

1ST EDITION

Microsoft Cybersecurity Architect Exam Ref SC-100

Get certified with ease while learning how to develop
highly effective cybersecurity strategies



DWAYNE NATWICK

Foreword by Rod Trent, Security Cloud Advocate, Microsoft

Appendix

Technical requirements

To follow along and complete the exercises within this book, you will need to have access to security, compliance, and identity services within **Microsoft 365** and **Azure**. This can be accomplished through a trial subscription available for Microsoft 365 and an available free month of Azure. Advanced security services will also require an **Enterprise + Mobility** license. The steps to set up these licenses will be covered later in this chapter.

Hands-On Section

Resources available and accessing Microsoft Learn

Earlier in this chapter, some of the resources available for preparing for the exam were mentioned. **Microsoft Learn** was mentioned along with the Microsoft docs, but Microsoft Learn requires its own section due to the amount of free content that it provides to help you prepare for an exam.

Accessing Microsoft Learn

Microsoft Learn is a great resource to get your learning path started. All the content on Microsoft Learn is free. When you create an account on Microsoft, learning progress is tracked and you can acquire badges along the way. In addition, Microsoft creates learning challenges periodically with prizes, such as free exam vouchers. You can create a free account by selecting the icon on the top right of the page and selecting **Sign in**, as shown in the following screenshot:



Figure 0.2 – Microsoft Learn site – Sign in

You can sign in with an existing Microsoft account or create one to get started, as shown here:

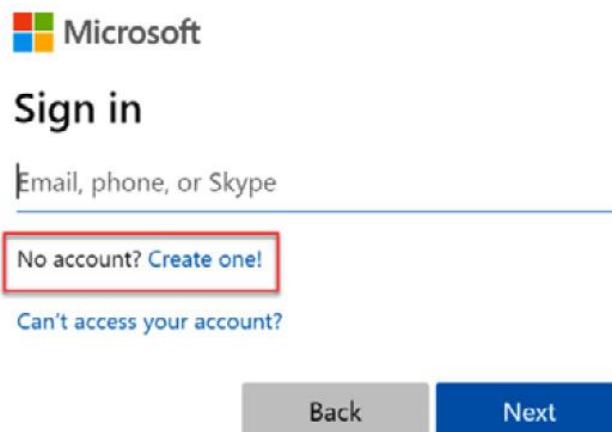


Figure 0.3 – Create or sign into a Microsoft account

You can get to Microsoft Learn by going to <https://www.microsoft.com/learn>.

Finding content on Microsoft Learn

Content on Microsoft Learn can be found in various ways. You can search for specific products, roles, or certifications. These options can be found on the selection ribbon at the top of the **Learn** home page, as shown in the following screenshot. The home page also provides several recommendations so that you can start learning:

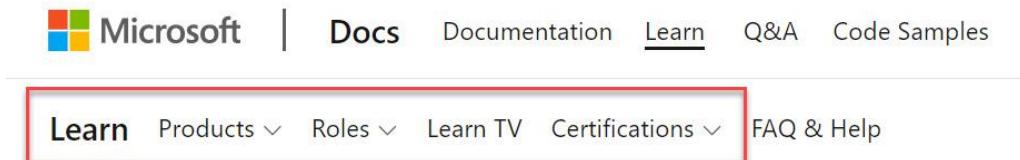


Figure 0.4 – Learn content navigation

From the Learn content navigation tabs, select a drop-down arrow to filter for content in the specific **Products**, **Roles**, or **Certifications** areas:

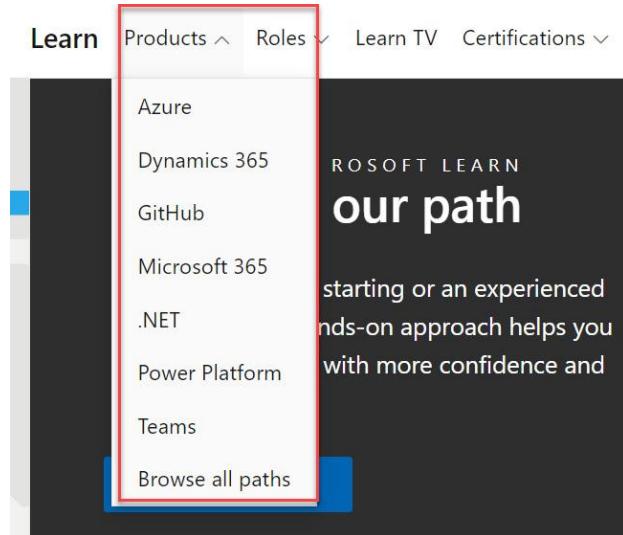


Figure 0.5 – Filter categories under the Products drop-down

Once you have selected the area of interest, or simply chosen to browse all, you can search for specific topics and filter even further on individual courses or learning paths, as shown in the following screenshot:

The screenshot shows the Microsoft Learn homepage. At the top, there's a navigation bar with links for Microsoft Learn, Documentation, Training, Certifications, Q&A, Code Samples, Shows, and Events. A search bar and a sign-in button are also at the top. Below the navigation, a banner says "Browse all learning paths and modules". A sub-banner below it says "Learn new skills and discover the power of Microsoft products with step-by-step guidance. Start your journey today by exploring our learning paths and modules." On the left, there's a "Filter" sidebar with sections for Types (Learning Path, Module), Levels (Advanced, Beginner, Intermediate), and Subjects (Business applications, Data and AI, Digital and application innovation, Infrastructure, Modern life, Modern work, Search, ads, and news, Security). The main area shows a grid of 9 items, each representing a module or learning path. Each item has a title, duration, rating, and a "Save" button.

Figure 0.6 – Browsing all content in Microsoft Learn

In this section, you learned how to access Microsoft Learn and browse for modules and learning paths. The next section will assist you in finding content specific to the SC-100 exam.

Exam pages on Microsoft Learn

Another common area within Microsoft Learn is its **exam pages**. For any exam provided by Microsoft, there is an exam page and a certification page that is located within Microsoft Learn. These pages provide an overview of the exam or certification, the roles of individuals that may be interested in the exam, the objective areas for the exam, scheduling the exam, and the Microsoft Learn learning path to prepare for the exam. These pages are extremely helpful when you are preparing specifically for an exam rather than just learning general technical knowledge. The following screenshot shows how to search for the SC-100 exam:

The screenshot shows the Microsoft Learn "Browse Certifications and Exams" page. A search bar at the top contains the text "sc-100". The results show 2 results for "sc-100". The first result is "Exam SC-100: Microsoft Cybersecurity Architect (beta)" under the "EXAM" category. The second result is "Microsoft Certified: Cybersecurity Architect Expert" under the "CERTIFICATION" category. Both results show their respective logos, titles, descriptions, and the "Save" button.

Figure 0.7 – Browsing for the SC-100 exam

The following screenshot shows the exam page for the SC-100 exam:

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

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

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

Exam SC-100: Microsoft Cybersecurity Architect

Languages: English, Japanese, Chinese (Simplified), Korean, German, French, Spanish, Portuguese (Brazil), Russian, Arabic (Saudi Arabia), Chinese (Traditional), Italian, Indonesian (Indonesia)

Retirement date: none

This exam measures your ability to accomplish the following technical tasks: design a Zero Trust strategy and architecture; evaluate Governance Risk Compliance (GRC) technical strategies and security operations strategies; design security for infrastructure; design a strategy for data and applications; and recommend security best practices and priorities.

[Schedule exam >](#)

United States

\$165 USD*

Price based on the country or region in which the exam is proctored.

Official practice test for Microsoft Cybersecurity Architect
All objectives of the exam are covered in depth so you'll be ready for any question on the exam.

Skills measured

- The English language version of this exam was updated on November 4, 2022. Download the study guide in the preceding "Tip" box for more details about the skills measured on this exam.
- Design a Zero Trust strategy and architecture (30-35%)
- Evaluate Governance Risk Compliance (GRC) technical strategies and security operations strategies (10-15%)
- Design security for infrastructure (10-15%)
- Design a strategy for data and applications (15-20%)
- Recommend security best practices and priorities (20-25%)

Figure 0.8 – SC-100 exam page

As you continue to prepare for the SC-100 exam, it is recommended that you use this exam page as a reference.

You should now have access to log in and browse the content on Microsoft Learn. The next section will help you sign up for a trial subscription to Microsoft 365 services and sign up for a month of free Azure services.

Creating a Microsoft 365 trial subscription

If you are new to Microsoft 365 and Azure, getting hands-on experience is important not just for exam preparation, but also for professional development. If you are getting certified to open doors to new job opportunities, you must understand the administration portals and how to work within them. This book will provide some exercises that will get you familiar with how to work within Microsoft 365, advanced security and compliance solutions, and Azure Active Directory. To follow along with these steps, it is recommended that you have a subscription to **Microsoft 365** and **Enterprise + Mobility**. The steps for creating these while using a 30-day trial will be provided in the next few sections.

Office 365 or Microsoft 365 trial subscription

Many of the features and capabilities discussed within the exam objectives require an enterprise-level license within Microsoft 365. The available enterprise licenses are **E3** and **E5**. Microsoft offers 30-day trial licenses of these, so as you prepare for the exam, you can create this trial subscription and be able to follow along with the exercises.

To get started, navigate to <https://www.microsoft.com/en-us/microsoft-365/enterprise/compare-office-365-plans> and select **Try for free** under the **Office 365 E5** plan:



Figure 0.9 – Office 365 trial subscription sign-up

Follow the steps to create an account, as shown in the following screenshot. If you have already created an account, you may need to use a different email address to obtain the free trial:

A screenshot of the Microsoft Office 365 E5 trial sign-up form. The form is titled "Office 365 E5 Trial" and indicates "One month free with payment details". It consists of three main sections: "About you", "Sign-in details", and "Payment info and finish". The "About you" section shows a progress bar with three steps: "About you" (selected), "Sign-in details", and "Payment info and finish". Below the progress bar, the heading "Let's get you started" is displayed. A placeholder text "Enter your work or school email address, we'll check if you need to create a new account for Office 365 E5 Trial." is present, followed by an "Email" input field with a note "This is required" and a "Next" button. To the right of the form, there is a sidebar titled "What is Office 365 E5 Trial?". It lists "Fully installed Office apps for PC and Mac" (Word, Excel, PowerPoint, OneDrive, Access, Project) and "Premium services" (Teams, SharePoint, Yammer, OneDrive, Planner, Power BI). There is also a small chart icon at the bottom of the sidebar.

Figure 0.10 – Office 365 E5 subscription sign-up form

After completing the form and creating your Microsoft 365 tenant, you will have access to Microsoft 365 services and the administration panel. The next section will guide you through signing up for an additional add-on service that will be required to follow along with the exercises within this book and full hands-on preparation for your exam.

Enterprise Mobility + Security subscription

In addition to the Office 365 E5 trial subscription, you will need access to advanced security and compliance features and an Azure Active Directory Premium license for many of the solutions and services that will be discussed within the exam objectives. The best way to obtain these features is through an **Enterprise Mobility + Security E5** license. Microsoft also offers this as a 30-day free trial. Follow these steps:

1. To get started, navigate to <https://www.microsoft.com/en-us/microsoft-365/enterprise-mobility-security/compare-plans-and-pricing>.
1. Then, select **Try now** under the **Enterprise Mobility + Security E5** plan, as shown in the following screenshot:

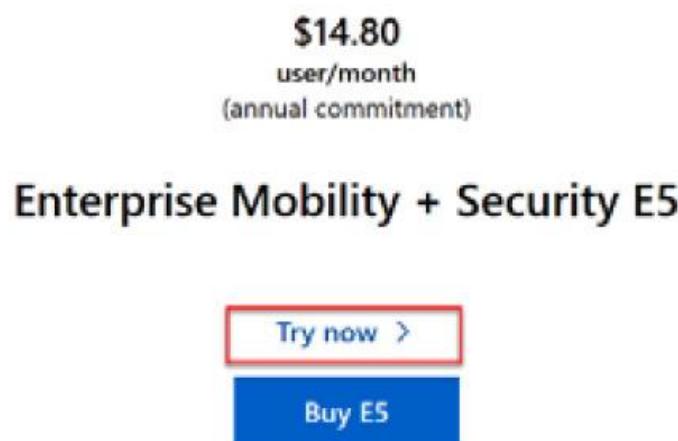


Figure 0.11 – EMS E5 trial subscription sign-up

This is an add-on license for Microsoft 365, so you should enter the same email address that you used to sign up for the Office 365 E5 subscription in the box shown in the following screenshot:

Thank you for choosing **Enterprise Mobility + Security E5**

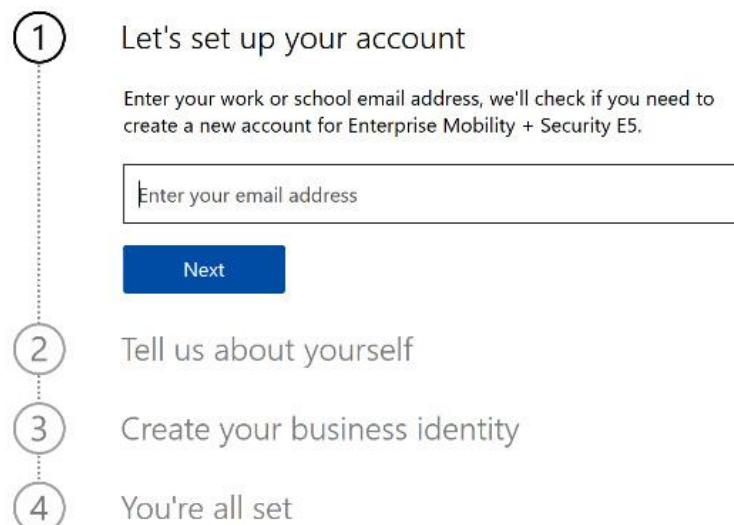


Figure 0.12 – EMS E5 subscription sign-up form

You should now have everything that you need for your hands-on exam preparation and to follow along with the exercises within this book. The next section will provide an overview of the objectives that will be covered in the exam and throughout this book.

Setting up a free month of Azure services

Since this exam includes security, compliance, and identity services for Microsoft 365 and Azure, it is recommended that you have access to Azure as well. Microsoft offers a free month of services from Azure. If you have not taken advantage of this offer previously, you can sign up at <https://azure.microsoft.com/>.

From here, you can select **Free account** at the top right or **Get started for free** in the middle of the page, as shown in the following screenshot:

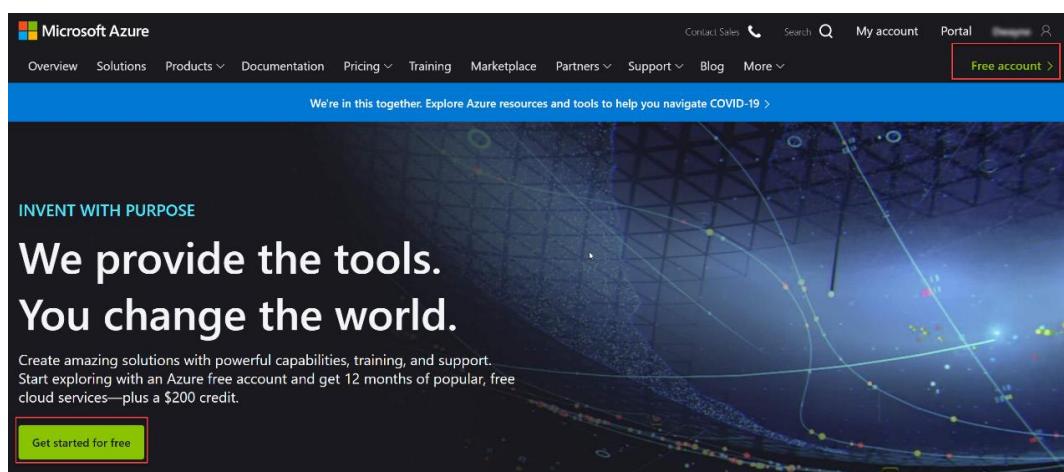


Figure 0.13 – Microsoft Azure sign-up page

In the next section, we will discuss the objectives of the exam and how they are weighted for each objective to assist in your exam preparation.

Figures

How do you want to take your exam? [Exam delivery option descriptions](#)

- At a local test center
- Online from my home or office
- I have a Private Access Code

Figure 0.1 – Location selection when scheduling your exam



Figure 0.2 – Microsoft Learn site – Sign in

Certification details

Complete one prerequisite

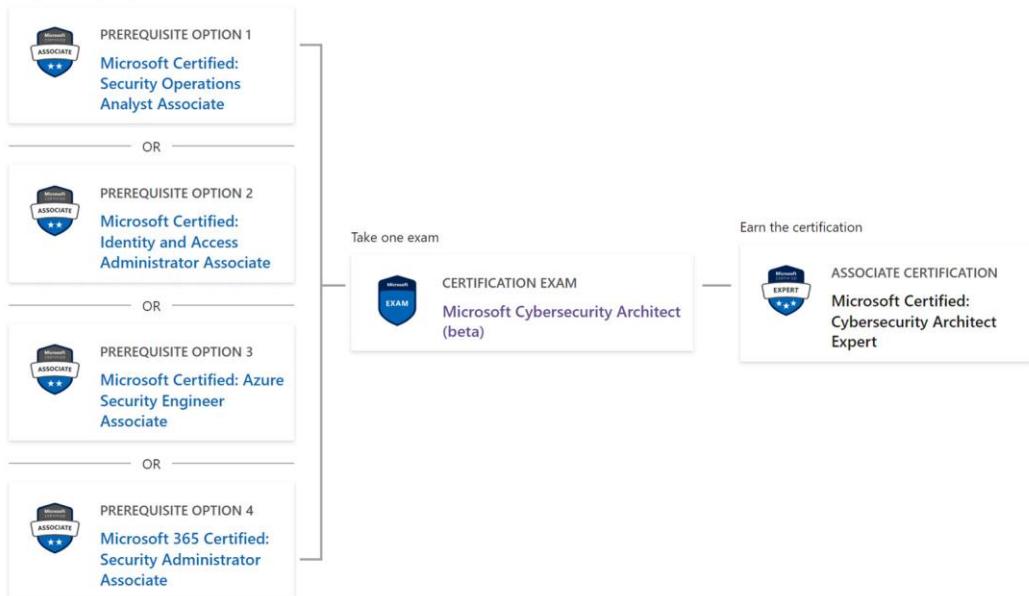


Figure 0.14 – Cybersecurity Architect Expert certification details

Table

Objective	Weight
Design a zero-trust strategy and architecture	30-35%
Evaluate Governance, Risk, and Compliance (GRC) technical strategies and security operations strategies	20-25%
Design security for infrastructure	20-25%
Design a strategy for data and applications	20-25%

Table 0.1 – Exam objectives

Links

More information can be found at <https://docs.microsoft.com/en-us/learn/certifications/exams/sc-100>.

To access and search Microsoft docs, simply go to <https://docs.microsoft.com>.

The Microsoft Cybersecurity Architect learning path on Microsoft Learn can be found at <https://docs.microsoft.com/en-us/learn/certifications/exams/sc-100>.

The lab guides can be found at <https://github.com/MicrosoftLearning>.

Additional details on the topics that make up these objectives can be found at
<https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWVbXN>.

Chapter 1

Figures

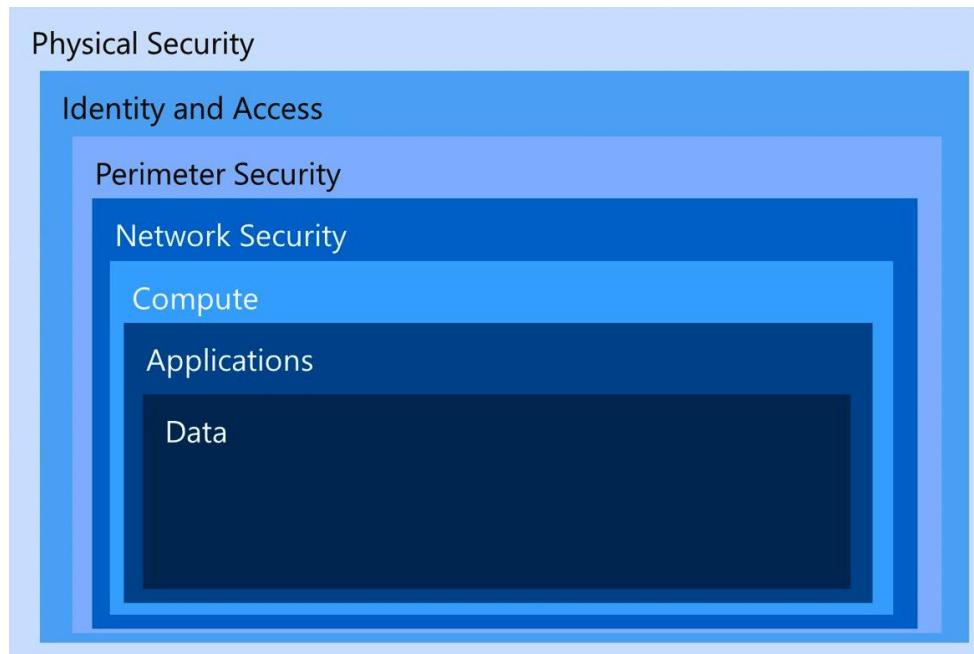


Figure 1.1 – Defense-in-depth security

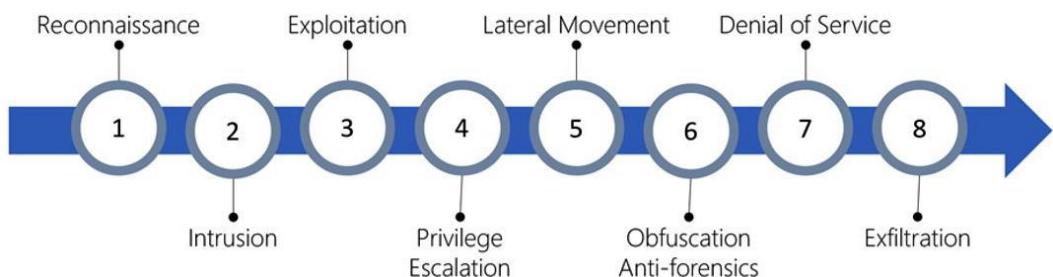


Figure 1.2 – Stages of a cyber attack



Figure 1.3 – Diagram of the zero-trust model architecture

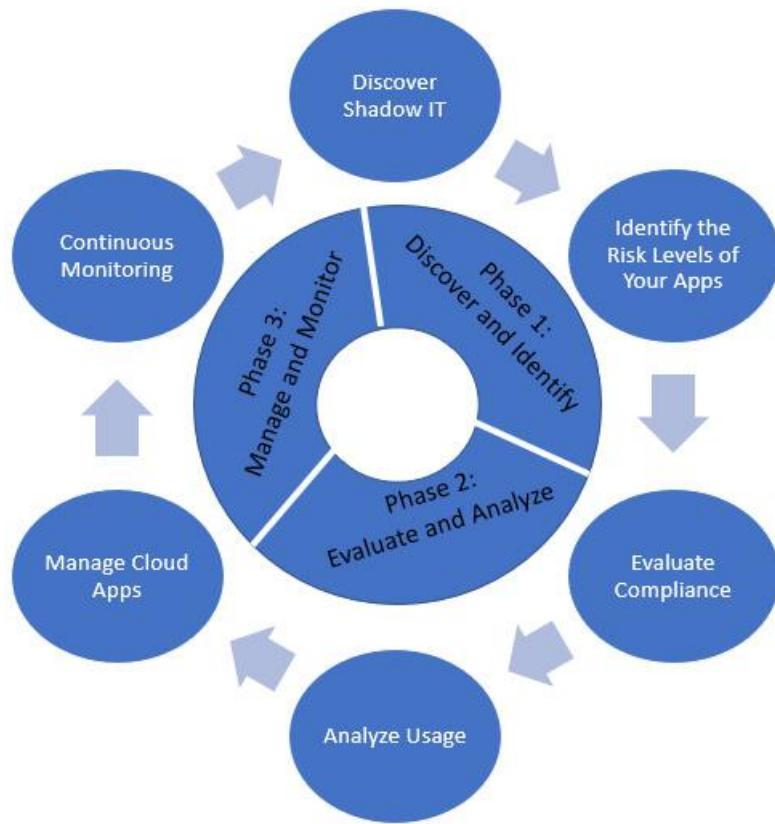


Figure 1.4 – Shadow IT prevention life cycle

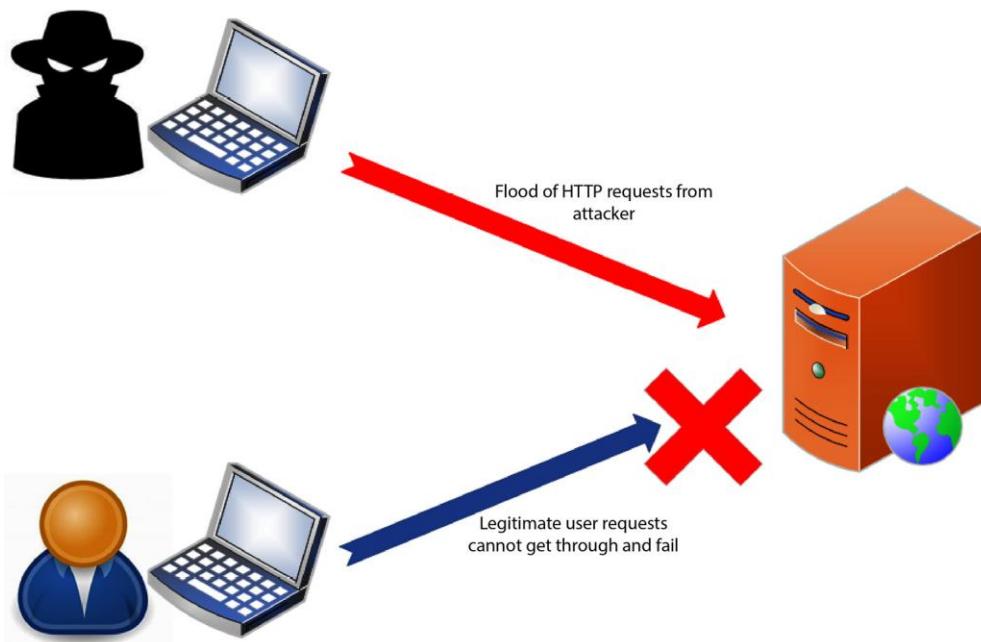


Figure 1.5 – A denial-of-service attack

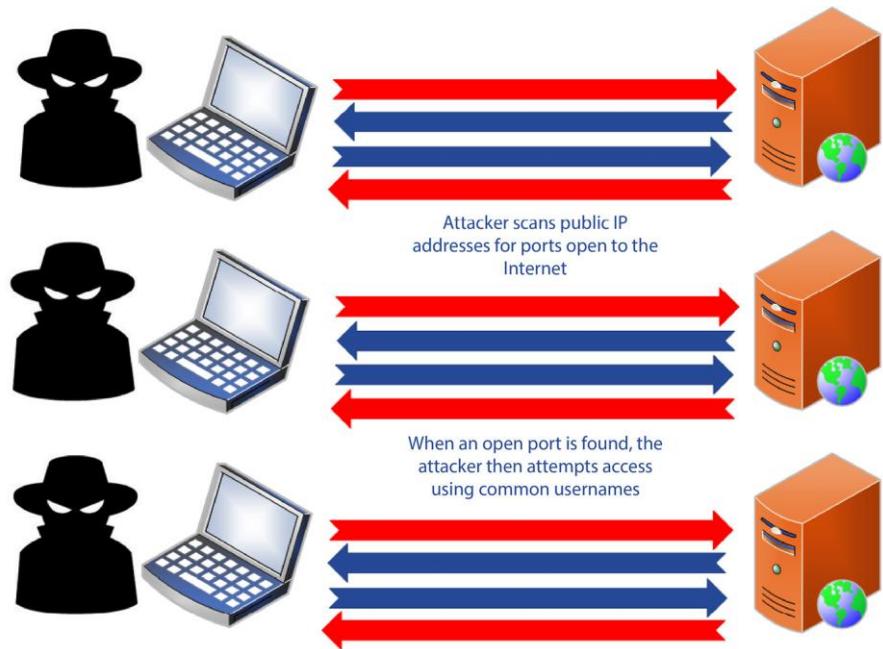


Figure 1.6 – A brute-force attack

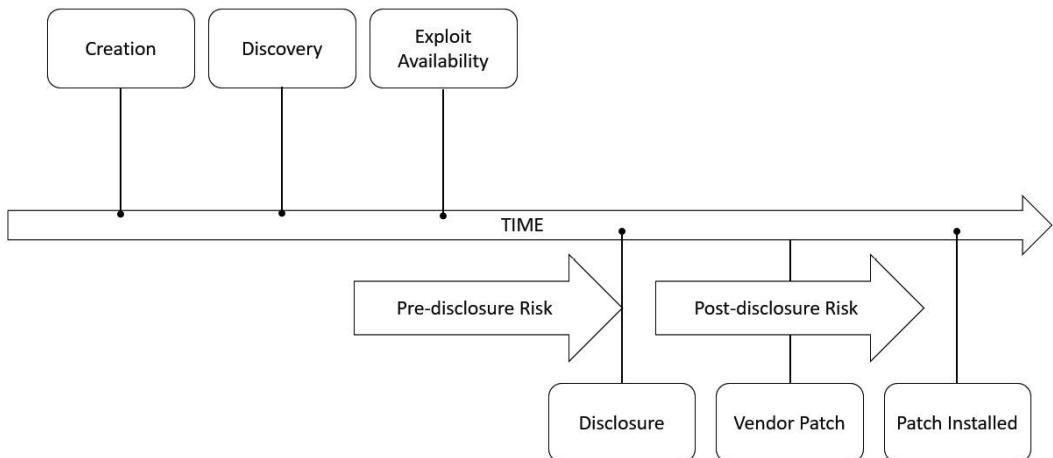


Figure 1.7 – Vulnerability exploit life cycle

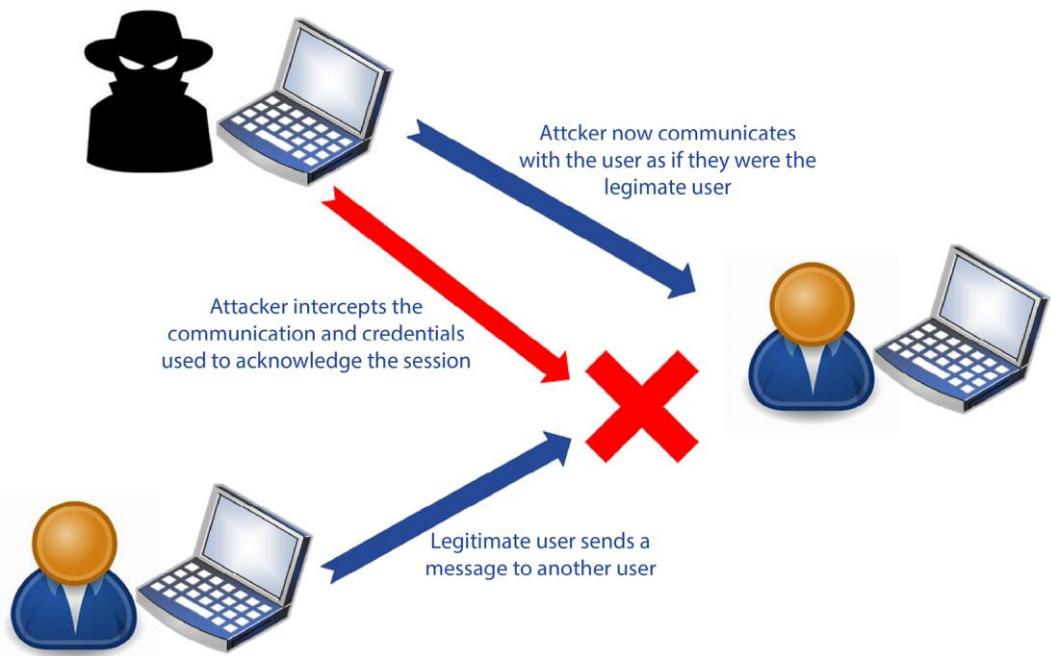


Figure 1.8 – Identity spoofing

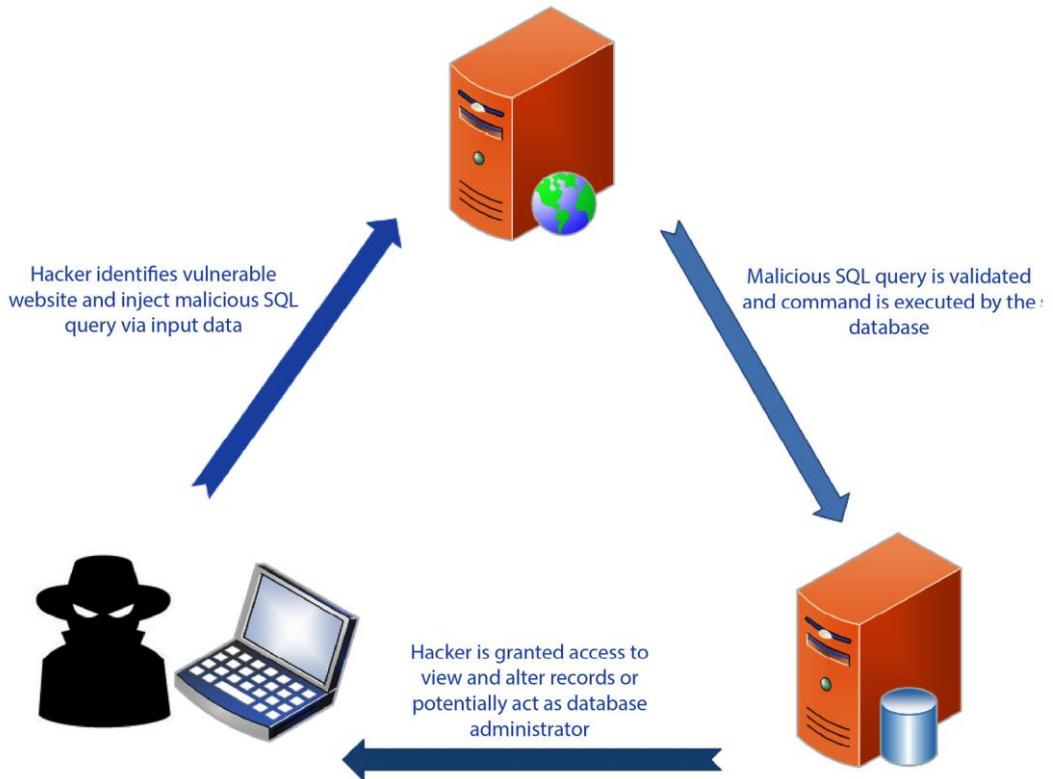


Figure 1.9 – A SQL injection attack

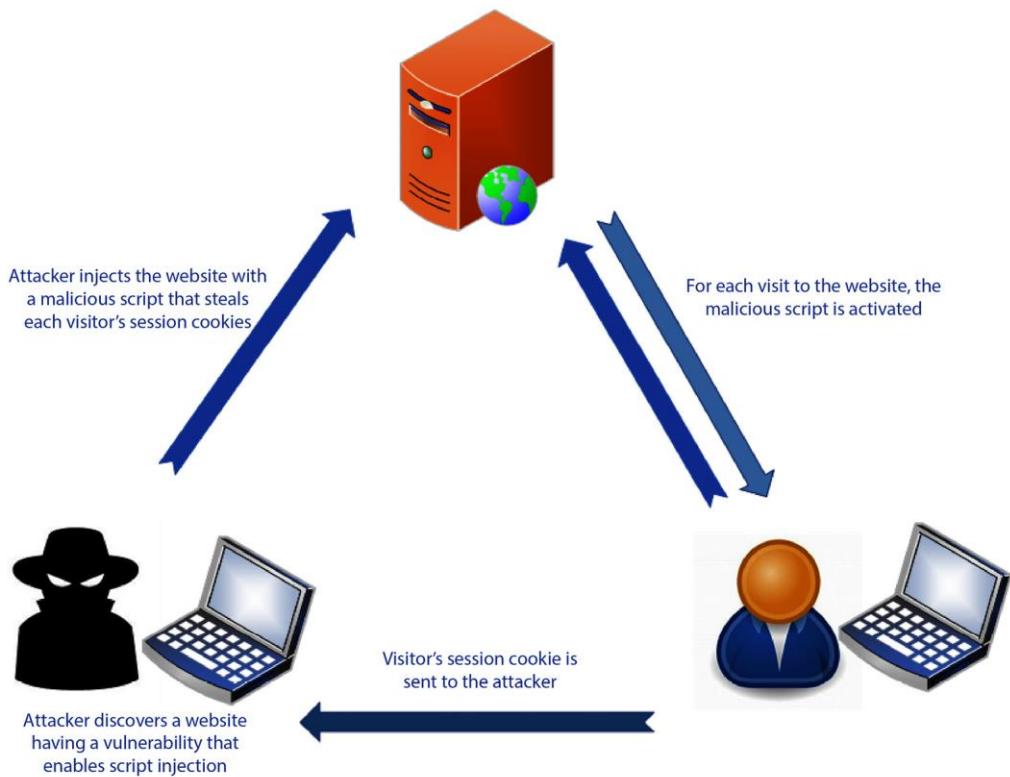


Figure 1.10 – A cross-site scripting attack

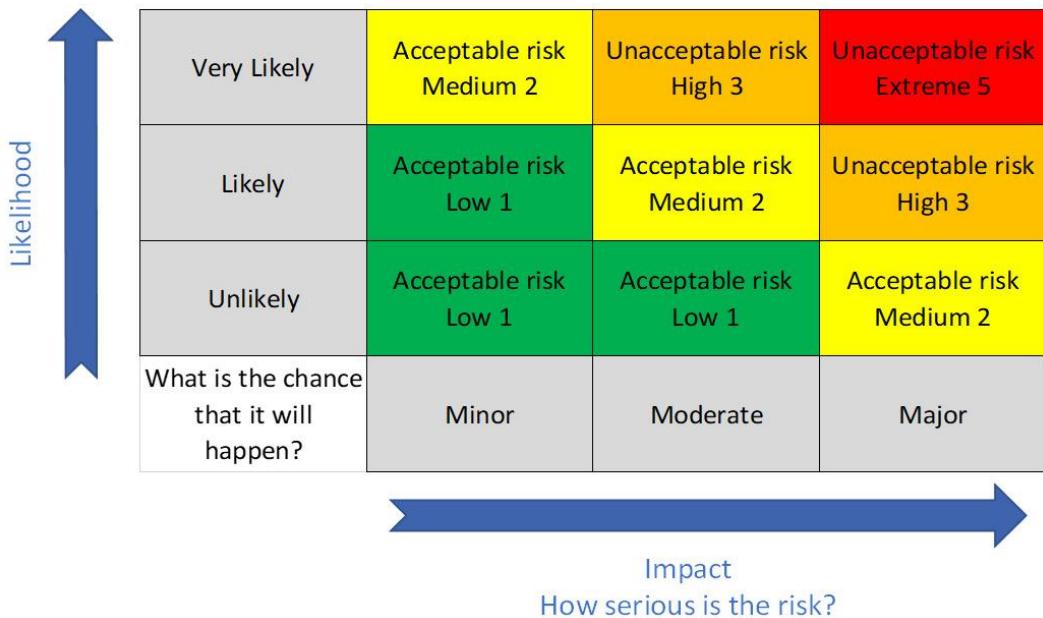


Figure 1.11 – Security risk

Table

Responsibility	On-Premises	IaaS	PaaS	SaaS
Data governance and rights management	Customer	Customer	Customer	Customer
Client endpoints	Customer	Customer	Customer	Customer
Account and access management	Customer	Customer	Customer	Customer
Identity and directory infrastructure	Customer	Customer	Microsoft/ Customer	Microsoft/ Customer
Application	Customer	Customer	Microsoft/ Customer	Microsoft
Network controls	Customer	Customer	Microsoft/ Customer	Microsoft
Operating system	Customer	Customer	Microsoft	Microsoft
Physical hosts	Customer	Microsoft	Microsoft	Microsoft
Physical network	Customer	Microsoft	Microsoft	Microsoft
Physical data center	Customer	Microsoft	Microsoft	Microsoft

Table 1.1 – Shared responsibility in the cloud

Responsibility	IaaS	PaaS	SaaS
Data governance and rights management	Customer	Customer	Customer
Client endpoints	Customer	Customer	Customer
Account and access management	Customer	Customer	Customer
Identity and directory infrastructure	Customer	Microsoft/ Customer	Microsoft/ Customer
Application	Customer	Microsoft/ Customer	Microsoft
Network controls	Customer	Microsoft/ Customer	Microsoft
Operating system	Customer	Microsoft	Microsoft
Physical hosts	Microsoft	Microsoft	Microsoft
Physical network	Microsoft	Microsoft	Microsoft

Responsibility	IaaS	PaaS	SaaS
Physical data center	Microsoft	Microsoft	Microsoft

Table 1.2 – Shared responsibility for SaaS, PaaS, and IaaS

Links

Further information can be found at this link: <https://csrc.nist.gov/glossary/term/cybersecurity>. At this link, you will find the definition of cybersecurity and the various approaches that can be taken toward it.

For more information on the MITRE ATT&CK framework, go to this link: <https://attack.mitre.org/>

When architecting a security operations infrastructure, many solutions utilize the MITRE ATT&CK for hunting and identifying threats. For more information, please use the following link: <https://attack.mitre.org/matrices/enterprise/cloud/>.

The **Cloud Security Alliance (CSA)** also provides guidance about common attacks and threats to cloud environments. More information can be found at this link:

<https://cloudsecurityalliance.org/press-releases/2019/08/09/csa-releases-new-research-top-threats-to-cloud-computing-egregious-eleven/>

A great resource to keep up with the most current risks is the **OWASP Top Ten Web Application Security Risks**: <https://owasp.org/www-project-top-ten/>.

Chapter 2

Figures

Microsoft Cybersecurity Reference Architecture (MCRA)

Capabilities	Azure Native Controls	People
Zero Trust User Access	Security Operations	Multi-Cloud and Cross-Platform
Secure Access Service Edge (SASE)	Attack Chain Coverage	Operational Technology

Figure 2.1 – MCRA topics

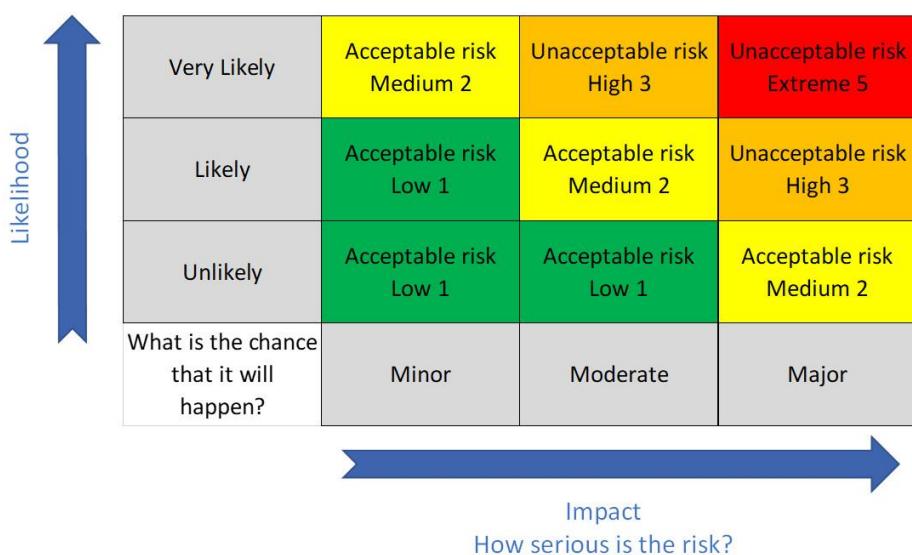


Figure 2.2 – Risk assessment matrix

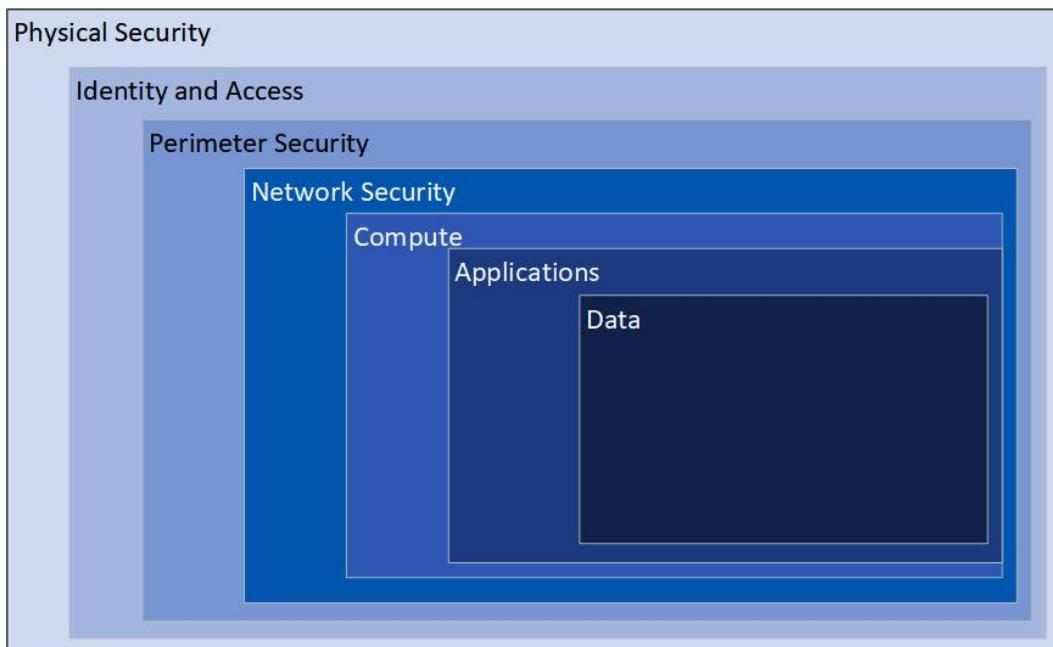


Figure 2.3 – Defense-in-depth security diagram

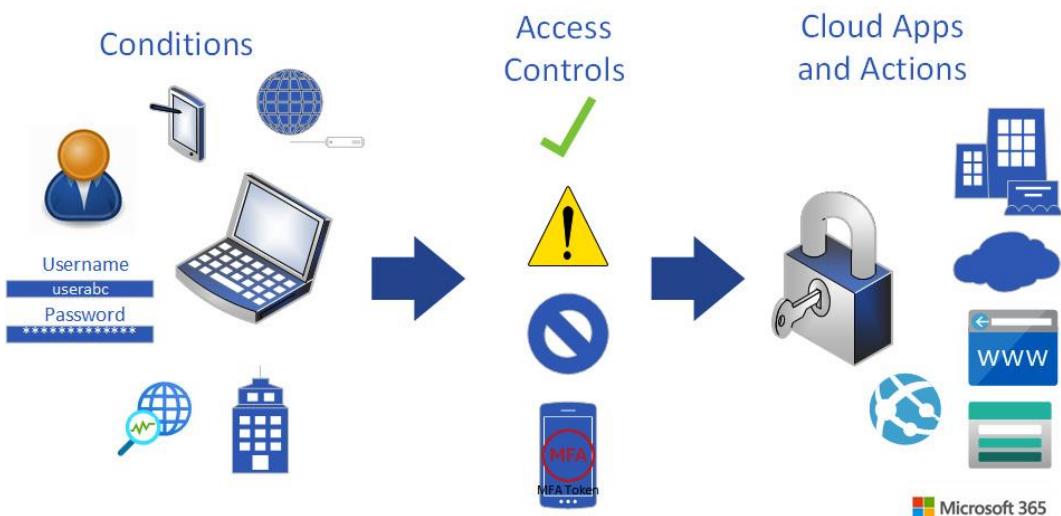


Figure 2.4 – Zero trust with Conditional Access

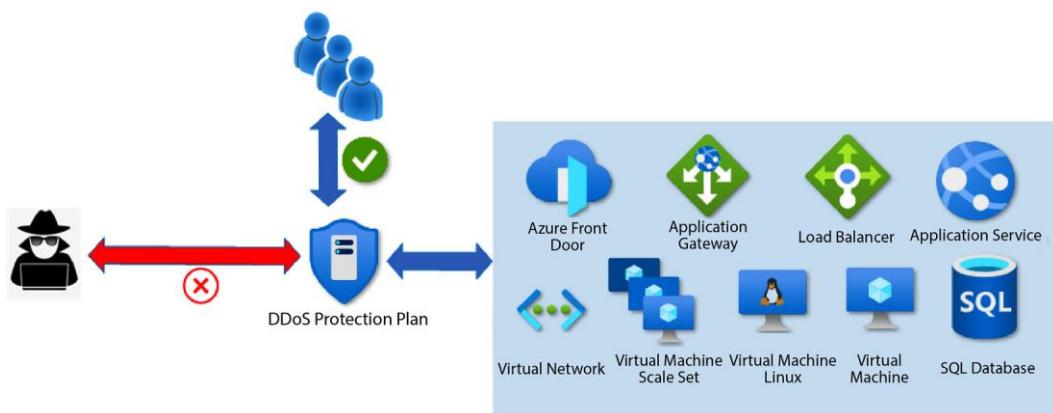


Figure 2.5 – Microsoft DDoS protection

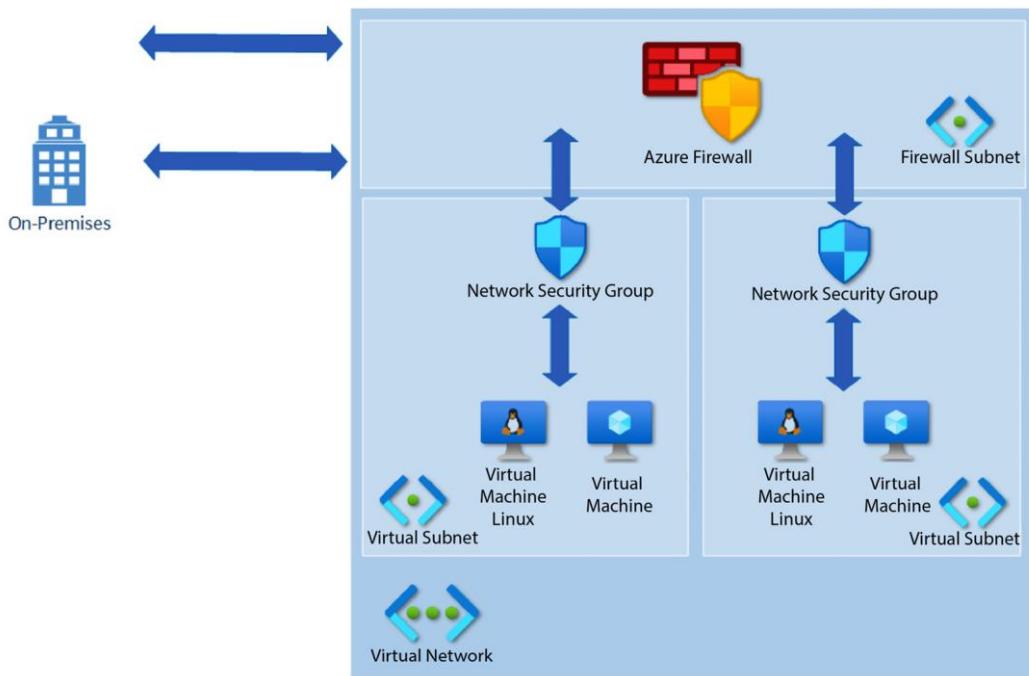


Figure 2.6 – Azure Firewall

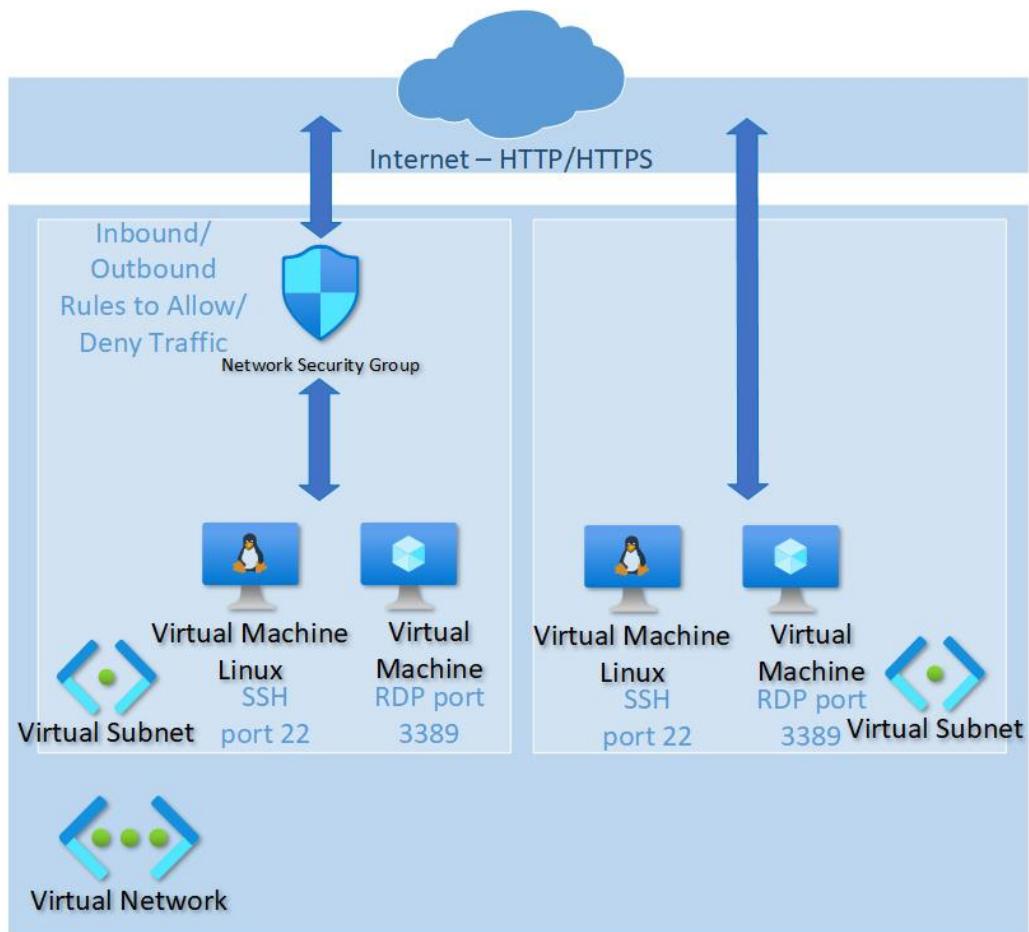


Figure 2.7 – Network security groups for network perimeter protection

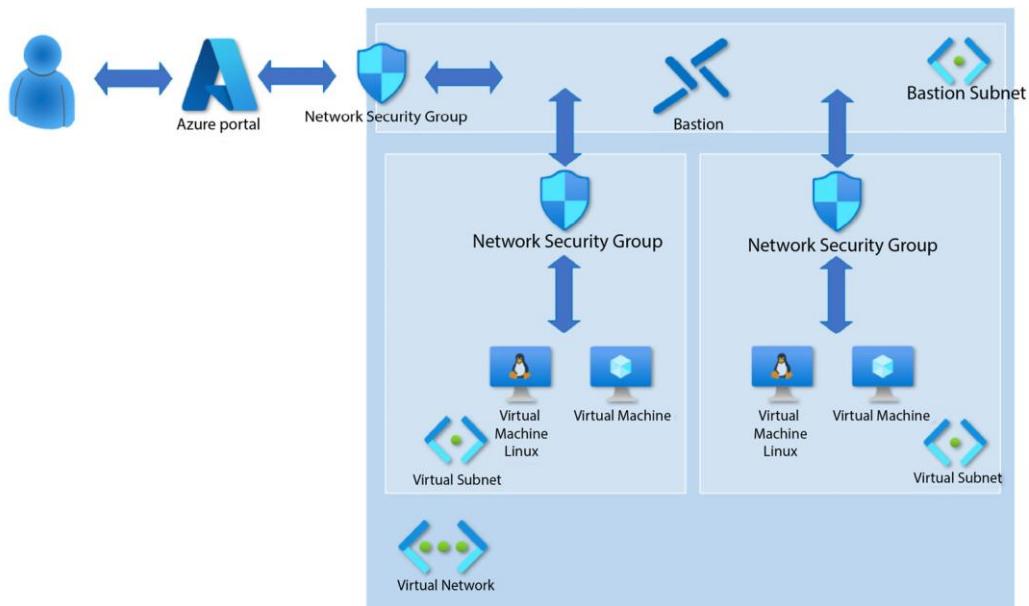


Figure 2.8 – Azure Bastion for virtual machine remote management

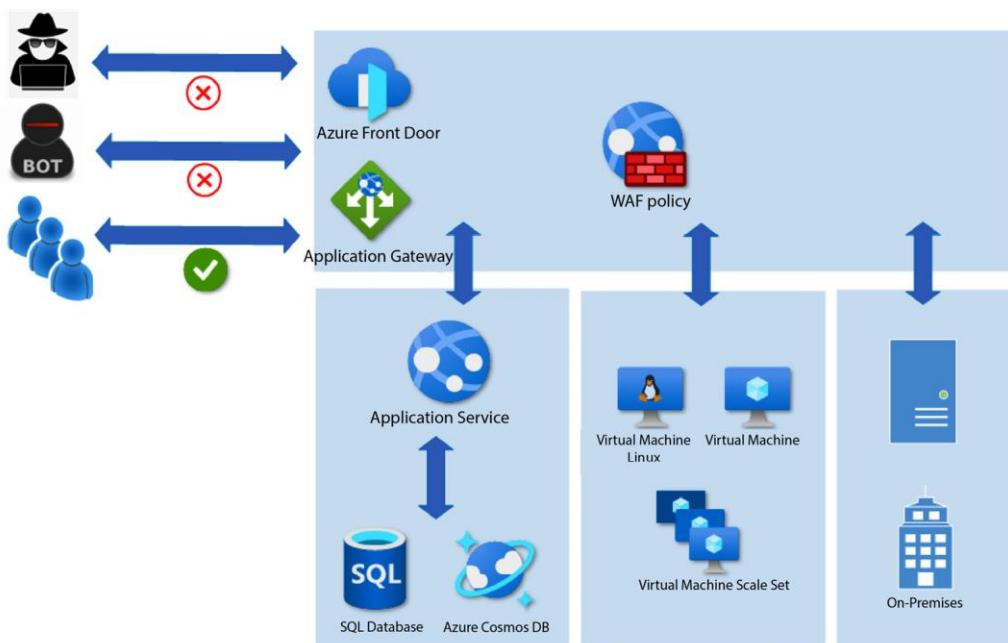


Figure 2.9 – Web application firewall diagram

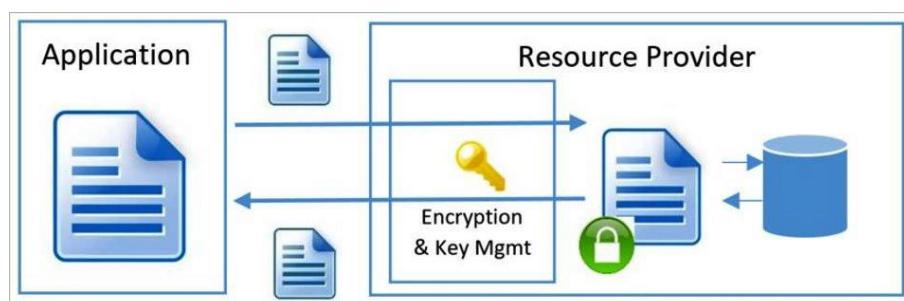


Figure 2.10 – Data encrypted at rest

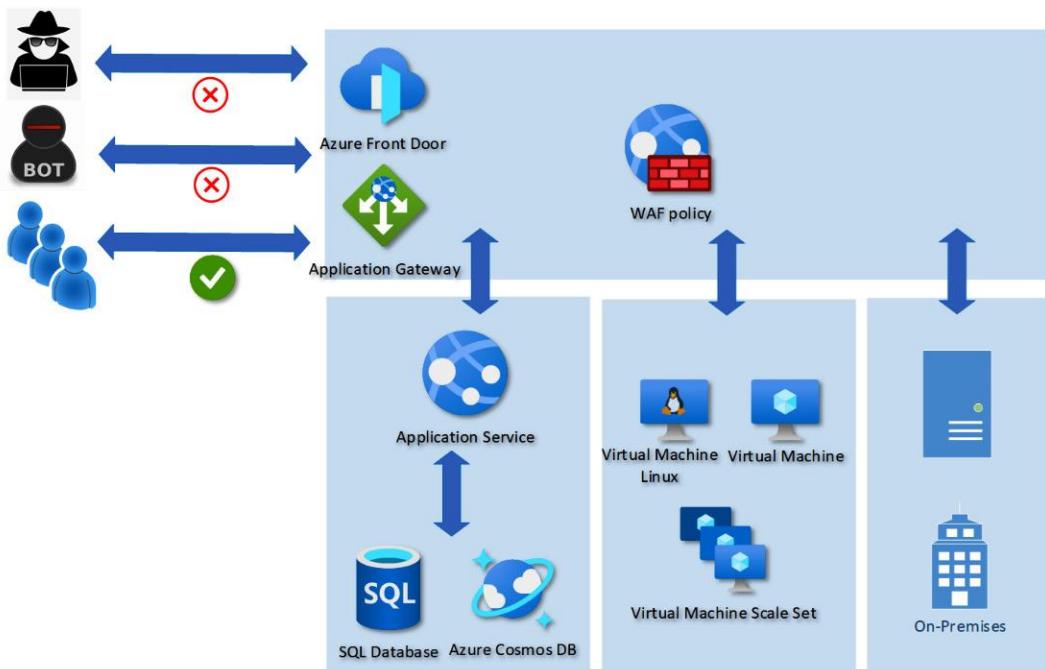


Figure 2.11 – WAF filtering traffic

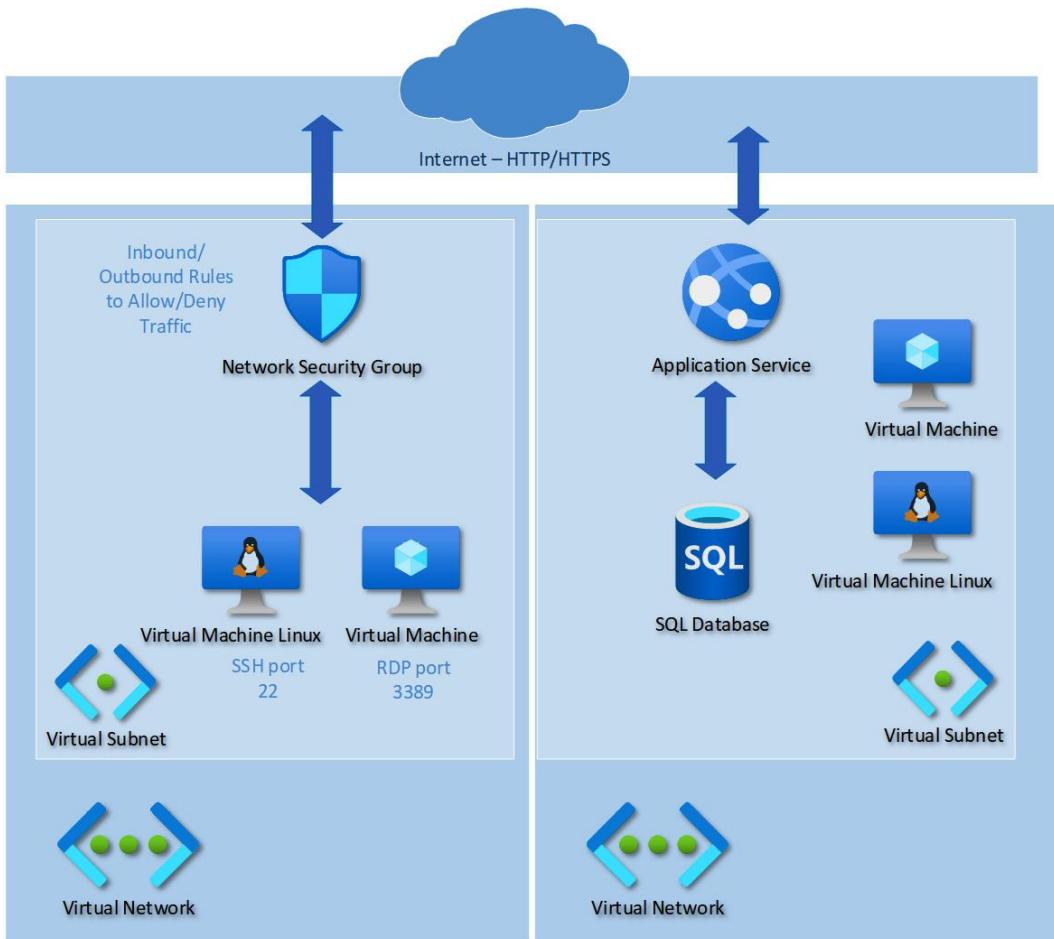


Figure 2.12 – Network segmentation

Links

The MCRA and the various diagrams and templates can be found at this link:

<https://docs.microsoft.com/en-us/security/cybersecurity-reference-architecture/mcra>.

The following is a good resource if you would like to learn more about cyber threat analysis:

<https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final>.

More information on physical security within Microsoft data centers can be found at this link:

<https://docs.microsoft.com/en-us/azure/security/fundamentals/physical-security#physical-security>.

The following link provides more information on Microsoft Entra: <https://docs.microsoft.com/en-us/entra/>.

More information on the OWASP Top 10 can be found at <https://owasp.org/www-project-top-ten/>

For guidance on resiliency and business continuity, NIST 800-160 provides some guidance here:

<https://csrc.nist.gov/publications/detail/sp/800-160/vol-2-rev-1/final>.

Chapter 3

Figures

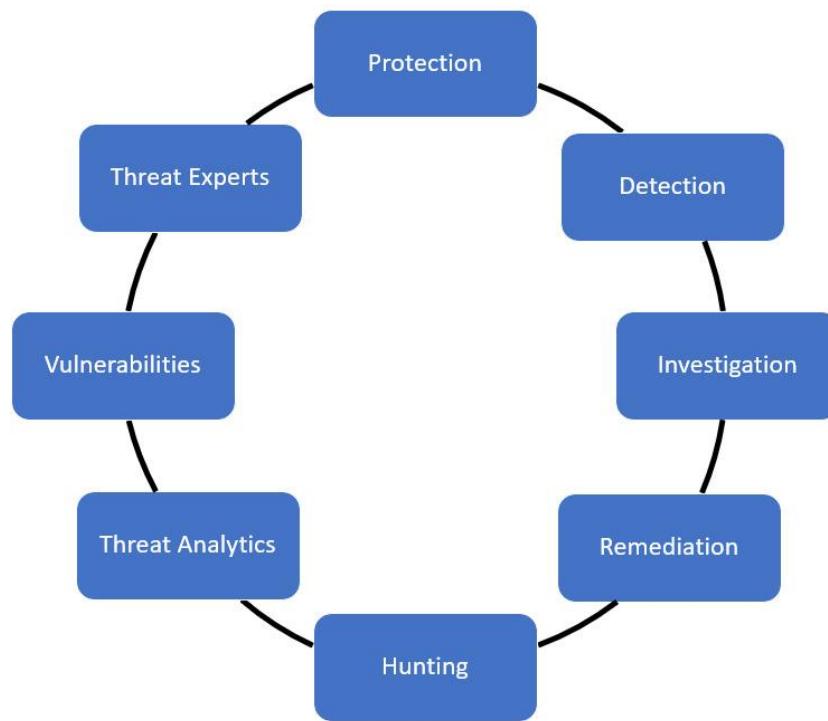


Figure 3.1 – Security operations strategy to manage threats



Figure 3.2 – Microsoft Defender for Cloud Apps Shadow IT protection

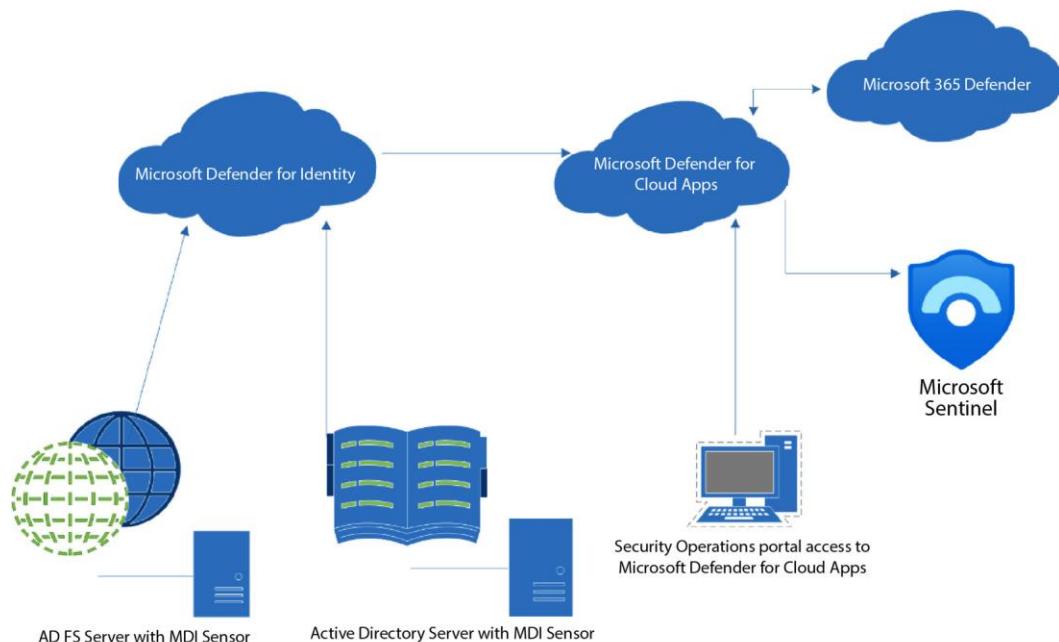


Figure 3.3 – Microsoft Defender for Identity

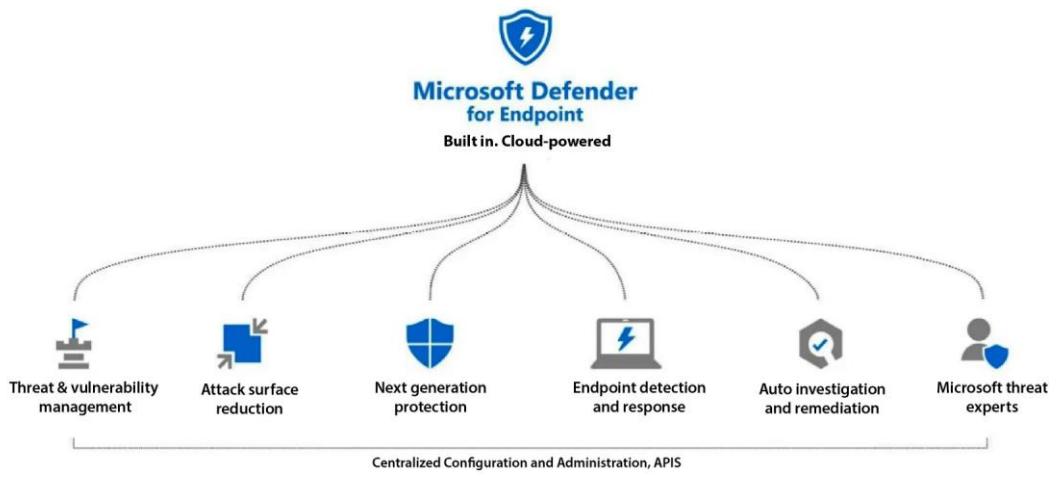


Figure 3.4 – Microsoft Defender for Endpoint



Figure 3.5 – Microsoft Defender for Office 365

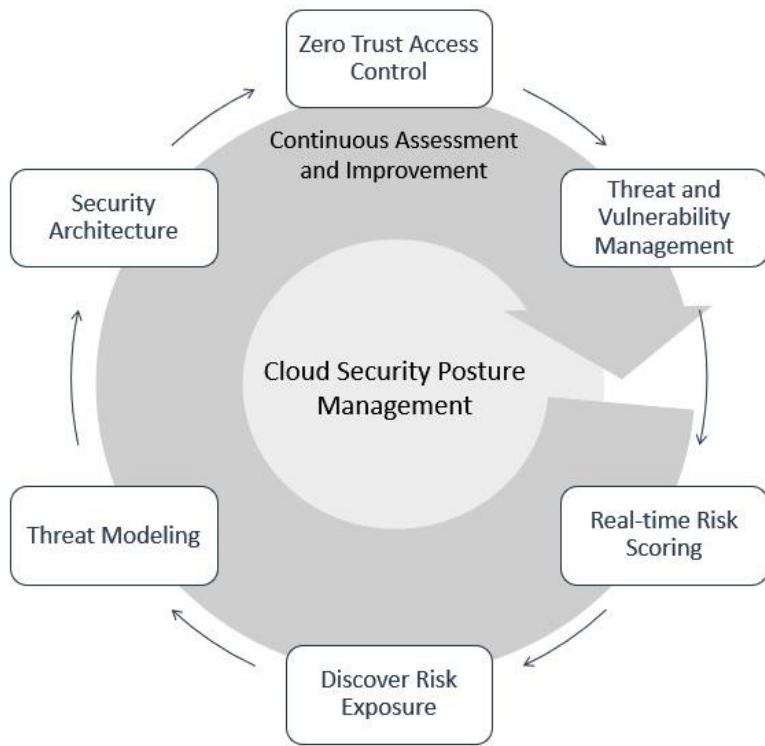


Figure 3.6 – Microsoft Defender for Cloud security posture management

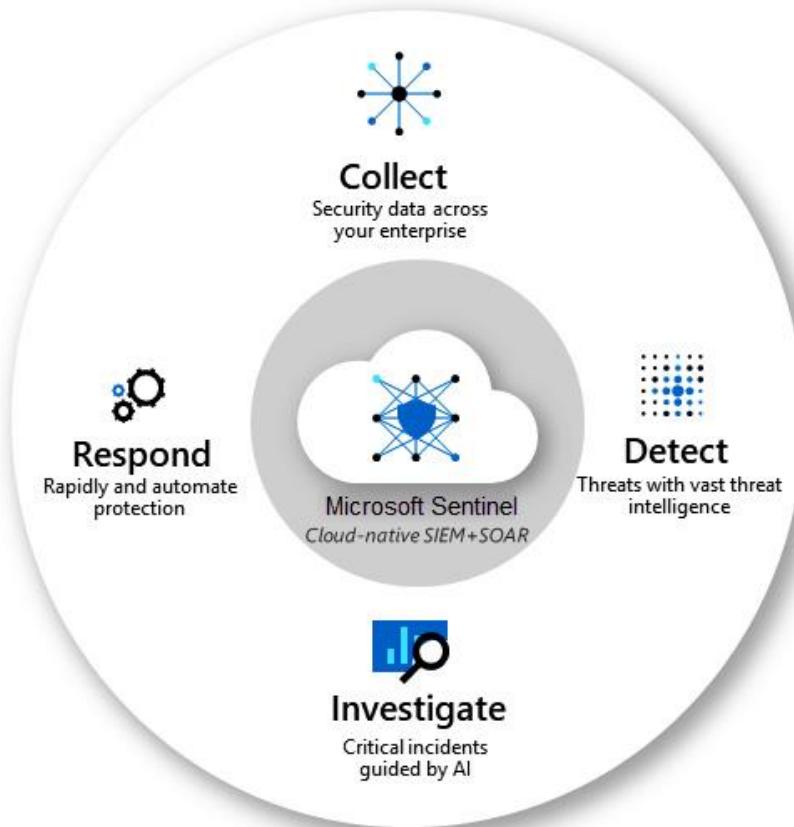


Figure 3.7 – Microsoft Sentinel SIEM and SOAR

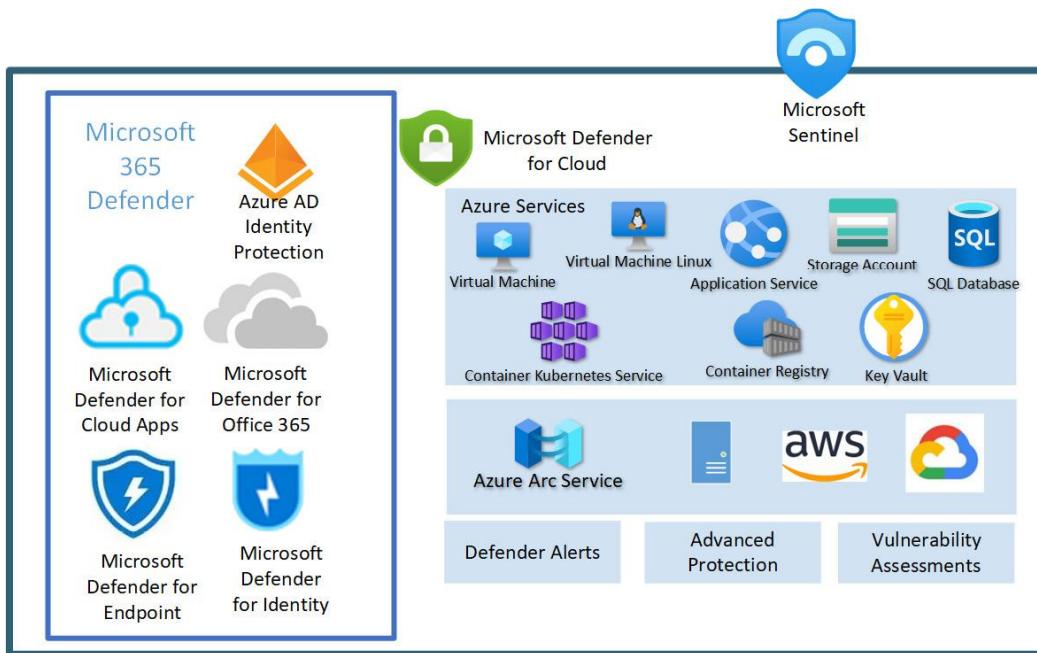


Figure 3.8 – Microsoft 365 Defender and Microsoft Sentinel

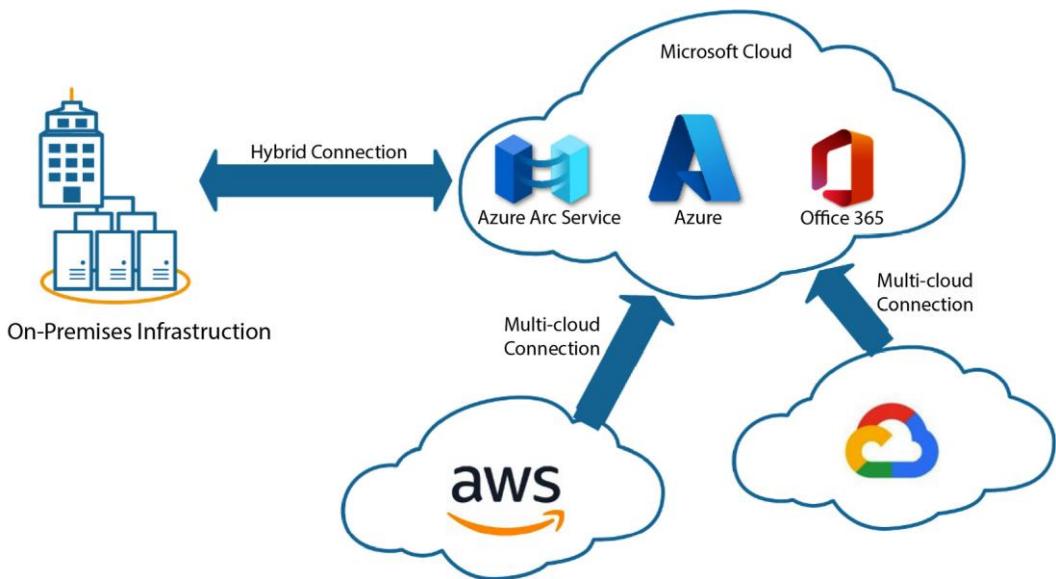


Figure 3.9 – Hybrid and multi-cloud architecture

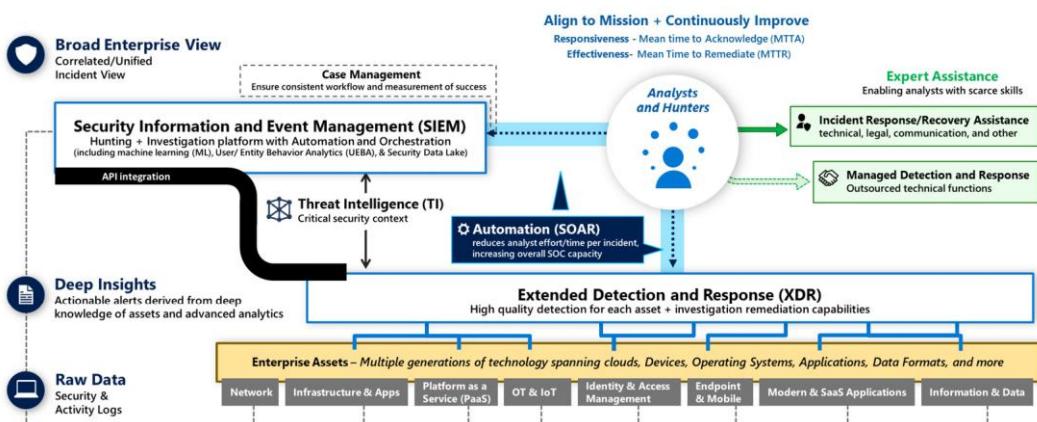


Figure 3.10 – Security operations technology usage

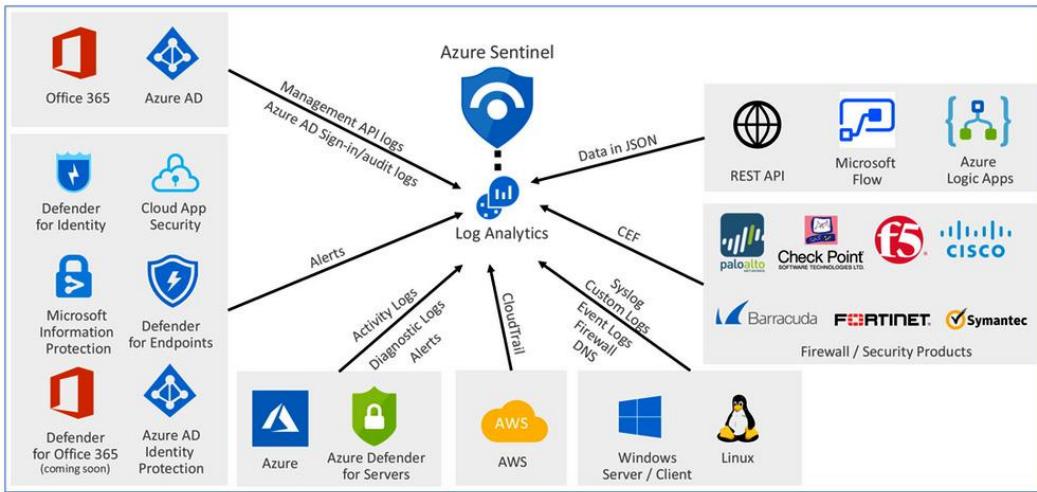


Figure 3.11 – Microsoft Sentinel architecture

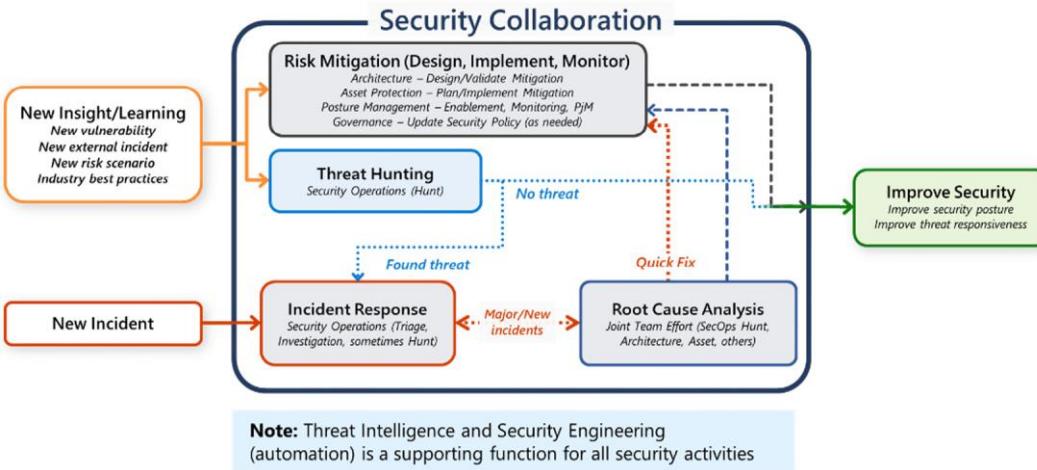


Figure 3.12 – Security operations continuous improvement process

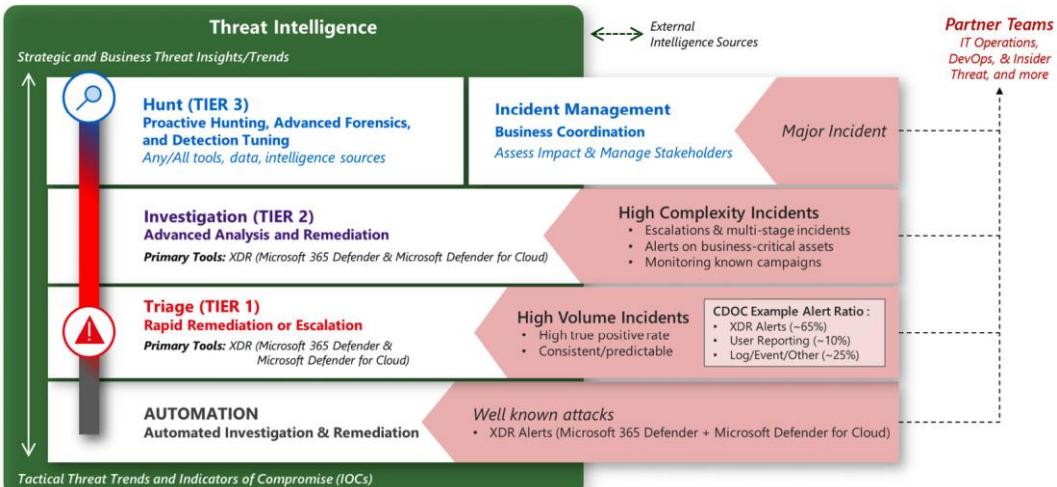


Figure 3.13 – Security operations functional tiers

Links

The Microsoft SOC model can be found at this link: <https://www.microsoft.com/en-us/security/blog/2019/02/21/lessons-learned-from-the-microsoft-soc-part-1-organization/>.

The Microsoft Security Development Lifecycle can be found here: <https://www.microsoft.com/en-us/securityengineering/sdl/>.

Microsoft Security Response Center program information can be found here:
<https://www.microsoft.com/en-us/msrc>.

MISA information can be found here: <https://www.microsoft.com/en-us/security/business/intelligent-security-association>.

For additional information on Microsoft's best practices for SIEM and SOAR, please review the MCRA: <https://docs.microsoft.com/en-us/security/cybersecurity-reference-architecture/mcra>.

More information on this approach can be found at this link:
<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>

More information on the Microsoft Graph Security API can be found at this link:
<https://docs.microsoft.com/graph/api/resources/security-api-overview?view=graph-rest-1.0>.

Information on Microsoft Threat Intelligence can be found at this link:
<https://www.microsoft.com/en-us/security/business/>

Microsoft also publishes information on the global threat landscape on the Microsoft Security Intelligence page, which can be found here: <https://www.microsoft.com/en-us/wdsi/threats>

Chapter 4

Figures

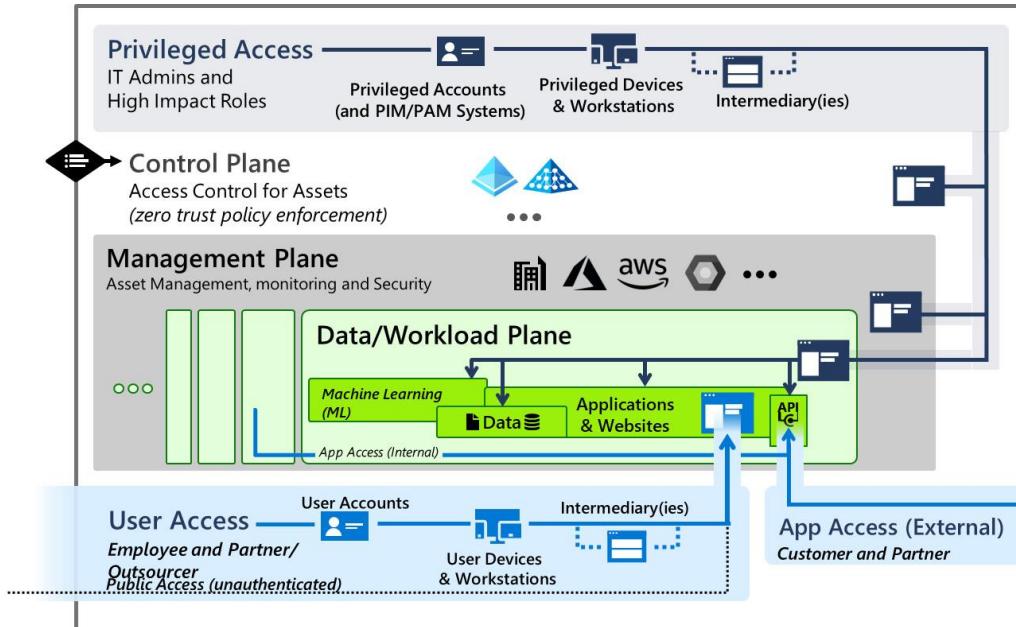


Figure 4.1: Identity and access control for secure access

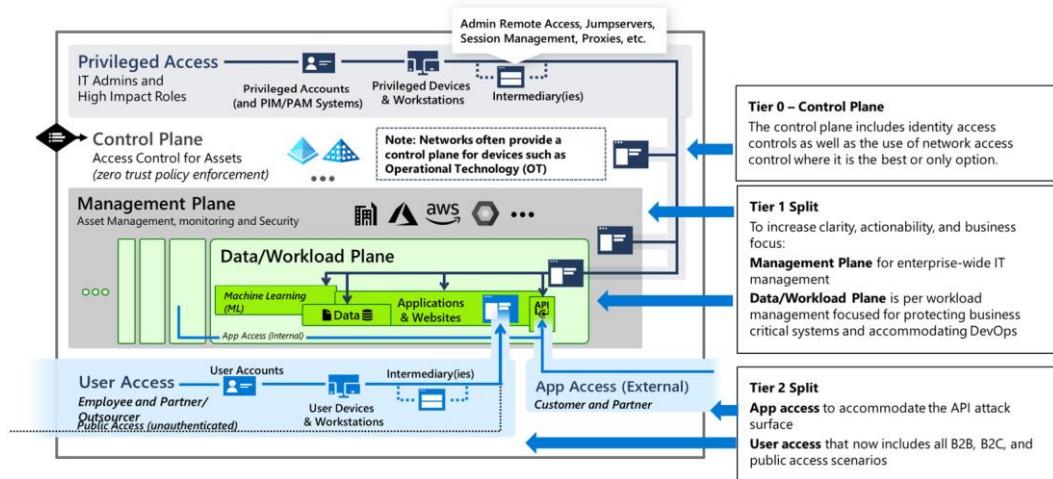


Figure 4.2: Identity and access model for the enterprise

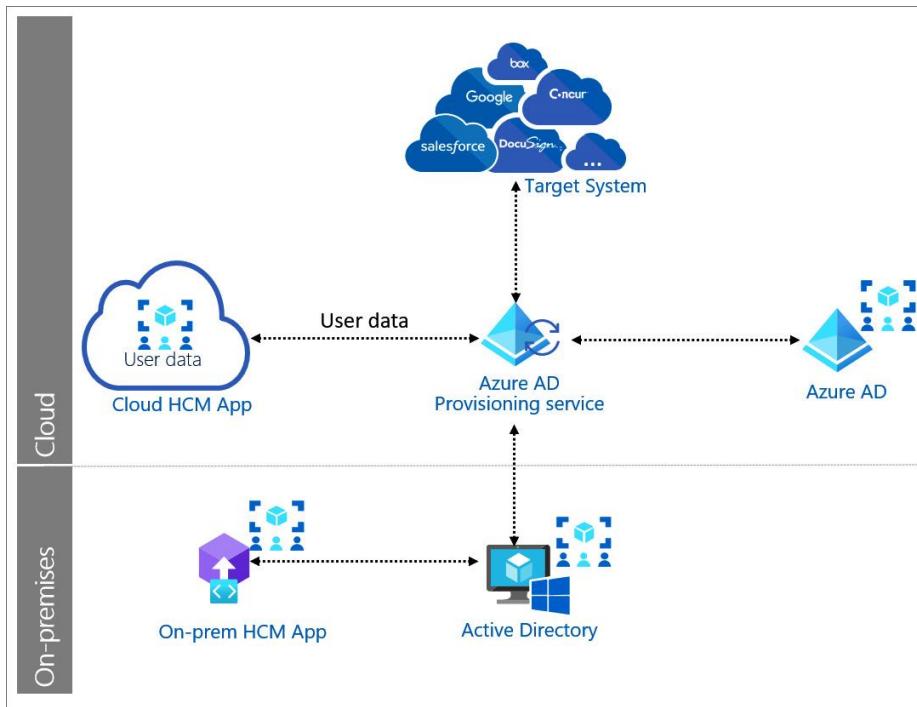


Figure 4.3: SCIM Azure AD provisioning diagram

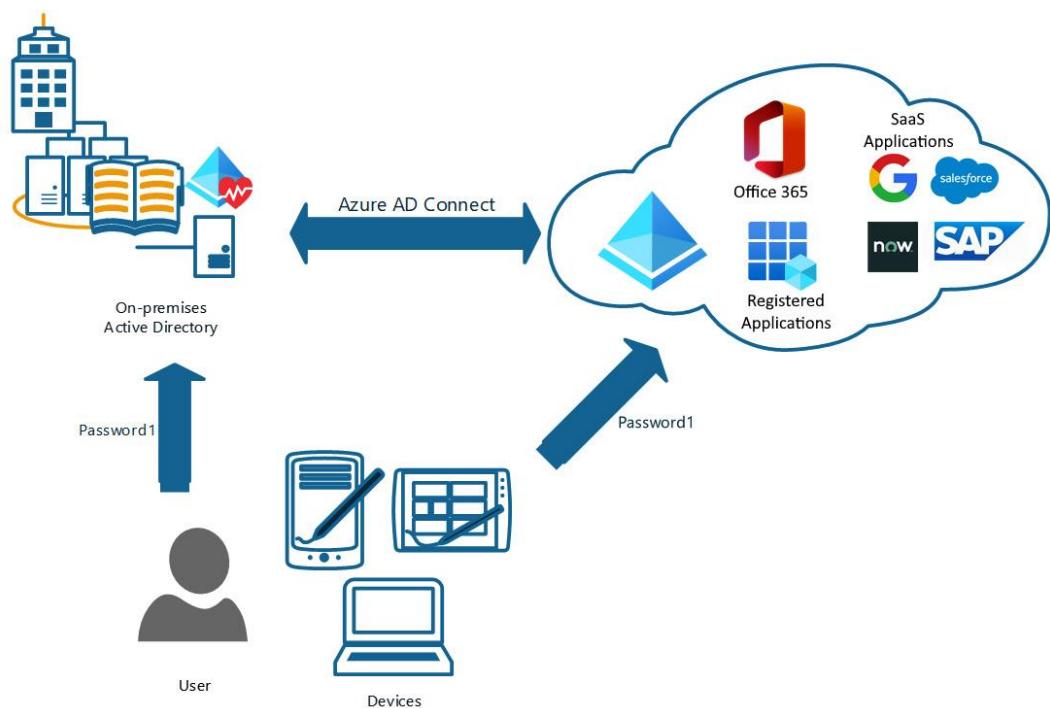


Figure 4.4: An overview of PHS

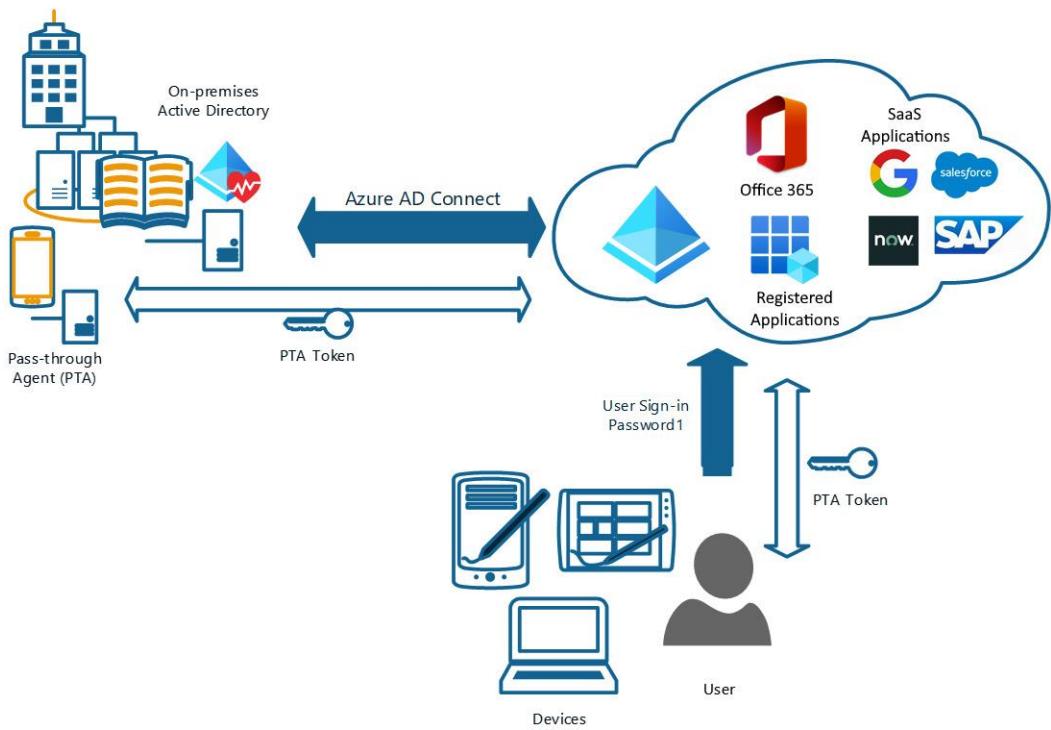


Figure 4.5: An overview of pass-through synchronization

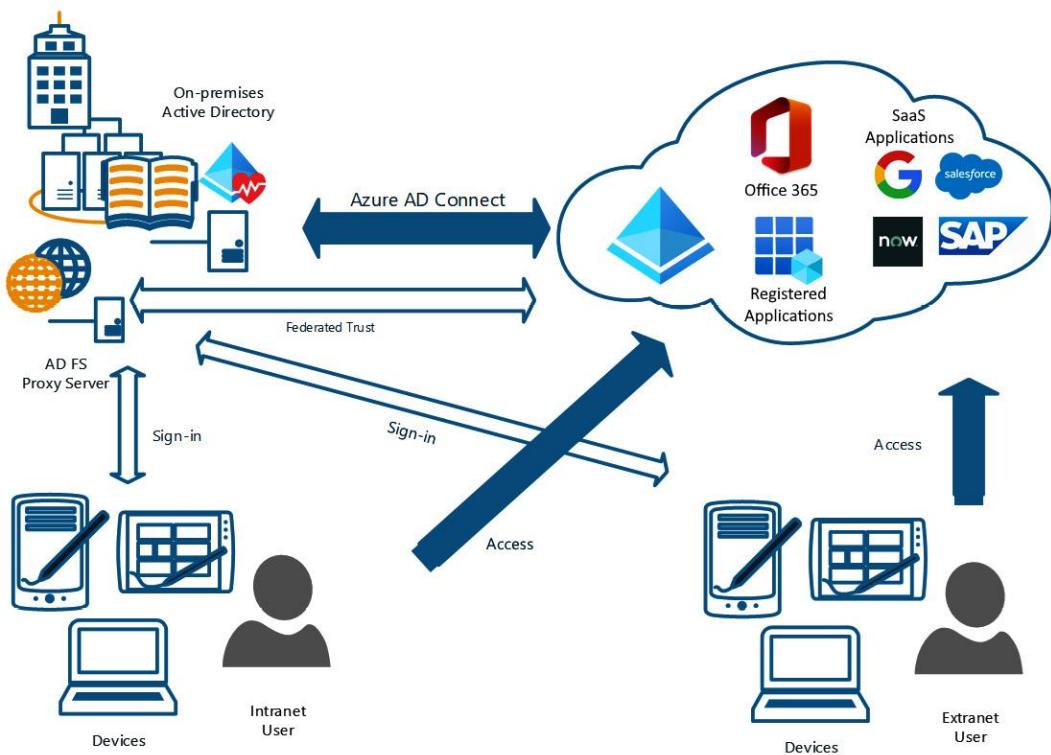


Figure 4.6: An overview of AD FS synchronization

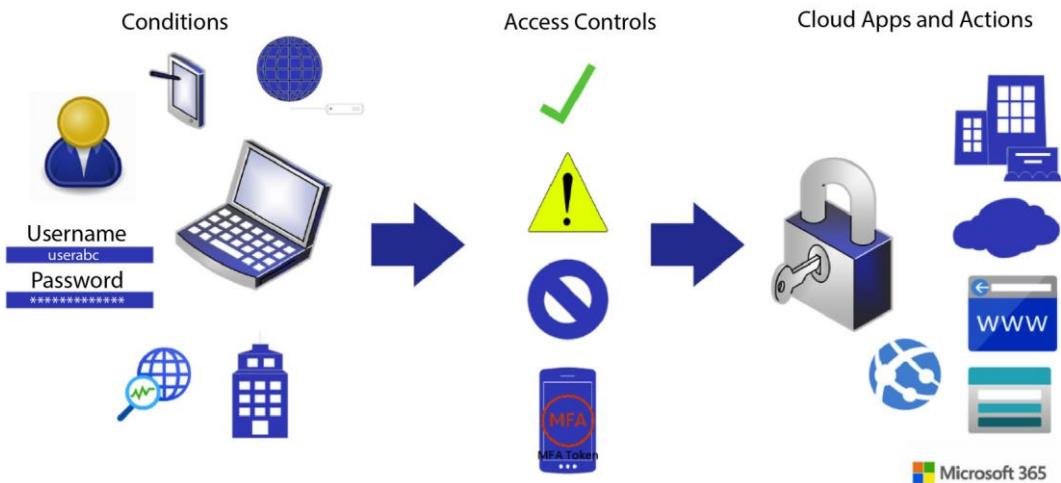


Figure 4.7: CA workflow

Links

For more information on how to use SCIM in Azure AD, please go to the following link:

<https://docs.microsoft.com/azure/active-directory/fundamentals/sync-scim>

There are some prerequisites and aspects that are out of scope within Azure AD Connect that you should understand. The installation prerequisites can be found at this link:

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-install-prerequisites>.

Additional information on PHS can be found at this link: <https://docs.microsoft.com/en-us/azure/active-directory/hybrid/what-is-phs>

For additional information on the configuration of AD FS synchronization, you can read more here: <https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-fed-management>.

The full list of licensing requirements can be found at this link:

<https://docs.microsoft.com/azure/active-directory/conditional-access/overview>

Some commonly used CA policies can be found on the Microsoft Docs website at this link:

<https://docs.microsoft.com/azure/active-directory/conditional-access/plan-conditional-access>

The differences between Microsoft 365 groups and security groups can be found at this link:

<https://learn.microsoft.com/en-us/microsoft-365/community/all-about-groups>.

Additional information on emergency access or “break-glass” accounts can be found at this link:

<https://docs.microsoft.com/en-us/azure/active-directory/roles/security-emergency-access>

Additional information on these stages for Cloud tenant administration can be found at this link:

<https://docs.microsoft.com/en-us/azure/active-directory/roles/security-planning>

Chapter 5

Figure

The screenshot shows the 'Settings | Defender plans' page in the Microsoft Azure portal. The 'Defender plans' section is selected in the left sidebar. A red box highlights the 'Save' button at the top left. The main area displays four Defender plans: 'Defender CSPM' (Free, N/A resources, Full monitoring coverage, On), 'Servers' (Plan 2 (\$15/Server/Mo), 6 servers, Partial monitoring coverage, On), 'App Service' (\$15/Instance/Month, 0 instances, Full monitoring coverage, On), and 'Databases' (Selected: 4/4, Protected: 1/1 instance, Full monitoring coverage, On). Each plan has an 'On' and 'Off' button in its status row. A red arrow points to the 'On' button for the 'Databases' plan.

Figure 5.1 – Turning on and saving Defender plans settings

The screenshot shows the 'Recommendations' page in the Microsoft Azure portal. The 'Secure score recommendations' tab is selected. It displays a secure score of 30% (11/15 controls, 15/45 recommendations). Below this, there's a 'Resource health' summary with a red bar indicating 11 Unhealthy resources, 4 Healthy resources, and 3 Not applicable resources. The 'Governance (preview)' section shows 0/0 Overdue recommendations and 15/15 Unassigned recommendations. The main table lists 10 recommendations with columns for Name, Max score, Current score, Potential score increase, Status, and Unhealthy resources. Each recommendation includes an 'Insights' column with a small chart. A red box highlights the 'Name' column header.

Figure 5.2 – Security posture recommendations

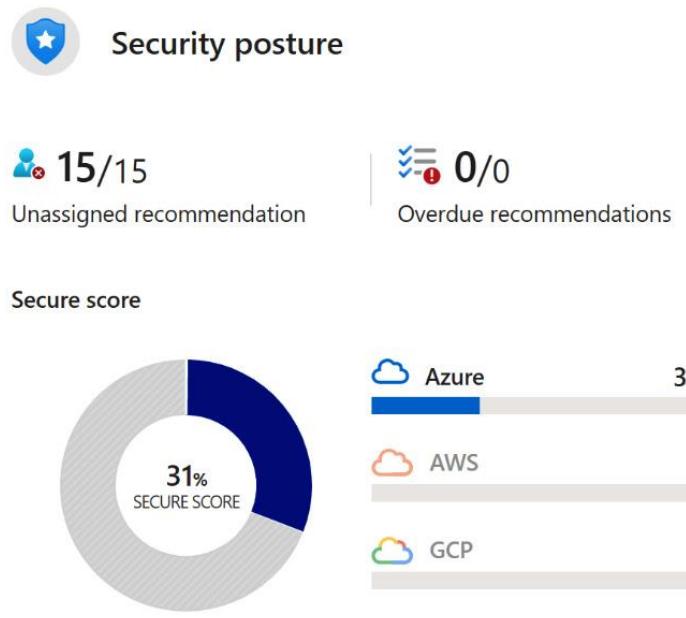


Figure 5.3 – The Security posture overview tile



Figure 5.4 – The Regulatory compliance overview tile

The screenshot shows the Microsoft Defender for Cloud Regulatory compliance dashboard. On the left, there's a sidebar with navigation links like 'Search', 'Cloud Security Explorer (Preview)', 'Workbooks', 'Community', 'Diagnose and solve problems', 'Cloud Security' (selected), 'Security posture', 'Regulatory compliance' (selected), 'Workload protections', 'Firewall Manager', 'DevOps Security (Preview)', 'Management' (selected), 'Environment settings', 'Security solutions', and 'Workflow automation'. The main content area displays the 'Microsoft cloud security benchmark' with various compliance controls listed under 'NS. Network Security'. Each control has a status icon (red or green), a name, and a 'Control details' button. A note at the top says: 'You can now fully customize the standards you track in the dashboard. Update your dashboard by selecting 'Manage compliance policies' above.' Below the controls is a link to 'Microsoft cloud security benchmark applied to the subscription Microsoft Azure Sponsorship'.

Figure 5.5 – The Azure Security Benchmark compliance controls

This screenshot shows the Microsoft Defender for Cloud Regulatory compliance dashboard with a different set of controls. The sidebar shows 'Cloud Security' (selected), 'Regulatory compliance' (selected), and 'Management' (selected). The main content area shows controls under 'IR. Incident Response' and 'PV. Posture and Vulnerability Management'. Each control has a status icon (green or red), a name, and a 'Control details' button. A note at the top says: 'You can now fully customize the standards you track in the dashboard. Update your dashboard by selecting 'Manage compliance policies' above.' Below the controls is a link to 'Microsoft cloud security benchmark applied to the subscription Microsoft Azure Sponsorship'.

Figure 5.6 – Regulatory Compliance color representation

This screenshot shows the Microsoft Defender for Cloud Regulatory compliance dashboard with a focus on 'PV. Posture and Vulnerability Management' controls. The sidebar shows 'Management' (selected). The main content area lists controls from PV-1 to PV-6. Below this is a table titled 'Customer responsibility' showing resource types, failed resources, and compliance status. The table has four columns: Customer responsibility, Resource type, Failed resources, and Resource compliance status. The first row shows 'Machines should be configured securely' with 'Virtual machines' as the resource type, '3 of 5' failed resources, and a mostly red progress bar. The second row shows 'SQL databases should have vulnerability findings resolved' with 'SQL servers' as the resource type, '1 of 1' failed resources, and a mostly red progress bar. The third row shows 'SQL servers on machines should have vulnerability findings resolved' with 'Azure resources' as the resource type, '0 of 0' failed resources, and a green progress bar.

Customer responsibility	Resource type	Failed resources	Resource compliance status
Machines should be configured securely	Virtual machines	3 of 5	<div style="width: 60%; background-color: #c0392b; height: 10px;"></div>
SQL databases should have vulnerability findings resolved	SQL servers	1 of 1	<div style="width: 10%; background-color: #c0392b; height: 10px;"></div>
SQL servers on machines should have vulnerability findings resolved	Azure resources	0 of 0	<div style="width: 100%; background-color: #2e7131; height: 10px;"></div>

Figure 5.7 – Security control recommendations

SQL databases should have vulnerability findings resolved ...

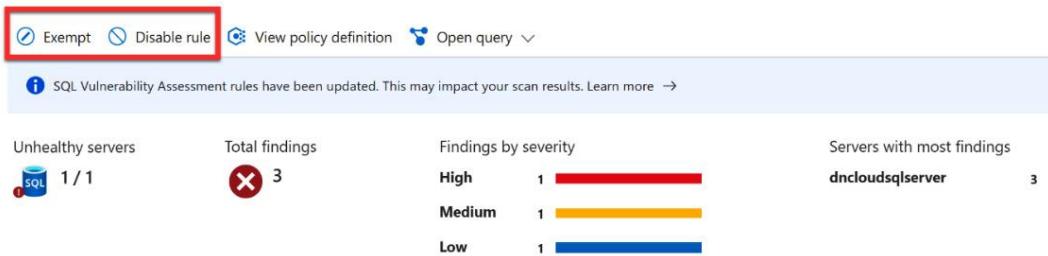


Figure 5.8 – Recommendation resolution

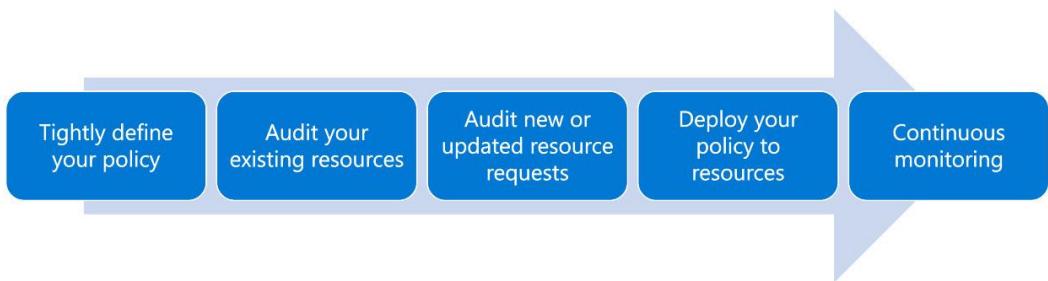


Figure 5.9 – Azure Policy workflow

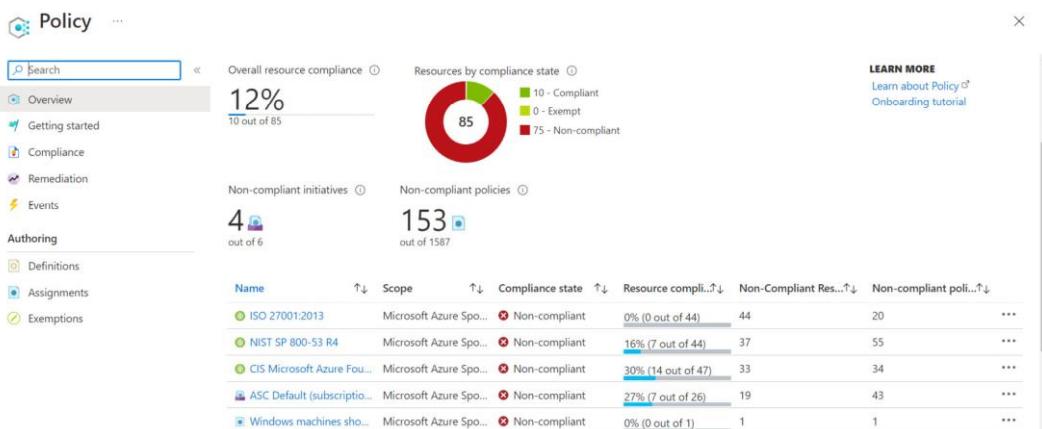


Figure 5.10 – Policy compliance overview

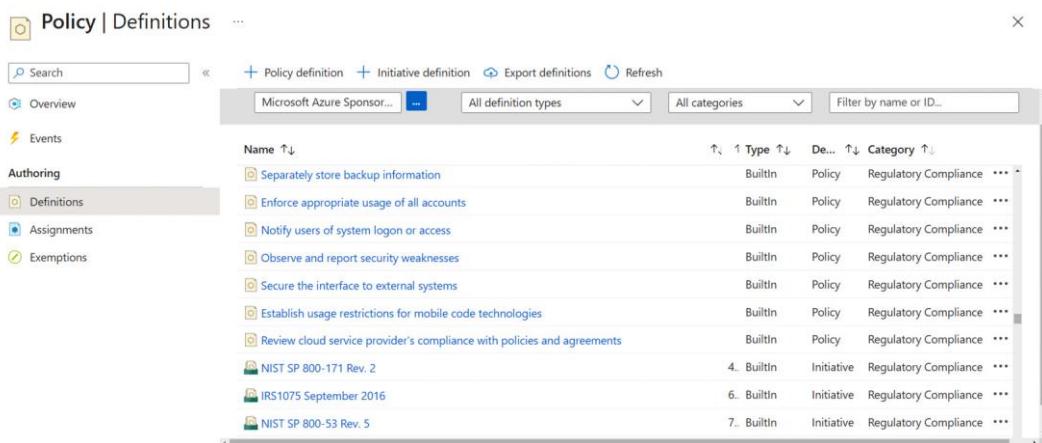


Figure 5.11 – Built-in policies and + Policy definition and + Initiative definition

Name ↑↓	↑↓	↑↓	Type ↑↓	Definition type ↑↓	Category ↑↓
Azure Cosmos DB allowed locations			Builtin	Policy	Cosmos DB
Configure backup on virtual machines without a given tag to an existing recovery services vault in the same location			Builtin	Policy	Backup
Audit resource location matches resource group location			Builtin	Policy	General
Configure backup on virtual machines with a given tag to an existing recovery services vault in the same location			Builtin	Policy	Backup
Allowed locations			Builtin	Policy	General
Allowed locations for resource groups			Builtin	Policy	General

Figure 5.12 – Allowed location policies

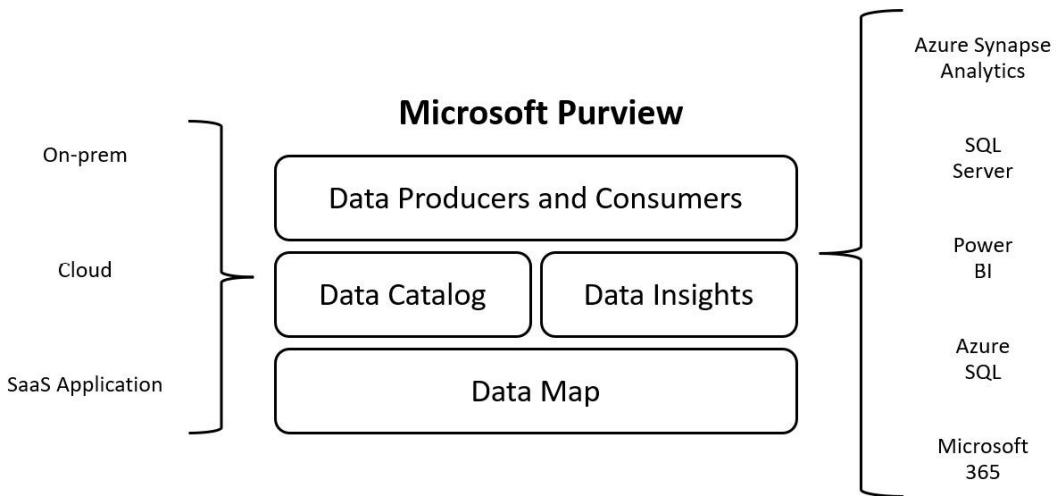


Figure 5.13 – Microsoft Purview for data privacy governance

Links

More information on Microsoft Purview can be found at this link: <https://learn.microsoft.com/en-us/purview/purview>

Chapter 6

Figure

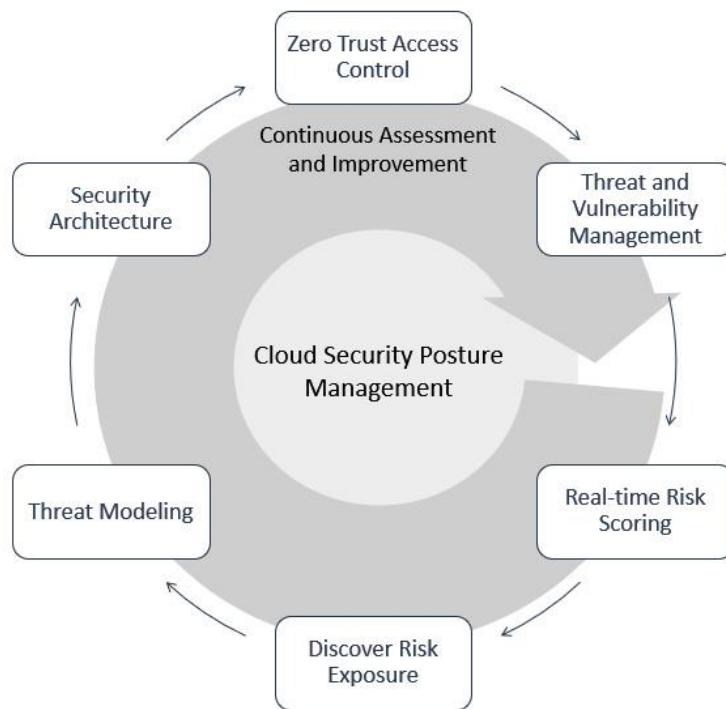


Figure 6.1 – Cloud security posture management – continuous assessment and improvement

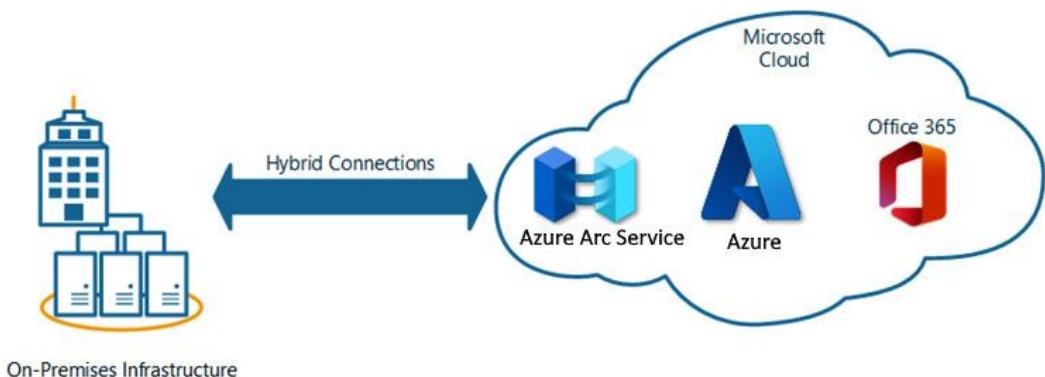


Figure 6.2 – Hybrid infrastructure diagram

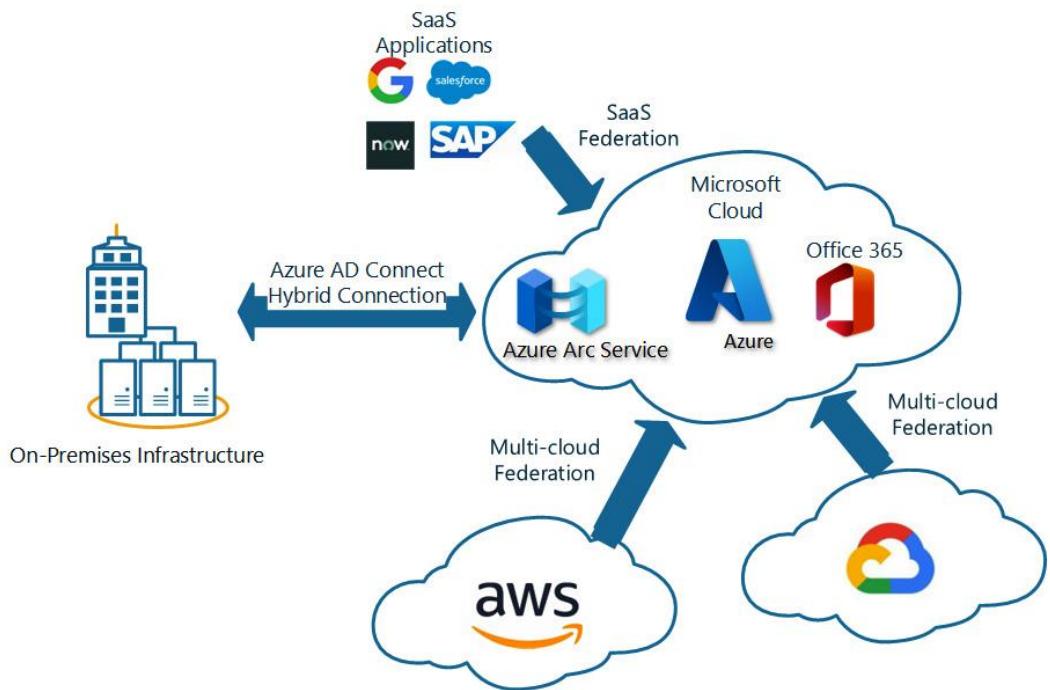


Figure 6.3 – Multi-cloud infrastructure diagram

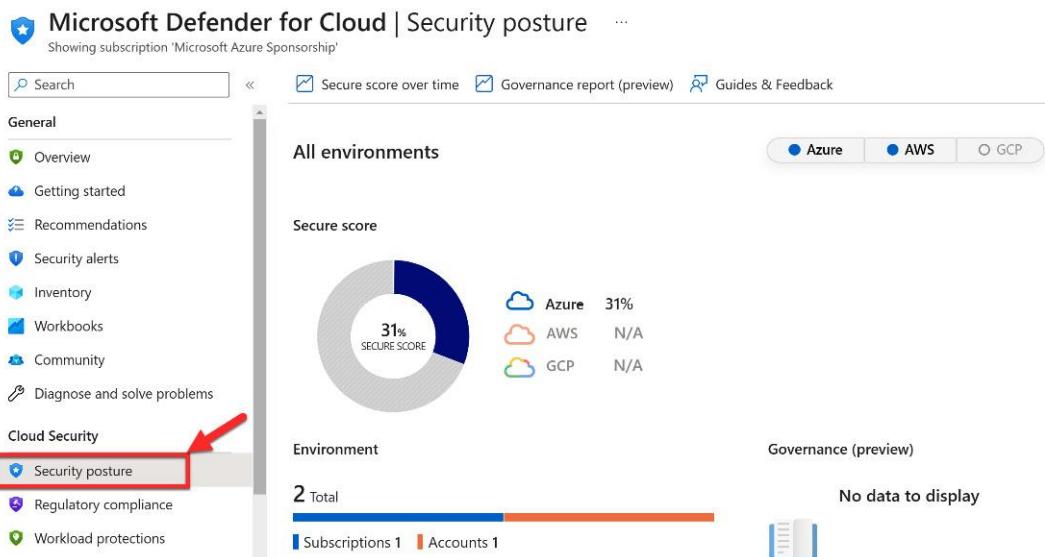


Figure 6.11 – Security posture in the Cloud Security menu

The screenshot shows the Microsoft Defender for Cloud | Security posture dashboard. On the left, a sidebar lists categories like General, Overview, Getting started, Recommendations, Security alerts, Inventory, Workbooks, Community, and Diagnose and solve problems. Under Cloud Security, 'Security posture' is selected. The main area displays two sections: 'Unhealthy resources' (11/18) and 'Recommendations' (45). Below this, a table lists environments: 'Microsoft Azure Sponsorship' (Secure score: 31%, 11 of 15 unhealthy resources) and 'AWS account' (Secure score: N/A, 0 of 0 unhealthy resources). A red arrow points to the 'View recommendation...' link for the Azure environment.

Figure 6.12 – Subscription security posture recommendations

The screenshot shows the 'Secure score recommendations' page. It lists 16 recommendations, with one specifically highlighted: 'Enable MFA'. This recommendation has a current score of 0.00 and a potential score increase of +18%. A red arrow points to the 'Potential score increase' column header.

Name	Max score	Current score	Potential score increase	Status	Unhealthy resources
Enable MFA	10	0.00	+ 18%	Unassigned	1 of 1 resources
Secure manage...	8	1.60	+ 11%	Unassigned	4 of 5 resources
Remediate vuln...	6	0.00	+ 11%	Unassigned	5 of 5 resources
Apply system u...	6	6.00	+ 0%	Completed	0 of 5 resources
Encrypt data in t...	4	2.67	+ 2%	Unassigned	1 of 3 resources

Figure 6.13 – Potential score increase

This screenshot shows a detailed view of the 'Enable MFA' recommendation. It includes the current score (0.00), potential score increase (+18%), and a note at the bottom stating 'MFA should be ena...'. A red arrow points to this note.

Figure 6.14 – Enable MFA recommendation list

MFA should be enabled on accounts with owner permissions on subscriptions

Exempt View policy definition Open query

Multiple changes to identity recommendations will be available soon. Learn more →

Description

Multi-Factor Authentication (MFA) should be enabled for all subscription accounts with owner permissions to prevent a breach of accounts or resources.

Remediation steps ←

Manual remediation:

To enable MFA using conditional access you must have an Azure AD Premium license and have AD tenant admin permissions.

- Select the relevant subscription or click 'Take action' if it's available. The list of user accounts without MFA appears.
- Click 'Continue'. The Azure AD Conditional Access page appears.
- In the Conditional Access page, add the list of users to a policy (create a policy if one doesn't exist).
- For your conditional access policy, ensure the following:
 - In the 'Access controls' section, multi-factor authentication is granted.
 - In the 'Cloud Apps or actions' section's 'Include' tab, check that Application Id for 'Microsoft Azure Management' App or 'All apps' is selected. In the 'Exclude' tab, check that it is not

Figure 6.15 – Remediation steps within the security posture recommendations



Figure 6.16 – Microsoft Defender for Cloud enhanced security protection

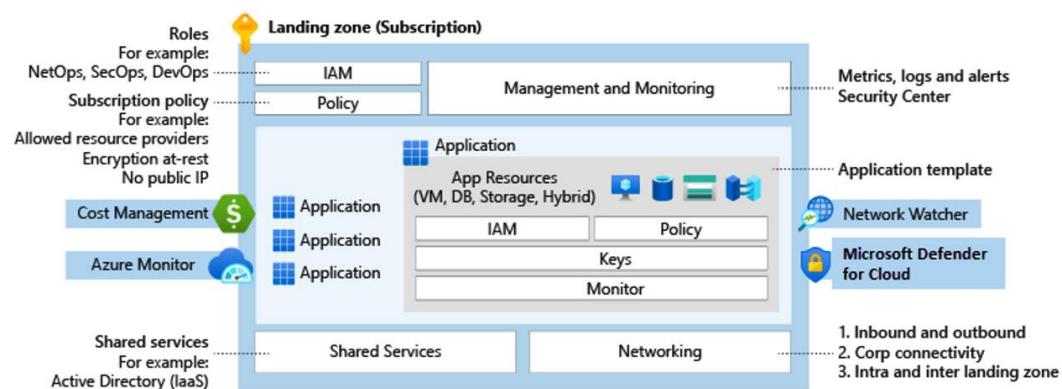


Figure 6.23 – Diagram of the components of an Azure landing zone

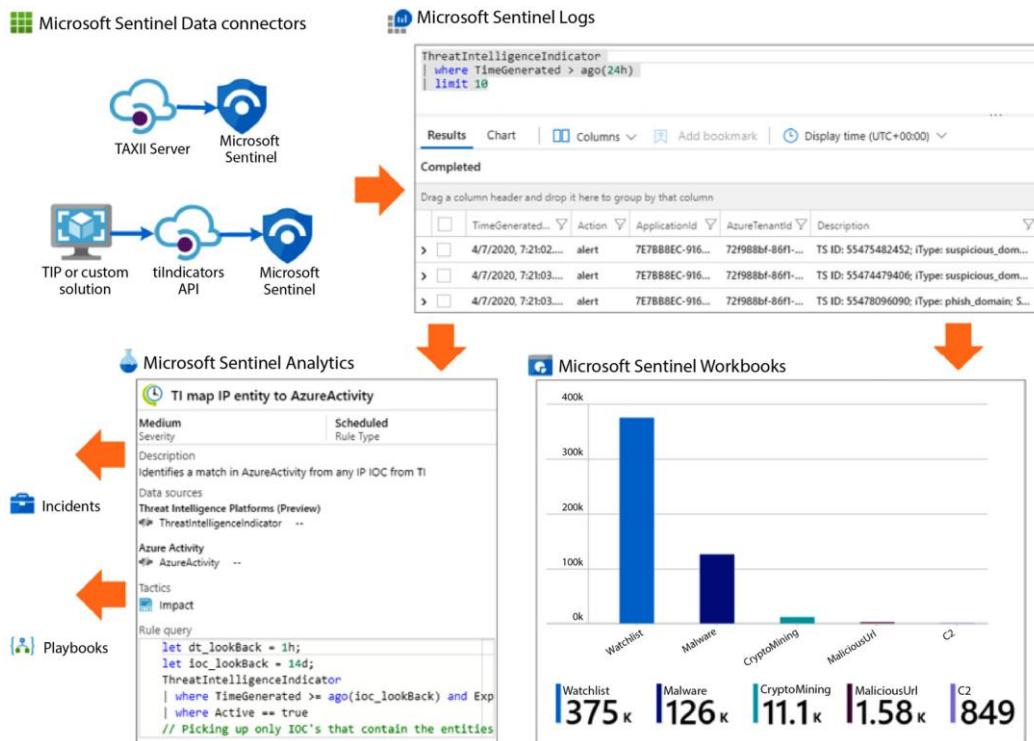


Figure 6.24 – Microsoft Sentinel tools for threat intelligence

The risk assessment matrix diagram includes a vertical blue arrow labeled "Likelihood" pointing upwards and a horizontal blue arrow pointing right labeled "Impact: How serious is the risk?".

Likelihood	Very Likely	Acceptable risk Medium 2	Unacceptable risk High 3	Unacceptable risk Extreme 5
Likely	Acceptable risk Low 1	Acceptable risk Medium 2	Unacceptable risk High 3	
Unlikely	Acceptable risk Low 1	Acceptable risk Low 1	Acceptable risk Medium 2	
What is the chance that it will happen?	Minor	Moderate	Major	

Figure 6.25 – Risk assessment matrix

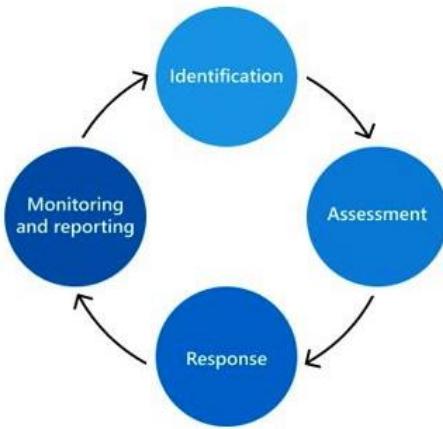


Figure 6.26 – Risk assessment and mitigation life cycle

Tables

Design Area and Methodology	Objective	Microsoft Documentation
Security	Provides controls and protection processes for securing cloud environments	https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/landing-zone/design-area/security
Management	Creates ongoing operations procedures and management baselines, as well as protection and recovery capabilities	https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/landing-zone/design-area/management
Governance	Provides policies to automate auditing and enforcement of compliance	https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/landing-zone/design-area/governance
Ready and automation	Utilizes tools and templates to deploy and automate the creation of landing zones and resources	https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/landing-zone/design-area/platform-automation-devops

Table 6.1 – Azure Landing Zone design areas and methodology

Hands-On Section

Evaluating the security posture by using benchmarks

Let's look at how you can evaluate and make adjustments to your CSPM by utilizing the Azure Security Benchmark by walking through the **Regulatory compliance** section of Microsoft Defender for Cloud:

2. In the Azure portal (<https://portal.azure.com/>), search for and navigate to **Microsoft Defender for Cloud**.
3. Navigate to **Regulatory compliance** under **Cloud Security** on the menu, as shown in *Figure 6.4*:

The screenshot shows the Microsoft Defender for Cloud interface. The title bar reads "Microsoft Defender for Cloud | Regulatory compliance" and "Showing subscription 'Microsoft Azure Sponsorship'". The left sidebar has sections for "Cloud Security" (Security posture, Regulatory compliance, Workload protections), "Management" (Environment settings, Security solutions), and "Community" (Diagnose and solve problems). The main area is titled "Azure Security Benchmark" and shows "21 of 43 passed controls". It also says "Lowest compliance regulatory standards" and lists four standards with progress bars: SOC TSP (1/13), ISO 27001:2013 (2/17), PCI DSS 3.2.1 (12/43), and Azure CIS 1.1.0 (36/71). A tooltip message says: "You can now fully customize the standards you track in the dashboard. Update your dashboard by selecting 'Manage compliance policies' above."

Figure 6.4 – Regulatory compliance in the Cloud Security menu

4. If this section is not available to you, you will need to go to your subscription in **Environment settings** to turn on the Microsoft Defender plans. These steps will be reviewed in the *Evaluating the security posture of cloud workloads* section.
5. Next, scroll down within the **Regulatory compliance** overview dashboard and select **Azure Security Benchmark**. This is usually the default selection as the first tab. Note the tabs for the additional **Regulatory compliance** standards that are active within your subscription, as shown in *Figure 6.5*:

The screenshot shows the Microsoft Defender for Cloud interface. In the top left, there's a shield icon followed by the text "Microsoft Defender for Cloud | Regulatory compliance". Below it, it says "Showing subscription 'Microsoft Azure Sponsorship'". The top navigation bar includes links for "Search", "Download report", "Manage compliance policies", "Open query", "Compliance over time workbook", and more. On the left, a sidebar lists "Recommendations", "Security alerts", "Inventory", "Workbooks", "Community", "Diagnose and solve problems", "Cloud Security" (with "Security posture" and "Regulatory compliance" under it), and "Workload protections". The "Regulatory compliance" section is currently selected. The main content area has a header "Azure Security Benchmark V3" which is highlighted with a red box and a red arrow pointing to it from the left sidebar. Below this, other compliance standards are listed: "PCI DSS 3.2.1", "SOC TSP", "NIST SP 800 53 R4", and "Azure CIS 1.1.0". A note states: "Under each applicable compliance control is the set of assessments run by Defender for Cloud that are associated with that control. If they are all green, it means those assessments are currently passing; this does not ensure you are fully compliant with that control. Furthermore, not all controls for any particular regulation are covered by Defender for Cloud assessments, and therefore this report is only a partial view of your overall compliance status." At the bottom of this section is a link "Azure Security Benchmark is applied to the subscription Microsoft Azure Sponsorship" and a checkbox "Expand all compliance controls".

Figure 6.5 – List of regulatory compliance options

6. Scroll down to view the compliance controls for Azure Security Benchmark. These controls match the documentation for the compliance benchmark or standard that you are viewing. Documentation for these controls for Azure Security Benchmark can be found here: <https://learn.microsoft.com/en-us/security/benchmark/azure/overview>. **Figure 6.6** shows a list of these controls in Microsoft Defender for Cloud:

✓ ✖ NS. Network Security
✓ ✖ IM. Identity Management
✓ ✖ PA. Privileged Access
✓ ✖ DP. Data Protection
✓ ✖ AM. Asset Management
✓ ✖ LT. Logging and Threat Detection
✓ ✓ IR. Incident Response
✓ ✖ PV. Posture and Vulnerability Management
✓ ✖ ES. Endpoint Security
✓ ✖ BR. Backup and Recovery
✓ ✓ DS. DevOps Security
✓ ● GS. Governance and Strategy

Figure 6.6 – List of Azure Security Benchmark controls

7. These control sections provide a quick review of your level of compliance and security posture within the current infrastructure:
 - Green check marks show that you are fully compliant with this control
 - Red check marks show that you are missing controls
 - If the control is gray, you currently do not have any applicable areas of your environment that apply to this control

8. Select one of the controls with a red check mark – for example, **NS. Network Security** – as shown in **Figure 6.7**:

<input checked="" type="checkbox"/>	NS. Network Security	
<input checked="" type="checkbox"/>	NS-1. Establish network segmentation boundaries	Control details MS C
<input checked="" type="checkbox"/>	NS-2. Secure cloud services with network controls	Control details MS C
<input checked="" type="checkbox"/>	NS-3. Deploy firewall at the edge of enterprise network	Control details MS C
<input checked="" type="checkbox"/>	NS-4. Deploy intrusion detection/intrusion prevention systems (IDS/IPS)	Control details MS C
<input checked="" type="checkbox"/>	NS-5. Deploy DDoS protection	Control details MS C
<input checked="" type="checkbox"/>	NS-6. Deploy web application firewall	Control details MS C
<input checked="" type="checkbox"/>	NS-7. Simplify network security configuration	Control details MS C
<input checked="" type="checkbox"/>	NS-8. Detect and disable insecure services and protocols	Control details MS C
<input checked="" type="checkbox"/>	NS-9. Connect on-premises or cloud network privately	Control details MS C
<input checked="" type="checkbox"/>	NS-10. Ensure Domain Name System (DNS) security	Control details MS C

Figure 6.7 – Network Security controls

9. The **MS** and **C** boxes denote the responsibility of Microsoft and Customer, respectively. Selecting the drop-down of the control will provide the resources and recommendations to further evaluate what needs to be done from a customer responsibility perspective to increase the security posture, as shown in **Figure 6.8**:

<input checked="" type="checkbox"/>	NS. Network Security		
<input checked="" type="checkbox"/>	NS-1. Establish network segmentation boundaries	Control details MS C	
			
Customer responsibility	Resource type	Failed resources	Resource complian...
Adaptive network hardening recommends	Virtual machines	4 of 5	<div style="width: 80%; background-color: #f08080;"></div>
All network ports should be restricted on I	Virtual machines	4 of 5	<div style="width: 80%; background-color: #f08080;"></div>
Subnets should be associated with a netw	Subnets	2 of 3	<div style="width: 66.67%; background-color: #f08080;"></div>
Non-internet-facing virtual machines shou	Virtual machines	0 of 5	<div style="width: 0%; background-color: #cccccc;"></div>
Internet-facing virtual machines should	Virtual machines	0 of 5	<div style="width: 0%; background-color: #9acd32;"></div>

Figure 6.8 – Recommended security controls to increase security posture

As a cybersecurity architect that is evaluating a customer's environment to provide recommendations for increasing security posture, you should be reviewing these recommendations and providing guidance for how to implement these to the various administration and architecture teams. Selecting these recommendations shows the non-compliant and compliant resources, as well as the steps to remediate these resources for security control compliance. These steps can be repeated for other compliance standards with the same control headings that match the documentation for the standards. **Figure 6.9** shows the list for PCI-DSS 3.2.1:

- ✓ ✘ 1. Install and maintain a firewall configuration to protect cardholder data
- ✓ ✘ 2. Do not use vendor-supplied defaults for system passwords and other security parameters
- ✓ ✘ 3. Protect stored cardholder data
- ✓ ✘ 4. Encrypt transmission of cardholder data across open, public networks.
- ✓ ✓ 5. Protect all systems against malware and regularly update anti-virus software or programs.
- ✓ ✘ 6. Develop and maintain secure systems and applications
- ✓ ✘ 7. Restrict access to cardholder data by business need to know
- ✓ ✘ 8. Identify and authenticate access to system components
- ✓ ● 9. Restrict physical access to cardholder data
- ✓ ✘ 10. Track and monitor all access to network resources and cardholder data
- ✓ ✘ 11. Regularly test security systems and processes
- ✓ ● 12. Maintain a policy that addresses information security for all personnel
- ✓ ● A1. Protect each entity's (that is, merchant, service provider, or other entity) hosted environment and data, per A1.1 through A1.4:

Figure 6.9 – PCI-DSS 3.2.1 list of security control requirements

Evaluating the security posture of cloud workloads

Now that we understand the features and functionality of Microsoft Defender for Cloud, let's look at how we can configure resources to manage your security posture:

1. Let's start by logging into <https://portal.azure.com>. Then, in the search bar, enter Microsoft Defender for Cloud. Select **Microsoft Defender for Cloud**, as shown in **Figure 6.17**:

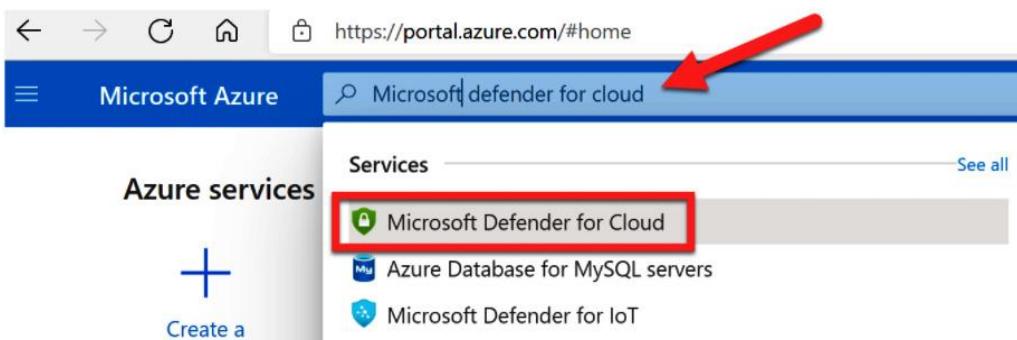


Figure 6.17 – Navigating to Microsoft Defender for Cloud

2. This will take you to the Microsoft Defender for Cloud **Overview** tile.
3. In the **Overview** tile, locate **Environment settings** in the **Management** menu, as shown in **Figure 6.18**:

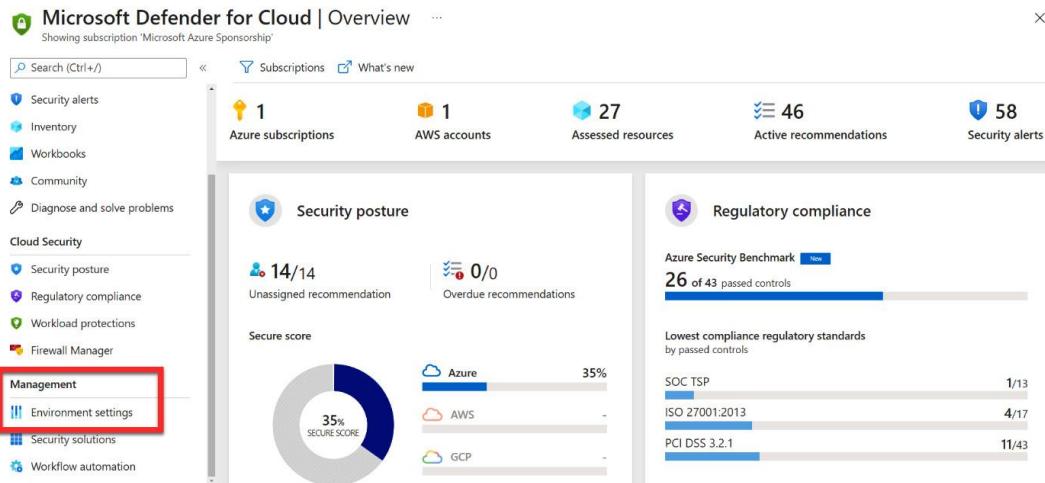


Figure 6.18 – Environment settings in Microsoft Defender for Cloud

4. Select your subscription. This will take you to the **Settings | Defender plans** page. Within the **Defender plans** settings, select **Enable all** to enable all Microsoft Defender for Cloud plans, as shown in *Figure 6.19*:

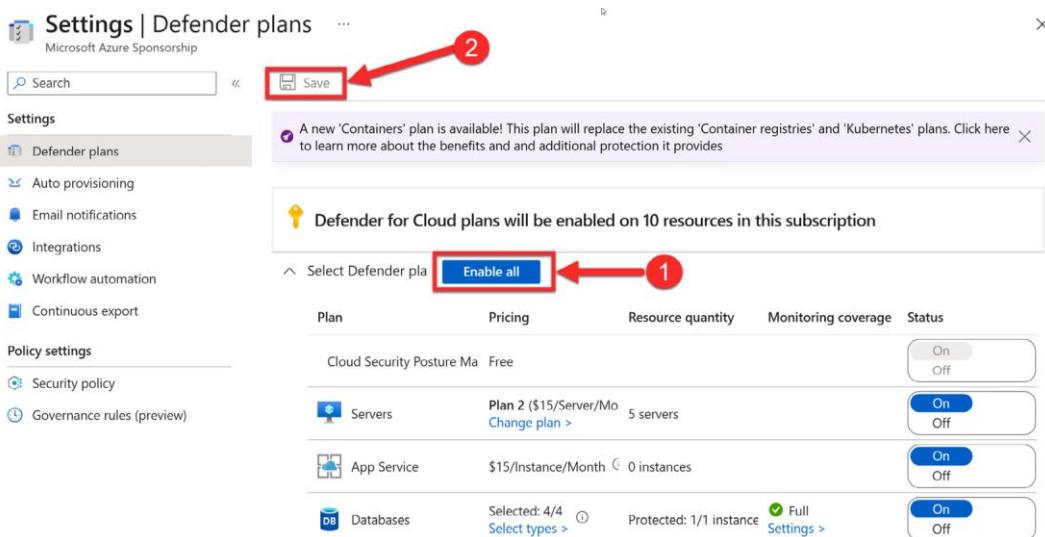


Figure 6.19 – Enabling Defender for Cloud enhanced security plans

This will allow you to manage the security posture for hybrid and multi-cloud resources.

When enabling the Defender for Cloud plans, you enable the additional features available for Microsoft Defender for Cloud. Currently, CSPM features are free for customers. Among the additional features enabled with Defender, plans include Just in Time Virtual Machine Access, Adaptive application controls, Network hardening, Threat protection for servers, and PaaS. When these Defender plans are enabled, you unlock additional vulnerability and threat alerts that can be accessed within the **Workload protections** section under the **Cloud Security** menu, as shown in *Figure 6.20*:

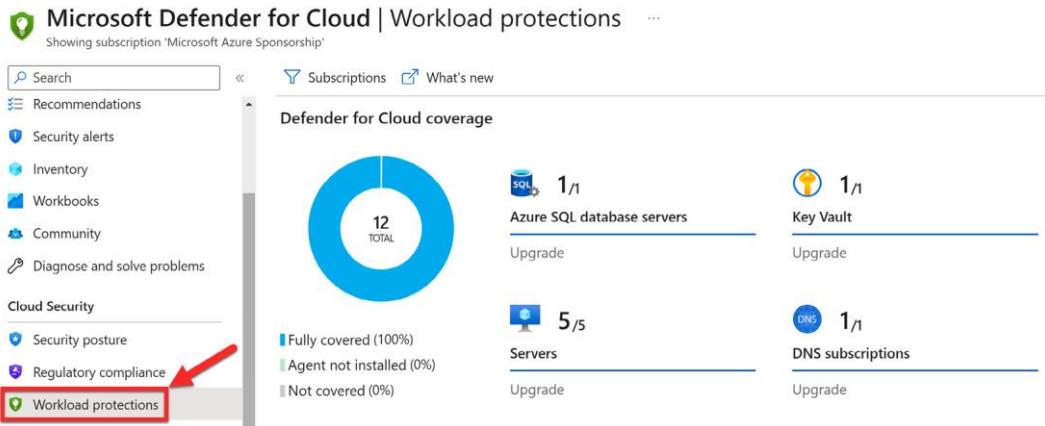


Figure 6.20 – Workload protections in the Cloud Security menu

Within the **Workload protections** dashboard, you can scroll down and review the security posture for the workloads within the scope of the enabled Defender plans, as shown in **Figure 6.21**:



Figure 6.21 – Advanced protection for Defender plans

Selecting one of these workloads will provide additional recommendations for hardening the security posture of these workloads. The **Network Map** area is a very helpful feature that you can use to evaluate potential exposure within virtual networks and virtual machines. **Figure 6.22** shows how you can use this network map to view additional recommendations for network and VM hardening. The red exclamation points denote potential vulnerabilities and areas of recommended security improvements:

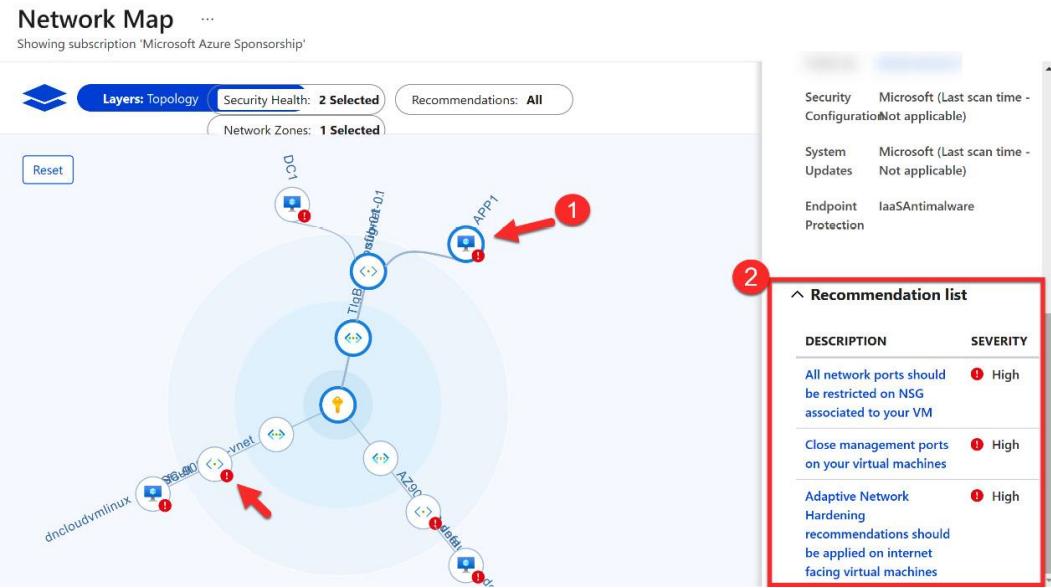


Figure 6.22 – Network map and security posture recommendations

Links

For the full list of regulatory and benchmark standards available, please see this link:

<https://learn.microsoft.com/en-us/azure/defender-for-cloud/update-regulatory-compliance-packages>.

Microsoft 365 Defender has a similar dashboard for SaaS applications and workspace devices. This can be further reviewed and evaluated at <https://security.microsoft.com>

More information on each of these plans can be found at this link: <https://docs.microsoft.com/en-us/azure/defender-for-cloud/defender-for-cloud-introduction>.

Chapter 7

Figures

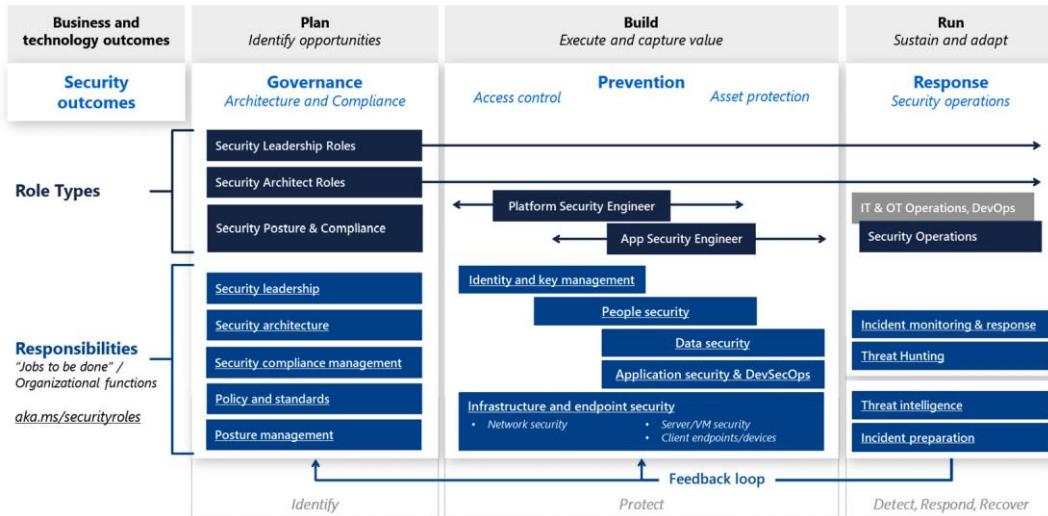


Figure 7.1 – Security roles and responsibilities

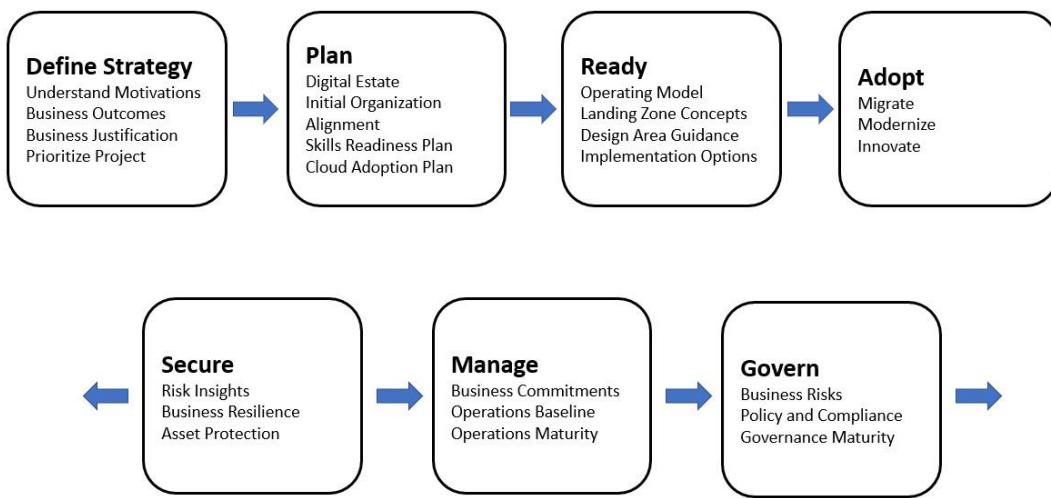


Figure 7.2 – CAF

Microsoft Endpoint Manager admin center

Home > Endpoint security | Overview > Endpoint security

Endpoint security | Security baselines

Search

Overview

All devices

Security baselines

Security tasks

Manage

Manage and monitor the baseline security status of all your enrolled devices. For more information about the data reported here, see the Intune documentation.

Security Baselines	Associated Profi...	Versions
Security Baseline for Windows 10 and later	0	1
Microsoft Defender for Endpoint Baseline	0	1
Microsoft Edge Baseline	0	1
Windows 365 Security Baseline (Preview)	0	1

Figure 7.3 – Endpoint security baselines

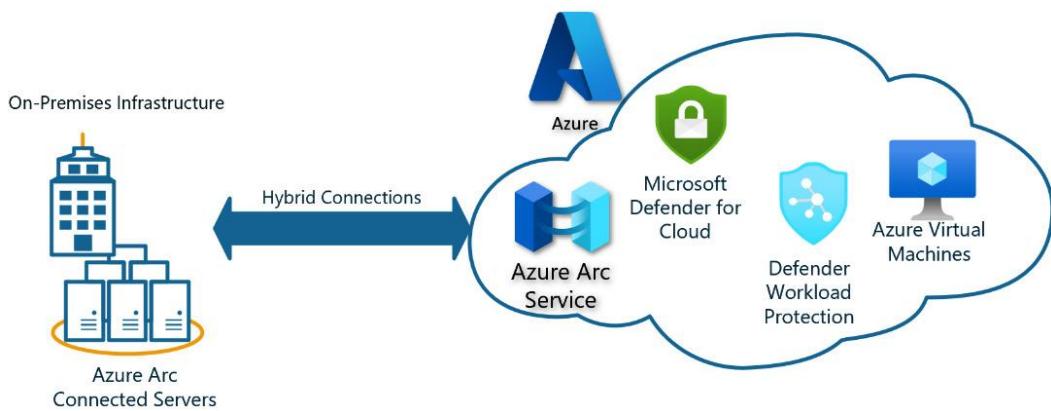


Figure 7.4 – Hybrid server infrastructure diagram

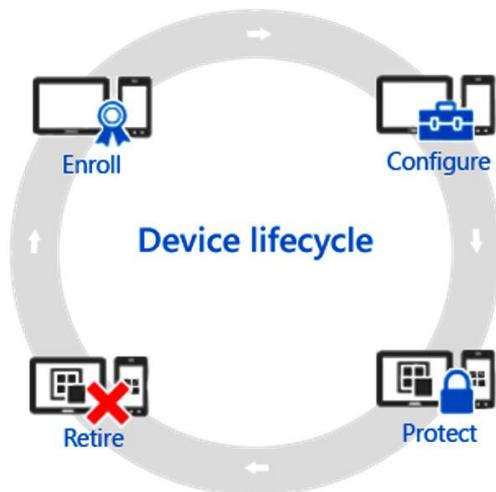


Figure 7.5 – Mobile device life cycle

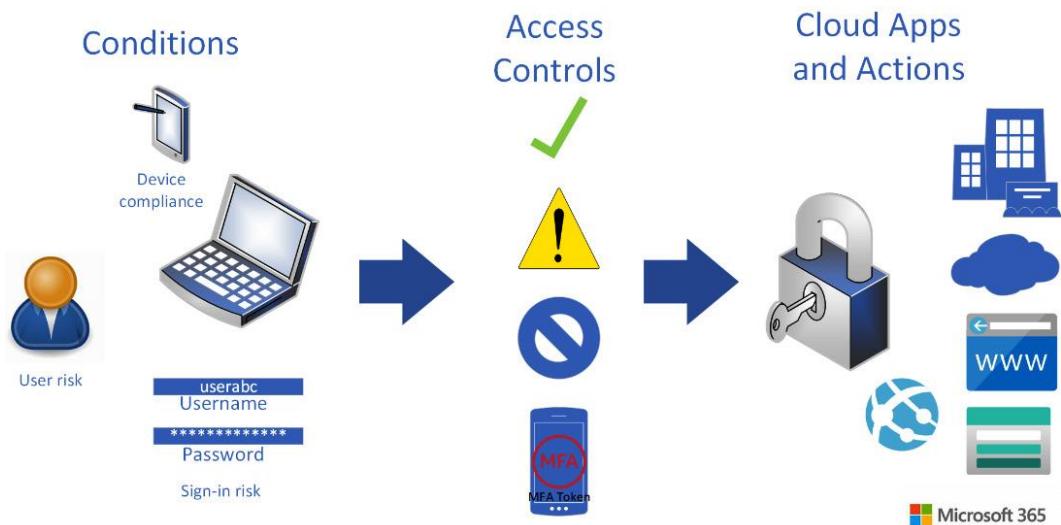


Figure 7.6 – Conditional Access policies for MDM-compliant devices

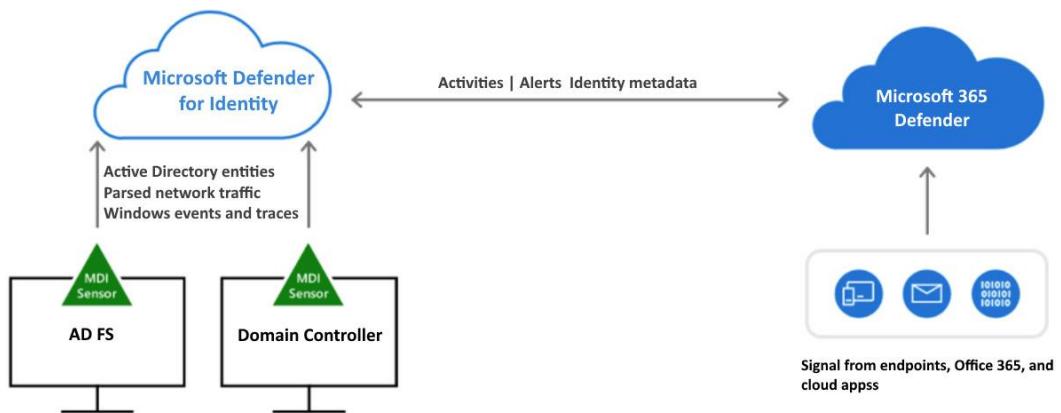


Figure 7.7 – Microsoft Defender for Identity communication workflow

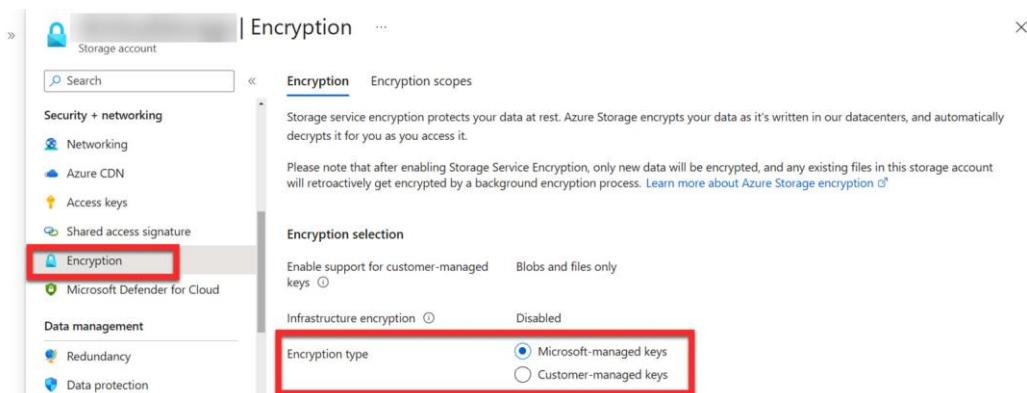


Figure 7.8 – Configuring customer-managed keys with Azure Key Vault



Figure 7.9 – CA validation with Azure Key Vault

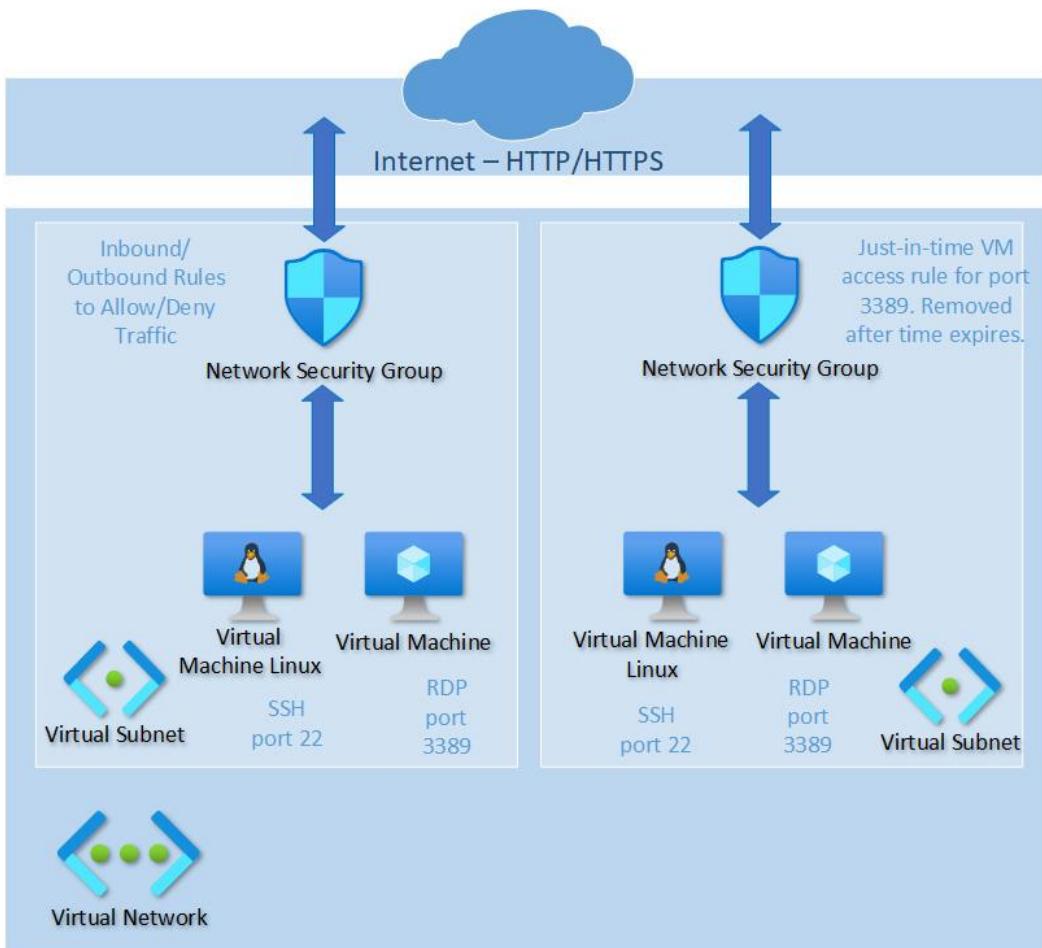


Figure 7.10 – NSG with a JIT virtual machine access inbound rule



Figure 7.11 – Remote access with Azure Bastion

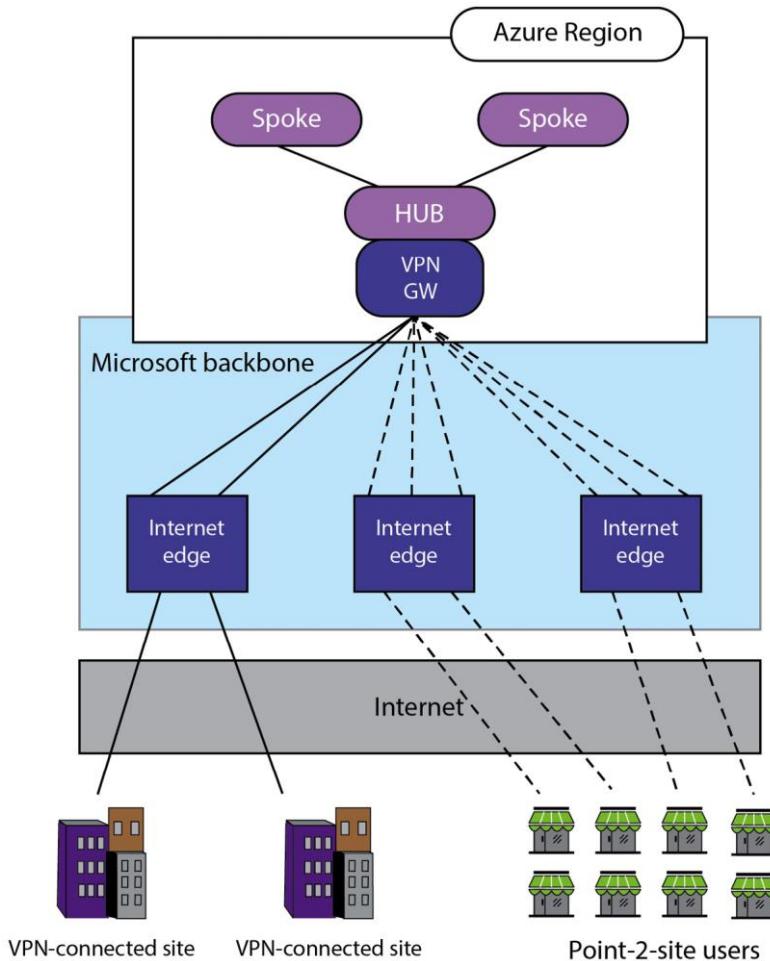


Figure 7.12 – Secure connectivity from Azure to on-premises sites

Links

Additional details on the security roles and responsibilities can be found at this link:

<https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/organize/cloud-security>.

Security guidelines for the CAF can be found here: <https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/secure/>.

For more information on the Microsoft guidance, you can review this link:

<https://learn.microsoft.com/en-us/windows/security/threat-protection/windows-security-configuration-framework/windows-security-baselines>

More information on Microsoft Endpoint Manager can be found at this link:

<https://docs.microsoft.com/en-us/mem/endpoint-manager-overview>.

Additional information on the defender services can be found at this link:

<https://docs.microsoft.com/en-us/microsoft-365/security/defender/microsoft-365-defender?view=o365-worldwide>.

Additional information on JIT virtual machine access can be found at this link:
<https://docs.microsoft.com/en-us/azure/defender-for-cloud/just-in-time-access-usage?tabs=jit-config-asc%2Cjit-request-asc>.

Additional information about Azure Bastion can be found at this link:
<https://docs.microsoft.com/en-us/azure/bastion/bastion-overview>.

Additional information about remote access with Azure Arc can be found at this link for Linux SSH:
<https://learn.microsoft.com/en-us/azure/azure-arc/servers/ssh-arc-overview>. For Windows Admin Center, see this link: <https://learn.microsoft.com/en-us/windows-server/manage/windows-admin-center/azure/manage-arc-hybrid-machines>.

Information on the NIST framework can be found at this link: <https://www.nist.gov/cybersecurity>.

Chapter 8

Figures

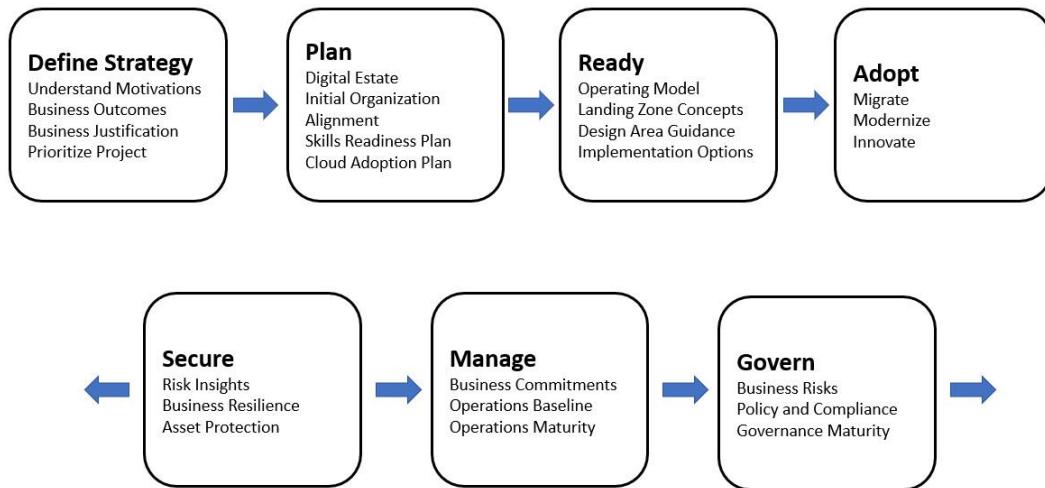


Figure 8.1 – Cloud Adoption Framework

Responsibility	On-premises	IaaS	PaaS	SaaS
Data governance and Rights Management	Customer	Customer	Customer	Customer
Client endpoints	Customer	Customer	Customer	Customer
Account and access management	Customer	Customer	Customer	Customer
Identity and directory Infrastructure	Customer	Customer	Microsoft/ Customer	Microsoft/ Customer
Application	Customer	Customer	Microsoft/ Customer	Microsoft
Network controls	Customer	Customer	Microsoft/ Customer	Microsoft
Operating system	Customer	Customer	Microsoft	Microsoft
Physical hosts	Customer	Microsoft	Microsoft	Microsoft
Physical network	Customer	Microsoft	Microsoft	Microsoft
Physical datacenter	Customer	Microsoft	Microsoft	Microsoft

Figure 8.2 – Shared responsibility for Microsoft Security

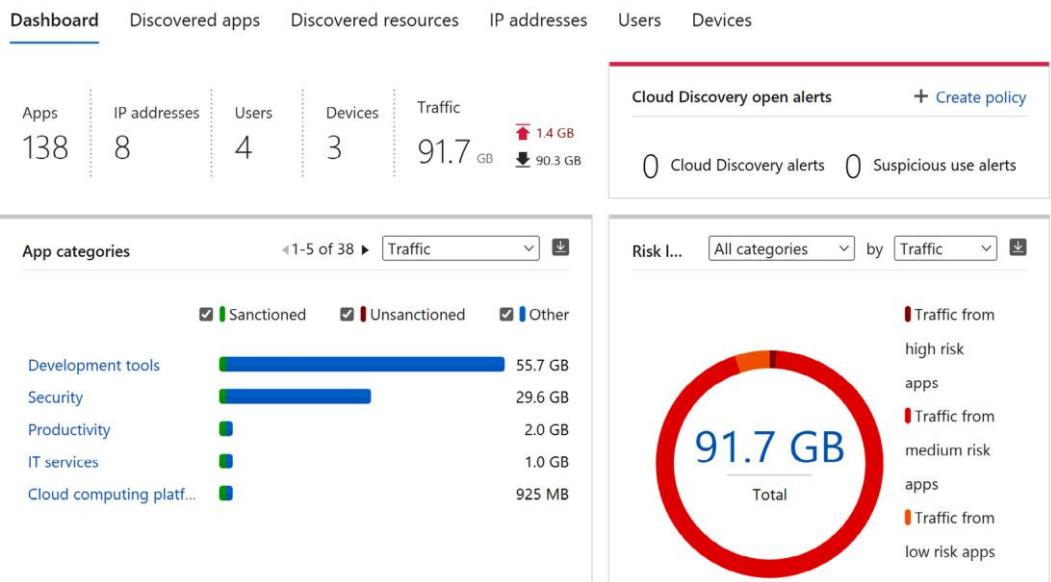


Figure 8.3 – Microsoft Defender for Cloud Apps discovery dashboard

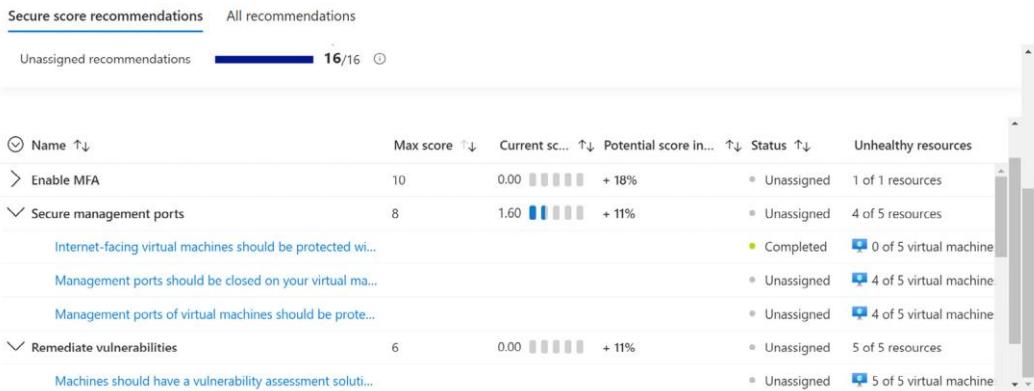


Figure 8.4 – Microsoft Defender for Cloud virtual machine security recommendations

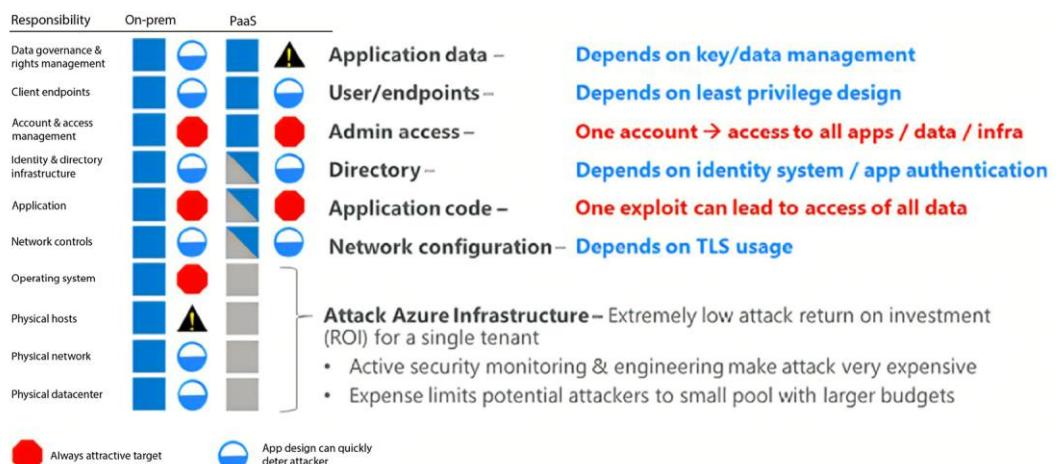


Figure 8.5 – Security controls for PaaS

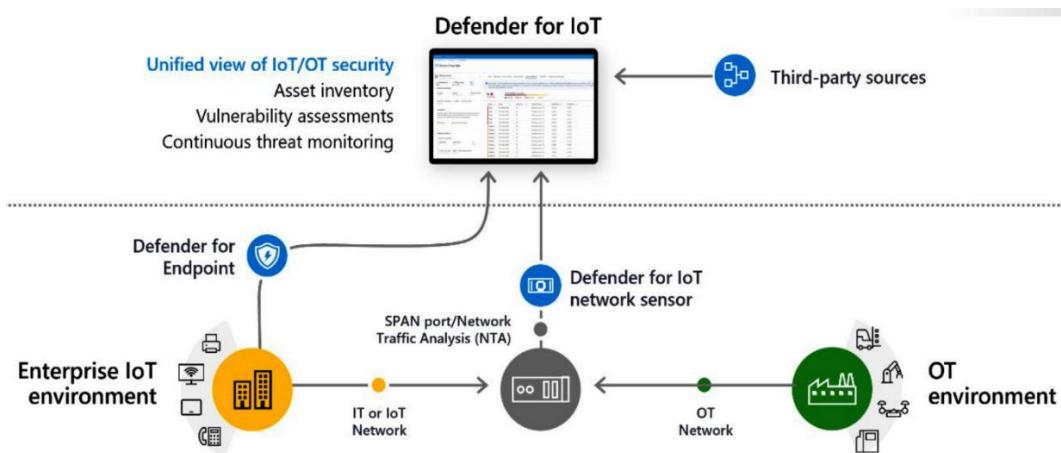


Figure 8.6 – Defender for IoT threat detection diagram

Figure 8.7 – Microsoft Defender for IoT getting started

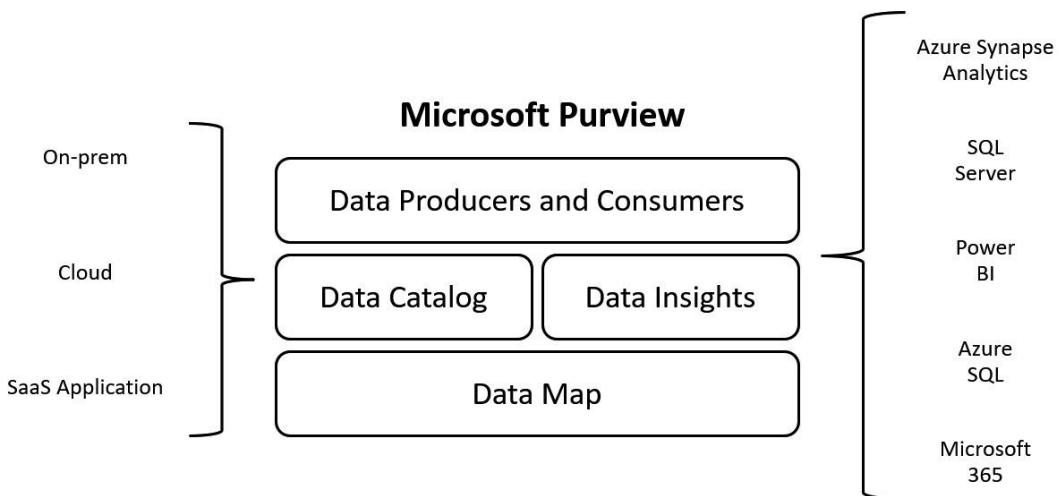


Figure 8.8 – Microsoft Purview data sources

Secure score recommendations		All recommendations			
Unassigned recommendations		16/16			
Max score ↑↓	Current score ↑↓	P... ↑↓	Status ↑↓	Unhealthy resources	
Transparent Data Encryption on SQL databases should be enabled	2.00	+ 4%	Completed	0 of 1 SQL database	
Remediate security configurations	4		Unassigned	3 of 6 resources	
Log Analytics agent should be installed on virtual machines			Completed	0 of 5 virtual machines	
Machines should be configured securely			Unassigned	2 of 5 virtual machines	
Vulnerabilities in security configuration on your Windows machine			Unassigned	2 of 4 virtual machines	
Vulnerabilities in security configuration on your Linux machine			Completed	0 of 1 virtual machine	
SQL servers should have vulnerability assessment configured			Unassigned	1 of 1 SQL server	
SQL databases should have vulnerability findings resolved					

Figure 8.9 – Microsoft Defender for Cloud SQL security recommendations

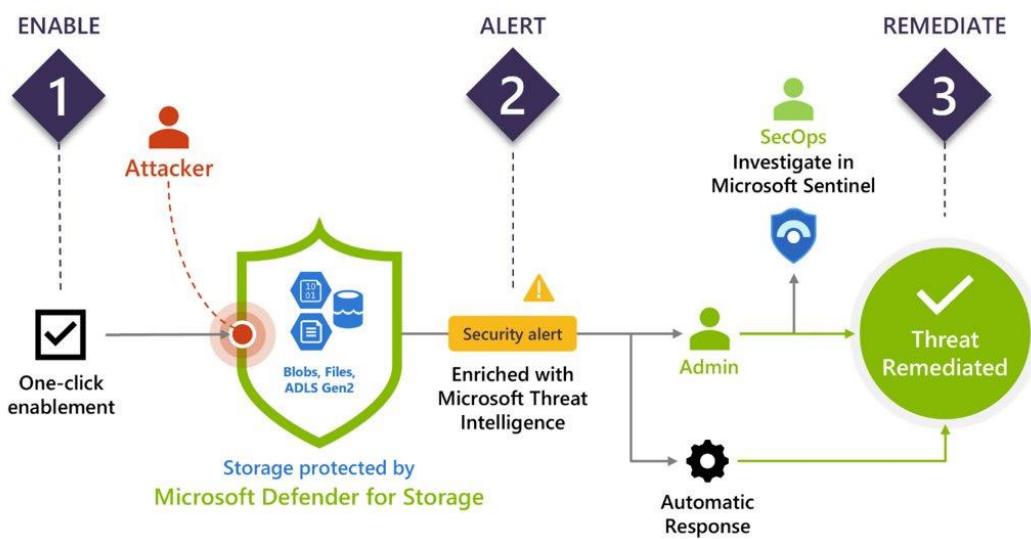


Figure 8.10 – Microsoft Defender for Storage threat protection

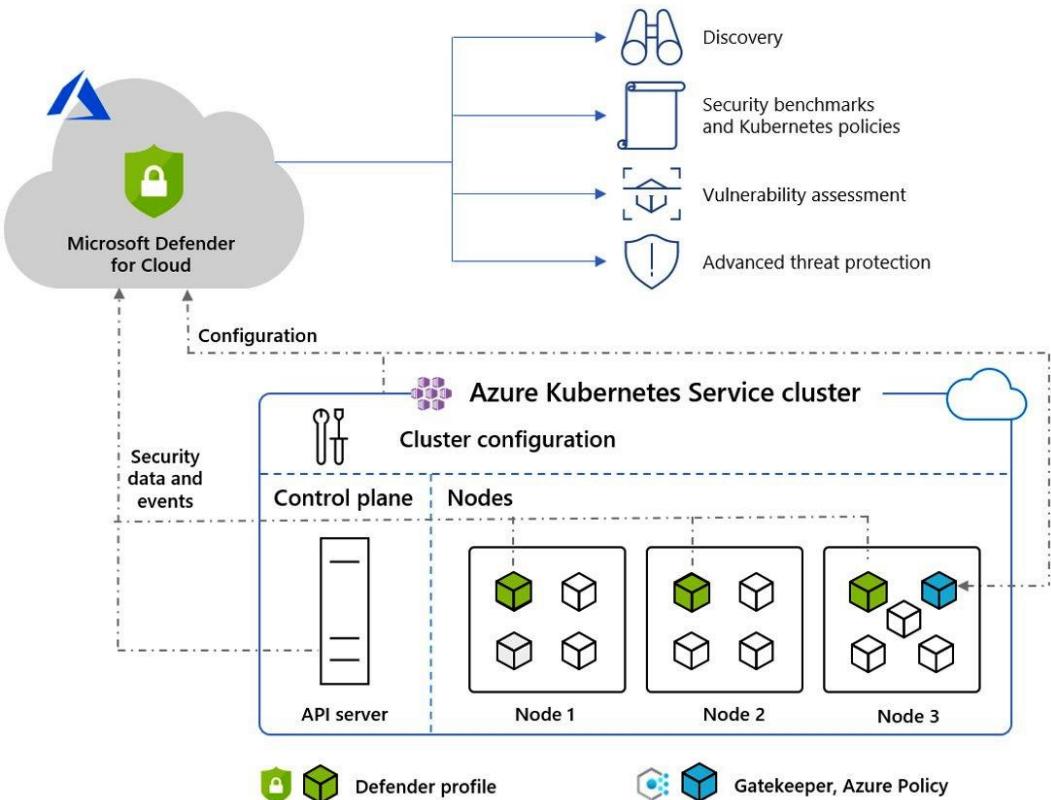


Figure 8.11 – Microsoft Defender for Containers policy orchestration

Links

Security guidelines for the CAF can be found here: <https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/secure/>.

For more information on Microsoft Defender for Cloud Apps, see this link:

<https://learn.microsoft.com/en-us/defender-cloud-apps/what-is-defender-for-cloud-apps>.

Additional information on Microsoft Defender for Cloud and protection for IaaS resources with Microsoft Defender for Servers can be found at this link: <https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-servers-introduction>.

The Azure Security Benchmark becomes a helpful tool for evaluating applications on PaaS resources within Microsoft Defender for Cloud. For more information, use this link:

<https://learn.microsoft.com/en-us/security/benchmark/azure/baselines/app-service-security-baseline>.

For more information on Defender for IoT, please review this link: <https://learn.microsoft.com/en-us/azure/defender-for-iot/organizations/getting-started>.

For more information on enabling the different Microsoft Defender for Databases plans, go to this link: <https://learn.microsoft.com/en-us/azure/defender-for-cloud/quickstart-enable-database-protections>.

More information on Microsoft Defender for Storage can be found at this link:

<https://learn.microsoft.com/en-us/azure/storage/common/azure-defender-storage-configure?tabs=azure-security-center>.

More information on Microsoft Defender for App Services can be found at this link:

<https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-app-service-introduction>.

More information on Microsoft Defender for Containers can be found at this link:

<https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-containers-introduction>.

Chapter 9

Figures



Figure 9.1 – Microsoft Defender for Cloud workload protection plans

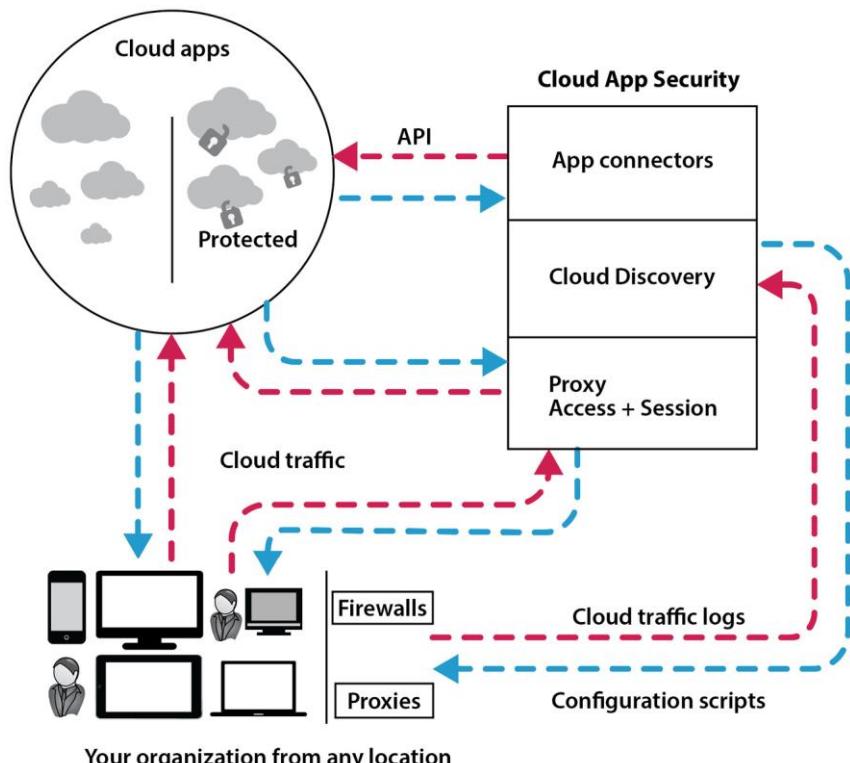


Figure 9.2 – Microsoft Defender for Cloud Apps protection workflow

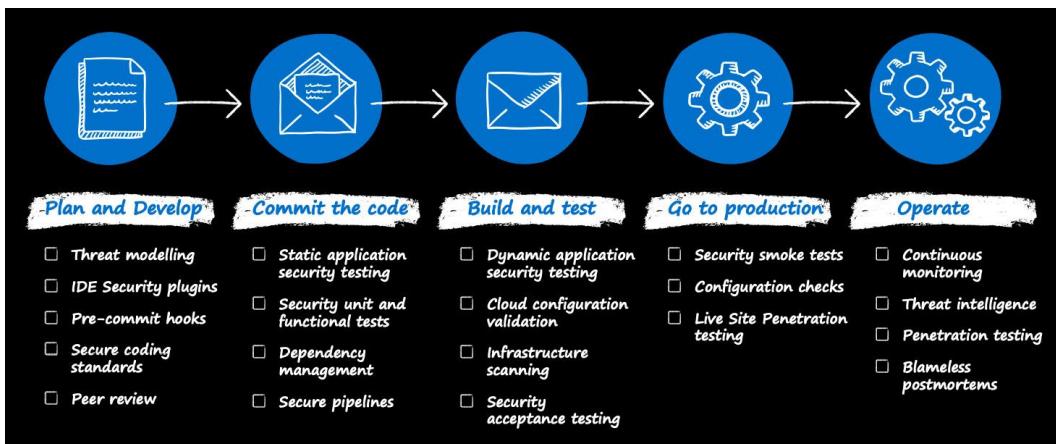


Figure 9.3 – DevSecOps and the CAF

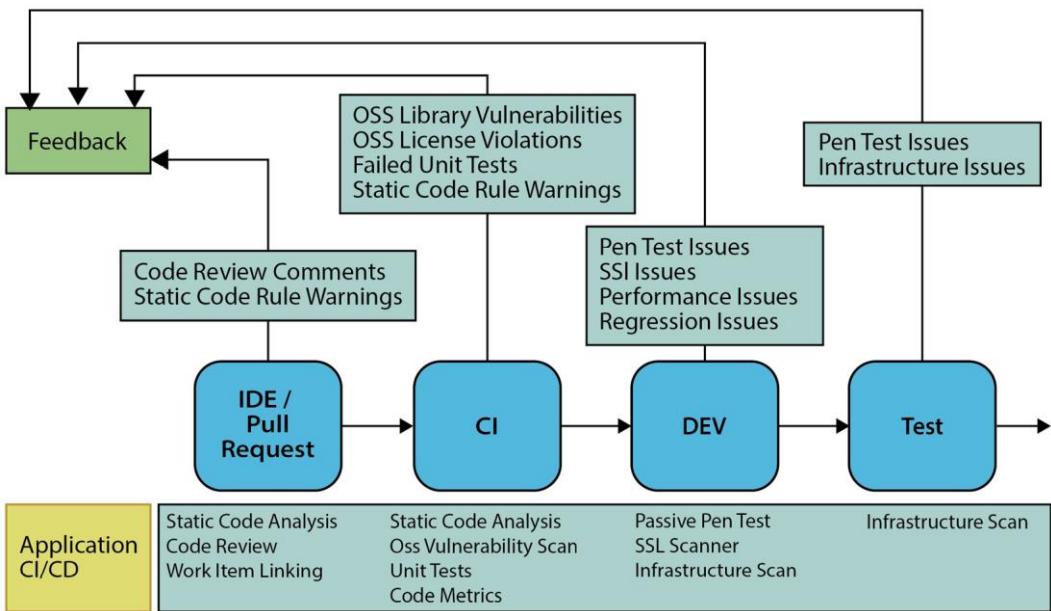


Figure 9.4 – Continuous feedback loop

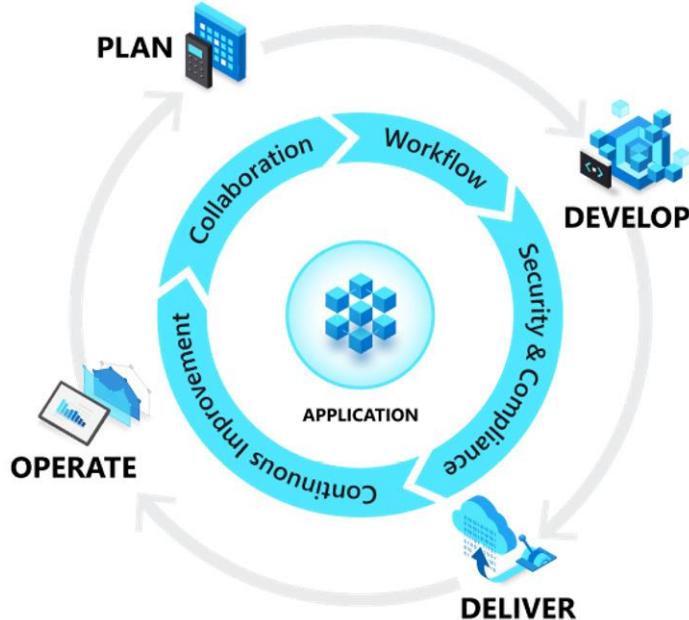


Figure 9.5 – Continuous life cycle of DevSecOps

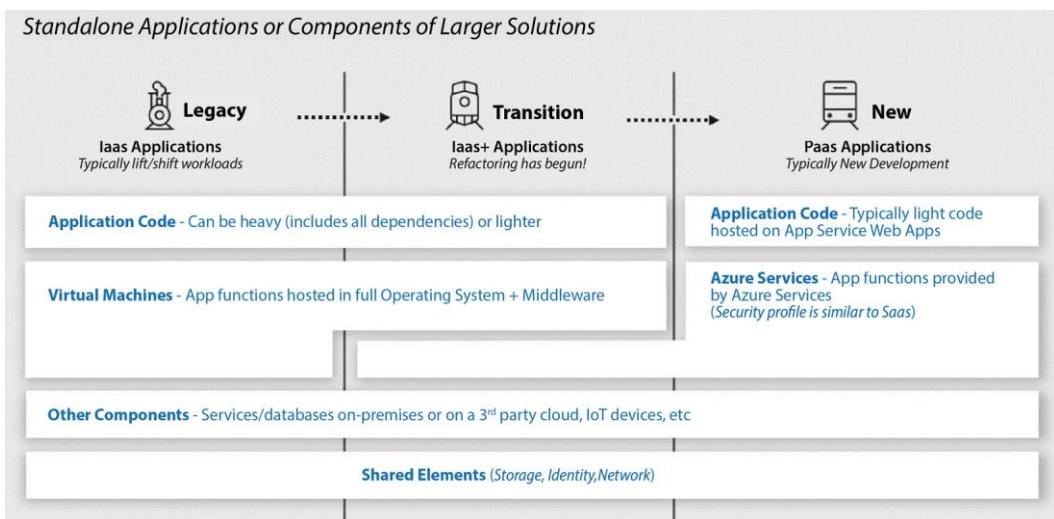


Figure 9.6 – Application evolution to PaaS

Links

More information on the CAF can be found at this link: <https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/overview>.

Additional information on SCIM can be found at this link: <https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/sync-scim>.

For more information on the DevSecOps life cycle process for application development, please see this link: <https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/secure/devsecops-controls>.

Some application security standards and frameworks that you may want to evaluate as you determine how to implement a shift left DevSecOps approach are as follows:

- Best practices for Application Registration: <https://docs.microsoft.com/en-us/azure/active-directory/develop/security-best-practices-for-app-registration>
- Threat modeling tool: <https://docs.microsoft.com/en-us/azure/security/develop/threat-modeling-tool>
- OWASP project for application security verification standards: <https://owasp.org/www-project-application-security-verification-standard/>
- NIST secure software development framework: <https://csrc.nist.gov/publications/detail/sp/800-218/final>
- STRIDE: <https://docs.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-threats>
- More information on DevSecOps can be found at this link: <https://learn.microsoft.com/en-us/devops/operate/security-in-devops>.

More information for baseline security for Azure App Services can be found at this link:

<https://learn.microsoft.com/en-us/security/benchmark/azure/baselines/app-service-security-baseline>.

Chapter 10

Figures



Figure 10.1 – The NIST RMF process

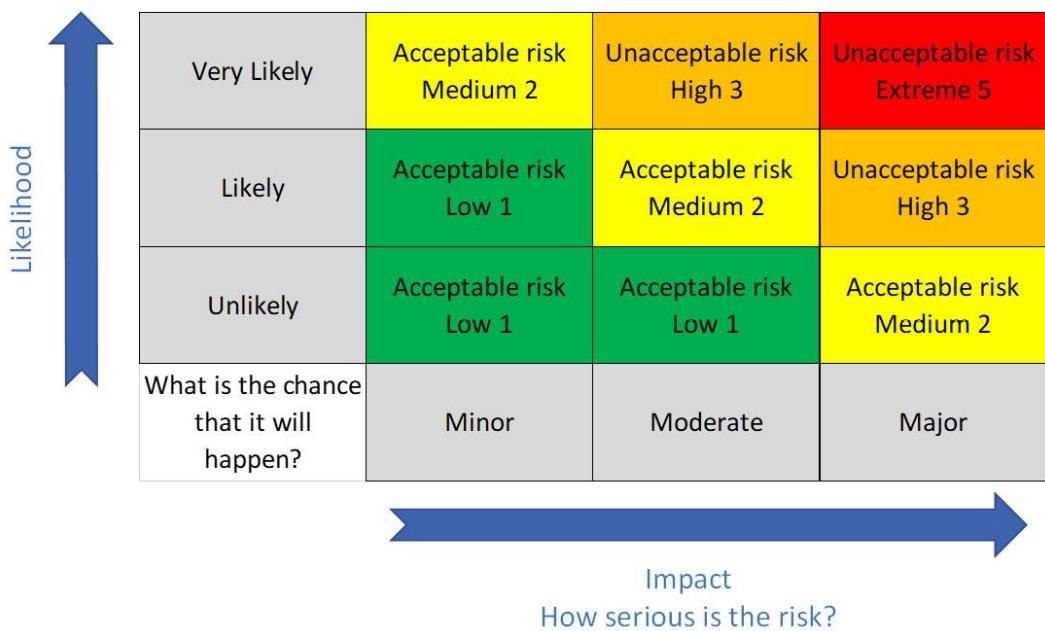


Figure 10.2 – Risk assessment categorizing

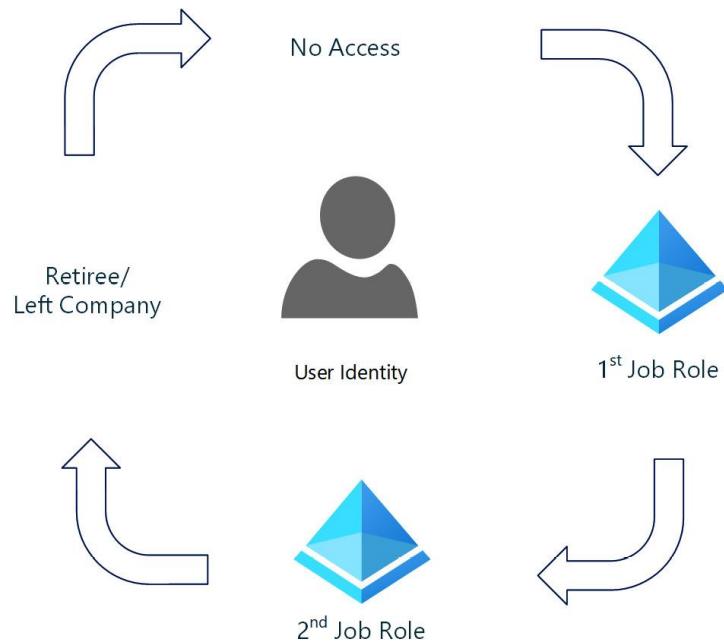


Figure 10.3 – Identity governance life cycle



Figure 10.4 – Zero-trust framework for data protection

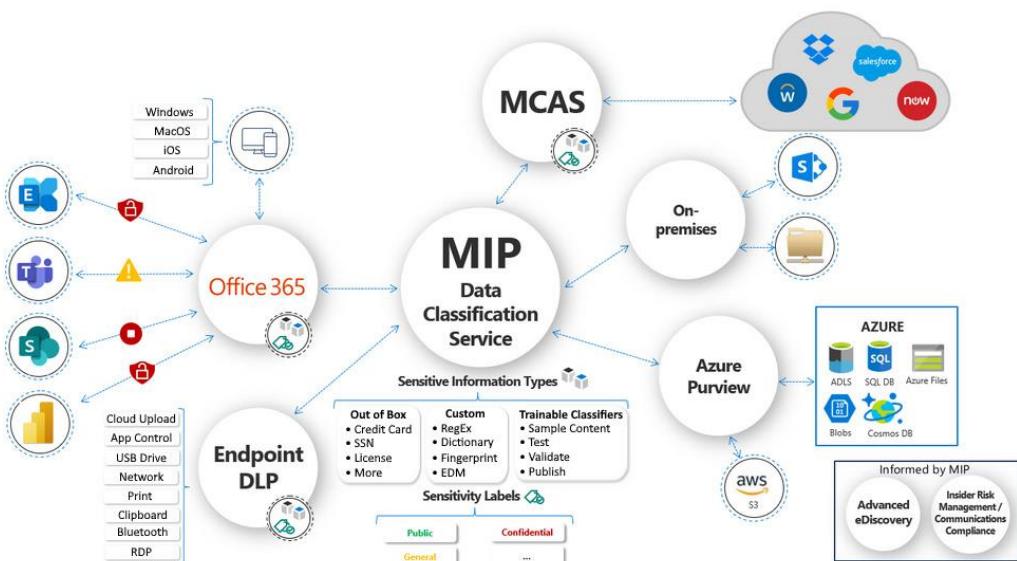


Figure 10.5 – Microsoft Information Protection workflow

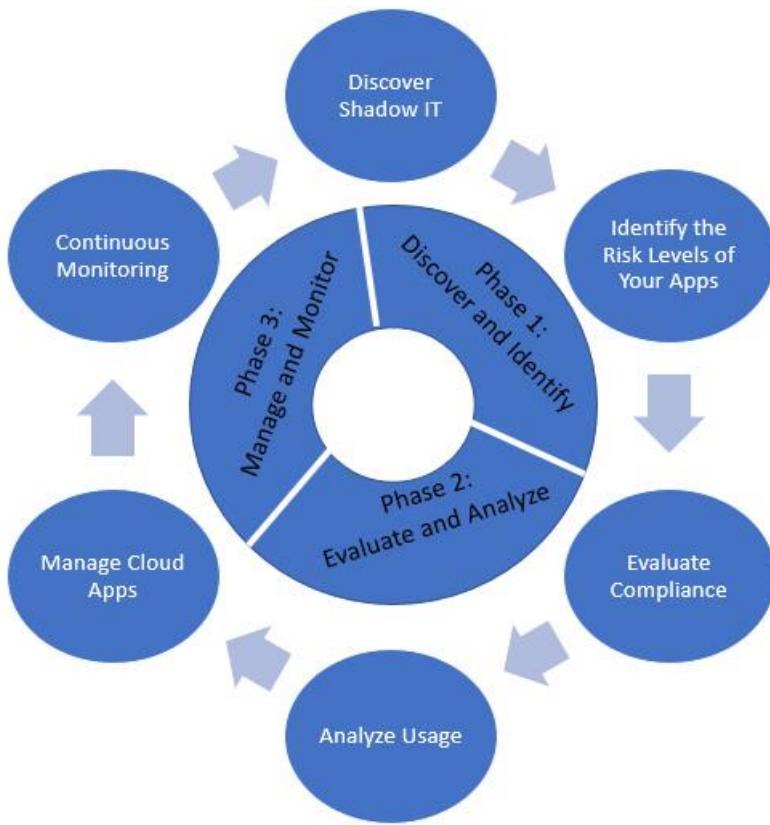


Figure 10.6 – Microsoft Defender for Cloud Apps protection workflow

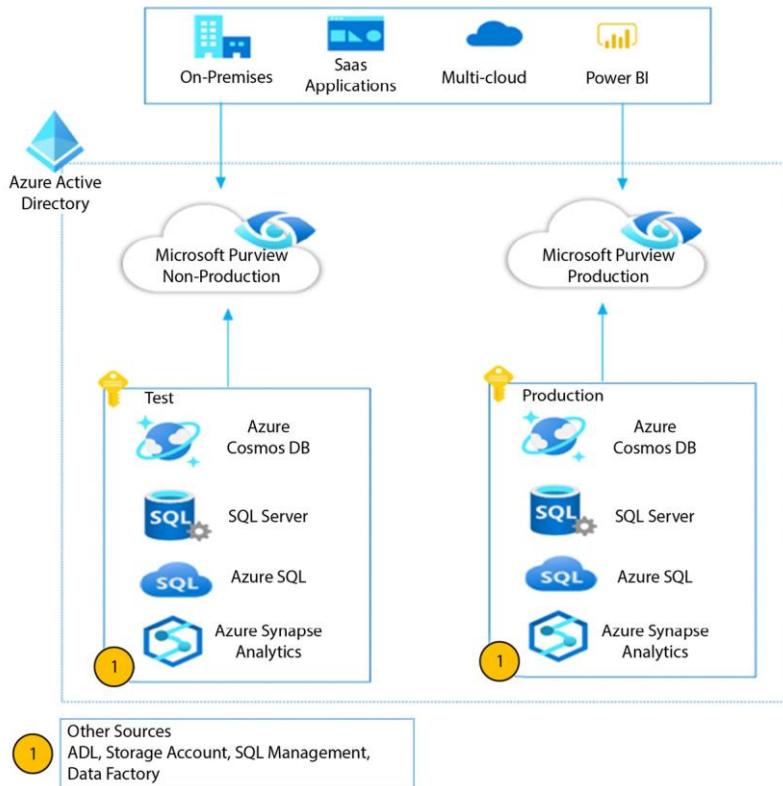


Figure 10.7 – Database segmentation for production and non-production

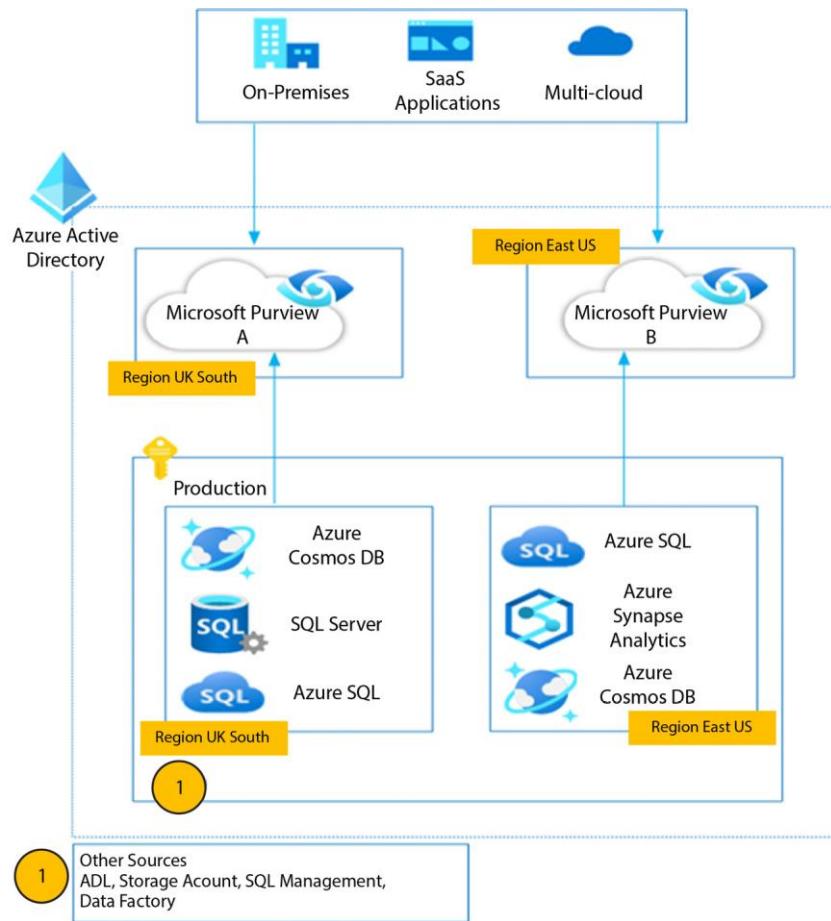


Figure 10.8 – Using Microsoft Purview to govern data sovereignty

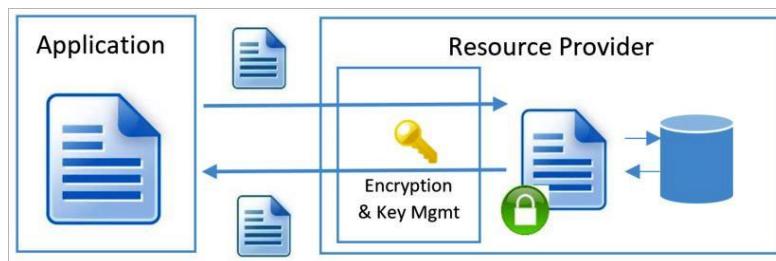


Figure 10.9 – Accessing data encrypted at rest

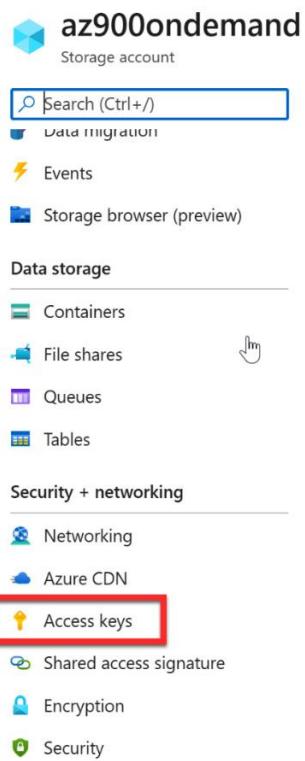


Figure 10.10 – Storage account access keys

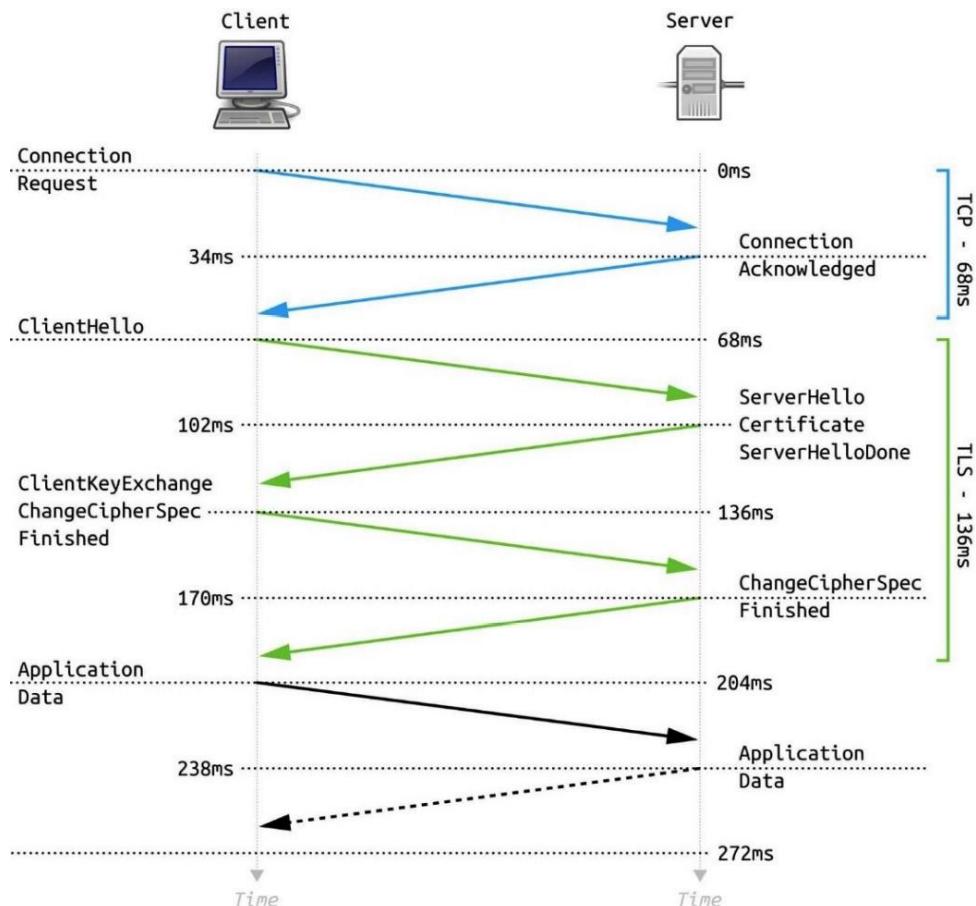


Figure 10.11 – TLS 1.2 handshake process

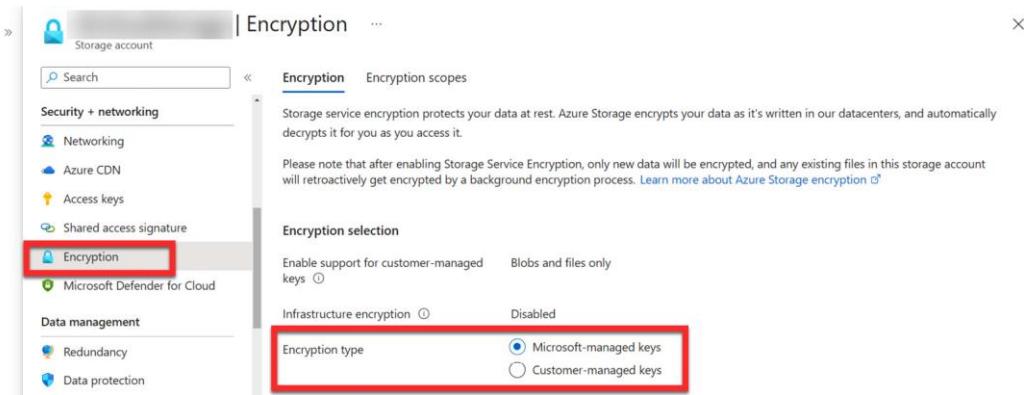


Figure 10.12 – Configuring customer-managed keys with Azure Key Vault

Links

Details on this framework can be found at this link: <https://csrc.nist.gov/Projects/risk-management/about-rmf>.

Additional information on Microsoft protection against ransomware can be found at this link: <https://learn.microsoft.com/en-us/azure/security/fundamentals/ransomware-protection>.

Architectural guidance for securing data can be found at this link: <https://learn.microsoft.com/en-us/azure/architecture/data-guide/scenarios/securing-data-solutions>

More information on Microsoft sensitivity labeling capabilities can be found at this link: <https://learn.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels-office-apps?view=o365-worldwide&preserve-view=true#support-for-sensitivity-label-capabilities-in-apps>.

More information on Data Loss Prevention can be found at this link: <https://learn.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels-office-apps?view=o365-worldwide&preserve-view=true#support-for-sensitivity-label-capabilities-in-apps>.

Information on Microsoft Purview can be found here: <https://learn.microsoft.com/en-us/microsoft-365/compliance/?view=o365-worldwide>.

Additional information on the zero-trust framework for securing data can be found at this link: <https://learn.microsoft.com/en-us/security/zero-trust/deploy/data>.

More information on how data security and privacy can be accomplished with Microsoft Defender for Cloud Apps can be found at this link: <https://learn.microsoft.com/en-us/defender-cloud-apps/cas-compliance-trust>.

Companies that are utilizing the Microsoft 365 suite of products can also integrate Microsoft Defender for Endpoint with Microsoft Defender for Cloud Apps. The steps to configure this integration can be found at this link: <https://learn.microsoft.com/en-us/defender-cloud-apps/mde-integration>.

For more information on SSE, please visit this link: <https://docs.microsoft.com/en-us/azure/storage/common/storage-service-encryption>.

For more information on ADE, please visit this link: <https://docs.microsoft.com/en-us/azure/security/fundamentals/azure-disk-encryption-vms-vmss>.

For more information on TDE, please visit this link: <https://docs.microsoft.com/en-us/azure/azure-sql/database/transparent-data-encryption-tde-overview?tabs=azure-portal>.

For more information on Azure Key Vault, please visit this link: <https://docs.microsoft.com/en-us/azure/key-vault/general/overview>.

More information on encryption best practices can be found at this link:

<https://learn.microsoft.com/en-us/azure/security/fundamentals/data-encryption-best-practices>.

Chapter 11: Case Study Responses and Final Assessment/Mock Exam

Throughout this book, you have learned about the objectives that you must master to pass the Microsoft Cybersecurity Architect exam (SC-100). The case studies throughout each section and chapter have provided you with some practical customer scenarios. These can be used for preparation and reference to help you understand the architecture of the security, compliance, and identity solutions available within Microsoft 365 and Microsoft Azure.

This chapter contains possible responses to those scenarios. There are also practice questions that can be used as a final assessment for additional preparation for passing the SC-100 exam. For information regarding the exam structure and content, review [*Appendix: Preparing for Your Microsoft Exam*](#).

This chapter contains the following sections:

- Case study sample responses
- Mock exam practice questions
- Mock exam answers and chapter reference

Case study sample responses

The following are possible responses to the case study scenarios throughout this book. These responses are based on common practices and knowledge. They are meant to provide guidance for architecting and recommending security solutions. They are not meant to be a right or wrong set of responses but should help you understand cybersecurity architecture and where Microsoft solutions can be utilized.

Chapter 4 – designing a zero-trust architecture

In this section, you will be given a company scenario and asked to complete several tasks to meet the requirements of the zero-trust architecture.

Company ABC has concerns across its Azure, on-premises, and SaaS applications' architecture. They have come to you for assistance in addressing their security concerns. They want you to provide suggestions on how they can use the security capabilities within Azure, Azure AD, and Microsoft 365 to enforce zero-trust methodologies across the company's technology infrastructure.

The possible responses for the company's areas of concern and requirements for enforcing Zero-trust include the following:

- Utilization of strong modern authentication techniques for all users, including cloud-native and on-premises directory users:
- The cybersecurity architect should develop a plan to migrate users to Azure AD as a cloud-native identity provider. For users to remain on Windows AD, you can utilize Azure AD Connect with either password hash or pass-through synchronization with password write-

back. This will allow modern authentication to new applications and the ability to utilize Azure AD MFA and Conditional Access policies.

- Applications that support modern authentication can be registered in Azure AD to use cloud-native identities for authentication and authorization.
- Guest users should only be allowed to access resources that are assigned to them, and they should be regularly reviewed:
- This can be accomplished utilizing Entitlement Management within Microsoft Entra Identity Governance
- Regular access reviews can be created with Company ABC project managers or supervisors as the reviewers
- Administrative users should have **Just-in-Time (JIT)** access to privileged resources and all access should be justified and audited:
- Microsoft Entra Identity Governance with **Privileged Identity Management (PIM)** provides JIT access. All enabled privileged access requires a justification and is audited.
- Migrating users to Azure AD as a cloud-native identity provider will allow this governance to be used across all users within the company.
- When accessing applications that contain sensitive information, users should be required to verify their identity:
- Planning, developing, and using Conditional Access policies to protect sensitive business applications should be done here. Applications and additional verification requirements for compliant devices and user-required MFA can be used for access and authorization.
- All user identities should be protected from common attacks:
- Azure AD Identity Protection will monitor user and sign-in risks. The risks include common attack vectors such as brute-force identity attacks.
- Azure AD Password protection can be used to protect against brute-force attacks by setting parameters for login frequency to block them. Password strength can be enforced by creating a dictionary of blocked passwords.
- Users that are accessing company resources from potentially dangerous locations should be forced to re-authenticate:
- Additional Conditional Access policies can be created that identify trusted and untrusted locations that can force changes in the password and/or MFA verification. Untrusted locations can also be blocked from allowing users to authenticate.
- Devices should be verified with proper security patches before accessing company resources:

- Microsoft Defender for Endpoint can be used to decrease the attack surface on Windows 10 and 11 devices
- All devices that are accessing company resources should be managed with Microsoft Intune MDM or MAM
- Conditional Access policies can be created to verify that devices follow Microsoft Intune policies before accessing applications
- Users should be analyzed for anomalous behavior and potential threats to identities:
- Azure AD Identity Protection will monitor user and sign-in risks. This solution will monitor for potential threats and anomalous user behavior.
- Creating a user risk policy can protect users, identify anomalies, and protect against unauthorized access from risky users.
- Network resources with sensitive information should not be accessible through publicly available connections:
- Network infrastructure and resources should be designed with VNet segmentation. Resources containing sensitive information should be on their own dedicated VNet. Access through the network should be protected more securely than VNet peering. Network and Application Security Groups should have rules for how traffic goes between VNet segments and subnets to the private VNets.
- Data on applications should also be identified, classified, and protected by using sensitivity labels. Sensitivity labels should be configured within DLP policies to decrease the potential for over-sharing of data by users.
- Data that is being accessed across networks, both private and public, can be protected with private endpoint connections or service endpoints within **Network Security Groups (NSGs)**.
- All activity and event data should be logged and can be reviewed:
- Azure Monitor should be turned on for all Azure resources
- Azure Arc can extend the monitoring to non-Azure resources
- Microsoft 365 monitors and logs SaaS activity
- Log Analytics and Microsoft Sentinel can be used to connect all data sources and provide a single location for monitoring and reviewing events and activities for malicious activity
- Reports can be generated for executive reviews and incident handling:
- Taking these steps when monitoring activities and events allows the creation of reports for review. This information can also be used in custom dashboards, workbooks, and Power BI.

Chapter 5 – designing for regulatory compliance

In this section, you will be given a company scenario and asked to complete several tasks to meet the requirements of adhering to regulatory, data residency, and privacy requirements.

Company ABC has concerns across its Azure, on-premises, and SaaS applications architecture. They have come to you for assistance in addressing their regulatory and privacy concerns. They want you to provide suggestions on how they can use the standards and regulatory compliance and privacy capabilities within Microsoft and Azure to govern data residency and data privacy across the company's technology infrastructure.

The possible responses for the company's areas of concern and requirements include the following:

- The company has recently begun to handle credit card transactions and they need to audit compliance with PCI-DSS:
- In the Microsoft 365 Purview compliance portal, the PCI-DSS assessment template can be run in the Compliance Score area to determine SaaS and Azure SQL Database compliance with PCI-DSS.
- In Azure, Microsoft Defender for Cloud can be used when turning on the Defender Plans. The PCI-DSS policy initiative can be enabled from within the Standards and Compliance menu. Resources will be assessed and audited for compliance and remediation actions will be provided as guidance.
- The company has expanded outside of the United States and is now doing business in Germany. They need to make sure that they are adhering to the standards for data residency within Germany:
- Azure Policy has built-in initiatives that can be enabled for various geographically-specific regulatory requirements.
- As a cybersecurity architect, you should be familiar with the residency requirements in certain countries. Germany is particularly stringent in their requirements, and the first recommendation that you should have is to create a segmented Azure Resource Group for the German region for proper governance.
- The company is concerned that data is not properly classified, and sensitive data may be exposed. They need a recommendation to identify any sensitive data and classify it:
- Microsoft Purview Compliance can be used for the identification and classification of sensitive data within Microsoft 365, Azure Storage, Azure SQL Database, and multi-cloud storage resources, such as AWS S3
- Sensitive data that is identified can be governed by sensitivity labels and policies to avoid the exposure of this data
- Data Loss Prevention policies can be used to avoid oversharing data

- With PCI-DSS, they need to make sure that encryption keys are not being managed by the individual Azure services, such as Azure Storage and SQL Database. They need a recommendation to better manage keys:
- Azure Key Vault provides the separation of duties and allows the company to manage the keys. They need additional configuration to change the encryption in Azure Storage and Azure SQL Database from Microsoft-managed to customer-managed keys.
- The company needs to audit current resources for PCI-DSS compliance and verify that all virtual machines are encrypted:
- Azure Policy can be enabled to address the need to audit resources for Azure Disk Encryption to be enabled on virtual machines that are monitored with Azure Monitor or Azure Arc
- Additional improvement recommendations and auditing for compliance can be accessed within Microsoft Defender for Cloud
- Users that are accessing intranet applications must not be allowed to use a public internet connection. How would you recommend securing this communication?
- Point-to-site VPN connections through a VPN Gateway should be designed to secure the communication channels of users accessing applications. Private endpoints can be created between applications and data within storage accounts and databases.

Chapter 6 – evaluating the security posture

In this section, you will be given a company scenario and asked to complete several tasks to meet the requirements to evaluate the company's security posture.

Company ABC has concerns about the security posture across its Azure, on-premises, and SaaS applications architecture. They have come to you for assistance in addressing their current security controls and the level of compliance with the Microsoft Security Benchmark and PCI-DSS 3.2.1. They want you to provide suggestions on how they can use regulatory compliance, secure score, and workload protections to decrease risks and vulnerabilities and create a better security posture.

The possible responses for the company's areas of concern and requirements include the following:

- The company has heard that the Azure Security Benchmark will provide a good start to building a secure environment and wants to know where its current environment stands with its security controls:
- Microsoft Defender for Cloud provides the evaluation and continuous assessment of resources by default within your tenant. The **Security Posture** menu provides the level of security with Secure Score improvement actions to increase the overall security posture.
- They would also like to evaluate their level of compliance with PCI-DSS 3.2.1 controls:
- Microsoft Defender plans need to be enabled. This will enable the Standards and Compliance dashboard to evaluate and audit resource compliance to PCI-DSS.

- The company has multiple virtual networks with virtual machines. They are concerned that they may have vulnerabilities on these networks and ports:
- The Microsoft Defender for Server plan will assess vulnerabilities and threats on virtual machines in Azure and non-Azure VMs that are using Azure Monitor or Azure Arc. Vulnerability assessments can also be enabled in Workload Protections.
- Network hardening and the network map can be evaluated within Workload Protections to view a map with open and exposed ports.
- The company wants to know what areas of security and governance should be included in its cloud architecture and cloud landing zones:
- Microsoft provides guidance and methodology. Links have been provided for security, management, governance, and readiness within this chapter:
- **Security:** Controls and protection processes for securing the cloud environments: <https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/landing-zone/design-area/security>
- **Management:** Creating ongoing operations procedures and management baselines, and protection and recovery capabilities: <https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/landing-zone/design-area/management>
- **Governance:** Policies to automate auditing and enforcement of compliance: <https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/landing-zone/design-area/governance>
- **Ready and automation:** Utilize tools and templates to deploy and automate the creation of landing zones and resources: <https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/landing-zone/design-area/platform-automation-devops>

Chapter 7 – designing a secure architecture for endpoints

In this section, you will be given a company scenario and asked to complete several tasks to meet the requirements to evaluate and create a strategy for securing server and client endpoints.

Company ABC has a hybrid architecture that utilizes AD DS on-premises domains and servers as well as Azure virtual machines. Servers within both environments are a combination of Linux and Windows. Users connect to these resources through Windows 10 laptops and mobile smartphones with iOS and Android operating systems.

You have been asked to provide recommendations on ways to secure the servers and user devices that will provide a central capability to manage through Microsoft solutions. The company has also asked you to evaluate its current security operations processes and provide recommendations to be more effective in utilizing best practices.

The possible responses for the company's areas of concern and requirements include the following:

- An on-premises server monitoring and management strategy:
- Azure Arc can extend this monitoring to non-Azure resources

- An Azure virtual machine monitoring and management strategy:
- Azure Monitor should be turned on for all Azure resources
- A remote administration strategy for on-premises and Azure virtual machines:
- Accessing virtual machines should be accomplished by utilizing Azure Bastion, or at a minimum, JIT virtual machine access through Microsoft Defender for Server plans
- A protection and security strategy for Windows, iOS, and Android devices:
- Microsoft Intune MDM configuration and compliance policies should be used here
- A remote access strategy for remote user devices to access applications. This includes supporting user devices:
- Microsoft Defender for Endpoint should be used to protect endpoints; access to these devices can be protected with Customer Lockbox features
- A security operations strategy for processes, procedures, and investigation:
- Log Analytics and Microsoft Sentinel can be used to connect all data sources and provide a single location for monitoring and reviewing events and activities for malicious activity. Microsoft 365 Defender and Microsoft Defender for Endpoint can be used to further investigate security incidents and threats.

Chapter 8 – security requirements for IaaS, PaaS, and SaaS

In this section, you will be given a company scenario and asked to complete several tasks to meet the requirements to evaluate and create a strategy for securing server and client endpoints.

Company ABC has a cloud architecture with a combination of IaaS, PaaS, and SaaS services. The current environment utilizes Microsoft 365 for collaboration tools with OfficeSuite and Microsoft Teams. They have an application built on Docker containers with an Azure SQL Database. They have a modern web application for the e-commerce site on Azure App Services with a CosmosDB database for global reach. Company ABC has also some SQL databases on Azure Virtual Machines that are connected to on-premises applications.

You have been asked to provide the security requirements necessary to secure the various connections and the solutions to put in place to manage the security posture for IaaS, PaaS, and SaaS solutions.

The possible responses for the company's areas of concern and requirements include the following:

- Security recommendations for virtual machine connections for SQL databases connected to on-premises resources:
- Microsoft Defender for Cloud policies will evaluate for security controls for these resources and workload protection plans with Defender for Server and Defender for Database to provide additional threat detection and alerts.
- Private connections with Private Link, Virtual WAN, ExpressRoute, and VPN Gateways can be used to secure connections without exposing them to the public internet.

- Security recommendations for Azure App Services with CosmosDB:
- Microsoft Defender for App services and Defender for databases will provide security recommendations
- Access between these resources should utilize private connections and not be exposed to the internet
- Security recommendations for the Docker container application with Azure SQL Database:
- Microsoft Defender for Databases provides guidance and recommendations for securing these resources
- Connections between containers and databases should be private and not exposed to the internet
- Security recommendations for Microsoft 365 services:
- Utilizing Microsoft 365 Defender capabilities across all Microsoft 365 resources, including Microsoft Defender for Cloud Apps for monitoring and managing compliance applications and determining shadow IT

Chapter 9 – security requirements for applications

In this section, you will be given a company scenario and asked to complete several tasks to meet the requirements to determine the security requirements for applications.

Company ABC is planning a data center exit for its application workloads. As part of this strategy, they want to apply a DevSecOps approach to application development and modernization. As applications are moved to the cloud, these applications should be monitored, managed, and secured by utilizing cloud security services.

You have been asked to provide the security requirements necessary to secure applications that are migrating to the cloud to IaaS and PaaS solutions.

The possible responses for the company's areas of concern and requirements include the following:

- Security requirements for lift and shift applications:
- All applications and data migration should be evaluated for any changes in the network and IaaS infrastructure before moving to cloud technologies
- Security baselines and policies should be in place and part of the new infrastructure landing zone before migration
- Security requirements for re-platformed applications:
- Plan and identify the security requirements and the changes in responsibility that will be in place when moving from IaaS to PaaS technologies
- Determine the security solutions that will be the company's requirements on the new platforms and turn on those capabilities

- Security requirements for re-factored applications:
- Plan for the requirements and the security that is available on the various App Services tiers
- Test the new application code and secure APIs used to connect to resources and applications
- Outline an approach for DevSecOps development for all applications migrating to Azure, including the following:
 - An application testing and deployment strategy:
 - SAST, DAST, and continuous runtime testing should be a part of the overall application testing and deployment strategy
 - An approval workflow for verifying application security:
 - Once the application code has been tested, the tests should be verified and approved for deployment to production

Chapter 10 – designing a strategy to secure data

Company ABC is planning a data center exit for its application and data workloads. As part of this strategy, they want to apply an approach to protect and provide resiliency to its data. As data and databases are moved to the cloud, this data should be protected, monitored, managed, and secured by utilizing cloud security services.

You have been asked to provide the security requirements necessary to secure data that is migrating to the cloud to SaaS, IaaS, and PaaS solutions. This includes making sure that data is not exposed when in transit or storage.

The possible responses for the company's areas of concern and requirements include the following:

- Security requirements for data at rest:
- Encryption should be enabled for all data across the company. This includes using Azure Key Vault for customer-managed keys.
- For storage accounts, **Storage Service Encryption (SSE)** should be used.
- For virtual machines, **Azure Disk Encryption (ADE)** should be used.
- For databases, **Transparent Data Encryption (TDE)** should be used.
- Security requirements for data in motion:
- All data transmission should utilize encrypted transmission channels with TLS/SSL over HTTPs, at a minimum. Where possible, secure VPN or dedicated communication channels should be designed into the network architecture.
- When possible, create service endpoints within NSGs to secure where data is transmitted.
- Security requirements for protecting data against attacks:
- Microsoft Defender plans for Azure databases and storage accounts can protect workloads and alert them about potential attacks.

- Microsoft 365 Defender protects data in SaaS applications through the utilization of Microsoft Defender for Cloud Apps. Additional solutions within the Microsoft 365 Defender portal can be used to identify threats and vulnerabilities.
- Microsoft Defender for Cloud Apps provides monitoring and protection from malicious activity and threats.
- Security requirements for classifying, protecting, and retaining data:
- Microsoft Purview compliance should be used to classify data across Microsoft 365, Azure, and multi-cloud data infrastructure
- Azure SQL Database has additional data classification and automated data masking capabilities

Mock exam practice questions

In this assessment, you can expect the following:

- Number of questions: 65
- Multiple choice and true/false

Questions

For a true exam experience, attempt this assessment as a closed book and give yourself 190 minutes to take the assessment. Have a notepad to answer the questions and then review the answers to grade your exam and determine areas needed for additional review. The recommendation for practice assessments is that you should be able to score 90% or better. Once you have attained this score, you should be ready to sit and pass the SC-100 exam. So, let's begin...

1. Planning and architecting security at multiple levels is known as _____.
 A. Defense in depth
 B. Zero trust
 C. Risk management
 D. Privileged access
2. When determining the security requirements for a cloud service, which service type has the most security responsibility on the customer?
 A. IaaS
 B. PaaS
 C. SaaS
 D. FaaS

3. In security operations, which team is used to run simulated attacks to test the security posture of the company?
 - A. Red team
 - B. Blue team
 - C. Yellow team
 - D. Purple team
4. In a cyber attack, where does an attacker steal data?
 - A. Lateral movement
 - B. Exploitation
 - C. Reconnaissance
 - D. Exfiltration
5. Zero-trust frameworks are built based on what statement?
 - A. Identity is the new perimeter
 - B. Identity is the new control plane
 - C. Trust no one, verify everything
 - D. Always use MFA
6. Microsoft provides guidance on planning and building security requirements with which of the following?
 - A. Microsoft Defender for Cloud
 - B. Azure Cloud Adoption Framework
 - C. Azure Security Benchmark
 - D. Microsoft Cybersecurity Reference Architecture
7. Microsoft provides guidance on planning for a zero-trust framework with which of the following?
 - A. Secure Access Service Edge
 - B. Rapid modernization plan
 - C. Threat analysis
 - D. Risk framework
8. What measures the percentage of loss of an asset when doing a risk analysis?

- A. Exposure factor
 - B. Single loss expectancy
 - C. Annualized loss expectancy
 - D. The annualized rate of occurrence
9. What does Microsoft provide in Azure to all customers to protect the perimeter of the Azure infrastructure?
- A. Azure Firewall
 - B. Web Application Firewall
 - C. Application Gateway
 - D. DDoS protection
10. What are two ways to build resiliency in a secure architecture?
- A. Network segmentation
 - B. Duplicate resources in separate regions
 - C. Single region architecture
 - D. Public access to virtual machines
11. When developing a security operations life cycle for managing threats, what is done at the threat analytics stage?
- A. Discover vulnerable assets
 - B. Stay informed with threat intelligence
 - C. Identify suspicious behaviors
 - D. Remediate compromised assets
12. In the process and procedures of security operations, what determines the time it takes to respond to a threat?
- A. Mean time to acknowledge
 - B. Mean time to remediate
 - C. Incidents remediated
 - D. Escalation between each tier
13. Monitoring non-Azure virtual machines can be accomplished by using which solution?
- A. Log Analytics

- B. Azure Monitor
 - C. Azure Arc
 - D. Network Watcher
14. If you want to monitor and manage third-party SaaS applications, such as Salesforce, you can create policies within which solution?
- A. Microsoft Defender for Cloud
 - B. Microsoft Defender for Endpoint
 - C. Microsoft Defender for Cloud Apps
 - D. Microsoft Defender for Identity
15. Tier 2 of managing a security incident is known as what?
- A. Triage
 - B. Hunt
 - C. Automation
 - D. Investigation
16. The principle of least privilege is defined as _____.
- A. The concept that a user or resource only has access to the applications and information required to perform their specific duties
 - B. The concept that a user has global administrator privileges to access all applications within the company
 - C. The concept that a user must request access to applications and information every time they need to complete their duties
 - D. The concept that a user has no administrator access, regardless of their job role
17. There are three levels of Identity and Access Management: traditional, advanced, and optimal. Which of the following characteristics is not included in optimal identity and access management?
- A. Password-less authentication
 - B. Multi-factor authentication is enforced
 - C. Single sign-on is not present
 - D. User behavior is analyzed in real time for possible risks
 - E. None of the above

18. You have created an Azure AD tenant. You also have an on-premises Windows AD that includes users and groups. What can you use to bring together a hybrid infrastructure for Azure AD cloud applications and synchronize on-premises users and groups for identity and access management?
- A. Application proxy
 - B. AD FS
 - C. Azure AD Connect
 - D. External identities
19. The verification workflow of a zero-trust identity model includes which of the following? Select all that apply.
- A. Signal
 - B. Trigger
 - C. Decision
 - D. Enforcement
20. Which service implements zero-trust for identity and access within Azure AD?
- A. Azure AD Identity Protection
 - B. Privileged Identity Management
 - C. Identity Governance
 - D. Conditional Access
21. What is the primary use of Microsoft Defender for Cloud Apps?
- A. Discovery apps to monitor for Shadow IT
 - B. Assigning cloud apps to users
 - C. Registering for cloud apps licensing
 - D. All of the above
22. Which service provides JIT administrator access that is time-bound to decrease the attack surface of elevated privileges?
- A. Identity Protection
 - B. Access Packages
 - C. Privileged Identity Management
 - D. Microsoft Defender for Cloud

23. Microsoft Sentinel's workflow provides the following, in order:

- A. Respond, collect, detect, investigate
- B. Collect, detect, investigate, respond
- C. Investigate, detect, collect, respond
- D. Detect, collect, investigate, respond

24. Concerning a cyber-attack, exfiltration is when:

- A. An attacker cuts off access to resources.
- B. An attacker has gained access to a system and is ready to exploit it. They will want to gain administrative-level access.
- C. An attacker has gained access to sensitive information, and they can remove that information to harm in some way.
- D. Attackers attempt to keep their access anonymous.

25. PCI-DSS and HIPAA are examples of what?

- A. Government standards
- B. Industry standards
- C. Regulatory standards
- D. Company standards

26. What is the last step in the Azure Policy workflow?

- A. Tightly define the policy
- B. Audit your existing resources
- C. Deploy your policy
- D. Continuously monitor your policy

27. How can you govern data residency within Azure resources?

- A. Create an allowed locations policy
- B. Enforce encryption on data
- C. Create an Azure backup policy
- D. Enforce Azure Resource groups

28. In Microsoft Defender for Cloud, what information can be used to find improvement actions that will create a better security posture based on the Azure Security Baseline?

- A. Compliance dashboard
 - B. Secure Score
 - C. Vulnerability scanning
 - D. JIT VM access
29. The first step in enforcing security posture management of your resources is what?
- A. Threat modeling
 - B. Real-time risk scoring
 - C. Zero-trust access control
 - D. Discover risk exposure
30. All resources within Azure are evaluated based on _____ to determine the Secure Score.
- A. PCI-DSS
 - B. CIS
 - C. Microsoft Security Benchmark
 - D. NIST 800-53
31. To evaluate the security posture and protect workloads, you must enable which of the following?
- A. Microsoft Sentinel
 - B. Microsoft Defender plans
 - C. Microsoft Defender for Identity
 - D. Microsoft Defender for Cloud Apps
32. When designing a secure cloud landing zone, which areas should be the focus?
- A. Security
 - B. Management
 - C. Governance
 - D. Automation
 - E. All of the above
33. The _____ framework provides guidance for a cloud journey and its continued security operations.

A. Well-architected

B. Risk management

C. Zero-trust

D. Cloud adoption

34. What can be used to detect the directory in AD DS from attacks on users?

A. Microsoft Defender for Endpoint

B. Azure AD Identity Protection

C. Microsoft Defender for Identity

D. Microsoft Defender for Server

35. What is the best option for managing company-owned devices with Microsoft Intune?

A. Conditional Access Policies

B. Identity Protection

C. Mobile Application Management

D. Mobile Device Management

36. What solution allows you to manage TLS/SSL certificates for securing your websites?

A. Data Loss Prevention

B. Azure Key Vault

C. Microsoft Defender for Cloud Apps

D. Azure AD App Registration

37. Secure remote access to Azure virtual machines can be accomplished by logging in to a remote session within the Azure portal using which of the following?

A. Jump box

B. JIT VM access

C. Azure Bastion

D. Public IP address

38. What solution can be used to identify applications that are being accessed on registered devices and the company network?

A. Microsoft Defender for Cloud Apps

B. Microsoft Defender for Endpoint

C. Microsoft Intune

D. Microsoft Defender for Cloud

39. What solution can be used to determine and detect the security requirements for warehouse environment sensors?

A. Microsoft Defender for Endpoint

B. Microsoft Defender for Servers

C. Microsoft Defender for IoT

D. Microsoft Defender for Apps

40. Enforcing compliance across all data and storage accounts in Microsoft 365, Azure, and multi-cloud is accomplished within which solution?

A. Microsoft Defender for Cloud

B. Microsoft Sentinel

C. Microsoft Purview

D. Microsoft 365 Defender

41. To avoid exposure of keys and secrets within Azure App Services, you should use which solution?

A. Azure AD App Registration

B. Microsoft Defender for App Services

C. Microsoft Defender for databases

D. Azure Key Vault

42. Data classification is governed by what Microsoft 365 service?

A. Sensitivity labels and policies

B. Retention labels and policies

C. Data loss prevention policies

D. Records management

43. Which type of application testing uses an “eye test” on the application code?

A. DAST

B. SAST

C. Runtime testing

D. Black-box testing

44. Within a DevSecOps life cycle, where do security and compliance fall within the workflow?

- A. Plan – Develop
- B. Develop – Deliver
- C. Deliver – Operate
- D. Operate – Plan

45. To protect and mitigate threats to applications, access to resources should be protected with a plan for _____.

- A. Identity and secret handling
- B. Segmentation and configuration
- C. Static and dynamic testing
- D. Data handling

46. Discovering applications being accessed from your network can be identified by using which of the following?

- A. Microsoft Defender for Cloud Apps
- B. Microsoft Defender for Cloud
- C. Microsoft Sentinel
- D. Azure Log Analytics

47. Static Application Security Testing should be done in which phase of the Cloud Adoption process?

- A. Plan and develop
- B. Commit the code
- C. Build and test
- D. Go to production
- E. Operate

48. When protecting against a possible ransomware attack, what can protect against data loss and allow for recovery?

- A. Azure Backup
- B. Privilege Identity Management

- C. Identity Governance
 - D. Azure Disk Encryption
49. Creating policies to automatically retain, delete, and store data takes place at what stage of the data protection process?
- A. Know your data
 - B. Protect your data
 - C. Prevent data loss
 - D. Govern your data
50. Governing data in databases can be accomplished with which solution?
- A. Microsoft Defender for Cloud Apps
 - B. Microsoft Purview
 - C. Microsoft Defender for Endpoint
 - D. Microsoft Defender for Identity
51. What is the best option for securing communication between Azure and on-premises data center resources?
- A. VPN Gateway
 - B. Application Gateway
 - C. HTTPS TLS link
 - D. Point-to-site VPN

Mock exam answers and chapter reference

We recommend that you review these answers after attempting to answer the aforementioned questions. Check your answers and review the sections within the chapters mentioned for additional clarification:

1. The answer is A. Planning and architecting security at multiple levels is known as Defense in Depth. The others are all additional security frameworks and methodologies that can be used throughout the Defense in Depth architecture design. ***Chapter 1, Cybersecurity in the Cloud.***
2. The answer is A. When determining the security requirements for a cloud service, IaaS has the most security responsibility to the customer. ***Chapter 1, Cybersecurity in the Cloud.***
3. The answer is A. In security operations, the red team is used to run simulated attacks to test the security posture of the company. ***Chapter 1, Cybersecurity in the Cloud.***

4. The answer is D. In a cyber attack, an attacker steals data during the exfiltration phase. [**Chapter 1, Cybersecurity in the Cloud**](#).
5. The answer is C. Zero-trust frameworks are built based on the statement of trust no one, verify everything. [**Chapter 1, Cybersecurity in the Cloud**](#).
6. The answer is D. Microsoft provides guidance on planning and building security requirements with the Microsoft Cybersecurity Reference Architecture. [**Chapter 2, Building an Overall Security Strategy and Architecture**](#).
7. The answer is B. Microsoft provides guidance on planning for a zero-trust framework with the Rapid Modernization plan. [**Chapter 2, Building an Overall Security Strategy and Architecture**](#).
8. The answer is A. The exposure factor measures the percentage of loss of an asset when doing a risk analysis. [**Chapter 2, Building an Overall Security Strategy and Architecture**](#).
9. The answer is D. DDoS protection is provided by Microsoft in Azure to all customers to protect the perimeter of the Azure infrastructure. [**Chapter 2, Building an Overall Security Strategy and Architecture**](#).
10. The answers are A and B. Network segmentation and duplicating resources in separate regions are two ways to build resiliency in a secure architecture. [**Chapter 2, Building an Overall Security Strategy and Architecture**](#).
11. The answer is B. When developing a security operations life cycle for managing threats, “Stay informed with threat intelligence” is done at the threat analytics stage. [**Chapter 3, Designing a Security Operations Strategy**](#).
12. The answer is A. In the process and procedures of security operations, the mean time to acknowledge determines the time it takes to respond to a threat. [**Chapter 3, Designing a Security Operations Strategy**](#).
13. The answer is C. Monitoring non-Azure virtual machines can be accomplished by using Azure Arc. [**Chapter 3, Designing a Security Operations Strategy**](#).
14. The answer is C. If you want to monitor and manage third-party SaaS applications, such as Salesforce, you can create policies in Microsoft Defender for Cloud Apps. [**Chapter 3, Designing a Security Operations Strategy**](#).
15. The answer is D. Tier 2 of managing a security incident is known as investigation. [**Chapter 3, Designing a Security Operations Strategy**](#).
16. The answer is A. The principle of least privilege is defined as the concept that a user or resource only has access to the applications and information required to perform their specific duties. [**Chapter 4, Designing an Identity Security Strategy**](#).

17. The answer is C. There are three levels of Identity and Access Management: traditional, advanced, and optimal. Single sign-on is present, so this answer is not included in optimal identity and access management. *Chapter 4, Designing an Identity Security Strategy*.
18. The answer is C. You have created an Azure AD tenant. You also have an on-premises Windows Active Directory that includes users and groups. Azure AD Connect is used to bring together a hybrid infrastructure for Azure AD cloud applications and synchronize on-premises users and groups for identity and access management. *Chapter 4, Designing an Identity Security Strategy*.
19. The answers are A, C, and D. The verification workflow of a zero-trust identity model includes signal, decision, and enforcement. *Chapter 4, Designing an Identity Security Strategy*.
20. The answer is D. Conditional Access is the service that implements zero-trust for identity within Azure AD. *Chapter 4, Designing an Identity Security Strategy*.
21. The answer is A. Discovery of apps to monitor for Shadow IT is a primary use of Microsoft Defender for Cloud Apps. *Chapter 4, Designing an Identity Security Strategy*.
22. The answer is C. Privileged Identity Management is the service that provides JIT administrator access that is time-bound to decrease the attack surface of elevated privileges. *Chapter 4, Designing an Identity Security Strategy*.
23. The answer is B. Microsoft Sentinel's workflow includes collect, detect, investigate, and respond. *Chapter 3, Designing a Security Operations Strategy*.
24. The answer is C. Concerning a cyber-attack, exfiltration is when an attacker has gained access to sensitive information, and they can remove that information to harm in some way. *Chapter 1, Cybersecurity in the Cloud*.
25. The answer is B. PCI-DSS and HIPAA are examples of Industry standards. *Chapter 5, Designing a Regulatory Compliance Strategy*.
26. The answer is D. Continuously monitoring your policy is the last step in the Azure Policy workflow. *Chapter 5, Designing a Regulatory Compliance Strategy*.
27. The answer is A. You govern data residency within Azure resources by creating an allowed location policy. *Chapter 5, Designing a Regulatory Compliance Strategy*.
28. The answer is B. In Microsoft Defender for Cloud, secure score can be used to find improvement actions that will create a better security posture based on the Azure Security Baseline. *Chapter 5, Designing a Regulatory Compliance Strategy*.
29. The answer is C. The first step in enforcing security posture management of your resources is zero-trust access control. *Chapter 6, Evaluating the Security Posture and Recommending Technical Strategies to Manage Risk*.

30. The answer is C. All resources within Azure are evaluated based on the Azure Security Benchmark to determine the Secure Score. *Chapter 6, Evaluating the Security Posture and Recommending Technical Strategies to Manage Risk.*
31. The answer is B. To evaluate the security posture and protect workloads, you must enable Microsoft Defender plans. *Chapter 6, Evaluating the Security Posture and Recommending Technical Strategies to Manage Risk.*
32. The answer is E. When designing a secure cloud landing zone, security, management, governance, and automation are all areas of focus. *Chapter 6, Evaluating the Security Posture and Recommending Technical Strategies to Manage Risk.*
33. The answer is D. The Cloud Adoption Framework provides guidance for a cloud journey and continued security operations. *Chapter 7, Designing a Strategy for Securing Server and Client Endpoints.*
34. The answer is C. Microsoft Defender for Identity can be used to secure the directory in AD DS from attacks on users. *Chapter 7, Designing a Strategy for Securing Server and Client Endpoints.*
35. The answer is D. The best option for managing company-owned devices with Microsoft Intune is Mobile Device Management. *Chapter 7, Designing a Strategy for Securing Server and Client Endpoints.*
36. The answer is B. Azure Key Vault allows you to manage TLS/SSL certificates for securing your websites. *Chapter 7, Designing a Strategy for Securing Server and Client Endpoints.*
37. The answer is C. Secure remote access to Azure virtual machines can be accomplished by logging in to a remote session within the Azure portal using Azure Bastion. *Chapter 7, Designing a Strategy for Securing Server and Client Endpoints.*
38. The answer is A. Microsoft Defender for Cloud Apps is a solution that can be used to identify applications that are being accessed on registered devices and the company network. *Chapter 8, Designing a Strategy for Securing SaaS, PaaS, and IaaS.*
39. The answer is C. Microsoft Defender for IoT is the solution that can be used to determine and enforce the security requirements for warehouse environment sensors. *Chapter 8, Designing a Strategy for Securing SaaS, PaaS, and IaaS.*
40. The answer is C. Enforcing compliance across all data and storage accounts in Microsoft 365, Azure, and multi-cloud is accomplished within Microsoft Purview. *Chapter 8, Designing a Strategy for Securing SaaS, PaaS, and IaaS.*
41. The answer is D. To avoid exposure of keys and secrets within Azure App Services, you should use Azure Key Vault. *Chapter 8, Designing a Strategy for Securing SaaS, PaaS, and IaaS.*

42. The answer is A. Data classification is governed by sensitivity labels and policies within Microsoft 365. [Chapter 10, Designing a Strategy for Securing Data](#).
43. The answer is B. SAST is the type of application testing where an “eye test” is used on the application code. [Chapter 9, Specifying Security Requirements for Applications](#).
44. The answer is B. Within a DevSecOps life cycle, security and compliance fall within the workflow within Develop and Deliver. [Chapter 9, Specifying Security Requirements for Applications](#).
45. The answer is A. To protect and mitigate threats to applications, access to resources should be protected with a plan for Identity and secrets handling. [Chapter 9, Specifying Security Requirements for Applications](#).
46. The answer is A. Discovering applications being accessed on your network can be identified by using Microsoft Defender for Cloud Apps. [Chapter 9, Specifying Security Requirements for Applications](#).
47. The answer is B. Static Application Security Testing should be done in the commit the code phase of the Cloud Adoption process. [Chapter 9, Specifying Security Requirements for Applications](#).
48. The answer is A. When protecting against a possible ransomware attack, Azure backup can protect against data loss and allow for recovery. [Chapter 9, Specifying Security Requirements for Applications](#).
49. The answer is D. Creating policies to automatically retain, delete, and store data takes place in the govern your data stage of the data protection process. [Chapter 10, Designing a Strategy for Securing Data](#).
50. The answer is B. Governing data in databases can be accomplished with Microsoft Purview. [Chapter 10, Designing a Strategy for Securing Data](#).
51. The answer is A. A VPN Gateway is the best option for securing communication between Azure and on-premises data center resources. [Chapter 10, Designing a Strategy for Securing Data](#).

Summary

This completes your assessment and preparation for the SC-100, Microsoft Cybersecurity Architect exam. Good luck with your continued success in your certification and professional journey!