encryption?

- ■ Use Azure encryption services to enforce double encryption to provide two or more independent layers of encryption to protect against compromises.
- ☐ Detect activity from unexpected locations or countries.
- ☐ Identify and control sensitive information (DLP); respond to sensitivity labels on content.

Explanation
Double encryption is the correct approach. The other strategies allow you to prioritize cloud threats and identify and protect sensitive data.

Multiple choice

Item 4. How can Tailwind Traders discover and manage Shadow IT in their network?

- ■ Monitor user activities for anomalies, protect data when it is exfiltrated, and prevent unprotected data from uploading to apps.
- ☐ Encrypt sensitive information in transit.
- ☐ Create a block download policy for unmanaged devices.

Explanation
Managing shadow IT includes monitoring user activy, protecting against data exfiltration and preventing unprotected data from being uploaded elsewhere.

Multiple choice

Item 5. What can Tailwind Traders do to classify sensitive information in the Azure environment?

- ■ Define which information is sensitive by using Microsoft Information Protection.
- ☐ Tune anomaly policies set IP ranges, and send feedback for alerts.
- ☐ Ensure that sensitive data relevant to Web APIs isn't stored in the browser's storage.

Explanation
Defining sensitive information with Microsoft Information Protection is key to classifying sensitive information in Azure. Tuning anomaly policies will help with prioritizing cloud threats. Preventing Web API data from being stored in the browsers cache will help mitigate threats to data.