Microsoft

Microsoft Official Course

SC-900T00

Security, Compliance, and Identity Fundamentals

SC-900T00

Security, Compliance, and Identity Fundamentals

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 Course Introduction

About this course

About this course

Course Description

This course provides foundational level knowledge on security, compliance, and identity concepts and related cloud-based Microsoft solutions.

Level:

Beginner

Audience

This course is targeted to those looking to familiarize themselves with the fundamentals of security, compliance, and identity (SCI) across cloud based and related Microsoft services.

This is a broad audience that may include business stakeholders, new or existing IT professionals, or students that have an interest in Microsoft security, compliance, and identity solutions.

The person taking this content should be familiar with Microsoft Azure and Microsoft 365 and wants to understand how Microsoft security, compliance, and identity solutions can span across these solution areas to provide a holistic and end-to-end solution.

The content for this course aligns to the SC-900 exam objective domain.

Prerequisites

- General understanding of networking and cloud computing concepts.
- General IT knowledge or any general experience working in an IT environment.
- General understanding of Microsoft Azure and Microsoft 365.

Expected learning

- Describe basic concepts of security, compliance, and identity.
- Describe the concepts and capabilities of Microsoft identity and access management solutions.

- Describe the capabilities of Microsoft security solutions.
- Describe the compliance management capabilities in Microsoft.

Course Syllabus

Module 1 - Describe basic concepts of security, compliance, and identity

Learn about core concepts, principles, and methodologies that are foundational to security, compliance, and identity solutions, including Zero-Trust, shared responsibility, our privacy principles, and more.

- Lesson 1 - Describe security and compliance concepts and methodologies.
- Lesson 2 - Describe identity concepts.

Module 2 - Describe the capabilities of Microsoft identity and access management solutions

Learn about Azure AD services and identity principals, secure authentication, access management capabilities, as well as identity protection and governance.

- Lesson 1 - Describe the basic services and identity types of Azure AD.
- Lesson 2 - Describe the authentication capabilities of Azure AD.
- Lesson 3 - Describe the access management capabilities of Azure AD.
- Lesson 4 - Describe the identity protection and governance capabilities of Azure AD.

Module 3 - Describe the capabilities of Microsoft security solutions

Learn about security capabilities in Microsoft. Topics covered will include network and platform capabilities of Azure, Azure security management, and Sentinel. You'll learn about threat protection with Microsoft 365 Defender, Microsoft 365 security management, and endpoint security.

- Lesson 1 - Describe the basic security capabilities in Azure.
- Lesson 2 - Describe the security management capabilities of Azure.
- Lesson 3 - Describe the security capabilities of Azure Sentinel.
- Lesson 4 - Describe the threat protection capabilities of Microsoft 365.
- Lesson 5 - Describe the security management capabilities of Microsoft 365.
- Lesson 6 - Describe endpoint security with Microsoft Intune.

Module 4 - Describe the compliance management capabilities in Microsoft

Learn about compliance solutions in Microsoft. Topics covered will include Compliance center, Information protection and governance in Microsoft 365, Insider Risk, audit, and eDiscovery solutions. Also covered are Azure resources governance capabilities.

- Lesson 1 - Describe the capabilities of Microsoft compliance solutions.
- Lesson 2 - Describe the information protection and governance capabilities of Microsoft 365.
- Lesson 3 - Describe the insider risk capabilities in Microsoft 365.
- Lesson 4 - Describe the eDiscovery and audit capabilities of Microsoft 365.
- Lesson 5 - Describe the resource governance capabilities in Azure.

SC-900 Certification Exam

The **SC-900**
Microsoft Security, Compliance, and Identity Fundamentals[1] certification exam is designed for candidates looking to demonstrate foundational level knowledge of security, compliance, and identity (SCI) across cloud-based and related Microsoft services.

This audience is broad and may include business stakeholders, new or existing IT professionals, or students who have an interest in Microsoft security, compliance, and identity solutions.

Candidates should be familiar with Microsoft Azure and Microsoft 365 and want to understand how Microsoft security, compliance, and identity solutions can span across these solution areas to provide a holistic and end-to-end solution.

This exam can be taken as an **optional** first step in learning about Microsoft security, compliance, and identity. While it would be a beneficial first step, validating foundational level knowledge, taking this exam is not a pre-requisite before taking any other Microsoft security-based certifications.

The exam includes four study areas. The percentages indicate the relative weight of each area on the exam. The higher the percentage, the more questions the exam will contain. Be sure to read the exam page for specifics about what skills are covered in each area.

SC-900 Study Areas	Weights
Describe the Concepts of Security, Compliance, and Identity	5-10%
Describe the capabilities of Microsoft Identity and Access Management Solutions	25-30%
Describe the capabilities of Microsoft Security Solutions	30-35%
Describe the Capabilities of Microsoft Compliance Solutions	25-30%

✓ This exam does not include a hands-on testing component.

1 https://docs.microsoft.com/learn/certifications/exams/sc-900

Module 1 Describe the concepts of security, compliance, and identity

Describe security and compliance concepts and methodologies

Introduction

As more business data is being accessed away from locations outside of the traditional corporate network, security has become an overriding concern. Organizations need to understand how they can best protect their data, regardless of where it's accessed from and whether it sits on their corporate network, or in the cloud.

This lesson introduces some important security concepts and methodologies. You'll learn about the Zero Trust model, the shared responsibility model, and defense in depth. You'll also cover common cyber security threats. The lesson introduces encryption and hashing as ways to protect data. Lastly, you will learn about the cloud adoption framework to guide adoption to the cloud.

After completing this lesson, you'll be able to:

- Describe the Zero Trust and shared responsibility models.
- Describe common security threats and ways to protect through the defense in-depth security model.
- Describe the concepts of encryption and hashing.
- Describe the cloud adoption framework.

Describe the Zero-Trust methodology

Zero Trust assumes everything is on an open and untrusted network, even resources behind the firewalls of the corporate network. The Zero Trust model operates on the principle of "**trust no one, verify everything.**"

Attackers' ability to bypass conventional access controls is ending any illusion that traditional security strategies are sufficient. By no longer trusting the integrity of the corporate network, security is strengthened.

In practice, this means that we no longer assume that a password is sufficient to validate a user so we add multi-factor authentication to provide additional checks. Instead of granting access to all devices on the corporate network, users are allowed access only to the specific applications or data that they need.

Zero Trust guiding principles

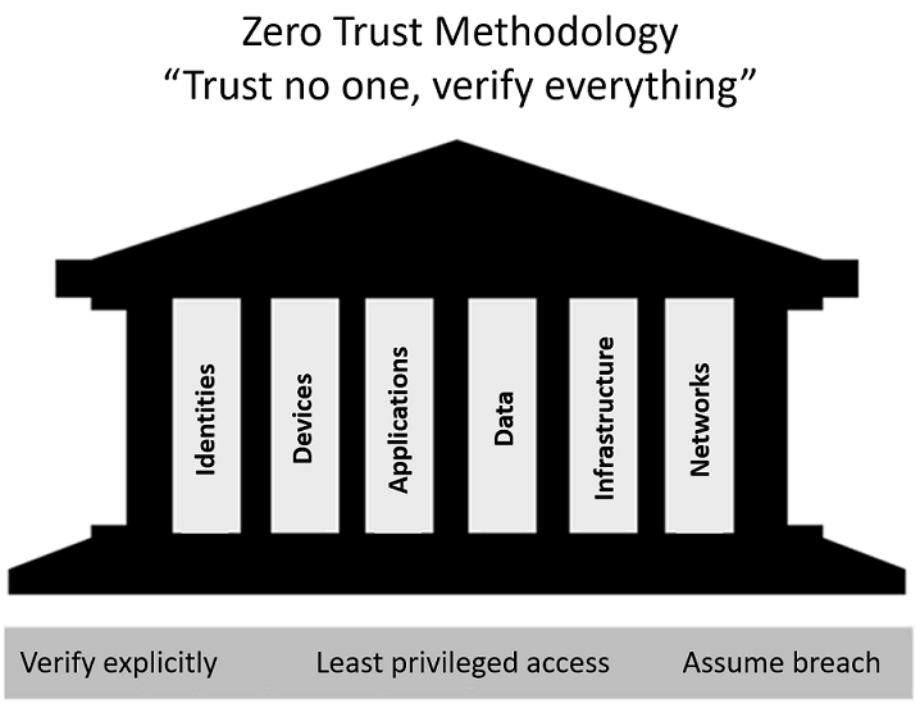
The Zero Trust model has three principles which guide and underpin how security is implemented. These are: verify explicitly, least privilege access, and assume breach.

- **Verify explicitly**. Always authenticate and authorize based on the available data points, including user identity, location, device, service or workload, data classification, and anomalies.
- **Least privileged access**. Limit user access with just-in-time and just-enough access (JIT/JEA), risk-based adaptive policies, and data protection to protect both data and productivity.
- **Assume breach**. Segment access by network, user, devices, and application. Use encryption to protect data, and use analytics to get visibility, detect threats, and improve your security.

Six foundational pillars

In the Zero Trust model, all elements work together to provide end-to-end security. These six elements are the foundational pillars of the Zero Trust model:

- **Identities** may be users, services, or devices. When an identity attempts to access a resource, it must be verified with strong authentication, and follow least privilege access principles.
- **Devices** create a large attack surface as data flows from devices to on-premises workloads and the cloud. Monitoring devices for health and compliance is an important aspect of security.
- **Applications** are the way that data is consumed. This includes discovering all applications being used, sometimes called Shadow IT because not all applications are managed centrally. This pillar also includes managing permissions and access.
- **Data** should be classified, labeled, and encrypted based on its attributes. Security efforts are ultimately about protecting data, and ensuring it remains safe when it leaves devices, applications, infrastructure, and networks that the organization controls.
- **Infrastructure**, whether on-premises or cloud based, represents a threat vector. To improve security, you assess for version, configuration, and JIT access, and use telemetry to detect attacks and anomalies. This allows you to automatically block or flag risky behavior and take protective actions.
- **Networks** should be segmented, including deeper in-network micro segmentation. Also, real-time threat protection, end-to-end encryption, monitoring, and analytics should be employed.



These six foundational pillars work together with the Zero Trust model to enforce organization security policies.

Refer to **An introduction to the Zero Trust methodology**[1] for a video recap on the pillars of the Zero Trust model.

Describe the shared responsibility model

The shared responsibility model identifies which security tasks are handled by the cloud provider, and which security tasks are handled by you, the customer.

In organizations running only on-premises hardware and software, the organization is 100 percent responsible for implementing security and compliance. With cloud-based services, that responsibility is shared between the customer and the cloud provider.

The responsibilities vary depending on where the workload is hosted:

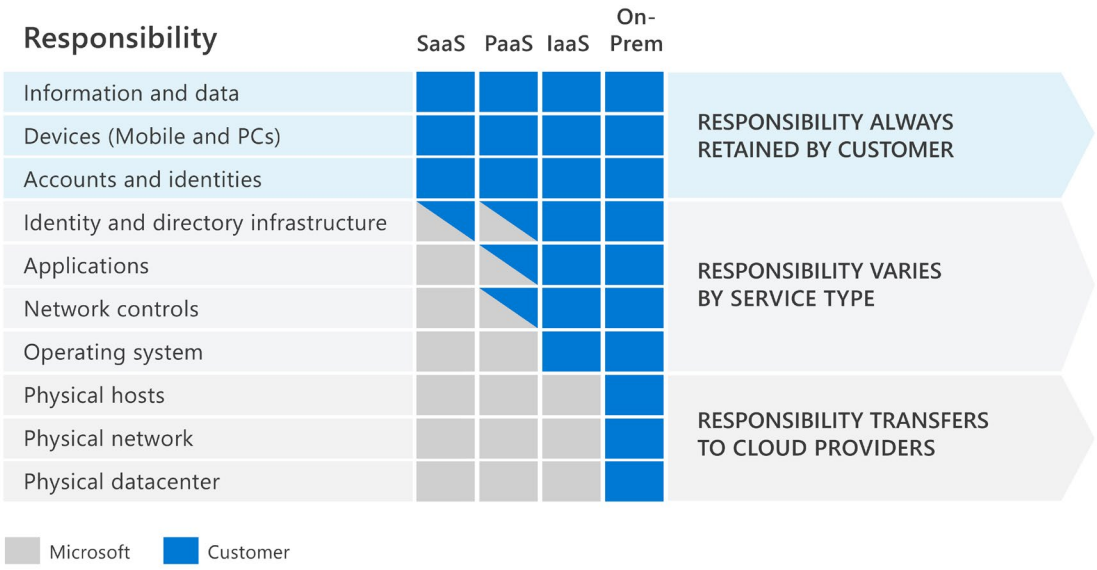
- Software as a Service (SaaS)
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)
- On-premises datacenter (On-prem)

The shared responsibility model makes responsibilities clear. When organizations move data to the cloud, some responsibilities transfer to the cloud provider and some to the customer organization.

The following diagram illustrates the areas of responsibility between the customer and the cloud provider, according to where data is held.

1 https://www.microsoft.com/videoplayer/embed/RE4J3ms

Shared responsibility model



On-premises datacenters

In an on-premises datacenter, you have responsibility for everything from physical security to encrypting sensitive data.

Infrastructure as a Service (IaaS)

Of all cloud services, IaaS requires the most management by the cloud customer. With IaaS, you're using the cloud provider's computing infrastructure. The cloud customer isn't responsible for the physical components, such as computers and the network, or the physical security of the datacenter. However, the cloud customer still has responsibility for software components such as operating systems, network controls, applications, and protecting data.

Platform as a Service (PaaS)

PaaS provides an environment for building, testing, and deploying software applications. The goal of PaaS is to help you create an application quickly without managing the underlying infrastructure. With PaaS, the cloud provider manages the hardware and operating systems, and the customer is responsible for applications and data.

Software as a Service (SaaS)

SaaS is hosted and managed by the cloud provider, for the customer. It's usually licensed through a monthly or annual subscription. Microsoft 365, Skype, and Dynamics 365 are all examples of SaaS software. SaaS requires the least amount of management by the cloud customer. The cloud provider is responsible for managing everything except data, devices, accounts, and identities.

For all cloud deployment types you, the cloud customer, own your data and identities. You're responsible for protecting the security of your data and identities, and on-premises resources.

In summary, responsibilities always retained by the customer organization include:

- Information and data
- Devices (mobile and PCs)
- Accounts and identities

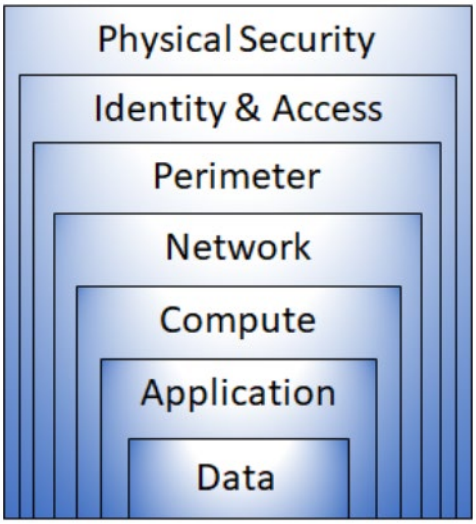
The benefit of the shared responsibility model is that organizations are clear about their responsibilities, and those of the cloud provider.

Describe defense in depth

Defense in depth uses a layered approach to security, rather than relying on a single perimeter. A defense in-depth strategy uses a series of mechanisms to slow the advance of an attack. Each layer provides protection so that, if one layer is breached, a subsequent layer will prevent an attacker getting unauthorized access to data.

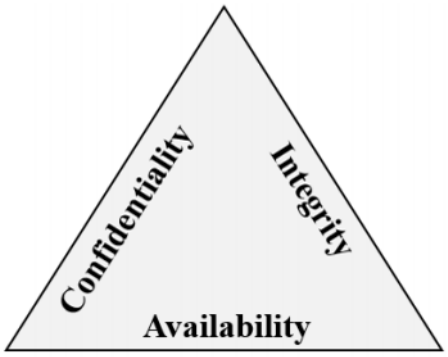
Example layers of security might include:

- **Physical** security such as limiting access to a datacenter to only authorized personnel.
- **Identity and access** security controls, such as multi-factor authentication or condition-based access, to control access to infrastructure and change control.
- **Perimeter** security including distributed denial of service (DDoS) protection to filter large-scale attacks before they can cause a denial of service for users.
- **Network** security, such as network segmentation and network access controls, to limit communication between resources.
- **Compute** layer security such as securing access to virtual machines either on-premises or in the cloud by closing certain ports.
- **Application** layer security to ensure applications are secure and free of security vulnerabilities.
- **Data** layer security including controls to manage access to business and customer data and encryption to protect data.



Confidentiality, Integrity, Availability (CIA)

Confidentiality, Integrity, Availability, or CIA, is a way to think about security trade-offs. This isn't a Microsoft model, but is common to all security professionals.



Confidentiality refers to the need to keep confidential sensitive data such as customer information, passwords, or financial data. You can encrypt data to keep it confidential, but then you also need to keep the encryption keys confidential. Confidentiality is the most visible part of security; we can clearly see need for sensitive data, keys, passwords, and other secrets to be kept confidential.

Integrity refers to keeping data or messages correct. When you send an email message, you want to be sure that the message received is the same as the message you sent. When you store data in a database, you want to be sure that the data you retrieve is the same as the data you stored. Encrypting data keeps it confidential, but you must then be able to decrypt it so that it's the same as before it was encrypted. Integrity is about having confidence that data hasn't been tampered with or altered.

Availability refers to making data available to those who need it. It's important to the organization to keep customer data secure, but at the same time it must also be available to employees who deal with customers. While it might be more secure to store the data in an encrypted format, employees need access to decrypted data.

While all sides of the CIA model are important, they also represent trade-offs that need to be made.

Describe common threats

There are different types of security threats. Some aim to steal data, some aim to extort money, and others to disrupt normal operations, such as a denial of service attack. This topic looks at some of the common threats.

Data breach

A data breach is when data is stolen, and this includes personal data. Personal data means any information related to an individual that can be used to identify them directly or indirectly.

Common security threats that can result in a breach of personal data include phishing, spear phishing, tech support scams, SQL injection, and malware designed to steal passwords or bank details.

Dictionary attack

A dictionary attack is a type of identity attack where a hacker attempts to steal an identity by trying a large number of known passwords. Each password is automatically tested against a known username. Dictionary attacks are also known as brute force attacks.

Ransomware

Malware is the term used to describe malicious applications and code that can cause damage and disrupt normal use of devices. Malware can give attackers unauthorized access, which allows them to use system resources, lock you out of your computer, and ask for ransom.

Ransomware is a type of malware that encrypts files and folders, preventing access to important files. Ransomware attempts to extort money from victims, usually in the form of cryptocurrencies, in exchange for the decryption key.

Cybercriminals that distribute malware are often motivated by money and will use infected computers to launch attacks, obtain banking credentials, collect information that can be sold, sell access to computing resources, or extort payment from victims.

Disruptive attacks

A Distributed Denial of Service (DDoS) attack attempts to exhaust an application's resources, making the application unavailable to legitimate users. DDoS attacks can be targeted at any endpoint that is publicly reachable through the internet.

Other common threats include coin miners, rootkits, trojans, worms, and exploits and exploit kits. Root-kits intercept and change standard operating system processes. After a rootkit infects a device, you can't trust any information that the device reports about itself.

Trojans are a common type of malware which can't spread on their own. This means they either have to be downloaded manually or another malware needs to download and install them. Trojans often use the same file names as real and legitimate apps so it's easy to accidentally download a trojan thinking that it is legitimate.

A worm is a type of malware that can copy itself and often spreads through a network by exploiting security vulnerabilities. It can spread through email attachments, text messages, file-sharing programs, social networking sites, network shares, removable drives, and software vulnerabilities.

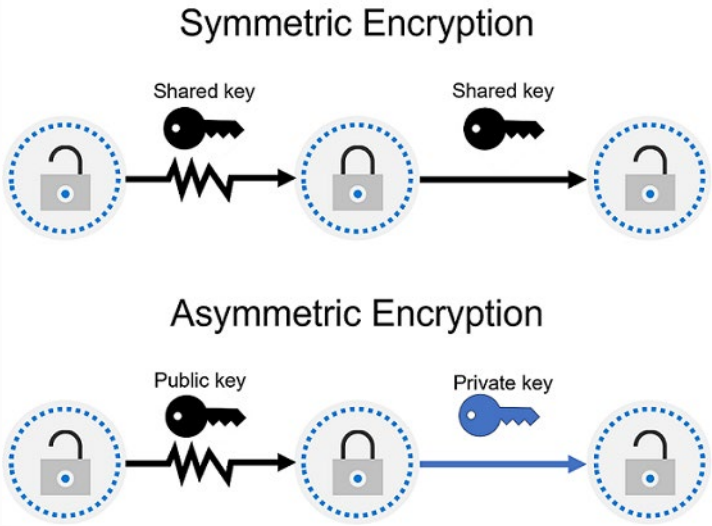
Exploits take advantage of vulnerabilities in software. A vulnerability is a weakness in your software that malware uses to get onto your device. Malware exploits these vulnerabilities to bypass your computer's security safeguards and infect your device.

These examples are just a few of the threats commonly seen. This is a continually evolving area and new threats emerge all the time.

Describe encryption and hashing

One way to mitigate against common cybersecurity threats is to encrypt sensitive or valuable data. Encryption is the process of making data unreadable and unusable to unauthorized viewers. To use or read encrypted data, it must be decrypted, which requires the use of a secret key.

There are two top-level types of encryption: symmetric and asymmetric. Symmetric encryption uses the same key to encrypt and decrypt the data. Asymmetric encryption uses a public key and private key pair. Either key can encrypt data, but a single key can't be used to decrypt encrypted data. To decrypt, you need a paired key. Asymmetric encryption is used for things like Transport Layer Security (TLS), such as the HTTPS protocol, and data signing. Encryption may protect data at rest, or in transit.



Encryption at rest

Data at rest is the data that's stored on a physical device, such as a server. It may be stored in a database or a storage account but, regardless of where it's stored, encryption of data at rest ensures the data is unreadable without the keys and secrets needed to decrypt it.

If an attacker obtained a hard drive with encrypted data and didn't have access to the encryption keys, they would be unable to read the data.

Encryption in transit

Data in transit is the data moving from one location to another, such as across the internet or through a private network. Secure transfer can be handled by several different layers. It could be done by encrypting the data at the application layer before sending it over a network. HTTPS is an example of encryption in transit.

Encrypting data in transit protects it from outside observers and provides a mechanism to transmit data while limiting the risk of exposure.

Hashing

Hashing uses an algorithm to convert the original text to a *unique* fixed-length hash value. Each time the same text is hashed using the same algorithm, the same hash value is produced. That hash can then be used as a unique identifier of its associated data.

Hashing is different to encryption in that it doesn't use keys, and the hashed value isn't then decrypted back to the original.

Hashing is used to store passwords. When a user enters their password, the same algorithm that created the stored hash creates a hash of the entered password. This is compared to the stored hashed version of the password. If they match, the user has entered their password correctly. A hashed password is more secure than storing plain text passwords, but hashing algorithms are also known to hackers. Because hash functions are deterministic (the same input produces the same output), hackers can use brute-force dictionary attacks by hashing the passwords. For every matched hash, they know the actual password. To mitigate this risk, passwords are often “salted”. This refers to adding a fixed-length random value to the

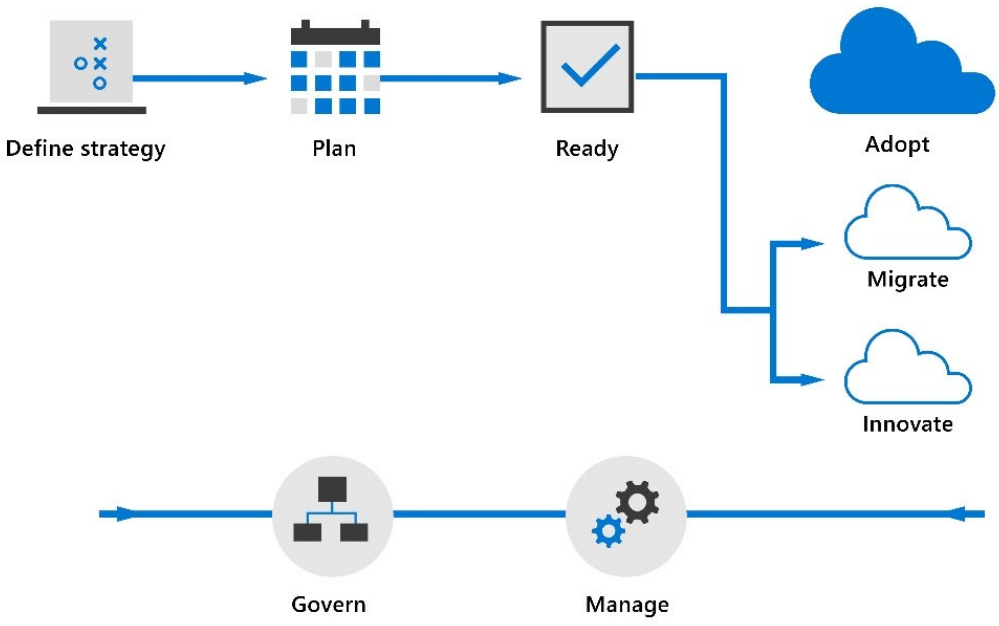
input of hash functions to create unique hashes for every input. As hackers can't know the salt value, the hashed passwords are more secure.

Describe the cloud adoption framework

Microsoft Cloud Adoption Framework for Azure consists of documentation, implementation guidance, best practices, and tools designed to help businesses to implement strategies necessary to succeed in the cloud. The Cloud Adoption Framework has been carefully designed based on cloud adoption best practices from Microsoft employees, customers, and partners. It provides a proven and consistent methodology for implementing cloud technologies.

Understand the lifecycle

Each of the following steps is part of the cloud adoption lifecycle.



1. **Strategy**: Define business justification and expected outcomes of adoption.
2. **Plan**: Align actionable adoption plans to business outcomes.
3. **Ready**: Prepare the cloud environment for the planned changes.

4. **Adopt**
    - **Migrate**: Migrate and modernize existing workloads.
    - **Innovate**: Develop new cloud-native or hybrid solutions.
5. **Govern**: Govern the environment and workloads.
6. **Manage**: Operations management for cloud and hybrid solutions.

Refer to **The Cloud Adoption Framework**[2], for a video overview of the cloud adoption lifecycle.

When your enterprise's digital transformation involves the cloud, understanding these fundamental concepts will help you during each step of the process.

Knowledge check

Multiple choice

Item 1. An organization has deployed Microsoft 365 applications to all employees. Who is responsible for the security of the personal data relating to these employees?

☐ The organization.

☐ Microsoft, the SaaS provider.

☐ The shared responsibility between your organization and Microsoft.

Multiple choice

Item 2. Which of the following measures might an organization implement as part of the defense in-depth security methodology?

☐ Locating all its servers in a single physical location.

☐ Multi-factor authentication for all users.

☐ Ensuring there's no segmentation of your corporate network.

Multiple choice

Item 3. The human resources organization want to ensure that stored employee data is encrypted. Which security mechanism would they use?

☐ Hashing.

☐ Encryption in transit.

☐ Encryption at rest.

2 https://www.microsoft.com/videoplayer/embed/RE4tyzr

Multiple choice

Item 4. An organization is moving their IT infrastructure to the cloud. They want to know how to create and implement business and technology strategies in a way that will help them succeed in the cloud. What guidance can they use to help them transition to the cloud?

- ☐ They should use Azure Policy for guidance on moving to the cloud.
- ☐ They should use the Microsoft Cloud Adoption Framework for guidance on moving to the cloud.
- ☐ They should use the Azure Cloud Succeed Framework.

Summary and resources

In this lesson, you have learned about some important security concepts and methodologies. You have learned about the Zero Trust methodology, and how the guiding principles of *verify explicitly, least privilege access*, and *assume breach* strengthens security. You learned how the six foundational elements of identity, devices, applications, data, infrastructure, and networks are used in the Zero Trust model.

This lesson also looked at the shared responsibility model, which considers who is responsible for what as organizations migrate their workloads to the cloud. You learned about the Microsoft Cloud Adoption Framework. You also learned about defense in depth, and how the security principles of *confidentiality, integrity*, and *availability* help to guide security decisions.

Finally, you learned about common cybersecurity threats including threats to business and personal data and how to protect your data.

Now that you've completed this lesson, you should be able to:

- Describe the Zero Trust and shared responsibility models.
- Describe common security threats and ways to protect through the defense in-depth security model.
- Describe the concepts of encryption and hashing.
- Describe the cloud adoption framework.

Learn more

To learn more about the topics discussed in this lesson, see:

- **Zero Trust Resource Center**[3]
- **Shared responsibility in the cloud**[4]
- **Azure defense in depth**[5]
- **What is the Microsoft Cloud Adoption Framework for Azure?**[6]

3 https://docs.microsoft.com/security/zero-trust/
4 https://docs.microsoft.com/azure/security/fundamentals/shared-responsibility
5 https://azure.microsoft.com/resources/videos/defense-in-depth-security-in-azure/
6 https://docs.microsoft.com/azure/cloud-adoption-framework/overview

Describe identity concepts

Introduction

Everyone, and every device, has an identity that can be used to gain access to resources. Identity is the way in which people and things are identified on your corporate network, and in the cloud. Being certain about who or what is accessing your organization's data and other resources is a fundamental part of securing your environment. This is known as identity and access management and is made up of two key steps: authenticating and authorizing identities.

After completing this lesson, you'll be able to:

- Describe the concept of identity as a security perimeter.
- Describe the difference between authentication and authorization.
- Describe the concepts associated with identity-related services.

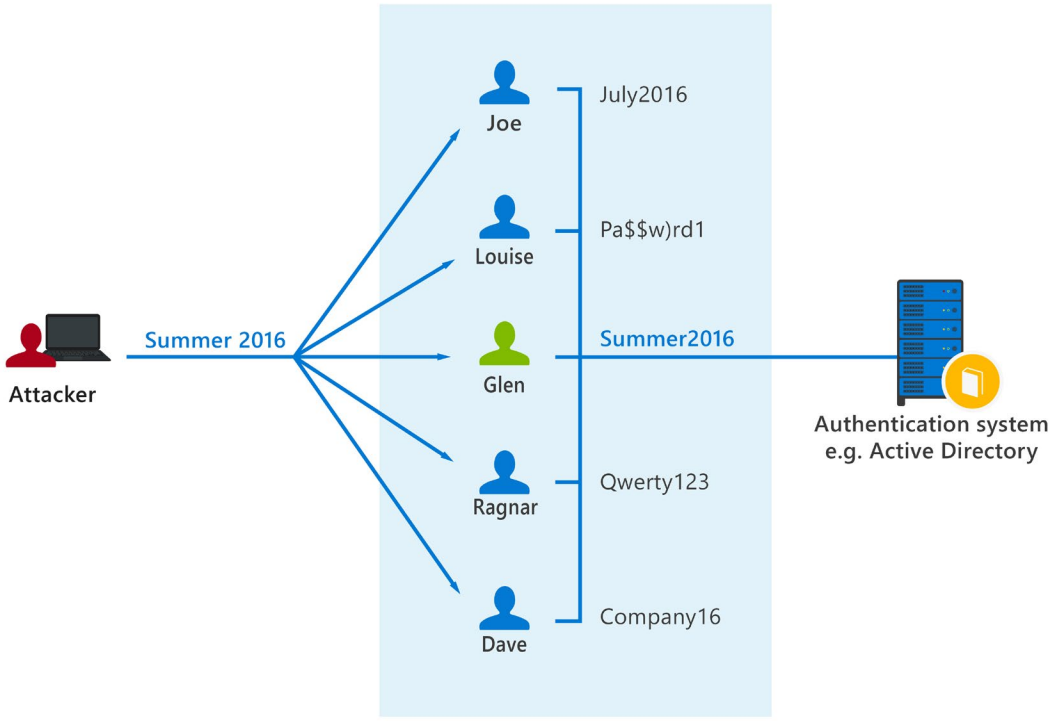
Common identity attacks

Some of the most common types of security threats that organizations face today are identity attacks. Identity attacks are designed to steal the credentials used to validate or authenticate that someone or something is who they claim to be. The result is identity theft.

Password based attacks

Password based attacks include password spray attacks and brute force attacks. A password spray attack attempts to match a username against a list of weak passwords.

Brute force attacks try many passwords against one or more accounts, sometimes using dictionaries of commonly used passwords. When a user has assigned a weak password to their account, the hacker will find a match, and gain access to that account.



Phishing

A phishing attack is when a hacker sends an email that appears to come from a reputable source. The email contains a credible story, such as a security breach, instructing the user to sign in and change their password. Instead of going to a legitimate website, the user is directed to the scammer's website where they enter their username and password. The hacker has now captured the user's identity, and their password.

Although many phishing scam emails are badly written and easy to identify, when users are busy or tired, they make mistakes and are more easily deceived. As hackers become more sophisticated, their phishing emails become more difficult to identify.

Spear phishing

A spear phishing scam is a variant on phishing. Hackers build databases of information about users, which can be used to create highly credible emails. The email may appear to come from someone in your organization who is requesting information. Although careful scrutiny might uncover the fraud, users might not read it carefully enough and send the requested information or log in to the web site before they realize the fraud. It is called spear phishing because it is highly targeted.

To protect against all types of identity attacks, robust identity security and monitoring are needed. Risk detections in Azure AD Identity Protection include any identified suspicious actions related to user accounts.

There are two types of risk: **user risk** and **sign-in risk**. **User risk** represents the probability that a given identity or account is compromised. **Sign-in risk** represents the probability that a given authentication request isn't authorized by the identity owner.

Identity as the primary security perimeter

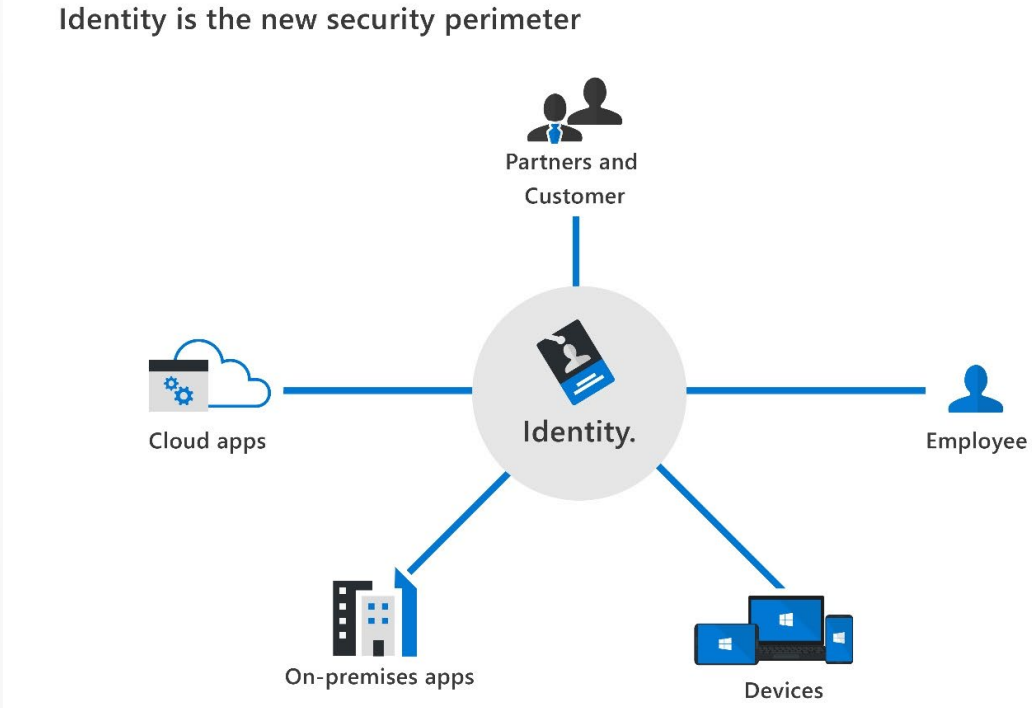
Digital collaboration has changed. Your employees and partners now expect to be able to collaborate and access organizational resources from anywhere, on any device, and without impacting their productivity. In addition, there has been an acceleration in the number of people working from home.

Enterprise security needs to adapt to this new reality. The security perimeter can no longer be viewed as the on-premises network, it now extends to:

- SaaS applications for business-critical workloads that may be hosted outside the corporate network.
- The personal devices that employees are using to access corporate resources (BYOD or bring your own device) while working from home.
- The unmanaged devices used by partners or customers when interacting with corporate data or collaborating with employees
- IoT devices installed throughout your corporate network and inside customer locations.

The traditional perimeter-based security model is no longer enough. Identity has become the new security perimeter that enables organizations to secure their assets.

But what do we mean by an identity? An identity is how someone or something can be verified and authenticated to be who they say they are. An identity may be associated with a user, an application, a device, or something else.



Four pillars of identity

Identity is a concept that spans an entire environment, so organizations need to think about identity broadly. There are four fundamental pillars of identity that organizations need to consider when creating

an identity infrastructure, which is the collection of processes, technologies, and policies for managing digital identities and controlling how identities can be used to access resources.

- **Administration**. Administration is about the creation and management of identities for users, devices, and services. As an administrator you manage how and under what circumstances the characteristics of identities can change (be created, updated, deleted).
- **Authentication**. The authentication pillar tells the story of how much assurance for a particular identity is enough. In other words, how much does an IT system need to know about an identity in order to have sufficient proof that they really are who they say they are? It involves the act of challenging a party for legitimate credentials. Authentication is sometimes shortened to AuthN.
- **Authorization**. The authorization pillar is about processing the incoming identity data to determine the level of access an authenticated person or service has within the application/service that it wants to access. Authorization is sometimes shortened to AuthZ.
- **Auditing**. The auditing pillar is about tracking who does what, when, where, and how. Auditing includes having in-depth reporting, alerts, and governance of identities.

Addressing each of these four pillars is key to a comprehensive and robust identity and access control solution.

Modern authentication and the role of the identity provider

Modern authentication is an umbrella term for authentication and authorization methods between a client, such as your laptop or phone, and a server, such as a website or application. At the center of modern authentication is the role of the ***identity provider***. An identity provider creates, maintains, and manages identity information while providing authentication, authorization, and auditing services.

With modern authentication, all services, including all authentication services, are provided by a central identity provider. The information that is used to authenticate the user with the server is stored and managed centrally by the identity provider.

With a central identity provider, organizations can establish authentication and authorization policies, monitor user behavior, identify suspicious activities, and reduce malicious attacks.

For information about modern authentication and how it works with a central identity provider watch **Azure Active Directory: Authentication fundamentals - The basics**[7].

In a client-server scenario using modern authentication (as described in the video), the client communicates with the identity provider by providing an identity which can be authenticated. Once the identity (which can be a user or an application) has been verified, the identity provider issues a *security token* which the client sends to the server. The server validates the security token through its *trust relationship* with the identity provider. By using the security token and the information that is contained within the token, the user or application can gain access to the required resources on the server. In this scenario, the token and the information contained in the token is stored and managed by the identity provider. The centralized identity provider is providing the authentication service.

Microsoft Azure Active Directory is an example of a cloud-based identity provider. Other examples of identity providers include Twitter, Google, Amazon, LinkedIn, and GitHub.

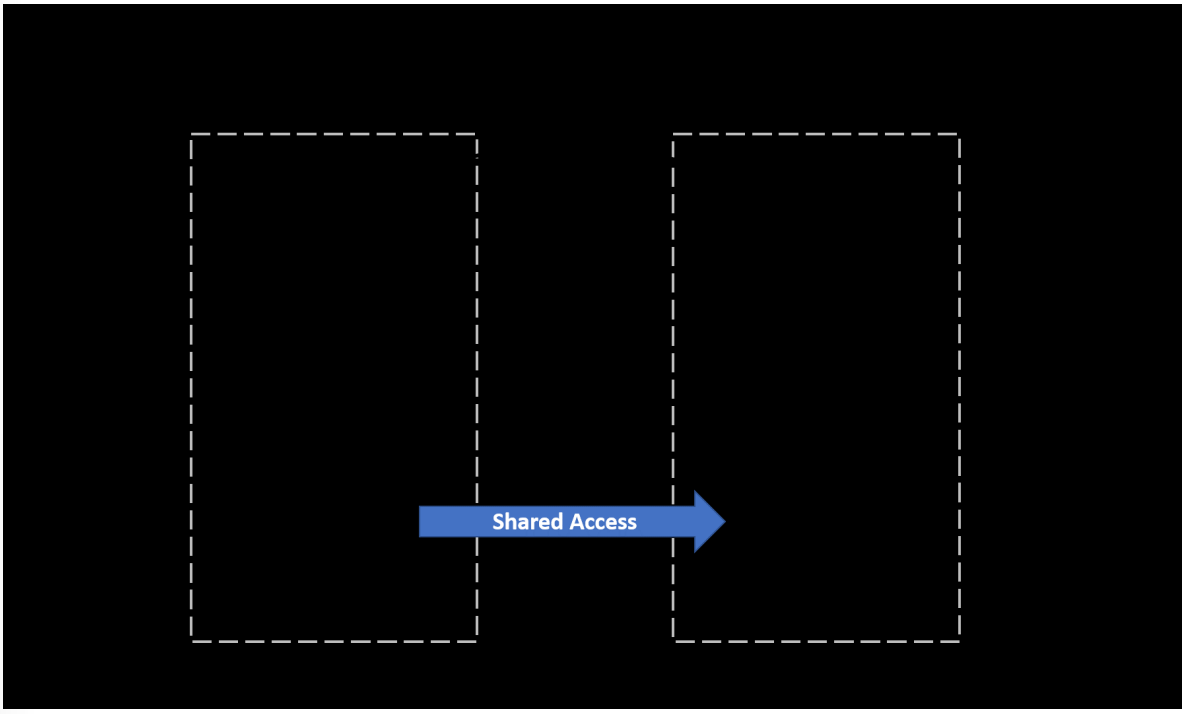
7 https://www.microsoft.com/videoplayer/embed/RE4Kdt9

Single sign-on

Another fundamental capability of an identity provider and "modern authentication" is the support for single sign-on (SSO). With SSO, the user logs in once and that credential is used to access multiple applications or resources.
When you set up single sign-on to work between multiple identity providers, it is called federation.

The concept of Federated Services

Federation enables the access of services across organizational or domain boundaries by establishing trust relationships between the respective domain's identity provider. With federation, there is no need for a user to maintain a different username and password when accessing resources in other domains.



The simplified way to think about this federation scenario is as follows:

- The website uses the authentication services of Identity Provider A (IdP-A).
- The user authenticates with Identity Provider B (IdP-B).
- IdP-A has a trust relationship configured with IdP-B.
- When the user's credentials are passed to the website, the website trusts the user and allows access.

With federation, trust is not always bi-directional. Although IdP-A may trust IdP-B and allow the user in domain B to access the website in domain A, the opposite is not true, unless that trust relationship is configured.

A common example of federation in practice is when a user logs into a third-party site with their social media account, such as Twitter. In this scenario, Twitter is an identity provider, and the third-party site may be using a different identity provider, such as Azure AD. There is a trust relationship between Azure AD and Twitter.

The concept of directory services and Active Directory

In the context of a computer network, a directory is a hierarchical structure that stores information about objects on the network. A directory service stores directory data and makes this data available to network users, administrators, services, and applications.

Active Directory (AD) is a set of directory services developed by Microsoft as part of Windows 2000 for on-premises domain-based networks. The best-known Active Directory service is Active Directory Domain Services (AD DS). It stores information about members of the domain, including devices and users, verifies their credentials, and defines their access rights. A server running AD DS is a domain controller (DC).

AD DS is a central component in organizations with on-premises IT infrastructure. AD DS gives organizations the ability to manage multiple on-premises infrastructure components and systems using a single identity per user. AD DS does not, however, natively support mobile devices, SaaS applications, or line-of-business apps that require *modern authentication* methods.

The growth of cloud services, SaaS applications, personal devices being used at work, has resulted in the need for modern authentication, and an evolution of Active Directory-based identity solutions.

Azure Active Directory is the next evolution of identity and access management solutions by providing organizations with an Identity as a Service (IDaaS) solution for all their apps across cloud and on-premises.
In this course we will focus on Azure AD, Microsoft's cloud-based identity provider.

To learn more visit **Compare Active Directory to Azure Active Directory**[8].

Knowledge check

Multiple choice

Item 1. What type of security risk does a phishing scam pose?

- ☐ Ethical risk.
- ☐ Physical risk.
- ☐ Identity risk.

Multiple choice

Item 2. What is a benefit of single sign-on?

- ☐ A central identity provider can be used.
- ☐ The user signs in once and then can access many applications or resources.
- ☐ Passwords always expire after 72 days.

8 https://docs.microsoft.com/azure/active-directory/fundamentals/active-directory-compare-azure-ad-to-ad

Multiple choice

Item 3. Which relationship allows federated services to gain access to resources?

- ☐ Claim relationship.
- ☐ Shared access relationship.
- ☐ Trust relationship.

Multiple choice

Item 4. Authentication is the process of doing what?

- ☐ Verifying that a user or device is who they say they are.
- ☐ The process of profiling user behavior.
- ☐ Enabling federated services.

Summary and resources

In this lesson, you've learned about some common identity security threats and basic identity concepts. You learned about identity as the new security perimeter, and authentication, authorization, and the role of Active Directory. You also looked at the concept of federated services to access resources that belong to another organization.

Now that you've completed this lesson, you should be able to:

- Describe the concept of identity as a security perimeter.
- Describe the difference between authentication and authorization.
- Describe the concepts associated with identity-related services.

Learn more

For more information on the topics covered in this lesson, see:

- **Protecting your organization against password spray attacks**[9]
- **Identity protection risks**[10]
- **Authentication vs authorization**[11]
- **Identity providers for External Identities**[12]
- **Compare Active Directory to Azure Active Directory**[13]

9 https://www.microsoft.com/security/blog/2020/04/23/protecting-organization-password-spray-attacks/
10 https://docs.microsoft.com/azure/active-directory/identity-protection/concept-identity-protection-risks
11 https://docs.microsoft.com/azure/active-directory/develop/authentication-vs-authorization
12 https://docs.microsoft.com/azure/active-directory/external-identities/identity-providers
13 https://docs.microsoft.com/azure/active-directory/fundamentals/active-directory-compare-azure-ad-to-ad

Answers

Multiple choice

Item 1. An organization has deployed Microsoft 365 applications to all employees. Who is responsible for the security of the personal data relating to these employees?

■ The organization.

☐ Microsoft, the SaaS provider.

☐ The shared responsibility between your organization and Microsoft.

Explanation
In the shared responsibility model, the customer organization always has responsibility for their data, including personal data relating to employees.

Multiple choice

Item 2. Which of the following measures might an organization implement as part of the defense in-depth security methodology?

☐ Locating all its servers in a single physical location.

■ Multi-factor authentication for all users.

☐ Ensuring there's no segmentation of your corporate network.

Explanation
Multi-factor authentication is an example of defense in-depth at the identity and access layer.

Multiple choice

Item 3. The human resources organization want to ensure that stored employee data is encrypted. Which security mechanism would they use?

☐ Hashing.

☐ Encryption in transit.

■ Encryption at rest.

Explanation
Encryption at rest could be part of a security strategy to protect stored employee training data.

Multiple choice

Item 4. An organization is moving their IT infrastructure to the cloud. They want to know how to create and implement business and technology strategies in a way that will help them succeed in the cloud. What guidance can they use to help them transition to the cloud?

☐ They should use Azure Policy for guidance on moving to the cloud.

■ They should use the Microsoft Cloud Adoption Framework for guidance on moving to the cloud.

☐ They should use the Azure Cloud Succeed Framework.

Explanation
The Cloud Adoption Framework has been carefully designed based on cloud adoption best practices from Microsoft employees, customers, and partners. It provides a proven and consistent methodology for implementing cloud technologies.

Multiple choice

Item 1. What type of security risk does a phishing scam pose?

☐ Ethical risk.

☐ Physical risk.

■ Identity risk.

Explanation
A phishing scam is an example of an identity attack.

Multiple choice

Item 2. What is a benefit of single sign-on?

☐ A central identity provider can be used.

■ The user signs in once and then can access many applications or resources.

☐ Passwords always expire after 72 days.

Explanation
With single sign-on a user signs in once and can then access a number of applications or resources.

Multiple choice

Item 3. Which relationship allows federated services to gain access to resources?

☐ Claim relationship.

☐ Shared access relationship.

■ Trust relationship.

Explanation
Federated services use a trust relationship to allow access to resources.

Multiple choice

Item 4. Authentication is the process of doing what?

■ Verifying that a user or device is who they say they are.

☐ The process of profiling user behavior.

☐ Enabling federated services.

Explanation
Authentication is the process of verifying that a user or device is who they say they are.

Module 2 Describe the capabilities of Microsoft identity and access management solutions

Describe the basic services and identity types of Azure AD

Introduction

When it comes to security, your organization can no longer rely on its network boundary. To allow employees, partners, and customers to collaborate securely, identity has become the new security perimeter. Using an identity provider gives your organization the ability to manage all aspects of identity security.

This lesson introduces you to Azure Active Directory (Azure AD), Microsoft's cloud-based identity and access management service. In this module, you'll learn about the benefits of using a cloud-based identity provider, including single sign-on for users. You'll also find out about the different Azure AD editions, the identity types supported by Azure AD, and how you can use it to support external users.

After completing this lesson, you'll be able to:

- Describe what Azure AD does.
- Describe the identity types that Azure AD supports.

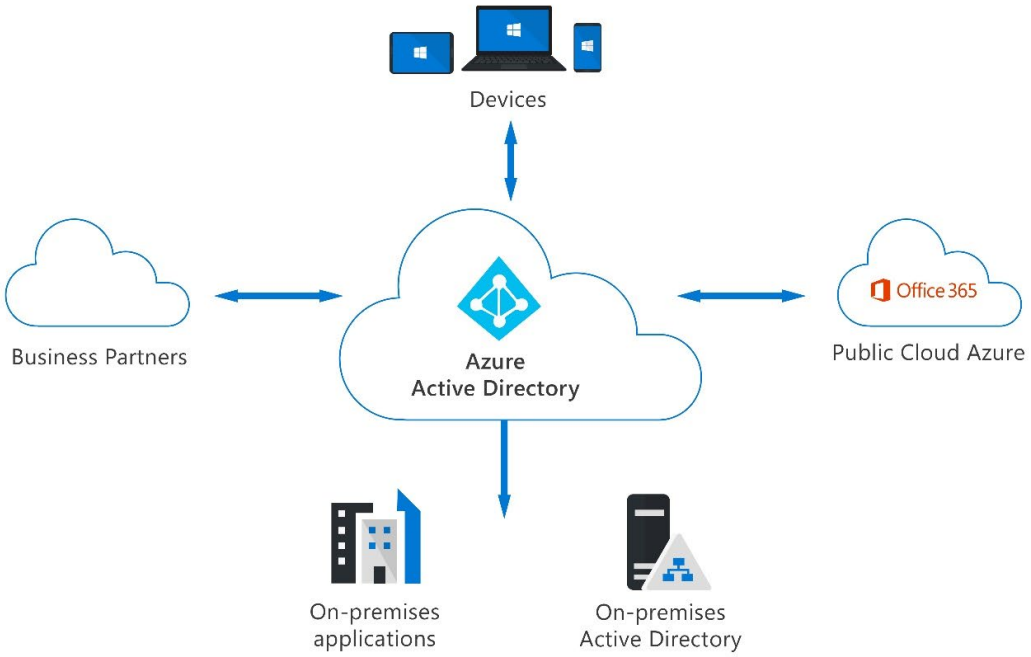
Describe Azure Active Directory

Azure Active Directory (Azure AD) is Microsoft's cloud-based identity and access management service. Organizations use Azure AD to enable their employees, guests, and others to sign in and access the resources they need, including:

- Internal resources, such as apps on your corporate network and intranet, and cloud apps developed by your own organization.
- External services, such as Microsoft Office 365, the Azure portal, and any SaaS applications used by your organization.

Azure AD simplifies the way organizations manage authorization and access by providing a single identity system for their cloud and on-premises applications. Azure AD can be synchronized with your existing on-premises Active Directory, synchronized with other directory services, or used as a standalone service.

Azure AD also allows organizations to securely enable the use of personal devices, such as mobiles and tablets, and enable collaboration with business partners and customers.



Azure AD is used by IT admins to control access to corporate apps and resources, based on business requirements. It can also be set up to require multi-factor authentication when accessing important organizational resources. Azure AD can be used to automate user provisioning between an existing Windows Server AD and cloud apps, including Microsoft 365. Finally, Azure AD provides powerful tools to automatically help protect user identities and credentials and to meet an organization's access governance requirements.

Developers use Azure AD as a standards-based approach for adding single sign-on (SSO) to their apps, so that users can sign in with their pre-existing credentials. Azure AD also provides APIs that allow developers to build personalized app experiences using existing organizational data.

Each Microsoft 365, Office 365, Azure, or Dynamics 365 Online subscription automatically uses an Azure AD tenant. Users of these services can take advantage of Azure AD services such as self-service password reset, provided it has been configured by their organization's admins.

Azure AD is available in four editions: Free, Office 365 Apps, Premium P1, and Premium P2. For more information on what is included with each of these editions, refer to **Azure Active Directory Pricing**[1].

1 https://azure.microsoft.com/pricing/details/active-directory/

Describe the Azure AD identity types

Azure AD manages different types of identities: users, service principals, managed identities, and devices. In this topic, we consider each type of Azure AD identity.

User

A user identity is a representation of something that is managed by Azure AD. Employees and guests are represented as users in Azure AD. If you have several users with the same access needs, you can create a group. Groups allow you to assign access permissions to all the members of the group, instead of having to assign the access rights individually.

Azure AD business-to-business (B2B) collaboration, a feature within External Identities, includes the capability to add guest users. With B2B collaboration, an organization can securely share applications and services with guest users from another organization.

Interactive guide

In the following interactive guide, you will add a new user to Azure Active Directory. Select the link below to get started.

Interactive guide - Add a new user to Azure Active Directory[2]

Service Principal

A service principal is a security identity used by applications or services to access specific Azure resources. You can think of it as an identity for an application.

For an application to delegate its identity and access functions to Azure AD, the application must first be registered with Azure AD. The process of registering the application creates a globally unique app object which is stored in your home tenant or directory. A service principal is created in each tenant where the application is used and references the globally unique app object. The service principal defines what the app can do in the tenant, such as who can access the app, and what resources the app can access.

Managed Identity

A managed identity is an identity in Azure Active Directory that is automatically managed by Azure. Managed identities are typically used to manage the credentials for authenticating a cloud application with an Azure service.

There are several benefits to using managed identities, including:

- Application developers can authenticate to services that support managed identities for Azure resources. For a complete list of services, refer to **Azure Services that support managed identities**[3].
- Any Azure service that supports Azure AD authentication can use managed identities to authenticate to another Azure service, for example accessing Azure Key Vault.
- Managed identities can be used without any additional cost.

There are two types of managed identities: system-assigned and user-assigned.

2 https://edxinteractivepage.blob.core.windows.net/edxpages/Security%20fundamentals/LP02M02%20-%20Create%20a%20New%20User%20in%20Azure%20Active%20Directory/index.html?azure-portal=true

3 https://docs.microsoft.com/azure/active-directory/managed-identities-azure-resources/services-support-managed-identities

System-assigned. Some Azure services allow you to enable a managed identity directly on a service instance. When you enable a system-assigned managed identity, an identity is created in Azure AD that is tied to the lifecycle of that service instance. When the resource is deleted, Azure automatically deletes the identity for you. By design, only that Azure resource can use this identity to request tokens from Azure AD.

User-assigned. You may also create a managed identity as a standalone Azure resource. A user-assigned managed identity is assigned to one or more instances of an Azure service. You can create a user-assigned managed identity and assign it to one or more instances of an Azure service. In the case of user-assigned managed identities, the identity is managed separately from the resources that use it.

The following table summarizes the differences between system-assigned and user-assigned managed identities:

Property	System-assigned managed identity	User-assigned managed identity
Creation	Created as part of an Azure resource, such as an Azure virtual machine or Azure App Service.	Created as a stand-alone Azure resource.
Life cycle	Shared life cycle with the Azure resource. When the parent resource is deleted, the managed identity is also deleted.	Independent life cycle. Must be explicitly deleted.
Sharing across Azure resources	Cannot be shared. Associated with a single Azure resource.	Can be shared. A user-assigned managed identity can be associated with more than one Azure resource.
Common use cases	Workloads that are contained within a single Azure resource. Workloads for which you need independent identities, such as an application that runs on a single virtual machine.	Workloads that run on multiple resources and which can share a single identity. Workloads that need pre-authorization to a secure resource as part of a provisioning flow. Workloads where resources are recycled frequently, but permissions should stay consistent. For example, a workload where multiple virtual machines need to access the same resource.

Device

A device is a piece of hardware, such as a mobile device, laptop, server, or printer. Device identities can be set up in different ways in Azure AD, which determine properties such as who owns the device. Managing devices in Azure AD allows an organization to protect its assets by using tools such as Microsoft Intune to ensure standards for security and compliance. Azure AD also enables single sign-on to devices, apps, and services from anywhere through these devices.

There are multiple options for getting devices into Azure AD:

- **Azure AD registered devices** can be Windows 10, iOS, Android, or macOS devices. Devices that are Azure AD registered are typically owned personally, rather than by the organization. They are signed in with a personal Microsoft account or another local account.

- **Azure AD joined** devices exist only in the cloud. Azure AD joined devices are owned by an organization and signed in with an organization Azure AD account. Users sign in to their devices with their Azure AD or synced Active Directory work or school accounts. You can configure Azure AD joined devices for all Windows 10 devices (except Windows 10 Home).
- **Hybrid Azure AD joined devices** can be Windows 7, 8.1, or 10 or Windows Server 2008 or newer. Devices that are hybrid Azure AD joined are owned by an organization and are signed in with an Active Directory Domain Services account belonging to that organization. They exist in the cloud and on-premises.

IT admins can use tools like Microsoft Intune, a mobile device management (MDM) solution, to manage devices. Refer to **Microsoft Intune**[4] for more information.

Describe the types external identities

Today's world is about collaboration, working with people both inside and outside of your organization. That means that you sometimes need to provide access to your organization's applications or data to external users.

Azure AD External Identities is a set of capabilities that enable organizations to allow access to external users, such as customers or partners. Your customers, partners, and other guest users can "bring their own identities" to sign in.

The ability for external users to "bring their own identities" to sign in is enabled through Azure AD support of external identity providers like other Azure AD tenants, Facebook, Google, or enterprise identity providers. Admins can set up federation with identity providers so your external users can sign in with their existing social or enterprise accounts instead of creating a new account just for your application.

There are two different Azure AD External Identities: B2B or B2C.

- B2B collaboration allows you to share your apps and resources with external users.
- B2C is an identity management solution for consumer/customer facing apps.

B2B collaboration

B2B collaboration allows you to share your organization's applications and services with guest users from other organizations, while maintaining control over your own data. B2B collaboration uses an invitation and redemption process, allowing external users to access your resources with their credentials. Developers can customize the invitation and redemption process using Azure AD business-to-business APIs.

With B2B collaboration, external users are managed in the same directory as employees but are typically annotated as guest users. Guest users can be managed the same way as employees, added to the same groups, and so on. With B2B, SSO to all Azure AD-connected apps is supported.

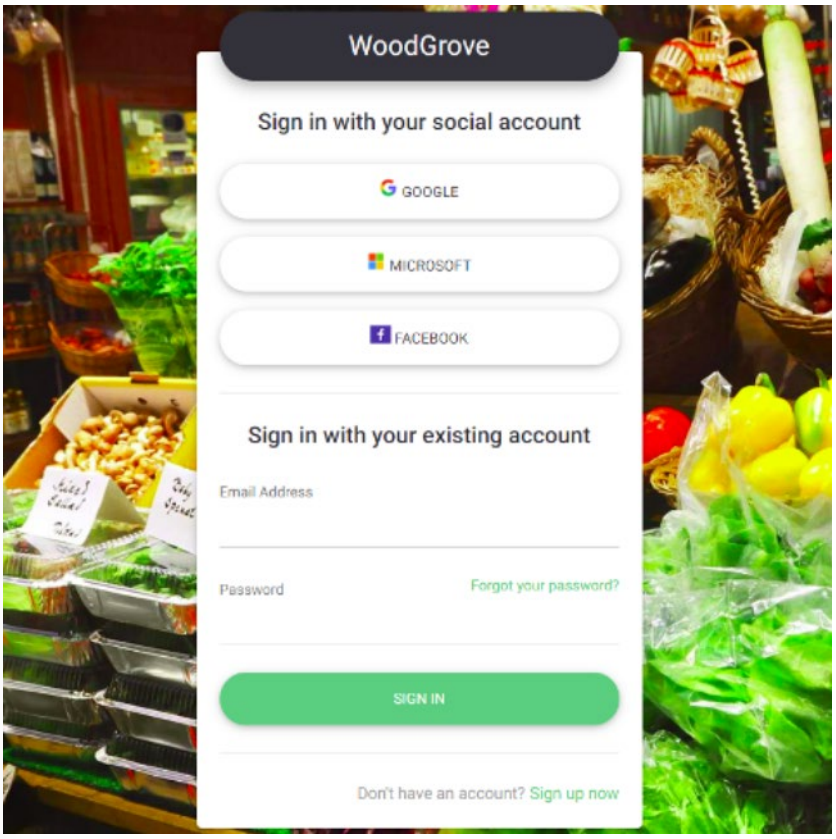
B2C access management

Azure AD B2C is a customer identity access management (CIAM) solution. Azure AD B2C allows external users to sign in with their preferred social, enterprise, or local account identities to get single sign-on to your applications. Azure AD B2C can support millions of users and billions of authentications per day. It takes care of the scaling and safety of the authentication platform, monitoring, and automatically handling threats like denial-of-service, password spray, or brute force attacks.

4 https://docs.microsoft.com/mem/intune/fundamentals/what-is-intune

With Azure AD B2C, external users are managed in the Azure AD B2C directory, separately from the organization's employee and partner directory. With Azure AD B2C, SSO to customer owned apps within the Azure AD B2C tenant is supported.

Azure AD B2C is an authentication solution that you can customize with your brand so that it blends seamlessly with your web and mobile applications.



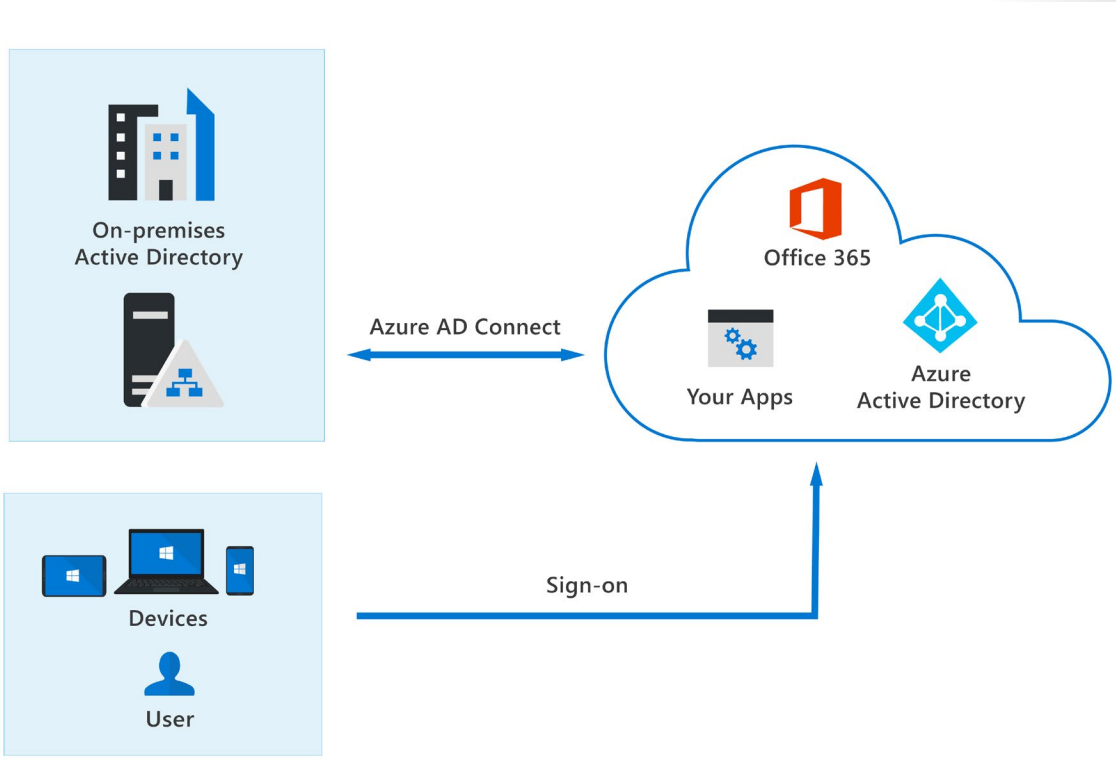
Azure AD External Identities is a feature of Premium P1 and P2 Azure AD editions, and pricing is based on Monthly Active Users. Refer to **Azure AD pricing** [5] for more details.

Describe the concept of hybrid identities

Organizations may use the hybrid identity model, or the cloud only identity model. In the hybrid model, identities are created in Windows Active Directory or another identity provider, and then synchronized to Azure AD. In the cloud-only model, identities are created and wholly managed in Azure AD. Whether identities are created on-premises or in the cloud, users can access both cloud and on-premises resources.

With the hybrid model, users accessing both on-premise and cloud apps are hybrid users managed in the on-premise Active Directory. When you make an update in your on-premises AD DS, all updates to user accounts, groups, and contacts are synchronized to your Azure AD. The synchronization is managed with *Azure AD Connect*.

5 https://azure.microsoft.com/pricing/details/active-directory/external-identities/



When using the hybrid model, authentication can either be done by Azure AD, which is known as *managed authentication*. Or Azure AD redirects the client requesting authentication to another identity provider, which is known as *federated authentication*.

One of three authentication methods can be used (they are listed in order of resilience):

1. **Password hash synchronization**. This is 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 any additional infrastructure being needed. Password hash synchronization is a type of managed authentication.
2. **Pass-through authentication (PTA)**. 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 an on-premises Active Directory, which ensures that the password validation doesn't happen in the cloud. PTA is a type of managed authentication.
3. **Federated authentication**. Azure AD hands off the authentication process to a separate trusted authentication system, such as on-premises Active Directory Federation Services (AD FS), to validate the user's password.

Knowledge check

Multiple choice

Item 1. Your organization is launching a new app for customers. You want your customers to use a sign-in screen that is customized with your brand identity. Which type of Azure External identity authentication solution should you use?

- ☐ Azure AD B2B
- ☐ Azure AD B2C
- ☐ Azure AD Hybrid identities

Multiple choice

Item 2. Within your organization, all your users have Microsoft 365 cloud identities. Which identity model should you use?

- ☐ Hybrid
- ☐ Cloud-only
- ☐ On-premises only

Multiple choice

Item 3. You have developed an app and want users to be able to sign in with their Facebook, Google, or Twitter credentials. What type of authentication will you use?

- ☐ Service principal authentication
- ☐ Azure AD B2C
- ☐ User assigned identities

Summary and resources

In this lesson, you've gained an insight into the features and capabilities of Azure Active Directory. You've learned about the different Azure AD editions, the identity types supported by Azure AD, and how you can use it to support external users. Finally, you learned about the hybrid model, where all user identities are managed in your on-premises Active Directory Domain Services (AD DS) directory, and changes are synchronized to your Azure AD.

Now that you've completed this lesson, you should be able to:

- Describe what Azure AD does.
- Describe the identity types that Azure AD supports.

Learn more

For more information on the topics covered in this lesson, see:

- **What is Azure Active Directory?**[6]

6 https://docs.microsoft.com/azure/active-directory/fundamentals/active-directory-whatis

- **Azure Active Directory Pricing**[7]
- **Azure AD Licenses**[8]
- **Azure Active Directory External Identities**[9]
- **Managed identities**[10]
- **Services that support managed identities for Azure resources**[11]
- **What is Azure AD Connect?**[12]
- **Choose the right authentication method for your Azure Active Directory hybrid identity solution**[13]
- **Azure AD registered devices**[14]
- **Azure AD joined devices**[15]
- **Hybrid Azure AD joined devices**[16]

7 https://azure.microsoft.com/pricing/details/active-directory/
8 https://docs.microsoft.com/azure/active-directory/fundamentals/active-directory-whatis#what-are-the-azure-ad-licenses
9 https://docs.microsoft.com/azure/active-directory/external-identities/compare-with-b2c
10 https://docs.microsoft.com/azure/active-directory/managed-identities-azure-resources/overview
11 https://docs.microsoft.com/azure/active-directory/managed-identities-azure-resources/services-support-managed-identities
12 https://docs.microsoft.com/azure/active-directory/hybrid/whatis-azure-ad-connect
13 https://docs.microsoft.com/azure/active-directory/hybrid/choose-ad-authn
14 https://docs.microsoft.com/azure/active-directory/devices/concept-azure-ad-register
15 https://docs.microsoft.com/azure/active-directory/devices/concept-azure-ad-join
16 https://docs.microsoft.com/azure/active-directory/devices/concept-azure-ad-join-hybrid

Describe the authentication capabilities of Azure AD

Introduction

In this lesson, you will learn about the authentication capabilities of Azure AD. Authentication is the process of verifying an identity to be legitimate. Passwords are commonly used to authenticate users, but they have many problems. Passwords are difficult for users to remember, and easy for hackers to guess. Because good passwords are necessarily difficult to remember, users often use the same password for multiple applications, providing multiple points of entry for a compromised identity.

In this lesson you will learn about multi-factor authentication, and how it improves security. You will also learn about the password protection and management capabilities of Azure AD.

After completing this lesson, you will be able to:

- Describe the authentication methods of Azure AD.
- Describe the password protection and management capabilities of Azure AD.

Describe the different authentication methods of Azure AD

Legacy applications have relied on a single form of authentication, most often a password. However, passwords are problematic for users, and easily compromised. *Multi-factor authentication* (MFA) requires more than one form of verification to prove that an identity is legitimate, such as a trusted device or a fingerprint scan. That means that even when an identity's password has been compromised, a hacker cannot gain entry to a resource.

Multi-factor authentication dramatically improves the security of an identity, whilst still being simple for users. The additional authentication factor must be something that is difficult for an attacker to obtain or duplicate.

To learn more about the problem with passwords, and why multi-factor authentication is so important watch **The new sign-in standard: Passwordless authentication**[17].

Azure Active Directory Multi-Factor Authentication works by requiring:

- **Something you know** – typically a password or PIN **and**
- **Something you have** – such as a trusted device that is not easily duplicated, like a phone or hardware key **or**
- **Something you are** - biometrics like a fingerprint or face scan.

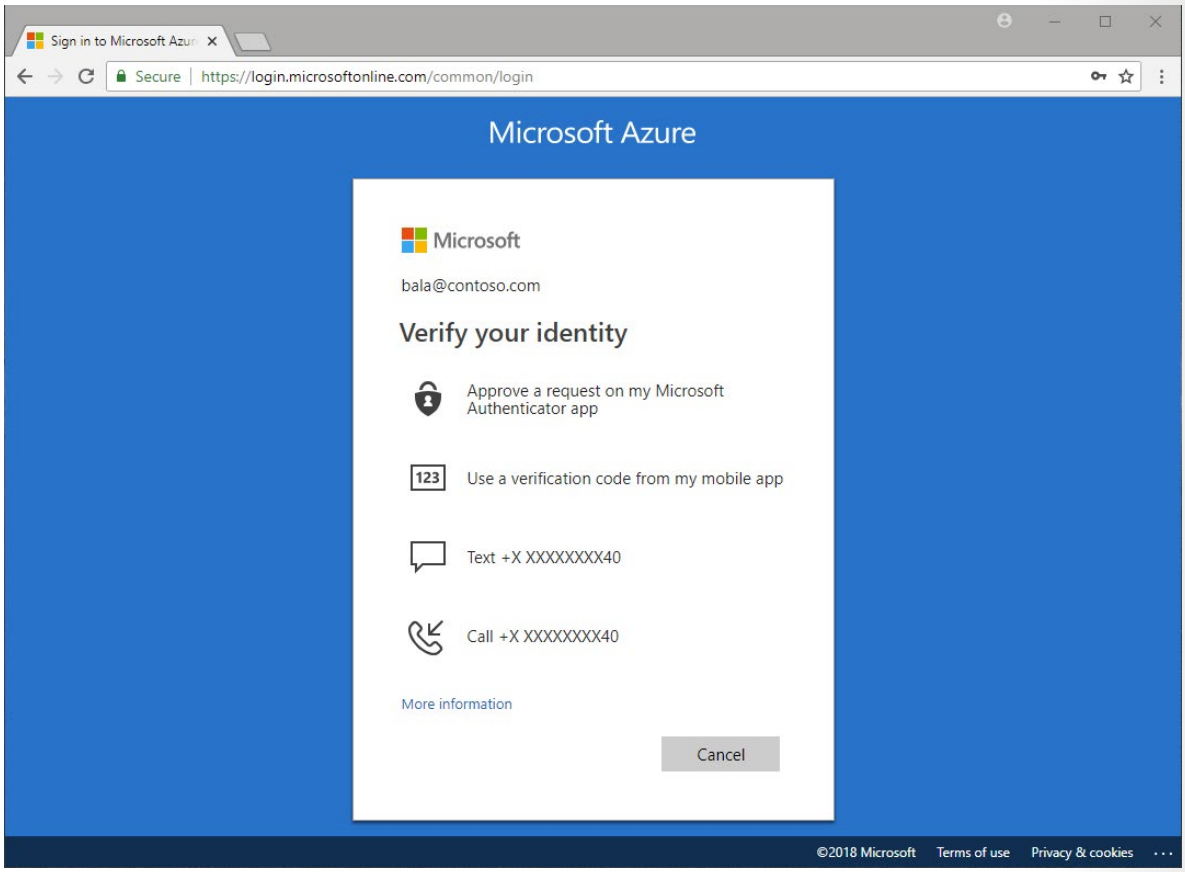
Multi-factor authentication verification prompts are configured to be part of the Azure AD sign-in event. Azure AD automatically requests and processes multi-factor authentication, without you making any changes to your applications or services. When a user signs in, they receive an MFA prompt, and can choose from one of the additional verification forms that they've registered.

An administrator can require certain verification methods, or the user can access their MyAccount to edit or add verification methods.

17 https://www.microsoft.com/en-us/videoplayer/embed/RE4zhD7

The following additional forms of verification can be used with Azure Active Directory multi-factor authentication:

- Microsoft Authenticator app
- SMS
- Voice call
- OATH Hardware token



Security defaults and MFA

Security defaults are a set of basic identity security mechanisms recommended by Microsoft. When enabled, these recommendations will be automatically enforced in your organization. The goal is to ensure that all organizations have a basic level of security enabled at no extra cost. These defaults enable some of the most common security features and controls, including:

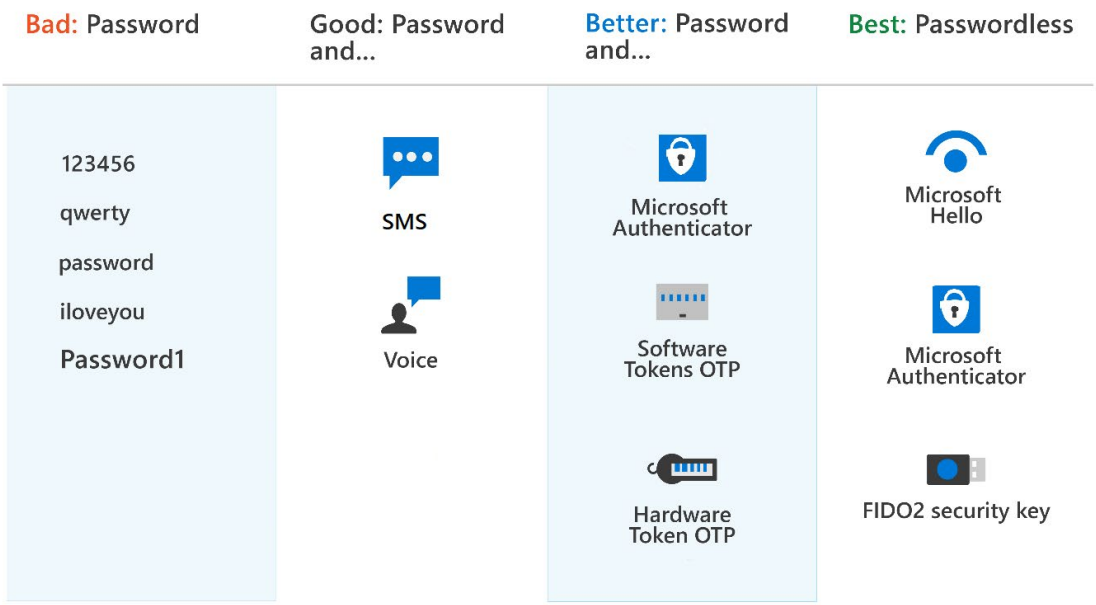
- Enforcing Azure Active Directory Multi-Factor Authentication registration for all users
- Forcing Administrators to use Multi-Factor Authentication
- Requiring all users to perform Multi-Factor Authentication when needed

Security defaults are a great option for organizations that want to increase their security posture but don't know where to start, or for organizations using the free tier of Azure AD licensing. Security defaults

may not be appropriate for organizations with Azure AD premium licenses or more complex security requirements. To learn more, refer to **What are security defaults?**[18]

Describe Multi-factor authentication in Azure AD

In the previous topic you learned about multi-factor authentication, and why it improves security. In this topic, we consider the different authentication methods that can be used with Azure AD multi-factor authentication.



Passwords

Passwords have many problems. If they're easy enough to remember, they're easy for a hacker to compromise. Strong passwords, which aren't easily hacked, are difficult to remember and have an impact on user productivity when forgotten.

Password and additional verification

With modern authentication and security features in Azure AD, passwords are supplemented or replaced with more secure authentication methods.

Phone

You can also use your phone as an additional means of authentication, configured for either phone calls or text message.

18 https://docs.microsoft.com/azure/active-directory/fundamentals/concept-fundamentals-security-defaults

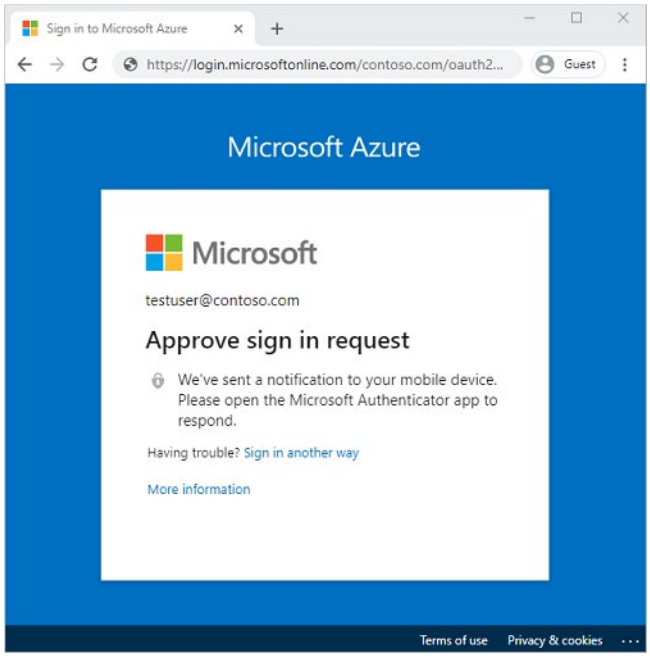
If you set up your additional security verification to receive a phone call, you'll receive a phone call from Microsoft asking you to press a key on your mobile device to verify your identity.

If you set up your additional security verification to receive a text message, you will be sent a code by text. You then enter the code to verify your identity.

Microsoft Authenticator app

The Microsoft Authenticator app is a phone app that allows you to securely verify your identity. The Authenticator app can be used to provide the additional authentication required for two-step or multi-factor authentication. Microsoft Authenticator can also be configured to use biometrics, such as a fingerprint or facial scan.

To use Microsoft Authenticator, you must download the phone app from the Microsoft store, and register your Microsoft account. Microsoft Authenticator is available for Android and iOS. When a user chooses Authenticator as their additional authentication method, a notification is pushed to the phone or tablet. if the notification is legitimate, the user selects **Approve**, otherwise, they select **Deny**.



OATH

OATH (Open Authentication) is an open standard that specifies how time-based one-time passwords (TOTP) codes are generated. One-time password codes can be used to authenticate a user. OATH TOTP can be implemented using either software or hardware to generate the codes.

Software OATH tokens are typically applications such as the Microsoft Authenticator app and other authenticator apps.

OATH TOTP hardware tokens typically come with a secret key, pre-programmed in the token, which must be input into Azure AD. Users are associated with a specific hardware token. The hardware token does a refresh of the code every 30 or 60 seconds.

Passwordless Authentication

Passwordless authentication is based on “something you are” rather than “something you know”. For example, a biometric facial scan used in Windows Hello for Business is an example of “something you are”. A fingerprint scan used by the Microsoft Authenticator app or a FIDO2 security device, is also “something you are”.

Passwordless authentication with Azure AD, such as with the Microsoft Authenticator app or FIDO keys, is particularly applicable for shared PCs and where a mobile phone isn't a viable option, such as for help desk personnel, public kiosk, or hospital team.

Biometrics

Biometric sign-in uses human characteristics, such as a hand, iris, face, or fingerprint. Windows Hello uses facial or fingerprint biometric data to authenticate a user. You'll learn more about Windows Hello in the next topic. The Microsoft Authenticator app can also be used in passwordless mode, using biometric data such as a fingerprint scan, or a facial scan.

FIDO2

FIDO is an abbreviation for Fast Identity Online, an alliance which promotes open authentication standards and aims to reduce the reliance on passwords as a form of authentication.

Azure AD supports FIDO2, a passwordless authentication method that can come in different forms. FIDO2 allows users to sign in using an external security key. The external key may be a USB device, lightning connector, Bluetooth, or NFC. In whichever form FIDO2 is implemented, the user never has to enter a password.

Users can also register and select a FIDO2 security key as their main means of authentication.

Describe Windows Hello

Windows Hello, an authentication feature built into Windows 10, replaces passwords with strong two-factor authentication on PCs and mobile devices. This authentication consists of a new type of user credential that is tied to a device and uses a biometric or PIN.

Windows Hello lets users authenticate to:

- A Microsoft account.
- An Active Directory account.
- An Azure Active Directory (Azure AD) account.
- Identity Provider Services or Relying Party Services that support Fast ID Online (FIDO) v2.0 authentication (in preview)

After initial verification of the user during enrollment, Windows Hello is set up on the user's device and Windows asks the user to set a gesture, which can be a biometric, such as a fingerprint, or a PIN. The user provides the gesture to verify their identity. Windows then uses Windows Hello to authenticate users.

Windows stores PIN and biometric data securely on the local device; it's never sent to external devices or servers. That means there is no single collection point that an attacker might compromise.

There are two configurations for Windows Hello: Windows Hello and Windows Hello for Business.

- Windows Hello is configured by a user on their personal device and is referred to as Windows Hello for convenience PIN. It uses a PIN or biometric gesture and is unique to that device. Windows Hello convenience PIN is not backed by asymmetric (public/private key) or certificate-based authentication.
- Windows Hello for Business is configured by Group Policy or mobile device management (MDM) policy, such as Microsoft Intune, and always uses key-based or certificate-based authentication. This makes it much more secure than Windows Hello convenience PIN. By default, Windows Hello convenience PIN is disabled on all domain-joined computers.

Why is Windows Hello safer than a password?

Windows Hello in Windows 10 enables users to sign in to their device using a PIN. Although a PIN looks much like a password, a Windows Hello PIN is more secure because it's tied to the specific device on which it was set up. Without the hardware, the PIN is useless.

A regular password is transmitted to a server where it can be intercepted in transmission or stolen from a server. A PIN is local to the device; it isn't transmitted anywhere, and it isn't stored on a server.

The Windows Hello PIN is backed by a Trusted Platform Module (TPM) chip, which is a secure crypto processor that is designed to carry out cryptographic operations. The chip includes multiple physical security mechanisms to make it tamper resistant, and malicious software is unable to tamper with the security functions of the TPM. Many mobiles phones and modern laptops have TPM.

Describe self-service password reset in Azure AD

Self-service password reset (SSPR) is a feature of Azure AD that allows users to change or reset their password, without administrator or help desk involvement.

If a user's account is locked or they forget their password, users can follow a prompt to reset their password and get back to work. Self-service password reset has several benefits:

- It increases security, as help desks add an additional security layer, which could be compromised.
- It saves the organization money by reducing the number of calls and requests to help desk staff.
- It increases productivity, allowing the user can get back to work faster.

Self-service password reset works in the following scenarios:

- Password change - when a user knows their password but wants to change it to something new.
- Password reset - when a user can't sign in, such as when they forgot password, and want to reset their password.
- Account unlock - when a user can't sign in because their account is locked out and want to unlock their account.

To use self-service password reset, users must be:

- Assigned an Azure AD license.
- Enabled for SSPR by an administrator.
- Registered, with the authentication methods they want to use. Two or more authentication methods are recommended in case one is unavailable.

The following authentication methods are available for SSPR:

- Mobile app notification

- Mobile app code
- Email
- Mobile phone
- Office phone
- Security questions

When a user resets their password using self-service password reset, that password can also be written back to an on-premises Active Directory. Password writeback allows users to use their updated credentials with on-premises devices and applications without a delay.

To keep users informed about account activity, admins can configure e-mail notifications to be sent when an SSPR event happens. These notifications can cover both regular user accounts and admin accounts. For admin accounts, this notification provides an additional layer of awareness when a privileged administrator account password is reset using SSPR. All global admins would be notified when SSPR is used on an admin account.

Interactive Guide

In this interactive guide, you'll enable self-service password reset for users in Azure Active Directory. Select the link below to get started.

Interactive guide - enable self-service password reset for users in Azure Active Directory.[19]

Describe password protection & management capabilities of Azure AD

Password Protection is a feature of Azure AD, which reduces the risk of users setting weak passwords. Azure AD Password Protection detects, and blocks known weak passwords and their variants, and can also block additional weak terms that are specific to your organization.

With Azure AD Password Protection, default global banned password lists are automatically applied to all users in an Azure AD tenant. To support your own business and security needs, you can define entries in a custom banned password list. When users change or reset their passwords, these banned password lists are checked to enforce the use of strong passwords.

You should use additional features like Azure Active Directory multi-factor authentication, not just rely on strong passwords enforced by Azure AD Password Protection.

Global banned password list

A global banned password list with known weak passwords is automatically updated and enforced by Microsoft. This is maintained by the Azure AD Identity Protection team, who analyze security telemetry data to find weak or compromised passwords. Examples of passwords that might be blocked are P@$$w0rd or Passw0rd1 and all variations. Variations are created using an algorithm that transposes text case and letters to numbers such as l to an 1. Variations on Password1 might include Passw0rd1, Pass0rd1, and a number of others. These passwords are then checked and added to the global banned password list and made available to all Azure AD users. The global banned password list is automatically applied and cannot be disabled.

19 https://edxinteractivepage.blob.core.windows.net/edxpages/Security%20fundamentals/LP02M03%20-%20Enable%20SSPR%20in%20Azure%20Active%20Directory/index.html?azure-portal=true

If an Azure AD user tries to set their password to one of these weak passwords, they receive a notification to choose a more secure password. The global banned list is sourced from real-world, actual password spray attacks. This approach improves the overall security and effectiveness, and the password validation algorithm also uses smart fuzzy-matching techniques. As a result, Azure AD Password Protection efficiently detects and blocks millions of the most common weak passwords from being used in your enterprise.

Custom banned password lists

Additionally, admins can create custom banned password lists to support specific business security needs. The custom banned password list prohibits passwords such as the organization name or location. Passwords added to the custom banned password list should be focused on organizational-specific terms such as:

- Brand names
- Product names
- Locations, such as company headquarters
- Company-specific internal terms
- Abbreviations that have specific company meaning

The custom banned password list is combined with the global banned password list to block variations of all the passwords.

Banned password lists are a feature of Azure AD Premium 1 or 2.

Protecting against password spray

Azure AD Password Protection helps you defend against password spray attacks. Most password spray attacks submit a small number of the known weakest passwords against each of the accounts in an enterprise. This technique allows the attacker to quickly search for an easily compromised account and avoid potential detection thresholds.

Azure AD Password Protection efficiently blocks all known weak passwords likely to be used in password spray attacks. This protection is based on real-world security telemetry data from Azure AD, which is used to build the global banned password list.

Hybrid security

For hybrid security, admins can integrate Azure AD password protection with an on-premises Active Directory environment. A component installed in the on-prem environment receives the global banned password list and custom password protection policies from Azure AD. Domain controllers then use them to process password change events. This hybrid approach makes sure that wherever a user changes their password, Azure AD password protection is applied.

Although password protection improves the strength of passwords, you should still use best practice features like Azure Active Directory multi-factor authentication. Passwords alone, even strong ones, are not as secure as multiple layers of security.

Knowledge check

Multiple choice

Item 1. After hearing of a security breach at a competitor, you want to improve identity security within your organization. What should you implement immediately to provide the greatest protection to user identities?

- ☐ Multi-factor authentication.
- ☐ Require biometrics for all sign-in.
- ☐ Require strong passwords for all identities.

Multiple choice

Item 2. To improve identity security within your organization, you want to implement Windows Hello for Business. When explaining the benefits of Windows Hello for Business to your colleagues, which of the following is true?

- ☐ Windows Hello is an authentication feature built into Windows Server 2012 R26.
- ☐ Windows Hello is an alternative to multi-factor authentication.
- ☐ Windows Hello for Business is more secure because it uses PINs and biometric data to authenticate users.

Multiple choice

Item 3. You've been asked to find ways to reduce IT costs, without compromising security. Which feature should you consider implementing?

- ☐ Self-service password reset.
- ☐ Biometric sign-in on all devices.
- ☐ FIDO2.

Summary and resources

In this lesson, you've seen why passwords are a problematic form of authentication. You've learned about the different types of authentication that can be used with Azure AD, including biometric data, Windows Hello, Microsoft Authenticator app, and using your phone for voice or SMS authentication.

You've learned how Azure AD can be configured to allow users to reset their own passwords, and how Azure AD Password Protection mitigates against the inherent risks associated with passwords.

Now that you've completed this lesson, you should be able to:

- Describe the secure authentication methods of Azure AD.
- Describe the password protection and management capabilities of Azure AD.

Learn more

- **What are security defaults?**[20]

20 https://docs.microsoft.com/azure/active-directory/fundamentals/concept-fundamentals-security-defaults

- **Licensing requirements for Azure Active Directory self-service password reset**[21]
- **FIDO2 security keys**[22]
- **Windows Hello biometrics in the enterprise**[23]
- **Windows Hello for Business**[24]
- **Windows Hello for Business Group Policy**[25]
- **What is Azure Active Directory Authentication?**[26]

21 https://docs.microsoft.com/azure/active-directory/authentication/concept-sspr-licensing
22 https://docs.microsoft.com/azure/active-directory/authentication/concept-authentication-passwordless#fido2-security-keys
23 https://docs.microsoft.com/windows/security/identity-protection/hello-for-business/hello-biometrics-in-enterprise
24 https://docs.microsoft.com/windows/security/identity-protection/hello-for-business/hello-overview
25 https://docs.microsoft.com/windows/security/identity-protection/hello-for-business/hello-manage-in-organization
26 https://docs.microsoft.com/azure/active-directory/authentication/overview-authentication

Describe the access management capabilities of Azure AD

Introduction

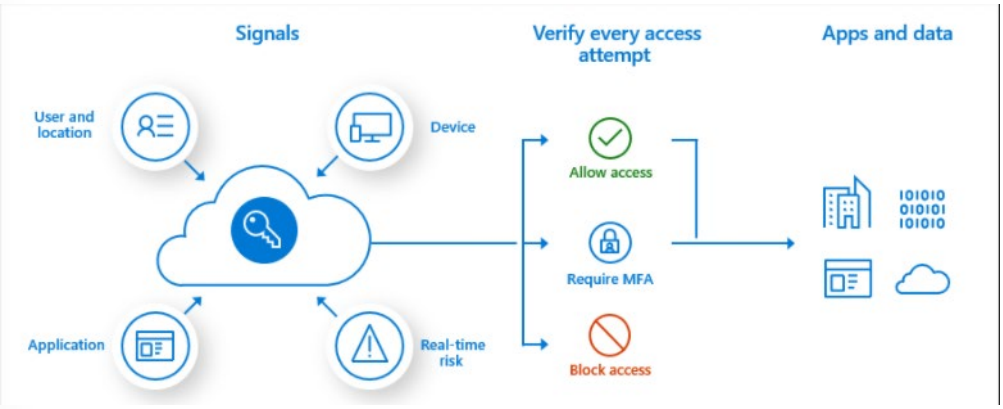
One of the main purposes of Azure AD is to manage access. The security perimeter has shifted away from organizational boundaries to user, device, and service identities. In this module, you will learn how Azure AD uses intelligent access management capabilities to protect organizational assets. This lesson considers how conditional access helps you to improve security, and how to use Azure AD roles to control access to Azure AD resources in a directory.

After completing this lesson, you'll be able to:

- Describe Conditional Access and its benefits.
- Describe Azure AD roles.

Describe conditional access in Azure AD

Conditional Access is a feature of Azure AD that provides an additional layer of security before allowing authenticated users to access data or other assets. Conditional Access is implemented through policies that are created and managed in Azure AD. A Conditional Access policy analyses signals including user, location, device, application, and risk to automate decisions for authorizing access to resources (apps and data).



A conditional access policy might state that IF a user belongs to a certain group, then they're required to provide multi-factor authentication to sign in to an application.

Watch this video, **Conditional Access**[27], to see how Conditional Access policies work.

Conditional Access signals

Conditional Access can use the following signals to control the who, what, and where of the policy:

- **User or group membership**. Policies can be targeted to specific users and groups (including admin roles), giving administrators fine-grained control over access.

27 https://www.microsoft.com/videoplayer/embed/RE4INyl

- **Named location information**. Named location information can be created using IP address ranges, then used when making policy decisions. Also, Administrators can opt to block or allow traffic from an entire countries IP range.
- **Device**. Users with devices of specific platforms or marked with a specific state can be used/
- **Application**. Users attempting to access specific applications can trigger different Conditional Access policies.
- **Real-time sign in risk detection**. Signals integration with Azure AD Identity Protection allows Conditional Access policies to identify risky sign-in behavior. Policies can then force users to perform password changes or multi-factor authentication to reduce their risk level or be blocked from access until an administrator takes manual action.
- **Cloud apps or actions**. Cloud apps or actions can include or exclude cloud applications or user actions that will be subject to the policy.
- **User risk**. For customers with access to Identity Protection, user risk can be evaluated as part of a Conditional Access policy. User risk represents the probability that a given identity or account is compromised. User risk can be configured for high, medium, low probability.

Access controls

Once the conditional access policy has been applied, an informed decision is reached whether to grant access, block access, or require additional verification. Common decisions are:

- Block access
- Grant access
- Require one or more conditions to be met before granting access:
    - Require multi-factor authentication.
    - Require device to be marked as compliant.
    - Require hybrid Azure AD joined device.
    - Require approved client app.
    - Require app protection policy.
    - Require password change.
- Control user access based on session controls to enable limited experiences within specific cloud applications. As an example, Conditional Access App Control, uses signals from Microsoft Cloud app security (MCAS) to block, download, cut, copy and print of sensitive documents, or to require labeling of sensitive files. Other session controls include sign-in frequency and application enforced restrictions. For selected applications, application enforced restrictions use device information to provide users with a limited or full experience, depending on the device state.

Conditional access policies can be targeted to members of specific groups or guests, for example, you can create a policy to exclude all guest accounts from accessing sensitive resources.
Conditional Access is a feature of paid Azure AD editions.

Interactive Guide

In this interactive guide, you'll create a conditional access policy for a group of users. Select the link below to get started.

Interactive guide - create a conditional access policy for a group of users.[28]

Describe Azure AD roles

Azure AD roles control permissions to manage Azure AD resources, such as allowing user accounts to be created, or billing information viewed. Azure AD supports built-in and custom roles.

Built-in roles

A few of the most common built-in roles include:

- *Global Administrator* - Users with this role have access to all administrative features in Azure Active Directory. The person who signs up for the Azure Active Directory tenant automatically becomes a Global Administrator.
- *User administrator* - Users with this role can create and manage all aspects of users and groups. Additionally, this role includes the ability to manage support tickets and monitor service health.
- *Billing administrator* – users with this role makes purchases, manages subscriptions, manages support tickets, and monitors service health.

There are many different built-in roles for different areas of responsibility. All built-in roles are pre-configured bundles of permissions designed for specific tasks.

Custom roles

Although there are many built-in admin roles in Azure AD, custom roles give flexibility when granting access.

Granting permission using custom Azure AD roles is a two-step process that involves creating a custom role definition, which consists of a collection of permissions that you add from a preset list. These permissions are the same permissions used in the built-in roles. Once you've created your role definition, you can assign it to a user by creating a role assignment. A role assignment grants the user the permissions in a role definition, at a specified scope. A custom role can be assigned at org-wide scope, meaning the role member has the role permissions over all resources in the organization. A custom role can also be assigned at an object scope. An example of an object scope would be a single application.

Unlike built-in roles, which are assigned at a tenant level and are pre-configured bundles of permissions designed for specific tasks; custom roles can be assigned at the resource level (such as a single application) and allow permissions to be added to a custom role definition.

Custom roles require an Azure AD Premium P1 or P2 license.

Azure AD role-based access control

Managing access using roles is known as role-based access control (RBAC). Azure AD built-in and custom roles are a form of RBAC in that Azure AD roles control access to Azure AD resources.

Only grant the access users need

It's a best practice, and more secure, to grant users the least privilege to get their work done. This means that if someone mostly manages users, you should assign the user administrator role, and not global

28 https://edxinteractivepage.blob.core.windows.net/edxpages/Security%20fundamentals/LP02M04%20-%20Create%20a%20Conditional%20Access%20Policy/index.html?azure-portal=true

administrator. This mitigates the risk of a user account being compromised, and a hacker locking you out of your account. By assigning least privileges, you limit the damage that could be done with a compromised account.

Knowledge check

Multiple choice

Item 1. You've been asked to implement conditional access for your organization, what must you do?

- ☐ Create and assign a policy that enforces organizational rules.
- ☐ Check that all users have multi-factor authentication enabled.
- ☐ Amend your apps to allow conditional access.

Multiple choice

Item 2. Sign in risk is a signal used by conditional access policies to decide whether to grant or deny access. What is sign in risk?

- ☐ The probability that the device is owned by the identity owner.
- ☐ The probability that the authentication request is authorized by the identity owner.
- ☐ The probability that the user is authorized to view data from a particular application.

Multiple choice

Item 3. You've been asked to review Azure AD roles assigned to users to improve organizational security. Which of the following should you implement?

- ☐ Remove all Global Admin roles assigned to users.
- ☐ Create custom roles.
- ☐ Replace Global Admin roles with specific Azure AD roles.

Summary and resources

In this lessib, you've learned about Conditional Access and how it's used to protect resources. You've seen how Conditional Access policies use *if then* statements with signals to determine whether to grant access, require more information, or block access.

You also learned about built-in admin roles, and custom roles in Azure AD. And you found out about the concept of least privilege access, and how this protects resources.

Now that you've completed this lesson, you'll be able to:

- Describe Conditional Access and its benefits.
- Describe Azure AD roles.

Learn more

For more information about the topics raised in this lesson, see:

- **Conditional Access**[29]
- **Security defaults**[30]
- **Understand roles in Azure Active Directory**[31]
- **Azure AD built-in roles**[32]
- **Overview of role-based access control in Azure Active Directory**[33]

29 https://docs.microsoft.com/azure/active-directory/conditional-access/overview
30 https://docs.microsoft.com/azure/active-directory/fundamentals/concept-fundamentals-security-defaults
31 https://docs.microsoft.com/azure/active-directory/roles/concept-understand-roles
32 https://docs.microsoft.com/azure/active-directory/roles/permissions-reference
33 https://docs.microsoft.com/azure/active-directory/roles/custom-overview

Describe the identity protection and governance capabilties of Azure AD

Introduction

Identity governance is concerned with balancing identity security with user productivity in a way that can be justified and audited. Azure AD provides many identity protection and governance capabilities, including Privileged Identity Management, Identity Protection, and terms of use statements.

After completing this lesson, you'll be able to:

- Describe the identity governance capabilities of Azure AD.
- Describe the benefits of Privileged Identity Management (PIM).
- Describe the capabilities of Azure AD Identity Protection.

Describe identity governance in Azure AD

Azure AD identity governance gives organizations the ability to do the following tasks:

- Govern the identity lifecycle.
- Govern access lifecycle.
- Secure privileged access for administration.

These actions can be completed for employees, business partners and vendors, and across services and applications, both on-premises and in the cloud.

It's intended to help organizations address these four key questions:

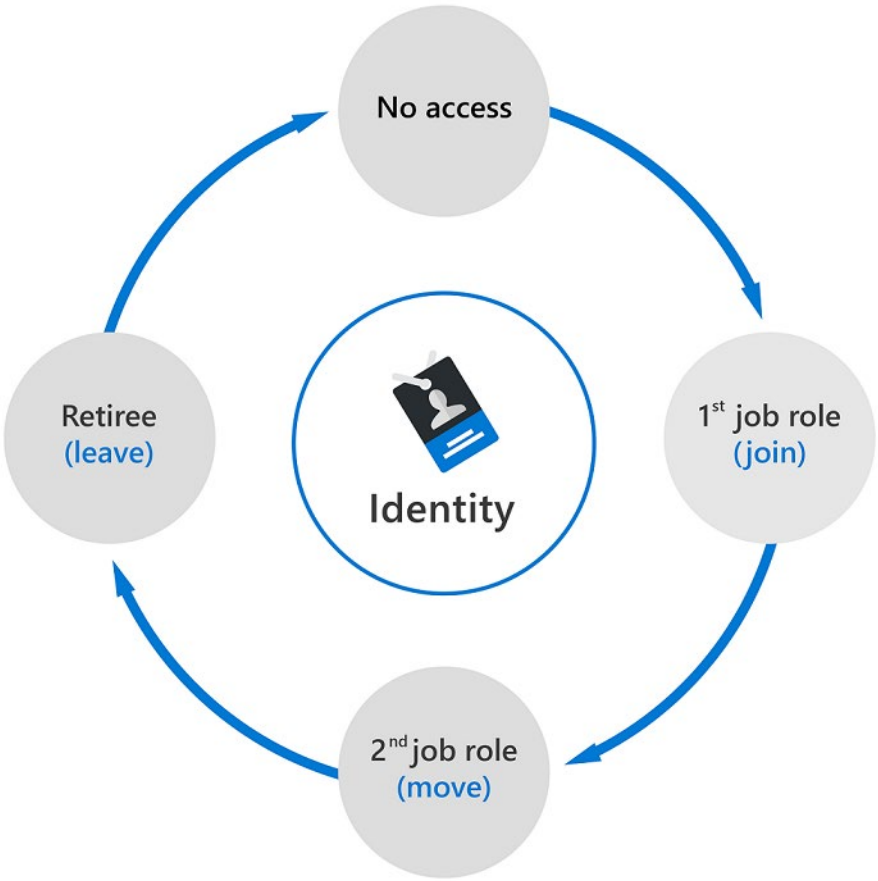
- Which users should have access to which resources?
- What are those users doing with that access?
- Are there effective organizational controls for managing access?
- Can auditors verify that the controls are working?

Identity lifecycle

Managing users' identity lifecycle is at the heart of identity governance.

When planning identity lifecycle management for employees, for example, many organizations model the "join, move, and leave" process. Or, when an individual first joins an organization, a new digital identity is created if one isn't already available. When an individual moves between organizational boundaries, more access authorizations may need to be added or removed to their digital identity. When an individual leaves, access may need to be removed, and the identity might no longer be required, other than for audit purposes.

The diagram below shows a simplified version of the identity lifecycle.



For many organizations, this identity lifecycle for employees is tied to the representation of that user in a human resources (HR) system such as Workday or SuccessFactors. The HR system is authoritative for providing the current list of employees, and some of their properties, such as name or department.

Azure AD Premium offers integration with cloud-based HR systems. When a new employee is added to an HR system, Azure AD can create a corresponding user account. Similarly, when their properties, such as department or employment status, change in the HR system, synchronization of those updates to Azure AD ensures consistency.

Azure AD Premium also includes Microsoft Identity Manager, which can import records from on-premises HR systems such as SAP HCM, Oracle eBusiness, and Oracle PeopleSoft.

In general, managing the lifecycle of an identity is about updating the access that users need, whether through integration with an HR system, or through the user provisioning applications.

Access lifecycle

Access lifecycle is the process of managing access throughout the user's organizational life. Users require different levels of access from the point at which they join an organization to when they leave it. At various stages in between, they'll need access rights to different resources depending on their role and responsibilities.

Organizations can automate the access lifecycle process through technologies such as dynamic groups. Dynamic groups enable admins to create attribute-based rules to determine membership of groups. When any attributes of a user or device change, the system evaluates all dynamic group rules in a directory to see if the change would trigger any users to be added or removed from a group. If a user or device satisfies a rule for a group, they're added as a member of that group. If they no longer satisfy the rule, they're removed.

Privileged access lifecycle

Monitoring privileged access is a key part of identity governance. When employees, vendors, and contractors are assigned administrative rights, there should be a governance process because of the potential for misuse.

Azure AD Privileged Identity Management (PIM), provides extra controls tailored to securing access rights. PIM helps you minimize the number of people who have access to resources across Azure AD, Azure, and other Microsoft online services. PIM provides a comprehensive set of governance controls to help secure your company's resources. PIM is a feature of Azure AD Premium P2.

Describe entitlement management, access reviews, and terms of use

Entitlement management is an identity governance feature that enables organizations to manage identity and access lifecycle at scale. Entitlement management automates access request workflows, access assignments, reviews, and expiration.

Enterprise organizations often face challenges when managing employee access to resources such as:

- Users may not know what access they should have, and even if they do, they might have difficulty locating the right individuals to approve it.
- When users find and receive access to a resource, they may hold on to access longer than is required for business purposes.
- Managing access for external users.

Entitlement management includes the following capabilities to address these challenges:

- Delegate the creation of access packages to nonadministrators. These access packages contain resources that users can request. The delegated access package managers then define policies that include rules such as which users can request access, who must approve their access, and when access expires.
- Managing external users. When a user who isn't yet in your directory requests access, and is approved, they're automatically invited into your directory and assigned access. When their access expires, if they have no other access package assignments, their B2B account in your directory can be automatically removed.

The video, **What is Azure AD entitlement management?**[34] introduces entitlement management, and looks at how access packages are used to give access to resources.

Entitlement management is a feature of Azure AD Premium P2.

34 https://www.microsoft.com/videoplayer/embed/RE4JXQr

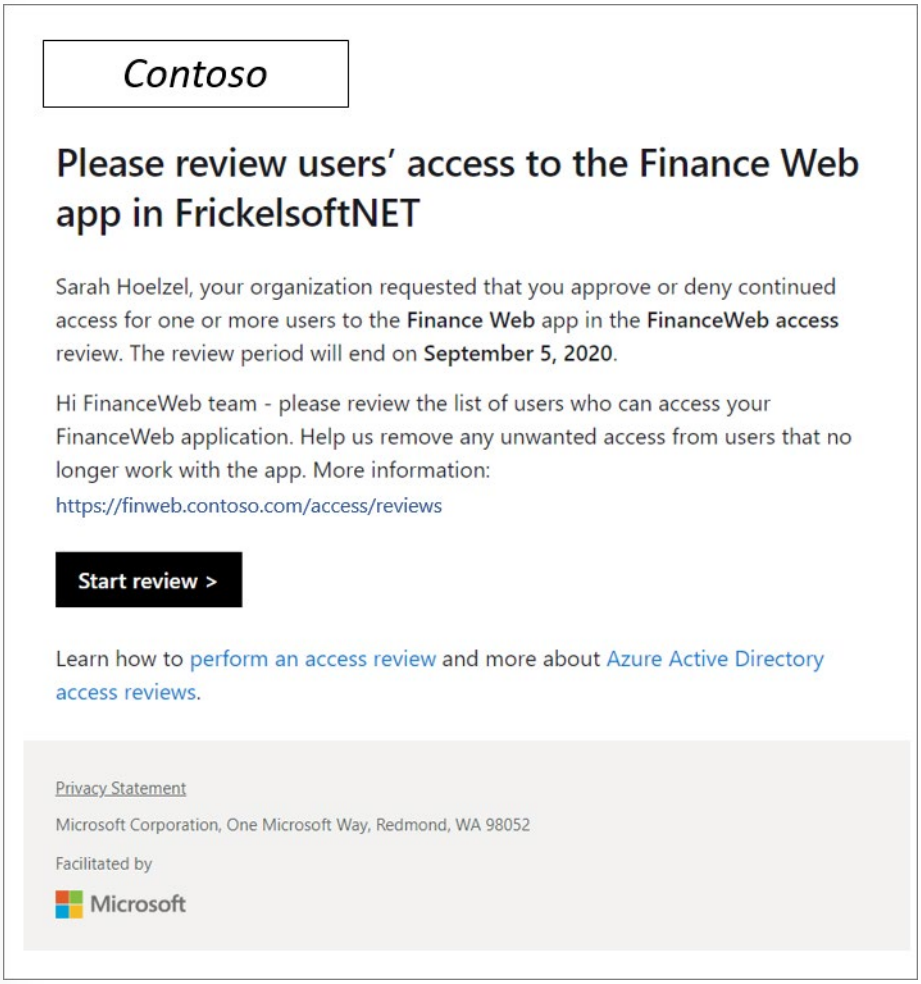
Azure AD access reviews

Azure Active Directory (AD) access reviews enable organizations to efficiently manage group memberships, access to enterprise applications, and role assignment. Regular access reviews ensure that only the right people have access to resources. Excessive access rights are a known security risk. However, when people move between teams, or take on or relinquish responsibilities, access rights can be difficult to control.

Access reviews are helpful when:

- You have too many users in privileged roles, such as global administrator.
- When automation isn't possible, such as when HR data isn't in Azure AD.
- You want to control business critical data access.
- Your governance policies require periodic reviews of access permissions.

Access reviews can be created through Azure AD access reviews, or Azure AD Privileged Identity Management (PIM). Access reviews can be used to review and manage access for both users and guests. When an access review is created, it can be set up so that each user reviews their own access, or to have one or more users review everyone's access. Similarly, all guests can be asked to review their own access, or have it looked at by one or more users.



Admins who create access reviews can track progress as the reviewers complete their process. No access rights are changed until the review is finished. You can, however, stop a review before it reaches its scheduled end.

When the review is complete, it can be set to manually or auto-apply changes to remove access from a group membership or application assignment, except for a dynamic group or a group that originates on-premises. In those cases, the changes must be applied directly to the group.

Access reviews are a feature of Azure AD Premium P2.

Azure AD terms of use

Azure AD terms of use allow information to be presented to users, before they access data or an application. Terms of use ensure users read relevant disclaimers for legal or compliance requirements.

Employees or guests can be required to accept terms of use in the following situations:

- Before they access sensitive data or an application.
- On a recurring schedule, so they're reminded of regulations.
- When terms of use are required in different languages.
- Based on user attributes, such as terms applicable to certain roles.
- Presenting terms for all users in your organization.

Terms of use are presented in a PDF format, using content that you create, such as an existing contract document. Terms of use can also be presented to users on mobile devices.

Conditional Access policies are used to require a terms of use statement being displayed, and ensuring the user has agreed to those terms before accessing an application. Admins can then view who has agreed to terms of use, and who has declined.

Describe the capabilities of Privileged identity Management

Privileged Identity Management (PIM) is a service in Azure Active Directory (Azure AD) that enables you to manage, control, and monitor access to important resources in your organization. These include resources in Azure AD, Azure, and other Microsoft online services such as Microsoft 365 or Microsoft Intune. PIM mitigates the risks of excessive, unnecessary, or misused access permissions. It requires justification to understand why users want permissions, and enforces multifactor authentication to activate any role.

PIM is:

- Just in time, providing privileged access only when needed, and not before.
- Time-bound, by assigning start and end dates that indicate when a user can access resources.
- Approval-based, requiring specific approval to activate privileges.
- Visible, sending notifications when privileged roles are activated.
- Auditable, allowing a full access history to be downloaded.

Privileged Identity Management is a feature of Azure AD Premium P2.

Why use PIM?

PIM reduces the chance of a malicious actor getting access by minimizing the number of people who have access to secure information or resources. By time-limiting authorized users, it reduces the risk of an authorized user inadvertently affecting sensitive resources. PIM also provides oversight for what users are doing with their administrator privileges. PIM mitigates the risk to organizations of elevated privileges.

For a more detailed look at PIM and why you might use it, watch **What is Privileged Identity Management?**[35].

Describe Azure Identity Protection

Identity Protection is a tool that allows organizations to accomplish three key tasks:

- Automate the detection and remediation of identity-based risks.
- Investigate risks using data in the portal.
- Export risk detection data to third-party utilities for further analysis.

Microsoft analyses 6.5 trillion signals per day to identify potential threats. These signals come from learnings Microsoft has acquired from their position in organizations with Azure AD, the consumer space with Microsoft Accounts, and in gaming with Xbox.

The signals generated by these services are fed to Identity Protection, so they can then be used by tools such as Conditional Access, which uses Identity Protection signals to make access decisions. These signals are also fed to security information and event management (SIEM) tools, such as Sentinel, for further investigation.

Identity Protection categorizes risk into three tiers: low, medium, and high. Additionally, it can calculate the sign-in risk, and user identity risk.

Sign-in risk is the probability that the sign-in wasn't performed by the user, and uses the following signals to calculate the risk:

- Atypical travel. Sign in from an atypical location based on the user's recent sign-ins.
- Anonymous IP address. Sign in from an anonymous IP address (for example: Tor browser, anonymized VPNs).

User risk is a probability that the user identity has been compromised, and uses the following signals to calculate the risk:

- Unfamiliar sign-in properties. Sign in with properties we've not seen recently for the given user.
- Malware linked IP address. Sign in from a malware linked IP address.
- Leaked Credentials. Indicates that the user's valid credentials have been leaked.
- Password spray. Indicates that multiple usernames are being attacked using common passwords in a unified, brute-force manner.
- Azure AD threat intelligence. Microsoft's internal and external threat intelligence sources have identified a known attack pattern.

These risk signals can trigger actions such as requiring users to provide multi-factor authentication, reset their password, or block access until an administrator takes action.

35 https://www.microsoft.com/videoplayer/embed/RE4JXQr

Identity Protection provides organizations with three reports that they can use to investigate identity risks in their environment. These reports are the **risky users**, **risky sign-ins**, and **risk detections** reports. Investigation of events is key to understanding and identifying any weak points in your security strategy.

After completing an investigation, admins will want to take action to remediate the risk or unblock users. Organizations also have the option to enable automated remediation using their risk policies. Microsoft recommends closing events as soon as possible because time matters when working with risk.

Identity protection is a feature of Azure AD Premium P2.

Knowledge check

Multiple choice

Item 1. Your organization has implemented important changes in their customer facing web-based applications. You want to ensure that any user who wishes to access these applications agrees to the legal disclaimers. Which Azure AD feature should you implement?

- ☐ Identity protection.
- ☐ Entitlement management.
- ☐ Azure AD Terms of Use.

Multiple choice

Item 2. Your organization is project-oriented with employees often working on more than one project at a time. Which solution is best suited to managing user access to your organization's resources?

- ☐ Azure Terms of Use.
- ☐ Identity protection.
- ☐ Entitlement management.

Multiple choice

Item 3. Your organization has recently conducted a security audit and found that four people who have left the organization were still active and assigned Global Admin roles. The users have now been deleted and you've been asked to recommend a solution to prevent a similar security lapse happening in future. Which solution should you recommend?

- ☐ Entitlement Management.
- ☐ Privileged Identity Management.
- ☐ Identity protection.

Multiple choice

Item 4. You've recently discovered that several user accounts in the Finance Department have been compromised. Your CTO has asked for your help in finding a solution to reduce the impact of compromised user accounts. They've asked you to look at three Azure AD features, which one should you recommend?

- ☐ Identity protection.
- ☐ Conditional access.
- ☐ Entitlement management.

Summary and resources

In this lesson, you learned how Azure AD provides tools to help you govern the identity lifecycle and the access lifecycle. You've seen how Azure AD can be synchronized with human resources (HR) systems to manage identity lifecycles at scale. You also learned how dynamic groups can automate attribute-based rules to determine who is in a particular group.

This lesson discussed entitlement management, which automates access requests, access assignments, reviews, and expiration. You also learned about how these reviews can help you monitor who has access to what resources.

Finally, you learned how Privileged Identity Management (PIM) can help you minimize the number of users who have access to important resources, and how Identity Protection can detect potential identity risks.

Now that you've completed this lesson, you should be able to:

- Describe the identity governance capabilities of Azure AD.
- Describe the benefits of PIM.
- Describe the capabilities of Azure AD Identity Protection.

Learn more

For more information about the topics raised in this lesson, see:

- **Azure AD Identity governance**[36]
- **Azure AD Privileged Identity Management**[37]
- **Azure AD access reviews**[38]
- **Azure terms of use statements**[39]
- **Dynamic groups in Azure AD**[40]
- **Azure entitlement management**[41]
- **Azure Identity Protection**[42]
- **Microsoft Identity Manager**[43]

36 https://docs.microsoft.com/azure/active-directory/governance/identity-governance-overview
37 https://docs.microsoft.com/azure/active-directory/privileged-identity-management/pim-configure
38 https://docs.microsoft.com/azure/active-directory/governance/access-reviews-overview
39 https://docs.microsoft.com/azure/active-directory/conditional-access/terms-of-use
40 https://docs.microsoft.com/azure/active-directory/enterprise-users/groups-dynamic-membership
41 https://docs.microsoft.com/azure/active-directory/governance/entitlement-management-overview
42 https://docs.microsoft.com/azure/active-directory/identity-protection/overview-identity-protection
43 https://docs.microsoft.com/microsoft-identity-manager/microsoft-identity-manager-2016

Answers

Multiple choice

Item 1. Your organization is launching a new app for customers. You want your customers to use a sign-in screen that is customized with your brand identity. Which type of Azure External identity authentication solution should you use?

- ☐ Azure AD B2B
- ■ Azure AD B2C
- ☐ Azure AD Hybrid identities

Explanation
Azure AD B2C is an authentication solution for customers that you can customize with your brand identity.

Multiple choice

Item 2. Within your organization, all your users have Microsoft 365 cloud identities. Which identity model should you use?

- ☐ Hybrid
- ■ Cloud-only
- ☐ On-premises only

Explanation
When all your users have cloud identities, you use the cloud-only model.

Multiple choice

Item 3. You have developed an app and want users to be able to sign in with their Facebook, Google, or Twitter credentials. What type of authentication will you use?

- ☐ Service principal authentication
- ■ Azure AD B2C
- ☐ User assigned identities

Explanation
Azure AD B2C allows external users to log in with their preferred social media account to sign in to your application, such as Facebook, Google, or Twitter.

Multiple choice

Item 1. After hearing of a security breach at a competitor, you want to improve identity security within your organization. What should you implement immediately to provide the greatest protection to user identities?

- ■ Multi-factor authentication.
- ☐ Require biometrics for all sign-in.
- ☐ Require strong passwords for all identities.

Explanation
Multi-factor authentication dramatically improves the security of an identity.

Multiple choice

Item 2. To improve identity security within your organization, you want to implement Windows Hello for Business. When explaining the benefits of Windows Hello for Business to your colleagues, which of the following is true?

- ☐ Windows Hello is an authentication feature built into Windows Server 2012 R26.
- ☐ Windows Hello is an alternative to multi-factor authentication.
- ■ Windows Hello for Business is more secure because it uses PINs and biometric data to authenticate users.

Explanation
Windows Hello for Business uses a PIN and biometric data to authenticate users and does not transmit data to an external server.

Multiple choice

Item 3. You've been asked to find ways to reduce IT costs, without compromising security. Which feature should you consider implementing?

- ■ Self-service password reset.
- ☐ Biometric sign-in on all devices.
- ☐ FIDO2.

Explanation
Self-service password reset allows users to change or reset their own passwords, thereby reducing the cost of providing administrators and help desk personnel.

Multiple choice

Item 1. You've been asked to implement conditional access for your organization, what must you do?

- ■ Create and assign a policy that enforces organizational rules.
- ☐ Check that all users have multi-factor authentication enabled.
- ☐ Amend your apps to allow conditional access.

Explanation
Conditional access is implemented using policies that enforce organizational rules.

Multiple choice

Item 2. Sign in risk is a signal used by conditional access policies to decide whether to grant or deny access. What is sign in risk?

- ☐ The probability that the device is owned by the identity owner.
- ■ The probability that the authentication request is authorized by the identity owner.
- ☐ The probability that the user is authorized to view data from a particular application.

Explanation
Sign in risk is the real-time calculation that a given authentication was made by the specific user's identity.

Multiple choice

Item 3. You've been asked to review Azure AD roles assigned to users to improve organizational security. Which of the following should you implement?

☐ Remove all Global Admin roles assigned to users.

☐ Create custom roles.

■ Replace Global Admin roles with specific Azure AD roles.

Explanation
By following the least privilege security model and assigning specific admin roles such as billing administrator, or user administrator to more users, instead of global admin roles, you can improve organizational security.

Multiple choice

Item 1. Your organization has implemented important changes in their customer facing web-based applications. You want to ensure that any user who wishes to access these applications agrees to the legal disclaimers. Which Azure AD feature should you implement?

☐ Identity protection.

☐ Entitlement management.

■ Azure AD Terms of Use.

Explanation
Azure AD terms of use allow information to be presented to users, before they access data or an application, and can be configured to require users to accept the terms of use.

Multiple choice

Item 2. Your organization is project-oriented with employees often working on more than one project at a time. Which solution is best suited to managing user access to your organization's resources?

☐ Azure Terms of Use.

☐ Identity protection.

■ Entitlement management.

Explanation
Entitlement management is well suited to handling project-based access needs. Entitlement management automates access requests, access assignments, reviews, and expiration for bundles of resources relevant to a project.

Multiple choice

Item 3. Your organization has recently conducted a security audit and found that four people who have left the organization were still active and assigned Global Admin roles. The users have now been deleted and you've been asked to recommend a solution to prevent a similar security lapse happening in future. Which solution should you recommend?

☐ Entitlement Management.

■ Privileged Identity Management.

☐ Identity protection.

Explanation
Privileged Identity Management mitigates the risks of excessive, unnecessary, or misused access permissions.

Multiple choice

Item 4. You've recently discovered that several user accounts in the Finance Department have been compromised. Your CTO has asked for your help in finding a solution to reduce the impact of compromised user accounts. They've asked you to look at three Azure AD features, which one should you recommend?

- ■ Identity protection.
- ☐ Conditional access.
- ☐ Entitlement management.

Explanation
Identity protection is a tool that allows organizations to utilize security signals to identify potential threats.

Module 3 Describe the capabilties of Microsoft security solutions

Describe the basic security capabilities in Azure

Introduction

The traditional network security perimeter is changing as more companies move to either a hybrid cloud environment, with some resources located on-premises and some in the cloud, or a fully cloud-based network solution. Protection of your organization's assets, resources, and data is essential.

Threats can come from any direction: for instance, a Denial of Service attack on your organization's services, or a hacker trying to access your network by attempting to penetrate your firewall. Azure offers a wide array of configurable security tools that can be customized to give you the security and control to meet your organization's needs.

In this lesson, you'll explore many different services and features of Azure that can help protect your networks, assets, and resources, including network security groups, Azure Firewall, and Azure DDoS protection. You'll also look at the different ways in which encryption is used to protect your data.

After completing this lesson, you'll be able to:

- Describe Azure security capabilities for protecting your network.
- Describe how Azure can protect your VMs.
- Describe how encryption on Azure can protect your data.

Describe Azure Network Security groups

In today's modern work environment, where more users are working remotely from home, managing access to assets and resource on your Azure virtual network (VNet) is essential.

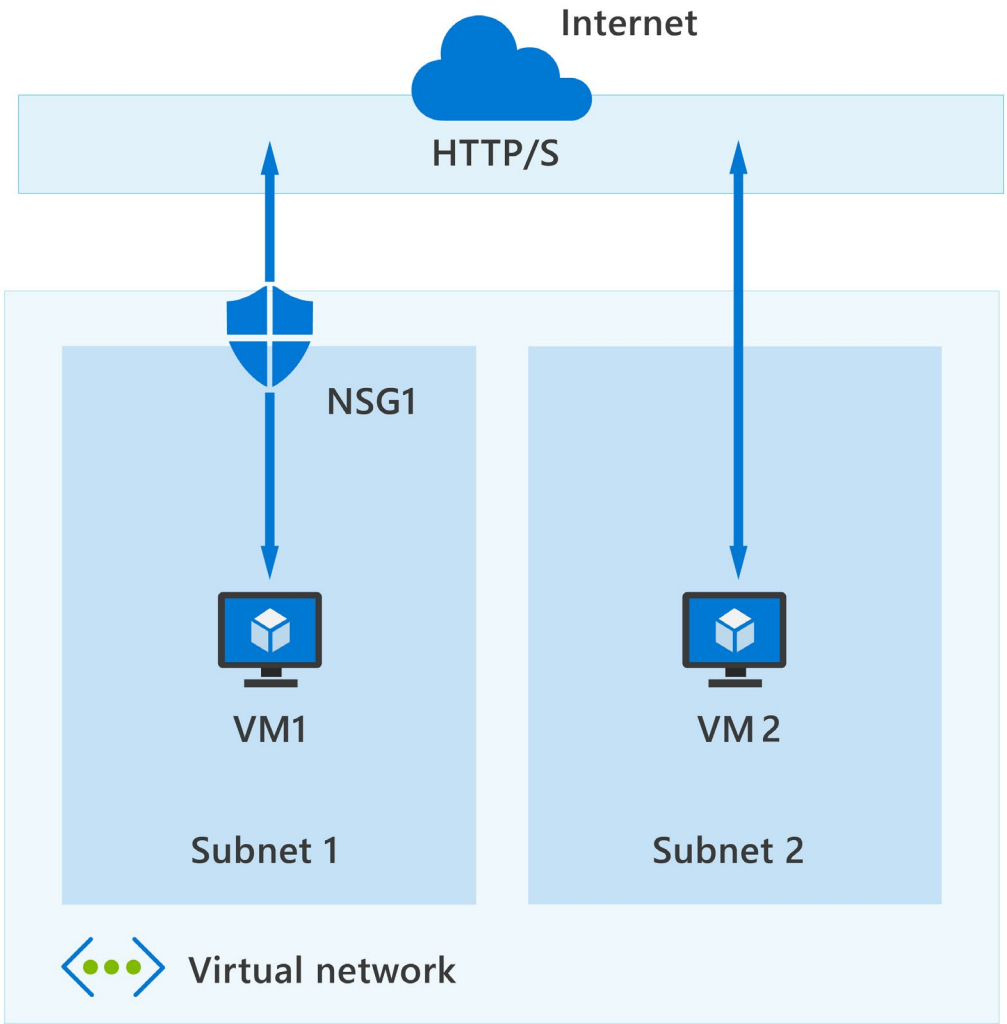
Here, you'll learn how Azure network security groups can automatically allow or deny traffic to your cloud-based resources and assets.

An Azure virtual network is similar to the network you'd find in your organization. It enables different Azure resources, for instance, an Azure virtual machine (VM), to securely communicate with other VNets, the internet, or your on-premises network. A VNet can be divided into multiple subnetworks (subnets), each with specific resources assigned to them. You can secure the resources within a subnet using network security groups.

Network security groups

Network security groups (NSGs) let you allow or deny network traffic to and from Azure resources that exist in your Azure virtual network; for example, a virtual machine. When you create an NSG, it can be associated with multiple subnets or network interfaces in your VNet. An NSG consists of rules that define how the traffic is filtered.

NSG security rules are evaluated by priority using five information points: source, source port, destination, destination port, and protocol to either allow or deny the traffic. As a guideline, you shouldn't create two security rules with the same priority and direction.



In the above, highly simplified, diagram you can see an Azure virtual network with two subnets that are connected to the internet, and each subnet has a virtual machine. Subnet 1 has an NSG assigned to it that's filtering inbound and outbound access to VM1, which needs a higher level of access. In contrast, VM2 could represent a public-facing machine that doesn't require an NSG.

Inbound and outbound security rules

As you've seen, an NSG controls access to resources on your virtual network and any subnets. An NSG is made up of inbound and outbound security rules. For each rule, you can specify a source and destination, port, protocol, and the required action if it's triggered. As previously mentioned, the rules are processed based on their priority. By default, Azure creates a series of rules, three inbound and three outbound rules, to provide a baseline level of security. You can't remove the default rules, but you can override them by creating new rules with higher priorities.

Each rule specifies one or more of the following properties:

- **Name**: Every NSG rule needs to have a unique name that describes its purpose. For example, Admin-AccessOnlyFilter.
- **Priority**: A number between 100 and 4096. Rules are processed in priority order, with lower numbers processed before higher numbers. When traffic matches a rule, processing stops. This means that any other rules with a lower priority (higher numbers) won't be processed.
- **Source or destination**: Specify either individual IP address or an IP address range, service tag (a group of IP address prefixes from a given Azure service), or application security group. Specifying a range, a service tag, or application security group, enables you to create fewer security rules.
- **Protocol**: What network protocol will the rule check? The protocol can be any of: TCP, UDP, ICMP or Any.
- **Direction**: Whether the rule should be applied to inbound or outbound traffic.
- **Port range**: You can specify an individual or range of ports. For example, you could specify 80 or 10000-10005. Specifying ranges enables you to be more efficient when creating security rules. You can't specify multiple ports or port ranges in the same security rule in NSGs created through the classic deployment model.
- **Action**: Finally, you need to decide what will happen when this rule is triggered.

There are limits to the number of security rules you can create in an NSG. Use Azure NSGs to automatically allow or deny traffic to your cloud-based resources and assets.

Describe Azure DDoS protection

Any company, large or small, can become the target of a large-scale network attack. The nature of these attacks against your network might be simply to make a statement, or simply because the attacker wanted a challenge.

Distributed Denial of Service Attacks

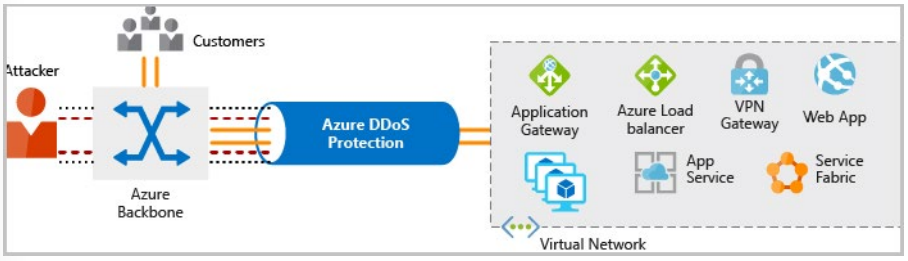
The aim of a Distributed Denial of Service (DDoS) attack is to overwhelm the resources on your applications and servers, making them unresponsive or slow for genuine users. A DDoS attack will usually target any public-facing endpoint that can be accessed through the Internet.

The three most popular types of Distributed Denial of Service attack are:

- **Volumetric attacks**: These are volume-based attacks that flood the network with seemingly legitimate traffic, overwhelming the available bandwidth. Legitimate traffic isn't able to get through. These types of attacks are measured in bits per second.
- **Protocol attacks**: Protocol attacks render a target inaccessible by exhausting server resources with false protocol requests that exploit weaknesses in layer 3 (network) and layer 4 (transport) protocols. These types of attacks are typically measured in packets per second.
- **Resource (application) layer attacks**: These attacks target web application packets, to disrupt the transmission of data between hosts.

What is Azure DDoS Protection

The Azure DDoS Protection service is designed to help protect your applications and servers by analyzing network traffic and discarding anything that looks like a DDoS attack.



In the diagram above, Azure DDoS Protection identifies the attacker's attempt to overwhelm the network. It blocks traffic from the attacker, ensuring that traffic never reaches Azure resources. Legitimate traffic from customers still flows into Azure without any interruption of service.

Azure DDoS Protection uses the scale and elasticity of Microsoft's global network to bring DDoS mitigation capacity to every Azure region. During a DDoS attack, Azure can scale your computing needs to meet demand. DDoS Protection can manage your cloud consumption by ensuring that your network load only reflects actual customer usage.

Azure DDoS Protection comes in two tiers:

- **Basic**: The Basic service tier is automatically enabled, for every property in Azure, at no extra cost. as part of the Azure platform. Always-on traffic monitoring and real-time mitigation of common network-level attacks provide the same defenses that Microsoft's online services use. Azure's global network is used to distribute and mitigate attack traffic across regions.
- **Standard**: The Standard service tier provides extra mitigation capabilities that are tuned specifically to Microsoft Azure Virtual Network resources. DDoS Protection Standard is simple to enable and requires no application changes. Protection policies are tuned through dedicated traffic monitoring and machine learning algorithms. Policies are applied to public IP addresses, which are associated with resources deployed in virtual networks, such as Azure Load Balancer and Application Gateway.

Azure DDoS pricing

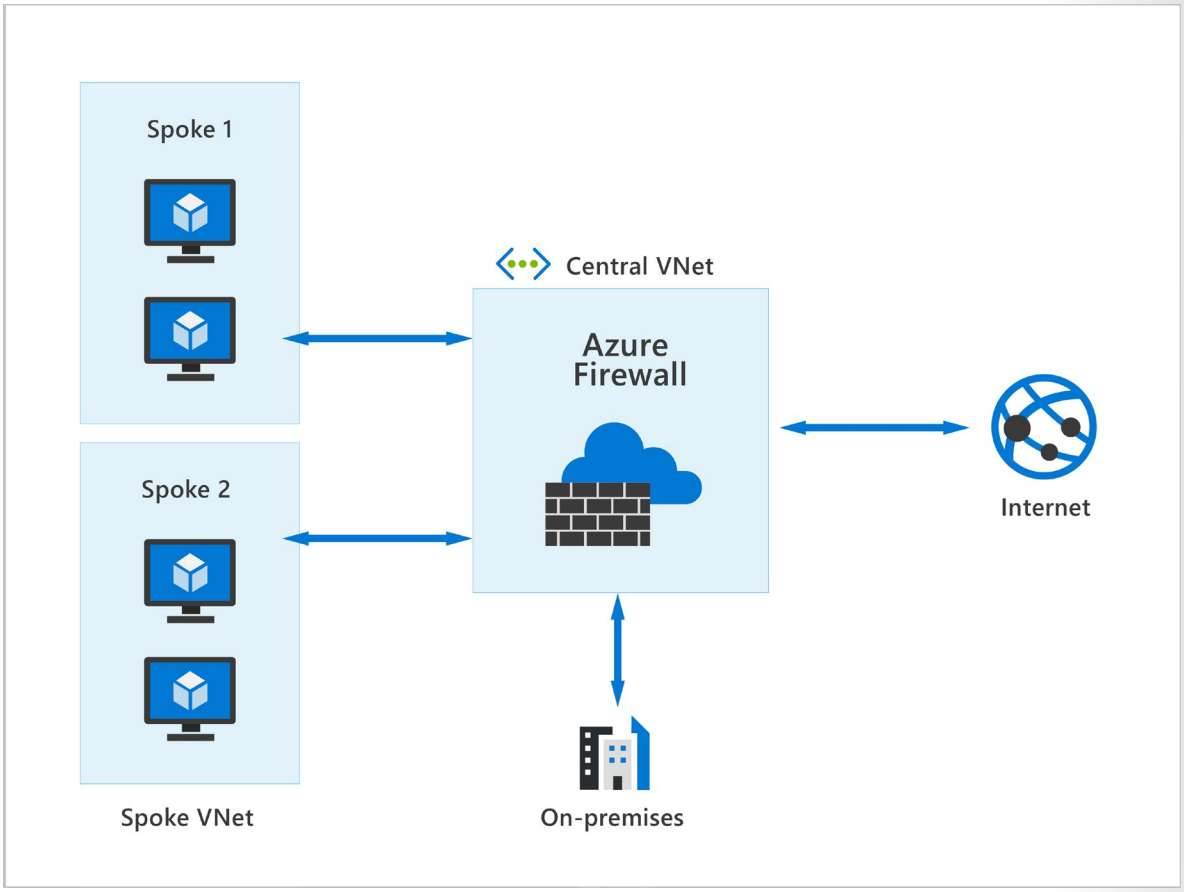
The DDoS Standard Protection service will have a fixed monthly charge. The fixed monthly charge includes protection for 100 resources. Protection for additional resources will be charged on a monthly per-resource basis.

For more information on pricing, visit the **Azure DDoS Protection pricing page**[1].

Use Azure DDoS to enable you to protect your devices and applications by analyzing traffic across your network, and taking appropriate action on suspicious traffic.

Describe what is Azure Firewall

Azure Firewall is a managed, cloud-based network security service that protects your Azure virtual network (VNet) resources from attackers. You can deploy Azure Firewall on any virtual network but the best approach is to use it on a centralized virtual network. All your other virtual and on-premises networks will then route through it. The advantage of this model is the ability to centrally exert control of network traffic for all your VNets across different subscriptions.



With Azure Firewall, you can scale up the usage to accommodate changing network traffic flows, so you don't need to budget for peak traffic. Network traffic is subjected to the configured firewall rules when you route it to the firewall as the subnet default gateway.

Key features of Azure Firewall

Azure Firewall comes with many features, including but not limited to:

- **Built-in high availability and availability zones**: High availability is built in so there's nothing to configure. Also, Azure Firewall can be configured to span multiple availability zones for increased availability.

1 https://azure.microsoft.com/pricing/details/ddos-protection/

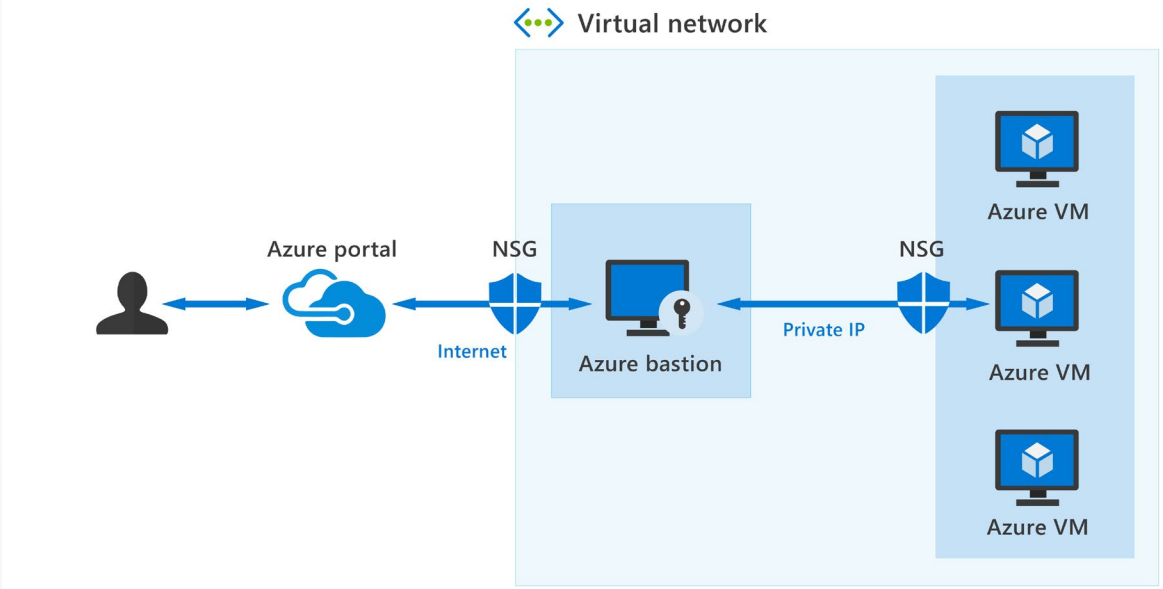
- **Network and application level filtering**: Use IP address, port, and protocol to support fully qualified domain name filtering for outbound HTTP(s) traffic and network filtering controls.
- **Outbound SNAT and inbound DNAT to communicate with internet resources**: Translate the private IP address of network resources to an Azure public IP address (source network address translation) to identify and allow traffic originating from the virtual network to internet destinations. Similarly, inbound internet traffic to the firewall public IP address is translated (Destination Network Address Translation) and filtered to the private IP addresses of resources on the virtual network.
- **Multiple public IP addresses**: Multiple public IP addresses (up to 250) can be associated wtih your firewall.
- **Threat intelligence**: Threat intelligence-based filtering can be enabled for your firewall to alert and deny traffic from/to known malicious IP addresses and domains.
- **Integration with Azure Monitor**: Integrated with Azure Monitor to enable collecting, analyzing, and acting on telemetry from Azure Firewall logs.

Use Azure Firewall to help protect the Azure resources you've connected to Azure Virtual Networks.

Describe what is Azure Bastion

Let's assume you've set up multiple virtual networks that use a combination of NSGs and Azure Firewalls to protect and filter access to the assets and resources, including virtual machines (VMs). You're now protected from external threats, but need to allow your developers and data scientist, who are working remotely, direct access to those VMs.

In a traditional model, you'd need to expose the Remote Desktop Protocol (RDP) and Secure Shell (SSH) ports to the internet. These protocols can be used to gain remote access to your VMs. This process creates a significant surface threat that can be exploited by attackers.



Azure Bastion provides secure and seamless RDP/SSH connectivity to your virtual machines directly from the Azure portal using Transport Layer Security (TLS). When you connect via Azure Bastion, your virtual machines don't need a public IP address, agent, or special client software.

Bastion provides secure RDP and SSH connectivity to all VMs in the virtual network in which it's provisioned. Using Azure Bastion protects your virtual machines from exposing RDP/SSH ports to the outside world, while still providing secure access using RDP/SSH.

Azure Bastion deployment is per virtual network, not per subscription/account or virtual machine. When you provision an Azure Bastion service in your virtual network, the RDP/SSH experience is available to all your VMs in the same virtual network.

Key features of Azure Bastion

The following features are available:

- **RDP and SSH directly in Azure portal**: You get to the RDP and SSH session directly in the Azure portal, using a single-click experience.
- **Remote session over TLS and firewall traversal for RDP/SSH**: Use an HTML5-based web client that's automatically streamed to your local device. You'll get your Remote Desktop Protocol (RDP) and Secure Shell (SSH) to traverse the corporate firewalls securely.
- **No Public IP required on the Azure VM**: Azure Bastion opens the RDP/SSH connection to your Azure virtual machine using private IP on your VM. You don't need a public IP.
- **No hassle of managing NSGs**: A fully managed platform PaaS service from Azure that's hardened internally to provide secure RDP/SSH connectivity. You don't need to apply any NSGs on an Azure Bastion subnet.
- **Protection against port scanning**: Because you don't need to expose your virtual machines to the internet, your VMs are protected against port scanning by rogue and malicious users located outside your virtual network.
- **Protect against zero-day exploits**: A fully platform-managed PaaS service. Because it sits at the perimeter of your virtual network, you don’t need to worry about hardening each virtual machine in the virtual network. The Azure platform protects against zero-day exploits by keeping the Azure Bastion hardened and always up to date for you.

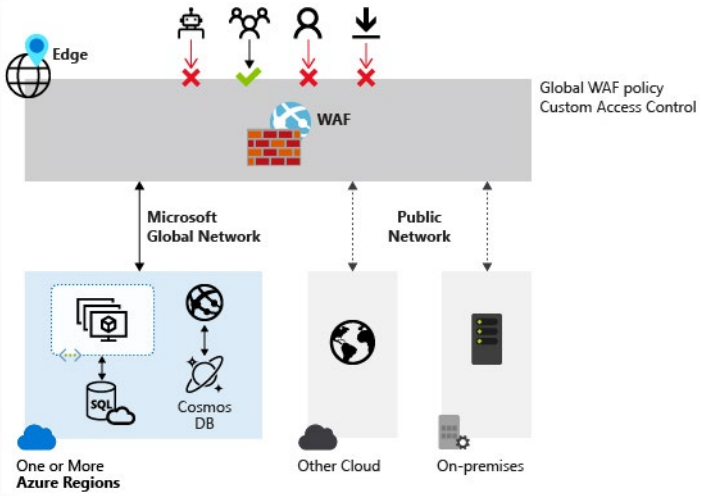
Use Azure Bastion to establish secure RDP and SSH connectivity to your virtual machines in Azure.

Describe what is Web Application Firewall

So far, we’ve looked at the traditional security concerns for the protection of your assets, resources, and data from external attack by using firewalls and network security groups. But there's another threat surface now being exploited by hackers: web applications.

Web applications are increasingly targeted by malicious attacks that exploit commonly known vulnerabilities, like SQL injection and cross-site scripting. Preventing such attacks in application code is challenging. It can require rigorous maintenance, patching, and monitoring.

Web Application Firewall (WAF) provides centralized protection of your web applications from common exploits and vulnerabilities. A centralized WAF helps make security management simpler, improves the response time to a security threat, and allows patching a known vulnerability in one place, instead of securing each web application. A WAF also gives application administrators better assurance of protection against threats and intrusions.



Supported services

WAF can be deployed with **Azure Application Gateway**[2], **Azure Front Door**[3], and **Azure Content Delivery Network (CDN)**[4] services from Microsoft. WAF has features that are customized for each specific service.

Use Azure WAF to achieve centralized protection for your web applications from common exploits and vulnerabilities.

Describe ways Azure encrypts data

Espionage, data theft, and data exfiltration are a real threat to any company. The loss of sensitive data can be crippling and have legal implications. For most organizations, data is their most valuable asset. In a layered security strategy, the use of encryption serves as the last and strongest line of defense.

Encryption on Azure

Microsoft Azure provides many different ways to secure your data, each depending on the service or usage required.

- **Azure Storage Service Encryption** helps to protect data at rest by automatically encrypting before persisting it to Azure-managed disks, Azure Blob Storage, Azure Files, or Azure Queue Storage, and decrypts the data before retrieval.
- **Azure Disk Encryption** helps you encrypt Windows and Linux IaaS 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 data disks.
- **Transparent data encryption (TDE)** helps protect Azure SQL Database and Azure Data Warehouse against the threat of malicious activity. It performs real-time encryption and decryption of the database, associated backups, and transaction log files at rest without requiring changes to the application.

2 https://docs.microsoft.com/azure/web-application-firewall/ag/ag-overview
3 https://docs.microsoft.com/azure/web-application-firewall/afds/afds-overview
4 https://docs.microsoft.com/azure/web-application-firewall/cdn/cdn-overview

What is Azure Key Vault?

Azure Key Vault is a centralized cloud service for storing your application secrets. Key Vault helps you control your applications' secrets by keeping them in a single, central location and by providing secure access, permissions control, and access logging capabilities. It's useful for different kinds of scenarios:

- **Secrets management**. You can use Key Vault to store securely and tightly control access to tokens, passwords, certificates, Application Programming Interface (API) keys, and other secrets.
- **Key management**. You can use Key Vault as a key management solution. Key Vault makes it easier to create and control the encryption keys used to encrypt your data.
- **Certificate management**. Key Vault lets you provision, manage, and deploy your public and private Secure Sockets Layer/ Transport Layer Security (SSL/ TLS) certificates for Azure, and internally connected, resources more easily.
- **Store secrets backed by hardware security modules (HSMs)**. The secrets and keys can be protected either by software or by FIPS 140-2 Level 2 validated HSMs.

Use the various ways in which Azure can encrypt your data to help you secure it, whatever the location or state.

Knowledge check

Multiple choice

Item 1. The security admin has created an Azure Network Security Group (NSG) to filter network traffic to a virtual machine. The admin wants to allow inbound traffic using the Remote Desktop Protocol (RDP), but the default NSG rules are currently blocking all inbound traffic that is not from another virtual network or an Azure load balancer. What does the security admin have to do to allow inbound traffic using RDP?

- ☐ Delete the default rule.
- ☐ Create a new network security rule that allows RDP traffic and that has a higher priority than the default rule.
- ☐ There is nothing the admin can do, RDP traffic is not supported with NSGs.

Multiple choice

Item 2. The security admin wants to protect Azure resources from DDoS attacks, which Azure DDoS Protection tier will the admin use to target Azure Virtual Network resources?

- ☐ Basic.
- ☐ Standard.
- ☐ Advanced.

Multiple choice

Item 3. Your organization has several virtual machines in Azure. The security admin wants to deploy Azure Bastion to get secure access to the virtual machines in Azure. What should the admin keep in mind?

- ☐ Azure Bastion is deployed per virtual network.
- ☐ Azure Bastion is deployed per subscription.
- ☐ Azure Bastion is deployed per virtual machine.

Multiple choice

Item 4. Much of your organization's application data is in Azure. The security admin wants to take advantage of the encryption capabilities in Azure, which service would the admin use to store the application's secrets?

- ☐ Transparent data encryption.
- ☐ Secrets management.
- ☐ Azure Key Vault.

Summary and resources

The traditional network security perimeter protects your organization's assets, resources, where data is essential. Azure offers a wide range of configurable security tools that are customized to give the security and control to meet your organization's needs.

You've explored the different service offerings provided by Microsoft Azure, including network security groups, using Web Application, and regular Azure Firewalls to protect access to your systems. You now understand the importance and use of encryption of data not only when stored, but also when in transit.

You've explored the nature of DDoS and how Azure helps protect your systems against that form of attack. Finally, you saw how Azure Bastion helps secure connections to any virtual machine in your estate.

Without these security tools, your organization would be vulnerable to data theft, unable to respond swiftly to malicious attacks on your web and data services, and wouldn't meet your security obligations.

Now that you've completed this lesson, you should be able to:

- Describe Azure's security capabilities for protecting your network.
- Describe how Azure can protect your VMs.
- Describe how encryption on Azure can protect your data.

Learn more

To find out more about any of the topics covered in this lesson, go to:

- **Network Security Groups**[5]
- **Azure DDoS Protection Standard overview**[6]
- **Azure Firewall**[7]

5 https://docs.microsoft.com/azure/virtual-network/network-security-groups-overview
6 https://docs.microsoft.com/azure/ddos-protection/ddos-protection-overview
7 https://docs.microsoft.com/azure/firewall/

- **Azure Bastion**[8]
- **Web Application firewall**[9]
- **Encryption**[10]

8 https://docs.microsoft.com/azure/bastion/
9 https://docs.microsoft.com/azure/web-application-firewall/
10 https://docs.microsoft.com/learn/modules/intro-to-security-in-azure/4-encryption

Describe the security management capabilities of Azure

Introduction

As more companies move their assets and resources into the cloud, keeping them safe is a primary consideration for all IT and security departments. Cybercrime is a multi-billion-dollar business. Failure to protect your organization can be costly from the loss of data and loss of reputation.

Microsoft Azure offers a suite of threat protection and detection systems to minimize and mitigate your threat surface across your whole estate and improve your overall cloud security posture.

In this lesson, you'll explore the capabilities and benefits of using Azure Security center, what Azure Secure score can tell you about your organization's level of security readiness, how Azure Defender can protect your organization's assets and resources. Finally, you'll explore the use of cloud security posture management and understand the security baseline in Azure.

After completing this lesson, you'll be able to:

- Describe the security management capabilities of Azure
- Describe the benefits and use cases of Azure Defender
- Understand CSPM and the security baseline.

Describe Cloud security posture management

Cloud-based systems are continually evolving and changing as companies move away from on-premises to the cloud. This move makes it difficult for any IT department to know if your data, assets, and resources are as fully protected as they used to be. Even a small misconfiguration of a new feature can increase the attack surface available for cybercriminals to exploit.

Cloud security posture management (CSPM) is a relatively new class of tools designed to improve your cloud security management. It assesses your systems and automatically alerts security staff in your IT department when a vulnerability is found. CSPM uses tools and services in your cloud environment to monitor and prioritize security enhancements and features.

CSPM uses a combination of tools and services:

- **Zero Trust-based access control**: Considers the active threat level during access control decisions.
- **Real-time risk scoring**: To provide visibility into top risks.
- **Threat and vulnerability management (TVM)**: Establishes a holistic view of the organization's attack surface and risk and integrates it into operations and engineering decision-making.
- **Discover sharing risks**: To understand the data exposure of enterprise intellectual property, on sanctioned and unsanctioned cloud services.
- **Technical policy**: Apply guardrails to audit and enforce the organization's standards and policies to technical systems.
- **Threat modeling systems and architectures**: Used alongside other specific applications.

The main goal for a cloud security team working on posture management is to continuously report on and improve the organization's security posture by focusing on disrupting a potential attacker's return on investment (ROI).

The function of CSPM in your organization might be spread across multiple teams, or there may be a dedicated team. CSPM can be useful to many teams in your organization:

- Threat intelligence team
- Information technology
- Compliance and risk management teams
- Business leaders and SMEs
- Security architecture and operations
- Audit team

Use CSPM to improve your cloud security management by assessing the environment, and automatically alerting security staff for vulnerabilities.

Describe the Azure Security center

Network security is an ever-changing and shifting battleground where a moment's hesitation can allow cybercriminals to compromise your security perimeter, and steal valuable assets and resources. Using Azure Security Center gives you infrastructure level security management to protect your data. It also provides advanced threat protection for on-premises, cloud, and hybrid workloads in the cloud, whether they're in Azure or not, as well as on-premises. Azure Security Center provides the tools you need to harden your network, secure services, and ensure you're on top of your security posture.

Azure Security Center addresses the three most urgent security challenges:

- **Rapidly changing workloads**: As organizations empower users to do more, the challenge is to ensure that the ever-changing services people use and create meet your security standards and follow best practices.
- **Increasingly sophisticated attacks**: Wherever your work is situated, the attacks keep getting more sophisticated. Securing your public internet-facing services is essential; otherwise, you'll be even more vulnerable.
- **Security skills are in short supply**: The number of security alerts and alerting systems far outnumbers the total of administrators who have the necessary background and experience to ensure your environments are protected.

To help protect against these challenges, Azure Security Center provides tools to:

- **Strengthen security posture**: Security Center assesses your environment and enables you to understand the status of your resources and whether they're secure.
- **Protect against threats**: Security Center assesses your workloads and raises threat prevention recommendations and security alerts.
- **Get secure faster**: In Security Center, everything is done in cloud speed. Because it's natively integrated, Security Center deployment is easy, giving you autoprovisioning and protection with Azure services.

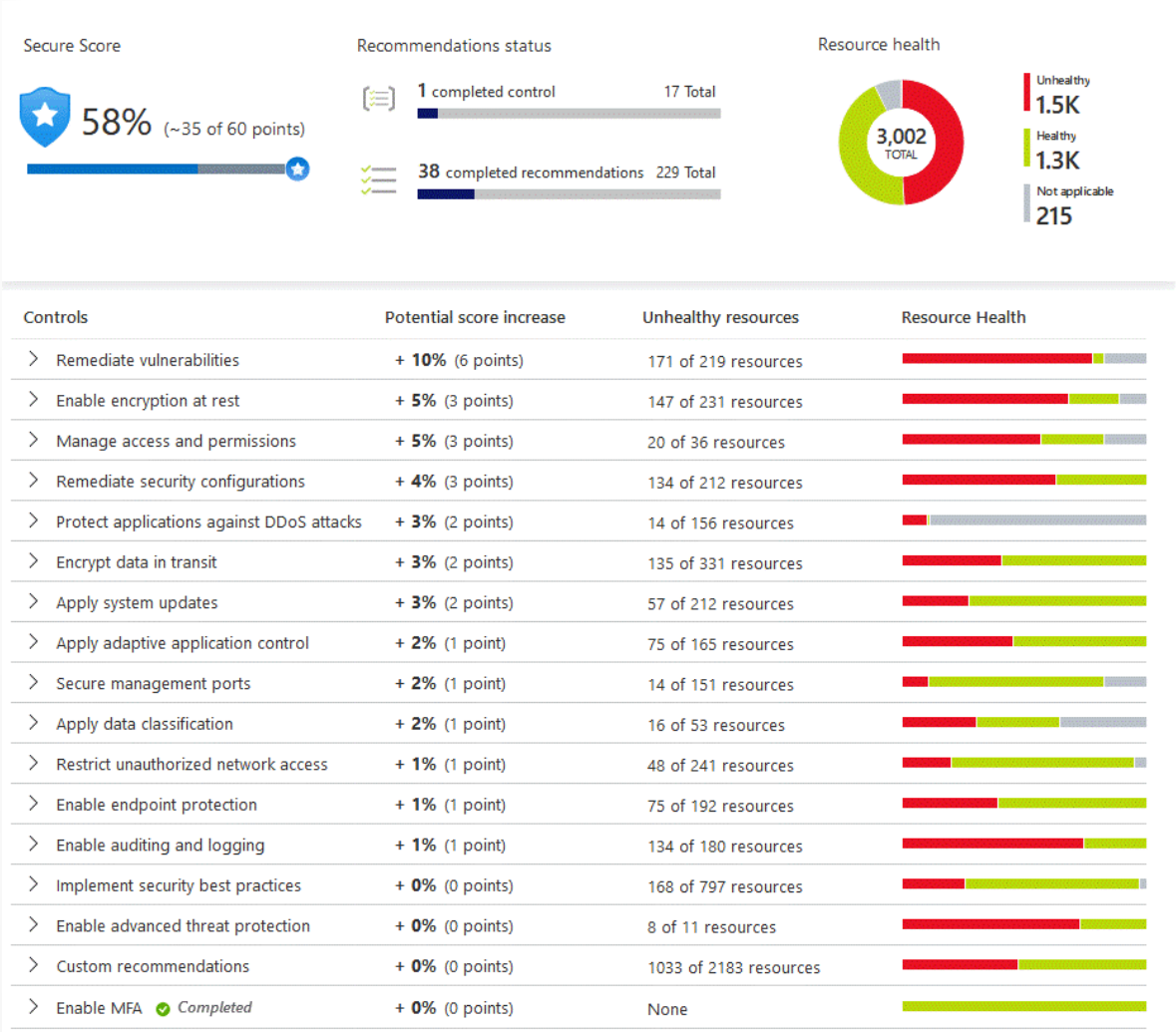
Also, Security Center protects non-Azure servers and virtual machines in the cloud or on-premises, for both Windows and Linux servers, by installing the Log Analytics agent. Azure virtual machines are autoprovisioned in Security Center.

Strengthen your security posture

You can improve your security posture using Azure Security Center to identify and perform hardening tasks across your machines, data services, and applications. With Azure Security Center, you can manage and enforce security policies to ensure compliance across your virtual machines, non-Azure servers, and Azure PaaS services.

Continuous assessment

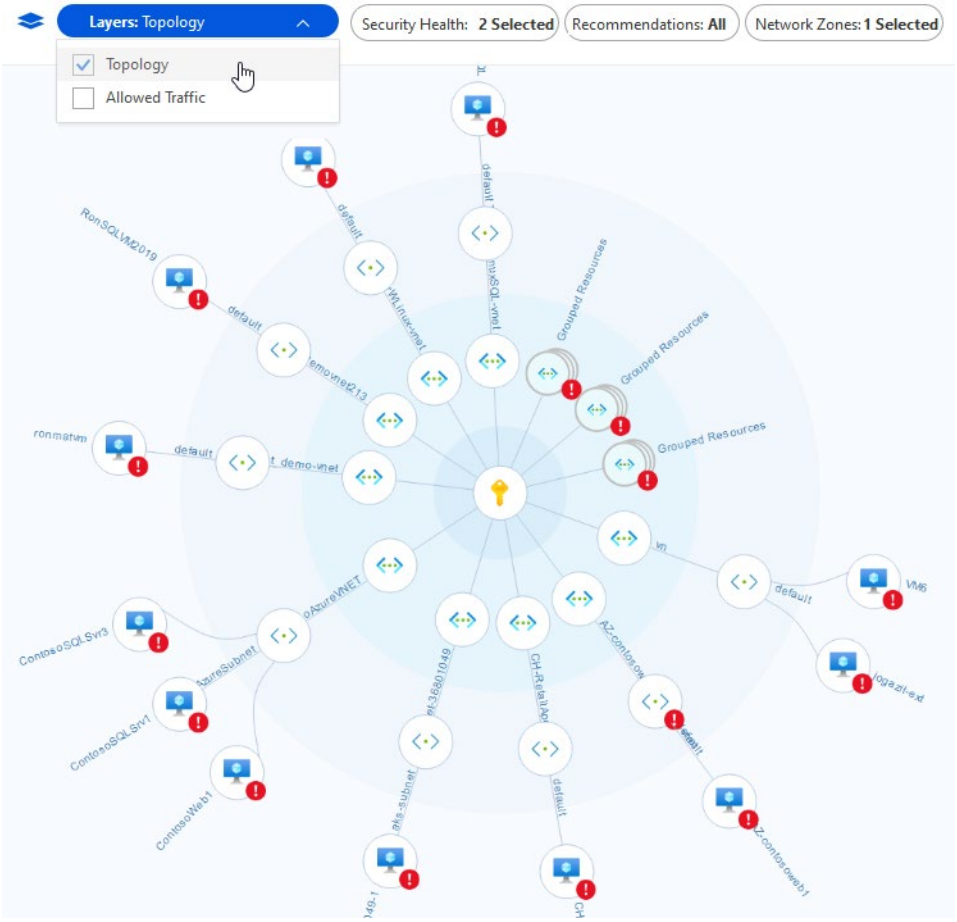
Security Center brings continuous assessment of your entire estate, discovering and reporting whether new and existing resources and assets are configured according to security compliance requirements. You'll get an ordered list of recommendations of what needs to be fixed to maintain maximum protection. Security Center groups the recommendations into security controls and adds a secure score value to each control. This process is crucial in enabling you to prioritize security work.



Network map

One of the most powerful Security Center tools for continuously monitoring the security status of your network is the network map. Use the map to look at the topology of your workloads, so you can see if

each node is properly configured. You'll see how your nodes are connected, which helps you block unwanted connections that could potentially make it easier for an attacker to creep along your network.



Protect against threats

With Azure Security Center's threat protection, you can detect and prevent threats on infrastructure as a service (IaaS), non-Azure servers, and platform as a service (PaaS). It comes with these features:

- **Integration with Microsoft Defender**: Security Center natively integrates with Microsoft Defender for Endpoint.
- **Protect PaaS**: Security Center helps you detect threats across Azure PaaS services. You can detect threats targeting Azure services, including Azure App Service, Azure SQL, Azure Storage Account, and more data services.
- **Block brute force attacks**: By reducing access to virtual machine ports, using the just-in-time VM access, you can harden your network by preventing unnecessary access.
- **Protect data services**: Get assessments for potential vulnerabilities across Azure SQL and Storage services and recommendations for mitigating them.

Security Center's threat protection automatically correlates alerts in your environment based on cyber kill-chain analysis. It helps you to better understand the full story of an attack campaign, where it started and the impact it had on your resources.

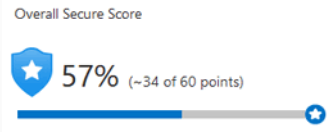
Get secure faster

With Security Center, organizations can get secure faster through integration with other Microsoft security solutions. Also, integration with Azure and its resources means you'll pull together a complete security story involving Azure Policy and built-in Security Center policies across all your Azure resources. You then ensure that the whole thing is automatically applied to newly discovered resources as you create them in Azure.

Describe Azure Secure score

Security Center continually assesses your resources, subscriptions, and organization for security issues. It then aggregates all the findings into a single score so you can quickly see your current security situation: the higher the score, the lower the identified risk level.

The secure score is shown in the Azure portal pages as a percentage value. The underlying values are also clearly presented:

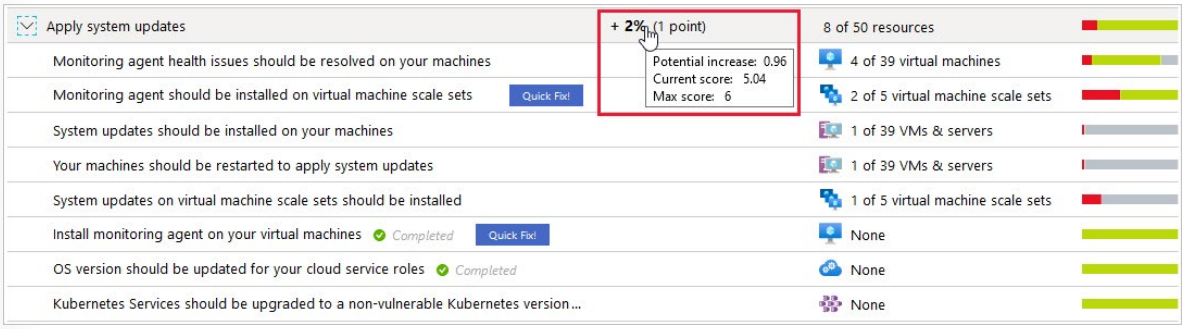


To increase your security and raise your score, review Security Center's recommendations page for the outstanding actions necessary. Each recommendation includes instructions to help you remediate the specific issue.

How is the security score calculated?

Every control in the recommendations list shows the potential secure score increase if you address the underlying problem. To get every possible security control point, all your resources must follow each security recommendation within the security control. For example, Security Center has multiple recommendations for how to secure your management ports. You must remediate them all to make a difference to your secure score.

For example, the security control called "Apply system updates" has a maximum score of six points. You can see it in the tooltip on the potential increase value of the control:



The maximum score for this control, *Apply system updates*, is always 6. In this example, there are 50 resources. Divide the maximum score by 50, and the result is that every resource contributes 0.12 points.

- **Potential increase** (0.12 x 8 unhealthy resources = 0.96): The remaining points available to you within the control. If you remediate all the recommendations, your score will increase by 2 percent (in this case, 0.96 points rounded up to 1 point).

- **Current score** (0.12 x 42 healthy resources = 5.04): The current score for this control. Each control contributes to the total score. In this example, the control is contributing 5.04 points to the current secure total.
- **Max score**: The maximum number of points you can gain by completing all recommendations within a control. The maximum score for a control indicates its relative significance. Use the max score values to triage the issues to work on first.

Improve your secure score

To improve your secure score, remediate security recommendations from your recommendations list. You can manually remediate each recommendation for every resource or, by using the Quick Fix! option when available, apply remediation for a recommendation to a group of resources.

Use secure score to monitor your security posture, and easily implement actions to improve it.

Interactive guide

If you're the Azure administrator for your organization, you'll need to be aware of the security of your Azure environment and improve your security posture accordingly. The following interactive click-through demonstrates how you can do this using Azure secure score. Select the link below to get started.

Interactive guide - Explore Azure secure score[11]

Describe Azure Defender

Azure Defender is a built-in tool that provides threat protection for workloads running in Azure, on-premises, and other clouds. Azure Defender is the leading Microsoft extended detection and response (XDR) solution for threat protection. Integrated with Azure Security Center, Azure Defender protects your hybrid data, cloud-native services and servers, and integrates with your existing security workflows.

Built-in policies come with each Azure Defender plan, and you can add custom policies and initiatives. Also, you can add regulatory standards, such as NIST and Azure CIS, and the Azure Security Benchmark for a truly customized view of your compliance.

You'll find the Azure Defender dashboard in Azure Security Center. It provides visibility and control of your organization's cloud workload protection (CWP) features across the network.

Scope of Azure Defender

Azure Defender comes with several different plans that can be enabled separately and will run simultaneously to provide a comprehensive defense for compute, data, and service layers in your environment. The Azure Defender plans you can select from are:

- **Azure Defender for servers** adds threat detection and advanced defenses for your Windows and Linux machines.
- **Azure Defender for App Service** uses the cloud scale to identify attacks targeting applications running over App Service.
- **Azure Defender for Storage** detects potentially harmful activity on your Azure Storage accounts. Data can be protected, whether stored as blob containers, file shares, or data lakes.

11 https://edxinteractivepage.blob.core.windows.net/edxpages/Security%20fundamentals/LP03M02%20-%20Use%20Azure%20secure%20score%20to%20improve%20your%20security%20posture/index.html?azure-portal=true

- **Azure Defender for SQL** extends Azure Security Center's data security package to secure your databases and their data wherever they're located.
- **Azure Defender for Kubernetes** provides the best cloud-native Kubernetes security environment hardening, workload protection, and run-time protection.
- **Azure Defender for container registries** protects all the Azure Resource Manager based registries in your subscription. Azure Defender scans all images pushed to the registry, or imported into the registry, or any images pulled within the last 30 days.
- **Azure Defender for Key Vault** is Azure-native, advanced threat protection for Azure Key Vault, providing an extra layer of security intelligence.

Hybrid cloud protection

You can defend your Azure environment, and add Azure Defender capabilities to the hybrid cloud environment:

- Protect your non-Azure servers.
- Protect your virtual machines in other clouds, including Amazon Web Services (AWS) and Google Cloud Platform (GCP).

To focus on what matters most, you can customize threat intelligence and prioritize alerts according to your specific environment.

Azure Defender alerts

When Azure Defender detects a threat in any area of your environment, it generates an alert. These alerts describe details of the affected resources, suggested remediation steps, and in some cases, an option to trigger a logic app in response. The alerts can also be exported into Azure Sentinel.

Advanced protection

Azure Defender uses advanced analytics for tailored recommendations as they relate to your resources. These analytics might include securing the management ports of your VMs with just-in-time access and adaptive application controls to create allow lists for what apps should and shouldn't run on your machines.

Vulnerability assessment

Azure Defender includes vulnerability scanning for your virtual machines and container registries. Review the findings from these vulnerability scanners and respond to them all from within Security Center.

Describe security baselines for Azure

Microsoft's cybersecurity group and the Center for Internet Security (CIS), have developed best practices to help establish security baselines for the Azure platform. A baseline is the implementation of the benchmark on the individual Azure service.

CIS benchmarks have been used with Azure security services and tools to make security and compliance easier for customer applications running on Azure services. Every service comes with a baseline that's already designed to help provide security for most common-use cases. These baselines also provide a consistent experience when securing your environment.

The Azure Security Benchmark

A benchmark contains security recommendations for a specific technology, such as Azure. The recommendations are categorized by the control to which they belong. The Azure Security Benchmark (ASB) provides prescriptive best practices and recommendations to help improve the security of workloads, data, and services on Azure. Some of the controls used in the ASB include network security, identity and access control, data protection, data recovery, incident response, and more.

Security baselines for Azure focus on cloud-centric control areas and apply guidance from the Azure Security Benchmark.

Each Azure security baseline includes the following information:

- **Azure ID**: The Azure Security Benchmark ID that corresponds to the recommendation.
- **Recommendation**: 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.
- **Responsibility**: Who is responsible for implementing the control? Possible scenarios are customer responsibility, Microsoft responsibility, or shared responsibility.
- **Azure Security Center monitoring**: Does Azure Security Center monitor the control?

Security baselines are included for many Azure services. As an example, refer to the **Azure security baseline for Security Center**[12]. The content is grouped by the security controls defined by the Azure Security Benchmark and the related guidance applicable to Azure Security Center. Refer to **Azure Security Benchmark documentation**[13] for a complete listing of the available baselines.

Describe the different Azure pricing tiers

Cloud security posture management is essential for every organization. Microsoft Azure lets you decide how much you need to meet your regulatory, compliance, and corporate security needs.

Security Center is offered in two modes:

Azure Defender off

Security Center without Azure Defender is enabled free of charge on all your Azure subscriptions when you visit the Azure Security Center dashboard in the Azure portal for the first time, or if enabled programmatically via API.

Azure Defender on

Enabling Azure Defender extends the free mode capabilities to workloads running in private and other public clouds, providing unified security management and threat protection across your hybrid cloud workloads.

For more information visit **Azure Defender pricing**[14].

12 https://docs.microsoft.com/azure/security-center/security-baseline
13 https://docs.microsoft.com/azure/security/benchmarks/
14 https://azure.microsoft.com/pricing/details/azure-defender/

Knowledge check

Multiple choice

Item 1. An organization is using Azure and wants to improve their security best practices. Which Azure specific benchmark would the IT security team need to consider?

- ☐ Azure Security Benchmark.
- ☐ Center for Internet Security.
- ☐ Microsoft cybersecurity group

Multiple choice

Item 2. Your organization is using Azure Security Center to assess your resources, subscriptions, and organization for security issues. Your organization's overall secure score is low and needs to improve. How would a security admin go about improving the score?

- ☐ Close old security recommendations.
- ☐ Remediate security recommendations.
- ☐ Move security recommendations to resolved.

Multiple choice

Item 3. An organization needs to continuously monitor the security status of its network. What Security Center tool would they use?

- ☐ Continuous assessment.
- ☐ Network map.
- ☐ Network assessment.

Summary and resources

You wanted to better understand the capabilities and benefits of using Azure's security management tools. You've explored the uses of Azure Security Center, and how to understand your security position using Azure secure score. Also, you've discovered the uses of Azure Defender and the different versions available. You looked at how cloud security posture management can benefit your security position. Finally, you examined Azure's security baselines.

Estate security is an essential part of every organization. Without these tools, protecting your organization's data, resources, and assets would be difficult. You'd require multiple layers of overlapping third-party software. There would be an overhead of extra maintenance with no guarantee of complete protection. It's easy to keep your systems secure using Azure's tools and services.

Now that you've completed this lesson, you should be able to:

- Describe the security management capabilities of Azure.
- Describe the benefits and use cases of Azure Defender.
- Understand CSPM and the security baseline.

Learn more

To find out more about any of the topics covered in this lesson, go to:

- **Azure Security Center**[15]
- **Azure secure score**[16]
- **Azure Defender**[17]
- **Security baselines**[18]
- **Azure Defender pricing**[19]

15 https://docs.microsoft.com/azure/security-center/security-center-introduction
16 https://docs.microsoft.com/azure/security-center/secure-score-security-controls
17 https://docs.microsoft.com/azure/security-center/azure-defender
18 https://docs.microsoft.com/azure/security/benchmarks/security-baselines-overview
19 https://azure.microsoft.com/pricing/details/azure-defender/

Describe the security capabilities of Azure Sentinel

Introduction

Every organization, whatever its size, is susceptible to security threats and attacks. Being able to collect data to gain visibility into your digital estate and detect, investigate, and respond to threats is central to any network security strategy.

In this lesson, you'll learn about the different security defenses that are available to protect your company's digital estate. You'll explore how Azure Sentinel provides a single solution for alert detection, threat visibility, proactive hunting, and threat response. Finally, you'll have a high-level understanding of Azure Sentinel costs.

After completing this lesson, you'll be able to:

- Describe the security concepts for SIEM, SOAR, and XDR.
- Describe how Azure Sentinel provides integrated threat protection.
- Describe the capabilities of Azure Sentinel.

Define the concepts of SIEM, SOAR, XDR

Protecting an organization's estate, resources, assets, and data from security breaches and attacks is an ongoing and escalating challenge. Recently, the business world changed almost overnight as large numbers of staff switched to remote working, creating an exploitable window for cybercriminals. IT departments rushed to patch and strengthen their staff's devices and their access to company assets and resources.

Cybercriminals will often escalate their activity in times of national or global crisis, looking to exploit the situation and find ways into your organization. Having a resilient and robust, industry-standard set of tools can help mitigate and prevent these exploits. Security incident and event management (SIEM), security orchestration automated response (SOAR), and extended detection and response (XDR) provide excellent security insights and security automation that can enhance an organization's network security perimeter.

Here, you'll gain a general understanding of the Azure tools that support SIEM, SOAR, and XDR in protecting your network's security perimeter.

What is security incident and event management (SIEM)?

A SIEM system is a tool that an organization uses to collect data from across the whole estate, including infrastructure, software, and resources. It does analysis, looks for correlations or anomalies, and generates alerts and incidents.

What is security orchestration automated response (SOAR)?

A SOAR system takes alerts from many sources, such as a SIEM system. The SOAR system then triggers action-driven automated workflows and processes to run security tasks that mitigate the issue.

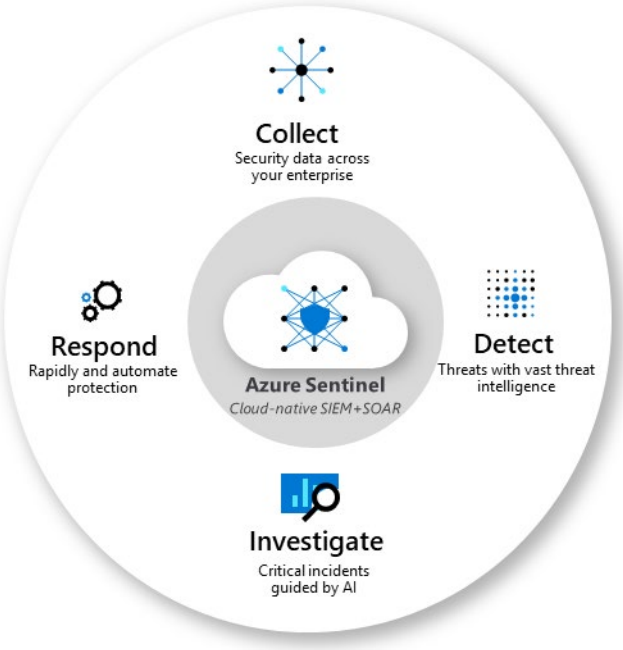
What is extended detection and response (XDR)?

An XDR system is designed to deliver intelligent, automated, and integrated security across an organization's domain. It helps prevent, detect, and respond to threats across identities, endpoints, applications, email, IoT, infrastructure, and cloud platforms.

To provide a comprehensive security perimeter, an organization needs to use a solution that embraces or combines all of the above systems.

Describe integrated threat protection with Sentinel

Effective management of an organization's network security perimeter requires the right combination of tools and systems. Microsoft Azure Sentinel is a scalable, cloud-native SIEM/SOAR solution that delivers intelligent security analytics and threat intelligence across the enterprise. It provides a single solution for alert detection, threat visibility, proactive hunting, and threat response.



This diagram shows the end-to-end functionality of Azure Sentinel.

- **Collect** data at cloud scale across all users, devices, applications, and infrastructure, both on-premises and in multiple clouds.
- **Detect** previously uncovered threats and minimize false positives using analytics and unparalleled threat intelligence.
- **Investigate** threats with AI and hunt suspicious activities at scale, tapping into decades of cybersecurity work at Microsoft.
- **Respond** to incidents rapidly with built-in orchestration and automation of common security tasks.

Azure Sentinel helps enable end-to-end security operations. It starts with log ingestion and continues through to automated response to security alerts.

Connect Sentinel to your data

Azure Sentinel comes with many connectors for Microsoft solutions, available out of the box and providing real-time integration. Included are Microsoft 365 Defender (formerly Microsoft Threat Protection) solutions, and Microsoft 365 sources, including Office 365, Azure AD, Microsoft Defender for Identity (formerly Azure ATP), Microsoft Cloud App Security, and more.

First, you must have your data ingested into Azure Sentinel, for which you need data connectors. There are data connectors that cover a wide range of scenarios and sources, including but not limited to:

- syslog
- Windows Event Logs
- Common Event Format (CEF)
- Trusted Automated eXchange of Indicator Information (TAXII), for threat intelligence
- Azure
- AWS services

Workbooks

After you connect data sources to Azure Sentinel, you can monitor the data using the Azure Sentinel integration with Azure Monitor Workbooks. You'll see a canvas for data analysis and the creation of rich visual reports within the Azure portal. Through this integration, Azure Sentinel allows you to create custom workbooks across your data. It also comes with built-in workbook templates that allow quick insights across your data as soon as you connect a data source.

Analytics

The power of Azure Sentinel comes into play here. Using built-in analytics alerts within the Azure Sentinel workspace, you'll get notified when anything suspicious occurs. There are various types of alerts, some of which you can edit to your own needs. Other alerts are built on machine learning models that are proprietary to Microsoft.

Manage incidents in Azure Sentinel

An incident is created when an alert that you've enabled is triggered. You can do standard incident management tasks like changing status or assigning incidents to individuals for investigation in Azure Sentinel. It also has investigation functionality, so you can visually investigate incidents by mapping entities across log data along a timeline.

Security automation and orchestration

You can use Azure Sentinel to automate some of your security operations and make your security operations center (SOC) more productive. Azure Sentinel integrates with Azure Logic Apps, so you can create automated workflows, or playbooks, in response to events. This functionality could be used for incident management, enrichment, investigation, or remediation.

Playbooks

A security playbook is a collection of procedures that can help automate and orchestrate your response. It can be run manually or set to run automatically when specific alerts are triggered. Security playbooks in

Azure Sentinel are based on Azure Logic Apps. You get all the power, customizability, and built-in templates of Logic Apps. Each playbook is created for the specific subscription you choose.

Investigation

Currently in preview, Azure Sentinel's deep investigation tools help you to understand the scope of a potential security threat and find the root cause. You choose an entity on the interactive graph to ask specific questions, then drill down into that entity and its connections to get to the root cause of the threat.

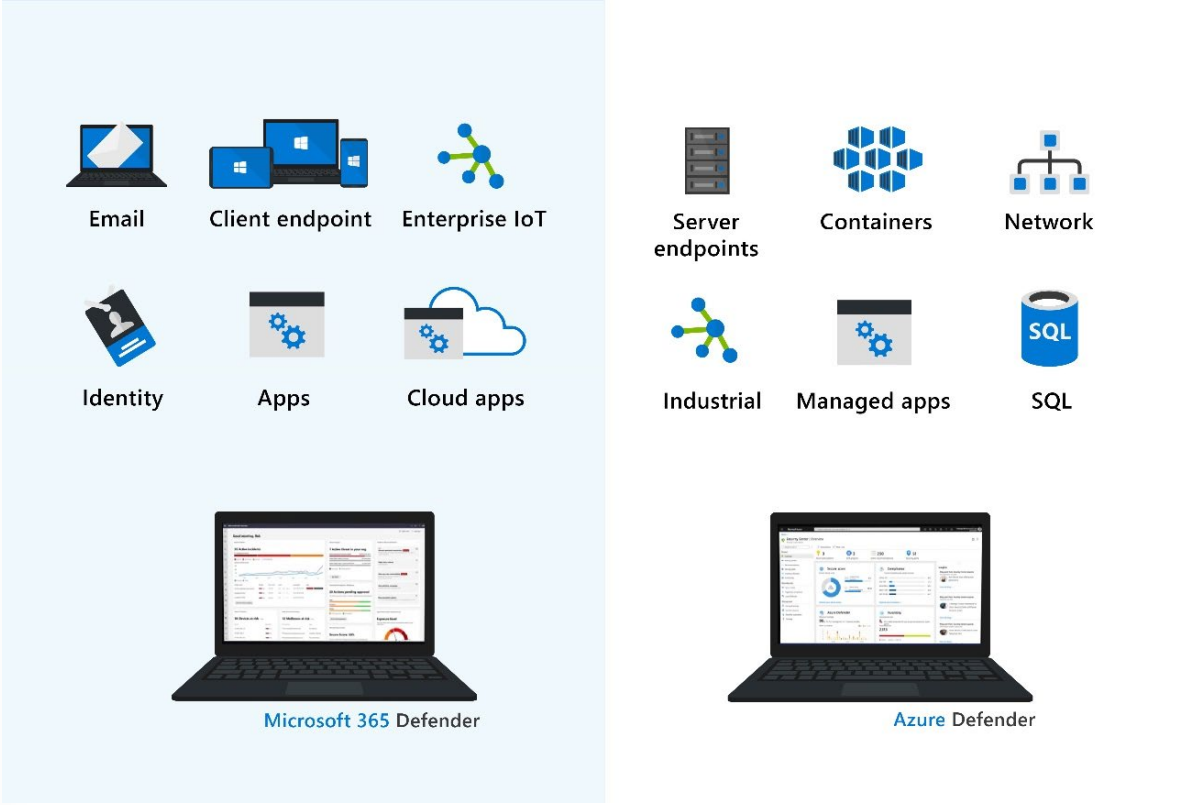
Hunting

Use Azure Sentinel's powerful hunting search-and-query tools, based on the MITRE framework, to hunt proactively for security threats across your organization's data sources, before an alert is triggered. After you discover which hunting query provides high-value insights into possible attacks, you can also create custom detection rules based on your query, and surface those insights as alerts to your security incident responders.

While hunting, you can bookmark interesting events, enabling you to return to them later, share them with others, and group them with other correlating events to create a compelling incident for investigation.

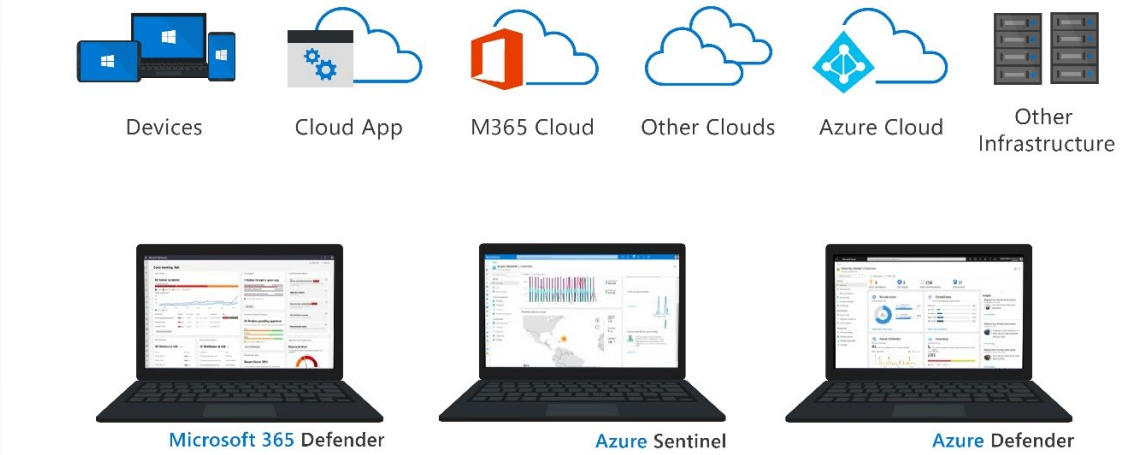
Integrated threat protection

Threat protection is a continuously evolving battle front. Cybercriminals look for any vulnerability they can exploit to steal, damage, or extort company data, assets, and resources. Microsoft provides a suite of tools that give extended detection and response (XDR) through Microsoft 365 Defender and Azure Defender.



Both tools integrate smoothly with Azure Sentinel to provide a complete and thorough threat protection capability for your organization.

SIEM and XDR Solutions



Azure Sentinel video presentation

In this video, **Azure Sentinel**[20], you'll explore many of the key features available in Azure Sentinel, including incidents, workbooks, hunting, notebooks, analytics, and playbooks.

Understand Sentinel costs

Azure Sentinel provides intelligent security analytics across your enterprise. The data for this analysis is stored in an Azure Monitor Log Analytics workspace. Billing is based on the volume of data ingested for analysis in Azure Sentinel and stored in the Azure Monitor Log Analytics workspace. There are two ways to pay for the Azure Sentinel service: Capacity Reservations and Pay-As-You-Go.

- **Capacity Reservations**: With Capacity Reservations, you're billed a fixed fee based on the selected tier, enabling a predictable total cost for Azure Sentinel.
- **Pay-As-You-Go**: With Pay-As-You-Go pricing, you're billed per gigabyte (GB) for the volume of data ingested for analysis in Azure Sentinel and stored in the Azure Monitor Log Analytics workspace.

For more information on pricing and a free trial of Azure Sentinel on an Azure Monitor Log Analytics workspace, visit **Azure Sentinel pricing**[21].

Knowledge check

Multiple choice

Item 1. As the lead admin, it is important to convince your team to start using Azure Sentinel. You've put together a presentation. What are the four security operation areas of Azure Sentinel that cover this area?

☐ Collect, Detect, Investigate, and Redirect.

☐ Collect, Detect, Investigate, and Respond.

☐ Collect, Detect, Investigate, and Repair.

Multiple choice

Item 2. Your estate has many different data sources where data is stored. Which tool should be used with Azure Sentinel to quickly gain insights across your data as soon as a data source is connected?

☐ Azure Monitor Workbooks.

☐ Playbooks.

☐ Microsoft 365 Defender.

Summary and resources

In this lesson, you learned about the security defenses available to protect your company's digital estate. You also discovered the key security operation areas that Azure Sentinel supports and how it integrates with your existing security systems. You get a single solution for alert detection, threat visibility, proactive hunting, and threat response.

20 https://www.microsoft.com/videoplayer/embed/RE4LHLR
21 https://azure.microsoft.com/pricing/details/azure-sentinel/

Now that you've completed this lesson, you should be able to:

- Describe the security concepts for SIEM, SOAR, and XDR.
- Describe how Azure Sentinel provides integrated threat protection.
- Describe the capabilities of Azure Sentinel.

Learn more

To find out more about any of the topics covered in this lesson, go to:

- **Integrated threat protection with SIEM and XDR**[22]
- **Microsoft delivers unified SIEM and XDR to modernize security operations**[23]
- **Azure Sentinel and SIEM**[24]
- **What is Azure Sentinel?**[25]
- **Azure Sentinel pricing**[26]

22 https://www.microsoft.com/security/business/threat-protection
23 https://www.microsoft.com/security/blog/2020/09/22/microsoft-unified-siem-xdr-modernize-security-operations/
24 https://azure.microsoft.com/services/azure-sentinel/
25 https://docs.microsoft.com/azure/sentinel/overview
26 https://azure.microsoft.com/pricing/details/azure-sentinel/

Describe the threat protection capabilities of Microsoft 365

Introduction

Security threat prevention is not limited to just network security. It also covers applications, email, collaborations, endpoints, cross SaaS solutions, identity, and more. With the integrated Microsoft 365 Defender solution, security professionals can stitch together the threat signals that each of these products receive and determine the full scope and impact of the threat; how it entered the environment, what it's affected, and how it's currently impacting the organization.

In this lesson, you'll see how the Microsoft Defender service can help protect your organization. You'll explore each of the different defender services to understand how they can protect: Identity, Office 365, Endpoint, and cloud apps.

After completing this lesson, you'll be able to:

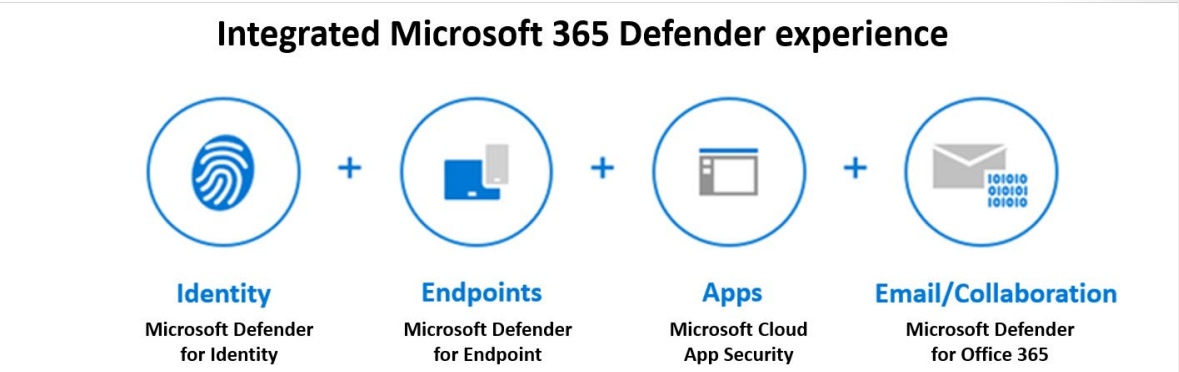
- Describe the Microsoft 365 Defender service.
- Describe how Microsoft 365 Defender provides integrated protection against sophisticated attacks.
- Describe how Microsoft Cloud App Security can help defend your data and assets.

Describe Microsoft 365 Defender services

Microsoft 365 Defender is an enterprise defense suite that protects against sophisticated cyberattacks. With 365 Defender, you can natively coordinate the detection, prevention, investigation, and response to threats across email, identity, and applications.

Refer to the **Microsoft 365 Defender overview**[27] for a video overview of Microsoft 365 Defender.

Microsoft 365 Defender allows admin's to assess threat signals from applications, email, and identity to determine an attack's scope and impact. It gives greater insight into how the threat occurred, what systems have been affected, and can take automated action to prevent or stop the attack.



Microsoft 365 Defender suite protects:

- **Identities with Microsoft Defender for Identity and Azure AD Identity Protection** - Microsoft Defender for Identity, uses Active Directory signals to identify, detect, and investigate advanced threats, compromised identities, and malicious insider actions directed at your organization.

27 https://www.microsoft.com/videoplayer/embed/RE4IPYr

- **Endpoints with Microsoft Defender for Endpoint** - Microsoft Defender for Endpoint is a unified endpoint platform for preventative protection, post-breach detection, automated investigation, and response.
- **Applications with Microsoft Cloud App security** - Microsoft Cloud App Security is a comprehensive cross-SaaS solution bringing deep visibility, strong data controls, and enhanced threat protection to your cloud apps.
- **Email and collaboration with Microsoft Defender for Office 365** - Defender for Office 365 safeguard your organization against malicious threats posed by email messages, links (URLs), and collaboration tools.

Use Microsoft Defender to protect your organization against sophisticated cyberattacks by coordinating your detection, prevention, investigation, and response to threats across identities, email, and applications.

Describe Microsoft Defender for Identity

Microsoft Defender for Identity, formerly Azure Advanced Threat Protection (Azure ATP), is a cloud-based security solution. It uses your on-premises Active Directory data (called signals) to identify, detect, and investigate advanced threats, compromised identities, and malicious insider actions directed at your organization. Microsoft Defender for Identity covers these key areas:

- Monitor and profile user behavior and activities.
- Protect user identities and reduce the attack surface.
- Identify suspicious activities and advanced attacks across the cyberattack kill-chain.

Monitor and profile user behavior and activities

Defender for Identity monitors and analyzes user activities and information across your network, including permissions and group membership, creating a behavioral baseline for each user. Defender for Identity then identifies anomalies with adaptive built-in intelligence. It gives insights into suspicious activities and events, revealing the advanced threats, compromised users, and insider threats facing your organization.

Protect user identities and reduce the attack surface

Defender for Identity gives invaluable insights on identity configurations and suggested security best practices. Through security reports and user profile analytics, Defender for Identity helps reduce your organizational attack surface, making it harder to compromise user credentials and advance an attack.

Defender for Identity security reports, help identify users and devices that authenticate using clear-text passwords. It also provides extra insights into how to improve security posture and policies.

Identify suspicious activities and advanced attacks across the cyberattack kill-chain

Typically, attacks are launched against any accessible entity, such as a low-privileged user. Attacks then quickly move laterally until the attacker accesses valuable assets. These assets might include sensitive accounts, domain administrators, and highly sensitive data. Defender for Identity identifies these advanced threats at the source throughout the entire cyberattack kill chain:

- Reconnaissance

- Compromised credentials
- Lateral movements
- Domain dominance

Investigate alerts and user activities

Defender for Identity is designed to reduce general alert noise, providing only relevant, important security alerts in a simple, real-time organizational attack timeline.

Use the Defender for Identity attack timeline view and the intelligence of smart analytics to stay focused on what matters. Also, you can use Defender for Identity to quickly investigate threats, and gain insights across the organization for users, devices, and network resources.

Microsoft Defender for Identity protects your organization from compromised identities, advanced threats, and malicious insider actions.

Describe Microsoft Defender for Office 365

Microsoft Defender for Office 365, formerly Office 365 Advanced Threat Protection, safeguards your organization against malicious threats posed by email messages, links (URLs), and collaboration tools, including Microsoft Teams, SharePoint Online, OneDrive for Business, and other Office clients.

Microsoft Defender for Office 365 covers these key areas:

- **Threat protection policies**: Define threat protection policies to set the appropriate level of protection for your organization.
- **Reports**: View real-time reports to monitor Microsoft Defender for Office 365 performance in your organization.
- **Threat investigation and response capabilities**: Use leading-edge tools to investigate, understand, simulate, and prevent threats.
- **Automated investigation and response capabilities**: Save time and effort investigating and mitigating threats.

Microsoft Defender for Office 365 is available in two plans. The plan you choose influences the tools you'll see and use. It's important to make sure you select the best plan to meet your organization's needs.

Microsoft Defender for Office 365 Plan 1

This plan offers configuration, protection, and detection tools for your Office 365 suite:

- **Safe Attachments**: Checks email attachments for malicious content.
- **Safe Links**: Links are scanned for each click. A safe link remains accessible, but malicious links are blocked.
- **Safe Attachments for SharePoint, OneDrive, and Microsoft Teams**: Protects your organization when users collaborate and share files by identifying and blocking malicious files in team sites and document libraries.
- **Anti-phishing protection**: Detects attempts to impersonate your users and internal or custom domains.
- **Real-time detections**: A real-time report that allows you to identify and analyze recent threats.

Microsoft Defender for Office 365 Plan 2

This plan includes all the core features of Plan 1, and provides automation, investigation, remediation, and simulation tools to help protect your Office 365 suite:

- **Threat Trackers**: Provide the latest intelligence on prevailing cybersecurity issues, and allow an organization to take countermeasures before there's an actual threat.
- **Threat Explorer**: A real-time report that allows you to identify and analyze recent threats.
- **Automated investigation and response (AIR)**: Includes a set of security playbooks that can be launched automatically, such as when an alert is triggered, or manually. A security playbook can start an automated investigation, provide detailed results, and recommend actions that the security team can approve or reject.
- **Attack Simulator**: Allows you to run realistic attack scenarios in your organization to identify vulnerabilities.

Microsoft Defender for Office 365 availability

Microsoft Defender for Office 365 is included in certain subscriptions, such as Microsoft 365 E5, Office 365 E5, Office 365 A5, and Microsoft 365 Business Premium.

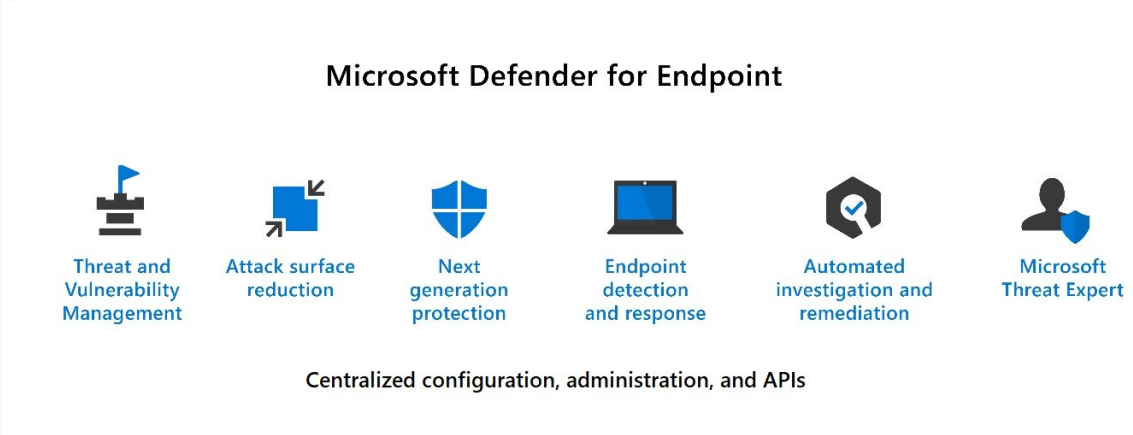
If your subscription doesn't include Defender for Office 365, you can purchase it as an add-on.

Use Microsoft 365 Defender for Office 365 to protect your organization's collaboration tools and messages.

Describe Microsoft Defender for Endpoint

Microsoft Defender for Endpoint, formerly Microsoft Defender Advanced Threat Protection, is a platform designed to help enterprise networks protect endpoints. It does so by preventing, detecting, investigating, and responding to advanced threats. Microsoft Defender for Endpoint embeds technology built into Windows 10 and MSFT cloud services.

This technology includes endpoint behavioral sensors that collect and process signals from the operating system, cloud security analytics that turn signals into insights, detections and recommendations, and threat intelligence to identify attacker tools, techniques, generate alerts.



Microsoft Defender for Endpoint includes:

- **Threat and vulnerability management**: A risk-based approach to the discovery, prioritization, and remediation of endpoint vulnerabilities and misconfigurations. It uses sensors on devices to avoid the need for agents or scans, and prioritizes vulnerabilities.
- **Attack surface reduction**: Reduces the places where your organization is vulnerable to cyberthreats and attacks by ensuring only *allowed* apps can run, and preventing apps from accessing dangerous locations.
- **Next generation protection**: Brings together machine learning, big data analysis, in-depth threat resistance research, and the Microsoft cloud infrastructure to protect devices in your enterprise organization.
- **Endpoint detection and response**: Provides advanced attack detections that are near real time and actionable. Security analysts can prioritize alerts, see the full scope of a breach, and take response actions to remediate threats.
- **Automated investigation and remediation**: The automated investigation feature uses inspection algorithms and processes used by analysts (such as playbooks) to examine alerts and take quick remediation action to resolve breaches. This process significantly reduces the volume of alerts that must be investigated individually.
- **Microsoft Threat Experts**: A managed threat hunting service that provides Security Operation Centers (SOCs) with monitoring and analysis tools to ensure critical threats don't get missed.
- **Management and APIs**: Provides APIs to integrate with other solutions.

Microsoft Defender for Endpoint includes Microsoft Secure Score for Devices to help you dynamically assess the security state of your enterprise network, identify unprotected systems, and take recommended actions to improve overall security. Microsoft Defender for Endpoint integrates with various components in the Microsoft Defender suite, and with other Microsoft solutions including Intune and Azure Security Center.

Use Microsoft Defender for Endpoint to protect your organization's endpoints and respond to advanced threats.

Describe Microsoft Cloud App Security

Moving to the cloud increases flexibility for employees and IT teams. However, it also introduces new challenges and complexities for keeping your organization secure. To get the full benefit of cloud apps and services, an IT team must find the right balance for supporting access while protecting critical data.

Microsoft Cloud App Security (MCAS) is a Cloud Access Security Broker (CASB). It's a comprehensive cross-SaaS solution that operates as an intermediary between a cloud user and the cloud provider. Microsoft Cloud App Security provides rich visibility to your cloud services, control over data travel, and sophisticated analytics to identify and combat cyberthreats across all your Microsoft and third-party cloud services. Use this service to gain visibility into Shadow IT by discovering the cloud apps being used. You can control and protect data in the apps after you sanction them to the service.

What is a Cloud Access Security Broker?

A CASB acts as a gatekeeper to broker real-time access between your enterprise users and the cloud resources they use, wherever they're located, and whatever device they're using.

CASBs address security gaps in an organization's use of cloud services. Protection is provided by many capabilities across these areas:

visibility to detect all cloud services, **data security**, **threat protection**, and **compliance**. These capability areas represent the basis of the Cloud App Security framework described below.

The Cloud App Security framework

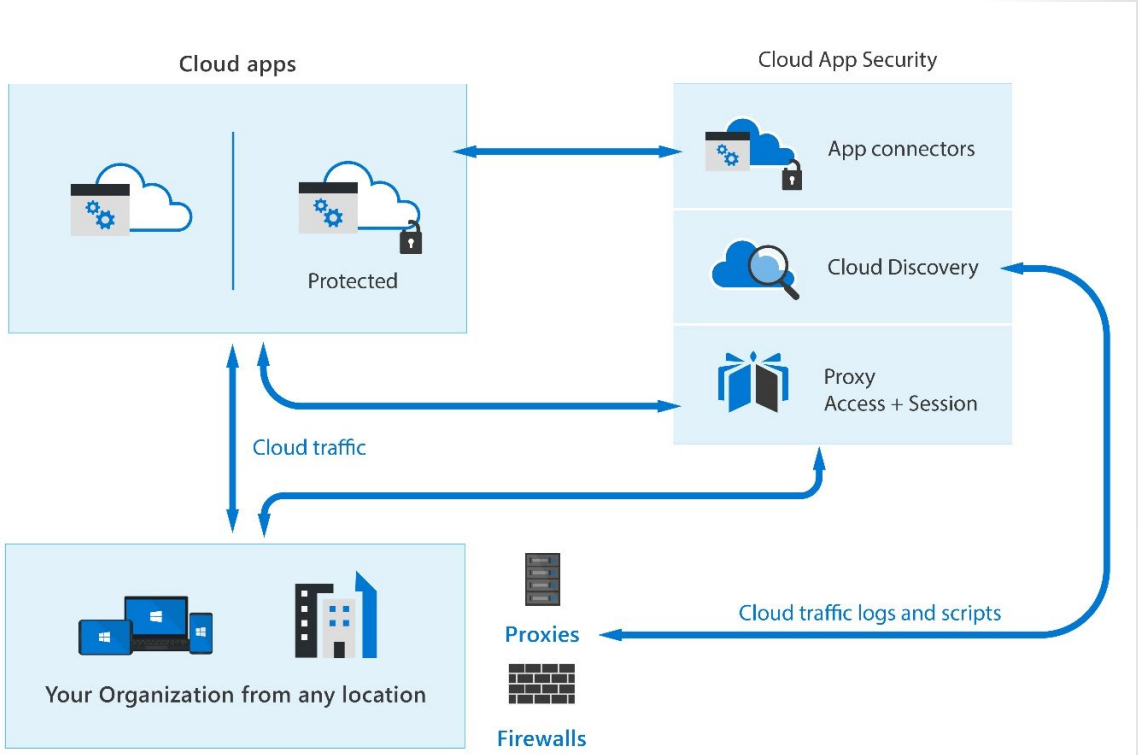
MCAS is built on a framework that provides the following capabilities:

- **Discover and control the use of Shadow IT**: Identify the cloud apps, and IaaS and PaaS services used by your organization. Investigate usage patterns, assess the risk levels and business readiness of more than 16,000 SaaS apps against more than 80 risks.
- **Protect your sensitive informationanywhere in the cloud**: Understand, classify, and protect the exposure of sensitive information at rest. Use out-of-the-box policies and automated processes to apply controls in real time across all your cloud apps.
- **Protect against cyberthreats and anomalies**: Detect unusual behavior across cloud apps to identify ransomware, compromised users, or rogue applications, analyze high-risk usage, and remediate automatically to limit risks.
- **Assess your cloud apps' compliance**: Assess if your cloud apps meet relevant compliance requirements, including regulatory compliance and industry standards. Prevent data leaks to non-compliant apps and limit access to regulated data.

Microsoft Cloud App Security architecture

Cloud App Security isn't only about how you strengthen or harden your servers to detect and prevent cyberattacks. It requires consideration on the architecture of your entire estate. How each server connects to its neighbor, and the routes that network traffic takes can make a significant difference your security model. Cloud App Security integrates visibility with your cloud by:

- Using Cloud Discovery to map and identify your cloud environment and the cloud apps your organization uses. Cloud Discovery uses your traffic logs to dynamically discover and analyze the cloud apps being used.
- Sanctioning and unsanctioning apps in your cloud. You can use Cloud App Security to sanction or unsanction apps in your organization by using the Cloud app catalog. It includes more than 16,000 cloud apps that are ranked and scored based on industry standards.
- Using straightforward app connectors that use provider APIs for visibility and governance of apps you connect to. App connectors use APIs from cloud app providers to integrate their cloud apps with MCAS, extending control and protection. These connectors also give you access to information directly from cloud apps, for Cloud App Security analysis.
- Using Conditional Access App Control protection to get real-time visibility and control over access and activities within your cloud apps.
- Helping you have continuous control by setting and then continually fine-tuning policies. You can use policies to define users' behavior in the cloud. Use policies to detect risky behavior, violations, or suspicious data points and activities in your cloud environment.



Office 365 Cloud App Security

Office 365 Cloud App Security is a subset of Microsoft Cloud App Security that provides enhanced visibility and control for Office 365. Office 365 Cloud App Security includes threat detection based on user activity logs, discovery of Shadow IT for apps with similar functionality to Office 365 offerings, control app permissions to Office 365, and apply access and session controls.

It offers a subset of the core MCAS features.

Enhanced Cloud App Discovery in Azure Active Directory

Azure Active Directory Premium P1 includes Azure Active Directory Cloud App Discovery at no extra cost. This feature is based on the Microsoft Cloud App Security Cloud Discovery capabilities that provide deeper visibility into cloud app usage in your organization.

It provides a reduced subset of the MCAS discovery capabilities.

Use Microsoft Cloud App Security to intelligently and proactively identify and respond to threats across your organization's Microsoft and non-Microsoft cloud services.

Interactive Guide

In this interactive guide, you'll get an introduction to the many services and capabilities available through the Cloud App Security portal, including Discover, Investigate, Control, and Alerts. Select the link below to get started.

Interactive guide - Explore the Cloud App Security portal[28]

Knowledge check

Multiple choice

Item 1. A lead admin for an organization is looking to protect against malicious threats posed by email messages, links (URLs), and collaboration tools. Which solution from the Microsoft 365 Defender suite is best suited for this purpose?

- ☐ Microsoft Defender for Office 365.
- ☐ Microsoft Defender for Endpoint.
- ☐ Microsoft Defender for Identity.

Multiple choice

Item 2. As the admin for team, you're required to provide a short presentation on the use and benefit of Microsoft Cloud App Security to your team. Which of the four MCAS pillars is responsible for identifying and controlling sensitive information?

- ☐ Threat protection.
- ☐ Compliance.
- ☐ Data Security.

Multiple choice

Item 3. Which of the following is a is a cloud-based security solution that identifies, detects, and helps to investigate advanced threats, compromised identities, and malicious insider actions directed at your organization?

- ☐ Microsoft Defender for Office 365
- ☐ Microsoft Defender for Identity
- ☐ Microsoft Cloud App Security

Summary and resources

You wanted to gain a better understanding of how to improve security and access to your organizations assets and data using the Microsoft 365 Defender services. You got a broad understanding of what Microsoft 365 Defender is, and each of the product items: Defender for Identity, Defender for Office 365, and Defender for Endpoint. Finally, you saw how Microsoft Cloud App Security (MCAS) can support access and maintain control of your critical data.

With an increase in demand for cloud services and access, it is more important than ever to maintain strong security. But there comes a balance between strong security and allowing your users to access the data. Without tools like Microsoft Defender, you would have to rely on different vendor solutions, which might not integrate fully or could leave gaps.

28 https://edxinteractivepage.blob.core.windows.net/edxpages/Security%20fundamentals/LP03M04%20-%20Describe%20threat%20protection%20with%20Microsoft%20365/index.html?azure-portal=true

Now that you've completed this lesson, you should be able to:

- Describe the Microsoft 365 Defender service.
- Describe how and when to implement Microsoft Defender for Identity.
- Describe how and when to implement Microsoft Defender for Office 365.
- Describe how and when to implement Microsoft Defender for Endpoint.
- Describe how Microsoft Cloud App Security can help defend your data and assets.

Learn more

To find out more about any of the topics covered in this lesson, please visit these links:

- **Microsoft 365 Defender**[29]
- **Microsoft Defender for Identity**[30]
- **Microsoft Defender for Office 365**[31]
- **Microsoft Defender for Endpoint**[32]
- **What is cloud app security**[33]
- **MCAS and Office 365 Cloud App Security**[34]
- **Getting started with MCAS**[35]

29 https://docs.microsoft.com/microsoft-365/security/mtp/microsoft-threat-protection
30 https://docs.microsoft.com/defender-for-identity/what-is
31 https://docs.microsoft.com/microsoft-365/security/office-365-security/office-365-atp
32 https://docs.microsoft.com/windows/security/threat-protection/microsoft-defender-atp/microsoft-defender-advanced-threat-protection
33 https://docs.microsoft.com/cloud-app-security/what-is-cloud-app-security
34 https://docs.microsoft.com/cloud-app-security/editions-cloud-app-security-o365
35 https://docs.microsoft.com/cloud-app-security/getting-started-with-cloud-app-security

Describe the security management capabilities of Microsoft 365

Introduction

The Microsoft 365 Defender portal, provides a centralized site where you can manage security across Microsoft identities, data, devices, and apps. Throughout this module, you will explore the capabilities of the Microsoft 365 Defender portal, including Microsoft Secure Score, dashboards, reports, and incident management.

After completing this lesson, you'll be able to:

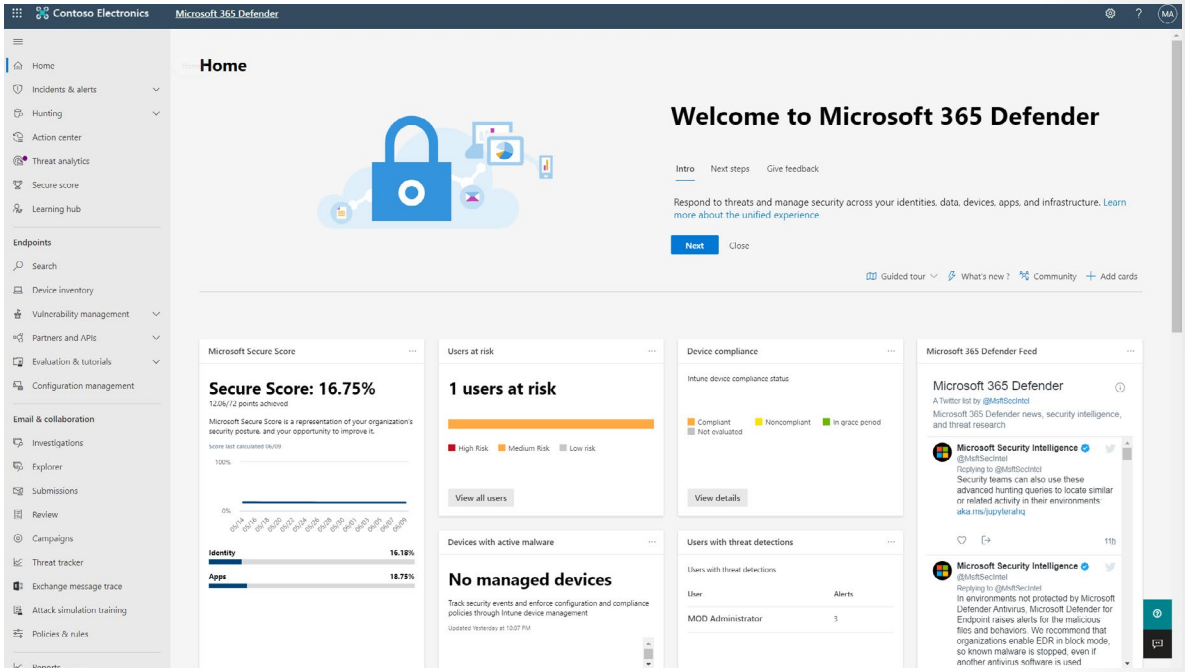
- Describe and explore Microsoft 365 Defender portal.
- Describe how to use Microsoft Secure score.
- Explore security reports and dashboards.
- Describe incidents and incident management capabilities.

Describe the Microsoft 365 Defender portal

The Microsoft 365 Defender portal (previously Microsoft 365 security center) combines protection, detection, investigation, and response to email, collaboration, identity, and device threats, in a central portal.

Here you can view the security health of your organization, act to configure devices, users, and apps, and get alerts for suspicious activity. The Microsoft 365 Defender portal helps security admins and security operations teams manage and protect their organization.

The Microsoft 365 Defender portal home page shows many of the common cards that security teams need. The composition of cards and data depends on the user role. Because the Microsoft 365 Defender portal uses role-based access control, different roles will see cards that are more meaningful to their day-to-day jobs.



The Microsoft 365 Defender portal allows admins to tailor the navigation pane to meet daily operational needs. Admins can customize the navigation pane to show or hide functions and services based on their specific preferences. Customization is specific to the individual admin, so other admins won't see these changes.

The navigation pane for the Microsoft 365 Defender portal includes these options and many more:

- **Home**: Get an at-a-glance view of the overall security health of your organization.
- **Incidents**: See the broader story of an attack by connecting the dots seen on individual alerts on entities. You'll know exactly where an attack started, what devices are impacted, who was affected, and where the threat has gone.
- **Alerts**: Have greater visibility into all the alerts across your Microsoft 365 environment. Includes alerts from Microsoft Cloud App Security, Microsoft Defender for Office 365, Azure Active Directory, Microsoft Defender for Identity, and Microsoft Defender for Endpoint. Available to E3 and E5 customers.
- **Hunting**: Proactively search for malware, suspicious files, and activities in your Microsoft 365 organization.
- **Action** center: Reduce the volume of alerts your security team must address manually, allowing them to focus on more sophisticated threats and other high-value initiatives.
- **Threat analytics** - Track and respond to emerging threats with an integrated Microsoft 365 Defender threat analytics experience
- **Secure Score**: Improve your overall security posture with Microsoft Secure Score. This page provides an all up summary of the different security features and capabilities you've enabled and includes recommendations for areas to improve.
- **Learning hub** - The Microsoft 365 Defender portal includes a learning hub that bubbles up official guidance from resources such as the Microsoft security blog, the Microsoft security community on YouTube, and the official documentation at docs.microsoft.com.
- **Endpoints** – Microsoft Defender for Endpoints delivers preventative protection, post-breach detection, automated investigation, and response for devices in your organization.

- **Email & collaboration** - Microsoft Defender for Office 365 helps organizations secure their enterprise with a set of prevention, detection, investigation and hunting features to protect email, and Office 365 resources.
- **Reports**: Get the detail and information you need to better protect your users, devices, apps, and more.
- **Permissions & roles**: Access to Microsoft 365 Defender is configured with Azure Active Directory global roles or by using custom roles.

IMPORTANT: You must be assigned an appropriate role, such as Global Administrator, Security Administrator, Security Operator, or Security Reader in Azure Active Directory to access the Microsoft 365 Defender portal.

The Microsoft 365 Defender portal is a specialized workspace designed to meet the needs of security teams and provides actionable insights to help reduce risks and safeguard your digital estate.

Describe how to use Microsoft Secure Score

Microsoft Secure Score, one of the tools in the Microsoft 365 Defender portal, is a representation of a company's security posture. The higher the score, the better your protection.

Secure Score helps organizations:

- Report on the current state of their security posture.
- Improve their security posture by providing discoverability, visibility, guidance, and control.
- Compare benchmarks and establish key performance indicators (KPIs).

Points are given for the following actions:

- Configuring recommended security features.
- Doing security-related tasks.
- Addressing the improvement action with a third-party application or software, or an alternate mitigation.

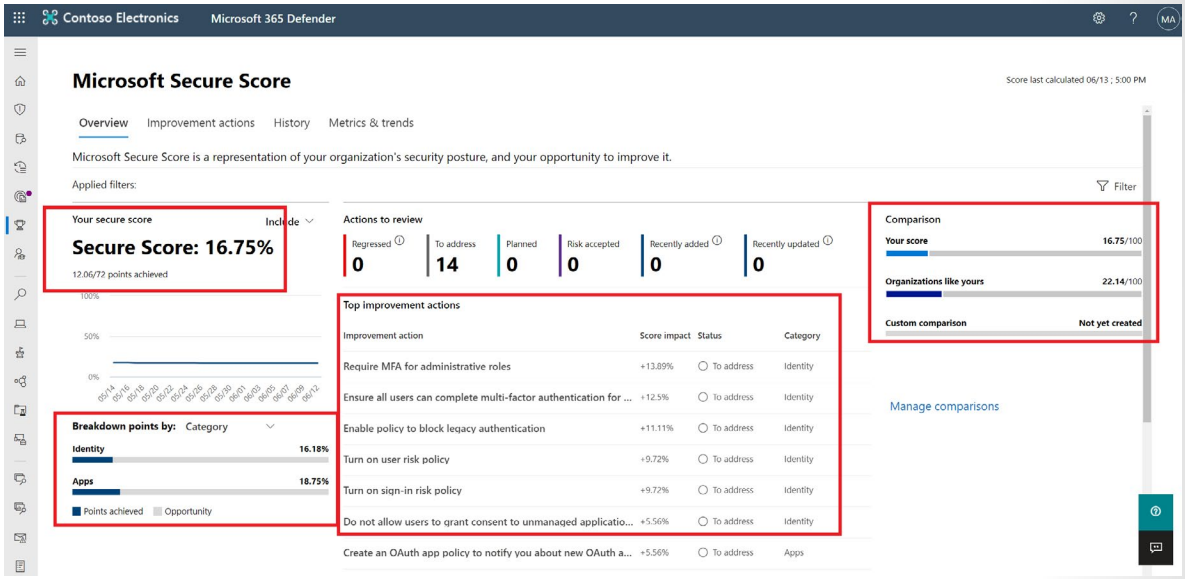
Some improvement actions only give points when fully completed. Others give partial points if they're completed for some devices or users. If you can't, or don't want to, enact one of the improvement actions, you can choose to accept the risk or remaining risk.

If you have a license for one of the supported Microsoft products, you'll see related recommendations. Secure Score will show all possible improvements for the product, whatever the license edition, subscription, or plan. You'll then see all the security best practices and improvements that can be made to your score.

Your absolute security posture, represented by Secure Score, stays the same whatever licenses your organization owns for a specific product. Keep in mind that security should be balanced with usability, and not every recommendation can work for your environment.

Currently Microsoft Secure Score supports recommendations for Microsoft 365 (including Exchange Online), Azure Active Directory, Microsoft Defender for Endpoint, Microsoft Defender for Identity, and Cloud App Security. New recommendations are being added to Secure Score all the time.

The image below shows an organization's Secure Score, a breakdown of the score by points, and the improvement actions that can boost the organization's score. Finally, it provides an indication of how well the organization's Secure Score compares to other similar organizations.



Differences between the Azure and Microsoft Secure Score

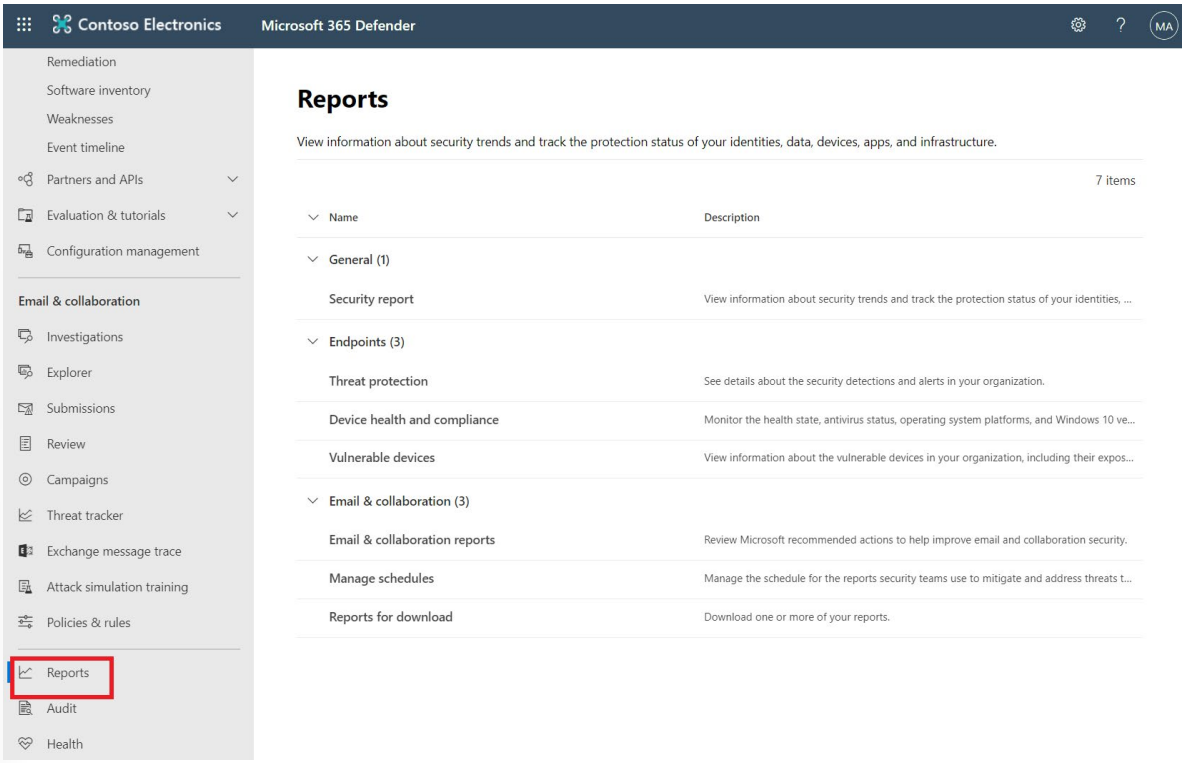
There's a Secure Score for both Microsoft 365 Defender and Azure Defender, but they're subtly different. Secure Score in the Azure Security Center is a measure of the security posture of your Azure subscriptions. Secure Score in the Microsoft 365 Defender portal is a measure of the security posture of the organization across your apps, devices, and identities.

Both the Azure and Microsoft Secure Score provide a list of steps you can take to improve your score. In Microsoft 365 Secure Score, these steps are called improvement actions. In the Azure Secure Score, scores are assessed for each subscription. The steps you can take to improve your score are called security recommendations and they're grouped into security controls.

Use Microsoft Secure Score to understand and rapidly improve your organization's security posture.

Explore Microsoft security reports and dashboards

The Microsoft 365 Defender portal includes a **Reports** section that includes a general security report, reports related to endpoints, and reports related to email and collaboration.



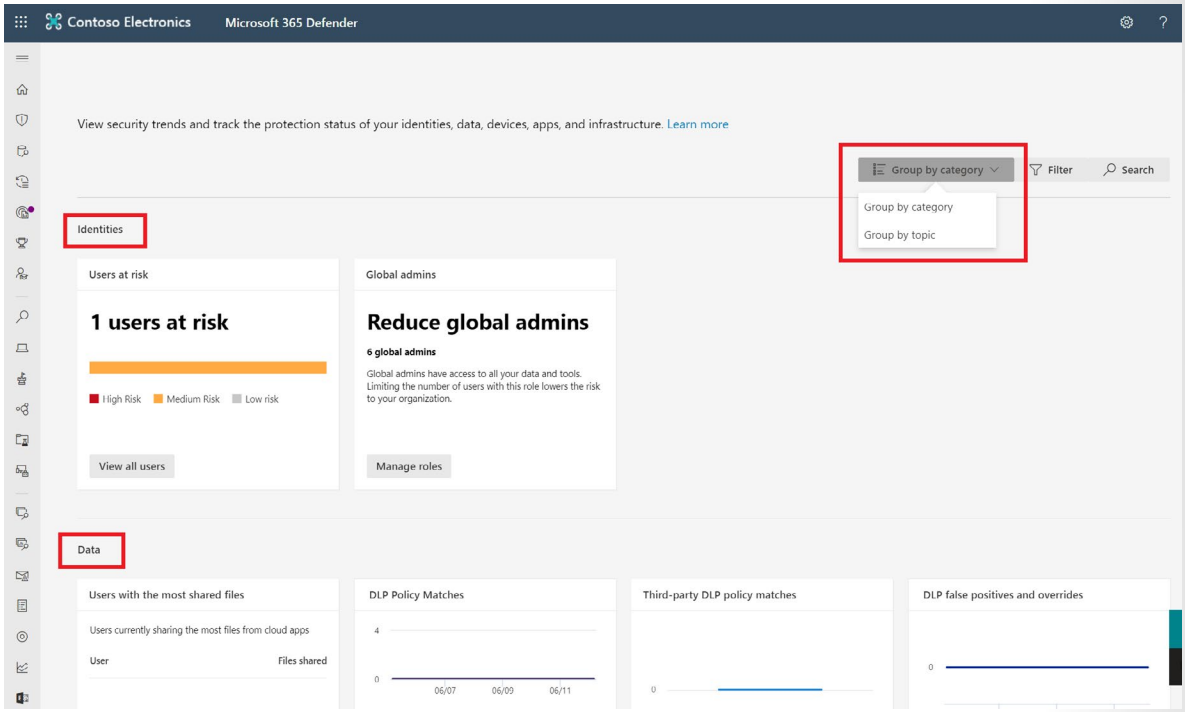
Security report

The general **security report** enables admins to view information about security trends and track the protection status of your identities, data, devices, apps, and infrastructure.

By default, cards are grouped by the following categories:

- **Identities** - user accounts and credentials.
- **Data** - email and document contents.
- **Devices** - computers, mobile phones, and other devices.
- **Apps** - programs and attached online services.

In the example below, the cards are grouped by category (only two of the four categories are shown in the image).



You can also group cards by topic, which will rearrange the cards and group them into the following areas:

- **Risk** - cards that highlight entities, such as accounts and devices, that might be at risk. These cards also highlight possible sources of risk, such as new threat campaigns and privileged cloud apps.
- **Detection trends** - cards that highlight new threat detections, anomalies, and policy violations.
- **Configuration and health** - cards that cover the configuration and deployment of security controls, including device onboarding states to management services.
- **Other** - all cards not categorized under other topics.

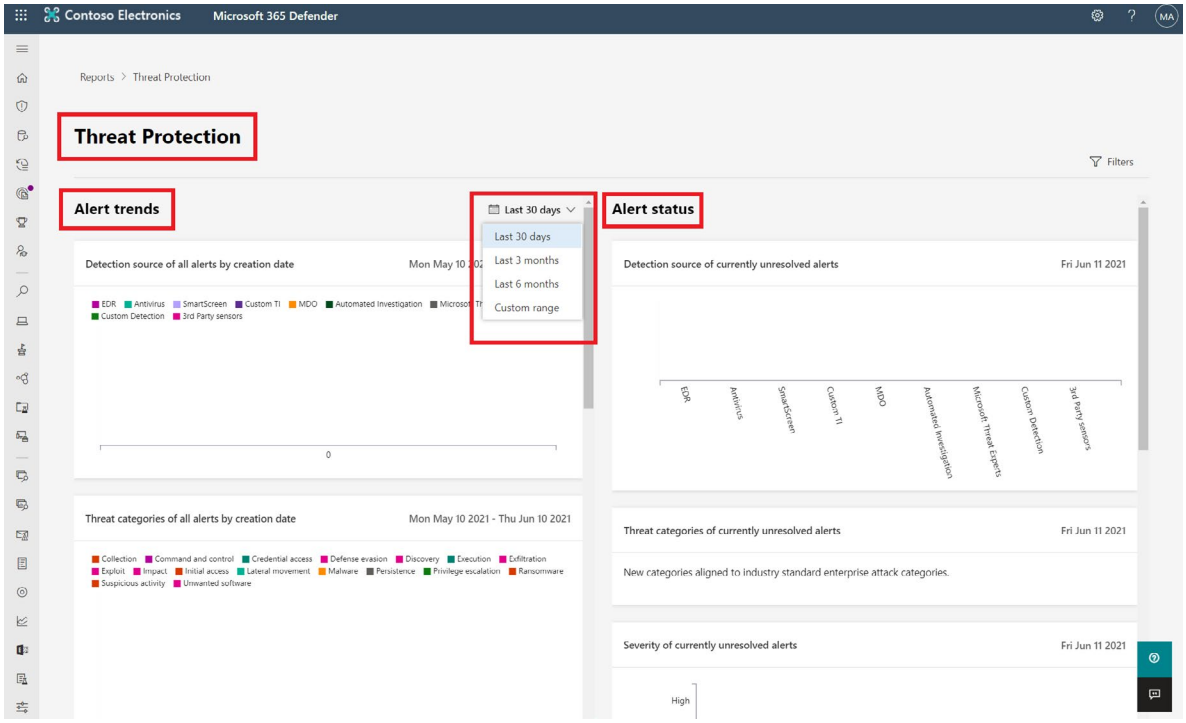
Endpoint reports

The endpoints section on the reports page includes a **threat protection report**, a **device health and compliance report**, and a **vulnerable devices report**.

- The **threat protection report** provides high-level information about alerts generated in your organization. The report includes trending information showing the detection sources, categories, severities, statuses, classifications, and determinations of alerts across time.

  The report's dashboard is structured into two sections:

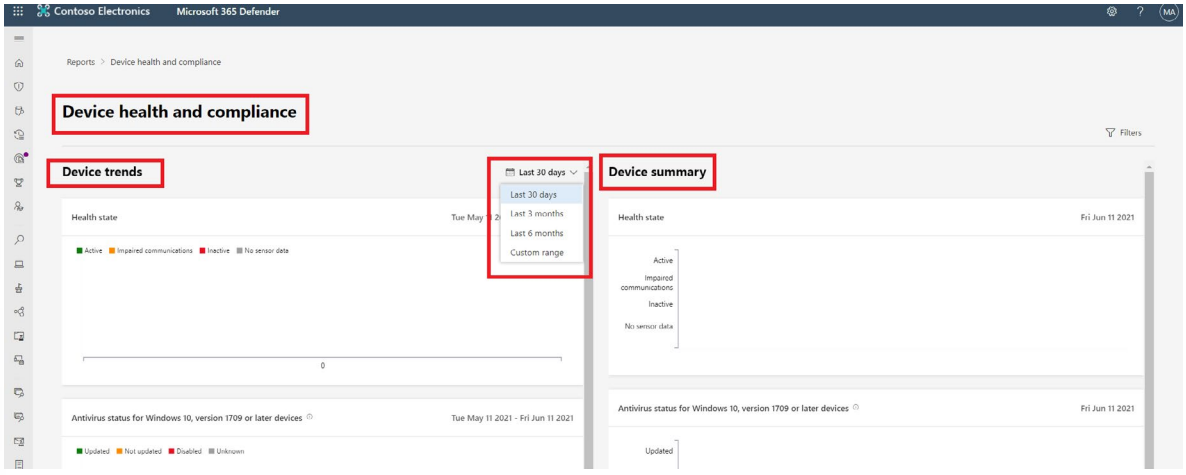
  - Alert trends - By default, the alert trends display alert information from the 30-day period ending in the latest full day. To gain better perspective on trends occurring in your organization, you can fine-tune the reporting period by selecting a time range (30 days, 3 months, 6 months, or custom)
  - Alert summary - The alert summary shows alert information scoped to the current day.



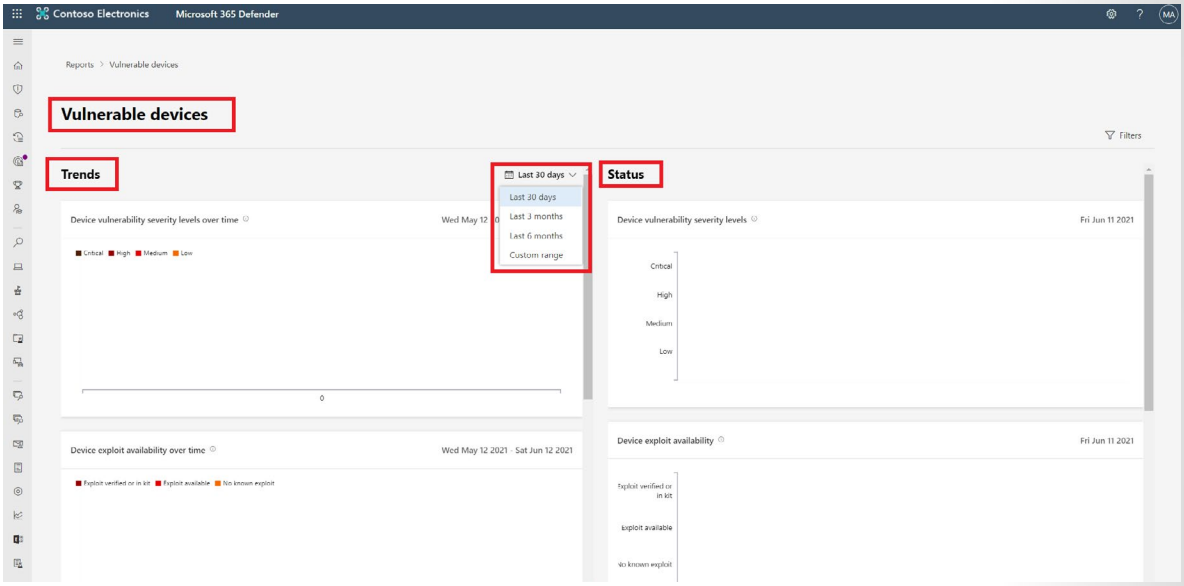
- The **device health and compliance report** enables admins to monitor the health state, antivirus status, operating system platforms, and Windows 10 versions for devices in your organization.

  This report's dashboard is also structured into two sections:

  - Device trends - By default, the device trends displays device information from the 30-day period ending in the latest full day. To gain better perspective on trends occurring in your organization, you can fine-tune the reporting period by adjusting the time period.
  - Device summary - The device summary shows device information scoped to the current day.

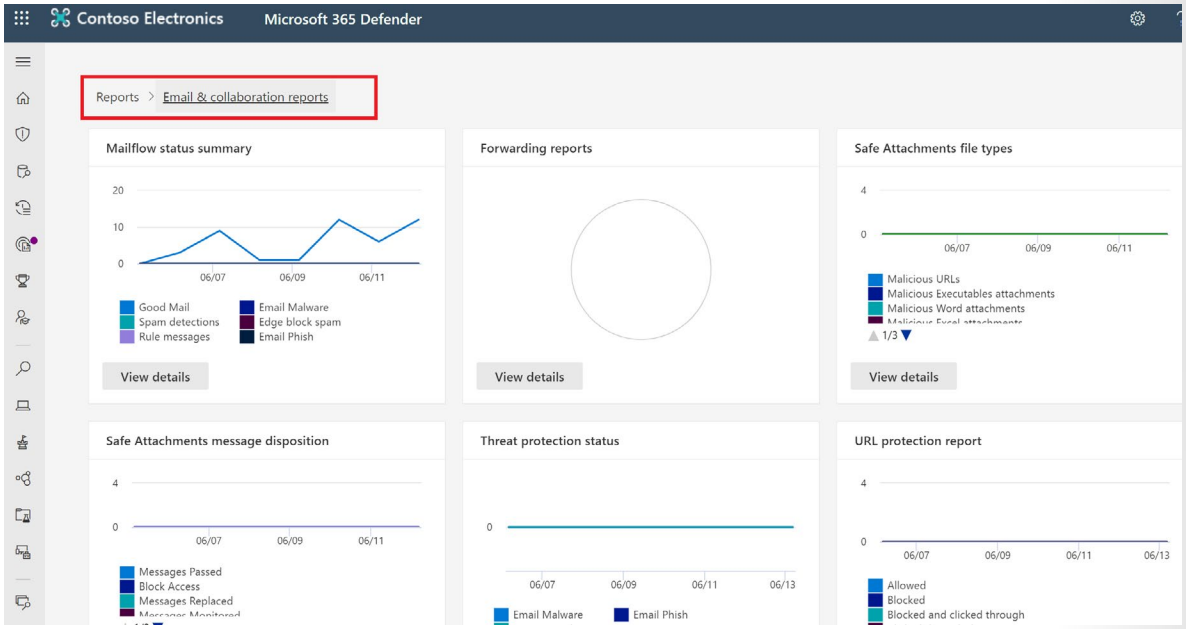


- The **vulnerable devices report** enables admins to view information about the vulnerable devices in your organization, including their exposure to vulnerabilities by severity level, exploitability, age, and more.



Email and collaboration reports

The **email and collaboration reports** enable admins to review Microsoft recommended actions to help improve email and collaboration security.



Describe Microsoft incidents and incident management capabilities

Incidents are a collection of correlated alerts created when a suspicious event is found. Alerts are generated from different device, user, and mailbox entities, and can come from many different domains. These alerts are automatically aggregated by Microsoft 365 Defender. It's the grouping of these related alerts that form an incident. The incident provides a comprehensive view and context of an attack.

Security personnel can use an incident to determine where an attack started, what methods were used, and to what extent the attack has progressed within the network. They can also determine the scope of the attack, and how many users, devices, and mailboxes were affected. The severity of the attack can also be determined.

Incident management

Managing incidents is critical in ensuring that threats are contained and addressed. In Microsoft 365 Defender, you can manage incidents on devices, users accounts, and mailboxes.

You can manage incidents by selecting one from the Incidents queue.

Incidents are automatically assigned a name based on an alert. You can edit the name of an incident, resolve it, then set its classification and determination. You can also assign the incident to yourself and add incident tags and comments.

When you investigate cases where you want to move alerts from one incident to another, you can also do so from the Alerts tab. You'll create a larger or smaller incident that includes all relevant alerts.

Watch **incident management**[36] for a video walk-through on how to manage an incident.

Take advantage of incidents to effectively and appropriately respond to alerts across your organization's environment.

Knowledge check

Multiple choice

Item 1. Admins in the organization are using the Microsoft 365 Defender portal on a daily basis. They want to quickly get an understanding of your organization's current security posture. Which capability in the Microsoft 365 Defender portal will they use?

- ☐ Reports.
- ☐ Secure score.
- ☐ Policies.

Multiple choice

Item 2. Which of the following describes what an admin would need to select to view security cards grouped by risk, detection trends, configuration, health, and more?

- ☐ Group by topic.
- ☐ Group by risk.
- ☐ Group by category.

36 https://www.microsoft.com/en-us/videoplayer/embed/RE4J3mt

Multiple choice

Item 3. An admin wants to get a comprehensive view of an attack, including where the attack started, what tactics were used, and how far the attack has gone in the network. What can the admin use to view this type of information?

- ☐ Alerts
- ☐ Reports
- ☐ Incidents

Summary and resources

You've seen several features of Microsoft security center where you can manage security across Microsoft identities, data, devices, and apps.

Now that you've completed this lesson, you should be able to:

- Describe and explore Microsoft 365 security center.
- Describe how to use Microsoft Secure Store.
- Explore security reports and dashboards.
- Describe incidents and incident management capabilities.

Learn more

- **Overview of the Microsoft 365 Defender portal**[37]
- **Microsoft Secure Score**[38]
- **Secure Score in Azure Security Center**[39]
- **Integrated reports**[40]
- **Threat protection report in Microsoft Defender for Endpoint**[41]
- **Device health and compliance report in Microsoft Defender for Endpoint**[42]
- **Incidents overview in Microsoft 365 Defender**[43]

37 https://docs.microsoft.com/microsoft-365/security/mtp/overview-security-center?view=o365-worldwide
38 https://docs.microsoft.com/microsoft-365/security/mtp/microsoft-secure-score?view=o365-worldwide
39 https://docs.microsoft.com/azure/security-center/secure-score-security-controls?WT.mc_id=Portal-Microsoft_Azure_Security
40 https://docs.microsoft.com/microsoft-365/security/mtp/overview-security-center?view=o365-worldwide#integrated-reports
41 https://docs.microsoft.com/microsoft-365/security/defender-endpoint/threat-protection-reports?view=o365-worldwide
42 https://docs.microsoft.com/microsoft-365/security/defender-endpoint/machine-reports?view=o365-worldwide
43 https://docs.microsoft.com/microsoft-365/security/mtp/incidents-overview?view=o365-worldwide

Describe endpoint security with Microsoft Intune

Introduction

In this lesson, you'll explore what Intune is and how to use Endpoint Security to manage devices with Microsoft Endpoint Manager.

After completing this lesson, you'll be able to:

- Describe what Intune is.
- Describe the tools available with Intune.
- Describe how to manage devices with Microsoft Endpoint Manager.

Describe what is Intune

Microsoft Intune is a cloud-based service that focuses on mobile device management (MDM) and mobile application management (MAM). You control how your organization's devices, including mobile phones, tablets, and laptops, are used. You can also configure specific policies to control applications. For example, you can prevent emails from being sent to people outside your organization.

Intune also allows people in your organization to use their personal devices for school or work. On personal devices, Intune helps make sure your organization data stays protected, and can isolate it from personal data.

With Intune, admins can:

- Support a diverse mobile environment and manage iOS/iPadOS, Android, Windows, and macOS devices securely.
- Set rules and configure settings on personal and organization-owned devices to access data and networks.
- Deploy and authenticate apps for both on-premises and mobile devices.
- Protect your company information by controlling the way users access and share information.
- Be sure devices and apps are compliant with your security requirements.

Mobile device management (MDM)

For devices that are owned by the business, organizations can maintain full control. This includes settings, features, and security. When these devices are enrolled with Intune, they'll receive rules and settings defined by Intune policies. For example, you can define password requirements.

When devices are enrolled and managed in Intune, administrators can:

- See the devices enrolled, and get an inventory of the ones accessing organization resources.
- Configure devices so they meet your security and health standards. For example, you probably want to block jailbroken devices.
- Push certificates to devices so users can easily access your Wi-Fi network, or use a VPN to connect to it.
- See reports on users and devices to determine if they're compliant.

- Remove organization data if a device is lost, stolen, or not used anymore.

To learn more, visit **Manage devices**[44].

Mobile application management (MAM)

Users with personal devices might not want their phone to be under full corporate control. Mobile application management (MAM) gives admins the ability to protect corporate data at the application level. Where users just want to access apps like email or Microsoft Teams, admins can use application protection policies, without requiring the device to be enrolled in Intune, supporting bring-your-own device (BYOD) scenarios.

MAM can be used with custom applications and store apps.

When apps are managed in Intune, administrators can:

- Add and assign mobile apps to user groups and devices, including users and devices in specific groups, and more.
- Configure apps to start or run with specific settings enabled and update existing apps already on the device.
- See reports on which apps are used and track their usage.
- Do a selective wipe by removing only organization data from apps.

To learn more, visit **Manage apps**[45].

Describe endpoint security with Intune

When admins want to configure and manage security tasks for at-risk devices, they can go to the Endpoint security node in Intune.

Manage devices

The Endpoint security node includes the *All devices* view, where you'll see a list of all devices from your Azure AD that are available in Microsoft Endpoint Manager.

From this view, you can select devices to drill in for more information, such the policies to which a device is not compliant. You can also use access from this view to remediate issues for a device, including restarting, start a scan for malware, or rotate BitLocker keys on a Windows 10 device.

For more information, visit **Manage devices with endpoint security in Microsoft Intune**[46].

Manage security baselines

Intune includes security baselines for Windows devices and a growing list of applications, including Microsoft Edge, Microsoft Defender for Endpoint (previously Microsoft Defender Advanced Threat Protection), and more. Security baselines are preconfigured groups of Windows settings that help admins apply recommended security. To learn more, visit **Use security baselines to configure Windows 10 devices in Intune**[47]

44 https://docs.microsoft.com/mem/intune/fundamentals/what-is-intune#manage-devices
45 https://docs.microsoft.com/mem/intune/fundamentals/what-is-intune#manage-apps
46 https://docs.microsoft.com/mem/intune/protect/endpoint-security-manage-devices
47 https://docs.microsoft.com/mem/intune/protect/security-baselines

As an example, the MDM Security Baseline automatically enables BitLocker for removable drives, automatically requires a password to unlock a device, and automatically disables basic authentication. Admins can also customize the baselines to enforce only those settings and values that are required.

Use policies to manage device security

Each Endpoint security policy focuses on aspects of device security like antivirus, disk encryption, firewalls, and areas such as endpoint detection and response and attack surface reduction, made available through integration with Microsoft Defender for Endpoint. To learn more, visit **Manage device security with endpoint security policies in Microsoft Intune**[48].

Endpoint security policies are one of several methods in Intune to configure settings on devices. When managing settings, it's important to understand what other methods being used in your environment can configure your devices and to avoid policy conflicts.

Use device compliance policy

Use device compliance policy to establish the conditions by which devices and users are allowed to access the corporate network and company resources. With compliance policies, admins can set the rules that devices and users must meet to be considered compliant. Rules can include OS versions, password requirements, device threat levels, and more. To learn more, visit **Use compliance policies to set rules for devices you manage with Intune**[49].

Device compliance policies are one of several methods in Intune to configure settings on devices. When managing settings, it's important to understand what other methods being used in your environment can configure your devices and to avoid policy conflicts.

Configure conditional access

Intune can be integrated with Azure AD conditional access policies to enforce compliance policies. Intune passes the results of your device compliance policies to Azure AD, which then uses conditional access policies to enforce which devices and apps can access your corporate resources.

The following are two common methods of using conditional access with Intune:

- Device-based conditional access, to ensure only managed and compliant devices can access network resources.
- App-based conditional access, which uses app protection policies to manage access to network resources by users on devices that aren't managed with Intune.

To learn more about using conditional access with Intune, visit **Learn about Conditional Access and Intune.**[50]

Integration with Microsoft Defender for Endpoint

Intune can integrate with Microsoft Defender for Endpoint (formerly Microsoft Defender ATP) for a Mobile Threat Defense solution. Integration can help prevent security breaches and limit the impact of breaches within an organization.

48 https://docs.microsoft.com/mem/intune/protect/endpoint-security-policy
49 https://docs.microsoft.com/mem/intune/protect/device-compliance-get-started
50 https://docs.microsoft.com/mem/intune/protect/conditional-access

Microsoft Defender for Endpoint works with devices that run:

- Android
- iOS/iPadOS
- Windows 10 or later

By integrating Intune with Microsoft Defender for Endpoint, organizations can take advantage of Microsoft Defender for Endpoint's Threat and Vulnerability Management (TVM), using Intune to remediate endpoint weakness identified by TVM.

To learn more visit **Enforce compliance for Microsoft Defender for Endpoint with Conditional Access in Intune**[51].

Role-based access control with Microsoft Intune

Role-based access control (RBAC) helps manage who has access to the organization's resources and what they do with them. By assigning roles to Intune users, admins limit what they'll see and change. Each role has a set of permissions that determine what users with that role can access and change within your organization.

To manage tasks in the Endpoint security node of the Microsoft Endpoint Manager admin center, an account must have RBAC permissions equal to the permissions provided by the built-in Intune role of **Endpoint Security Manager**. The Endpoint Security Manager role grants access to the Microsoft Endpoint Manager admin center. This role can be used by individuals who manage security and compliance features, including security baselines, device compliance, conditional access, and Microsoft Defender for Endpoint.

To learn more, visit **Role-based access control (RBAC) with Microsoft Intune**[52].

Video demonstration of Microsoft Endpoint Manager capabilities

Watch **Explore endpoint security**[53], to explore Endpoint Manager and some of its capabilities.

Knowledge check

Multiple choice

Item 1. Employees are allowed to bring and use their cell phones at work. The employees don't want their phone to be under full corporate control, but admins want to allow users to read emails and use Teams while protecting corporate data. Which of the following will allow admins to accomplish these goals?

☐ Mobile Application Management (MAM).

☐ Mobile Device Management (MDM).

☐ Role-based access control (RBAC).

51 https://docs.microsoft.com/mem/intune/protect/advanced-threat-protection
52 https://docs.microsoft.com/mem/intune/fundamentals/role-based-access-control
53 https://www.microsoft.com/en-us/videoplayer/embed/RE4LTIu

Multiple choice

Item 2. An organization uses different types of devices, including Windows, iOS, and Android devices. Admins for that organization have created a security baseline profile in Intune that they want to apply across the devices. To which devices can the security baseline profile be applied?

- ☐ Android devices.
- ☐ iOS devices.
- ☐ Windows devices.

Summary and resources

You wanted to understand the capabilities of Intune as it relates to endpoint security. You've explored some of the tools that are available with Intune. Also, you needed to know how to manage devices with Microsoft Endpoint Manager. You've learned about managing devices, security baselines, and using policies to manage device security.

Now that you've completed this lesson, you should be able to:

- Describe what Intune is.
- Describe the tools available with Intune.
- Describe how to manage devices with Microsoft Endpoint Manager.

Learn more

- **Microsoft Intune is an MDM and MAM provider for your devices**[54]
- **Manage endpoint security in Microsoft Intune**[55]
- **Role-based access control (RBAC) with Microsoft Intune**[56]
- **Common ways to use Microsoft Intune**[57]
- **Interactive guide: manage devices with Microsoft Endpoint Manager**[58]

54 https://docs.microsoft.com/mem/intune/fundamentals/what-is-intune?
55 https://docs.microsoft.com/mem/intune/protect/endpoint-security
56 https://docs.microsoft.com/mem/intune/fundamentals/role-based-access-control
57 https://docs.microsoft.com/mem/intune/fundamentals/common-scenarios
58 https://mslearn.cloudguides.com/guides/Manage%20devices%20with%20Microsoft%20Endpoint%20Manager

Answers

Multiple choice

Item 1. The security admin has created an Azure Network Security Group (NSG) to filter network traffic to a virtual machine. The admin wants to allow inbound traffic using the Remote Desktop Protocol (RDP), but the default NSG rules are currently blocking all inbound traffic that is not from another virtual network or an Azure load balancer. What does the security admin have to do to allow inbound traffic using RDP?

- ☐ Delete the default rule.
- ■ Create a new network security rule that allows RDP traffic and that has a higher priority than the default rule.
- ☐ There is nothing the admin can do, RDP traffic is not supported with NSGs.

Explanation
Default NSG rules cannot be deleted, but you can override them by creating new rules with higher priorities.

Multiple choice

Item 2. The security admin wants to protect Azure resources from DDoS attacks, which Azure DDoS Protection tier will the admin use to target Azure Virtual Network resources?

- ☐ Basic.
- ■ Standard.
- ☐ Advanced.

Explanation
The Standard service tier provides additional mitigation capabilities that are tuned specifically to Microsoft Azure Virtual Network resources.

Multiple choice

Item 3. Your organization has several virtual machines in Azure. The security admin wants to deploy Azure Bastion to get secure access to the virtual machines in Azure. What should the admin keep in mind?

- ■ Azure Bastion is deployed per virtual network.
- ☐ Azure Bastion is deployed per subscription.
- ☐ Azure Bastion is deployed per virtual machine.

Explanation
Azure Bastion deployment is per virtual network, not per subscription/account or virtual machine.

Multiple choice

Item 4. Much of your organization's application data is in Azure. The security admin wants to take advantage of the encryption capabilities in Azure, which service would the admin use to store the application's secrets?

- ☐ Transparent data encryption.
- ☐ Secrets management.
- ■ Azure Key Vault.

Explanation
Azure Key Vault is a centralized cloud service for storing your application secrets.

Multiple choice

Item 1. An organization is using Azure and wants to improve their security best practices. Which Azure specific benchmark would the IT security team need to consider?

■ Azure Security Benchmark.

☐ Center for Internet Security.

☐ Microsoft cybersecurity group

Explanation
The Azure Security Benchmark provides prescriptive best practices and recommendations to help improve the security of workloads, data, and services on Azure.

Multiple choice

Item 2. Your organization is using Azure Security Center to assess your resources, subscriptions, and organization for security issues. Your organization's overall secure score is low and needs to improve. How would a security admin go about improving the score?

☐ Close old security recommendations.

■ Remediate security recommendations.

☐ Move security recommendations to resolved.

Explanation
To improve your secure score, remediate security recommendations from your recommendations list.

Multiple choice

Item 3. An organization needs to continuously monitor the security status of its network. What Security Center tool would they use?

☐ Continuous assessment.

■ Network map.

☐ Network assessment.

Explanation
The network map provides a map of the topology of your network workloads, which lets you block unwanted connections.

Multiple choice

Item 1. As the lead admin, it is important to convince your team to start using Azure Sentinel. You've put together a presentation. What are the four security operation areas of Azure Sentinel that cover this area?

☐ Collect, Detect, Investigate, and Redirect.

■ Collect, Detect, Investigate, and Respond.

☐ Collect, Detect, Investigate, and Repair.

Explanation
A SIEM/SOAR solution uses collect, detect, investigate, and respond to identify and protect your organizations network perimeter.

Multiple choice

Item 2. Your estate has many different data sources where data is stored. Which tool should be used with Azure Sentinel to quickly gain insights across your data as soon as a data source is connected?

■ Azure Monitor Workbooks.

☐ Playbooks.

☐ Microsoft 365 Defender.

Explanation
Using the Azure Sentinel integration with Azure Monitor Workbooks, allows you to monitor data and provides versatility in creating custom workbooks.

Multiple choice

Item 1. A lead admin for an organization is looking to protect against malicious threats posed by email messages, links (URLs), and collaboration tools. Which solution from the Microsoft 365 Defender suite is best suited for this purpose?

■ Microsoft Defender for Office 365.

☐ Microsoft Defender for Endpoint.

☐ Microsoft Defender for Identity.

Explanation
Microsoft Defender for Office 365 safeguards your organization against malicious threats posed by email messages, links (URLs), and collaboration tools, including Microsoft Teams, SharePoint Online, OneDrive for Business, and other Office clients.

Multiple choice

Item 2. As the admin for team, you're required to provide a short presentation on the use and benefit of Microsoft Cloud App Security to your team. Which of the four MCAS pillars is responsible for identifying and controlling sensitive information?

☐ Threat protection.

☐ Compliance.

■ Data Security.

Explanation
Through the Data Security pillar, you can identify and control sensitive information and respond to classification labels on content.

Multiple choice

Item 3. Which of the following is a is a cloud-based security solution that identifies, detects, and helps to investigate advanced threats, compromised identities, and malicious insider actions directed at your organization?

☐ Microsoft Defender for Office 365

■ Microsoft Defender for Identity

☐ Microsoft Cloud App Security

Explanation
Microsoft Defender for Identity is a cloud-based security solution that identifies, detects, and helps you investigate advanced threats, compromised identities, and malicious insider actions directed at your organization.

Multiple choice

Item 1. Admins in the organization are using the Microsoft 365 Defender portal on a daily basis. They want to quickly get an understanding of your organization's current security posture. Which capability in the Microsoft 365 Defender portal will they use?

☐ Reports.

■ Secure score.

☐ Policies.

Explanation
Secure score in the M365 Defender portal will give you a snapshot of your organization's security posture, and provide you with details on how to improve it.

Multiple choice

Item 2. Which of the following describes what an admin would need to select to view security cards grouped by risk, detection trends, configuration, health, and more?

■ Group by topic.

☐ Group by risk.

☐ Group by category.

Explanation
You'd use this filter to view security cards grouped by risk, detection trends, configuration, health, and more.

Multiple choice

Item 3. An admin wants to get a comprehensive view of an attack, including where the attack started, what tactics were used, and how far the attack has gone in the network. What can the admin use to view this type of information?

☐ Alerts

☐ Reports

■ Incidents

Explanation
An incident is a collection of correlated alerts that make up the story of an attack.

Multiple choice

Item 1. Employees are allowed to bring and use their cell phones at work. The employees don't want their phone to be under full corporate control, but admins want to allow users to read emails and use Teams while protecting corporate data. Which of the following will allow admins to accomplish these goals?

■ Mobile Application Management (MAM).

☐ Mobile Device Management (MDM).

☐ Role-based access control (RBAC).

Explanation
This service will allow you to manage apps on your employees mobile devices without needing full control.

Multiple choice

Item 2. An organization uses different types of devices, including Windows, iOS, and Android devices. Admins for that organization have created a security baseline profile in Intune that they want to apply across the devices. To which devices can the security baseline profile be applied?

- ☐ Android devices.
- ☐ iOS devices.
- ■ Windows devices.

Explanation
Security baseline settings are used only on devices running Windows 10 version 1809 or later.

Module 4 Describe the capabilities of Microsoft compliance solutions

Describe the compliance management capabilities in Microsoft

Introduction

Organizations must stay in line with compliance-related legal and regulatory standards to protect their customers, partners, and themselves. Microsoft provides tools and capabilities to enable organizations to manage compliance.

In this lesson, you'll learn about the common compliance needs organizations are required to meet. You will know where to go to find compliance documentation by exploring the Service Trust Portal. You will also learn about Microsoft's privacy principles. You'll also explore solutions like the Microsoft 365 compliance center and the Compliance Manager, which can help manage and simplify compliance across an organization.

After completing this lesson, you'll be able to:

- Find compliance documentation.
- Describe Microsoft's privacy principles.
- Explore the Microsoft 365 compliance center.
- Describe the benefits of Compliance Manager.

Describe common compliance needs

Data has become more important than ever. Organizations, institutions, and entire societies generate and rely on data to function on a day-to-day basis. Any manipulation or loss of data can damage organizations, institutions, and societies alike. The sheer scale of data generated and the increasing reliance on it, means data management has become pivotal.

Governments are working hard to protect people by creating regulations (laws) that are designed to protect data through several measures including:

- Granting individuals the right to access their data at any time.
- Granting individuals the right to correct or delete data about them if needed.
- Introducing retention periods that dictate a minimum or maximum amount of time data should be stored.
- Enabling governments and regulatory agencies the right to access and examine data when necessary.
- Defining rules for what data can be processed and how that should be done.

Some regulations also require that data remains protected even if it's moved between geographic locations. For example, regulations in some countries require that any personal data transferred outside of their borders meets several conditions including:

- The destination country where personal data is to be transferred must be considered to have adequate protections for the data.
- Organizations must create appropriate safeguards, such as specific clauses that must be included in contracts with organizations or bodies that handle any personal data.

Common compliance regulations

Some of the regulations that organizations and institutions commonly work with include:

- **Health Insurance Portability and Accountability Act (HIPAA)** – introduces rules on how health-related information should be protected.
- **The Family Educational Rights and Privacy Act (FERPA)** – introduces rules to protect student information.
- **ISO 27701** – specifies rules and guidance to manage personal information, and demonstrate compliance.

Microsoft supports organizations' compliance needs with built-in tools and capabilities to help them protect information, manage data governance, and respond to regulatory requests.

Explore the Service Trust Portal

The Service Trust Portal provides information, tools, and other resources about Microsoft security, privacy, and compliance practices. Sign in with your Microsoft cloud services account to access all the available documentation.

From the main menu, you have access to:

- **Service Trust Portal** – home page.
- **Compliance Manager** – measures your progress in completing actions that help reduce risks around data protection and regulatory standards. To learn more, see the Microsoft Compliance Manager documentation in the Learn More section below.
- **Trust Documents** – links to a security implementation and design information.
- **Industries & Regions** – contains compliance information about Microsoft Cloud services organized by industry, and region. The Industry Solutions link currently displays the home page for Financial Services. The Regional Solutions links currently have information for: Australia, Canada, Czech Republic, Denmark, Germany, Poland, Romania, Spain, and the United Kingdom.

- **Trust Center** - links to the Microsoft Trust Center, which provides more information about security, compliance, and privacy in the Microsoft Cloud.
- **Resources** - links to resources including Information about the features and tools available for data governance and protection in Office 365, the Microsoft Global Datacenters, and Frequently Asked Questions.
- **My Library** - allows you to add documents and resources that are relevant to your organization, everything is in one place. You can also opt to have email notifications sent when a document is updated, as well as the frequency you receive notifications.

Interactive guide

Explore the Service Trust Portal through an interactive click-through guide. Select the link below to get started.

Explore the Service Trust Portal[1]

Describe Microsoft's privacy principles

Microsoft's products and services run on trust. Microsoft focuses on six key privacy principles when making decisions about data. Privacy is about making meaningful choices about how and why data is collected and used. It's about ensuring that you have the information you need to make the choices that are right for you across all Microsoft products and services.

The six privacy principles are:

- **Control**: Putting you, the customer, in control of your privacy with easy-to-use tools and clear choices.
- **Transparency**: Being transparent about data collection and use so that everyone can make informed decisions.
- **Security**: Protecting the data that is entrusted to Microsoft by using strong security and encryption.
- **Strong legal protections**: Respecting local privacy laws and fighting for legal protection of privacy as a fundamental human right.
- **No content-based targeting**: Not using email, chat, files, or other personal content to target advertising.
- **Benefits to you**: When Microsoft does collect data, it is used to benefit you, the customer, and to make your experiences better.

These principles form Microsoft's privacy foundation, and they shape the way that products and services are designed. To learn more visit **Privacy at Microsoft**[2].

Describe the Compliance Center

The Microsoft 365 compliance center brings together all of the tools and data that are needed to help understand and manage an organization's compliance needs.

Compliance center is available to customers with a Microsoft 365 SKU with one of the following roles:

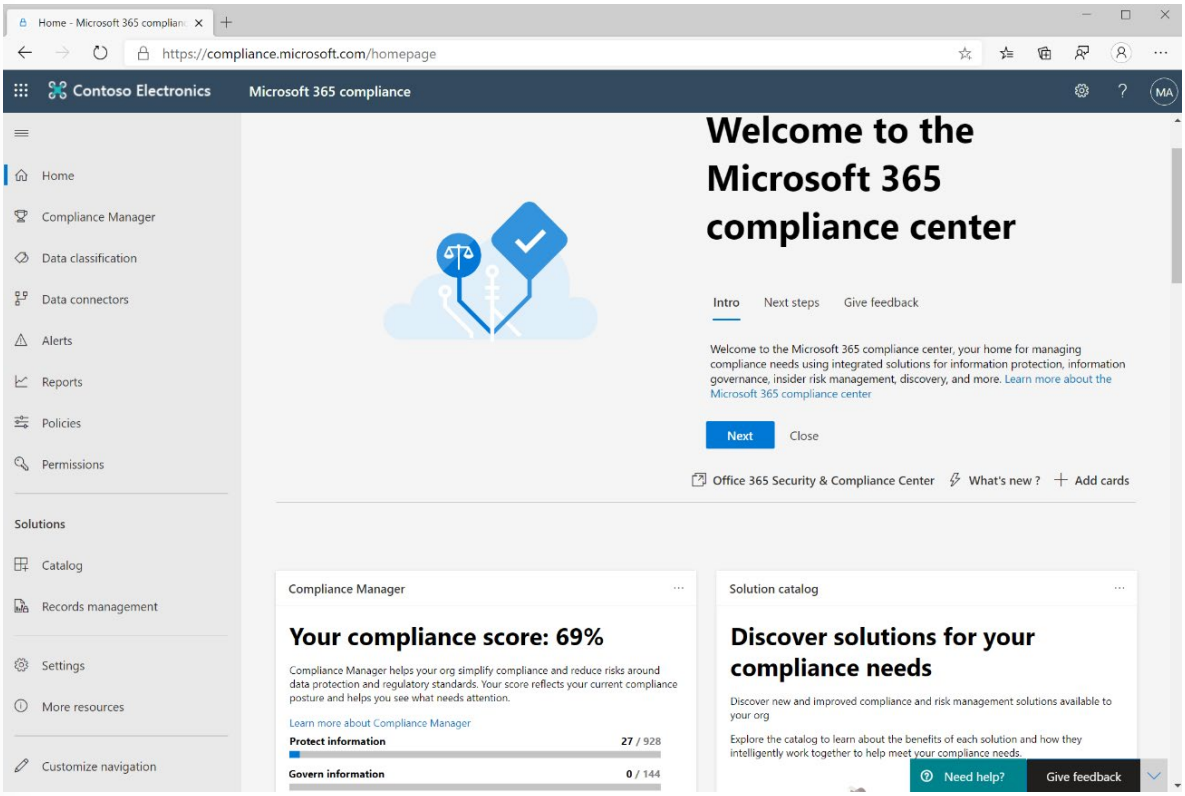
- Global administrator
- Compliance administrator

1 https://edxinteractivepage.blob.core.windows.net/edxpages/Security%20fundamentals/LP01M02%20Explore%20the%20Service%20Trust%20Portal/index.html?azure-portal=true

2 https://privacy.microsoft.com/

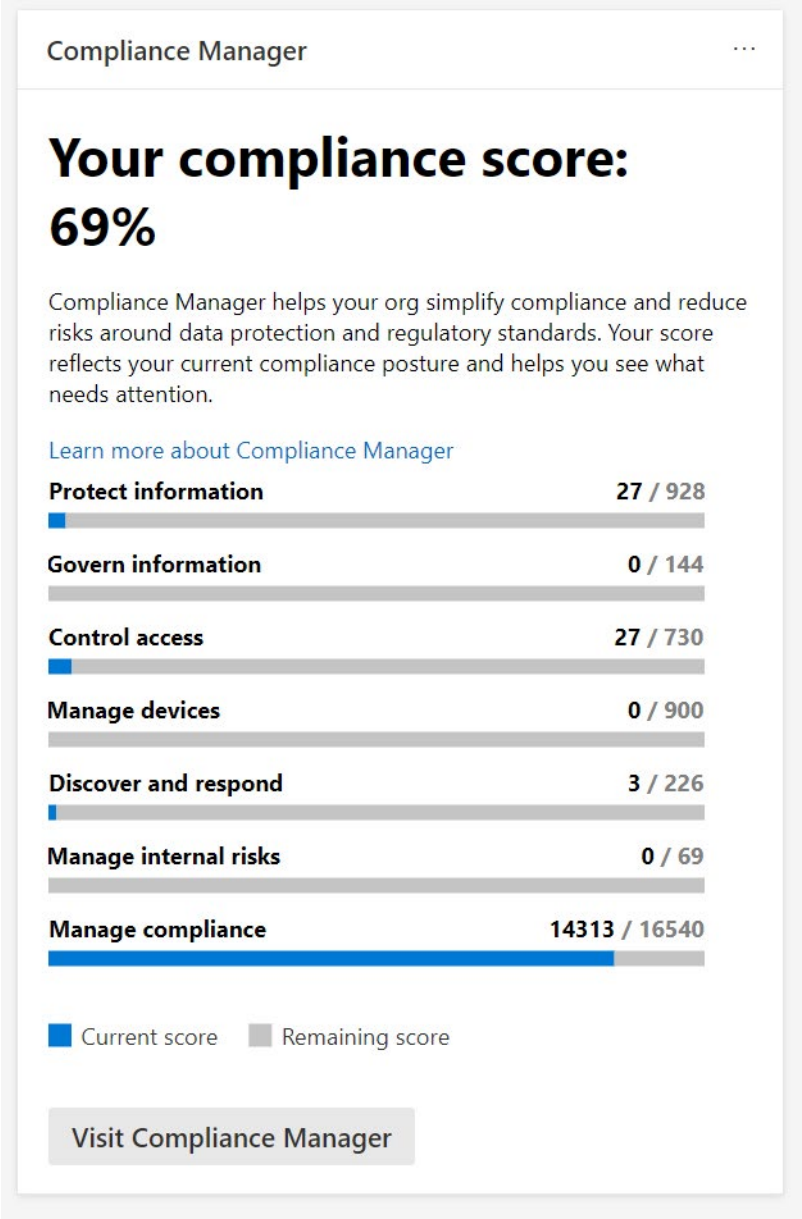
- Compliance data administrator

When an admin signs in to the Microsoft 365 compliance center portal, they'll get a bird's-eye view of how the organization is meeting its compliance requirements, along with which solutions can be used to help with compliance, information about any active alerts, and more.



The default compliance center home page contains several cards including:

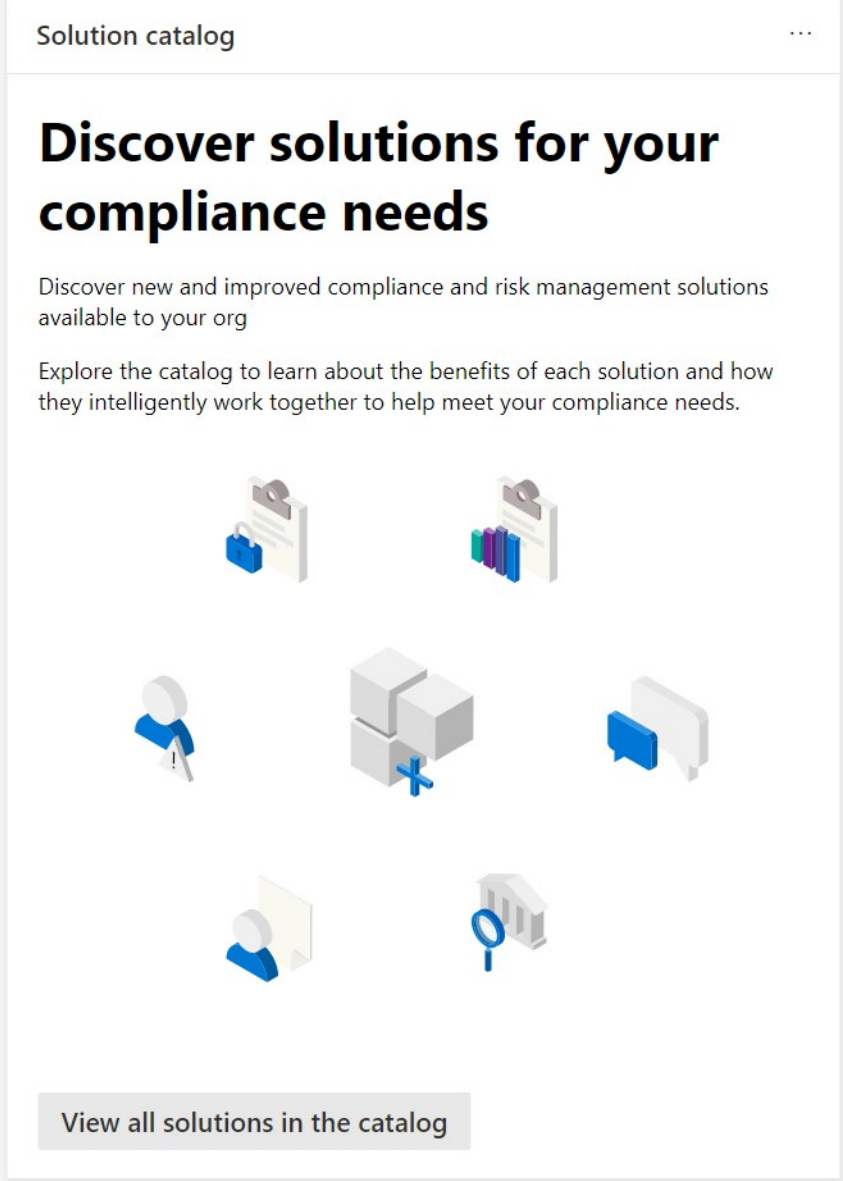
- The **compliance score** card. This card shows the compliance score, and will forward admins to the Compliance Manager where they can see a breakdown of the compliance score. Compliance score measures the progress in completing recommended improvement actions within controls. The score helps an organization to understand its current compliance posture. It also helps an organization to prioritize actions based on their potential to reduce risk.



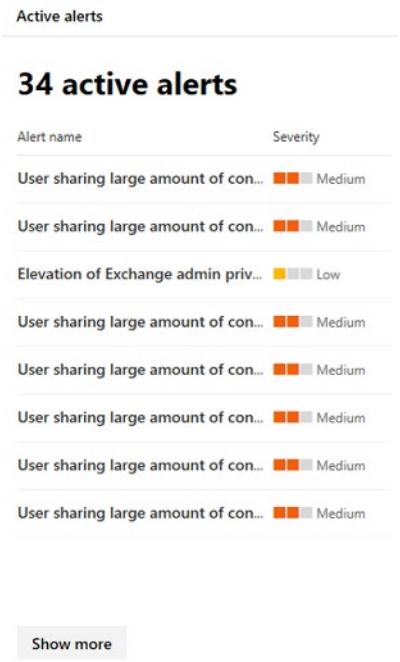
- The new **Solution catalog** card, links to collections of **integrated solutions**[3] that are used to manage end-to-end compliance scenarios across three compliance solutions areas:
  - The **Information protection & governance** section quickly shows you how to use Microsoft 365 compliance solutions to protect and govern data in your organization.
  - The **Insider risk management** section on the home page shows how your organization can identify, analyze, and act on internal risks before they cause harm.
  - The **Discovery & respond section** on the home page shows how your organization can quickly find, investigate, and respond to compliance issues with relevant data.

  A solution's capabilities and tools might include a combination of policies, alerts, reports, and more.

3 https://docs.microsoft.com/microsoft-365/compliance/microsoft-365-solution-catalog?view=o365-worldwide



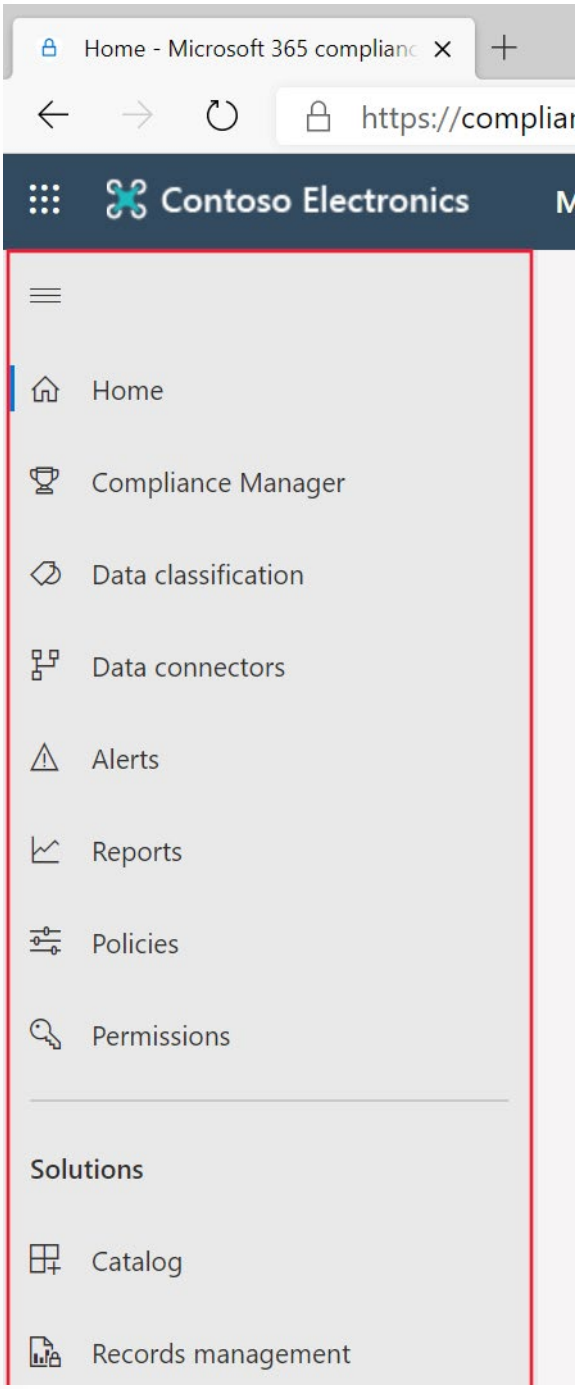
- The **Active alerts** card includes a summary of the most active alerts and a link where admins can view more detailed information, such as alert severity, status, category, and more.



Navigation

In addition to the cards on the home page, there's a navigation pane on the left of the screen that gives easy access to **alerts**[4], **reports**[5], **policies**[6], compliance solutions, and more. To add or remove options for a customized navigation pane, the **Customize navigation** control on the navigation pane can be used to configure which items appear there.

4 https://docs.microsoft.com/microsoft-365/security/office-365-security/alerts?view=o365-worldwide
5 https://docs.microsoft.com/microsoft-365/compliance/reports-in-security-and-compliance?view=o365-worldwide
6 https://docs.microsoft.com/microsoft-365/compliance/alert-policies?view=o365-worldwide



Interactive guide

In this interactive guide, you will explore some of the capabilities of the Microsoft 365 Compliance Center, your home for managing compliance needs using integrated solutions for information protection, information governance, insider risk management, discovery, and more. Select the link below to get started.

Interactive guide - Explore Compliance Center[7]

Describe Compliance Manager

Microsoft Compliance Manager is a feature in the Microsoft 365 Compliance Center that helps admins to manage an organization's compliance requirements with greater ease and convenience. Compliance Manager can help organizations throughout their compliance journey, from taking inventory of data protection risks, to managing the complexities of implementing controls, staying current with regulations and certifications, and reporting to auditors.

Refer to **Compliance Manager**[8] for a brief video overview.

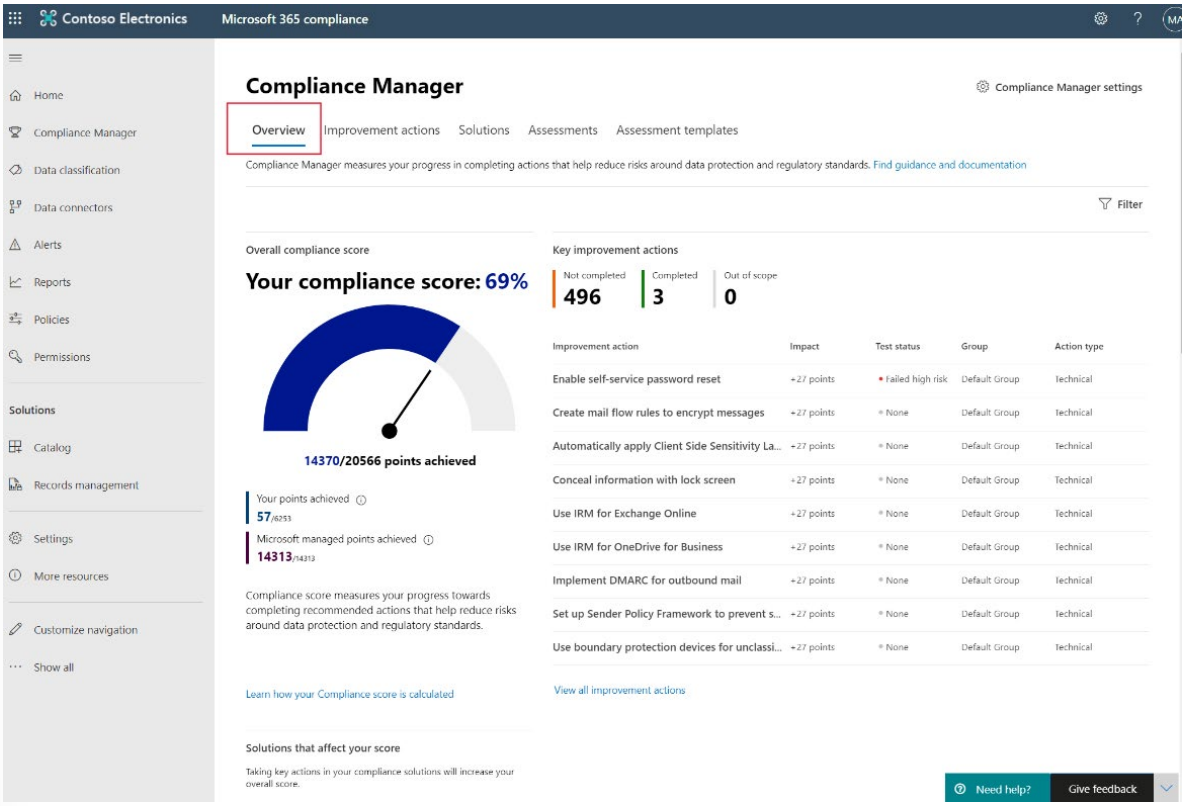
Compliance Manager helps simplify compliance and reduce risk by providing:

- Prebuilt assessments based on common regional and industry regulations and standards. Admins can also use custom assessment to help with compliance needs unique to the organization.
- Workflow capabilities that enable admins to efficiently complete risk assessments for the organization.
- Step-by-step improvement actions that admins can take to help meet regulations and standards relevant to the organization. Some actions will also be managed for the organization by Microsoft. Admins will get implementation details and audit results for those actions.
- Compliance score, which is a calculation that helps an organization understand its overall compliance posture by measuring how it's progressing with improvement actions.

The Compliance Manager dashboard shows the current compliance score, helps admins to see what needs attention, and guides them to key improvement actions.

7 https://edxinteractivepage.blob.core.windows.net/edxpages/Security%20fundamentals/LP04M02%20-%20Explore%20Compliance%20Center/index.html?azure-portal=true

8 https://www.microsoft.com/videoplayer/embed/RE4FGYZ



Compliance Manager uses several data elements to help manage compliance activities. As admins use Compliance Manager to assign, test, and monitor compliance activities, it's helpful to have a basic understanding of the key elements: controls, assessments, templates, and improvement actions.

Controls

A control is a requirement of a regulation, standard, or policy. It defines how to assess and manage system configuration, organizational process, and people responsible for meeting a specific requirement of a regulation, standard, or policy.

Compliance Manager tracks the following types of controls:

- **Microsoft-managed controls**: controls for Microsoft cloud services, which Microsoft is responsible for implementing.
- **Your controls**: sometimes referred to as customer-managed controls, these are implemented and managed by the organization.
- **Shared controls**: responsibility for implementing these controls is shared by the organization and Microsoft.

Assessments

An assessment is a grouping of controls from a specific regulation, standard, or policy. Completing the actions within an assessment helps to meet the requirements of a standard, regulation, or law. For example, an organization may have an assessment that, when the admin completes all actions within it, it helps to bring the organization's Microsoft 365 settings in line with ISO 27001 requirements.

Assessments have several components:

- **In-scope services**: the specific set of Microsoft services applicable to the assessment.
- **Microsoft-managed controls**: controls for Microsoft cloud services, which Microsoft implements for the organization.
- **Your controls**: these controls, sometimes referred to as customer-managed controls, are implemented and managed by the organization.
- **Shared controls**: responsibility for implementing these controls is shared by the organization and Microsoft.
- **Assessment score**: shows the progress in achieving total possible points from actions within the assessment that are managed by the organization and by Microsoft.

When creating assessments, an admin will assign them to a group. The admin can configure groups in whatever way is most logical for the organization. For example, they might group assessments by audit year, region, solution, teams within the organization, or some other way. Once the admin has created groups, the admin can **filter the Compliance Manager dashboard**[9] to view the score by one or more groups.

Templates

Compliance Manager provides templates to help admins to quickly create assessments. They can modify these templates to create an assessment optimized for their needs. Admins can also build a custom assessment by creating a template with their own controls and actions. For example, the admin may want a template to cover an internal business process control, or a regional data protection standard that isn't covered by one of Microsoft's 150-plus prebuilt assessment templates.

Improvement actions

Improvement actions help centralize compliance activities. Each improvement action provides recommended guidance that's intended to help organizations to align with data protection regulations and standards. Improvement actions can be assigned to users in the organization to do implementation and testing work. Admins can also store documentation, notes, and record status updates within the improvement action.

Benefits of Compliance Manager

Compliance Manager provides many benefits, including:

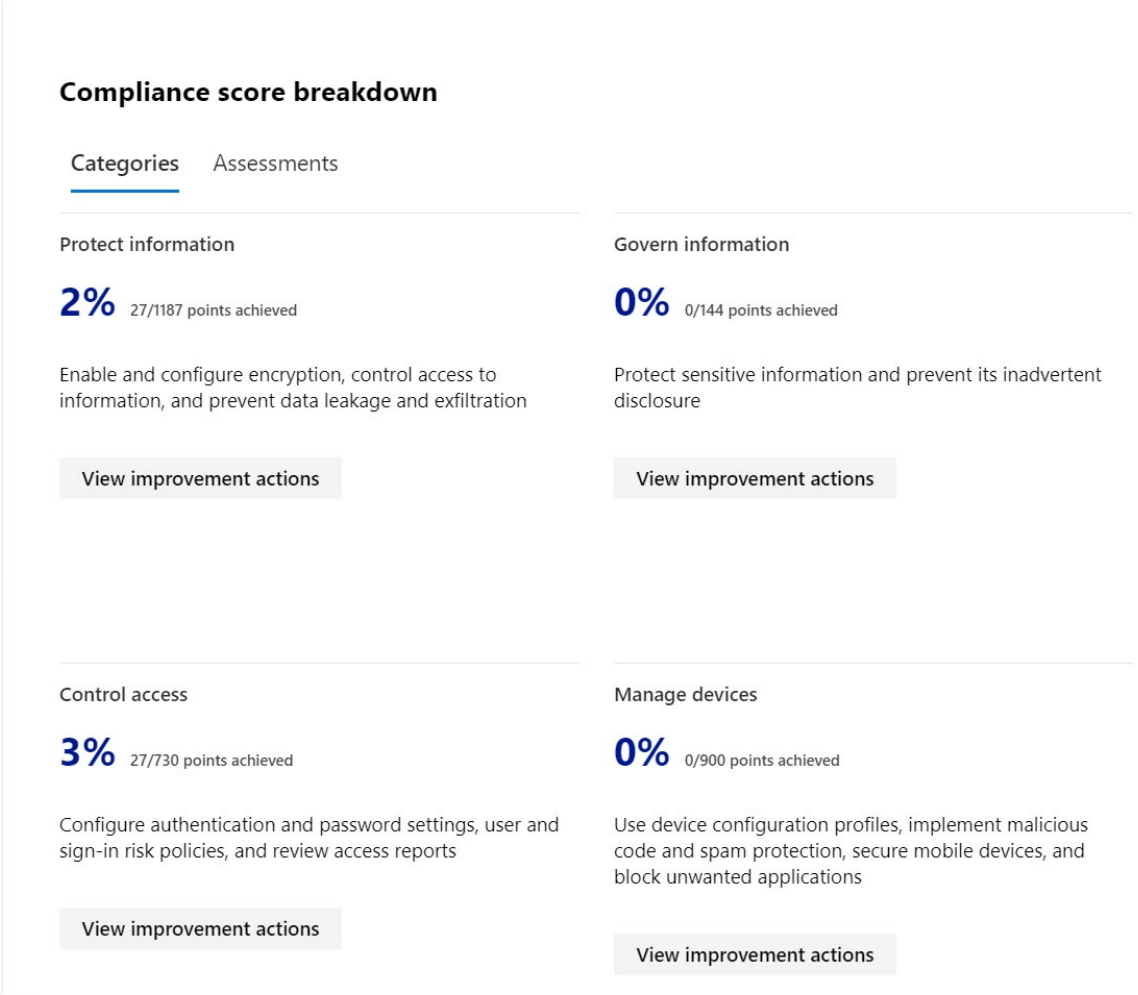
- Translating complicated regulations, standards, company policies, or other control frameworks into a simple language.
- Providing access to a large variety of out-of-the-box assessments and custom assessments to help organizations with their unique compliance needs.
- Mapping regulatory controls against recommended improvement actions.
- Providing step-by-step guidance on how to implement the solutions to meet regulatory requirements.
- Helping admins and users to prioritize actions that will have the highest impact on their organizational compliance by associating a score with each action.

9 https://docs.microsoft.com/microsoft-365/compliance/compliance-manager-setup?view=o365-worldwide#filtering-your-dashboard-view

Describe compliance score

Compliance score measures progress in completing recommended improvement actions within controls. The score can help an organization to understand its current compliance posture. It also helps organizations to prioritize actions based on their potential to reduce risk.

Admins can get a breakdown of the compliance score in the Compliance Manager overview pane:n of the compliance score in the Compliance Manager overview pane:



What is the difference between Compliance Manager and compliance score?

Compliance Manager is an end-to-end solution in Microsoft 365 compliance center to enable admins to manage and track compliance activities. Compliance score is a calculation of the overall compliance posture across the organization. The compliance score is available through Compliance Manager.

Compliance Manager gives admins the capabilities to understand and increase their compliance score, so they can ultimately improve the organization's compliance posture and help it to stay in line with compliance requirements.

How to understand the compliance score

The overall compliance score is calculated using scores that are assigned to actions. Actions come in two types:

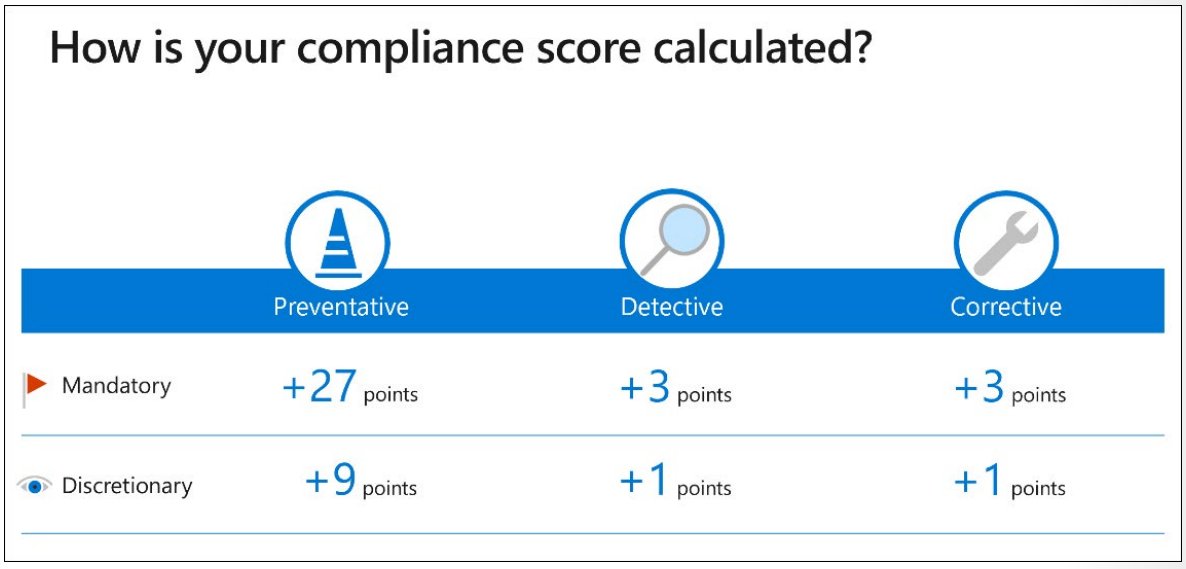
- **Your improved actions**: actions that the organization is expected to manage.
- **Microsoft actions**: actions that Microsoft manages for the organization.

These action types have points assigned to them that count towards the compliance score. Actions can also be considered technical or nontechnical, which also affects how they impact the overall compliance score. Actions are also assigned a score value based on whether they're categorized as mandatory, discretionary, preventative, detective, or corrective:

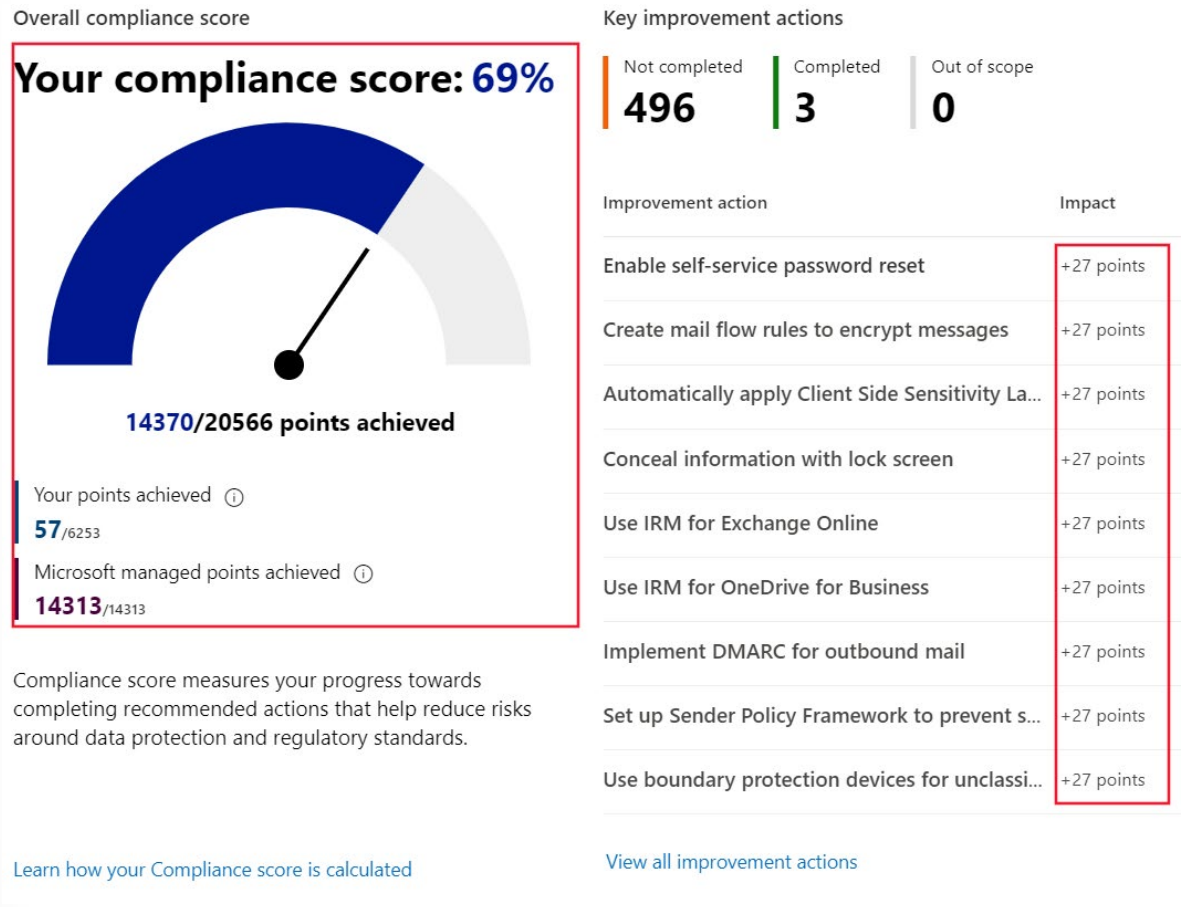
- **Mandatory** – these actions shouldn't be bypassed. For example, creating a policy to set requirements for password length or expiration.
- **Discretionary** – these actions depend on the users understanding and adhering to a policy. For example, a policy where users are required to ensure their devices are locked before they leave them.

The following are subcategories of actions that can be classified as mandatory or discretionary:

- **Preventative** actions are designed to handle specific risks, like using encryption to protect data at rest if there were breaches or attacks.
- **Detective** actions actively monitor systems to identify irregularities that could represent risks, or that can be used to detect breaches or intrusions. Examples of these types of actions are system access audits, or regulatory compliance audits.
- **Corrective** actions help admins to minimize the adverse effects of security incidents, by undertaking corrective measures to reduce their immediate effect or possibly even reverse damage.



Actions that are mandatory and preventative, with 27 points, provide the highest points value towards your compliance score.
Organizations accumulate points for every action completed. And the compliance score is shown as a percentage representing all the actions completed, compared with the ones outstanding:



Interactive guide

In this interactive guide, you'll explore compliance score. Select the link below to get started.

Interactive guide - Explore compliance score.[10]

Knowledge check

Multiple choice

Item 1. When browsing Microsoft compliance documentation in the Service Trust Portal, you have found several documents that are specific to your industry. What is the best way of ensuring you keep up to date with the latest updates?

- ☐ Save the documents to your My Library.
- ☐ Print each document so you can easily refer to them.
- ☐ Download each document.

10 https://edxinteractivepage.blob.core.windows.net/edxpages/Security%20fundamentals/LP04M02%20-%20Explore%20Compliance%20Score/index.html?azure-portal=true

Multiple choice

Item 2. A new admin has joined the team and needs to be able to access the Microsoft 365 Compliance Center. Which of the following roles could the admin use to access the Compliance Center?

- ☐ Compliance Administrator role.
- ☐ Helpdesk Administrator role.
- ☐ User Administrator role.

Multiple choice

Item 3. Your new colleagues on the admin team are unfamiliar with the concept of shared controls in Compliance Manager. How would the concept of shared controls be explained?

- ☐ Controls that both external regulators and Microsoft share responsibility for implementing.
- ☐ Controls that both your organization and external regulators share responsibility for implementing.
- ☐ Controls that both your organization and Microsoft share responsibility for implementing.

Multiple choice

Item 4. A customer has requested a presentation on how the Microsoft 365 Compliance Center can help improve their organization's compliance posture. The presentation will need to cover Compliance Manager and compliance score. What is the difference between Compliance Manager and compliance score?

- ☐ Compliance Manager is an end-to-end solution in Microsoft 365 Compliance Center to enable admins to manage and track compliance activities. Compliance score is a calculation of the overall compliance posture across the organization.
- ☐ Compliance Manager is an end-to-end solution in Microsoft 365 Compliance Center to enable admins to manage and track compliance activities. Compliance score is a score the organization receives from regulators for successful compliance.
- ☐ Compliance Manager is the regulator who will manage your compliance activities. Compliance score is a calculation of the overall compliance posture across the organization.

Summary and resources

In this lesson you learned about the various tools provided by Microsoft to manage compliance for your organization. You explored how compliance center and Compliance Manager can help organizations to manage compliance.

Without these tools, organizations couldn't manage compliance, and they would be at risk of not meeting required legal and regulatory standards. With these tools, they can stay in line with compliance requirements.

Now that you've completed this lesson, you should be able to:

- Find compliance documentation.
- Describe Microsoft's privacy principles.
- Explore the Microsoft 365 compliance center.
- Describe the benefits of Compliance Manager.

Learn more

- **Azure compliance documentation**[11]
- **Get started with the Microsoft Service Trust Portal**[12]
- **Service Trust Portal**[13]
- **Microsoft Trust Center**[14]
- **Privacy at Microsoft**[15]
- **Microsoft 365 compliance center**[16]
- **Microsoft Compliance Manager**[17]
- **Compliance score calculation**[18]
- **Compliance Manager frequently asked questions**[19]

11 https://docs.microsoft.com/azure/compliance/
12 https://docs.microsoft.com/microsoft-365/compliance/get-started-with-service-trust-portal
13 https://servicetrust.microsoft.com/
14 https://www.microsoft.com/trust-center
15 https://privacy.microsoft.com/
16 https://docs.microsoft.com/microsoft-365/compliance/microsoft-365-compliance-center?view=o365-worldwide
17 https://docs.microsoft.com/microsoft-365/compliance/compliance-manager
18 https://docs.microsoft.com/microsoft-365/compliance/compliance-score-calculation?view=o365-worldwide
19 https://docs.microsoft.com/microsoft-365/compliance/compliance-score-faq?view=o365-worldwide#what-is-the-difference-between-compliance-score-and-compliance-manager

Describe the information protection and governance capabilities of Microsoft 365

Introduction

Organizations need to protect all sorts of information, including financial and personal information. This must be done to ensure customers, employees, and the organization are protected from risks. The organization needs to stay in line with compliance standards wherever it operates.

Microsoft provides solutions that can help organizations to implement information protection and governance.

In this lesson, you'll learn about how Microsoft solutions and capabilities like data classification, records management, and data loss prevention, can help you implement information protection and governance.

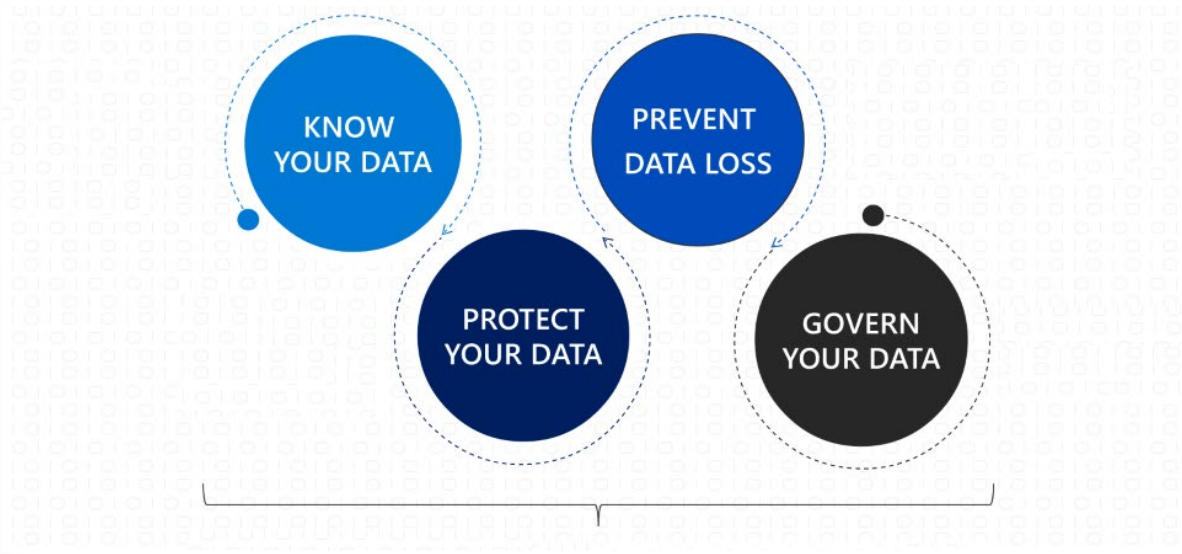
After completing this lesson, you'll be able to:

- Describe data classification capabilities.
- Describe records management.
- Describe data loss prevention.

Know your data, protect your data, and govern your data

Microsoft Information Protection discovers, classifies, and protects sensitive and business-critical content throughout its lifecycle across your organization. It provides the tools to know your data, protect your data, and prevent data loss.

Microsoft Information Governance manages your content lifecycle using solutions to import, store, and classify business-critical data so you can keep what you need and delete what you don't. It gives organizations the capabilities to govern their data, for compliance or regulatory requirements.
Microsoft Information Protection and Microsoft Information Governance work together to classify, protect, and keep your data where it lives, and wherever it goes.



- **Know your data**: Organizations can understand their data landscape and identify important data across on-premises, cloud, and hybrid environments. Capabilities and tools such as trainable classifiers, activity explorer, and content explorer allow organizations to know their data.
- **Protect your data**: Organizations can apply flexible protection actions including encryption, access restrictions, and visual markings.
- **Prevent data loss**: Organizations can detect risky behavior and prevent accidental oversharing of sensitive information. Capabilities such as data loss prevention policies and endpoint data loss prevention enable organizations to avoid data loss.
- **Govern your data**: Organizations can automatically keep, delete, and store data and records in a compliant manner. Capabilities like retention policies, retention labels, and records management enable organizations to govern their data.

Information and capabilities related to each of these areas are described throughout this lesson.

Describe data classification capabilities of compliance center

Organizations need to know their data to identify important information across the estate and ensure that data is handled in line with compliance requirements. Admins can enable their organization to know its data through data classification capabilities and tools in the Microsoft 365 compliance center, such as sensitive information types, trainable classifiers, content explorer, and activity explorer.

Sensitive information types

With Microsoft 365 compliance center, admins can identify and protect sensitive information types. Sensitive information types have set patterns that can be used to identify them. For example, an identification number in a region/country may be based on a specific pattern, like this:

123-456-789-ABC

Microsoft 365 includes many built-in sensitive information types based on patterns that are defined by a regular expression (regex) or a function.

Examples include:

- Credit card numbers
- Passport or identification numbers
- Bank account numbers
- Health service numbers

Refer to **Sensitive information type entity definitions**[20] for a listing of available built-in sensitive information types.

Data classification in Microsoft 365 also supports the ability to create custom sensitive information types to address organization-specific requirements. For example, an organization may need to create sensitive information types to represent employee IDs or project numbers.

Trainable classifiers

Trainable classifiers use artificial intelligence and machine learning to intelligently classify your data. They're most useful classifying data unique to an organization like specific kinds of contracts, invoices, or customer records. This method of classification is more about training a classifier to identify an item based on what the item is, not by elements that are in the item (pattern matching).
Two types of classifier are available:

- **Pre-trained classifiers** - Microsoft has created and pretrained many classifiers that you can start using without training them. These classifiers will appear with the status of **Ready to use**. Microsoft 365 comes with five pretrained classifiers that detect and classify things like resumes, source code, harassment, profanity, and threat (relates to committing violence or doing physical harm).
- **Custom trainable classifiers** - Microsoft supports the ability to create and train custom classifiers. They're most useful when classifying data unique to an organization, like specific kinds of contracts, invoices, or customer records.

To get a custom trainable classifier to accurately identify an item as being in a particular category of content, it must first be presented with many samples of the type of content in the category. This feeding of positive samples is known as seeding and is used to create a prediction model for the classifier.

The model gets tested to determine if the classifier can correctly distinguish between items that match the category and items that don't. The result of each prediction is manually verified, which serves as input to improve the accuracy of the prediction model.

After the accuracy score of the model has stabilized, the classifier can be published.
Trainable classifiers can then sort through items in locations like SharePoint Online, Exchange, and OneDrive, and classify the content.

NOTE: At this time, classifiers only work with items that are in English and that are not encrypted.

Understand and explore the data

Data classification can involve large numbers of documents and emails. To help administrators to easily derive insights and understanding, the overview section of the data classification pane in compliance center provides many details at a glance, including:

- The number of items classified as sensitive information and which classifications they are.
- Details on the locations of data based on sensitivity.

20 https://docs.microsoft.com/microsoft-365/compliance/sensitive-information-type-entity-definitions?view=o365-worldwide

- Summary of actions that users are taking on sensitive content across the organization.

Administrators can also use the content and activity explorers to gain a deeper understanding and guide their actions.

What is the content explorer?

The content explorer is available as a tab in the data classification pane of compliance center. It enables administrators to gain visibility into the content that has been summarized in the overview pane. Access to content explorer is highly restricted because it makes it possible to read the contents of scanned files. There are two roles that grant access to content explorer:

- Content explorer list viewer.
- Content explorer content viewer.

Anyone who wants to access content explorer must have an account in one or both of the role groups.

With content explorer, administrators get a current snapshot of individual items that have been classified across the organization. It enables administrators to further drill down into items by allowing them to access and review the scanned source content that's stored in different kinds of locations, such as Exchange, SharePoint, and OneDrive.

What is the activity explorer?

Activity explorer provides visibility into what content has been discovered and labeled, and where that content is. It makes it possible to monitor what's being done with labeled content across the organization. Admins gain visibility into document-level activities like label changes and label downgrades (such as when someone changes a label from confidential to public).

Admins use the filters to see all the details for a specific label, including file types, users, and activities. Activity explorer helps you understand what's being done with labeled content over time. Admins use activity explorer to evaluate if controls already in place are effective.

Here are a few of the activity types that can be analyzed:

- File copied to removable media
- File copied to network share
- Label applied
- Label changed

Admins can use more than 30 filters for data including:

- Date range
- Activity type
- Location
- User
- Sensitivity label
- Retention label

The value of understanding what actions are being taken with sensitive content is that admins can see if the controls that they've already put in place, such as **data loss prevention policies**[21], are effective or

21 https://docs.microsoft.com/microsoft-365/compliance/data-loss-prevention-policies?view=o365-worldwide

not. For example, if it's discovered that a large number of items labeled *Highly Confidential* have suddenly been downgraded to *Public*, admins can update policies and act to restrict undesired behavior as a response.

Explore Data classification in the compliance center

Watch **data classification**[22] for information on the various data classification capabilities available in the compliance center.

Describe sensitivity labels

Organizations must protect their data, to safeguard customers and business operations, and to meet compliance standards. Admins can enable their organization to protect its data, through capabilities and tools such as sensitivity labels and policies in Microsoft 365 compliance center.

Sensitivity labels

Sensitivity labels, available as part of information protection in the Microsoft 365 compliance center, enable the labeling and protection of content, without affecting productivity and collaboration. With sensitivity labels, organizations can decide on labels to apply to content such as emails and documents, much like different stamps are applied to physical documents.

Labels are:

- **Customizable**: Admins can create different categories specific to the organization, such as Personal, Public, Confidential, and Highly Confidential.
- **Clear text**: Because each label is stored in clear text in the content's metadata, third-party apps and services can read it and then apply their own protective actions, if necessary.
- **Persistent**. After you apply a sensitivity label to content, the label is stored in the metadata of that email or document. The label then moves with the content, including the protection settings, and this data becomes the basis for applying and enforcing policies.

Each item that supports sensitivity labels can only have one label applied to it, at any given time.

Sensitivity labels can be used to:

- **Encrypt** email only or both email and documents. When a document or email is encrypted, access to the content is restricted, so that:
  - It can be decrypted only by users authorized by the label's encryption settings.
  - Remains encrypted no matter where it stays, inside or outside your organization, even if the file is renamed.
  - It's encrypted both at rest (for example, in a OneDrive account) and in transit (for example, an email message as it traverses the internet).
- **Mark the content** when Office apps are used. Marking the content includes adding watermarks, headers, or footers. Headers or footers can be added to emails or documents that have the label applied. Watermarks can be applied to documents but not to email.
- **Apply the label automatically** in Office apps or recommend a label. Admins choose the types of sensitive information to be labeled. The label can be applied automatically or configured to prompt users to apply the recommended label.

22 https://www.microsoft.com/videoplayer/embed/RE4vx8x

- **Protect content in containers such as sites and groups** when this capability is enabled. This label configuration doesn't result in documents being automatically labeled. Instead, the label settings protect content by controlling access to the container where documents are stored.
- **Extend sensitivity labels to third-party apps and services**. Using the Microsoft Information Protection SDK, third-party apps can read sensitivity labels and apply protection settings.
- **Classify content without using any protection settings**. A classification can be assigned to content (just like a sticker) that persists and roams with the content as it's used and shared. The classification can be used to generate usage reports and view activity data for sensitive content.

Label policies

After sensitivity labels are created, they need to be published to make them available to people and services in the organization. Sensitivity labels are published to users or groups through label policies. Sensitivity labels will then appear in Office apps for those users and groups. The sensitivity labels can be applied to documents and emails.
Label policies enable admins to:

- **Choose the users and groups that can see labels**. Labels can be published to specific users, distribution groups, Microsoft 365 groups in Azure Active Directory, and more.
- **Apply a default label** to all new emails and documents that the specified users and groups create. Users can always change the default label if they believe the document or email has been mislabeled.
- **Require justifications for label changes**. If a user wants to remove a label or replace it, admins can require the user to provide a valid justification to complete the action. The user will be prompted to provide an explanation for why the label should be changed.
- **Require users to apply a label (mandatory labeling)**. It ensures a label is applied before users can save their documents, send emails, or create new sites or groups.
- **Link users to custom help pages**. It helps users to understand what the different labels mean and how they should be used.

Once a sensitivity label is applied to an email or document, any configured protection settings for that label are enforced on the content. For example, by choosing encryption settings for a sensitivity label, admins can protect content so that:

- Only users within the organization can open a confidential document or email.
- Only users in a specific department can edit and print a document or email, while all other users in the organization can only read it.
- Users can't forward or copy information from an email.
- Users can't open a document after a specified date.

Admins can also enable users to label and protect their files using the Windows File Explorer (to label extra file types, and more files simultaneously), by installing the Azure Information Protection unified labeling client on Windows devices.

Describe Data Loss Prevention

Data loss can harm an organization’s customers, business processes, and the organization itself. Organizations need to prevent data loss by detecting risky behavior and preventing sensitive information from being shared inappropriately. Admins can use data loss prevention policies, available in Microsoft 365 compliance center, to help their organization.

Data loss prevention (DLP) is a way to protect sensitive information and prevent its inadvertent disclosure. With DLP policies, admins can:

- **Identify, monitor, and automatically protect** sensitive information across Microsoft 365, including:
  - OneDrive for Business
  - SharePoint Online
  - Microsoft Teams
  - Exchange Online
- **Help users learn how compliance works** without interrupting their workflow. For example, if a user tries to share a document containing sensitive information, a DLP policy can send them an email notification and show them a policy tip.
- **View DLP reports** showing content that matches the organization's DLP policies. To assess how the organization is following a DLP policy, admins can see how many matches each policy has over time.

DLP policies protect content through the enforcement of rules that consist of:

- **Conditions** that the content must match before the rule is enforced.
- **Actions** that the admin wants the rule to take automatically when content that matches the conditions has been found.
- **Locations** where the policy will be applied, such as Exchange, SharePoint, OneDrive, and more.

For example, an admin can configure a DLP policy that helps detect information that's subject to a compliance regulation like the Health Insurance Portability and Accountability Act (HIPAA) across all SharePoint sites and OneDrive for Business. The admin can block the relevant documents from being shared inappropriately.

DLP policies protect information by identifying and automatically protecting sensitive data.
Here's some scenarios where DLP policies can help:

- Identify any document containing a credit card number stored in users' OneDrive for Business accounts.
- Automatically block an email containing employee personal information from being sent outside the organization.

A policy can contain one or more rules, and each rule consists of conditions and actions at a minimum. For each rule, when the conditions are met, the actions are taken automatically. Rules can be grouped into one policy, to help simplify management and reporting. The diagram below shows how multiple rules, each with their own conditions and actions, are grouped into a single policy:

The rules inside the policy are prioritized in how they're implemented. For example, in the above diagram, rule one will be prioritized before rule two, and so on.

What is endpoint data loss prevention?

Endpoint data loss prevention is how the protection and activity monitoring capabilities of DLP for sensitive content can be extended to Windows 10 devices. Admins can choose to target Windows 10 when creating a DLP policy (after onboarding the devices to Microsoft 365 compliance solutions). Endpoint DLP enables admins to audit and manage activities that users complete on sensitive content, including:

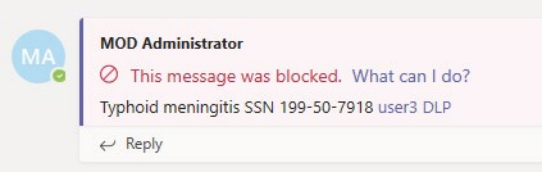
- Creating an item
- Renaming an item
- Copying items to removable media
- Copying items to network shares
- Printing documents
- Accessing items using unallowed apps and browsers

In the activity explorer, you can view information about what users are doing with sensitive content:

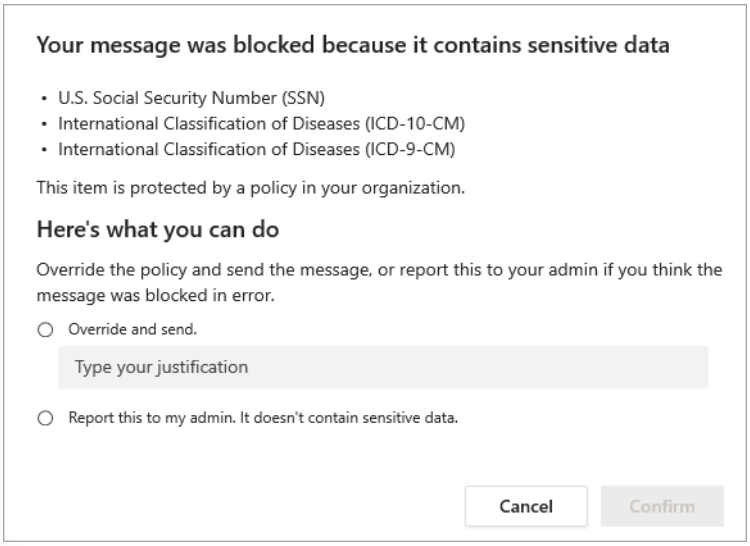
Admins use this information to enforce protective actions for content through controls and policies.

Data loss prevention in Microsoft Teams

Data loss prevention capabilities have been extended to Microsoft Teams chat and channel messages, including messages in private channels. With DLP, administrators can now define policies that prevent users from sharing sensitive information in a Teams chat session or channel, whether it's in a message, or a file. Just like with Exchange, Outlook, SharePoint, and OneDrive for Business, administrators can use DLP policy tips that will be displayed to the user to show them why a policy has been triggered. For example, the screenshot below shows a policy tip on a chat message that was blocked because the user attempted to share a U.S. Social Security Number:



The user can then find out more information about why their message was blocked by selecting the "What can I do?" link, and take appropriate action:



With DLP policies, Microsoft Teams can help users across organizations to collaborate securely and in a way that's in line with compliance requirements.

Describe Retention Polices and Retention Labels

Retention labels and policies help organizations to manage and govern information by ensuring content is kept only for a required time, and then permanently deleted. Applying retention labels and assigning retention policies helps organizations:

- **Comply proactively with industry regulations and internal policies** that require content to be kept for a minimum time.
- **Reduce risk when there's litigation or a security breach** by permanently deleting old content that the organization is no longer required to keep.
- **Ensure users work only with content that's current and relevant to them**.

When content has retention settings assigned, it stays in its original location. People can continue to work with their documents or mail as if nothing's changed. But if they edit or delete content that's included in the retention policy, a copy is automatically kept in a secure location. The secure locations and the retained content aren't visible to most people. In most cases, people don't even need to know that their content is subject to retention settings.

Retention settings work with the following different workloads:

- **SharePoint and OneDrive**[23]
- **Microsoft Teams**[24]
- **Yammer**[25]
- **Exchange**[26]

23 https://docs.microsoft.com/microsoft-365/compliance/retention-policies-sharepoint?view=o365-worldwide
24 https://docs.microsoft.com/microsoft-365/compliance/retention-policies-teams?view=o365-worldwide
25 https://docs.microsoft.com/microsoft-365/compliance/retention-policies-yammer?view=o365-worldwide
26 https://docs.microsoft.com/microsoft-365/compliance/retention-policies-exchange?view=o365-worldwide

When using retention policies and retention labels to assign retention settings to content, there are some points to understand about each. Listed below are just a few of the key points. For a more complete list visit **Compare capabilities for retention policies and retention labels**[27].

Retention policies

- Retention policies are used to assign the same retention settings to content at a site level or mailbox level.
- A single policy can be applied to multiple locations, or to specific locations or users.
- Items inherit the retention settings from their container specified in the retention policy. If a policy is configured to keep content, and an item is then moved outside that container, a copy of the item is kept in the workload's secured location. However, the retention settings don't travel with the content in its new location.

Retention labels

- Retention labels are used to assign retention settings at an item level, such as a folder, document, or email.
- An email or document can have only a single retention label assigned to it at a time.
- Retention settings from retention labels travel with the content if it's moved to a different location within your Microsoft 365 tenant.
- Admins can enable users in the organization to apply a retention label manually.
- A retention label can be applied automatically if it matches defined conditions.
- A default label can be applied for SharePoint documents.
- Retention labels support disposition review to review the content before it's permanently deleted.

Consider the following scenarios. If all documents in a SharePoint site should be kept for five years, it's more efficient to do with a retention policy than apply the same retention label to all documents in that site.

However, if some documents in that site should be kept for five years and others for 10 years, you'd need to apply a policy to the SharePoint site with a retention period of five years. You'd then apply a retention label to the individual item with a retention setting of 10 years.

Describe Records Management

Organizations of all types require a management solution to manage regulatory, legal, and business-critical records across their corporate data. Records management in Microsoft 365 helps an organization look after their legal obligations. It also helps to demonstrate compliance with regulations, and increases efficiency with regular disposition of items that are no longer required to be kept, no longer of value, or no longer required for business purposes. It provides the following capabilities:

- Labeling content as a record.
- Migrating and managing retention plans with file plan manager.
- Establishing retention and deletion policies within the record label.
- Triggering event-based retention.
- Reviewing and validating disposition.

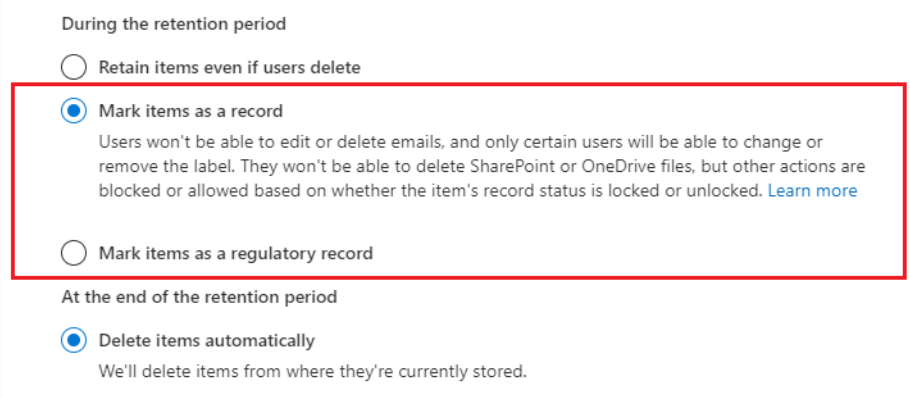
27 https://docs.microsoft.com/microsoft-365/compliance/retention?view=o365-worldwide#compare-capabilities-for-retention-policies-and-retention-labels

- Proof of records deletion.
- Exporting information about disposed items.
- Setting specific permissions for record manager functions in the organization.

When content is labeled as a record, the following happens:

- Restrictions are put in place to block certain activities.
- Activities are logged.
- Proof of disposition is kept at the end of the retention period.

To enable items to be marked as records, an administrator sets up retention labels.



Items such as documents and emails can then be marked as records based on those retention labels. Items might be marked as records, but they can also be shown as regulatory records. Regulatory records provide other controls and restrictions such as:

- A regulatory label can't be removed when an item has been marked as a regulatory record.
- The retention periods can't be made shorter after the label has been applied.

For more information on comparing, use the **Compare restrictions for what actions are allowed or blocked section**[28] of the documentation.

The most important difference is that if content has been marked as a regulatory record, nobody, not even a global administrator, can remove the label. Marking an item as a regulatory record can have irreversible consequences, and should only be used when necessary. As a result, this option isn't available by default, and has to be enabled by the administrator using PowerShell.

Common use cases for records management

Microsoft 365's records management capabilities are flexible. There are different ways in which records management can be used across an organization, including:

- Enabling administrators and users to manually apply retention and deletion actions for documents and emails.
- Automatically applying retention and deletion actions to documents and emails.
- Enabling site admins to set default retain and delete actions for all content in a SharePoint library, folder, or document set.

28 https://docs.microsoft.com/microsoft-365/compliance/records-management?view=o365-worldwide#compare-restrictions-for-what-actions-are-allowed-or-blocked

- Enabling users to automatically apply retain and delete actions to emails by using Outlook rules.

To ensure records management is used correctly across the organization, administrators can work with content creators to put together training materials. Documentation should explain how to apply labels to drive usage, and ensure a consistent understanding.

Knowledge check

Multiple choice

Item 1. Which part of the concept of know your data, protect your data, and prevent data loss addresses the need for organizations to automatically retain, delete, store data and records in a compliant manner?

- ☐ Know your data.
- ☐ Prevent data loss.
- ☐ Govern your data.

Multiple choice

Item 2. As part of a new data loss prevention policy, the compliance admin needs to be able to identify important information such as credit card numbers, across the organization's data. How can the admin address this requirement?

- ☐ Use activity explorer.
- ☐ Use sensitivity labels.
- ☐ Use sensitive information types.

Multiple choice

Item 3. Within the organization, some emails are confidential and should be encrypted so that only authorized users can read them. How can this requirement be implemented?

- ☐ Use the content explorer.
- ☐ Use sensitivity labels.
- ☐ Use Records Management.

Multiple choice

Item 4. Your organization uses Microsoft Teams to collaborate on all projects. The compliance admin wants to prevent users from accidentally sharing sensitive information in a Microsoft Teams chat session. What capability can address this requirement?

- ☐ Use data loss prevention policies.
- ☐ Use Records Management capabilities.
- ☐ Use retention policies.

Multiple choice

Item 5. Due to a certain regulation, your organization must now keep hold of all documents in a specific SharePoint site that contains customer information for five years. How can this requirement be implemented?

- ☐ Use sensitivity labels.
- ☐ Use the content explorer.
- ☐ Use retention policies.

Summary and resources

You've explored how Microsoft 365 capabilities like data classification, records management, and data loss prevention can help provide information protection and information governance across an organization.

Without these capabilities, an organization's information could be at risk, and it might not be compliant with legal and regulatory standards. However, by using these capabilities, organizations can provide information protection and governance to help avoid the risk of noncompliance.

Now that you've completed this lesson, you should be able to:

- Describe data classification capabilities.
- Describe records management.
- Describe data loss prevention.

Learn more

- **Know your data - data classification overview**[29]
- **Get started with content explorer**[30]
- **Learn about sensitivity labels**[31]
- **Get started with activity explorer**[32]
- **Learn about retention policies and retention labels**[33]
- **Microsoft Information Governance in Microsoft 365**[34]
- **Learn about records management in Microsoft 365**[35]

29 https://docs.microsoft.com/microsoft-365/compliance/data-classification-overview?view=o365-worldwide
30 https://docs.microsoft.com/microsoft-365/compliance/data-classification-content-explorer?view=o365-worldwide
31 https://docs.microsoft.com//microsoft-365/compliance/sensitivity-labels?view=o365-worldwide
32 https://docs.microsoft.com/microsoft-365/compliance/data-classification-activity-explorer?view=o365-worldwide
33 https://docs.microsoft.com/microsoft-365/compliance/retention?view=o365-worldwide
34 https://docs.microsoft.com/microsoft-365/compliance/manage-information-governance?view=o365-worldwide
35 https://docs.microsoft.com/microsoft-365/compliance/records-management?view=o365-worldwide

Describe the insider risk capabilities in Microsoft 365

Introduction

Organizations understand that risks can come from insiders, like contractors, or even employees. There's always a risk that people might share information with competitors after leaving the company. Organizations need to ensure that they're protected from these kinds of risks.

In this lesson, you'll learn how Microsoft 365 capabilities like insider risk management, communication compliance, information barriers, privileged access management, and Customer Lockbox can help you protect your organization.

After completing this lesson, you'll be able to:

- Describe how Microsoft 365 can help organizations identify insider risks and take appropriate action.
- Describe how Microsoft 365 helps organizations identify, investigate, and remediate malicious and inadvertent activities in your organization.

Describe the Insider Risk Management solution

Insider risk management is a solution in Microsoft 365 that helps minimize internal risks by enabling an organization to detect, investigate, and act on risky and malicious activities. Insider risk management is available in Microsoft 365 compliance center.

Managing and minimizing risk in an organization starts with understanding the types of risks found in the modern workplace. Some risks are driven by external events and factors, and are outside an organization's direct control. Other risks are driven by internal events and employee activities that can be eliminated and avoided. Some examples are risks from illegal, inappropriate, unauthorized, or unethical behavior and actions by employees and managers. These behaviors can lead to a broad range of internal risks from employees:

- Leaks of sensitive data and data spillage
- Confidentiality violations
- Intellectual property (IP) theft
- Fraud
- Insider trading
- Regulatory compliance violations

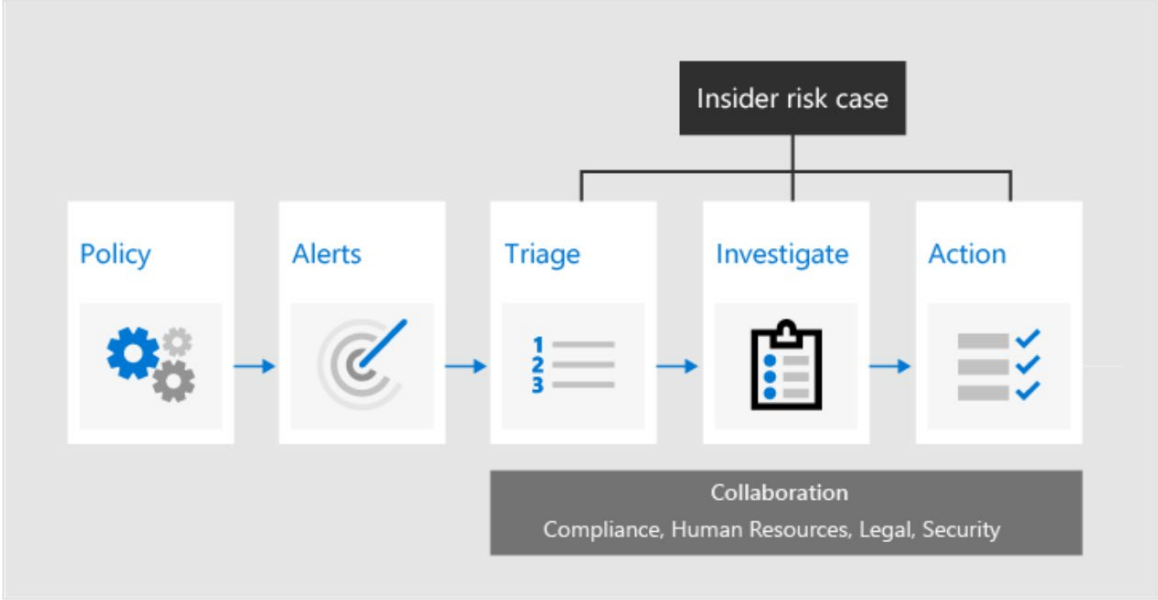
Insider risk management is centered around the following principles:

- **Transparency**: Balance user privacy versus organization risk with privacy-by-design architecture.
- **Configurable**: Configurable policies based on industry, geographical, and business groups.
- **Integrated**: Integrated workflow across Microsoft 365 compliance solutions.
- **Actionable**: Provides insights to enable user notifications, data investigations, and user investigations.

Insider risk management workflow

Insider risk management helps organizations to identify, investigate, and address internal risks. With focused policy templates, comprehensive activity signaling across Microsoft 365, and a flexible workflow,

organizations can take advantage of actionable insights to help identify and resolve risky behavior quickly.
Identifying and resolving internal risk activities and compliance issues with insider risk management in Microsoft 365 is achieved using the following workflow:



- **Policies** - Insider risk management policies are created using predefined templates and policy conditions that define what risk indicators are examined in Microsoft 365 feature areas. These conditions include how indicators are used for alerts, what users are included in the policy, which services are prioritized, and the monitoring time period.
- **Alerts** - Alerts are automatically generated by risk indicators that match policy conditions and are displayed in the **Alerts dashboard**. This dashboard enables a quick view of all alerts needing review, open alerts over time, and alert statistics for the organization.
- **Triage** - New activities that need investigation automatically generate alerts that are assigned a *Needs review* status. Reviewers in the organization can quickly identify these alerts and scroll through each to evaluate and triage. Alerts are resolved by opening a new case, assigning the alert to an existing case, or dismissing the alert. As part of the triage process, reviewers can view alert details for the policy match, view user activity associated with the match, see the severity of the alert, and review user profile information.
- **Investigate** - Cases are created for alerts that require deeper review and investigation of the details and circumstances around the policy match. The **Case dashboard** provides an all-up view of all active cases, open cases over time, and case statistics for the organization. Selecting a case on the dashboard opens it for investigation and review. This area is where risk activities, policy conditions, alerts details, and user details are synthesized into an integrated view for reviewers.
- **Action** - After cases are investigated, reviewers can quickly act to resolve the case or collaborate with other risk stakeholders in the organization.

    - Actions can be as simple as sending a notification when employees accidentally or inadvertently violate policy conditions.

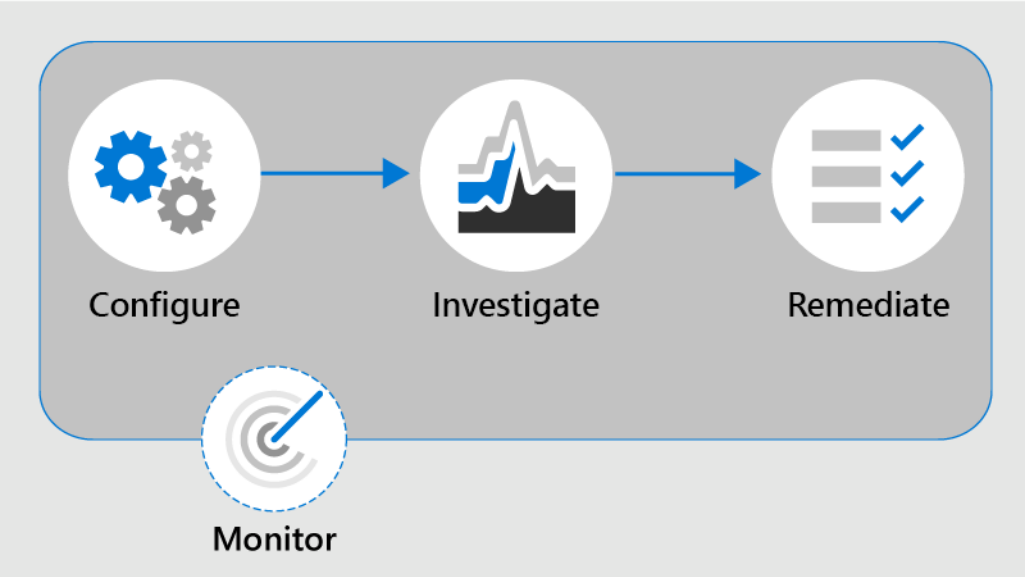
- In more serious cases, reviewers may need to share the insider risk management case information with other reviewers in the organization. Escalating a case for investigation makes it possible to transfer data and management of the case to Advanced eDiscovery in Microsoft 365.

Insider risk management can help you detect, investigate, and take action to mitigate internal risks in your organization in several common scenarios. These scenarios include data theft by employees, the intentional, or unintentional leak of confidential information, offensive behavior, and more.

Describe communication compliance

Communication compliance in Microsoft 365 compliance center helps minimize communication risks by enabling organizations to detect, capture, and take remediation actions for inappropriate messages. Predefined and custom policies in communication compliance make it possible to scan internal and external communications for policy matches so they can be examined by chosen reviewers.

Identifying and resolving compliance issues with communication compliance in Microsoft 365 uses the following workflow:



- **Configure** – in this step, admins identify compliance requirements and configure applicable communication compliance policies.
- **Investigate** – admins look deeper into the issues detected when matching your communication compliance policies. Tools and steps that help include alerts, issue management to help remediation, document reviews, reviewing user history, and filters.
- **Remediate** – remediate communications compliance issues. Options include resolving an alert, tagging a message, notifying the user, escalating to another reviewer, marking an alert as a false positive, removing a message in Teams, and escalating for investigation.
- **Monitor** – Keeping track and managing compliance issues identified by communication compliance policies spans the entire workflow process. Communication compliance dashboard widgets, export logs, and events recorded in the unified audit logs can be used to continually evaluate and improve your compliance posture.

Communication compliance enables reviewers to investigate scanned emails, and messages across Microsoft Teams, Exchange Online, Yammer, or third-party communications in an organization, taking

appropriate remediation actions to make sure they're compliant with the organization's message standards.

Some important compliance areas where communication compliance policies can assist with reviewing messages include:

- **Corporate policies** - Users have to follow corporate policies like usage and ethical standards in their day-to-day business communications. With communication compliance, admins can scan user communications across the organization for potential concerns of offensive language or harassment.
- **Risk management** - Communication compliance can help admins scan for unauthorized communication about projects that are considered to be confidential, such as acquisitions, earnings disclosures, and more.
- **Regulatory compliance** - Most organizations are expected to follow some regulatory compliance standards during their day-to-day operations. For example, a regulation might require organizations in the finance sector to review communications of its brokers to safeguard against potential insider trading, money laundering, or bribery. Communication compliance enables the organization to scan and report on these types of communications in a way that meets their requirements.

For a walk-through of the communication compliance capability refer to **Communication Compliance: Solution tutorial to identify inappropriate communication and quickly take action**[36].

Communication compliance is a powerful tool, that can help maintain and safeguard your staff, your data and your organization.

Describe information barriers

Microsoft 365 provides organizations with powerful communication and collaboration capabilities. However, an organization might want to restrict communications between some groups to avoid a conflict of interest from occurring in the organization, or to restrict communications between certain people to safeguard internal information. With information barriers, the organization can restrict communications among specific groups of users.

It's important to note that information barriers *only support two-way restrictions*. One-way restrictions, such as marketing, can communicate with day traders but day traders who can't communicate with marketing are *not supported*.

Information barriers are policies that admins can configure to prevent individuals or groups from communicating with each other. When information barrier policies are in place, people who shouldn't communicate with other specific users can't find, select, chat, or call those users. With information barriers, checks are in place to prevent unauthorized communication.

Here are some examples of how information barriers can be applied:

- **Education**: Students in one school can't look up contact details for students of other schools.
- **Legal**: Maintaining confidentiality of data obtained by the lawyer of one client from being accessed by a lawyer for the same firm representing a different client.
- **Professional services**: A group of people in a company is only able to chat with a client or specific customer via federation or guest access during a customer engagement.

Information barriers are supported in solutions like Microsoft Teams, OneDrive for Business, SharePoint Online, and more.

36 https://www.microsoft.com/videoplayer/embed/RE4xlaF

Information barriers in Microsoft Teams

In Microsoft Teams, information barrier policies determine and prevent the following kinds of unauthorized communications:

- Searching for a user
- Adding a member to a team
- Starting a chat session with someone
- Starting a group chat
- Inviting someone to join a meeting
- Sharing a screen
- Placing a call
- Sharing a file with another user
- Access to file through sharing link

If the people involved are included in an information barrier policy to prevent the activity, they cannot continue. Potentially, everyone included in an information barrier policy can be blocked from communicating with others in Microsoft Teams. When people affected by information barrier policies are part of the same team or group chat, they might be removed from those chat sessions and further communication with the group might not be allowed.

To learn more about the user experience with information barriers, visit **information barriers in Microsoft Teams**[37].

Describe privileged access management

Privileged access management allows granular access control over privileged admin tasks in Microsoft 365. It can help protect organizations from breaches that use existing privileged admin accounts with standing access to sensitive data or access to critical configuration settings.

Enabling privileged access management in Microsoft 365 allows organizations to operate with **zero standing access**. This means that any user who needs privileged access, must request permissions for access, and will receive only the level of access they need just when they need it, and with just-enough access to perform the job at hand. Zero standing access provides a layer of protection against standing administrative access vulnerabilities.

Privileged access management requires users to request just-in-time access to complete elevated and privileged tasks through a highly scoped and time-bounded approval workflow, described below:

1. **Configure a privileged access policy** - Configuring an approval policy allows the admin to define the specific approval requirements scoped at individual tasks.
2. **Access request** - Users can request access to elevated or privileged tasks. The privileged access feature sends the request to Microsoft 365 for processing against the configured privilege access policy and records the Activity in the Security & Compliance Center logs.
3. **Access approval** - An approval request is generated, and the pending request notification is emailed to approvers. If approved, the privileged access request is processed as an approval and the task is ready to be completed. If denied, the task is blocked and no access is granted to the requestor. The requestor is notified of the request approval or denial via email message.

37 https://docs.microsoft.com/MicrosoftTeams/information-barriers-in-teams

4. **Access processing** - For an approved request, the task is processed. The approval is checked against the privileged access policy and processed by Microsoft. All activity for the task is logged in the Security & Compliance Center.

For a detailed walk-through, watch **Privileged access management: Tour of scoped, just-in-time controls for granting admin role & task privileges**[38].

Privileged access management (PAM) sounds a lot like Privileged Identity Management (PIM), so what is the difference?

Privileged access management is defined and scoped at the task level, while Azure AD Privileged Identity Management applies protection at the role level with the ability to execute multiple tasks. Azure AD Privileged Identity Management primarily allows managing accesses for AD roles and role groups, while privileged access management in Microsoft 365 applies only at the task level.

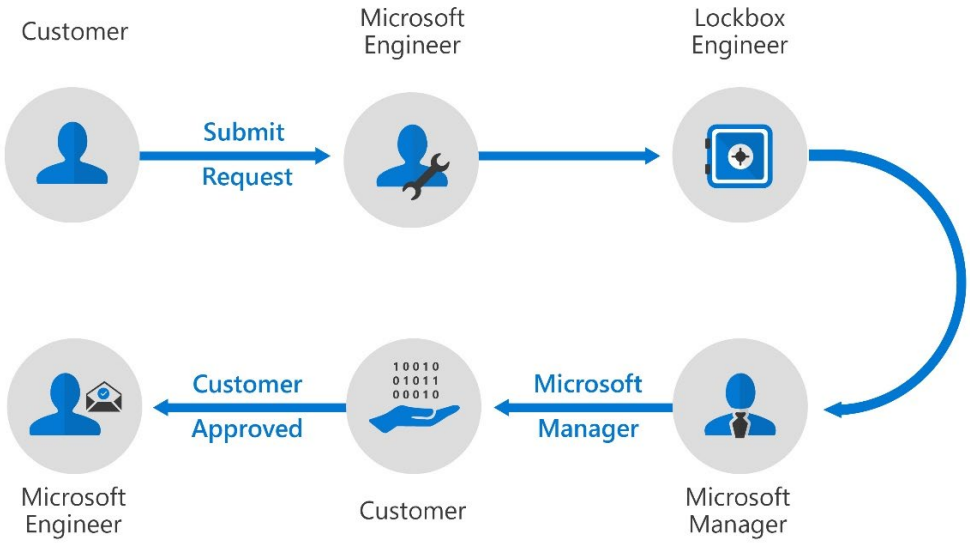
Describe customer lockbox

Occasionally, an organization might need Microsoft engineers help to help troubleshoot and fix reported issues. Usually, issues are fixed through extensive telemetry and debugging tools Microsoft has in place for its services. However, some cases require a Microsoft engineer to access the organization's content to determine the root cause and fix the issue.

Customer Lockbox ensures that Microsoft can't access the content to perform a service operation without explicit approval. Customer Lockbox brings the organization into the approval workflow for requests to access their content.

Customer Lockbox supports requests to access data in Exchange Online, OneDrive for Business, and SharePoint Online.
Here's what the process looks like:

38 https://www.microsoft.com/videoplayer/embed/RE4xqtC



1. Someone at an organization experiences an issue with their Microsoft 365 mailbox, as an example. After the user troubleshoots the issue, but can't fix it, they open a support request with Microsoft Support.
2. A Microsoft support engineer reviews the service request and determines a need to access the organization's tenant to repair the issue in Exchange Online.
3. The Microsoft support engineer logs into the Customer Lockbox request tool and makes a data access request that includes the organization's tenant name, service request number, and the estimated time the engineer needs access to the data.
4. After a Microsoft Support manager approves the request, Customer Lockbox sends the designated approver at the organization an email notification about the pending access request from Microsoft.
5. The approver signs-in to the Microsoft 365 admin center and approves the request. This step also triggers the creation of an audit record available by searching the audit log. If the customer rejects the request or doesn't approve the request within 12 hours, the request expires, and no access is granted to the Microsoft engineer.
6. After the approver from the organization approves the request, the Microsoft engineer receives the approval message, logs into the tenant in Exchange Online, and fixes the customer's issue. Microsoft engineers have the requested duration to fix the issue after which the access is automatically revoked.

Because Customer Lockbox follows a formal approval for access control, a common question is how this capability relates to Privileged Access Management, described in the previous topic, that also requires approval for access control. Customer Lockbox allows a level of access control for organizations *when Microsoft accesses data*. Privileged access management allows granular access control *within an organization* for all Microsoft 365 privileged tasks.

Knowledge check

Multiple choice

Item 1. The compliance admin for the organization wants explain the importance of insider risk management, to the business leaders? What use case would apply?

- ☐ To identify and protect against risks like an employee sharing confidential information.
- ☐ To identify and protect against malicious software across your network, such as ransomware.
- ☐ To identify and protect against devices shutting down at critical moments.

Multiple choice

Item 2. To comply with corporate policies, the compliance admin needs to be able to identify and scan for offensive language across the organization. What solution can the admin implement to address this need?

- ☐ Use Policy Compliance in Microsoft 365.
- ☐ Use Communication Compliance.
- ☐ Use information barriers.

Multiple choice

Item 3. An organization has many departments that collaborate through Microsoft Teams. To comply with business policies, the IT organization needs to make sure that users from one particular department are limited in their access and interactions with other departments. What solution can address this need?

- ☐ Use Communication Compliance.
- ☐ Use Customer Lockbox.
- ☐ Use information barriers.

Multiple choice

Item 4. The compliance team wants to control the use privileged admin accounts with standing access to sensitive data, so that admins receive only the level of access they need, when they need it. How can this requirement be implemented?

- ☐ Use Communication Compliance.
- ☐ Use privileged access management.
- ☐ Use the Audit log.

Multiple choice

Item 5. A customer has identified an issue that requires a Microsoft engineer to access the organization's content, to determine the root cause, and fix the issue. To protect the organization, the engineer shouldn't be able to access content and perform service operations without explicit approval. What capability can address this requirement?

- ☐ Use privileged access management.
- ☐ Use information barriers.
- ☐ Use Customer Lockbox.

Summary and resources

There are various capabilities available from Microsoft 365 to help protect organizations from insider risks.
Without these capabilities, organizations wouldn't be protected from insider risk, which could have serious negative financial and reputational consequences. Instead, organizations can prevent this from happening by protecting themselves from insider risk.

Now that you've completed this lesson, you should be able to:

- Describe how Microsoft 365 can help organizations identify insider risks and take appropriate action.
- Describe how Microsoft 365 helps organizations identify, investigate, and remediate malicious and inadvertent activities.

Learn more

- **Insider risk management in Microsoft 365**[39]
- **Get started with communication compliance**[40]
- **Learn about information barriers in Microsoft 365**[41]
- **Privileged access management**[42]
- **Customer Lockbox in Office 365**[43]

39 https://docs.microsoft.com/microsoft-365/compliance/insider-risk-management?view=o365-worldwide
40 https://docs.microsoft.com/microsoft-365/compliance/communication-compliance-configure?view=o365-worldwide#before-you-begin
41 https://docs.microsoft.com/microsoft-365/compliance/information-barriers?view=o365-worldwide
42 https://docs.microsoft.com/microsoft-365/compliance/privileged-access-management-overview?view=o365-worldwide
43 https://docs.microsoft.com/microsoft-365/compliance/customer-lockbox-requests?view=o365-worldwide

Describe the eDiscovery and audit capabilities of Microsoft 365

Introduction

Organizations may need to identify, collect, and/or audit information for legal, regulatory, or business reasons. With today's volume and variety of data, it’s vital that an organization can do this in an efficient and timely manner. Microsoft 365’s eDiscovery and audit capabilities can help organizations to achieve this goal.

In this module, you’ll learn about the eDiscovery capabilities in Microsoft 365.

After completing this lesson, you'll be able to:

- Describe the purpose of eDiscovery.
- Describe the capabilities of the content search tool.
- Describe the core and advanced eDiscovery workflows.
- Describe the core and advanced auditing capabilities of Microsoft 365.

Describe the purpose of eDiscovery

Sometimes a company may find themselves involved in litigation and they need to find electronic information to be used as evidence.

Electronic discovery or eDiscovery tools, can be used to search for content in Exchange Online mailboxes, Microsoft 365 Groups, Microsoft Teams, SharePoint Online and OneDrive for Business sites, Skype for Business conversations, and Yammer teams. You can search across mailboxes and sites in a single eDiscovery search by using the Content Search tool. And you can use Core eDiscovery cases to identify, hold, and export content found in mailboxes and sites.

If your organization has an Office 365 E5 or Microsoft 365 E5 subscription (or related E5 add-on subscriptions), you can further manage custodians and analyze content by using the Advanced eDiscovery solution in Microsoft 365.
Microsoft 365 provides the following eDiscovery tools:

- Content Search
- Core eDiscovery
- Advanced eDiscovery

Each of these tools is described in the subsequent topics.

Describe the capabilities of the content search tool

The Content Search eDiscovery tool, accessible from the compliance center in Office 365 or Microsoft 365, enables search for in-place items such as email, documents, and instant messaging conversations in your organization. Search for items is supported in the following services:

- Exchange Online mailboxes and public folders
- SharePoint Online sites and OneDrive for Business accounts
- Skype for Business conversations

- Microsoft Teams
- Microsoft 365 Groups
- Yammer Groups

To have access to the content search page to run searches and preview and export results, an administrator, compliance officer, or eDiscovery manager must be a member of the **eDiscovery Manager role** group in the Security and Compliance Center. For more information, visit **Assign eDiscovery permissions**[44].

Run a search

To start using the Content Search tool, you must choose content locations to search and configure a keyword query to find specific items. Or the user can just leave the query blank and return all items in the target locations.
Examples of some of the capabilities for running a search include:

- **Build search queries and use conditions** to narrow your search.
- **Configure search permissions filtering** so that an eDiscovery manager can only search for a subset of mailboxes or sites in your organization.
- **Run an ID list search** to search for specific mailbox email messages and other mailbox items using a list of Exchange IDs.
- **Search for Teams chat data** across on-premises users.
- **View keyword statistics** for the results of a search and then refine the query if necessary.
- **Search for third-party data** that your organization has imported to Microsoft 365.
- **Preserve Bcc recipients** to follow regulatory compliance and eDiscovery requirements that may require organizations to preserve mailbox content, including the ability to search for and reproduce details about all recipients of a message, not just those on the “to” and "cc" list.

Complete actions on content

After you run a search and refine it as necessary, the next step is to do something with the results returned by the search. You can export and download the results to your local computer or, if there is an email-based attack, you can delete the results of a search from user mailboxes.
You can also use scripts for advanced scenarios. Sometimes you have to do more advanced, complex, and repetitive content search tasks. To help make this easier, Microsoft has created a number of Security and Compliance Center PowerShell scripts to help complete complex content search-related tasks. Some of these scripts include:

- **Search-specific mailbox and site folders** (called a targeted collection) when you're confident that items responsive to a case are located in that folder.
- **Search the mailbox and OneDrive location** for a list of users.
- **Create, report on, and delete multiple searches** to quickly and efficiently identify, and cull search data.
- **Clone a content search** and quickly compare the results of different keyword search queries run on the same content locations; or use the script to save time by not having to reenter a large number of content locations when you create a new search.

44 https://docs.microsoft.com/microsoft-365/compliance/assign-ediscovery-permissions?view=o365-worldwide

Content Search is easy to use, but it's also a powerful tool. To learn more, visit the **content search overview**[45].

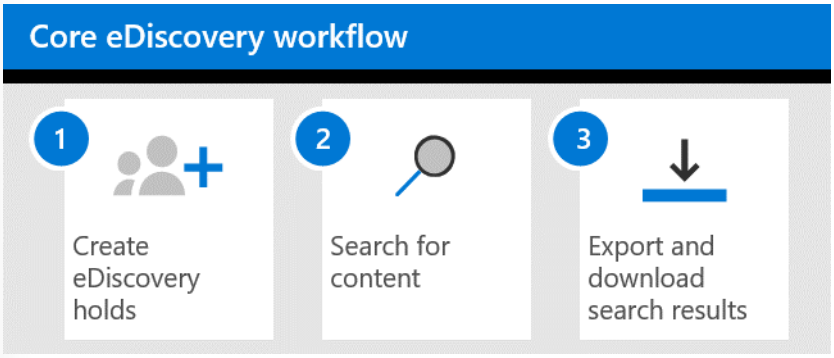
Describe the core eDiscovery workflow

Core eDiscovery in Microsoft 365 provides a basic tool that organizations can use to search and export content in Microsoft 365.

To access Core eDiscovery or be added as a member of a Core eDiscovery case, a user must be assigned the appropriate permissions. Specifically, a user must be added as a member of the **eDiscovery Manager role** group in the Office 365 Security and Compliance Center.

You start by creating an eDiscovery case, which starts from within **Microsoft 365 compliance center**. When you create a case, you must specify a name for it and optionally define a case number. You can assign members to the case. From that point, the case will be displayed in the eDiscovery page and the user can step through the workflow.

The workflow consists of creating holds, searching for content, and exporting and downloading search results.



Create an eDiscovery hold

You can use an eDiscovery case to create a hold to preserve content that might be relevant to the case. You can place a hold on the Exchange mailboxes and OneDrive for Business accounts of people you're investigating in the case. You can also place a hold on the mailboxes and sites that are associated with Microsoft Teams, Office 365 Groups, and Yammer Groups. When you place content locations on hold, it's preserved until you remove the hold from the content location, or until you delete the hold.

It may take up to 24 hours after you create the hold for it to take effect.

You have two options to scope the content that's preserved:

- You create an infinite hold where all content in the specified locations is placed on hold. Or you can create a query-based hold where only the content in the specified locations that matches a search query is placed on hold.
- You can specify a date range to preserve only the content that was sent, received, or created within that date range. Or you can hold all content in specified locations regardless of when it was sent, received, or created.

45 https://docs.microsoft.com/microsoft-365/compliance/search-for-content?view=o365-worldwide

Search for content in the case

When you've placed a hold, you can create and run searches for content that relates to the case. You start the search from within the home page for that specific case. Searches associated with a case can only be accessed by members assigned to it.

You can specify keywords, message properties such as sent and received dates, or document properties such as file names, or the date a document was last changed. You can use Boolean operators such as **AND**, **OR**, **NOT**, or **NEAR**. You can also search for sensitive information (for example, social security numbers) in documents, or search for documents that have been shared externally. If you don't specify keywords, all content located in the specified content locations will be included in the search results.

Export content from a case

You can export search results. Mailbox items are downloaded in a PST file or as individual messages. Content from SharePoint, OneDrive for Business sites, copies of native Office documents, and other documents are exported. A Results.csv file that contains information about every item that's exported and a manifest file (in XML format) that contains information about every search result is also exported.

You can export the results of both a single search or results from multiple searches associated with a case.

Close, reopen, and delete a core eDiscovery case

Core eDiscovery cases can be closed when the investigations or legal cases they were supporting have been completed. When a case is closed, any holds associated with it will be turned off. Once turned off, there's a 30-day grace period (referred to as a delay hold) on the content locations that were on hold. This helps ensure that content isn't deleted immediately and gives admins the chance to look for and restore any content before it's deleted permanently.

The main difference between an active and closed case is that eDiscovery holds are turned off for a closed case.
When you reopen a closed case, any holds that were in place when it was closed, won't be reinstated automatically. After reopening the case, you'll need to turn on previous holds. A reopened case will have its status changed from closed to active.

You can delete both active and closed cases. If you delete a case, all searches and exports in that case are also deleted, the case is removed from the list in the Microsoft 365 compliance center. The deleted case can't be reopened.

If the case you want to delete contains eDiscovery holds, you won't be able to delete it. You'll need to delete all the holds linked to the case and try and delete it again.

Interactive guide

As the admin for your organization, you've be asked to help with an ongoing investigation. For example, you need to collect information on whether a user has sent emails about the Winter project that is currently the subject of the investigation. The following interactive click-through demonstrates how you can do this using the Core eDiscovery workflow. Select the link below to get started.

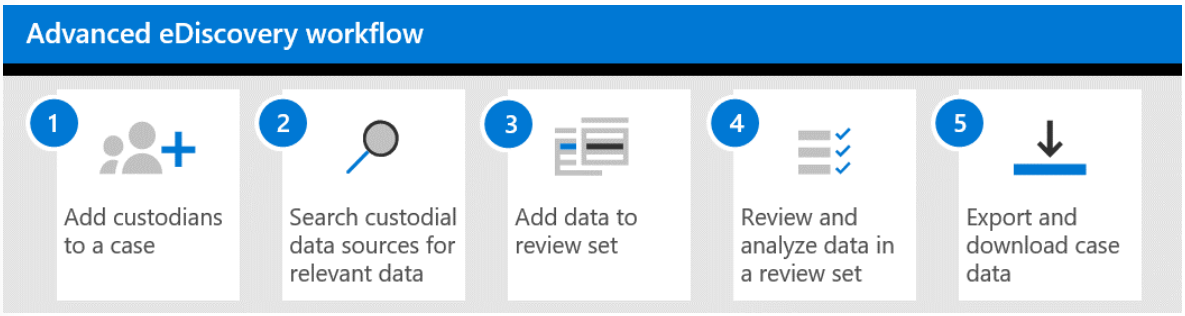
Interactive guide - Explore core eDiscovery[46]

46 https://edxinteractivepage.blob.core.windows.net/edxpages/Security%20fundamentals/LP04M05%20-%20Use%20eDiscovery%20to%20help%20with%20investigations/index.html?azure-portal=true

Describe the advanced eDiscovery workflow

The Advanced eDiscovery solution in Microsoft 365 builds on the existing core eDiscovery. This new solution provides an end-to-end workflow to preserve, collect, review, analyze, and export content that's relevant to your organization's internal and external investigations. It also lets legal teams manage the entire legal hold notification workflow to communicate with custodians involved in a case.

The built-in workflow of Advanced eDiscovery described below aligns with the Electronic Discovery Reference Model (EDRM), a framework that outlines standards for recovery and discovery of digital data.



1. **Add custodians to a case**. This is the first step after creating a case. Custodians are people who have administrative control of a document or electronic file that could be relevant to the case.
2. **Search custodial data sources for data relevant to the case**. After custodians have been added to a case, you can use the built-in search tool to find the custodian locations for data that might be relevant. You do this by using keywords, properties, and conditions to build your search queries, which will return search results that contain data that's likely to be relevant to the case. You can preview search results to quickly verify whether the data is relevant and revise your queries and rerun searches to improve results.
3. **Add data to a review set**. After configuring and verifying that a search result has provided you with the right data, you'll need to prepare your results for review and analysis. You can do this by adding the search results to a review set. Doing this means that items are copied from their location of origin to a secure location in Azure Storage. The data is also reindexed to optimize it for review and analysis. You can also add data to conversation review sets, which will provide you with the capabilities to reconstruct conversations, and enable you to review and export conversations like those in Microsoft Teams.
4. **Review and analyze data in a review set**. When your data is in a review set, you're ready to view and analyze the case data through a wide variety of capabilities and tools such as filters, queries, and tags. The goal of review and analysis is to reduce the data set to what is the most relevant to the case that's being investigated.
5. **Export and download case data**. Finally, you can export the data out of Advanced eDiscovery for external review. For example, for an external team of investigators. You export the data out of the review set, and then copy it to a different Azure Storage location. You can then use Azure Storage Explorer to download that data as an export package, to a local device. This export package will contain other components like a summary report, and an error report.

Use Advanced eDiscovery in Microsoft 365 to preserve, collect, review, analyze, and export data that's relevant to your organization's internal and external investigations.

Describe the core audit capabilities in Microsoft 365

The audit functionality in the Microsoft 365 compliance center allows organizations to view user and administrator activity through a unified audit log. For example, did an administrator reset a password? Did a user change a setting for a team in Microsoft Teams? A unified audit log supports the search of many users and/or admin activities across Microsoft 365 services, Dynamics 365, Microsoft Power Apps, Microsoft Power Automate, Power BI, Azure Active Directory, and more. For a detailed listing, visit **Search the audit log in the compliance center**[47].

When an audited activity is performed by a user or admin, an audit record is generated and stored in the audit log for the organization. The length of time that an audit record is kept (and searchable in the audit log) depends on the Office 365 or Microsoft 365 Enterprise subscription, and specifically the type of the license that's assigned to specific users. For core audit capability, the audit record is kept and searchable for 90 days.

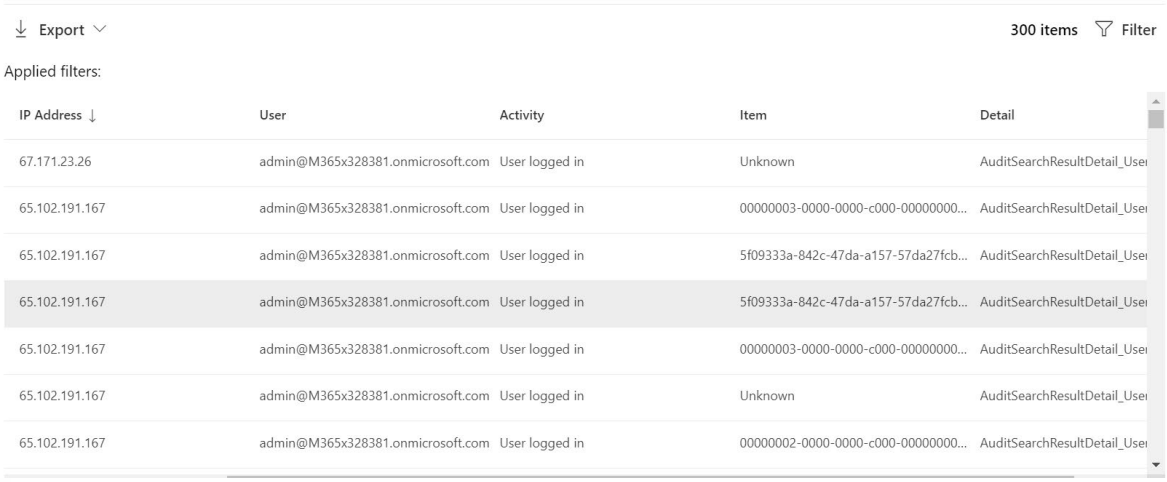
Searching the audit log requires the search capability to be turned on, and for the user doing the search to be assigned the appropriate role. The search criteria can be configured based on:

- Activities
- Start date and end date
- Users
- File, folder, or site

The results of the audit log search, which can be filtered and exported to a CSV file, contain the following information about each event returned by the search:

- **Date**: The date and time (in UTC format) when the event occurred.
- **IP address**: The IP address of the device that was used when the activity was logged. The IP address is displayed in either an IPv4 or IPv6 address.
- **User**: The user (or service account) who completed the action that triggered the event.
- **Activity**: The activity completed by the user. This is based on activities configured.
- **Item**: The object that was created or modified because of the corresponding activity. For example, the file that was viewed or modified, or the user account that was updated. Not all activities have a value in this column.
- **Detail**: Additional information about an activity. Again, not all activities have a value.

47 https://docs.microsoft.com/microsoft-365/compliance/search-the-audit-log-in-security-and-compliance?view=o365-worldwide



It can take up to 30 minutes or up to 24 hours after an event occurs for the corresponding audit log record to be returned in the results of an audit log search.

Describe Advanced Auditing

Advanced Audit helps organizations to conduct forensic and compliance investigations by increasing audit log retention that's required to conduct an investigation. Audit log retention provides access to crucial events that help determine the scope of compromise, and faster access to Office 365 Management Activity API.

These capabilities differentiate Advanced Audit from the core audit functionality described in the previous topic and require a Microsoft 365 E5 license, or a Microsoft 365 E3 or Office 365 E3 license with a Microsoft 365 E5 Compliance, or Microsoft 365 E5 eDiscovery and Audit add-on license.

Long-term retention of audit logs

Advanced Audit keeps all Exchange, SharePoint, and Azure Active Directory audit records for one year. Keeping audit records for longer periods can help with ongoing forensic or compliance investigations. Microsoft now has the capability to keep audit logs for 10 years. The 10-year retention of audit logs helps support long-running investigations and respond to regulatory, legal, and internal obligations.

NOTE: Retaining audit logs for 10 years requires an additional add-on license.

Access to crucial events for investigations

Advanced Auditing helps organizations to conduct forensic and compliance investigations by providing access to crucial events, such as when mail items were accessed, when mail items were replied to and forwarded, and when and what a user searched for in Exchange Online and SharePoint Online. These crucial events can help admins and users investigate possible breaches and determine the scope of compromise. Advanced Auditing provides the following crucial events:

- **MailItemsAccessed** - The MailItemsAccessed event is a mailbox auditing action that's triggered when mail data is accessed by mail protocols and mail clients. The MailItemsAccessed action can help investigators identify data breaches and determine the scope of messages that may have been compromised.

- **Send** - The Send event is also a mailbox auditing action and is triggered when a user does does any of the actions below . Investigators can use the Send event to identify emails sent from a compromised account. The audit record for a Send event contains information about the message. The actual content of the message isn't displayed. However, information such as when the message was sent, the InternetMessage ID, the subject line, and if the message contained attachments, are accessible. This auditing information can help investigators identify information about email messages sent from a compromised account or sent by an attacker.
  - Sends an email message
  - Replies to an email message
  - Forwards an email message

- **SearchQueryInitiatedExchange** - The SearchQueryInitiatedExchange event is triggered when a person uses the Search bar in Outlook on the web (OWA) to search for items in a mailbox. Investigators can use the SearchQueryInitiatedExchange event to determine if an attacker may have compromised an account, or tried to access sensitive information in the mailbox. The audit record for a SearchQueryInitiatedExchange event contains information such as the actual text of the search query. By looking at the search queries that an attacker may have made, an investigator can better understand the intent of the email data that was searched for.
- **SearchQueryInitiatedSharePoint** - Similar to searching for mailbox items, the SearchQueryInitiatedSharePoint event is triggered when a person searches for items in the SharePoint home site for your organization. Investigators can use the SearchQueryInitiatedSharePoint event to determine if an attacker tried to find (and possibly accessed) sensitive information in SharePoint. The audit record for a SearchQueryInitiatedSharePoint event also contains the actual text of the search query. By looking at the search queries that an attacker may have performed, an investigator can better understand the intent and scope of the file data being searched for.

High-bandwidth access to Office 365 Management Activity API

Organizations that access auditing logs through the Office 365 Management Activity API were previously restricted by throttling limits at the publisher level. This means that for a publisher pulling data on behalf of multiple customers, the limit was shared by all those customers.

With the release of Advanced Audit, Microsoft is moving from a publisher-level limit to a tenant-level limit. The result is that each organization will get their own fully allocated bandwidth quota to access their auditing data. The bandwidth isn't a static, predefined limit but is modeled on a combination of factors, including the number of seats in the organization and the type of Microsoft 365 license (organizations with an E5 license will get more bandwidth than non-E5 organizations).

Knowledge check

Multiple choice

Item 1. A new admin has joined the compliance team and needs access to Core eDiscovery to be able to add and remove members, create and edit searches, and export content from a case. To which role should the admin be assigned?

- ☐ Add them as a member of the eDiscovery Manager role group.
- ☐ Add them as a member of the eDiscovery review role.
- ☐ Add them as a member of the eDiscovery custodian role.

Multiple choice

Item 2. The compliance team needs to perform more advanced, complex, and repetitive content search tasks. What can enable the team to do more complex search tasks?

- ☐ Use the Microsoft 365 autocontent search client.
- ☐ Use the continuous eDiscovery autosearch client.
- ☐ Use the PowerShell scripts provided by Microsoft.

Multiple choice

Item 3. The compliance admin has been asked to use Advanced eDiscovery to help a legal team that is working on a case. What is the workflow the admin will use?

- ☐ Search custodial data, add custodians to a case, add data to a review set, review and analyze data, then finally export and download case data.
- ☐ Add custodians to a case, search custodial sources for relevant data, add data to a review set, review and analyze data, then finally export and download the case data.
- ☐ Add data to a review set, review and analyze data, add custodians to a case, search custodial sources for relevant data, then finally export and download the case data.

Multiple choice

Item 4. The audit team needs to conduct compliance investigations across emails. They need access to crucial events, such as when mail items were accessed, when mail items were replied to and forwarded. What capability can the team use?

- ☐ Use Advanced Auditing so that you access and investigate those events.
- ☐ Use Core Auditing so that you can access and investigate those events.
- ☐ Use alert policies to generate and view alerts on when users perform certain actions on emails.

Summary and resources

You've explored how eDiscovery and audit can help organizations to identify, collect, and/or audit information in a rapid and effective manner to meet legal requirements.

Now that you've completed this lesson, you should be able to:

- Describe the purpose of eDiscovery.
- Describe the capabilities of the content search tool.
- Describe the core and advanced eDiscovery workflows.
- Describe the core and advanced auditing capabilities of Microsoft 365.

Learn more

- **eDiscovery solutions in Microsoft 365**[48]
- **Search for content using the Content Search tool**[49]
- **Get started with Core eDiscovery**[50]
- **Overview of Microsoft 365 Advanced eDiscovery**[51]
- **Search the audit log in the compliance center**[52]
- **Advanced Audit in Microsoft 365**[53]
- **Turn audit log search on or off**[54]
- **API Throttling**[55]

48 https://docs.microsoft.com/microsoft-365/compliance/ediscovery?view=o365-worldwide
49 https://docs.microsoft.com/microsoft-365/compliance/search-for-content?view=o365-worldwide
50 https://docs.microsoft.com/microsoft-365/compliance/get-started-core-ediscovery?view=o365-worldwide
51 https://docs.microsoft.com/microsoft-365/compliance/overview-ediscovery-20?view=o365-worldwide
52 https://docs.microsoft.com/microsoft-365/compliance/search-the-audit-log-in-security-and-compliance?view=o365-worldwide
53 https://docs.microsoft.com/microsoft-365/compliance/advanced-audit?view=o365-worldwide
54 https://docs.microsoft.com/microsoft-365/compliance/turn-audit-log-search-on-or-off?view=o365-worldwide
55 https://docs.microsoft.com/office/office-365-management-api/office-365-management-activity-api-reference#api-throttling

Describe the resource governance capabilities in Azure

Introduction

Azure has the capabilities that admins need to ensure that resources are governed properly, that they're secure, and in line with the organization's compliance requirements.

In this module, you'll learn about the resource governance capabilities available for Azure.

After completing this module, you should be able to:

- Describe some of the resource governance capabilities in Azure.

Describe the use of Azure Resource locks

Before we can describe the use of Azure Resource Manager locks, it is important to first understand what Azure Resource Manager is. Azure Resource Manager is the deployment and management service for Azure. Azure Resources Manager provides a management layer that enables administrators to create, update, and delete resources in an Azure account. Admins can use management features such resource locks to secure resources after deployment.

Resource locks can be used to prevent resources from being accidentally deleted or changed. Even with role-based access control policies in place there is still a risk that people with the right level of access could delete a critical resource. Azure Resource Manager locks prevent users from accidentally deleting or modifying a critical resource, and can be applied to a subscription, a resource group, or a resource. For example, there may be times when an administrator needs to lock a subscription, a resources group, or a resource. A lock would be applied in these situations to prevent users from accidentally deleting or modifying a critical resource.

A lock level can be set to **CanNotDelete** or **ReadOnly**. In the portal, the locks are called **Delete** and **Read-only** respectively.

- **CanNotDelete** means authorized users can still read and modify a resource, but they can't delete the resource.
- **ReadOnly** means authorized users can read a resource, but they can't delete or update the resource. Applying this lock is similar to restricting all authorized users to the permissions granted by the Reader role.

A resource can have more than one lock. For example, a resource may have a ReadOnly lock and a CanNotDelete lock. When you apply a lock at a parent scope, all resources within that scope inherit that lock. Even resources you add later inherit the lock from the parent. The most restrictive lock in the inheritance takes precedence.

Resource Manager locks apply only to operations that happen in the management plane. The locks don't restrict how resources perform their functions. If a lock is applied, changes to the actual resource are restricted, but resource operations aren't restricted. For example, a ReadOnly lock on an Azure SQL Database logical server prevents deletion or modification of the server. However, it doesn't prevent you from creating, updating, or deleting data in the databases on that server.

Interactive guide

A development team in your organization uses an Azure Storage account to store some of their content. As the Azure administrator, you've been asked to help ensure that the storage account can't be deleted.

In this interactive demonstration, you'll lock a storage account, verify the lock works, and then remove the lock. Select the link below to get started.

Interactive guide - Use Azure resource lock to lock resources[56].

Describe what is Azure Blueprints

Azure Blueprints provide a way to define a repeatable set of Azure resources. Azure Blueprints enable development teams to rapidly provision and run new environments, with the knowledge that they're in line with the organization's compliance requirements. Teams can also provision Azure resources across several subscriptions simultaneously, meaning they can achieve shorter development times and quicker delivery.

Azure Blueprints are a declarative way to orchestrate the deployment of various resource templates and other artifacts such as:

- Role Assignments
- Policy Assignments
- Azure Resource Manager templates (ARM templates)
- Resource Groups

Blueprint objects are replicated to multiple Azure regions. This replication provides low latency, high availability, and consistent access to your blueprint objects, whatever region Azure Blueprints deploys your resources to.

With Azure Blueprints, the relationship between the blueprint definition (*what should be deployed*) and the blueprint assignment (*what was deployed*) is preserved. This connection supports improved tracking and auditing of deployments.

Azure Blueprints helps ensure Azure resources are deployed in a way that's in line with compliance requirements. However, a service like Azure Policy should be used to continuously monitor resources and ensure a continuation with compliance requirements.

Describe Azure policy

Azure Policy is designed to help enforce standards and assess compliance across your organization. Through its compliance dashboard, you can access an aggregated view to help evaluate the overall state of the environment. You can drill down to a per-resource, or per-policy level granularity. You can also use capabilities like bulk remediation for existing resources and automatic remediation for new resources, to resolve issues rapidly and effectively. Common use cases for Azure Policy include implementing governance for resource consistency, regulatory compliance, security, cost, and management.

Azure Policy evaluates all resources in Azure and Arc enabled resources (specific resource types hosted outside of Azure).

Azure Policy evaluates whether the properties of resources match with business rules. These business rules are described using **JSON**[57] format, and referred to as **policy definitions**[58]. For simplified management, you can group together multiple business rules to form a single **policy initiative**[59]. After business

56 https://edxinteractivepage.blob.core.windows.net/edxpages/Security%20fundamentals/LP04M07%20-%20Use%20Azure%20resource%20lock%20to%20lock%20resources/index.html?azure-portal=true
57 https://docs.microsoft.com/azure/governance/policy/concepts/definition-structure
58 https://docs.microsoft.com/azure/governance/policy/overview#policy-definition
59 https://docs.microsoft.com/azure/governance/policy/overview#initiative-definition

rules have been formed, you can assign the policy definition, or policy initiative, to any scope of resources that are supported, such as management groups, subscriptions, resource groups, or individual resources.

Evaluation outcomes

Azure Policy evaluates resources at specific times during the resource lifecycle and the policy assignment lifecycle, and for regular ongoing compliance evaluation. The following events or times will trigger an evaluation:

- A resource has been created, deleted, or updated in scope with a policy assignment.
- A policy or an initiative is newly assigned to a scope.
- A policy or an initiative that's been assigned to a scope is updated.
- The standard compliance evaluation cycle (happens once every 24 hours).

Organizations will vary in how they respond to non-compliant resources. Here are some examples:

- Deny a change to a resource.
- Log changes to a resource.
- Alter a resource before or after a change.
- Deploy related compliant resources.

With Azure Policy, responses like these are made possible by using **effects**[60], which are specified in policy definitions.

What's the difference between Azure Policy and Azure role-based access control (RBAC)?

It's important not to confuse Azure Policy and Azure RBAC. You use Azure Policy to ensure that the resource state is compliant to your organization's business rules, no matter who made the change or who has permission to make changes. Azure Policy will evaluate the state of a resource, and act to ensure the resource stays compliant.

Azure RBAC focuses instead on managing user actions at different scopes. Azure RBAC manages who has access to Azure resources, what they can do with those resources, and what areas they can access. If actions need to be controlled, then you would use Azure RBAC. If an individual has access to complete an action, but the result is a non-compliant resource, Azure Policy still blocks the action.

Azure RBAC and Azure Policy should be used together to achieve full scope control in Azure.

60 https://docs.microsoft.com/azure/governance/policy/concepts/effects

Knowledge check

Multiple choice

Item 1. The compliance admin for the organization wants to ensure that users can access the resources they need, but not accidentally delete resources. Which Azure resource lock level can the admin set to ensure that users can read and modify a resource, but can't delete the resource?

- ☐ ReadOnly
- ☐ CanNotDelete
- ☐ UpdateAndDelete

Multiple choice

Item 2. Which tool can enable an organization's development team to rapidly provision and run new resources, in a repeatable way that is in line with the organization's compliance requirements?

- ☐ Azure Policy
- ☐ Azure Rapid Build
- ☐ Azure Blueprints

Multiple choice

Item 3. As the compliance admin for your organization, you need to ensure that Azure resources meet your organization's business rules? Which Azure capability should you use?

- ☐ Use Azure role-based access control (RBAC).
- ☐ Use Azure Policy.
- ☐ Use Azure resource locks.

Summary and resources

You've seen how admins can use the resource governance capabilities in Azure to ensure that resources for their organization are governed properly, so that they are secure, and in line with the organization's compliance requirements.

Now that you've completed this lesson, you should be able to:

- Describe some of the resource governance capabilities in Azure.

Learn more

- **Lock resources to prevent unexpected changes**[61]
- **What is Azure Resource Manager**[62]
- **What is Azure Blueprints?**[63]

61 https://docs.microsoft.com/azure/azure-resource-manager/management/lock-resources
62 https://docs.microsoft.com/azure/azure-resource-manager/management/overview
63 https://docs.microsoft.com/azure/governance/blueprints/overview

- **What is Azure Policy?**[64]

64 https://docs.microsoft.com/azure/governance/policy/overview

Answers

Multiple choice

Item 1. When browsing Microsoft compliance documentation in the Service Trust Portal, you have found several documents that are specific to your industry. What is the best way of ensuring you keep up to date with the latest updates?

■ Save the documents to your My Library.

☐ Print each document so you can easily refer to them.

☐ Download each document.

Explanation
By saving the documents to your My Library you will be prompted to say when you want to be notified of updates.

Multiple choice

Item 2. A new admin has joined the team and needs to be able to access the Microsoft 365 Compliance Center. Which of the following roles could the admin use to access the Compliance Center?

■ Compliance Administrator role.

☐ Helpdesk Administrator role.

☐ User Administrator role.

Explanation
This is one of the multiple roles you can use to access the Compliance Center.

Multiple choice

Item 3. Your new colleagues on the admin team are unfamiliar with the concept of shared controls in Compliance Manager. How would the concept of shared controls be explained?

☐ Controls that both external regulators and Microsoft share responsibility for implementing.

☐ Controls that both your organization and external regulators share responsibility for implementing.

■ Controls that both your organization and Microsoft share responsibility for implementing.

Explanation
Both your organization and Microsoft work together to implement these controls.

Multiple choice

Item 4. A customer has requested a presentation on how the Microsoft 365 Compliance Center can help improve their organization's compliance posture. The presentation will need to cover Compliance Manager and compliance score. What is the difference between Compliance Manager and compliance score?

- ■ Compliance Manager is an end-to-end solution in Microsoft 365 Compliance Center to enable admins to manage and track compliance activities. Compliance score is a calculation of the overall compliance posture across the organization.
- ☐ Compliance Manager is an end-to-end solution in Microsoft 365 Compliance Center to enable admins to manage and track compliance activities. Compliance score is a score the organization receives from regulators for successful compliance.
- ☐ Compliance Manager is the regulator who will manage your compliance activities. Compliance score is a calculation of the overall compliance posture across the organization.

Explanation
Compliance Manager provides admins with the capabilities to understand and improve their compliance score so that they can ultimately improve the organization's compliance posture and help it to stay in line with its compliance requirements..

Multiple choice

Item 1. Which part of the concept of know your data, protect your data, and prevent data loss addresses the need for organizations to automatically retain, delete, store data and records in a compliant manner?

- ☐ Know your data.
- ☐ Prevent data loss.
- ■ Govern your data.

Explanation
Capabilities like retention policies, retention labels, and records management enable organizations to govern their data.

Multiple choice

Item 2. As part of a new data loss prevention policy, the compliance admin needs to be able to identify important information such as credit card numbers, across the organization's data. How can the admin address this requirement?

- ☐ Use activity explorer.
- ☐ Use sensitivity labels.
- ■ Use sensitive information types.

Explanation
Microsoft provides built-in sensitive information types that you can use to identify data such as credit card numbers.

Multiple choice

Item 3. Within the organization, some emails are confidential and should be encrypted so that only authorized users can read them. How can this requirement be implemented?

☐ Use the content explorer.

■ Use sensitivity labels.

☐ Use Records Management.

Explanation
Sensitivity labels help ensure that emails can only be decrypted only by users authorized by the label's encryption settings.

Multiple choice

Item 4. Your organization uses Microsoft Teams to collaborate on all projects. The compliance admin wants to prevent users from accidentally sharing sensitive information in a Microsoft Teams chat session. What capability can address this requirement?

■ Use data loss prevention policies.

☐ Use Records Management capabilities.

☐ Use retention policies.

Explanation
With data loss prevention policies, administrators can now define policies that can prevent users from sharing sensitive information in a Microsoft Teams chat session or Teams channel, whether this information is in a message, or in a file.

Multiple choice

Item 5. Due to a certain regulation, your organization must now keep hold of all documents in a specific SharePoint site that contains customer information for five years. How can this requirement be implemented?

☐ Use sensitivity labels.

☐ Use the content explorer.

■ Use retention policies.

Explanation
You can use retention policies to define data retention for all documents in a SharePoint site.

Multiple choice

Item 1. The compliance admin for the organization wants explain the importance of insider risk management, to the business leaders? What use case would apply?

■ To identify and protect against risks like an employee sharing confidential information.

☐ To identify and protect against malicious software across your network, such as ransomware.

☐ To identify and protect against devices shutting down at critical moments.

Explanation
Use risk management to help protect your organization against these risks.

Multiple choice

Item 2. To comply with corporate policies, the compliance admin needs to be able to identify and scan for offensive language across the organization. What solution can the admin implement to address this need?

☐ Use Policy Compliance in Microsoft 365.

■ Use Communication Compliance.

☐ Use information barriers.

Explanation
Communication Compliance helps minimize communication risks by enabling you to detect, capture, and take remediation actions for inappropriate messages in the organization.

Multiple choice

Item 3. An organization has many departments that collaborate through Microsoft Teams. To comply with business policies, the IT organization needs to make sure that users from one particular department are limited in their access and interactions with other departments. What solution can address this need?

☐ Use Communication Compliance.

☐ Use Customer Lockbox.

■ Use information barriers.

Explanation
With information barriers, you're able to restrict communications among specific groups of users when necessary.

Multiple choice

Item 4. The compliance team wants to control the use privileged admin accounts with standing access to sensitive data, so that admins receive only the level of access they need, when they need it. How can this requirement be implemented?

☐ Use Communication Compliance.

■ Use privileged access management.

☐ Use the Audit log.

Explanation
You can use privileged access management to require users to request just-in-time access to complete certain tasks.

Multiple choice

Item 5. A customer has identified an issue that requires a Microsoft engineer to access the organization's content, to determine the root cause, and fix the issue. To protect the organization, the engineer shouldn't be able to access content and perform service operations without explicit approval. What capability can address this requirement?

☐ Use privileged access management.

☐ Use information barriers.

■ Use Customer Lockbox.

Explanation
Customer Lockbox brings your organization into the approval workflow. The engineer will ask for access, and will only have access for the stated duration they've requested.

Multiple choice

Item 1. A new admin has joined the compliance team and needs access to Core eDiscovery to be able to add and remove members, create and edit searches, and export content from a case. To which role should the admin be assigned?

■ Add them as a member of the eDiscovery Manager role group.

☐ Add them as a member of the eDiscovery review role.

☐ Add them as a member of the eDiscovery custodian role.

Explanation
Members of this role group can create and manage Core eDiscovery cases. They can also add and remove members, place an eDiscovery hold on users, create and edit searches, and export content from a Core eDiscovery case.

Multiple choice

Item 2. The compliance team needs to perform more advanced, complex, and repetitive content search tasks. What can enable the team to do more complex search tasks?

☐ Use the Microsoft 365 autocontent search client.

☐ Use the continuous eDiscovery autosearch client.

■ Use the PowerShell scripts provided by Microsoft.

Explanation
Microsoft has created many Security & Compliance Center PowerShell scripts to help complete complex content search-related tasks.

Multiple choice

Item 3. The compliance admin has been asked to use Advanced eDiscovery to help a legal team that is working on a case. What is the workflow the admin will use?

☐ Search custodial data, add custodians to a case, add data to a review set, review and analyze data, then finally export and download case data.

■ Add custodians to a case, search custodial sources for relevant data, add data to a review set, review and analyze data, then finally export and download the case data.

☐ Add data to a review set, review and analyze data, add custodians to a case, search custodial sources for relevant data, then finally export and download the case data.

Explanation
The workflow will help you to get the best out of Advanced eDiscovery, and is in line with common eDiscovery practices.

Multiple choice

Item 4. The audit team needs to conduct compliance investigations across emails. They need access to crucial events, such as when mail items were accessed, when mail items were replied to and forwarded. What capability can the team use?

■ Use Advanced Auditing so that you access and investigate those events.

☐ Use Core Auditing so that you can access and investigate those events.

☐ Use alert policies to generate and view alerts on when users perform certain actions on emails.

Explanation
Advanced Auditing helps organizations to conduct forensic and compliance investigations by providing access to these crucial events.

Multiple choice

Item 1. The compliance admin for the organization wants to ensure that users can access the resources they need, but not accidentally delete resources. Which Azure resource lock level can the admin set to ensure that users can read and modify a resource, but can't delete the resource?

☐ ReadOnly

■ CanNotDelete

☐ UpdateAndDelete

Explanation
This lock will ensure users can still read and modify the resource, without being able to delete it.

Multiple choice

Item 2. Which tool can enable an organization's development team to rapidly provision and run new resources, in a repeatable way that is in line with the organization’s compliance requirements?

☐ Azure Policy

☐ Azure Rapid Build

■ Azure Blueprints

Explanation
Azure Blueprint will enable your development teams to define a repeatable set of Azure resources, and achieve shorter development times and faster delivery.

Multiple choice

Item 3. As the compliance admin for your organization, you need to ensure that Azure resources meet your organization's business rules? Which Azure capability should you use?

☐ Use Azure role-based access control (RBAC).

■ Use Azure Policy.

☐ Use Azure resource locks.

Explanation
Azure Policy evaluates whether the properties of resources match with business rules.