

Microsoft Cybersecurity Architect Exam Ref SC-100, Second Edition

Preface:

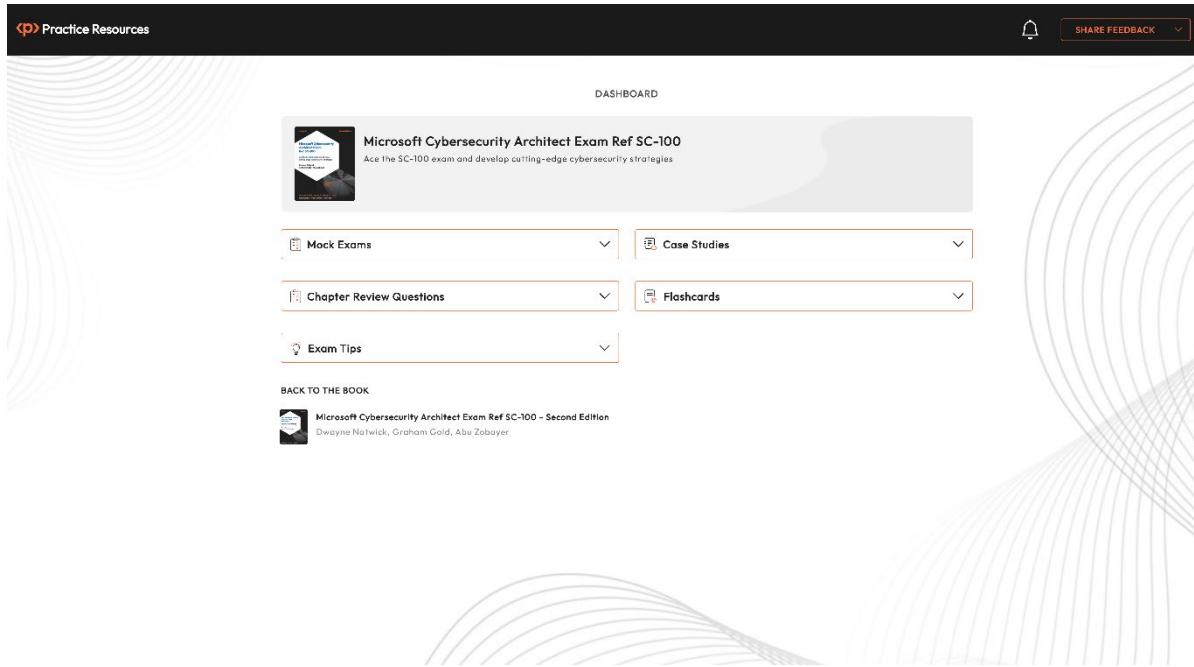


Figure 0.1 – Online exam-prep platform on a desktop device

Chapter 1: Cybersecurity in the Cloud

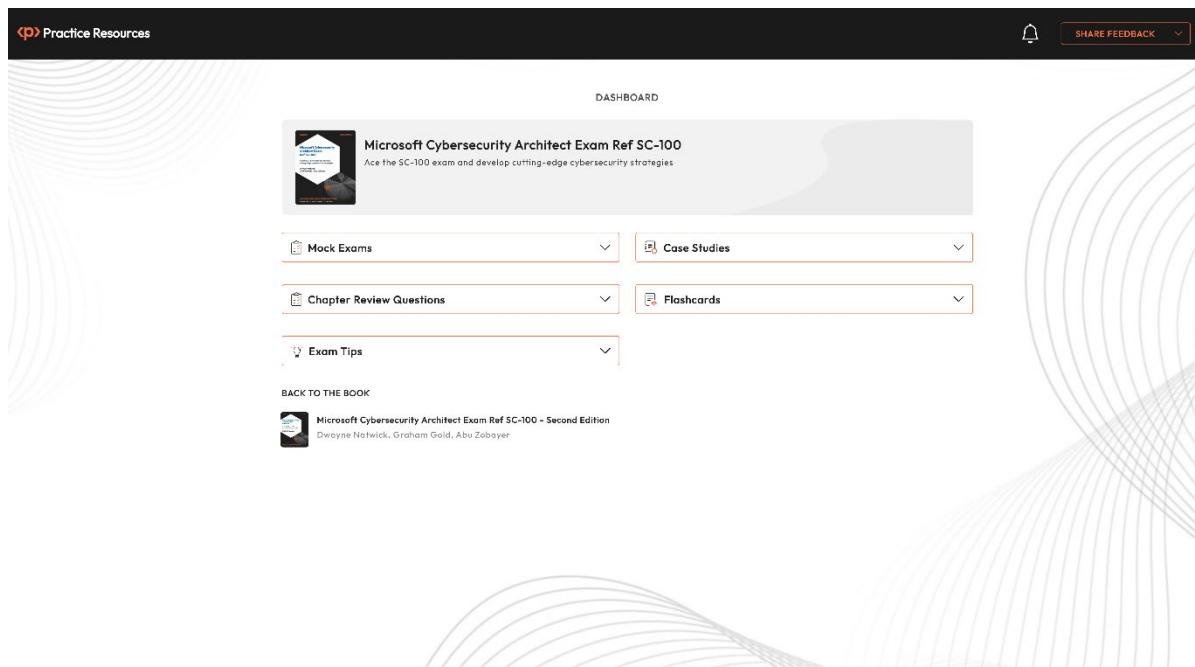


Figure 1.1: Dashboard interface of the online practice resources

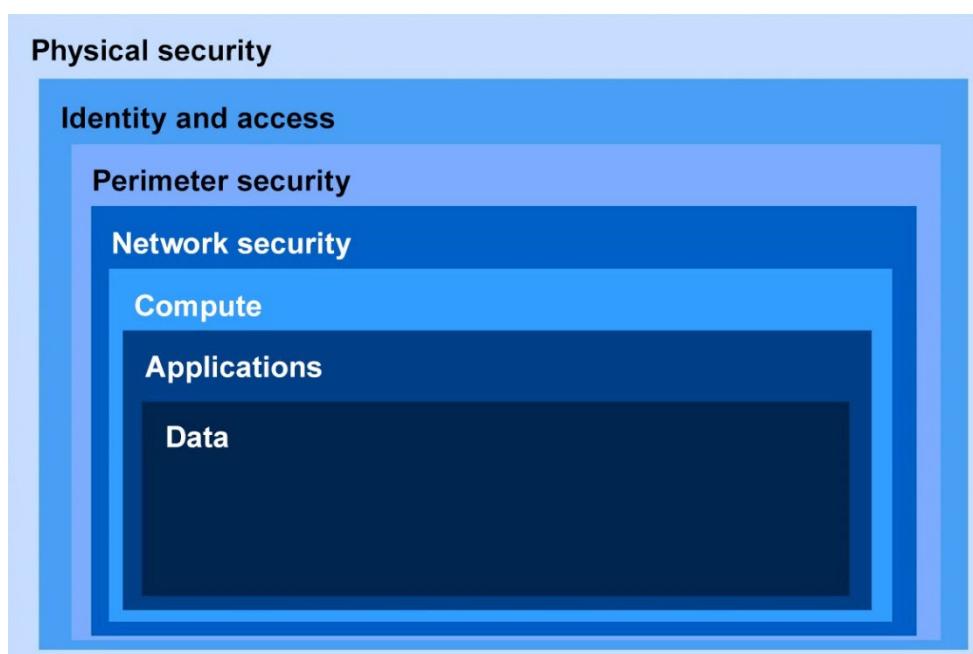
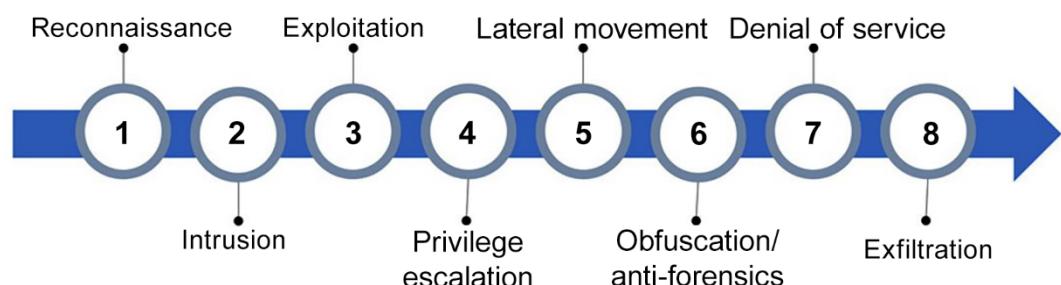


Figure 1.2: Logical layers of defense-in-depth posture/infrastructure

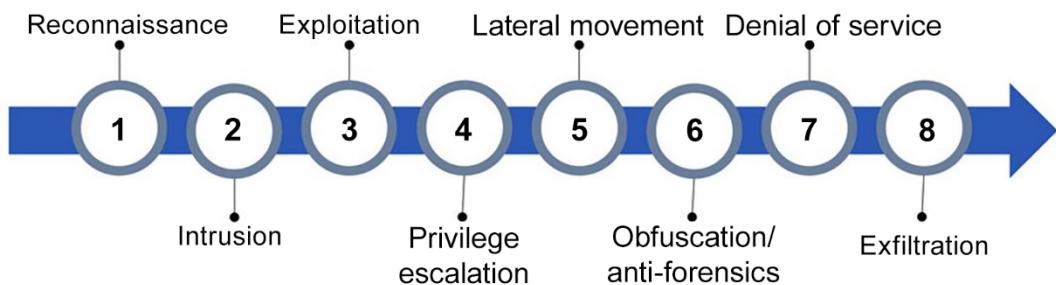


Figure 1.3: Stages of the Cyber Kill Chain

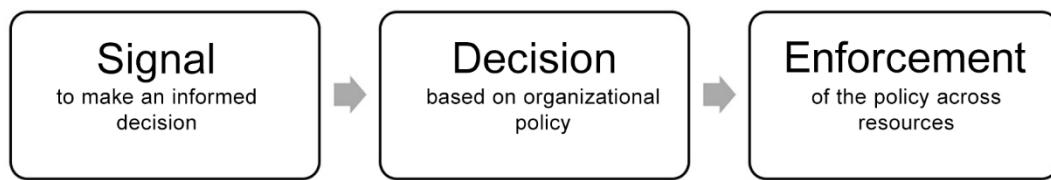


Figure 1.4: A flowchart where an initial signal leads to an informed decision based on organizational policy, which is then enforced across resources



Figure 1.5: Shadow IT prevention life cycle

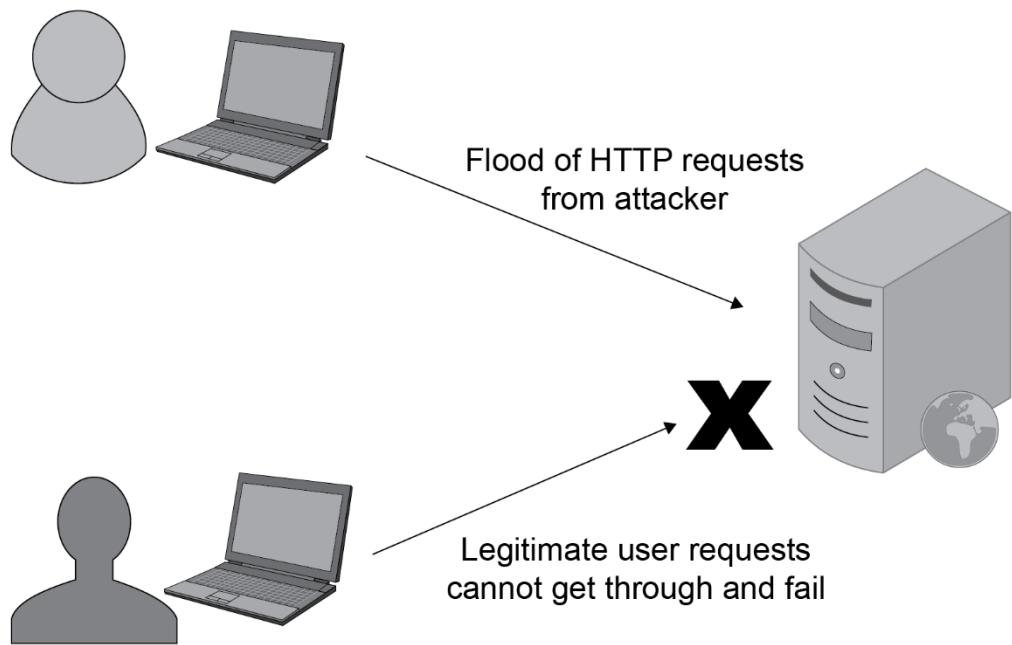


Figure 1.6: Illustration of a denial-of-service attack

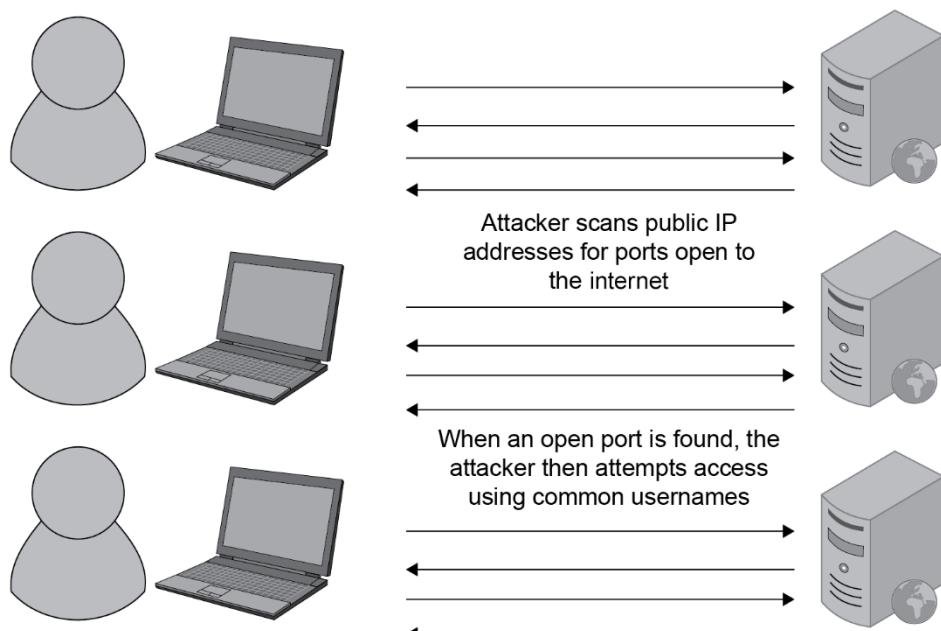


Figure 1.7: An attacker scanning public IP addresses for open ports, then attempting to gain access using common usernames once an open port is found

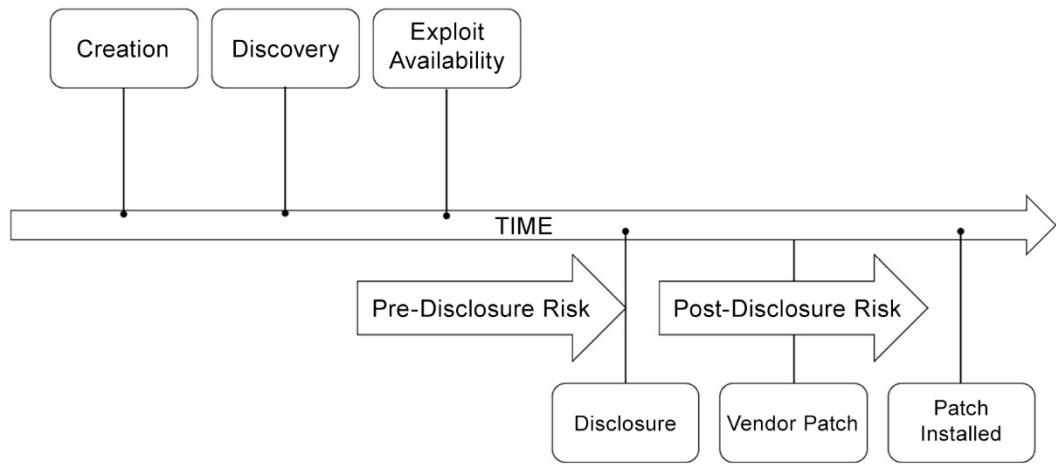


Figure 1.8: The vulnerability management life cycle

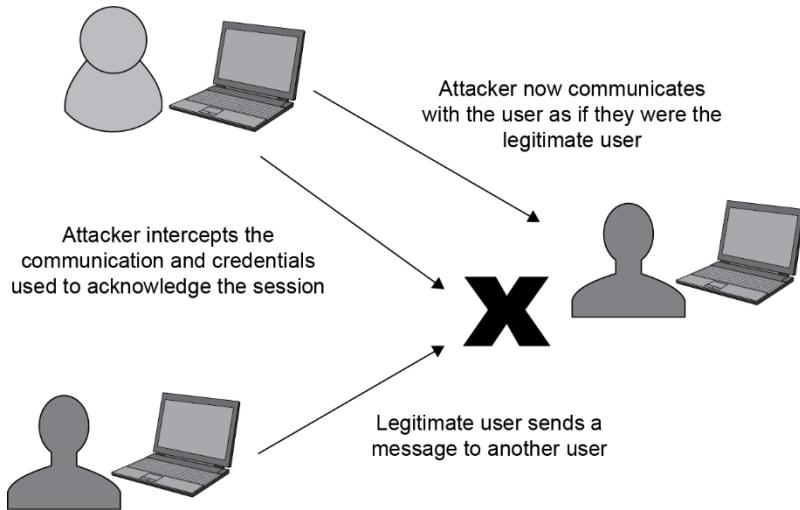


Figure 1.9: Attacker-in-the-Middle (AiTM) attack: Attacker intercepts and impersonates users in a communication

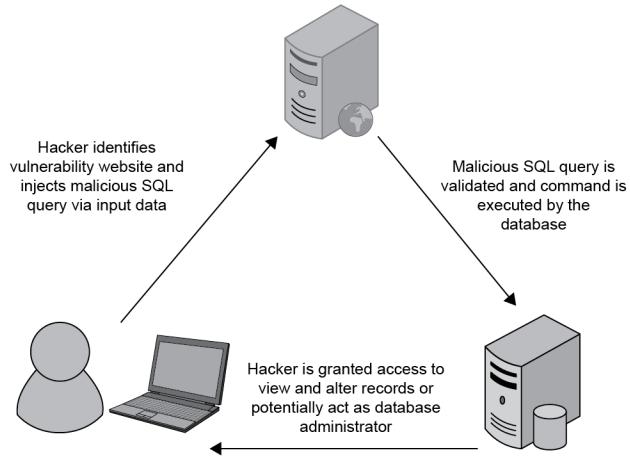


Figure 1.10: SQL injection attack: Hacker injects malicious SQL to access and manipulate database records

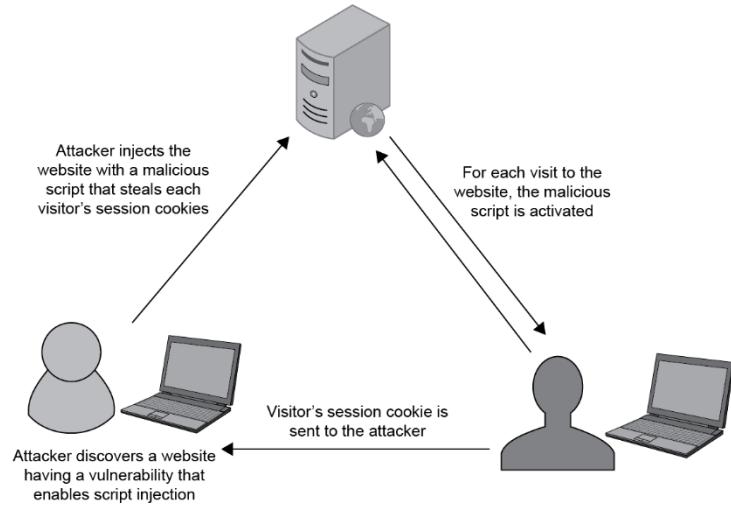


Figure 1.11: Cross-site scripting (XSS) attack: An attacker injects a malicious script into a vulnerable website to steal visitors' session cookies

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

Impact
How Serious is the Risk?

Figure 1.12: Security risk matrix visualized

Chapter 2: Build an Overall Security Strategy and Architecture

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

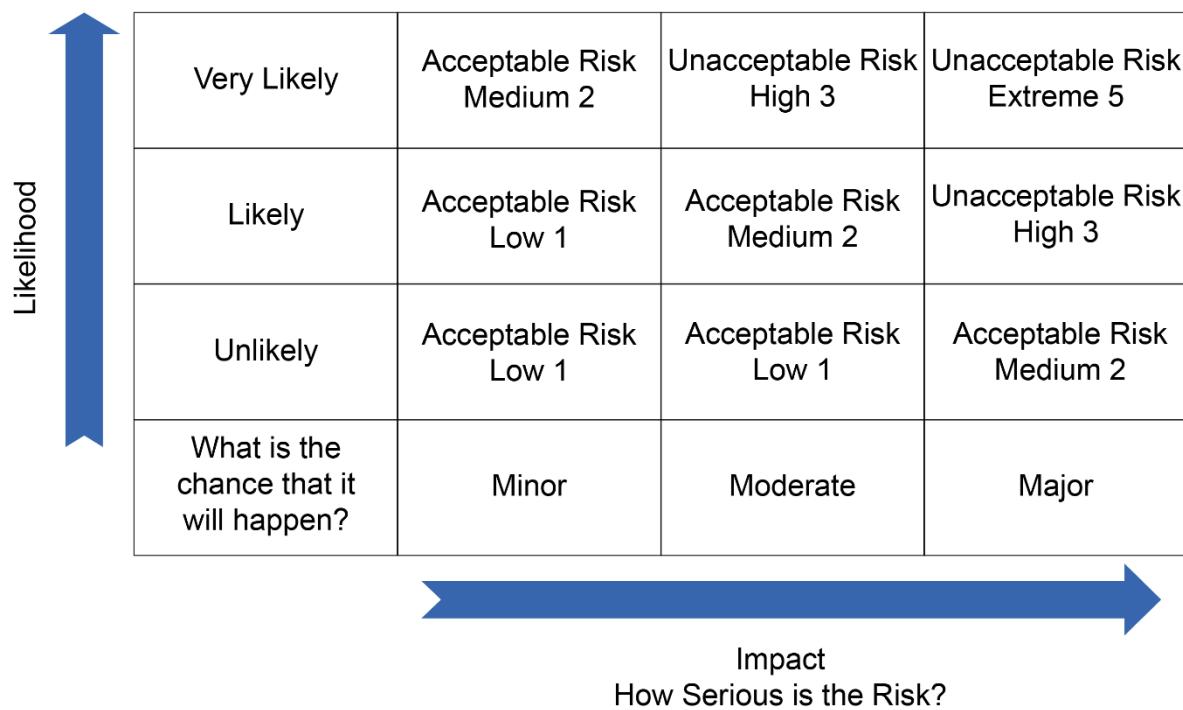


Figure 2.2 – Risk assessment matrix

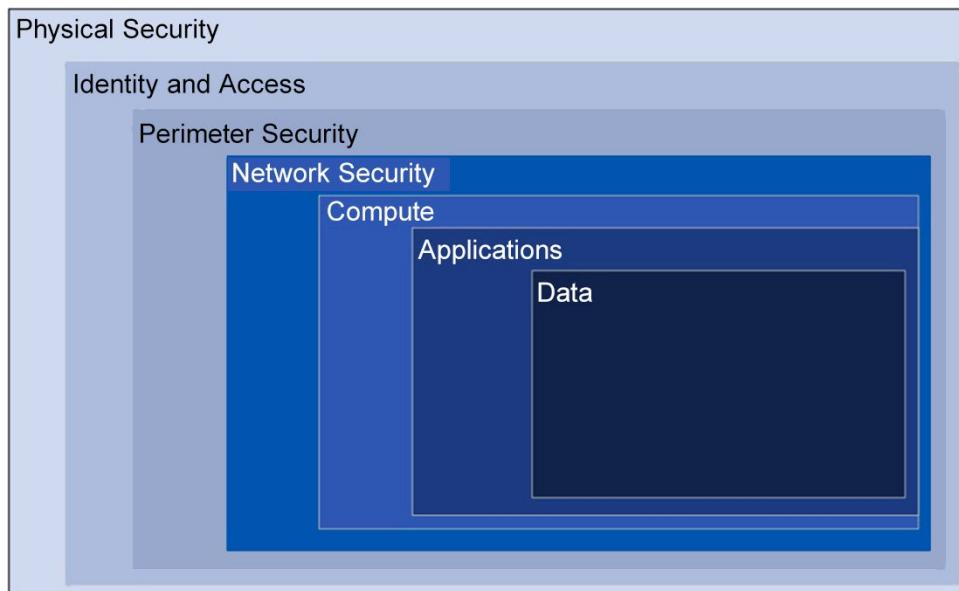


Figure 2.3 – Defense-in-depth security diagram

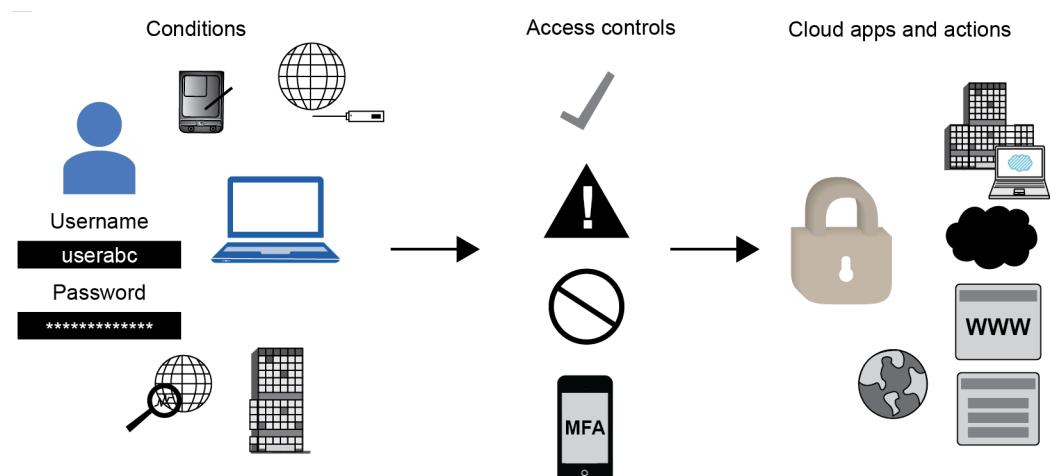


Figure 2.4 – Zero trust with Conditional Access

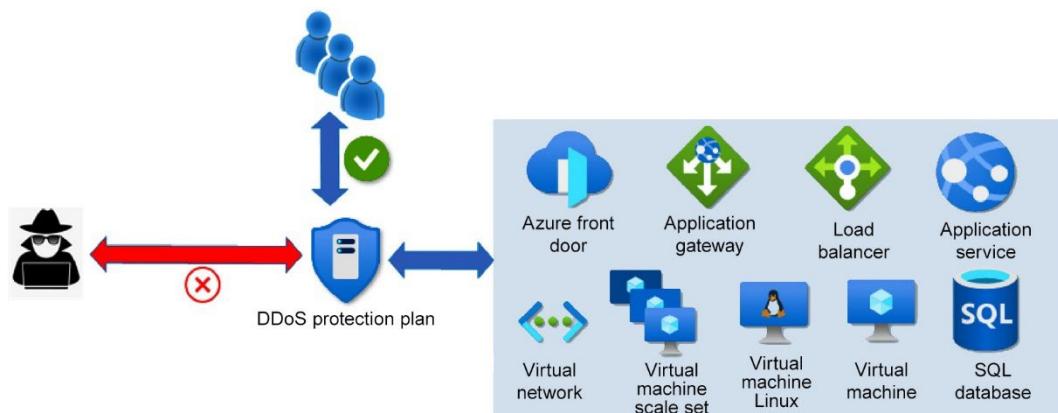


Figure 2.5 – Azure DDoS Protection

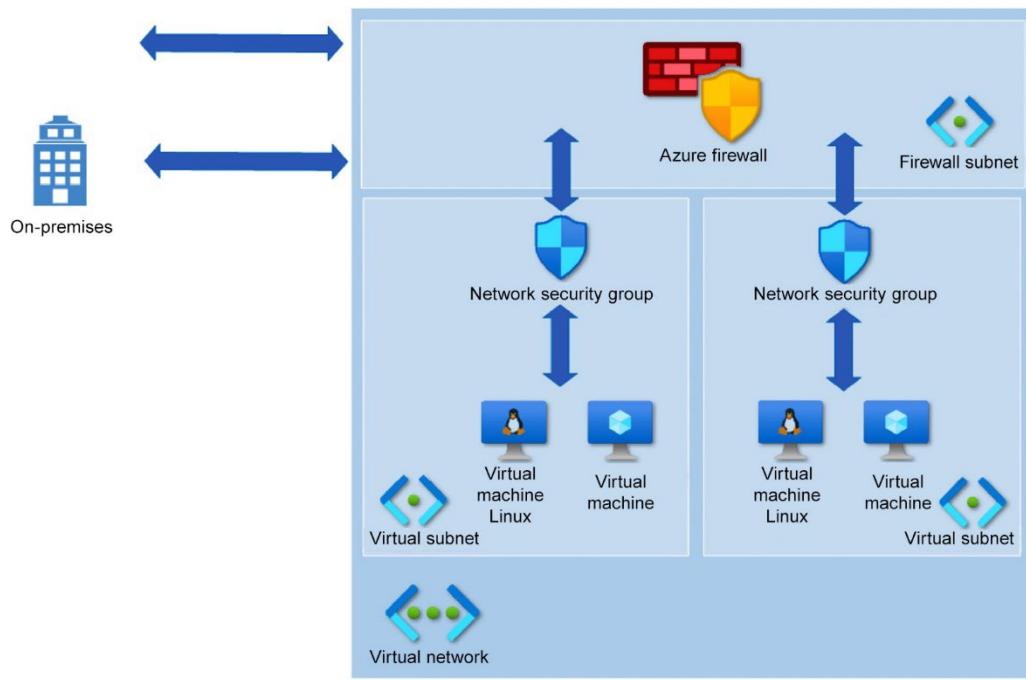


Figure 2.6 – Azure Firewall

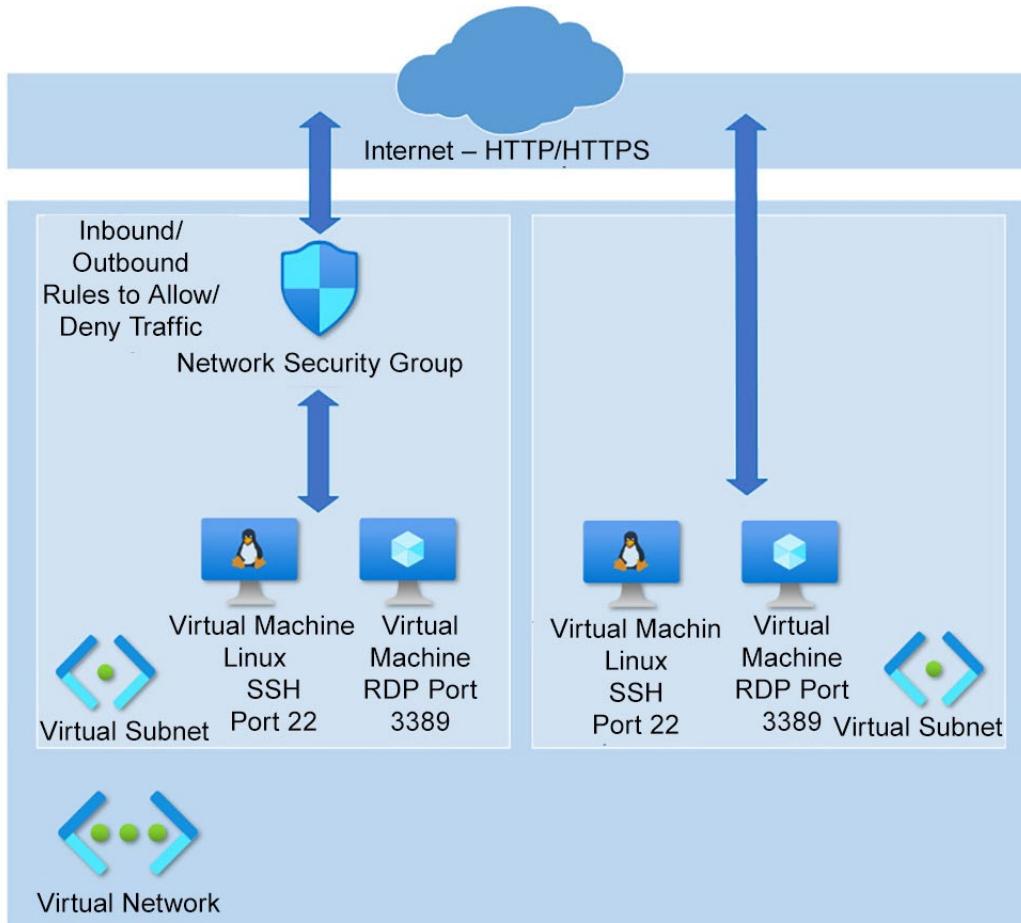


Figure 2.7 – Network security groups for network perimeter protection

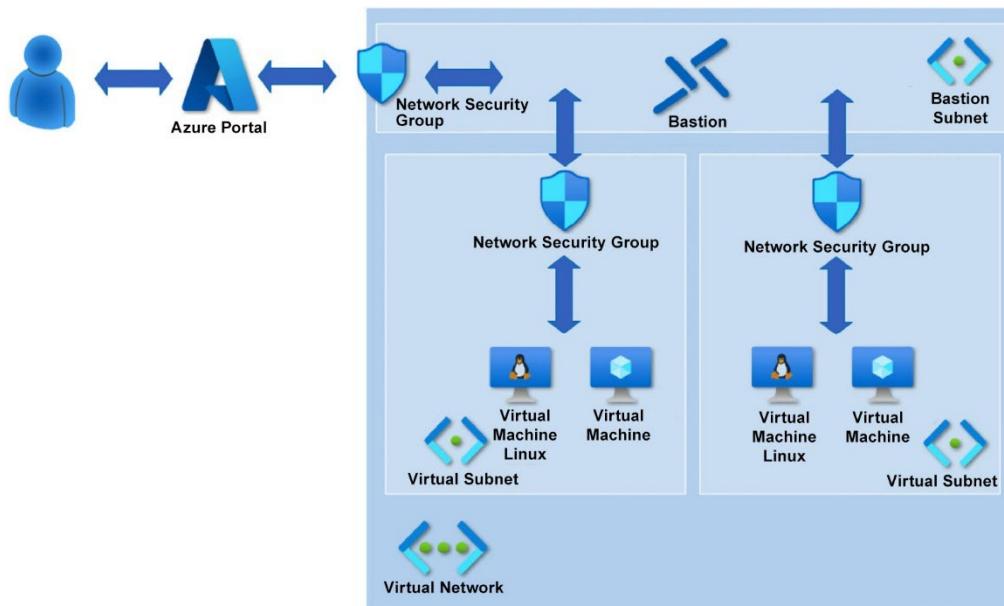


Figure 2.8 – Azure Bastion for virtual machine remote management

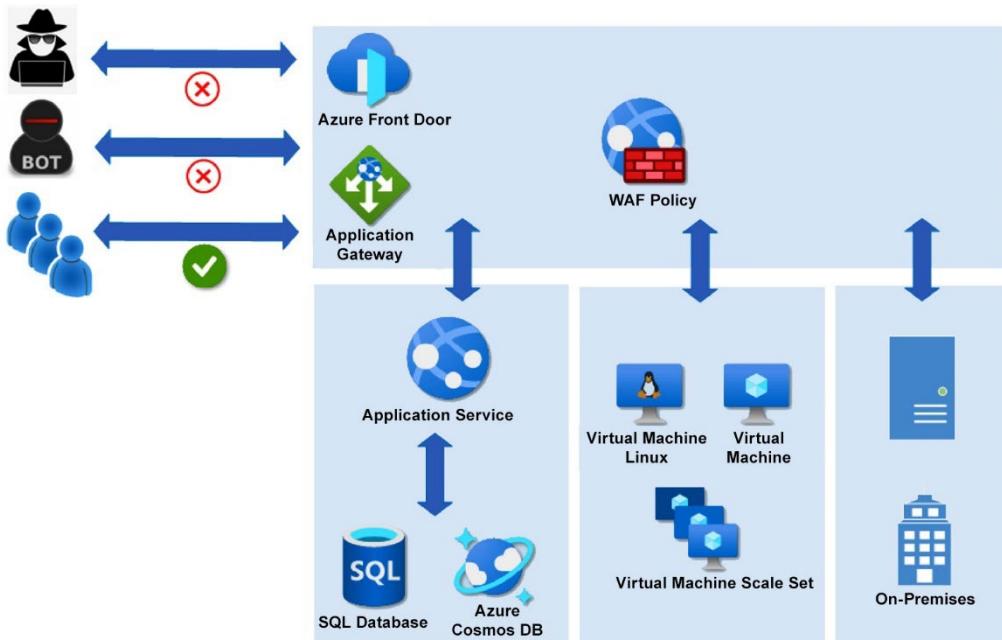


Figure 2.9 – WAF diagram

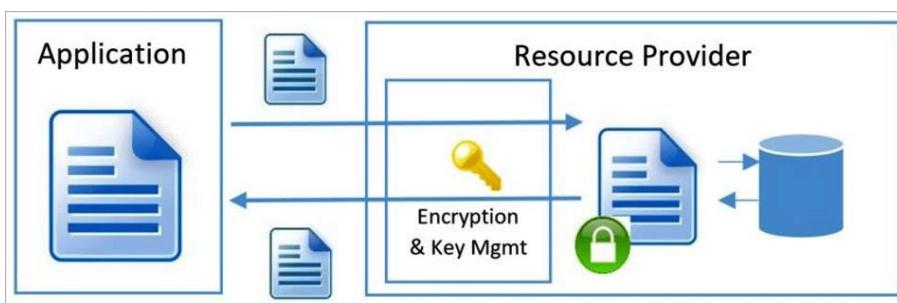


Figure 2.10 – Data encrypted at rest

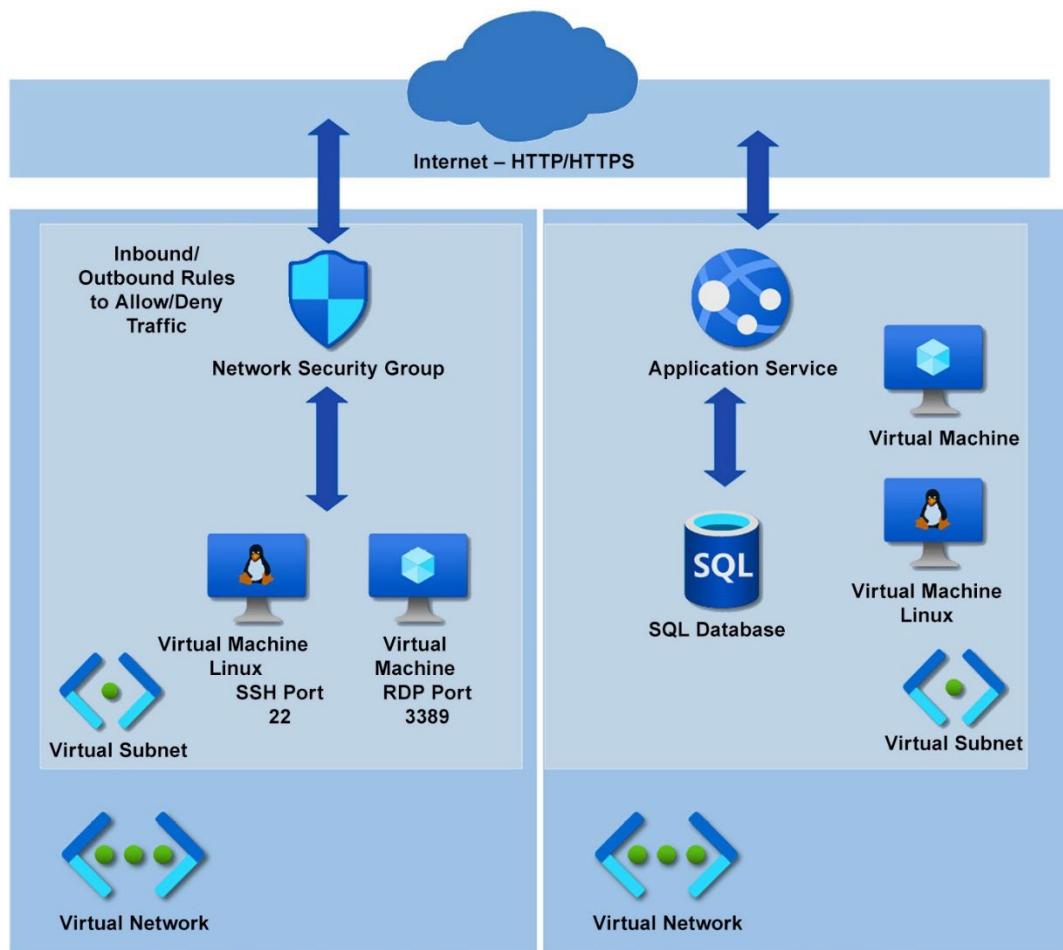


Figure 2.11 – Network segmentation

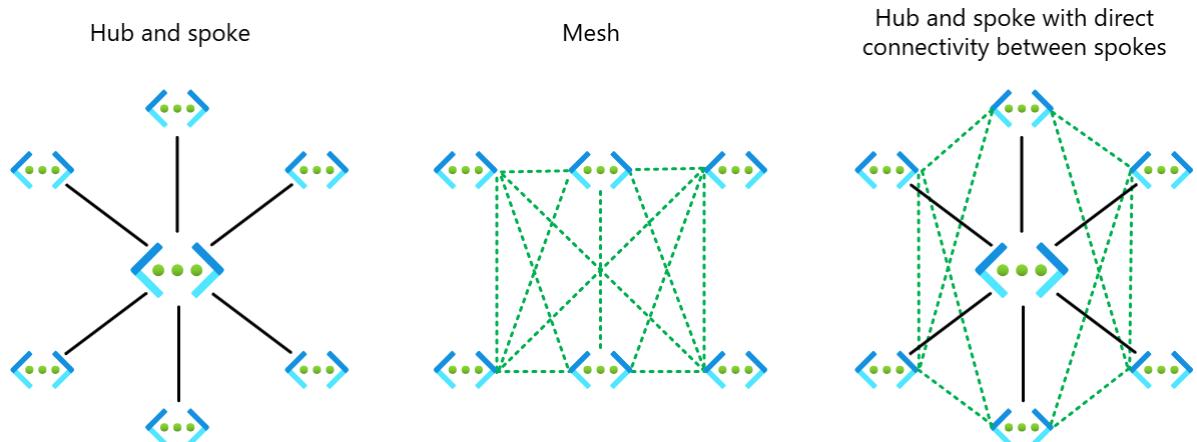


Figure 2.12 – Network topologies

Chapter 3: Design a Security Operations Strategy

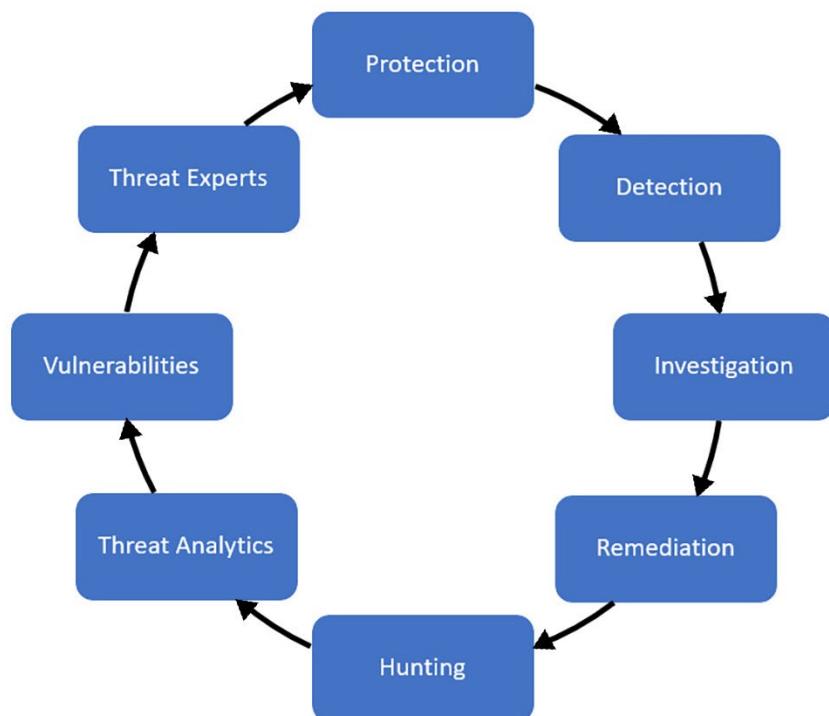


Figure 3.1 – A security operations strategy to manage threats

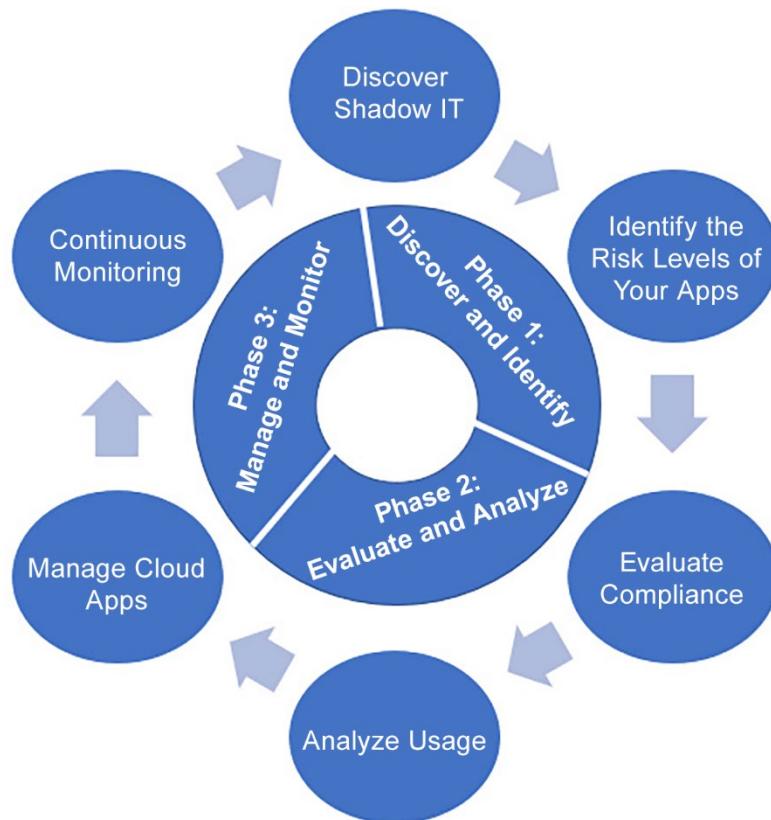


Figure 3.2 – Microsoft Defender for Cloud Apps’ shadow IT protection

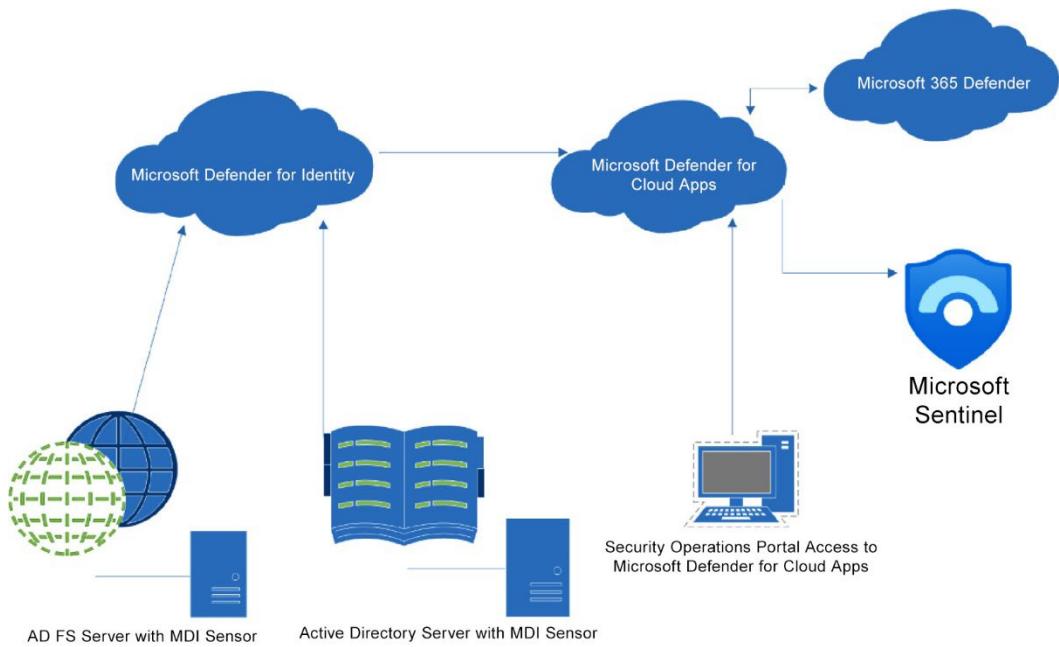


Figure 3.3 – MDI

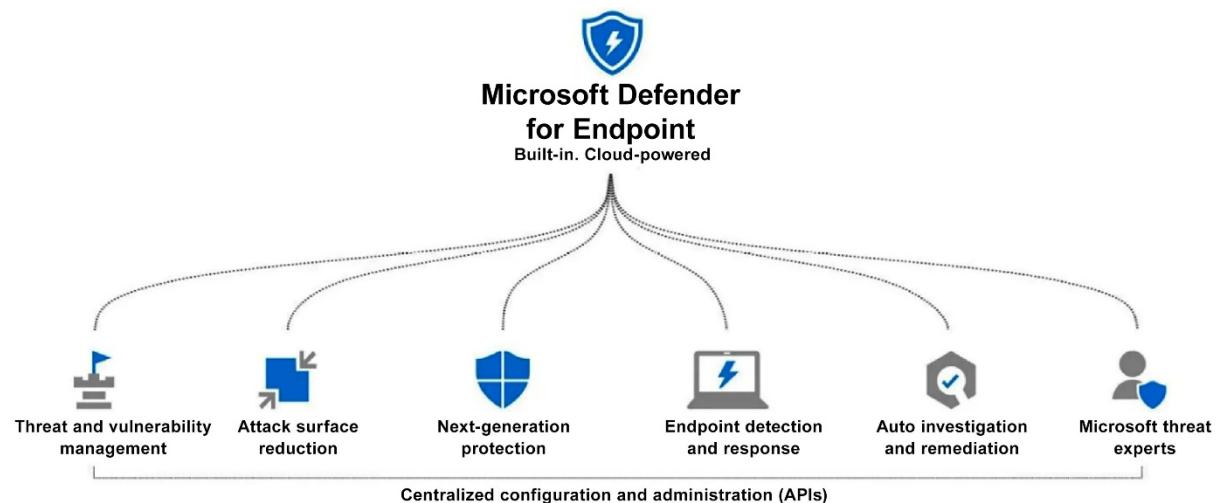


Figure 3.4 – Microsoft Defender for Endpoint

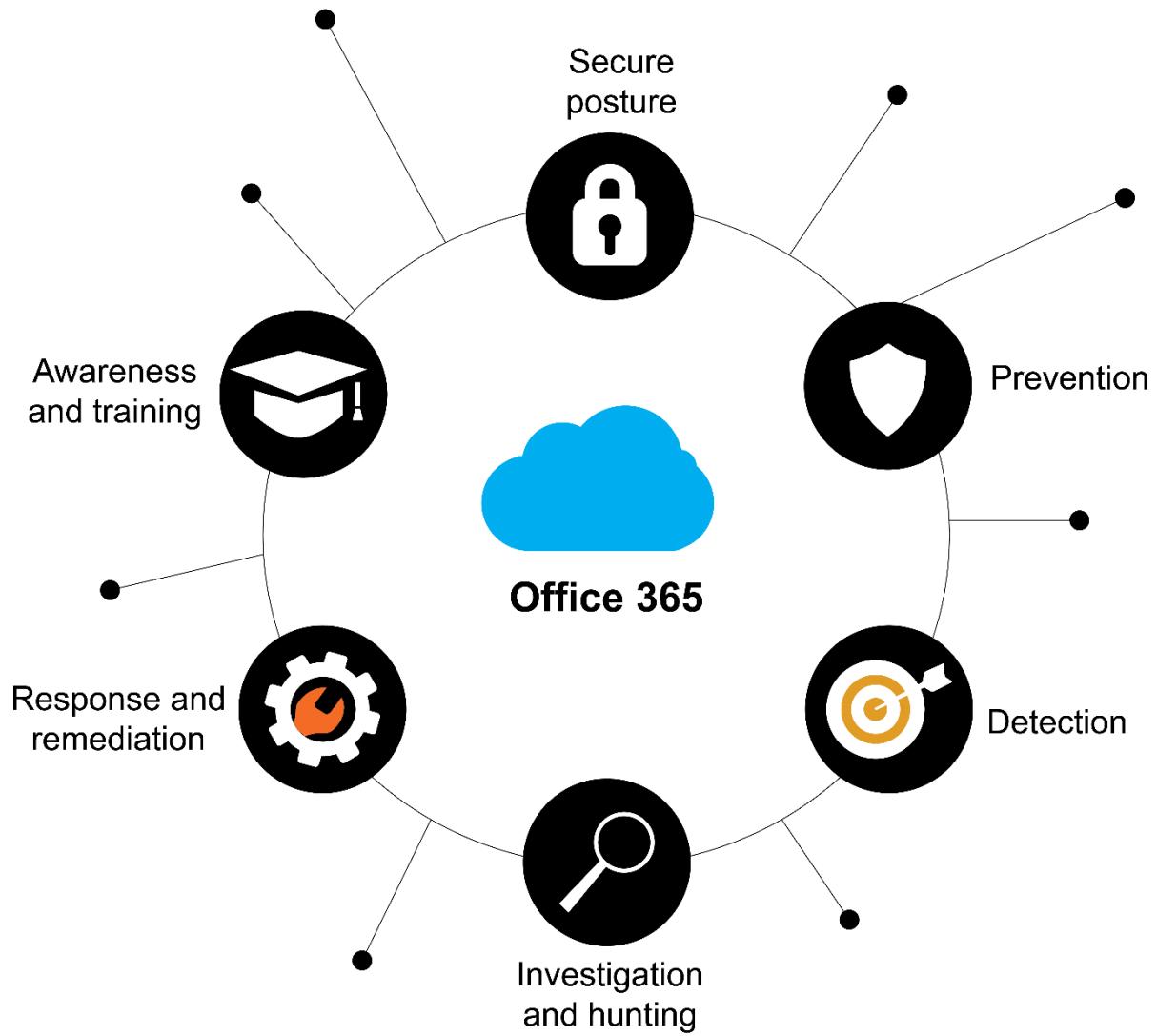


Figure 3.5 – Microsoft Defender for Office 365

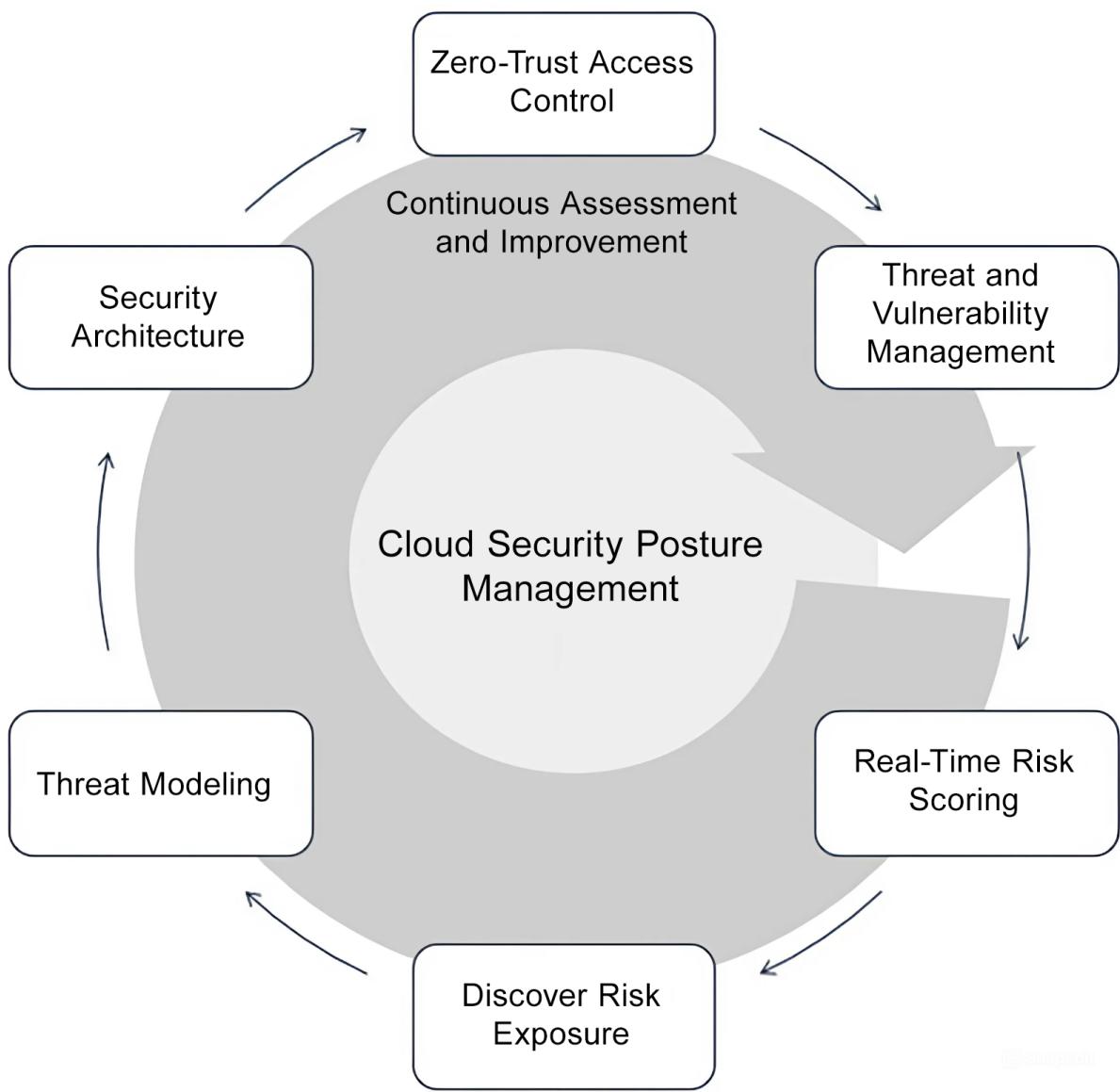


Figure 3.6 – Microsoft Defender for Cloud security posture management

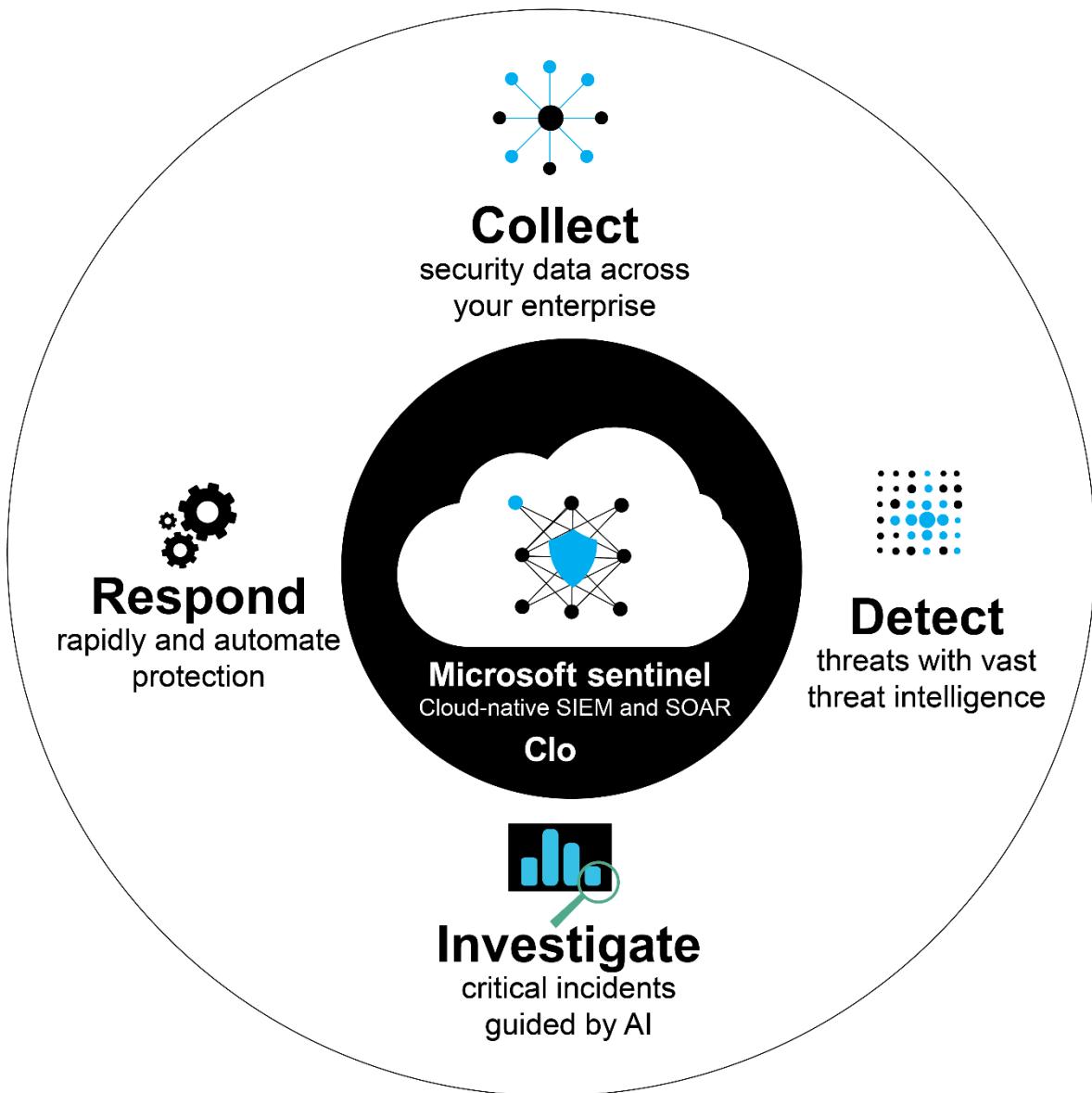


Figure 3.7 – Microsoft Sentinel SIEM and SOAR

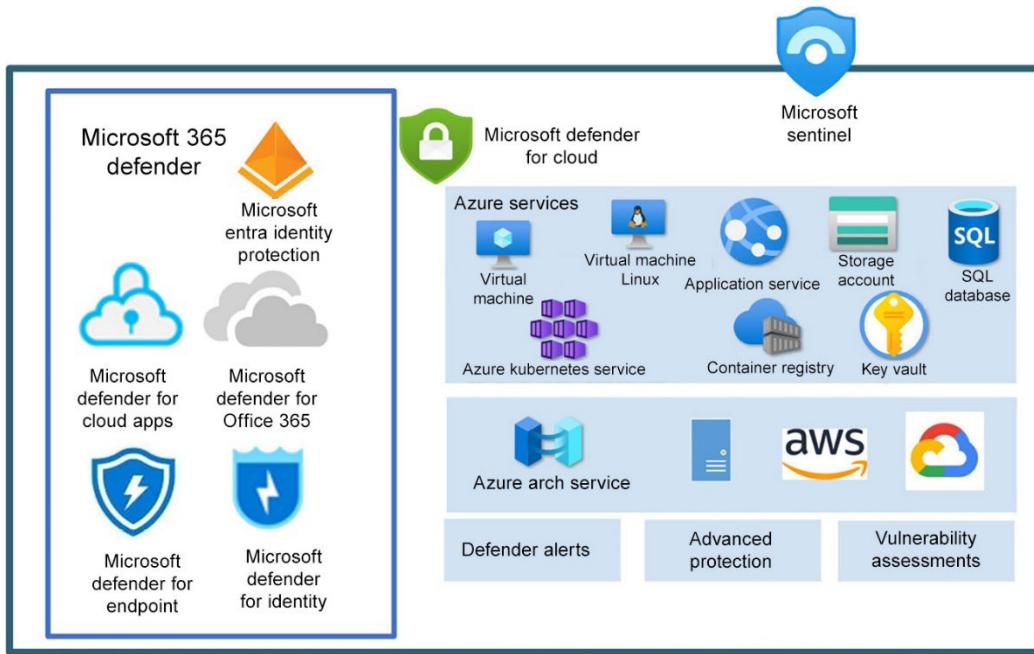


Figure 3.8 – Microsoft Defender for Office 365 and Microsoft Sentinel

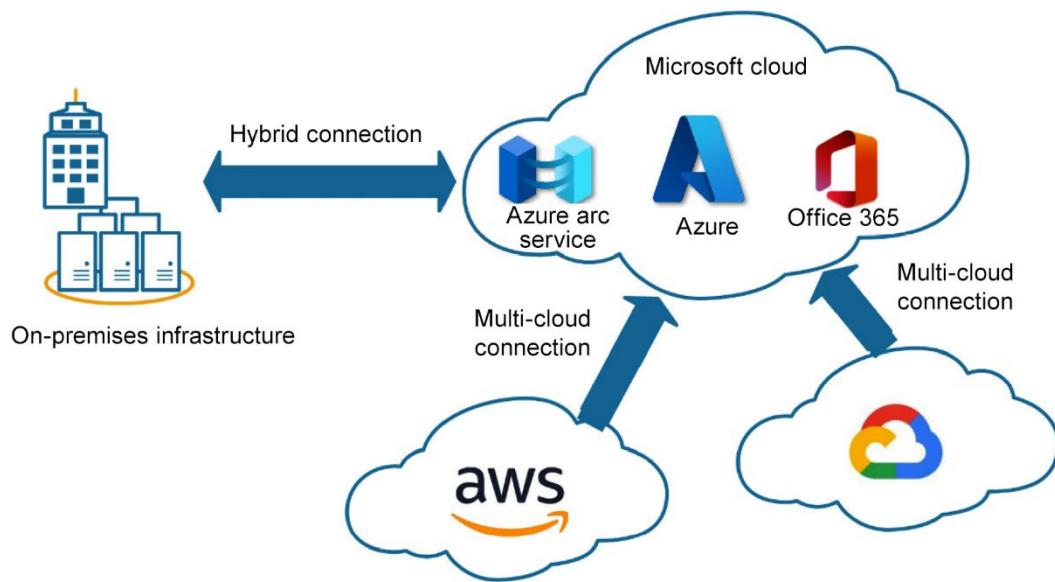


Figure 3.9 – Hybrid and multi-cloud architecture

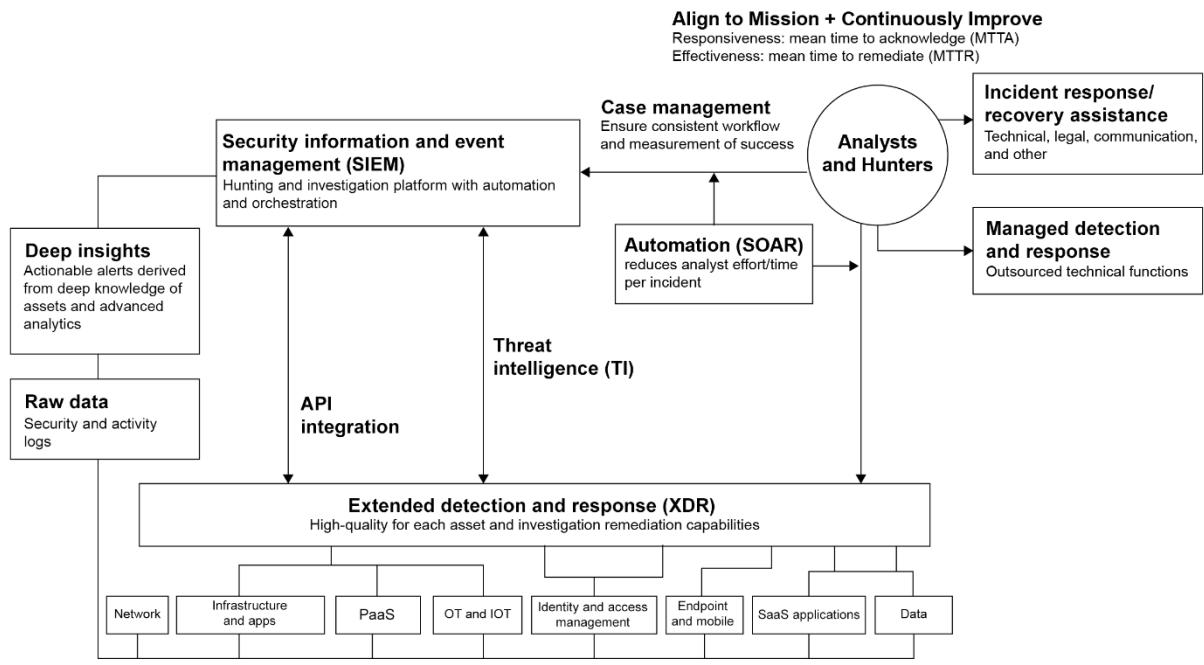


Figure 3.10 – Security operations technology usage

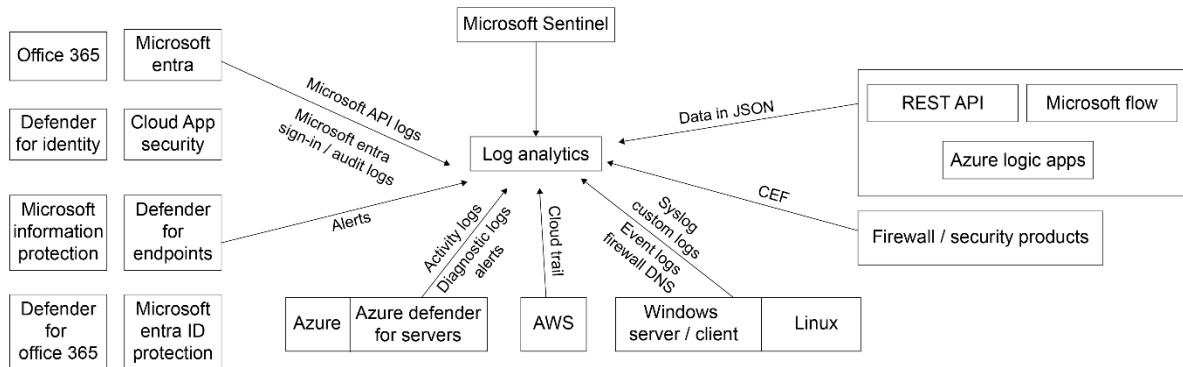


Figure 3.11 – Microsoft Sentinel architecture

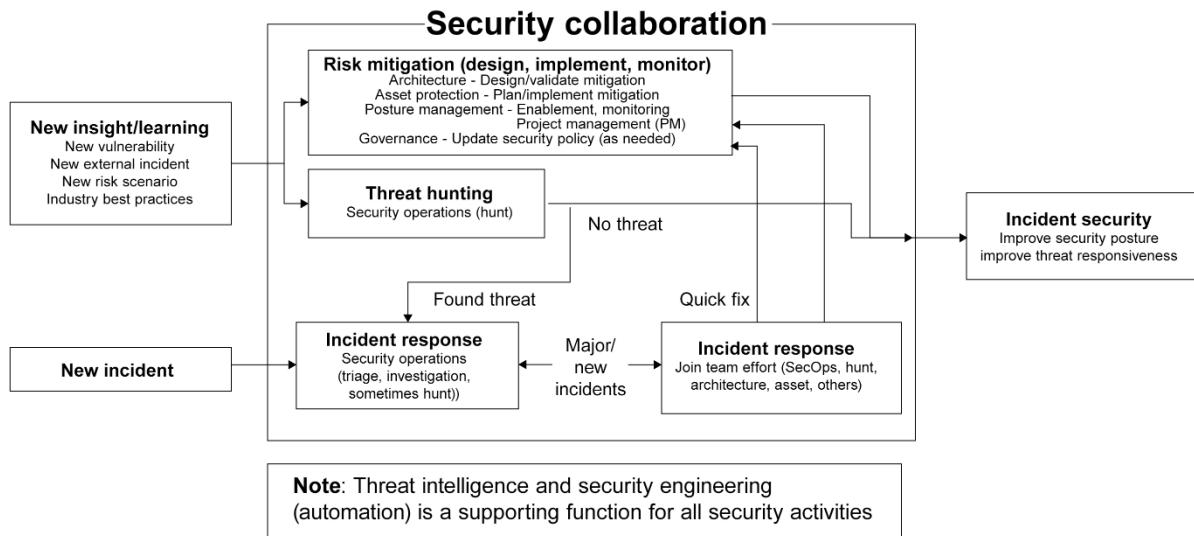


Figure 3.12 – The security operations continuous improvement process

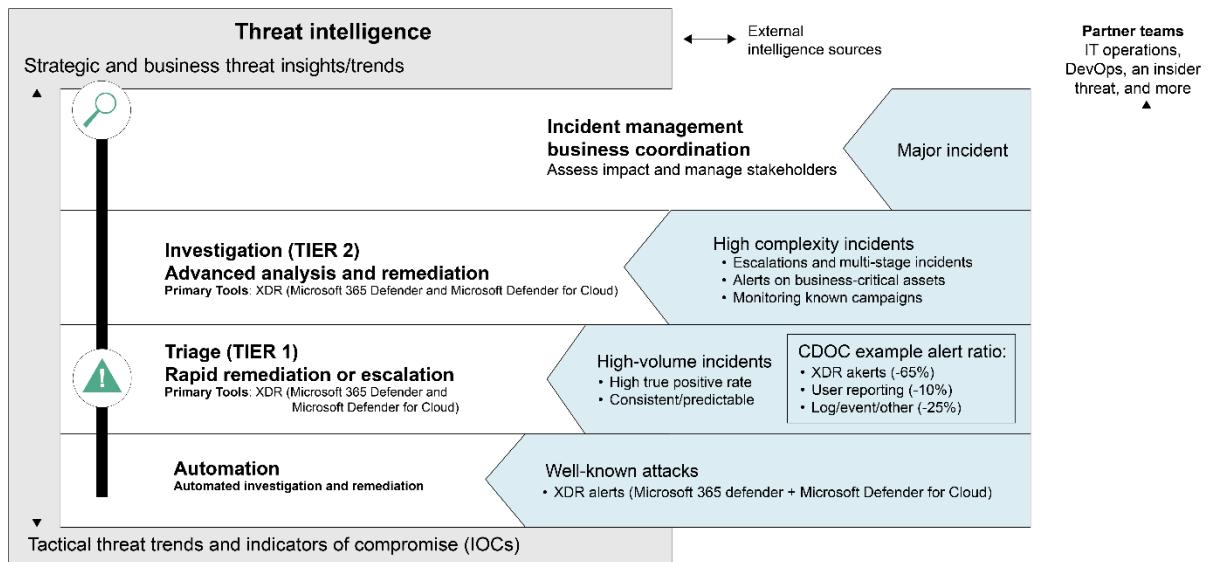


Figure 3.13 – The security operations functional tiers

Chapter 4: Design an Identity Security Strategy

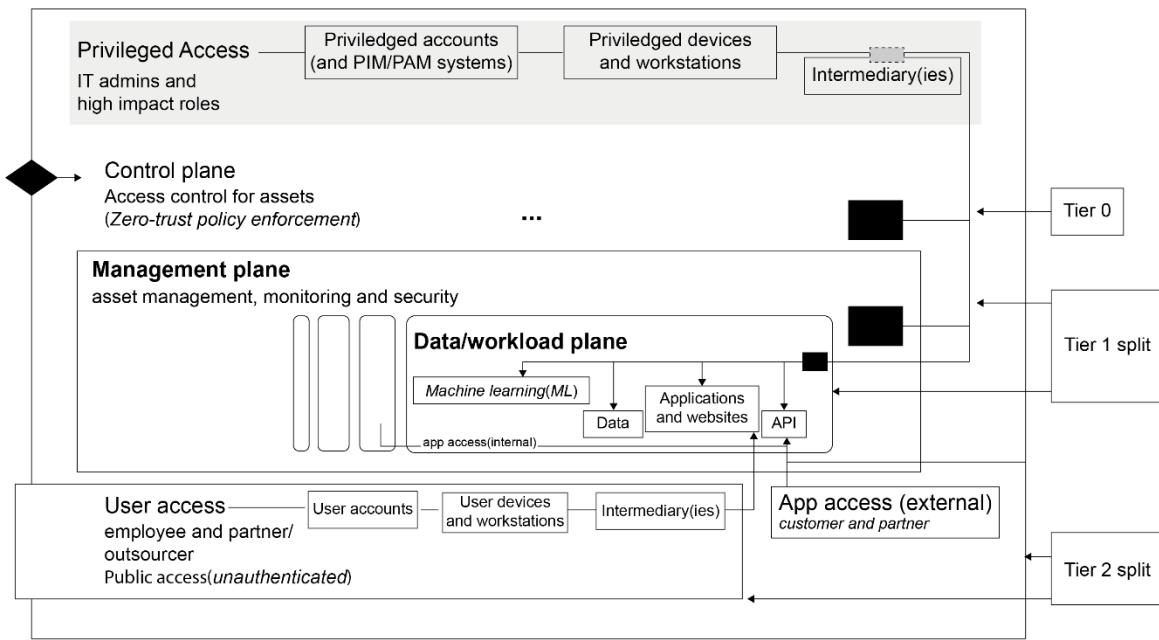


Figure 4.1: Expanded visualization of identity and access controls for secure access

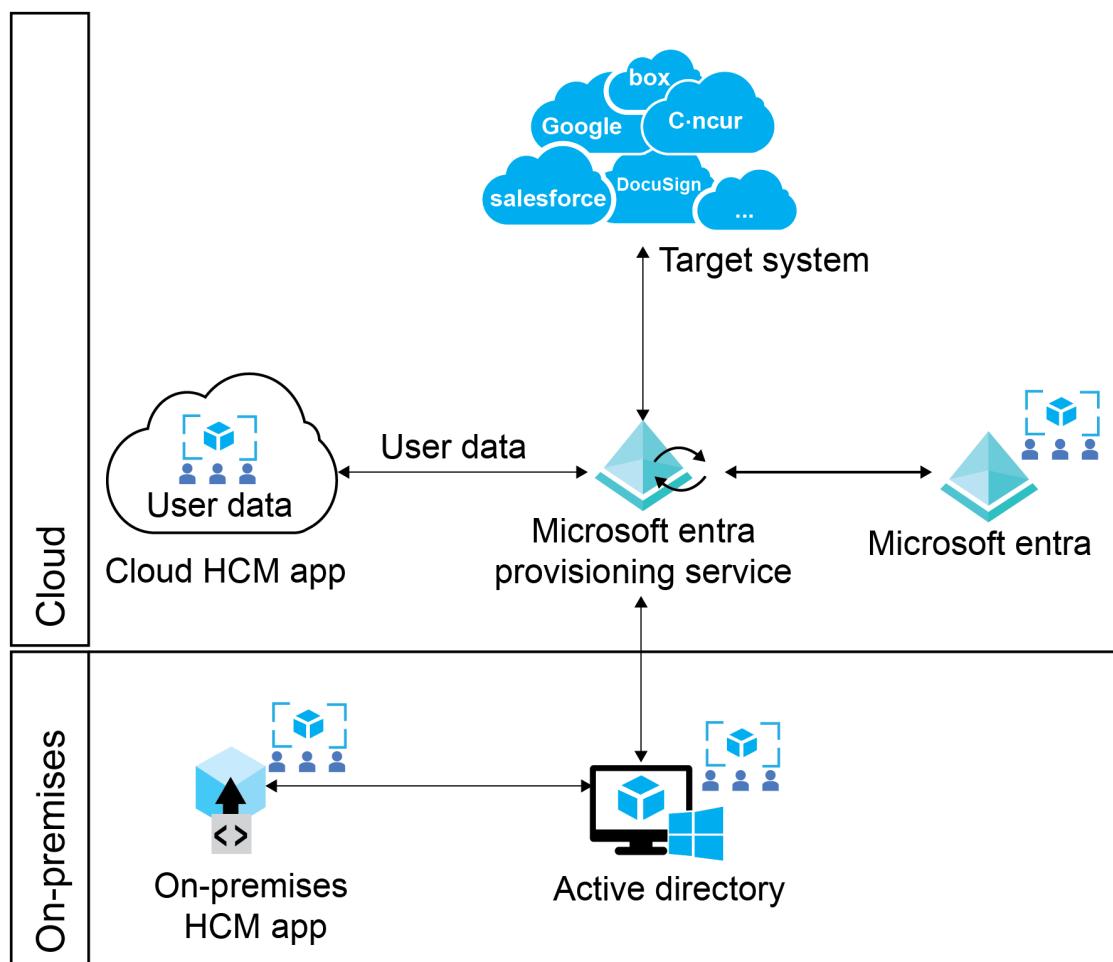


Figure 4.2: SCIM Microsoft Entra provisioning diagram

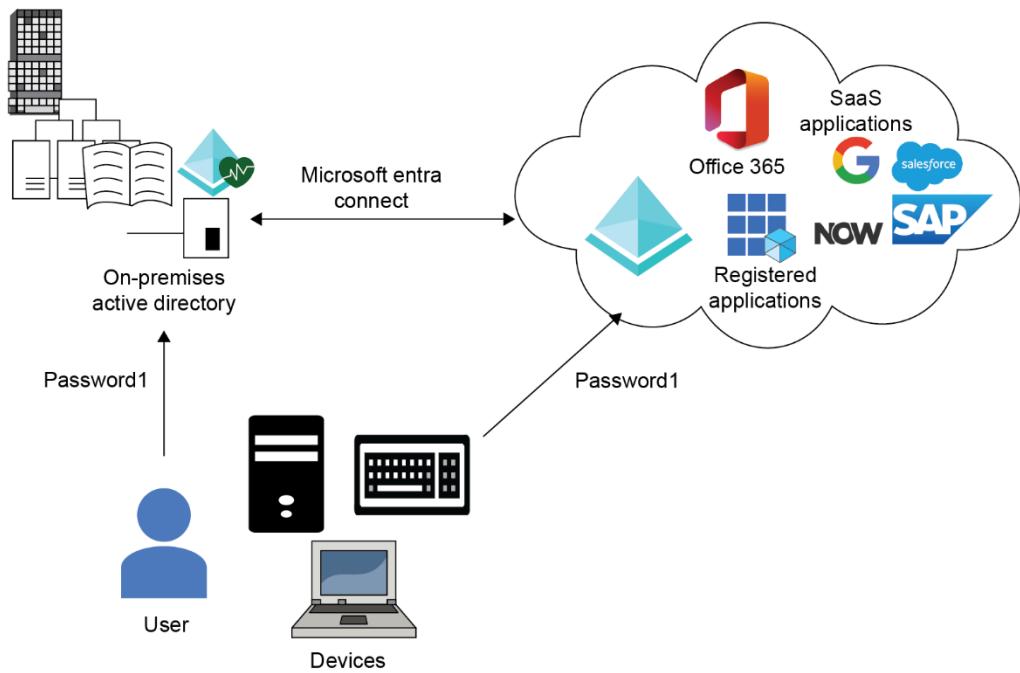


Figure 4.3: Overview of PHS, showing the flow from user devices to on-premises Active Directory and Microsoft Entra Connect

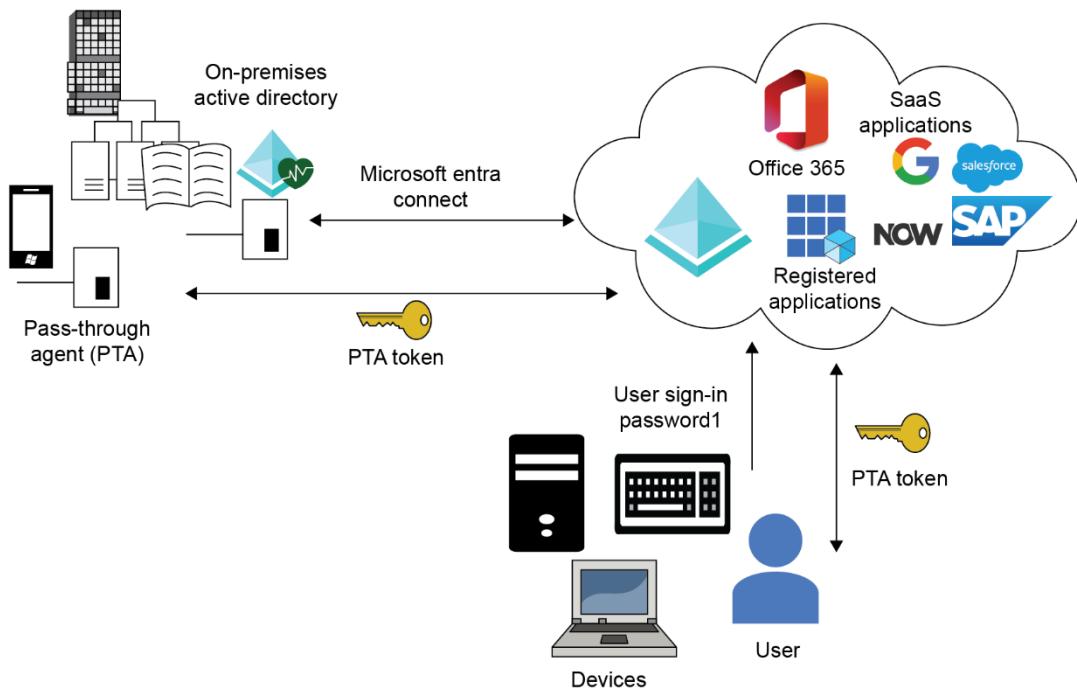


Figure 4.4: An overview of PTS, with the key difference from PHS being the dependency on communication between on-premises Active Directory and Microsoft Entra

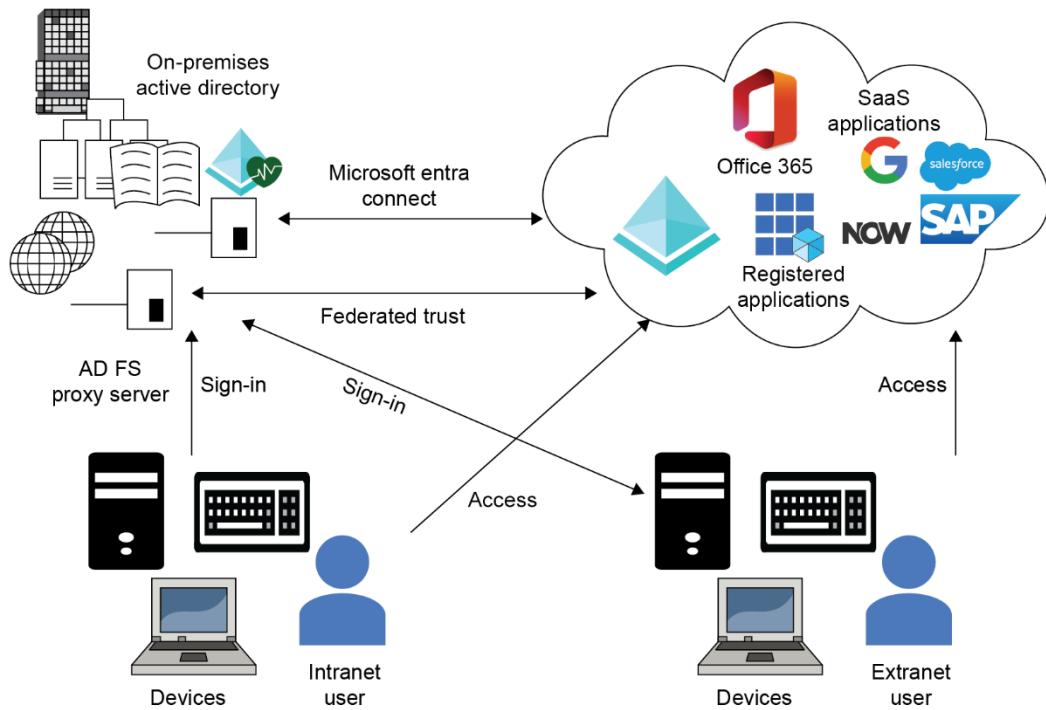


Figure 4.5: An overview of AD FS synchronization flows

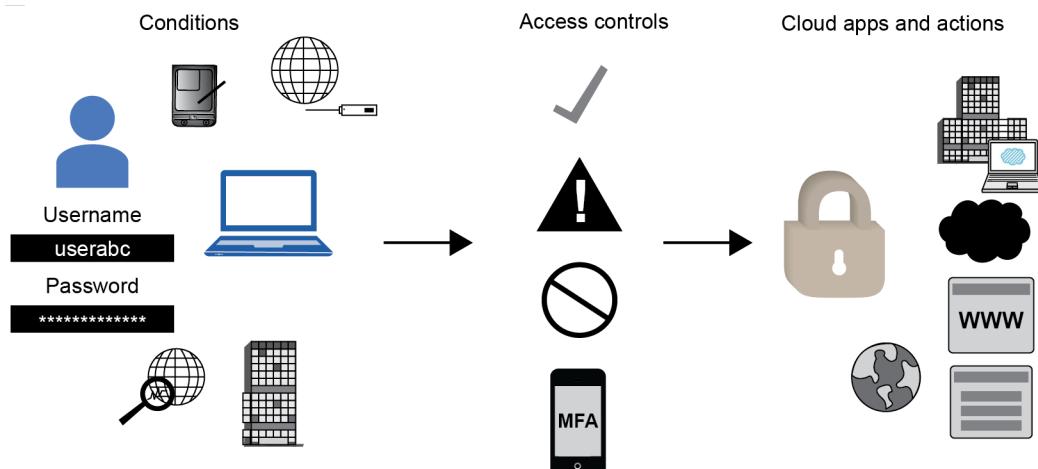


Figure 4.6: A CA workflow showing the flow of evaluation of user access, from left to right

Chapter 5: Design a Regulatory Compliance Strategy

The screenshot shows the 'Settings | Defender plans' page in the Microsoft Azure portal. On the left, there's a sidebar with 'Defender plans' selected. The main area lists four services: 'Defender CSPM', 'Servers', 'App Service', and 'Databases'. Each service has a 'Status' column with two options: 'On' (highlighted with a red arrow) and 'Off'. A 'Save' button is located at the top left of the main content area.

Plan	Pricing	Resource quantity	Monitoring coverage	Status
Defender CSPM	Free (preview) Details >	N/A	Full Settings >	On Off
Servers	Plan 2 (\$15/Server/Mo) Change plan >	6 servers	Partial Settings >	On Off
App Service	\$15/Instance/Month Details >	0 instances	Full Settings >	On Off
Databases	Selected: 4/4 Select types >	Protected: 1/1 instance	Full Settings >	On Off

Figure 5.1: Turning on and saving Defender plans settings

The screenshot shows the 'Recommendations' page in the Microsoft Azure portal. At the top, it displays a secure score of 93% and 10 active secure score recommendations. Below this, there's a section for 'Attack path' which says 'We didn't find attack paths in your environment'. The main area is a table of recommendations, each with columns for Name, Max score, Current score, Potential score increase, Status, Unhealthy resources, and Insights. The table includes rows for enabling MFA, managing access and permissions, auditing and logging, enhanced security features, security best practices, protecting against DDoS attacks, and restricting unauthorized network access.

Name	Max score	Current score	Potential score increase	Status	Unhealthy resources	Insights
Enable MFA	10	10.00	+ 7%	Completed	0 of 1 resources	Green bar
Manage access and permissions	4	4.00		Unassigned	0 of 1 resources	Yellow bar
Enable auditing and logging	1	0.00	+ 7%	Unassigned	1 of 1 resources	Red bar
Enable enhanced security features	Not scored	Not scored		Completed	1 of 1 resources	Red bar
Implement security best practices	Not scored	Not scored		Unassigned	1 of 4 resources	Grey bar
Protect applications against DDoS attacks	Not scored	Not scored		Completed	0 of 1 resources	Grey bar
Restrict unauthorized network access	Not scored	Not scored		Unassigned	0 of 1 resources	Grey bar

Figure 5.2: Security posture recommendations



Security posture

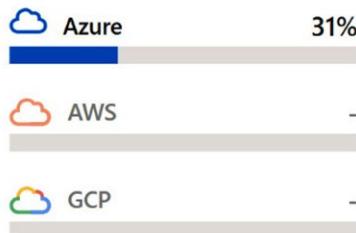
15/15

Unassigned recommendation

0/0

Overdue recommendations

Secure score



[Explore your security posture >](#)

Figure 5.3: The Security posture overview tile



Regulatory compliance

Azure Security Benchmark

[New](#)

24 of 43 passed controls

Lowest compliance regulatory standards
by passed controls

SOC TSP

1/13

ISO 27001:2013

2/17

PCI DSS 3.2.1

11/43

[Improve your compliance >](#)

Figure 5.4: The Regulatory compliance overview tile

The screenshot shows the Microsoft Defender for Cloud Regulatory compliance dashboard. The left sidebar includes links for Cloud Security Explorer (Preview), Workbooks, Community, Diagnose and solve problems, Cloud Security (Security posture, Regulatory compliance, Workload protections, Firewall Manager, DevOps Security (Preview)), Management (Environment settings, Security solutions, Workflow automation), and Home. The main content area displays the Microsoft cloud security benchmark with recommendations for Network Security (NS) and Cloud Security (PV). Each recommendation has a 'Control details' link and MS/C status indicators.

Figure 5.5: The Azure Security Benchmark compliance controls

This screenshot is similar to Figure 5.5 but focuses on the PV (Posture and Vulnerability Management) section of the Microsoft cloud security benchmark. It lists seven controls under PV-1 through PV-7, each with a 'Control details' link and MS/C status indicators. The sidebar and top navigation bar are identical to Figure 5.5.

Figure 5.6: Regulatory compliance color representation

The screenshot shows the security control recommendations section. It starts with a list of six controls under PV (Posture and Vulnerability Management) and then transitions to a table titled 'Automated assessments - Azure'. The table has four columns: Resource type, Failed resources, and Resource compliance status. The compliance status is indicated by colored bars: red for 1 of 1 failed resource, green for 0 of 0 failed resources, and yellow for other intermediate states. The table lists five specific assessments with their corresponding resource types and failure counts.

Automated assessments - Azure	Resource type	Failed resources	Resource compliance status
Machines should be configured to periodically check for missing system updates	Virtual machines	1 of 1	Red
SQL servers on machines should have vulnerability findings resolved	Azure resources	0 of 0	Green
System updates should be installed on your machines (powered by Azure Update Manager)	Azure resources	0 of 0	Green
Azure running container images should have vulnerabilities resolved	Azure resources	0 of 0	Green
Machines should be configured securely	Azure resources	0 of 0	Green

Figure 5.7: Security control recommendations

SQL databases should have vulnerability findings resolved

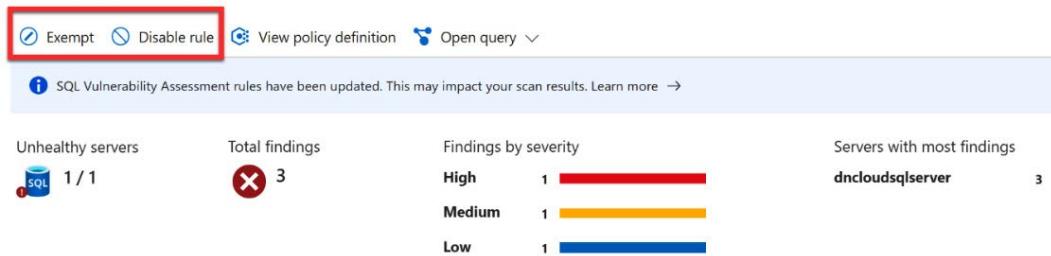


Figure 5.8: Recommendation resolution



Figure 5.9: Azure Policy workflow

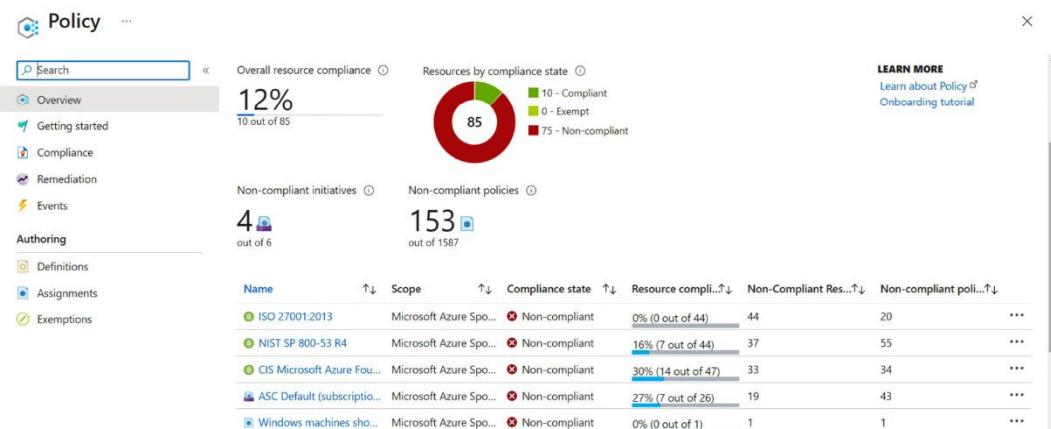


Figure 5.10: Policy compliance overview

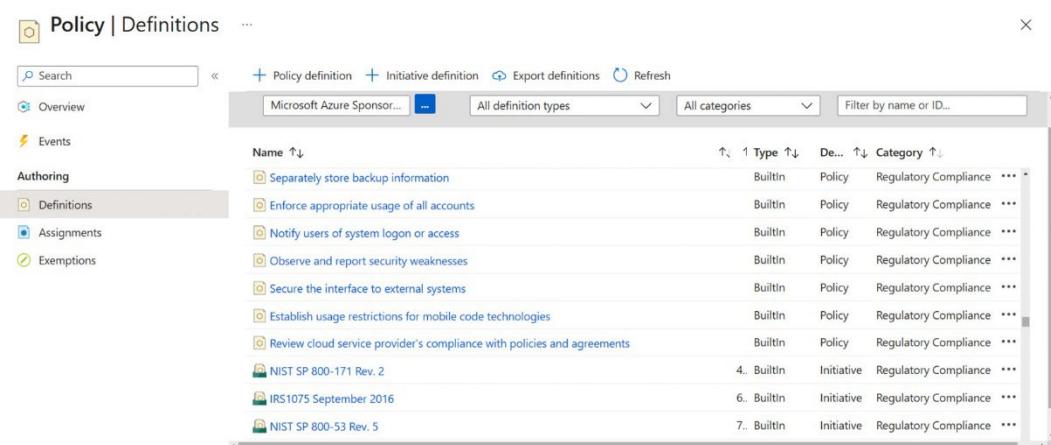


Figure 5.11: Built-in policies and + Policy definition and + Initiative definition

Name ↑	Latest version (preview) ↑	Definition location ↑	Policies ↑	Type ↑	Definition type ↑	Category ↑
Allowed locations for resource groups	1.0.0			Builtin	Policy	General
Configure subscriptions to set up preview features	1.0.1			Builtin	Policy	General
Allowed locations	1.0.0			Builtin	Policy	General
Audit usage of custom RBAC roles	1.0.1			Builtin	Policy	General
Allowed resource types	1.0.0			Builtin	Policy	General
Do not allow deletion of resource types	1.0.1			Builtin	Policy	General
Not allowed resource types	2.0.0			Builtin	Policy	General
Do Not Allow MCPP resources	1.0.0			Builtin	Policy	General
Do Not Allow M365 resources	1.0.0			Builtin	Policy	General

Figure 5.12: Allowed location policies

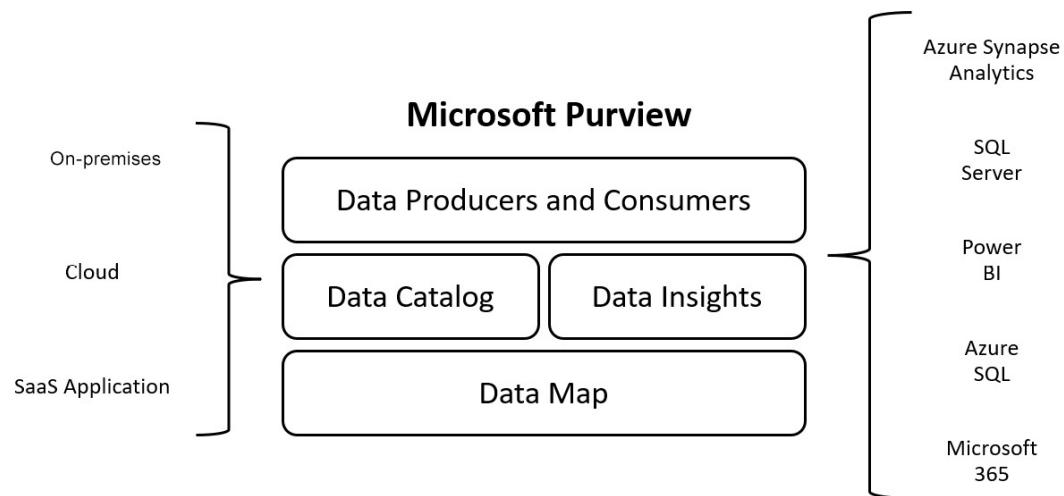


Figure 5.13: Microsoft Purview for data privacy governance

Chapter 6: Evaluate Security Posture and Recommend Technical Strategies to Manage Risk

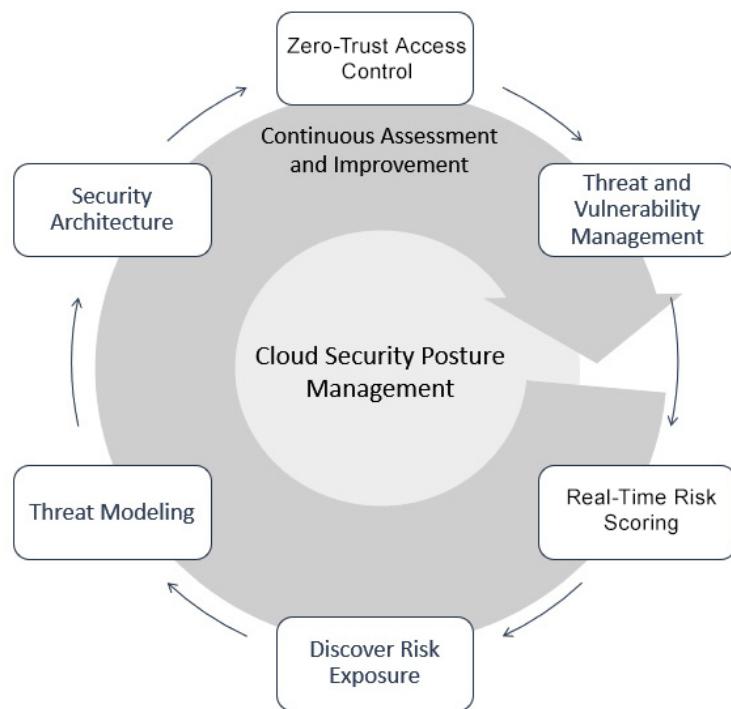


Figure 6.1: CSPM – continuous assessment and improvement

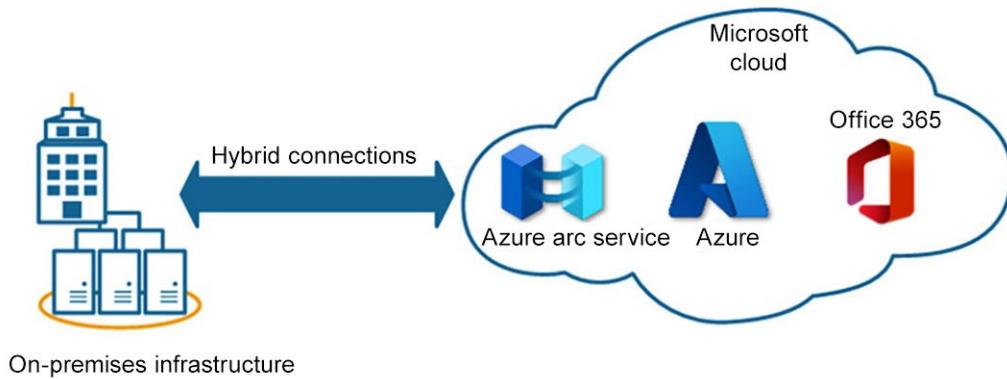


Figure 6.2: Hybrid infrastructure diagram

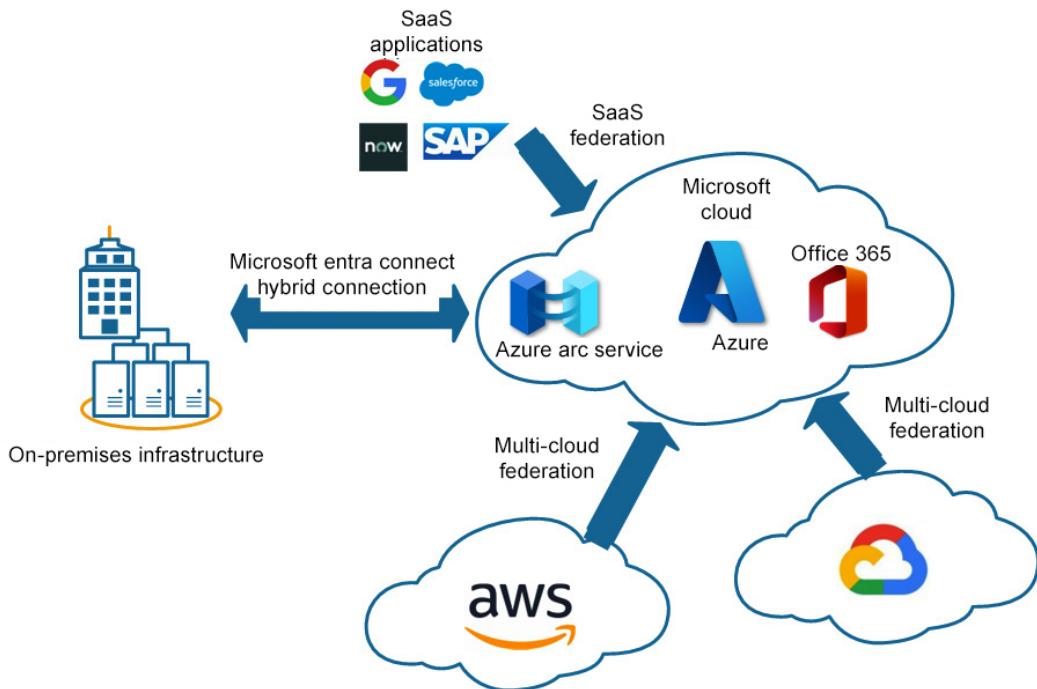


Figure 6.3: Multi-cloud infrastructure diagram

The screenshot shows the Microsoft Defender for Cloud interface under the 'Regulatory compliance' section. The left sidebar includes 'Community', 'Diagnose and solve problems', 'Cloud Security' (with 'Security posture', 'Regulatory compliance' highlighted with a red box, and 'Workload protections'), and 'Management' (with 'Environment settings' and 'Security solutions'). The main content area displays the 'Azure Security Benchmark' with '21 of 43 passed controls'. To the right, it shows 'Lowest compliance regulatory standards' with four items: SOC TSP (1/13), ISO 27001:2013 (2/17), PCI DSS 3.2.1 (12/43), and Azure CIS 1.1.0 (36/71).

Figure 6.4: Regulatory compliance in the Cloud Security menu

The screenshot shows the Microsoft Defender for Cloud | Regulatory compliance dashboard. On the left, there's a sidebar with various security categories like Cloud Security, Regulatory compliance (which is selected and highlighted in grey), Workload protections, Data security, Firewall Manager, DevOps security, Management, and Environment settings. The main area has a header with 'Download report', 'Manage compliance standards', 'Open query', 'Compliance over time workbook', and a message about customizing standards. Below this is a section titled 'Microsoft cloud security benchmark' which is also highlighted with a red border. It includes links to 'CIS Azure Foundations v1.1.0' and 'CIS Azure Foundations v1.3.0'. A note states: 'Recommendations from Microsoft Defender for Cloud - Regulatory Compliance should not be interpreted as a guarantee of compliance. It is up to you to evaluate and validate the effectiveness of customer controls per your regulatory environment. These services are subject to the terms and conditions in the [licensing terms](#)'. There's also a link to 'Microsoft cloud security benchmark is applied to the subscription ctaz-prod' and a checkbox for 'Expand all compliance controls'.

Figure 6.5: List of regulatory compliance options

- ✓ ✖ 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

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

Figure 6.7: Network security controls

^ ✖ NS. Network Security

→ NS-1. Establish network segmentation boundaries [Control details](#) [MS] [C]

Customer responsibility	Resource type	Failed resources	Resource compliance...
Adaptive network hardening recommends	Virtual machines	4 of 5	<div style="width: 80%;"><div style="width: 20%; background-color: red;"></div><div style="width: 80%; background-color: limegreen;"></div></div>
All network ports should be restricted on I	Virtual machines	4 of 5	<div style="width: 80%;"><div style="width: 20%; background-color: red;"></div><div style="width: 80%; background-color: limegreen;"></div></div>
Subnets should be associated with a netw	Subnets	2 of 3	<div style="width: 66%;"><div style="width: 33%; background-color: red;"></div><div style="width: 66%; background-color: limegreen;"></div></div>
Non-internet-facing virtual machines shou	Virtual machines	0 of 5	<div style="width: 0%;"><div style="width: 0%; background-color: grey;"></div></div>
Internet-facing virtual machines should	Virtual machines	0 of 5	<div style="width: 100%; background-color: limegreen;"></div>

Figure 6.8: Recommended security controls to increase security posture

- ▽ ✖ 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

Microsoft Defender for Cloud

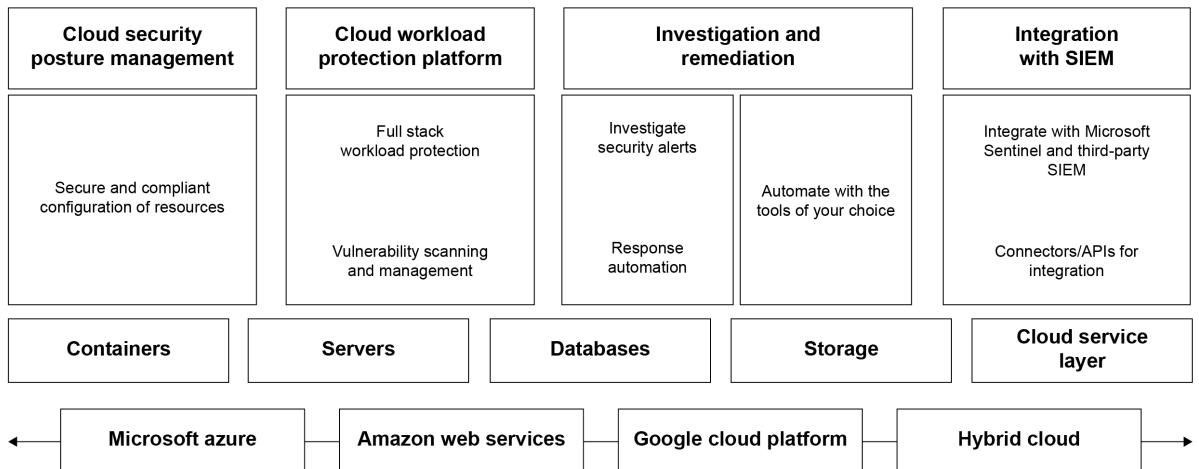


Figure 6.10: Microsoft Defender for Cloud capabilities

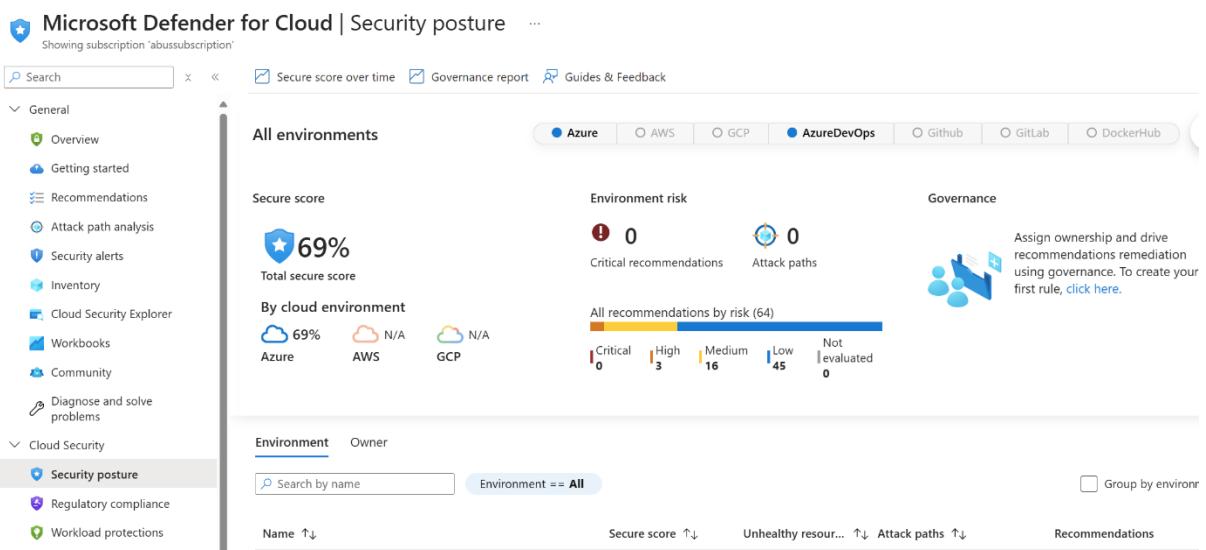


Figure 6.11: Security posture in the Cloud Security menu

The screenshot shows the Microsoft Defender for Cloud Security posture dashboard. On the left, a sidebar lists categories like General, Security alerts, and Workbooks. The 'Security posture' section is selected. At the top right, it displays a score of 11/18 for Unhealthy resources and 45 Recommendations. Below this, there's a table for the 'Environment' tab, showing two rows: 'Microsoft Azure Sponsorship' (Secure score: 31%, 11 of 15 recommendations) and 'AWS account' (Secure score: N/A, 0 of 0 recommendations). A red arrow points to the 'View recommendation...' link for the Azure subscription row.

Figure 6.12: Subscription security posture recommendations

The screenshot shows the 'Recommendations' page. It has a header with refresh, CSV download, and search functions. Below is a table titled 'Secure score recommendations' for the 'Azure' environment. The columns include Name, Max score, Current score, Potential score increase, Status, and Unhealthy resources. A red arrow points to the 'Potential score increase' column header. The table lists several recommendations, such as 'Enable MFA' (Max score 10, Current score 0.00, +18% potential increase, Unassigned status, 1 resource unhealthy).

Figure 6.13: Potential score increase

Name	Max score	Current score	Potential score increase
Enable MFA	10	0.00	+ 18%
MFA should be ena...			
MFA should be ena...			

Figure 6.14: Enable MFA recommendations 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.

1. Select the relevant subscription or click 'Take action' if it's available. The list of user accounts without MFA appears.
2. Click 'Continue'. The Azure AD Conditional Access page appears.
3. In the Conditional access page, add the list of users to a policy (create a policy if one doesn't exist).
4. For your conditional access policy, ensure the following:
 - a. In the 'Access controls' section, multi-factor authentication is granted.
 - b. 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

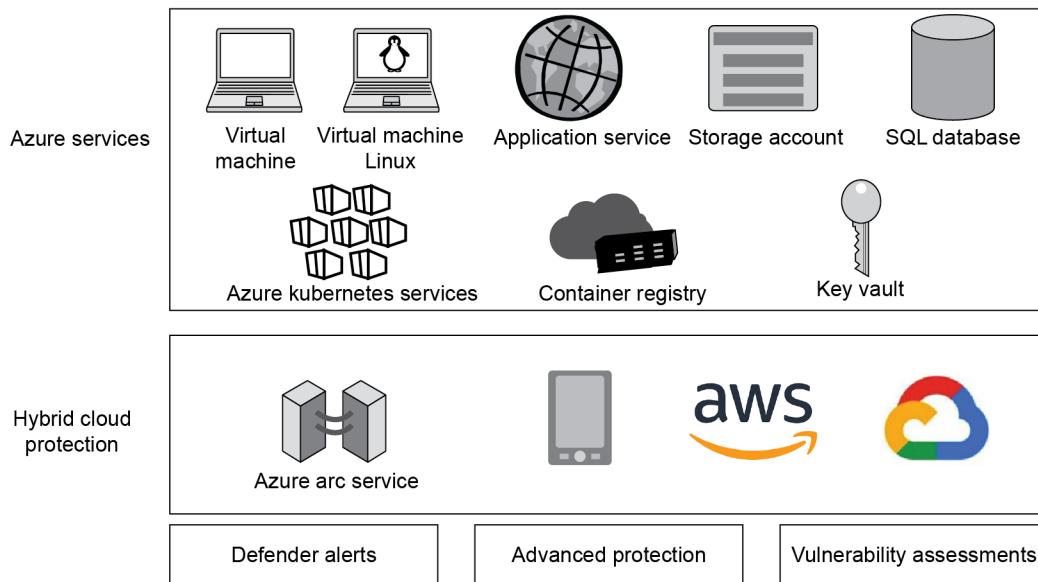


Figure 6.16: Microsoft Defender for Cloud enhanced security protection

The screenshot shows the Microsoft Azure portal interface. At the top, there is a blue header bar with the Microsoft Azure logo and a search bar containing the text "Microsoft defender for cloud". A red arrow points from the text in the search bar down to the "Services" list below. The "Services" list includes:

- Microsoft Defender for Cloud (highlighted with a red box)
- Azure Database for MySQL servers
- Microsoft Defender for IoT

On the left side, there is a sidebar with the "Azure services" heading and a "Create a" button.

Figure 6.17: Navigating to Microsoft Defender for Cloud

The screenshot shows the Microsoft Defender for Cloud Overview page. On the left, a navigation sidebar includes links for Security alerts, Inventory, Workbooks, Community, Diagnose and solve problems, Cloud Security (Security posture, Regulatory compliance, Workload protections, Firewall Manager), Management, Environment settings (highlighted with a red box), Security solutions, and Workflow automation. The main dashboard displays key metrics: 1 Azure subscription, 1 AWS account, 27 Assessed resources, 46 Active recommendations, and 58 Security alerts. It also features two cards: 'Security posture' (14/14 Unassigned recommendation, 0/0 Overdue recommendations, Secure score 35% for Azure) and 'Regulatory compliance' (Azure Security Benchmark 26 of 43 passed controls, showing compliance with SOC TSP, ISO 27001:2013, and PCI DSS 3.2.1).

Figure 6.18: Environment settings in Microsoft Defender for Cloud

The screenshot shows the Settings | Defender plans page. The left sidebar lists Settings (Defender plans, Auto provisioning, Email notifications, Integrations, Workflow automation, Continuous export), Policy settings (Security policy, Governance rules (preview)), and a Microsoft Azure Sponsorship banner. The main area shows a message about a new 'Containers' plan replacing existing ones. Below is a table titled 'Defender for Cloud plans will be enabled on 10 resources in this subscription'. It includes a 'Select Defender plan' dropdown (set to 'Enable all') and a 'Save' button (highlighted with a red box). The table lists four resources: Cloud Security Posture Ma (Free, Status: Off), Servers (Plan 2 (\$15/Server/Mo, Change plan >, 5 servers, Status: Off), App Service (\$15/Instance/Month, 0 instances, Status: Off), and Databases (Selected: 4/4, Select types >, Protected: 1/1 instance, Full Settings >, Status: Off).

Figure

6.19: Enabling Defender for Cloud enhanced security plans

The screenshot shows the Microsoft Defender for Cloud Workload protections dashboard. On the left, a sidebar menu includes 'Workload protections' which is highlighted with a red arrow. The main area displays 'Defender for Cloud coverage' with a total of 12 items. Below this are four sections: 'Azure SQL database servers' (1/1), 'Key Vault' (1/1), 'Servers' (5/5), and 'DNS subscriptions' (1/1). Each section has an 'Upgrade' link.

Figure 6.20: Workload protections in the Cloud Security menu

The screenshot shows the Microsoft Defender for Cloud Workload protections dashboard. The 'Workload protections' menu item is highlighted with a red box. The main area displays 'Security alerts' with a bar chart showing alert counts over time. Below this is the 'Advanced protection' section, which is also highlighted with a red box. This section contains seven tiles: 'VM vulnerability assessment' (5 Unprotected), 'Just-in-time VM access' (4 Unprotected), 'Adaptive application control' (2 Unprotected), 'Container image sca' (None Unprotect), 'SQL vulnerability assessment' (1 Unprotected), 'File integrity monitoring', 'Network map', and 'IoT security'.

Figure 6.21: Advanced protection for Defender plans

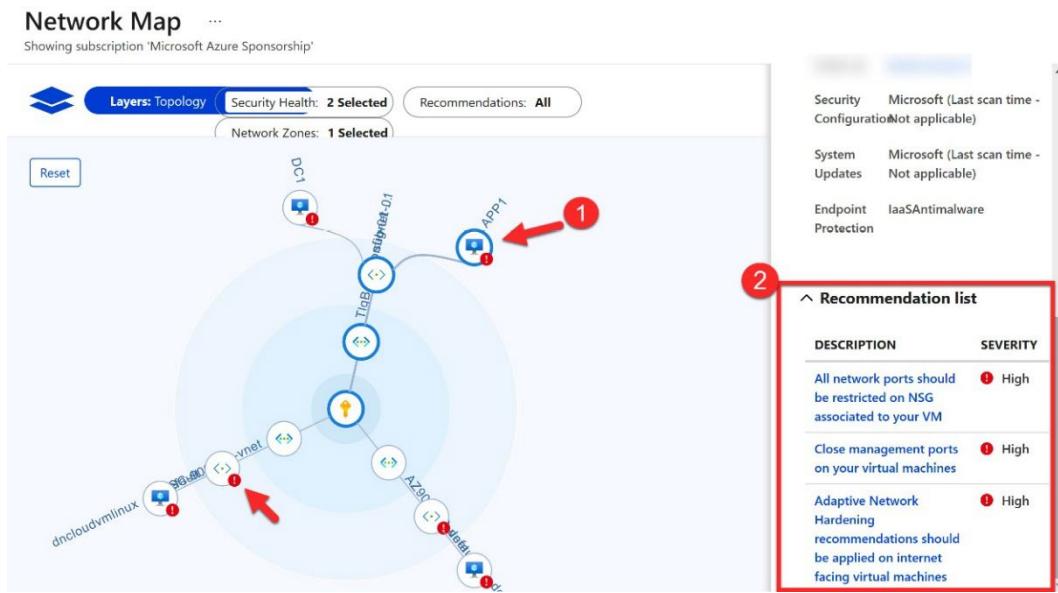


Figure 6.22: Network map and security posture recommendations

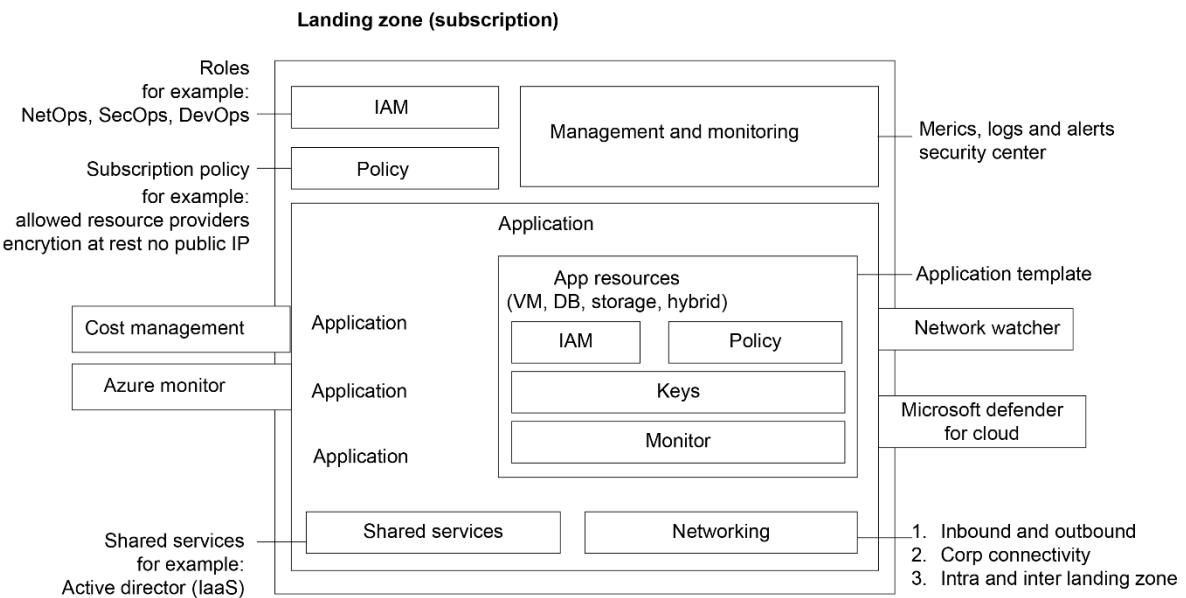


Figure 6.23: Diagram of the components of an Azure landing zone

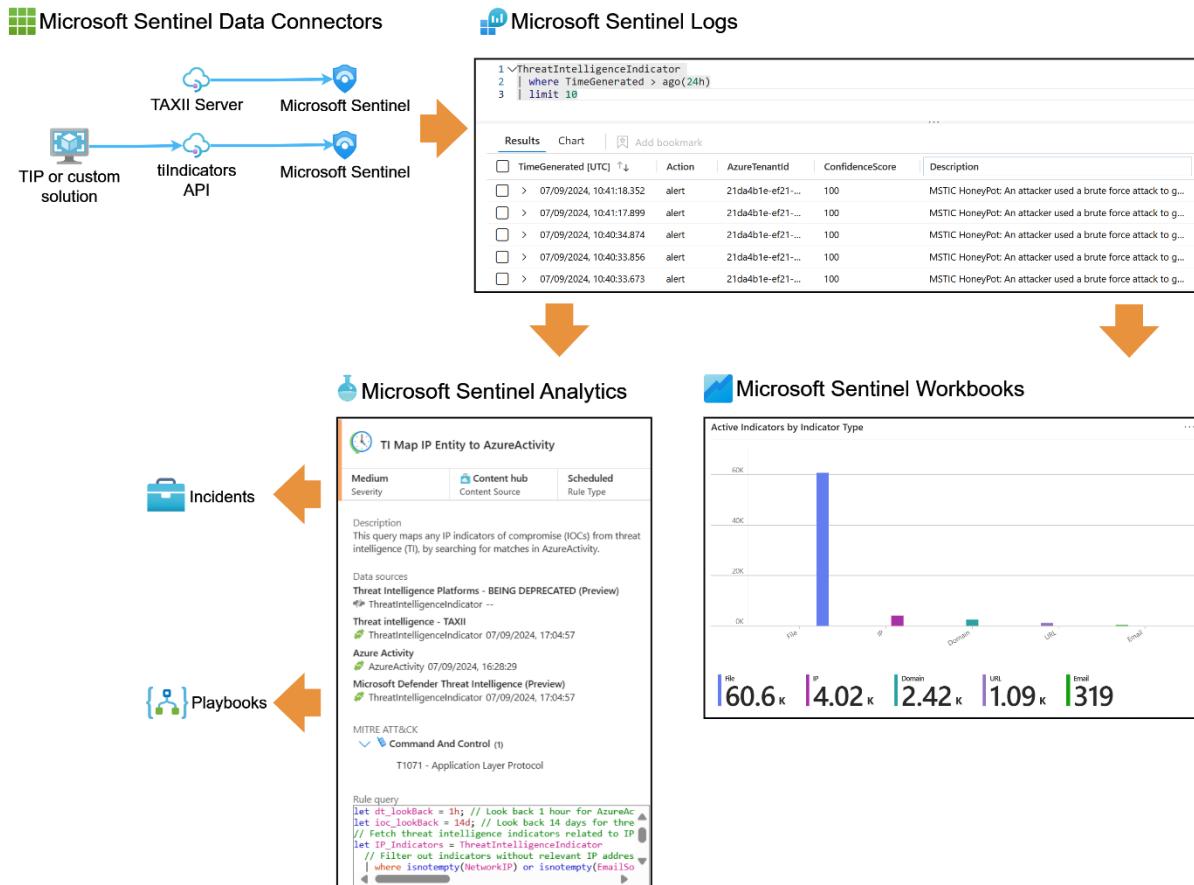


Figure 6.24: Microsoft Sentinel tools for threat intelligence

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	

Impact →

How Serious is the Risk?

Figure 6.25: Risk assessment matrix

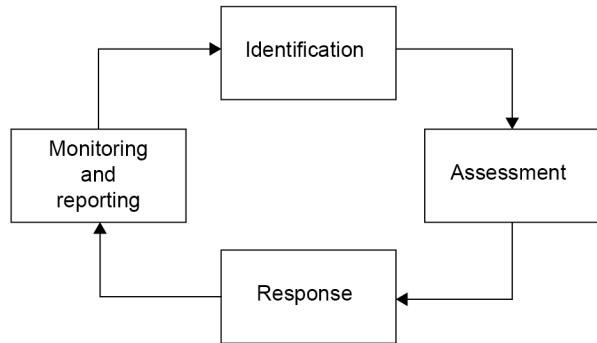


Figure 6.26: Risk assessment and mitigation life cycle

The screenshot shows the Microsoft Defender External Attack Surface Management (EASM) interface within the Azure portal. The top navigation bar includes 'myworkspace' and 'Inventory'. The left sidebar menu is collapsed under 'General' and shows 'Overview', 'Inventory' (which is selected and highlighted in grey), 'Inventory changes', 'Dashboards', 'Manage', and 'Help'. The main content area features a heading 'Welcome to Microsoft Defender External Attack Surface Management (EASM)!'. Below it, a sub-section explains that Microsoft maintains an inventory of internet-facing devices and services (assets) used to discover an organization's attack surface. It also encourages users to search for pre-built attack surfaces to understand their organization's internet exposure. A large, central network graph visualization displays numerous nodes (represented by colored dots) connected by lines, forming a complex web of relationships. At the bottom of the main content area, there is a search bar labeled 'Search for an organization' and a link 'Create a custom attack surface'.

Figure 6.27: Screenshot of Defender for EASM in Azure portal

Chapter 7: Design a Strategy for Securing Server and Client Endpoints

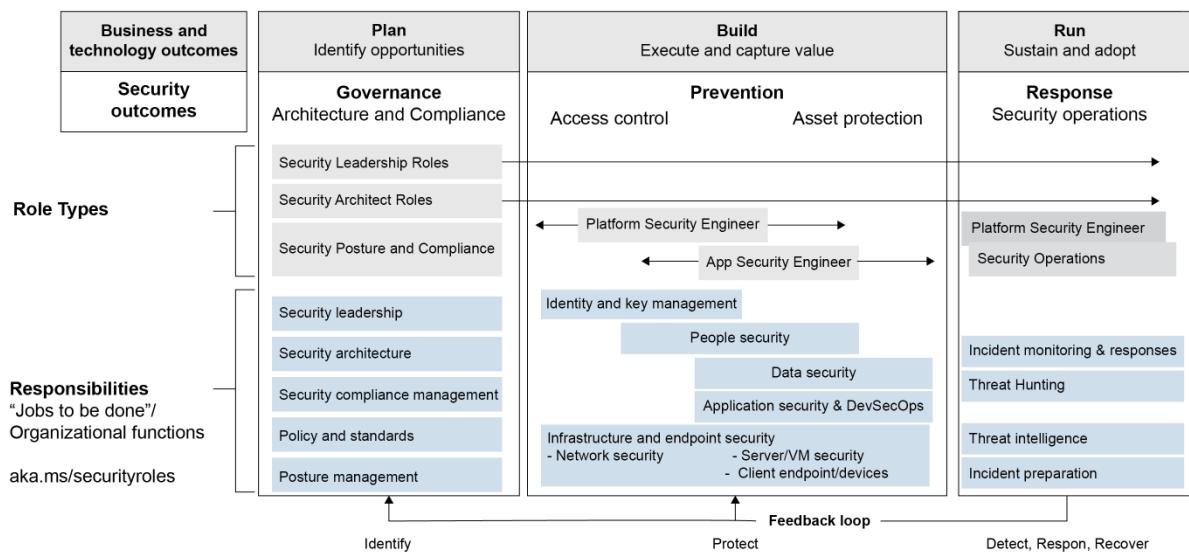


Figure 7.1: A flowchart that outlines a structured approach to cybersecurity, divided into five phases: Govern, Plan, Build, Operate, and Sustain

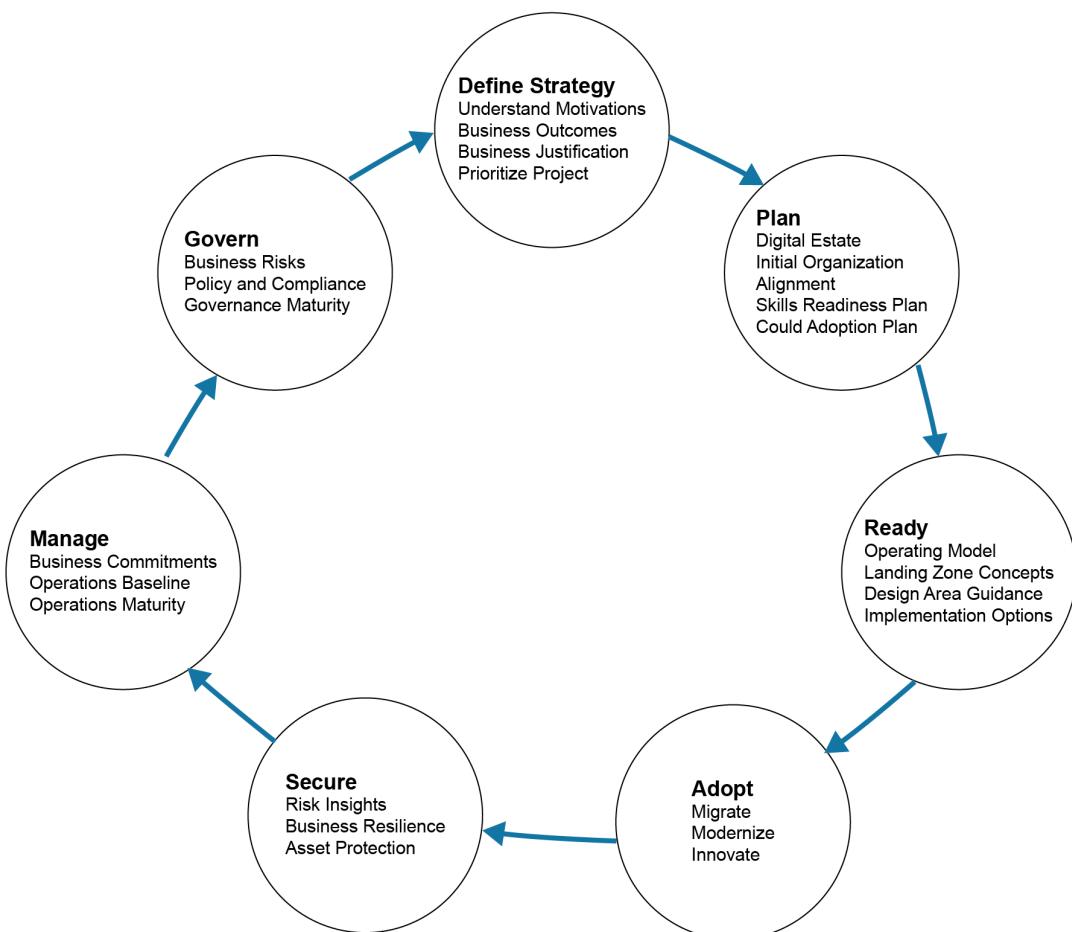


Figure 7.2: CAF depicted as a cyclical lifecycle: Define Strategy, Plan, Ready, Adopt, Secure, Manage, Govern, and then start again

Microsoft Endpoint Manager admin center

Home > Endpoint security | Overview > Endpoint security

Endpoint security | Security baselines

Search

Overview

- 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: Microsoft Endpoint Manager admin center on the “Endpoint security | Security baselines” pages

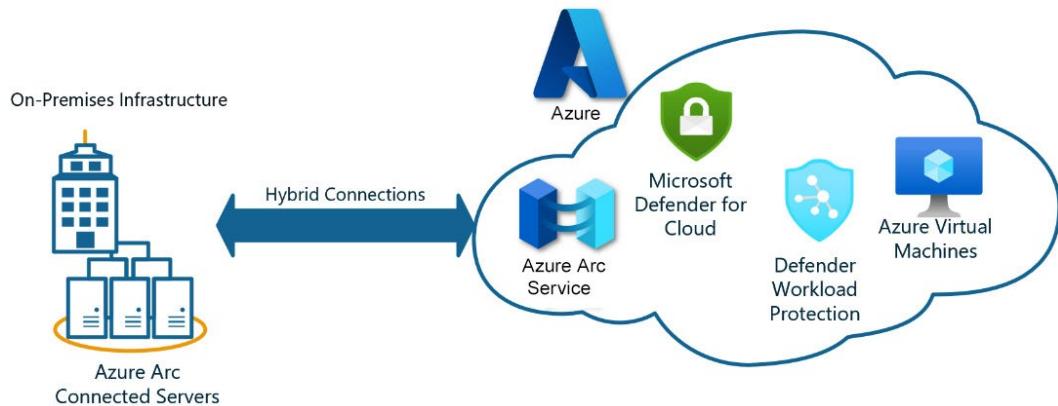


Figure 7.4: Hybrid server infrastructures

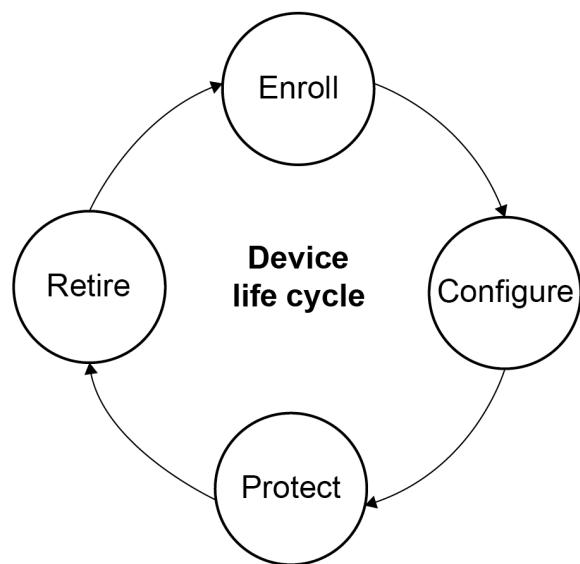


Figure 7.5: Mobile device life cycle – from Enrol, through Configure, Protect, and then Retire

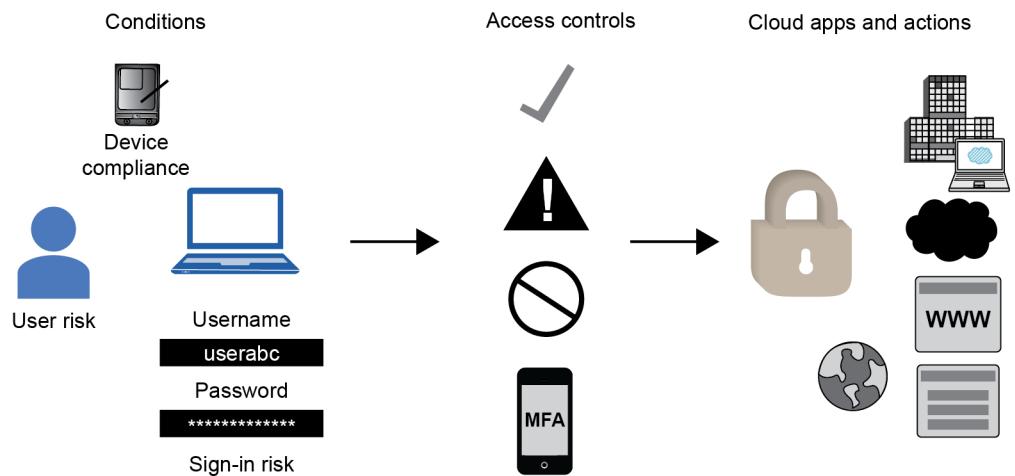


Figure 7.6: Conditional Access policies for MDM-compliant devices, highlighting the various conditions that can be evaluated

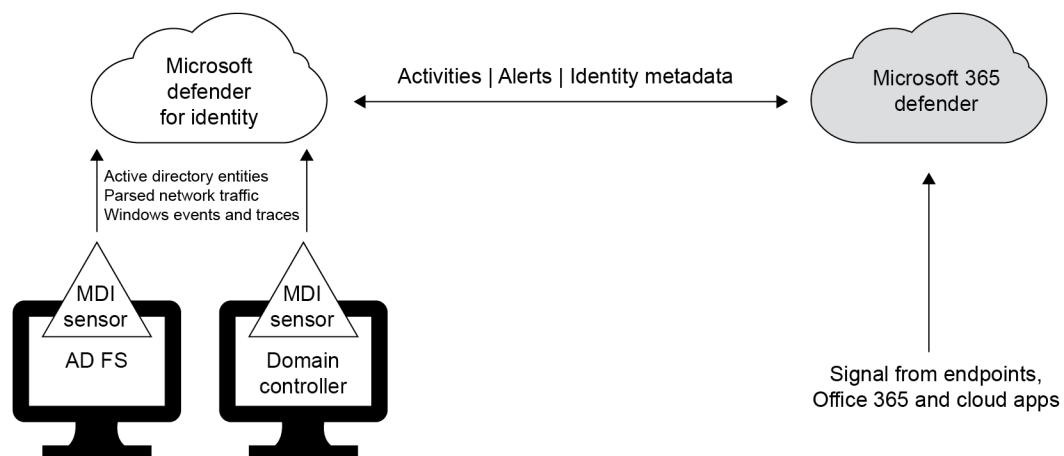


Figure 7.7: Microsoft Defender for Identity (MDI) integrating with Microsoft 365 Defender

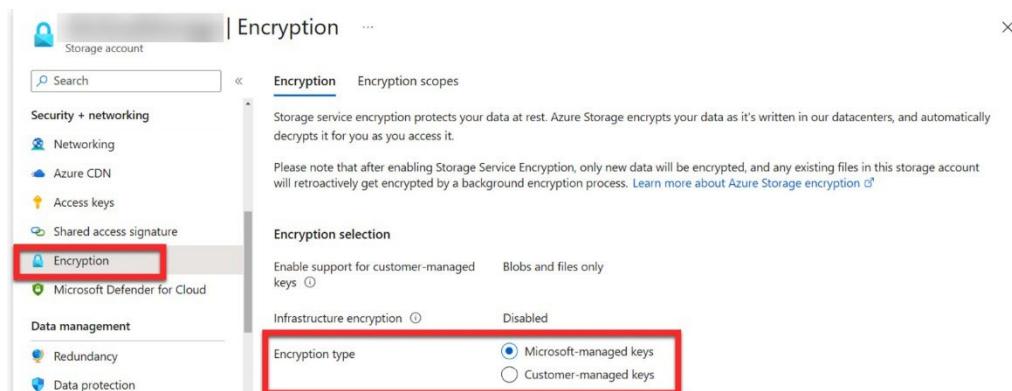


Figure 7.8: Configuring customer-managed keys with Azure Key Vault – a screenshot from the Azure portal

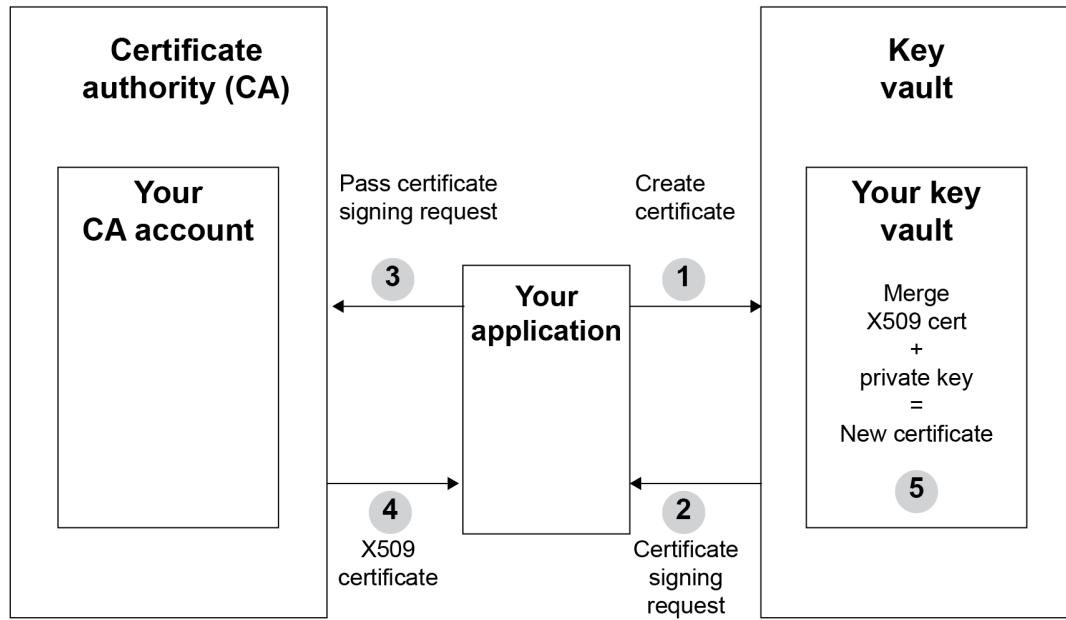


Figure 7.9: CA validation process with Azure Key Vault

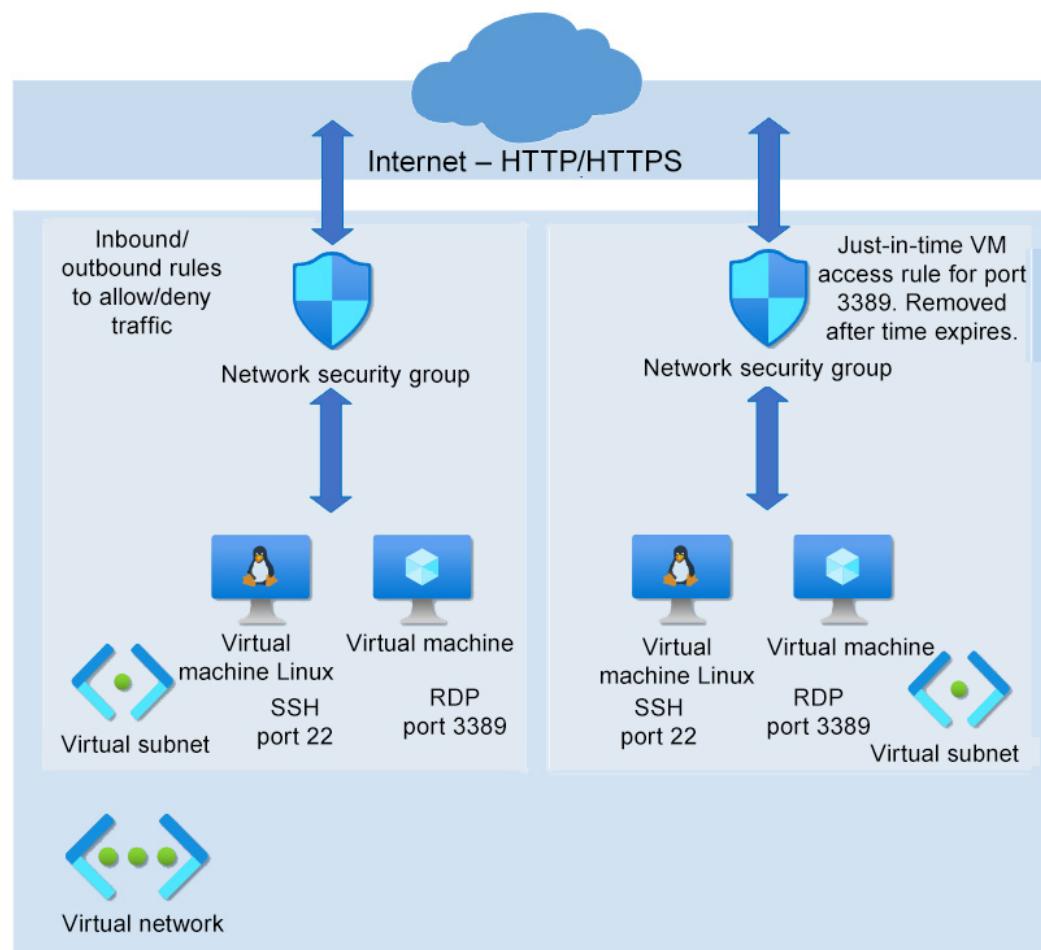


Figure 7.10: NSG with a JIT virtual machine access inbound rule

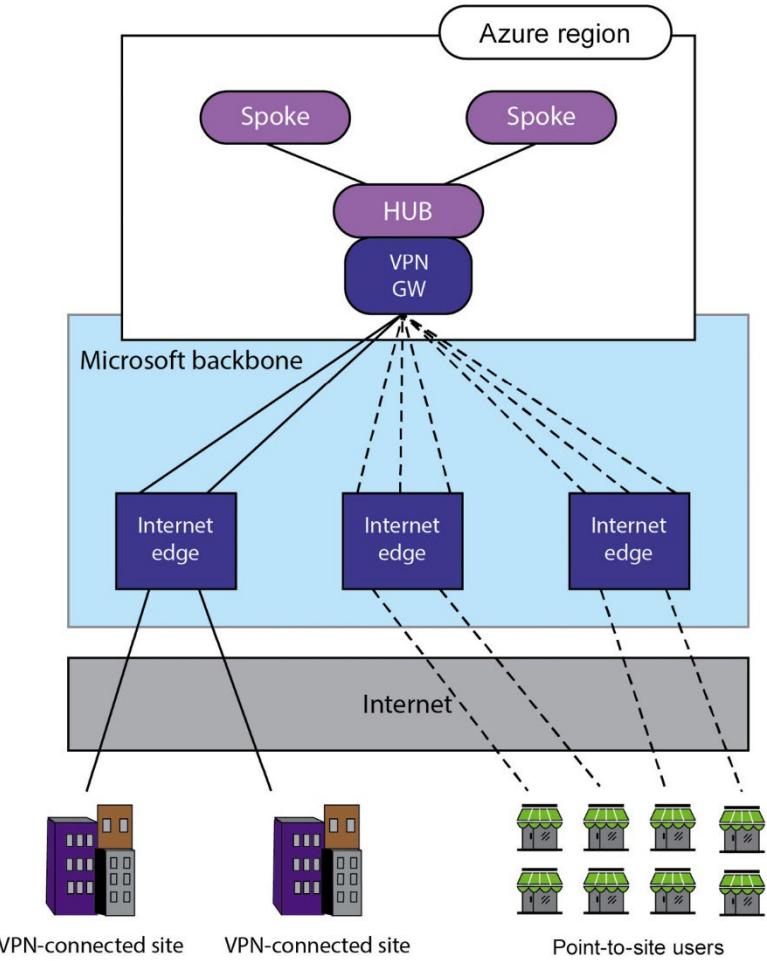


Figure 7.11: Secure connectivity from Azure to on-premises sites

Chapter 8: Design a Strategy for Securing SaaS, PaaS, and IaaS

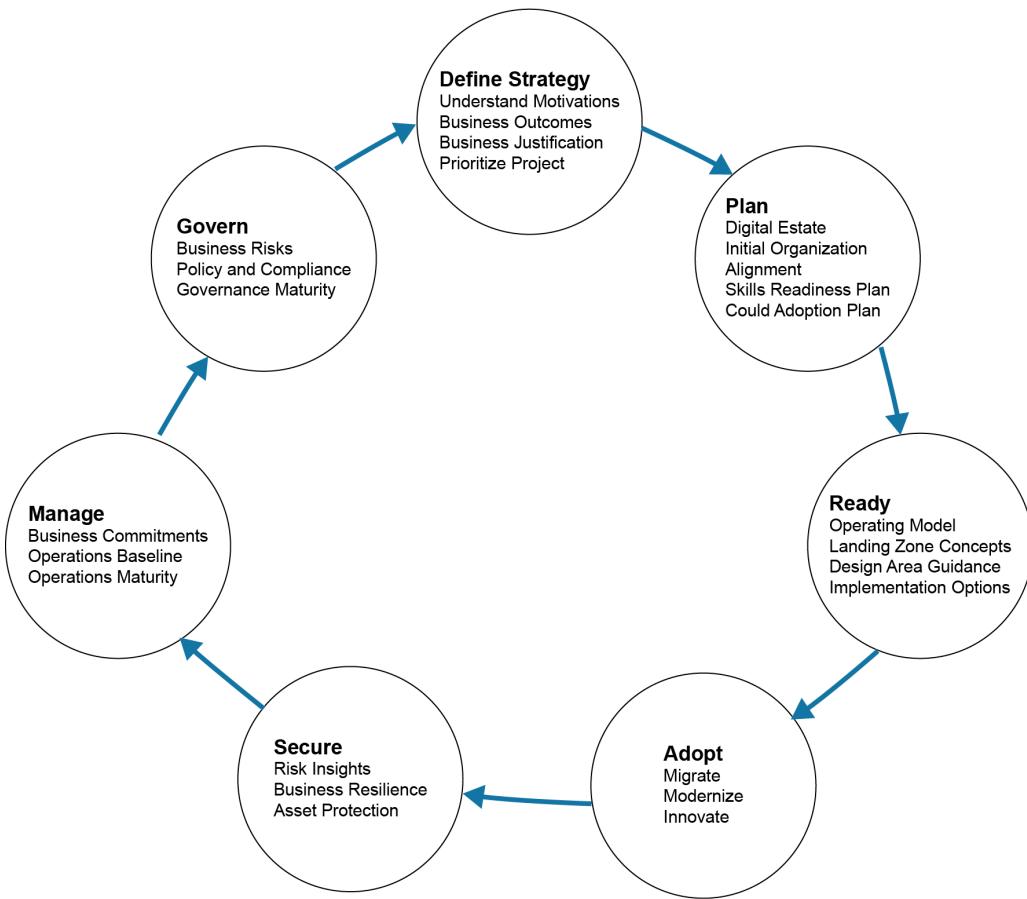


Figure 8.1 – CAF

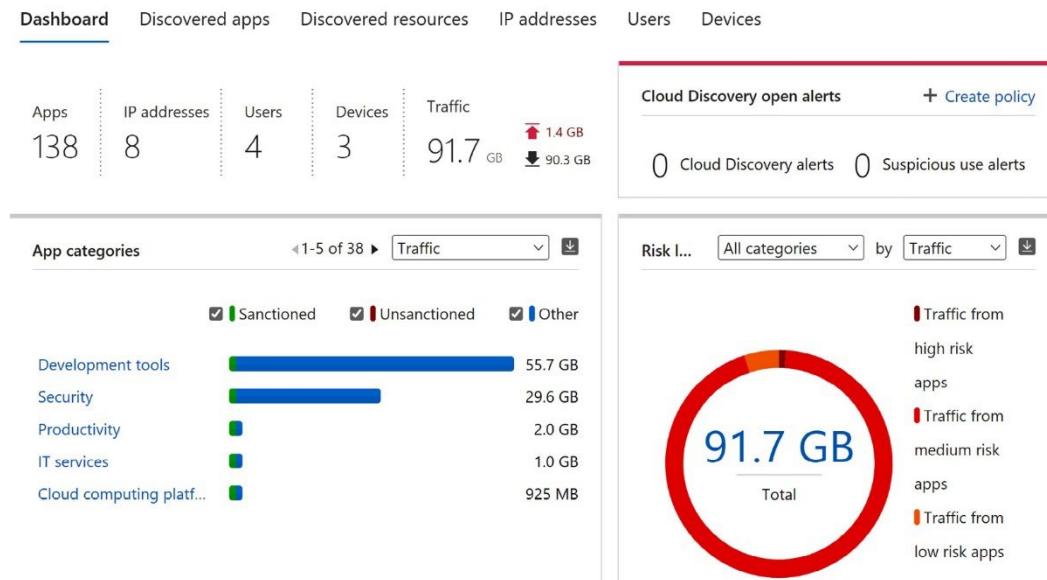


Figure 8.2 – The Microsoft Defender for Cloud Apps discovery dashboard

Secure score recommendations All recommendations

Unassigned recommendations 16/16

Name ↑↓	Max score	Current sc...	Potential score in...	Status ↑↓	Unhealthy resources
> Enable MFA	10	0.00	+ 18%	Unassigned	1 of 1 resources
✓ Secure management ports	8	1.60	+ 11%	Unassigned	4 of 5 resources
				Completed	0 of 5 virtual machine
				Unassigned	4 of 5 virtual machine
				Unassigned	4 of 5 virtual machine
✓ Remediate vulnerabilities	6	0.00	+ 11%	Unassigned	5 of 5 resources
				Unassigned	5 of 5 virtual machine

Figure 8.3 – Microsoft Defender for Cloud virtual machine security recommendations

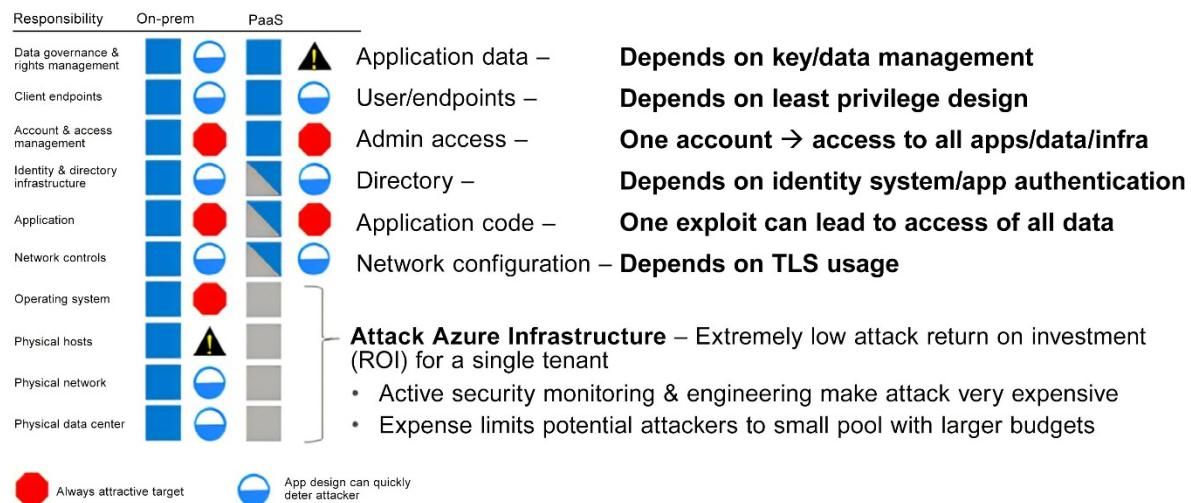


Figure 8.4 – Security controls for PaaS

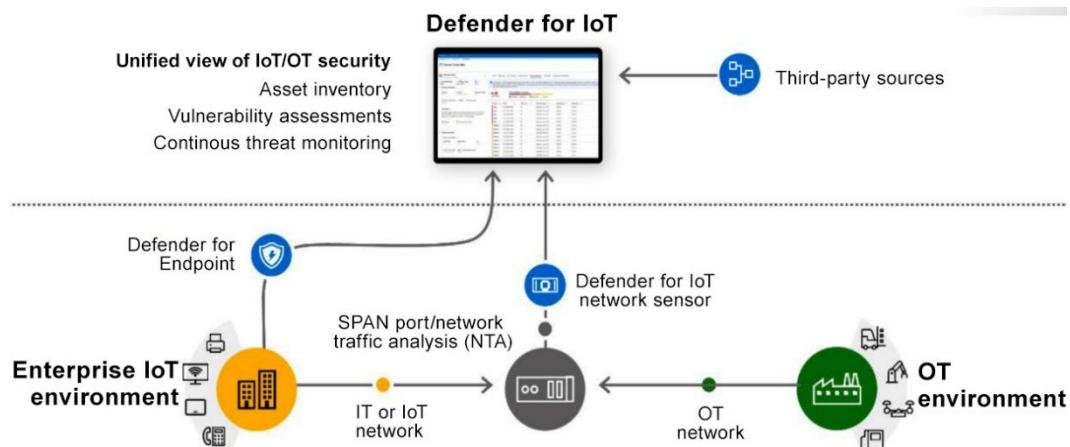


Figure 8.5 – Defender for IoT threat detection diagram

Home > **Defender for IoT | Getting started** Showing subscription 'ctaz-prod'

Get started Sensor On-premises management console Updates

Getting started

- Device inventory
- Alerts
- Recommendations (Preview)
- Workbooks
- Firmware analysis (Preview)

Management

- Sites and sensors
- Plans and pricing

Troubleshooting + Support

- Diagnose and solve problems

Welcome to Microsoft Defender for IoT

Defender for IoT delivers agentless, network-layer security for continuous IoT/OT asset discovery, vulnerability management, and threat detection in operational and enterprise networks. No changes to existing environments are required. In addition, the solution integrates with Microsoft Sentinel and 3rd-party SOC tools such as Splunk, IBM QRadar, ServiceNow, and others. Defender for IoT has zero impact on network performance and can be deployed fully on-premises or in Azure-connected environments.

[Read more about the solution](#)

Operational networks (OT/ICS)
Discover, monitor, and protect devices across your OT, ICS, IIoT, and BMS networks.

Enterprise networks (IoT)
Gain full visibility into unmanaged IoT devices across your enterprise networks. [Learn more](#)

What else?
Deploy an on-premises management console [Optional integration for alerts, investigation, and threat hunting in a single pane of glass](#)
Connect to Microsoft Sentinel
Join the community

Figure 8.6 – Microsoft Defender for IoT getting started

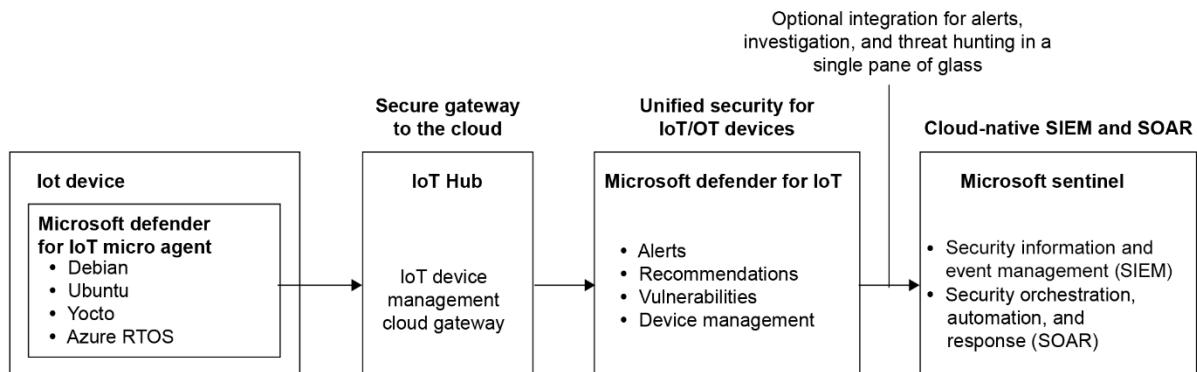


Figure 8.7 – Microsoft Defender for IoT micro agent architecture

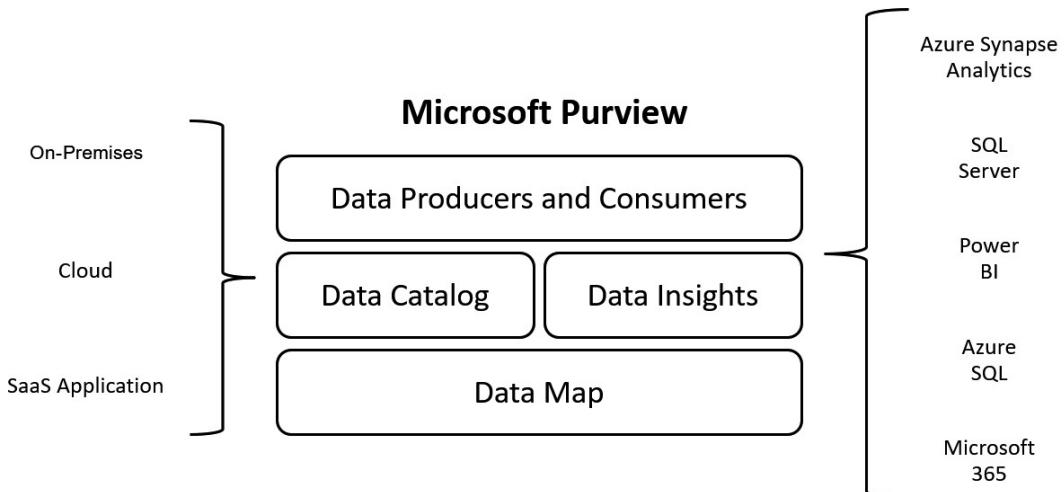


Figure 8.8 – Microsoft Purview data sources

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

Figure 8.9 – Microsoft Defender for Cloud SQL security recommendations

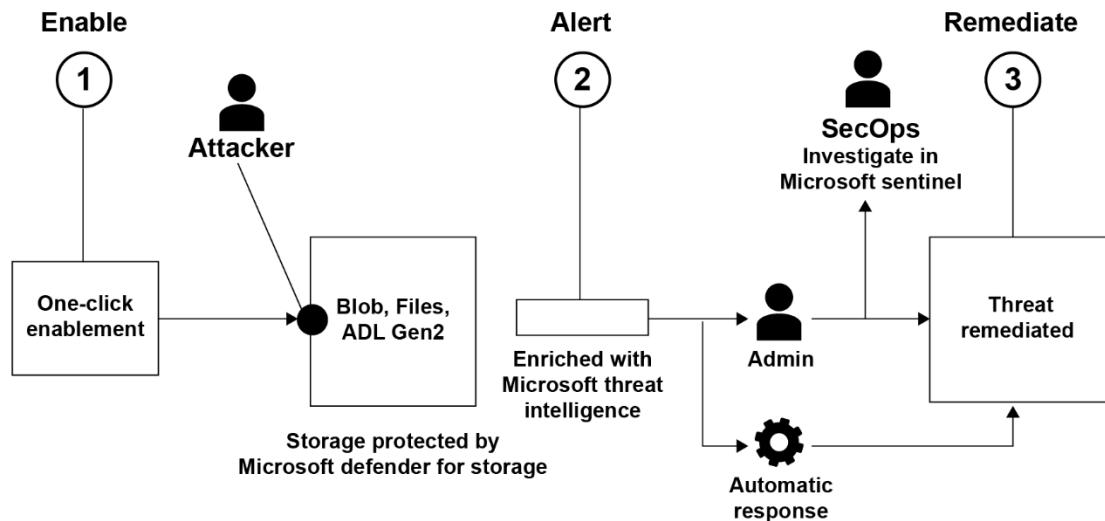


Figure 8.10 – Microsoft Defender for Storage threat protection

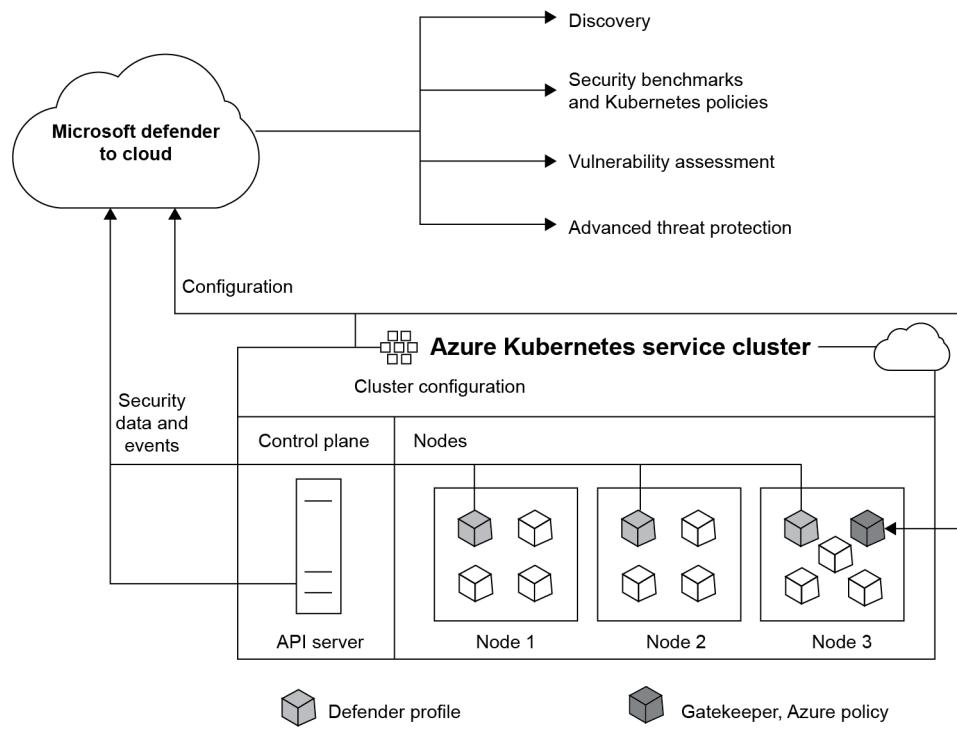


Figure 8.11 – Diagram illustrating the architecture of a cloud computing security system, specifically focusing on Microsoft Defender for Cloud integrated with an Azure Kubernetes Service (AKS) cluster

Screenshot of the Azure portal showing the configuration of network access for an Azure AI service.

The URL is: Home > sc100_packtrg > sc100

The page title is: **sc100 | Networking** (Azure AI services multi-service account)

The left sidebar shows the following navigation items:

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Resource Management** (selected)
- Keys and Endpoint
- Pricing tier
- Networking** (selected)
- Identity
- Cost analysis
- Properties
- Locks
- Security

The main content area shows the following configuration:

- Firewalls and virtual networks** tab is selected.
- Allow access from** section:
 - Selected Networks and Private Endpoints** (radio button selected)
 - All networks**
 - Disabled**
- Virtual networks** section:
 - Secure your Azure AI services account with virtual networks.
 - + Add existing virtual network**
 - + Add new virtual network**

Virtual Network	Subnet	Address range	Endpoint Status	Resource group	Subscription
vnet01	1			sc100_packtrg	ctaz-prod
- Firewall** section:
 - Add IP ranges to allow access from the internet or your on-premises networks.
 - Add your client IP address (2.125.69.22)** (checkbox)
- Address range** section:
 - IP address or CIDR** input field (empty)
- Exceptions** section (empty)

Figure 8.12 – Configuring network access for an Azure AI service in the Azure portal

Chapter 9: Specify Security Requirements for Applications

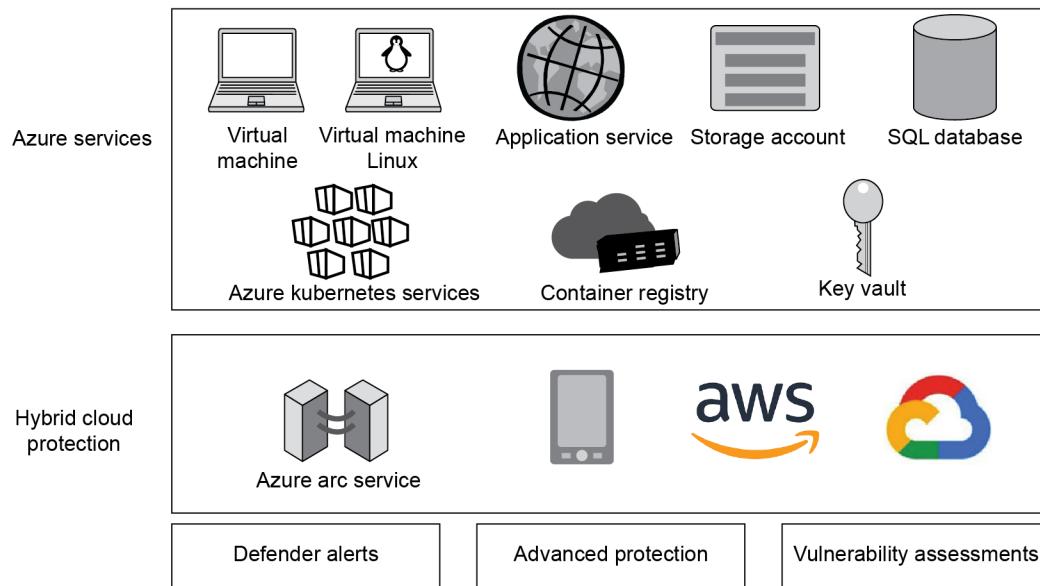


Figure 9.1: Microsoft Defender for Cloud workload protection plans

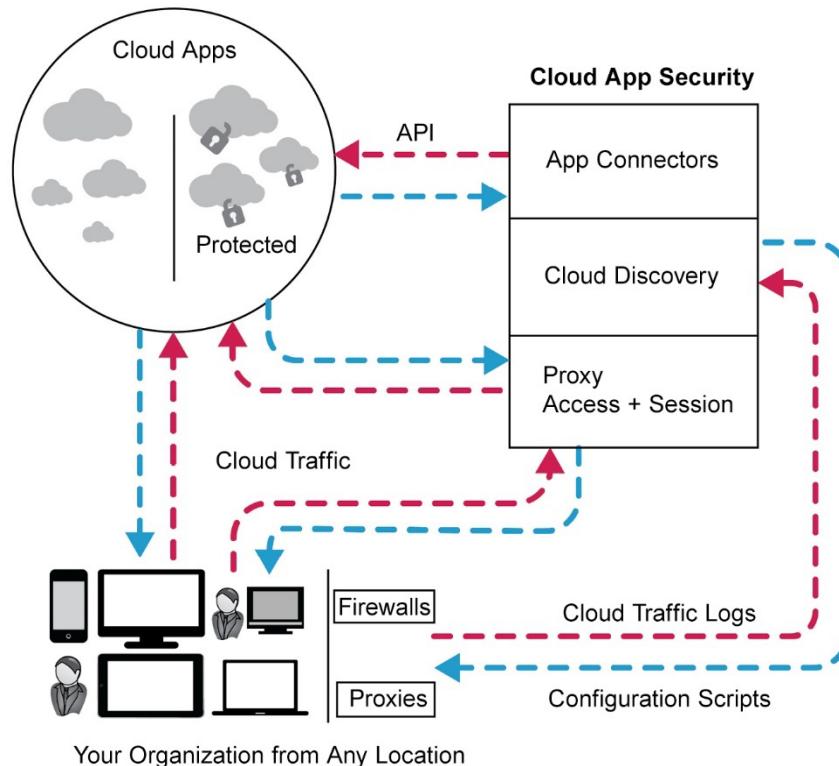


Figure 9.2: Microsoft Defender for Cloud Apps protection workflow

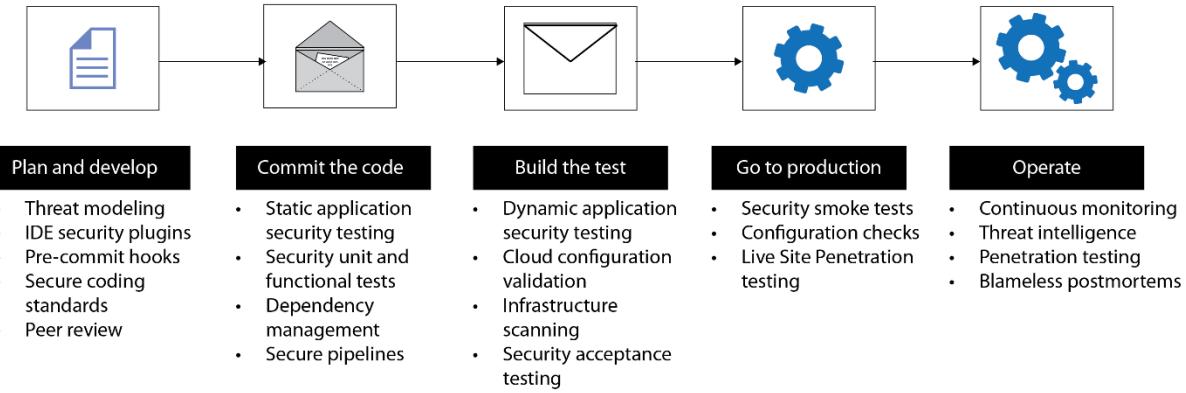


Figure 9.3: DevSecOps and the CAF

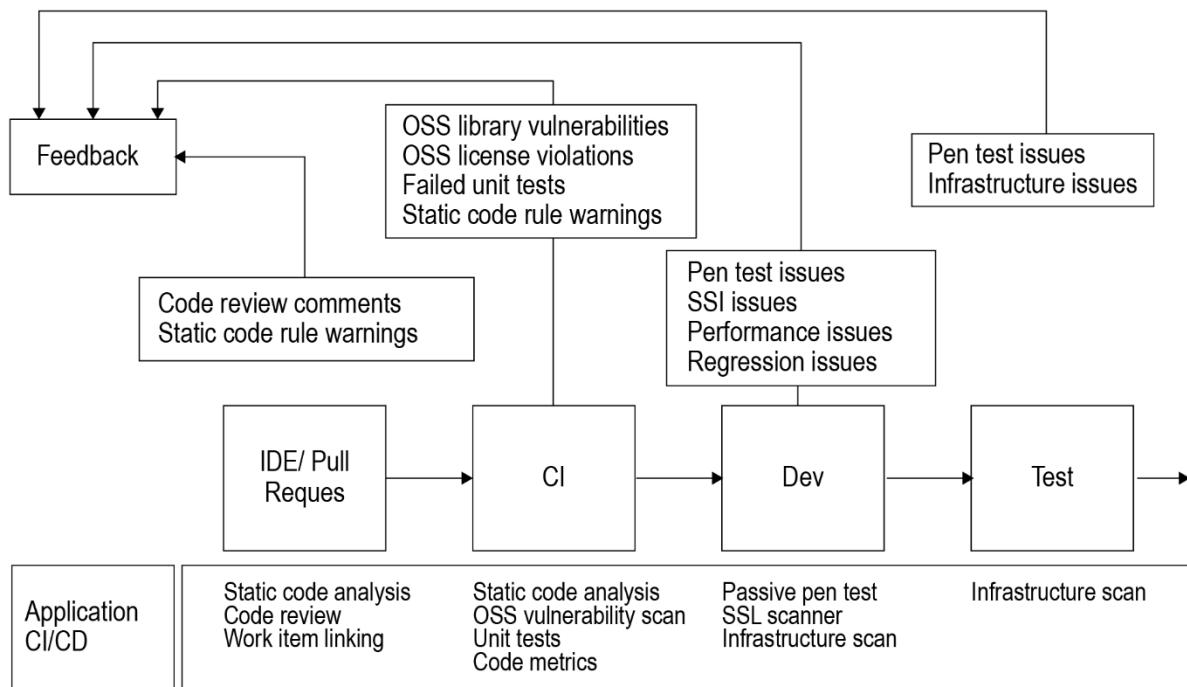


Figure 9.4: Continuous feedback loop

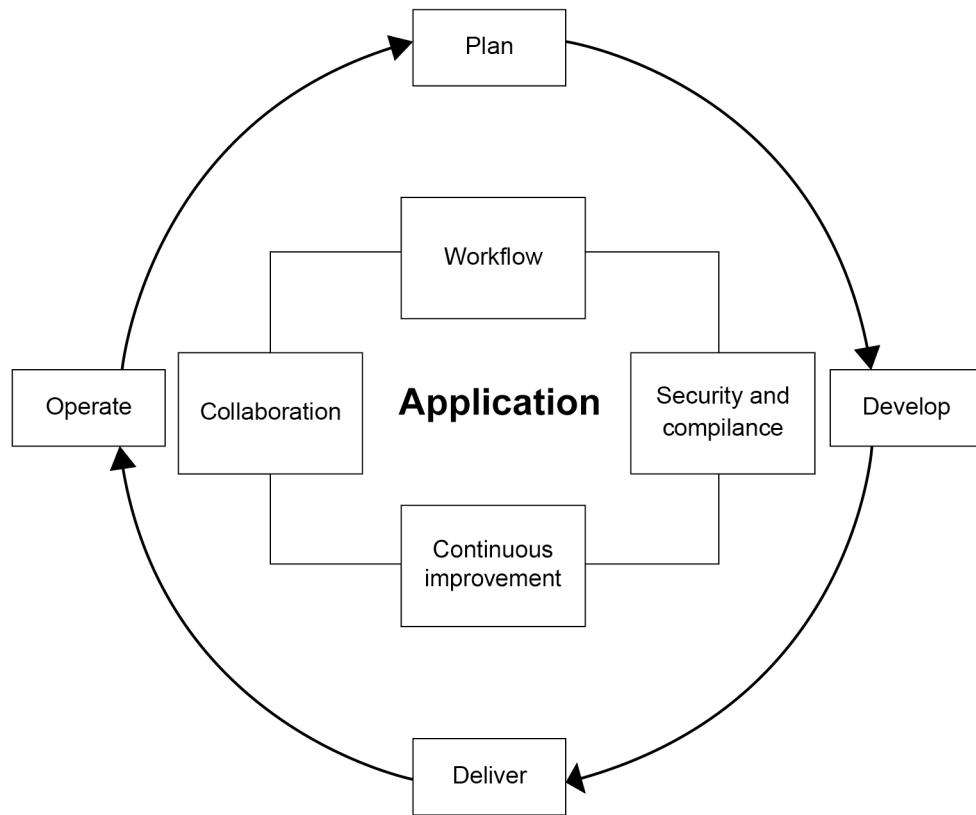


Figure 9.5: Continuous life cycle of DevSecOps



Figure 9.6: Devices sending data to data sources through APIs

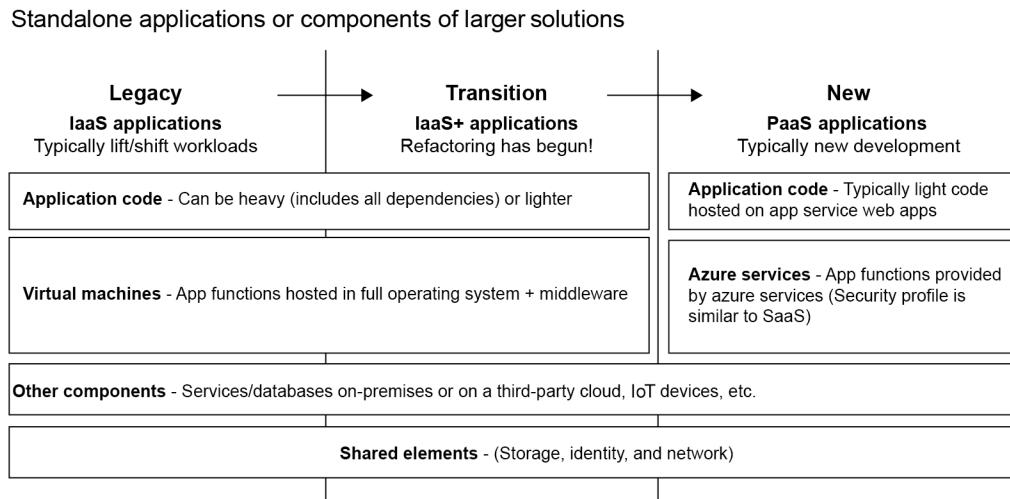


Figure 9.7: Application evolution to PaaS

Chapter 10: Design a Strategy for Securing Data

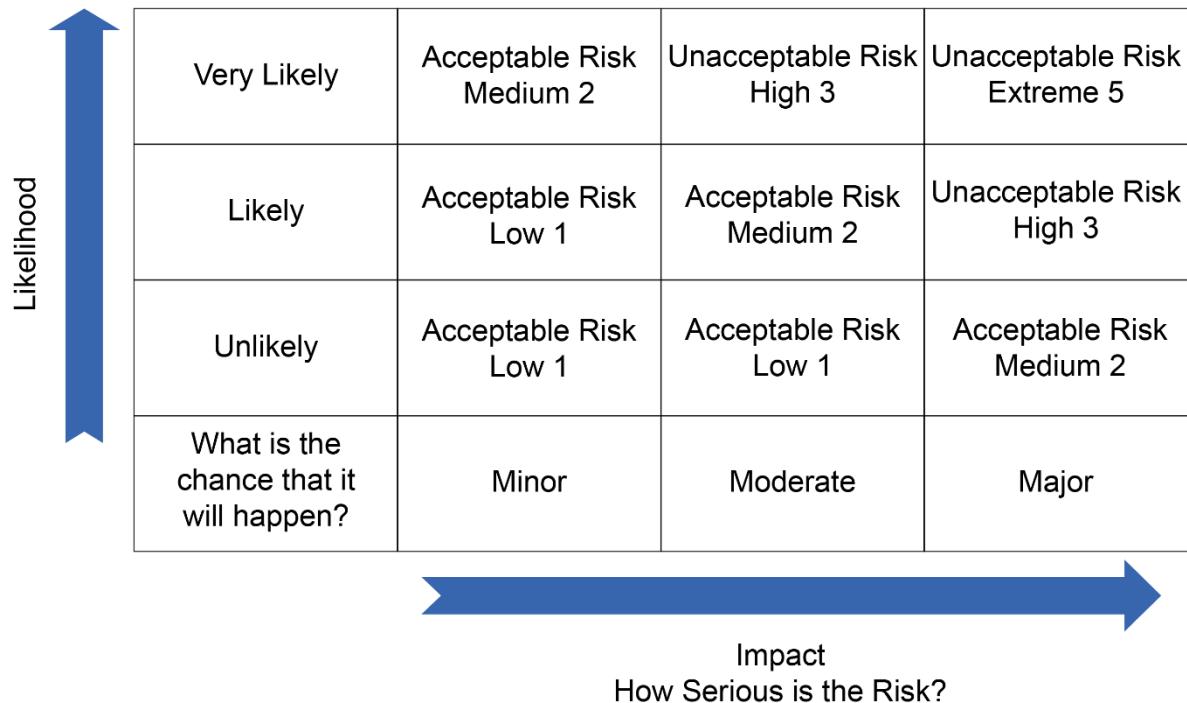


Figure 10.1: Risk assessment categorization

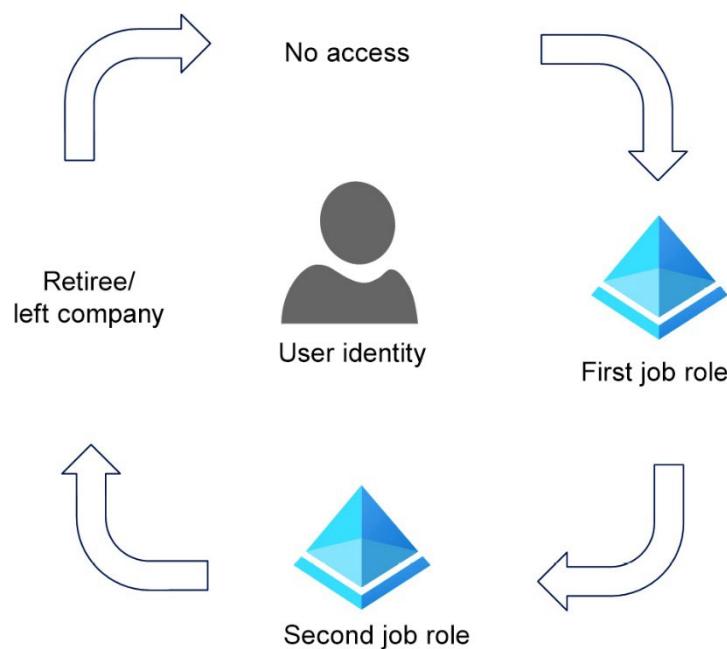


Figure 10.2: Identity governance life cycle

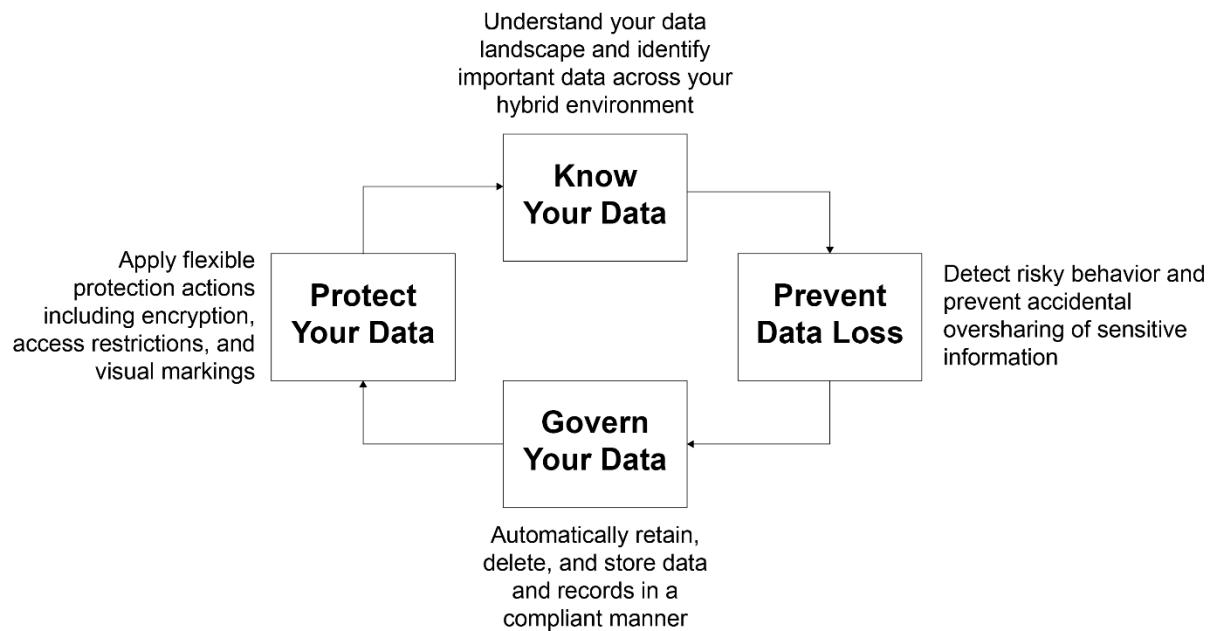


Figure 10.3: Zero-trust framework for data protection

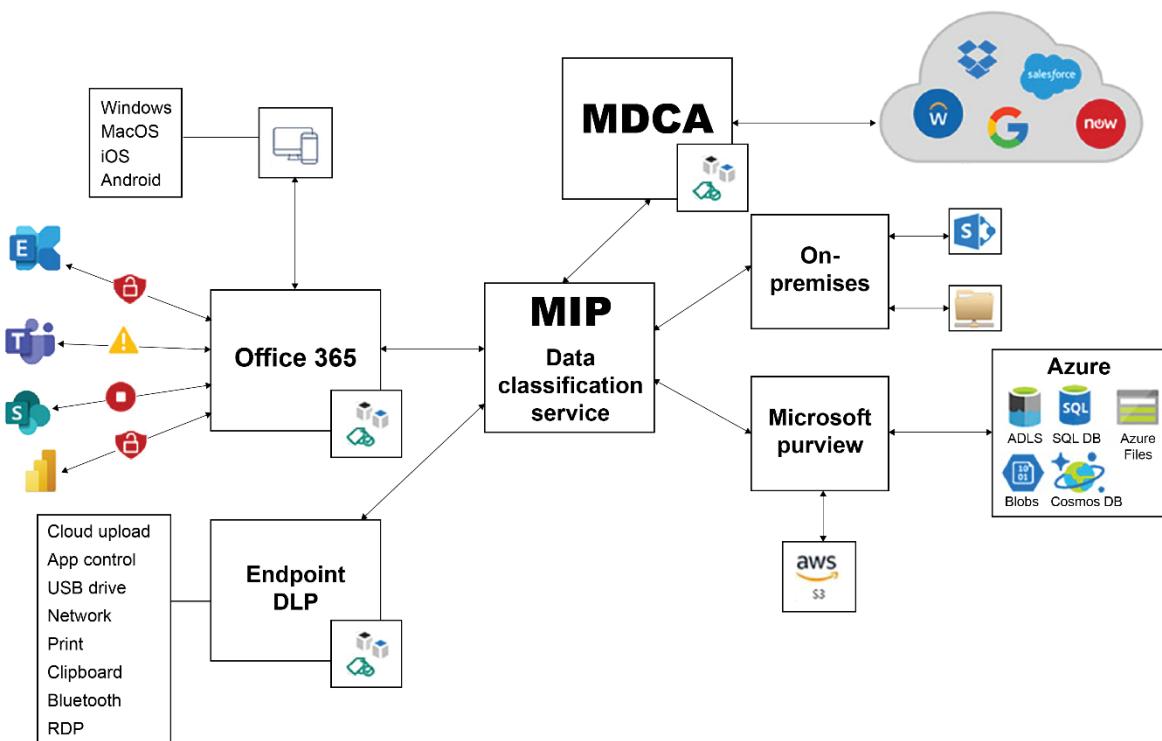


Figure 10.4: Microsoft Information Protection (MIP) workflow



Figure 10.5: Microsoft Defender for Cloud Apps workflow

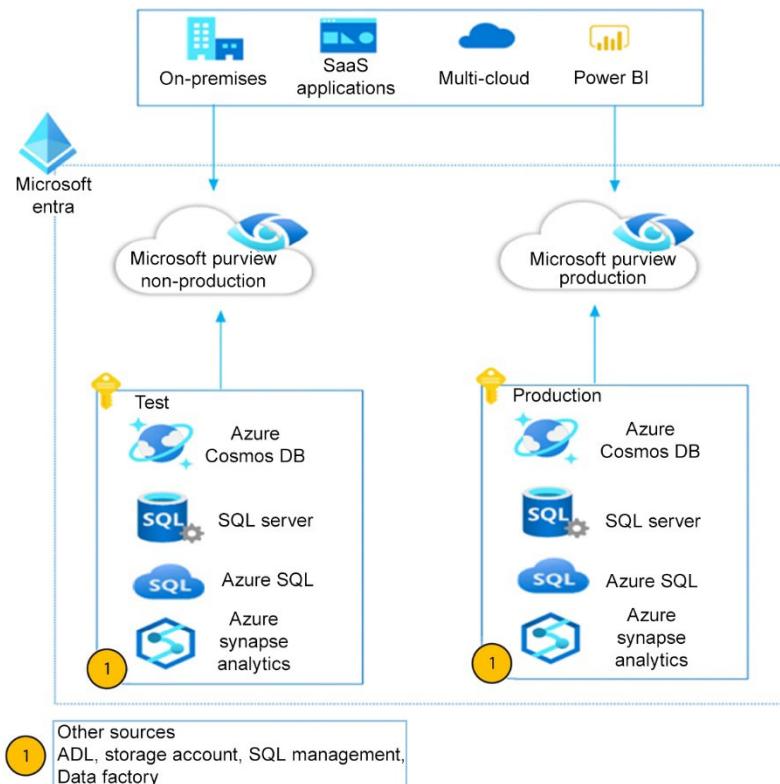


Figure 10.6: Database segmentation for production and non-production

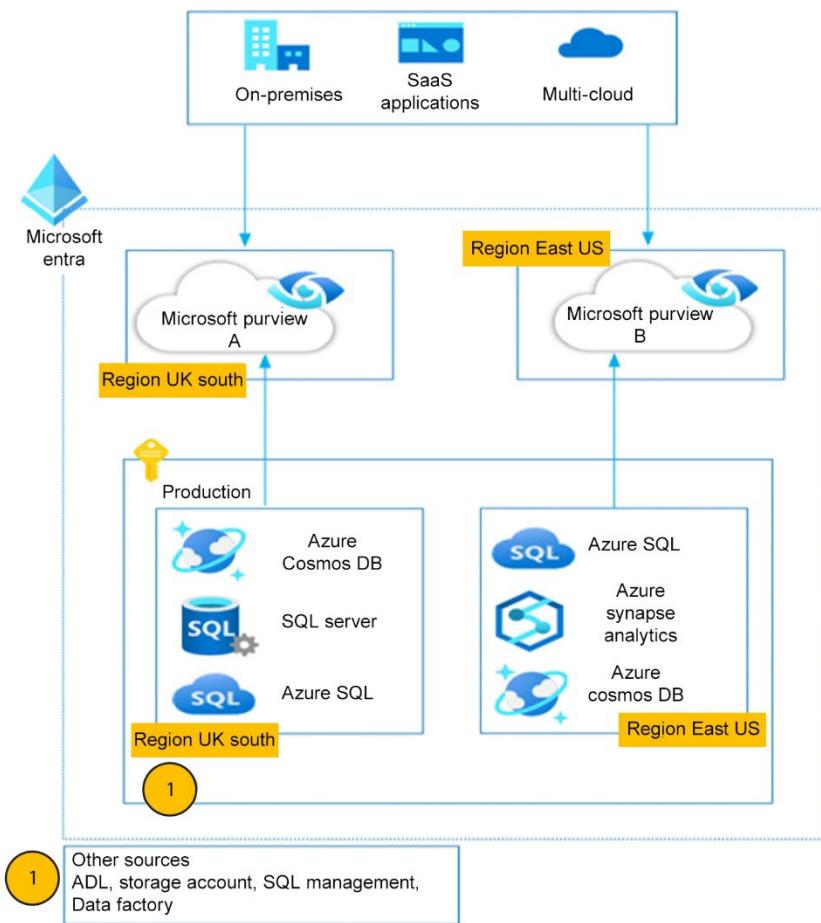


Figure 10.7: Using Microsoft Purview for data sovereignty

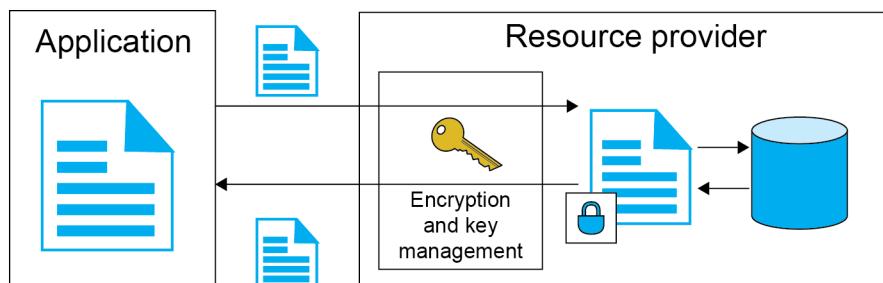
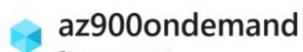


Figure 10.8: Accessing data encrypted at rest



Storage account

Search (Ctrl+ /)

Data migration

Events

Storage browser (preview)

Data storage

Containers

File shares

Queues

Tables

Security + networking

Networking

Azure CDN

Access keys

Shared access signature

Encryption

Security

Figure 10.9: Storage account access keys

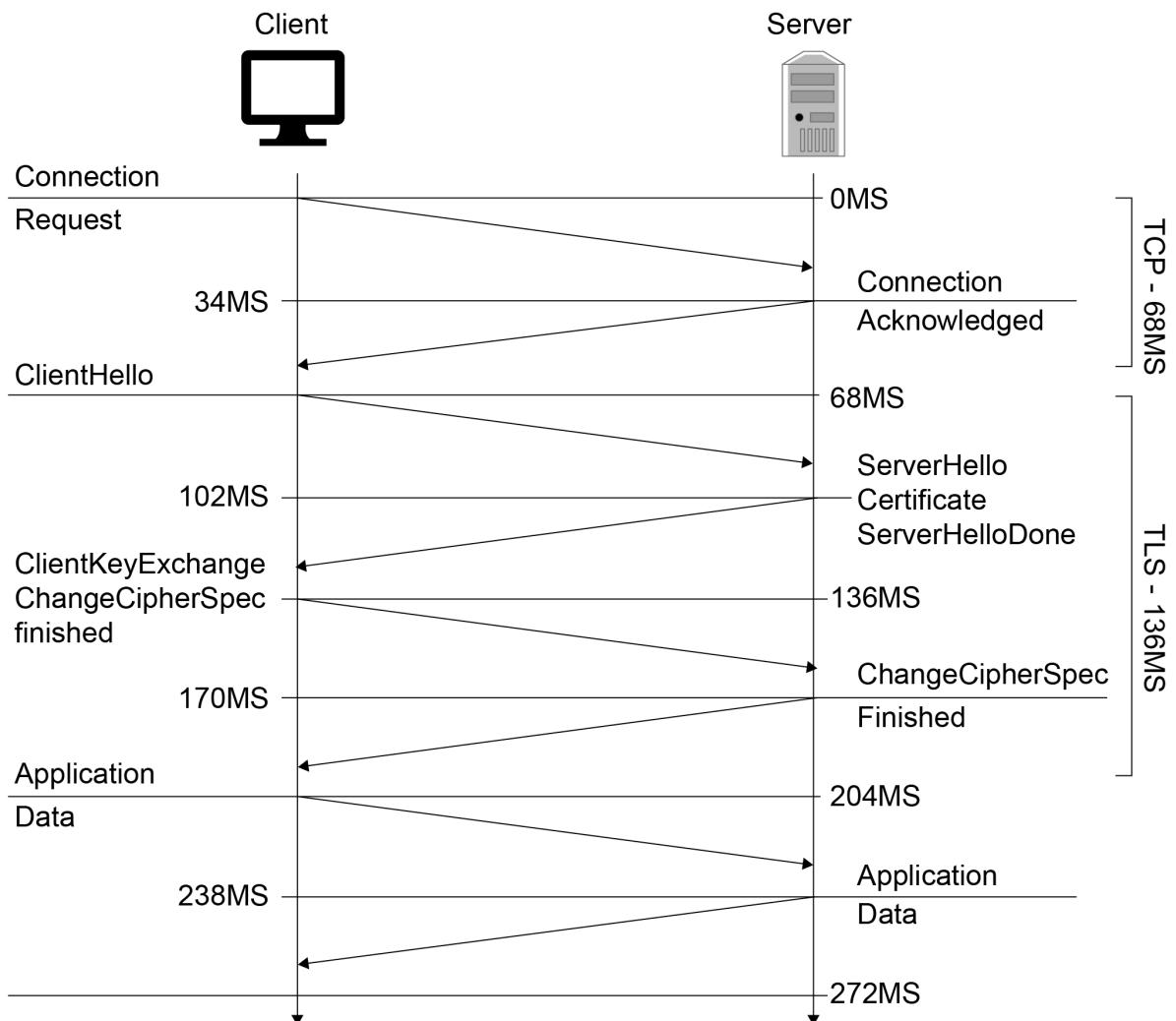


Figure 10.10: TLS 1.2 handshake process

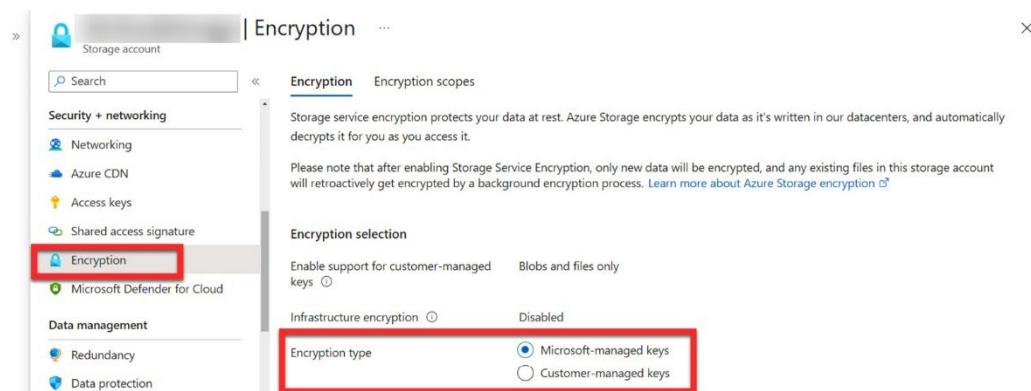


Figure 10.11: Configuring customer-managed keys with Azure Key Vault

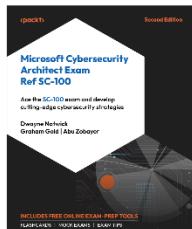
Chapter 11: Accessing the Online Practice Resources

cp Practice Resources

REPORT ISSUE

UNLOCK YOUR PRACTICE RESOURCES

You're about to unlock the free online content that came with your book. Make sure you have your book with you before you start, so that you can access the resources in minutes.



Microsoft Cybersecurity Architect Exam Ref SC-100

Book ISBN: 9781836208518

Dwayne Natwick • Graham Gold • Abu Zobayer • Oct 2024 • 500 pages

Do you have a Packt account?

Yes, I have an existing Packt account No, I don't have a Packt account

PROCEED

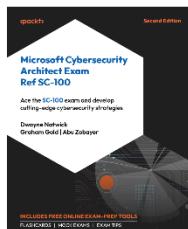
Figure 11.2: Unlock page for the online practice resources

cp Practice Resources

REPORT ISSUE

UNLOCK YOUR PRACTICE RESOURCES

You're about to unlock the free online content that came with your book. Make sure you have your book with you before you start, so that you can access the resources in minutes.



Microsoft Cybersecurity Architect Exam Ref SC-100

Book ISBN: 9781836208518

Dwayne Natwick • Graham Gold • Abu Zobayer • Oct 2024 • 500 pages

ENTER YOUR PURCHASE DETAILS

Enter Unique Code *

[Where To Find This?](#)

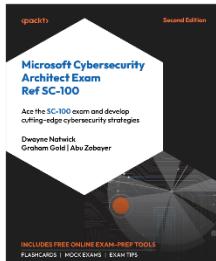
Check this box to receive emails from us about new features and promotions on our other certification books. You can opt out anytime.

REQUEST ACCESS

Figure 11.3: Enter your unique sign-up code to unlock the resources

PACKT PRACTICE RESOURCES

You've just unlocked the free online content that came with your book.



Microsoft Cybersecurity Architect Exam Ref SC-100

 Book ISBN: 9781836208518

Dwayne Natwick • Graham Gold • Abu Zobayer • Oct 2024 • 500 pages

 **Unlock Successful**

Click the following link to access your practice resources at any time.

Pro Tip: You can switch seamlessly between the ebook version of the book and the practice resources. You'll find the ebook version of this title in your [Owned Content](#)

[OPEN PRACTICE RESOURCES](#) 

Figure 11.4: Page that shows up after a successful unlock

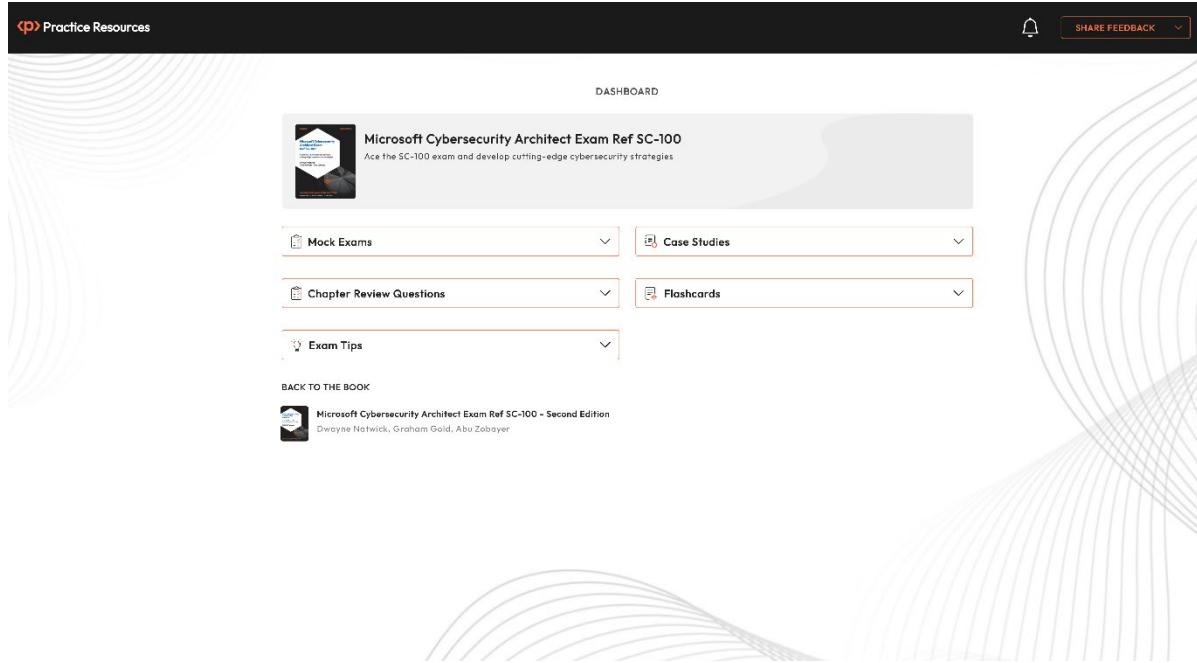


Figure 11.5: Dashboard page for SC-100 practice resources

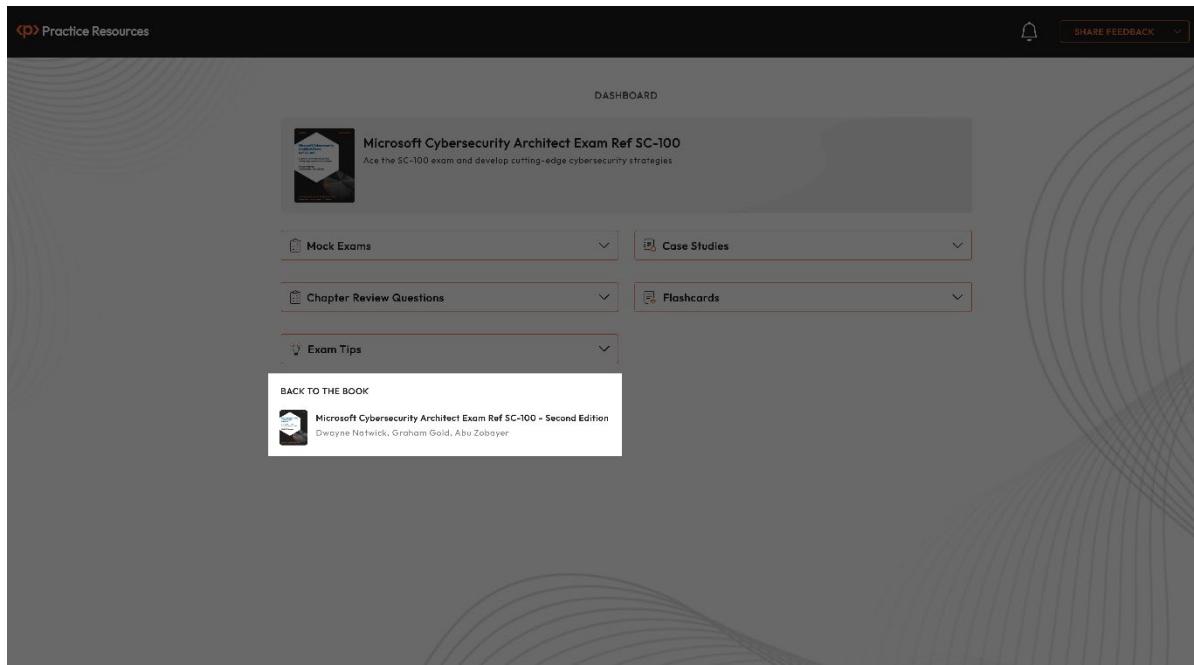


Figure 11.7: Dashboard page for SC-100 practice resources