Microsoft Cybersecurity Architect Exam Ref SC-100, Second Edition

Preface:

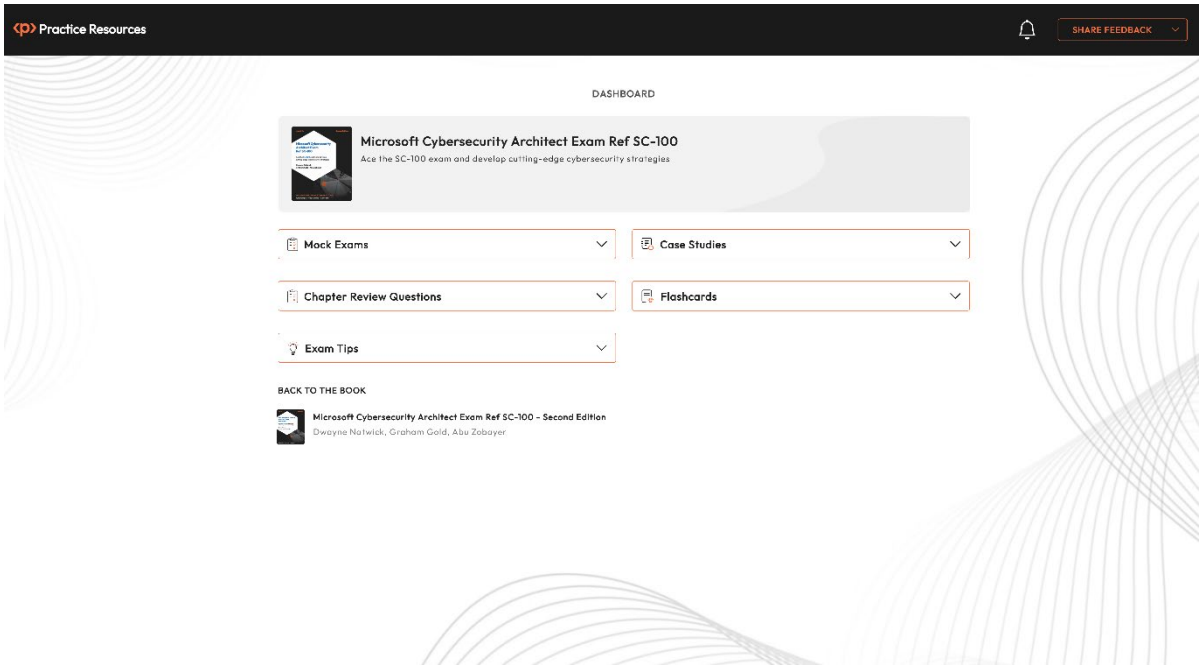


Figure 0.1 – Online exam-prep platform on a desktop device

Chapter 1: Cybersecurity in the Cloud

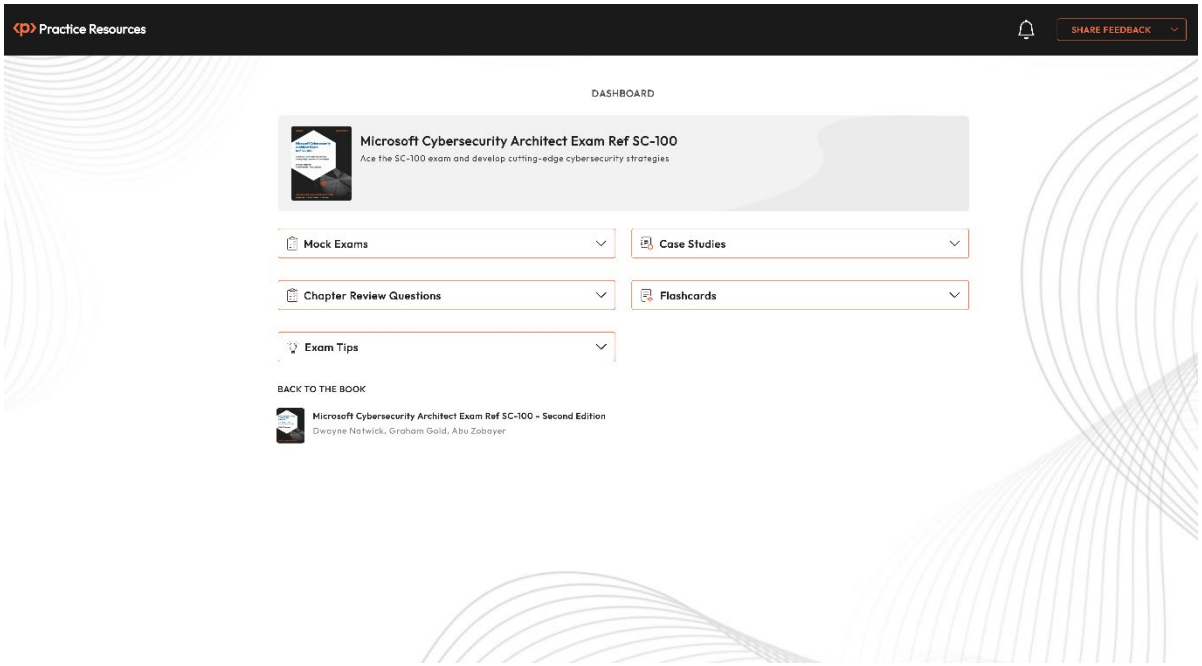
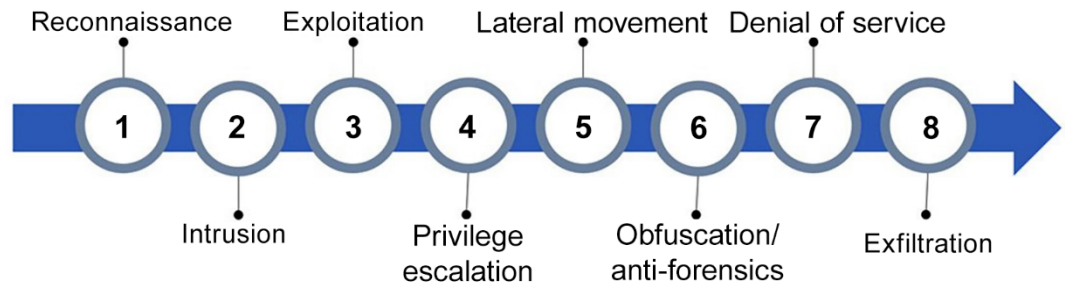


Figure 1.1: Dashboard interface of the online practice resources



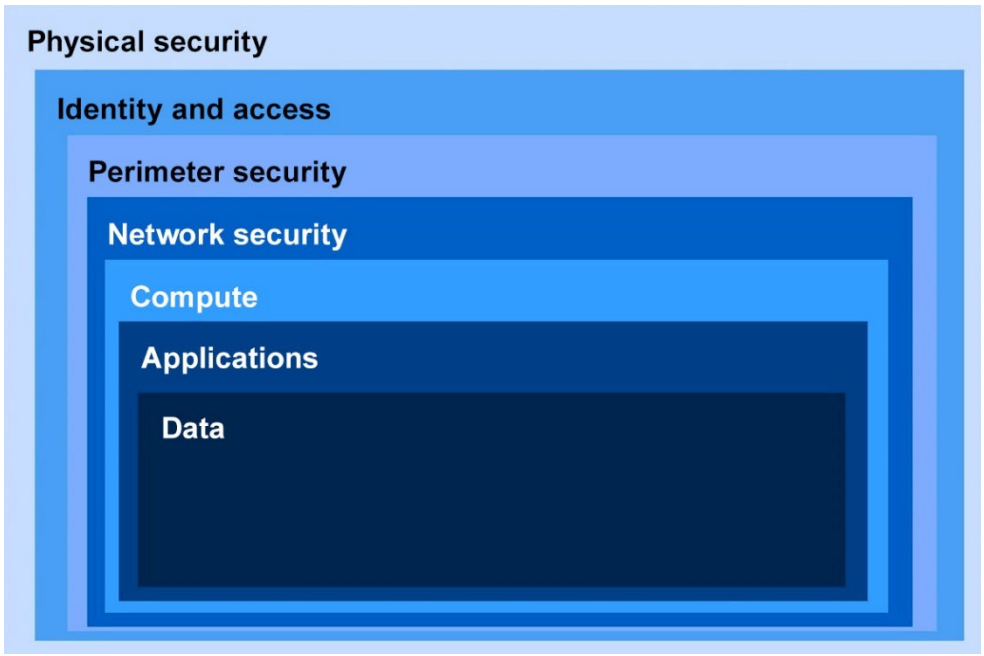


Figure 1.2: Logical layers of defense-in-depth posture/infrastructure

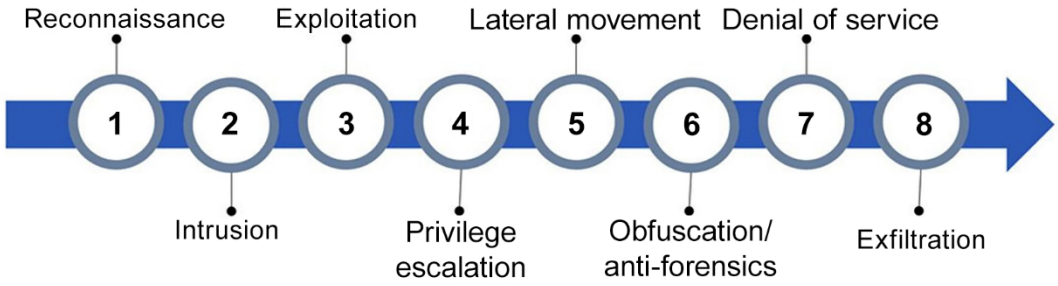


Figure 1.3: Stages of the Cyber Kill Chain

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

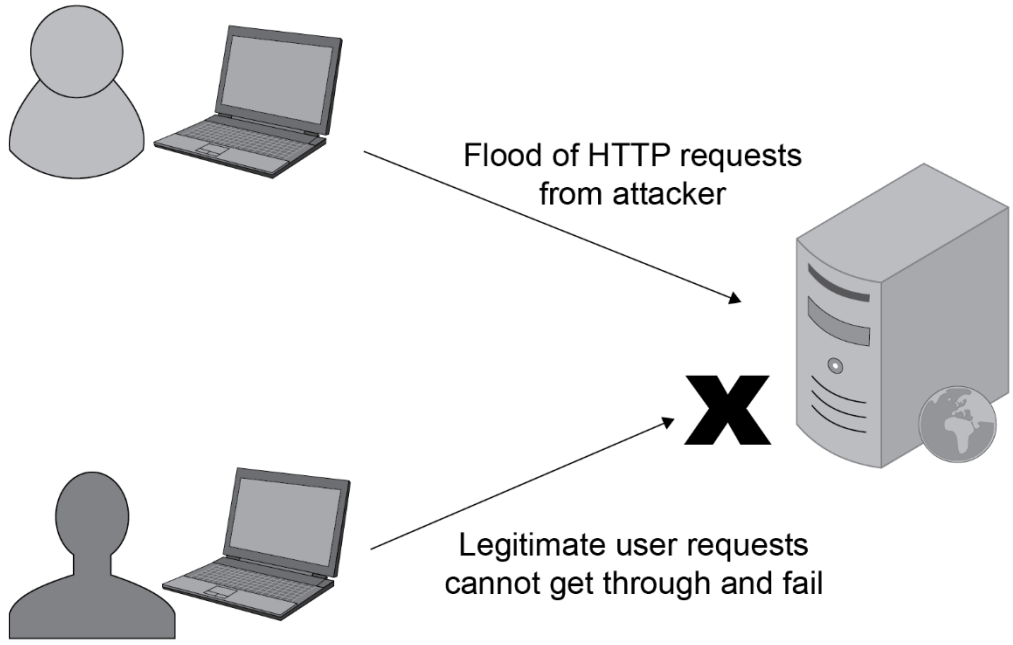


Figure 1.6: Illustration of a denial-of-service attack

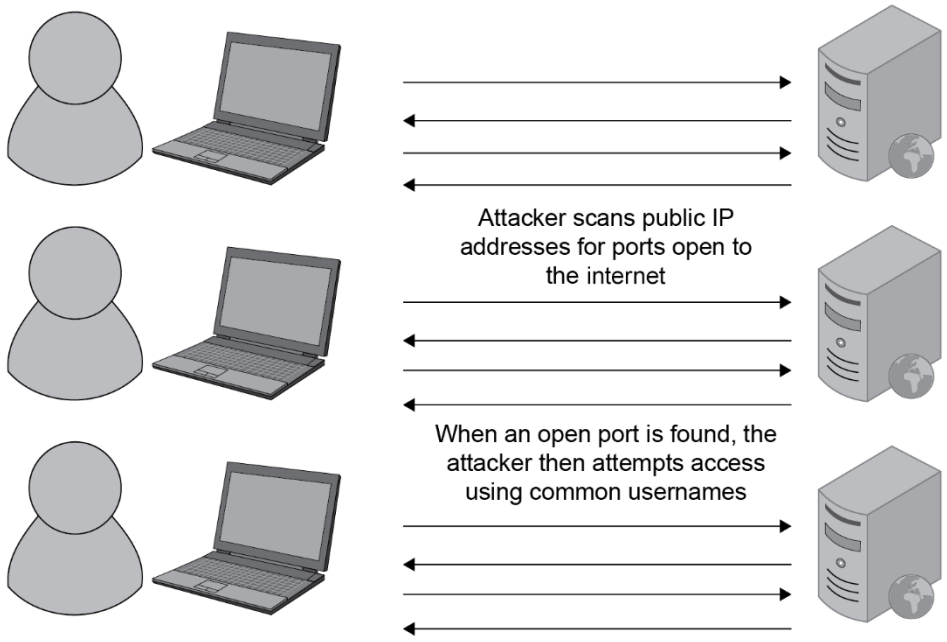


Figure 1.7: An attacker scanning public IP addresses for open ports, then attempting to gain access using common usernames once an open port is found

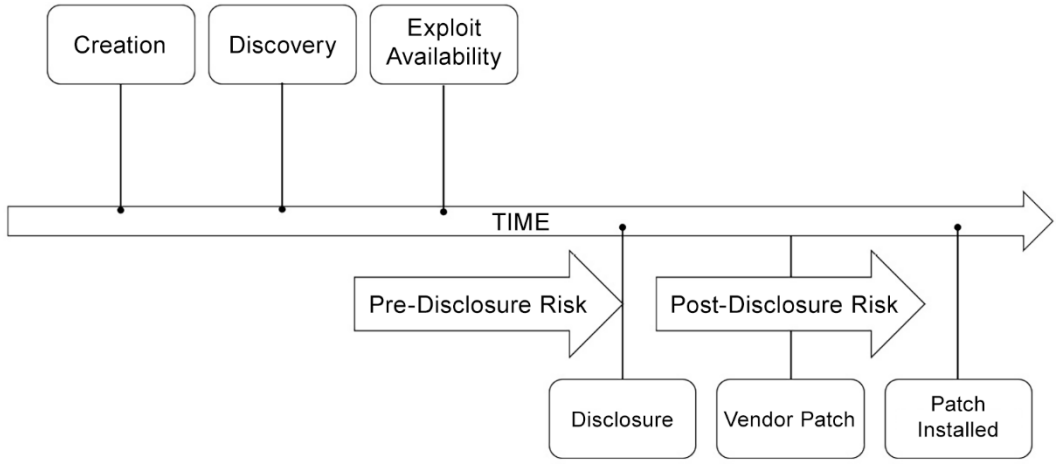


Figure 1.8: The vulnerability management life cycle

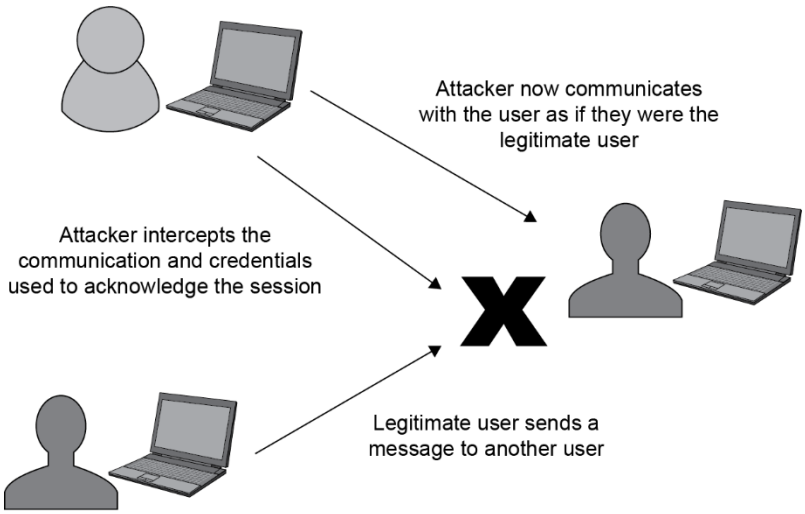


Figure 1.9: Attacker-in-the-Middle (AiTM) attack: Attacker intercepts and impersonates users in a communication

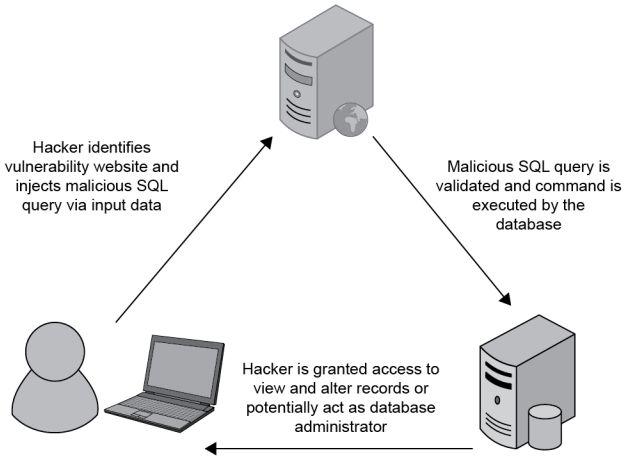


Figure 1.10: SQL injection attack: Hacker injects malicious SQL to access and manipulate database records

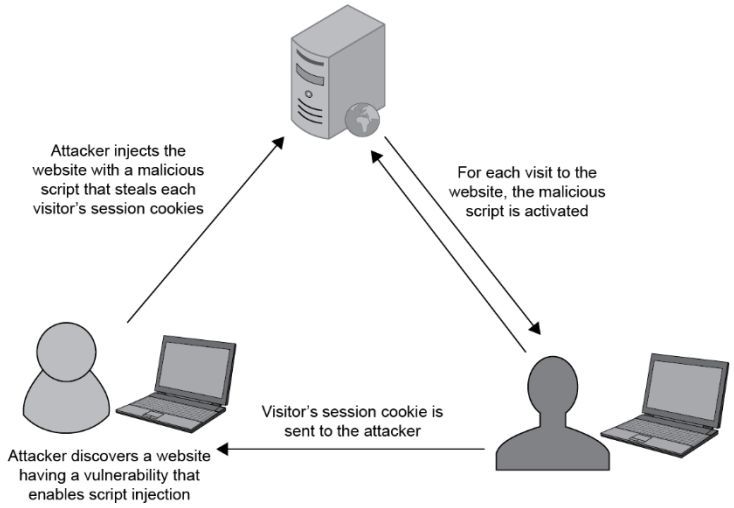


Figure 1.11: Cross-site scripting (XSS) attack: An attacker injects a malicious script into a vulnerable website to steal visitors' session cookies

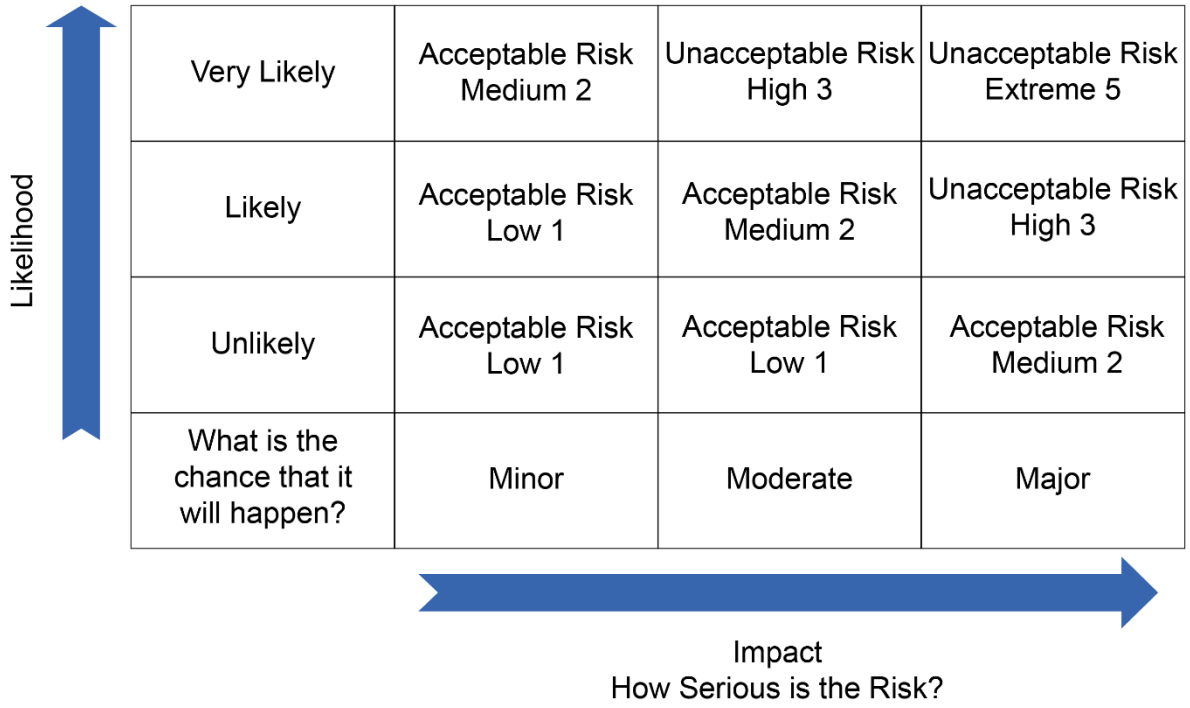


Figure 1.12: Security risk matrix visualized

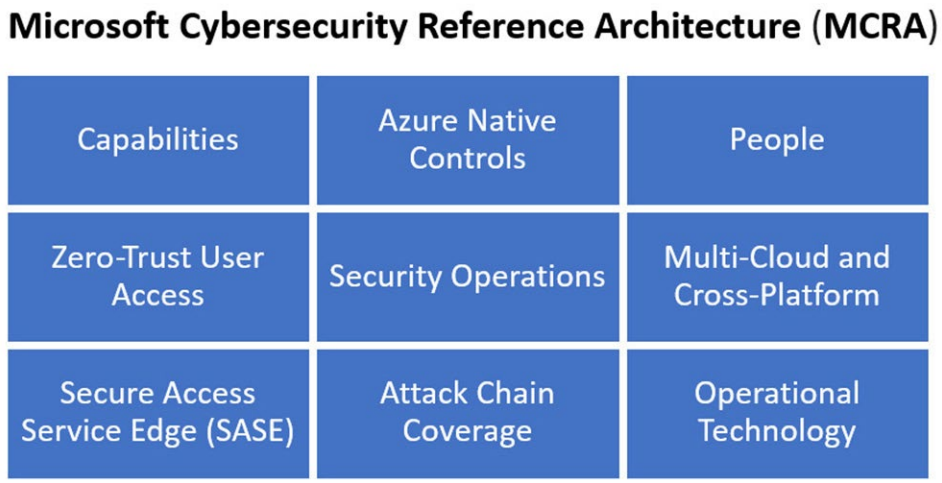


Figure 2.1 – MCRA topics

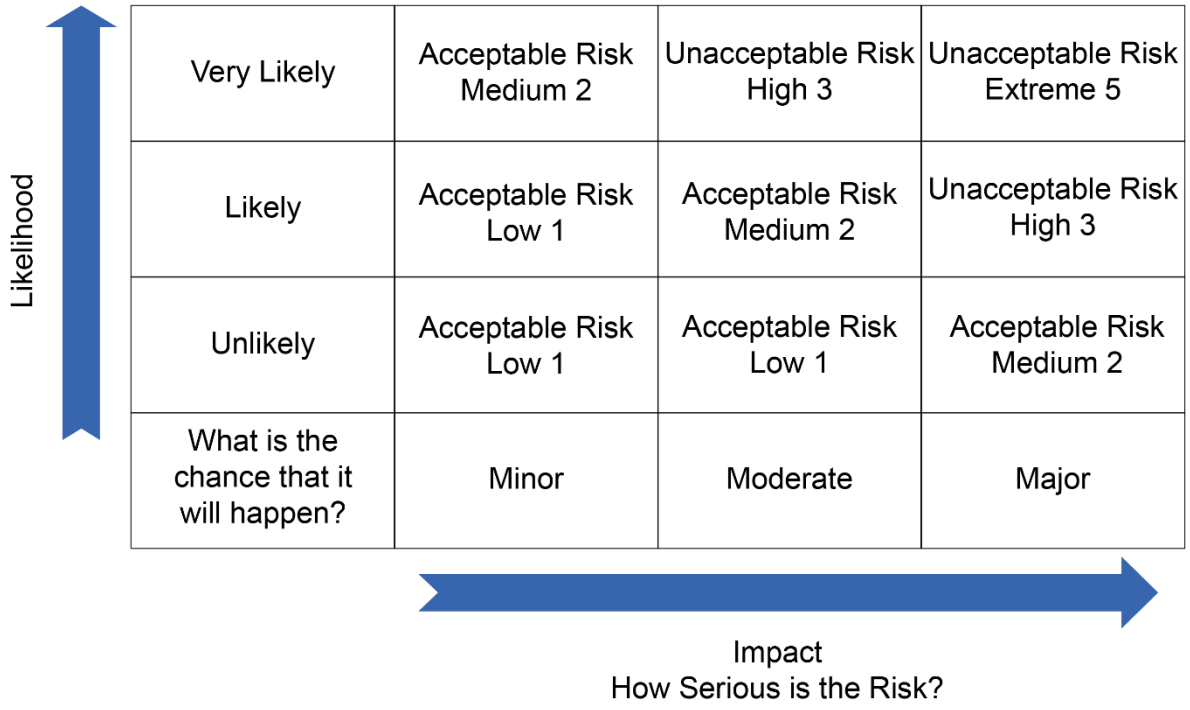


Figure 2.2 – Risk assessment matrix

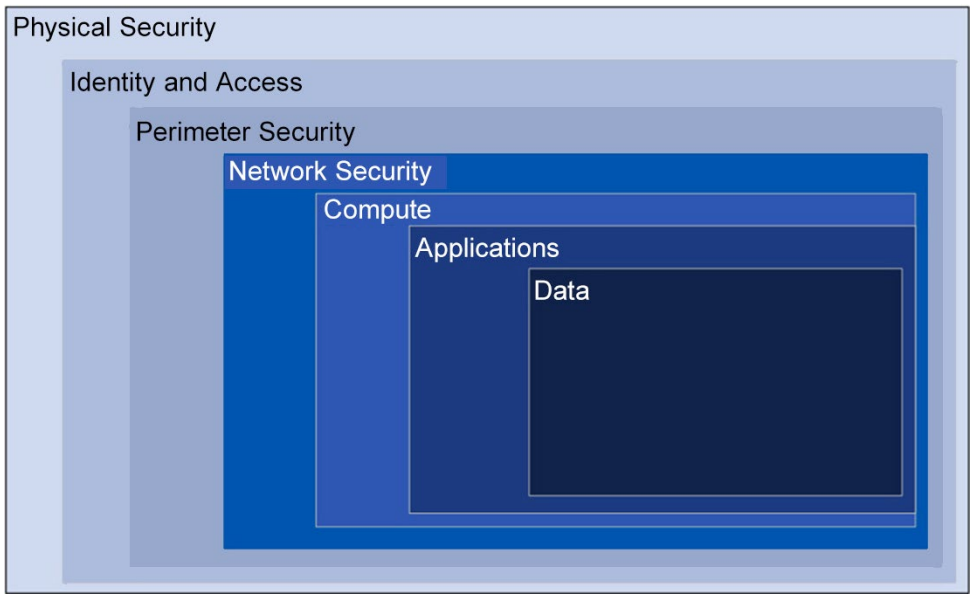


Figure 2.3 – Defense-in-depth security diagram

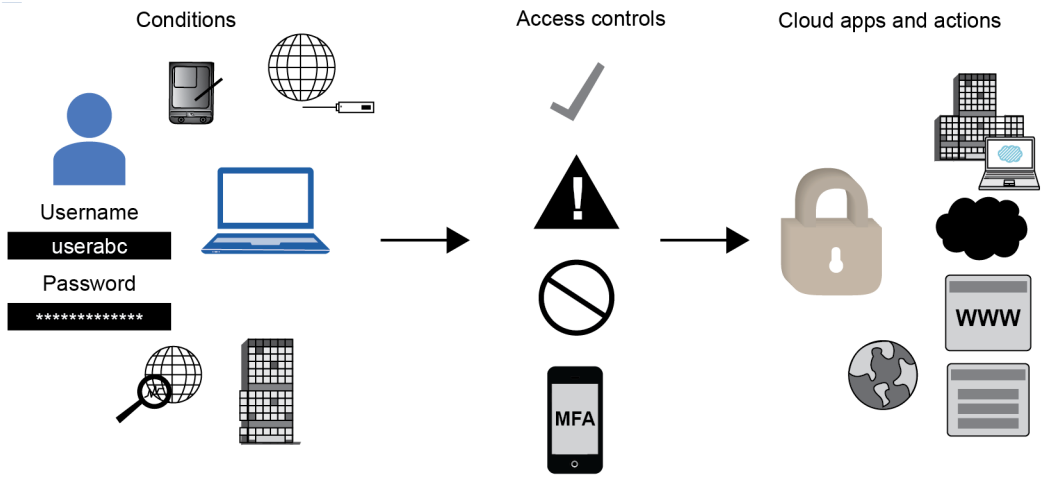


Figure 2.4 – Zero trust with Conditional Access

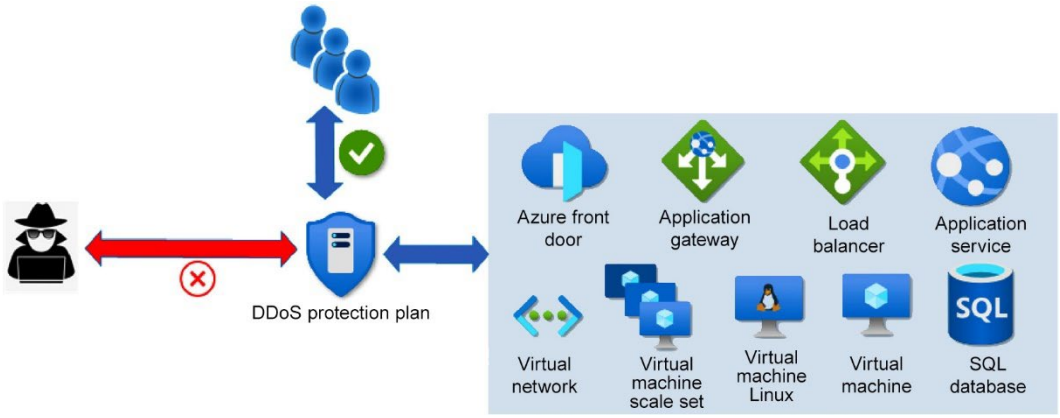


Figure 2.5 – Azure DDoS Protection

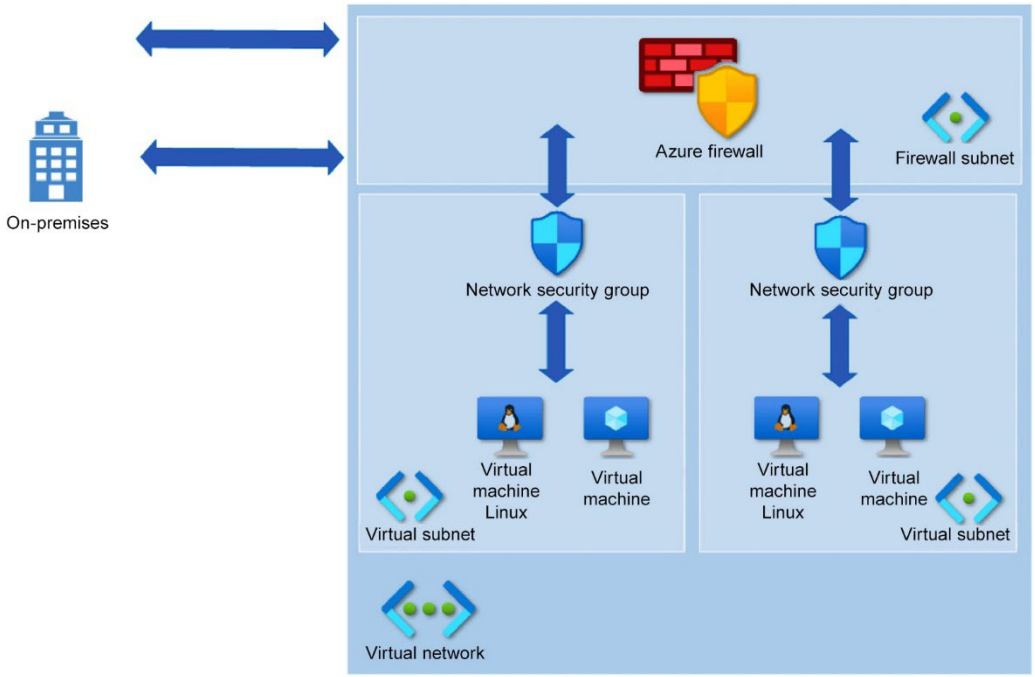


Figure 2.6 – Azure Firewall

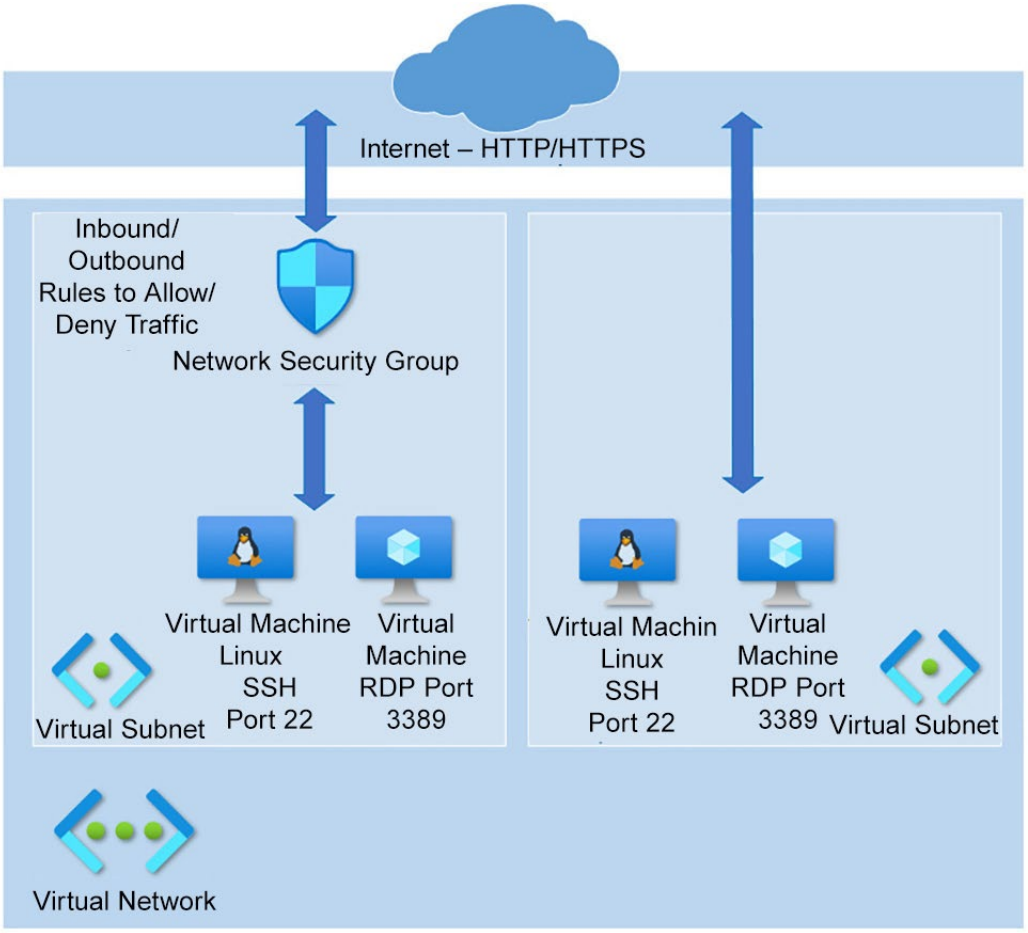


Figure 2.7 – Network security groups for network perimeter protection

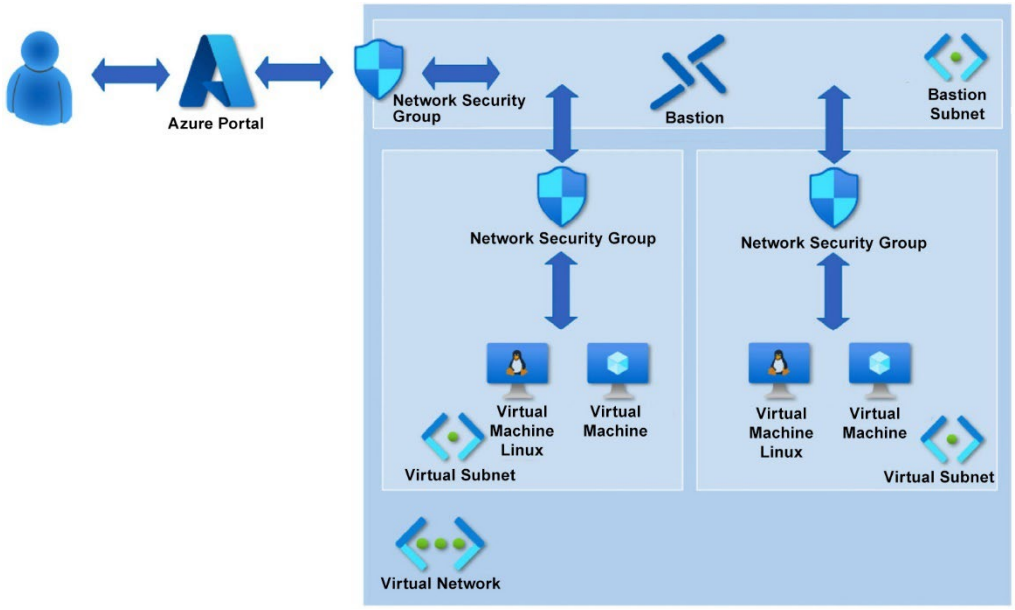


Figure 2.8 – Azure Bastion for virtual machine remote management

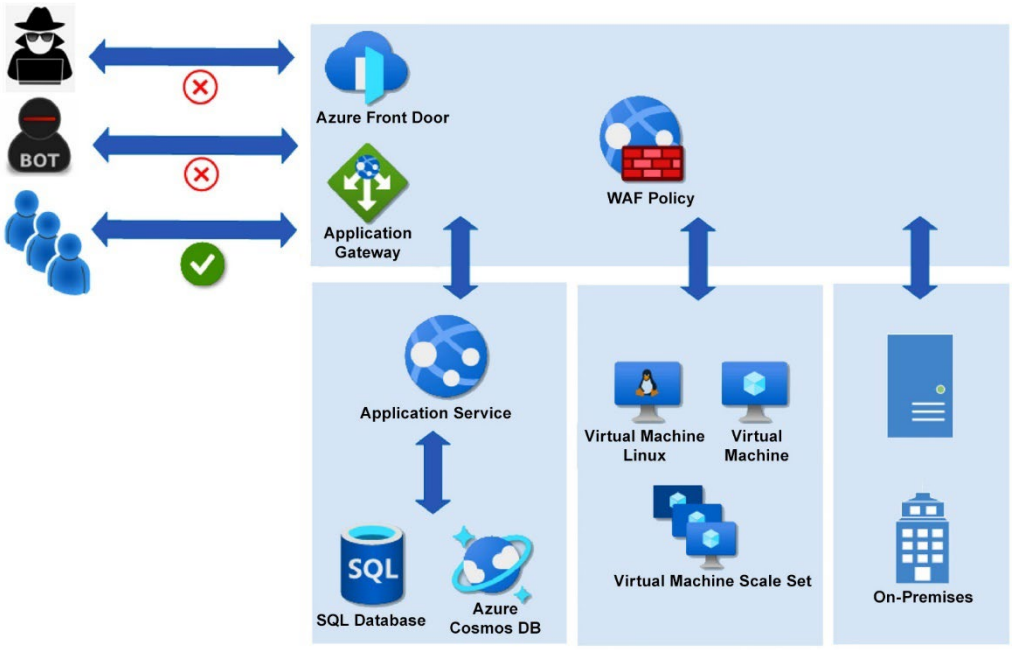


Figure 2.9 – WAF diagram

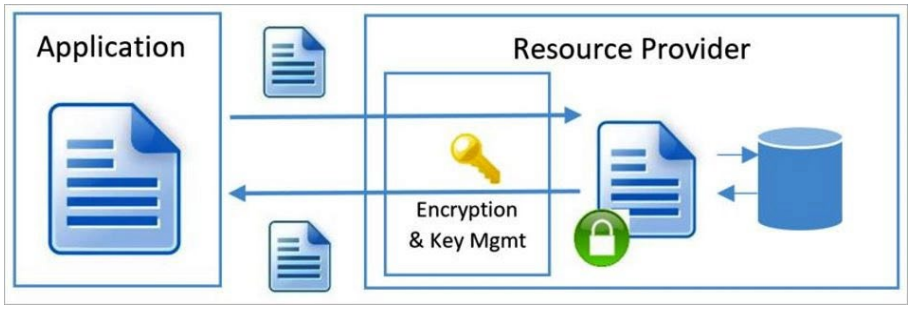


Figure 2.10 – Data encrypted at rest

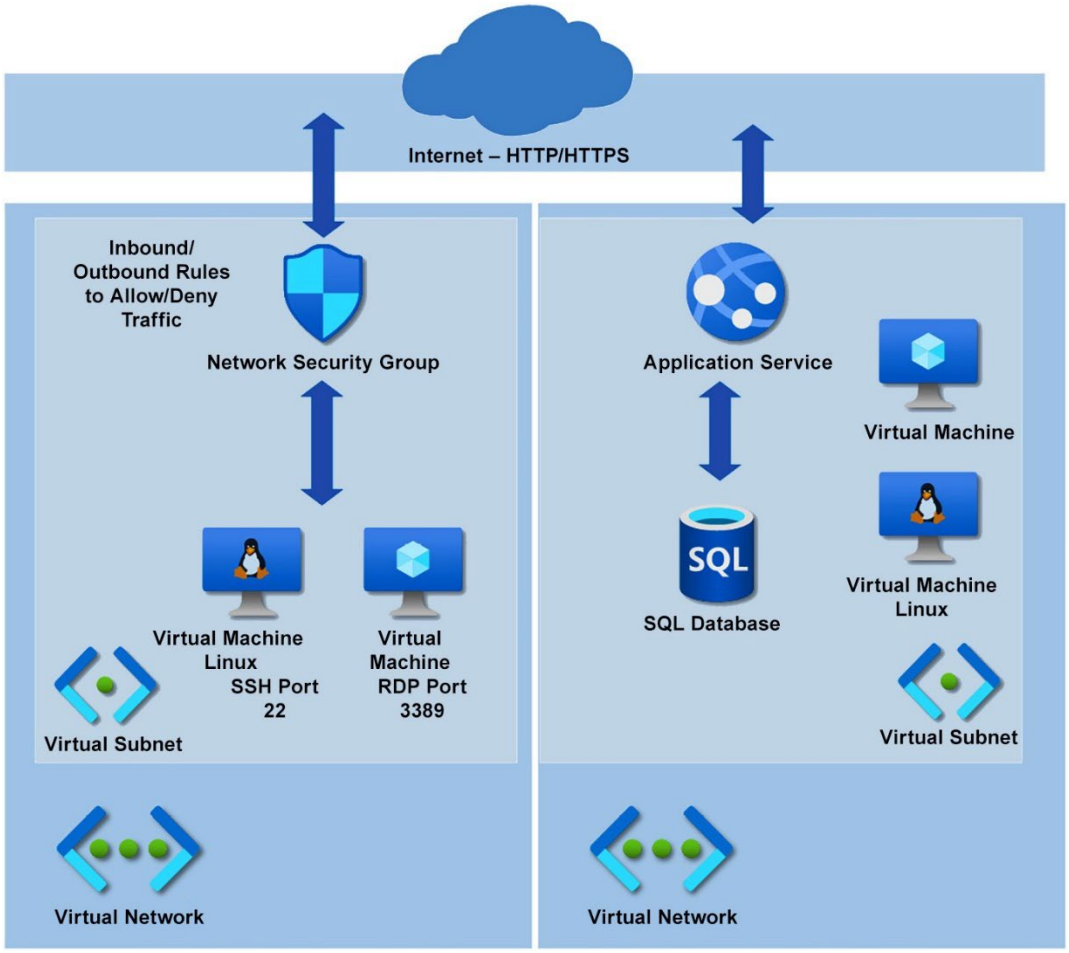


Figure 2.11 – Network segmentation

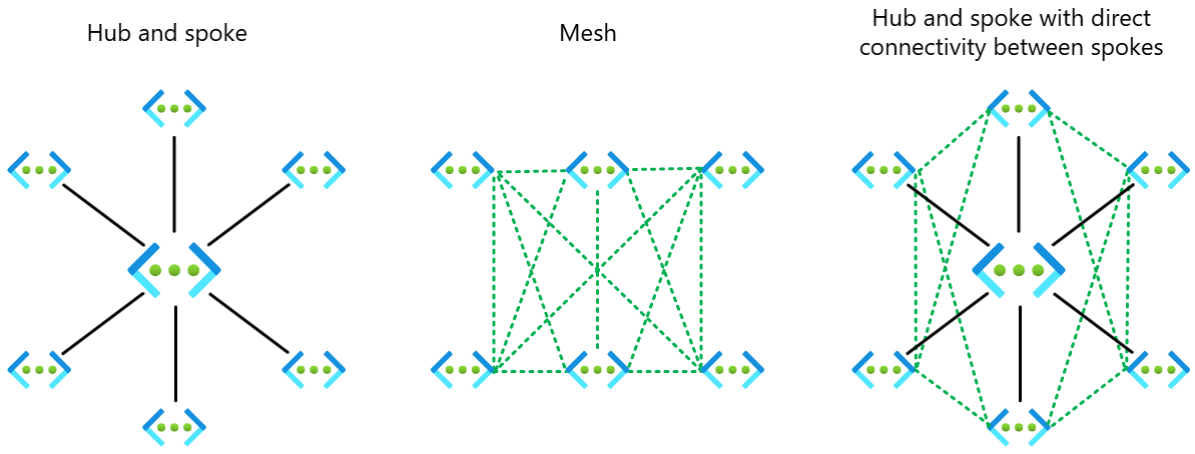


Figure 2.12 – Network topologies

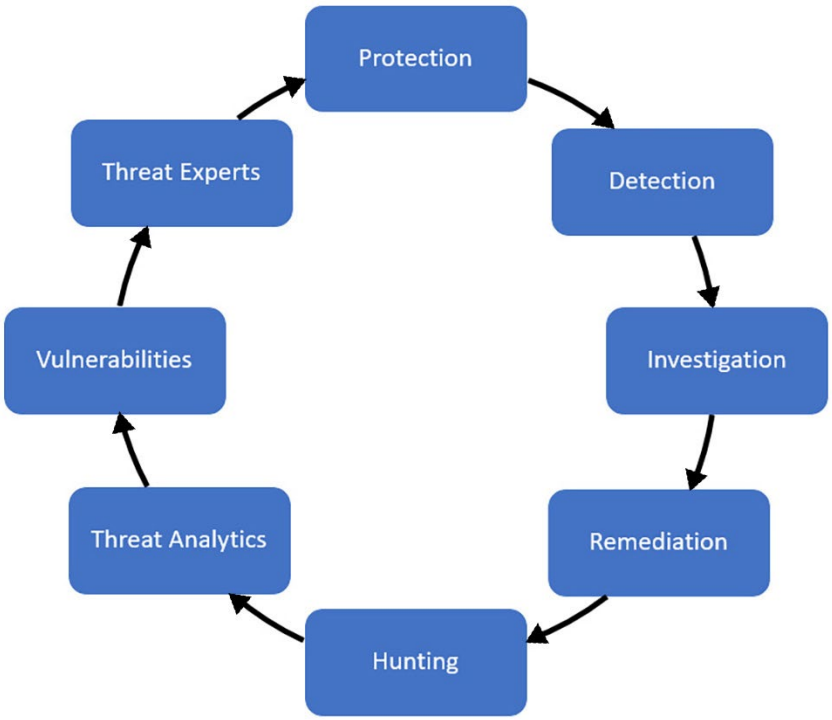


Figure 3.1 – A security operations strategy to manage threats

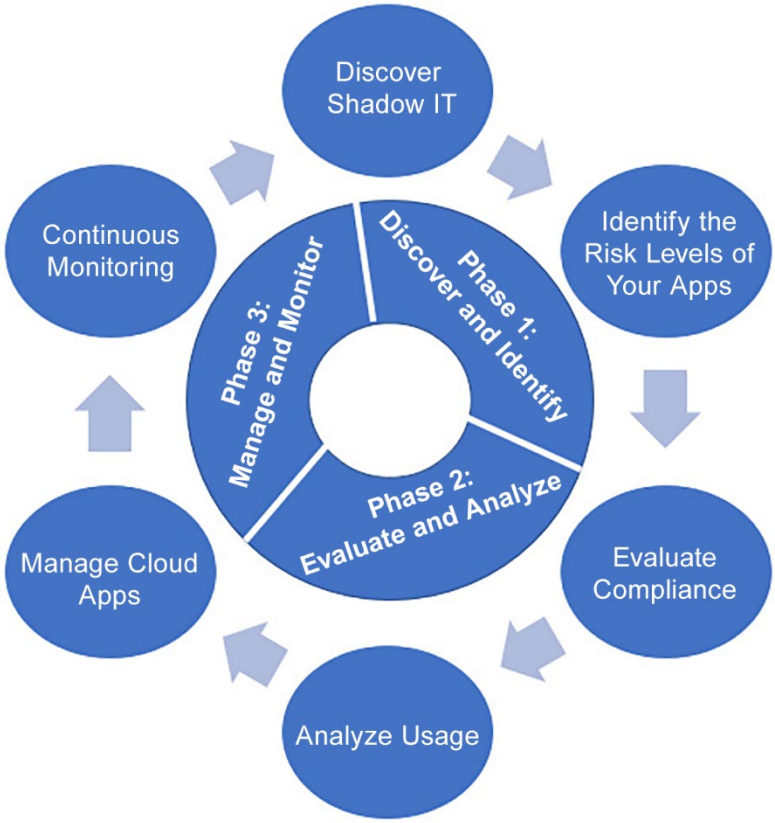


Figure 3.2 – Microsoft Defender for Cloud Apps' shadow IT protection

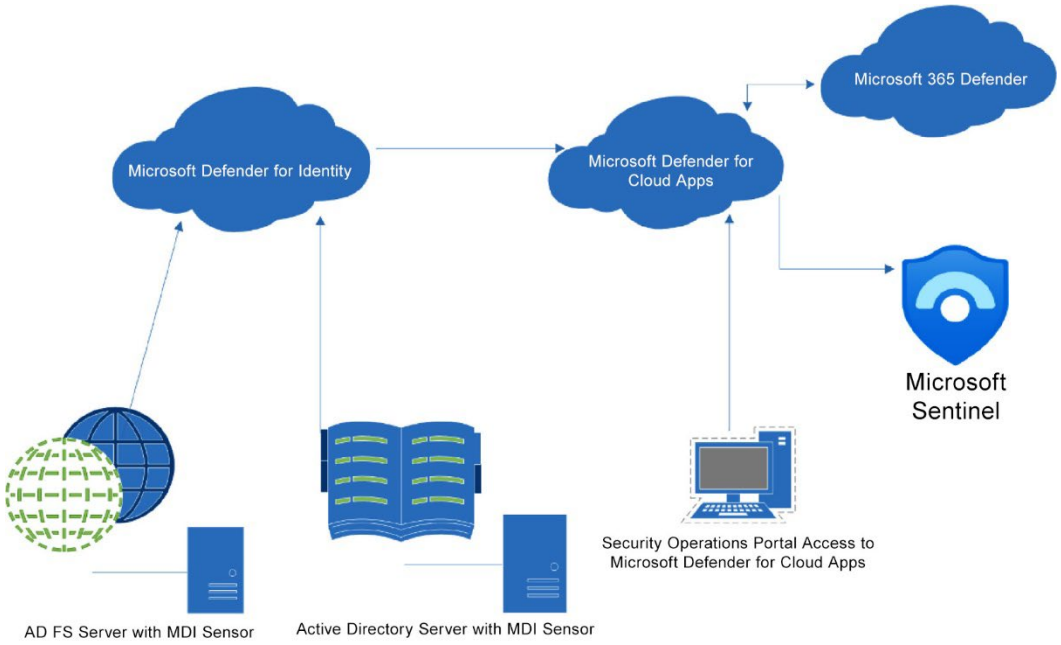


Figure 3.3 – MDI

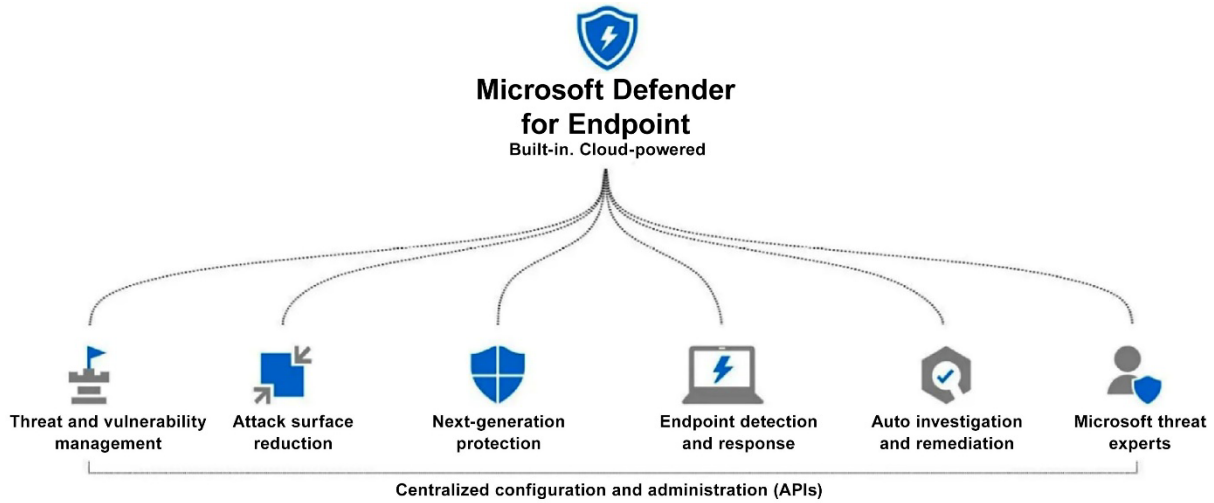


Figure 3.4 – Microsoft Defender for Endpoint

Figure 3.5 – Microsoft Defender for Office 365

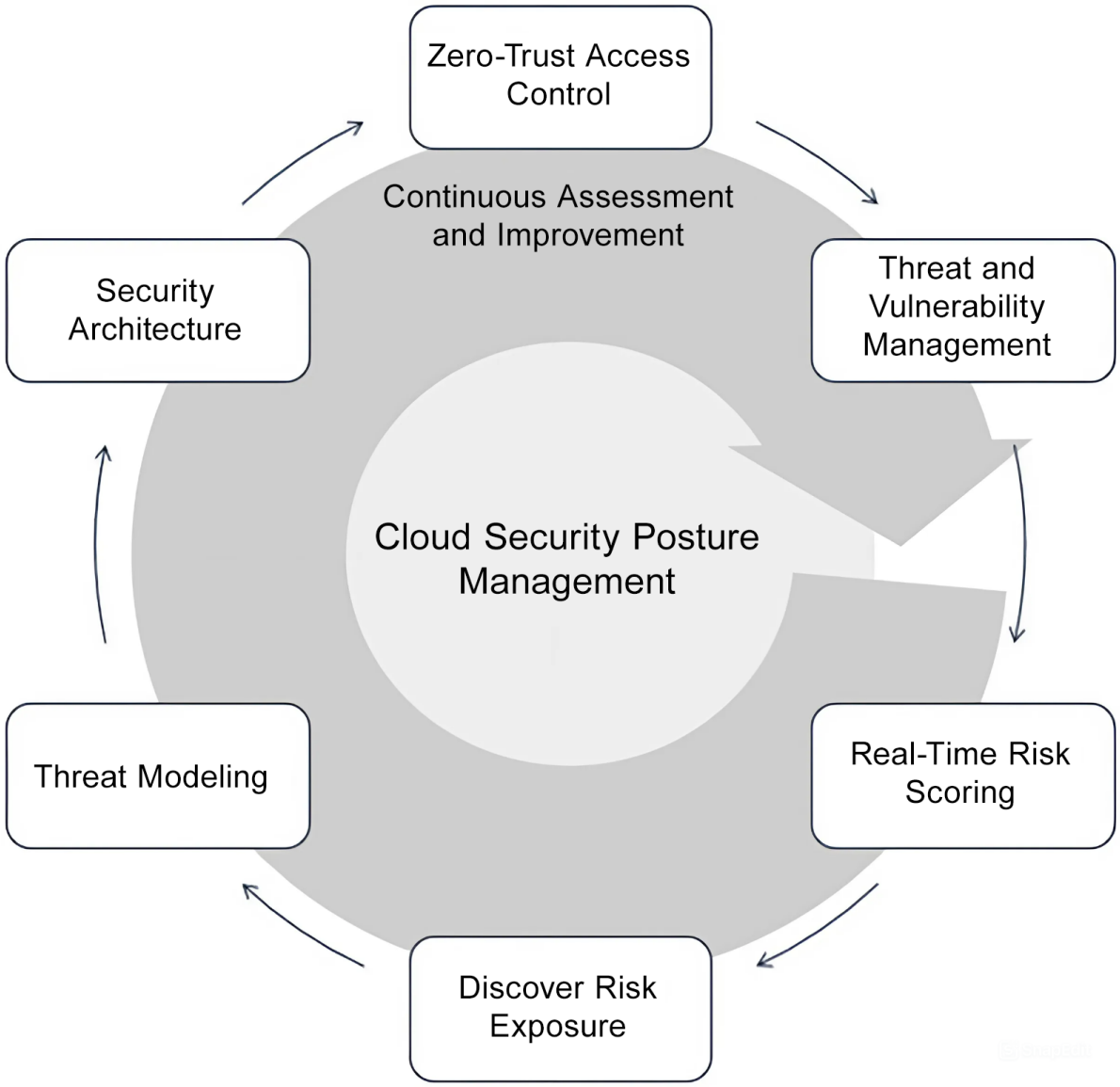


Figure 3.6 – Microsoft Defender for Cloud security posture management

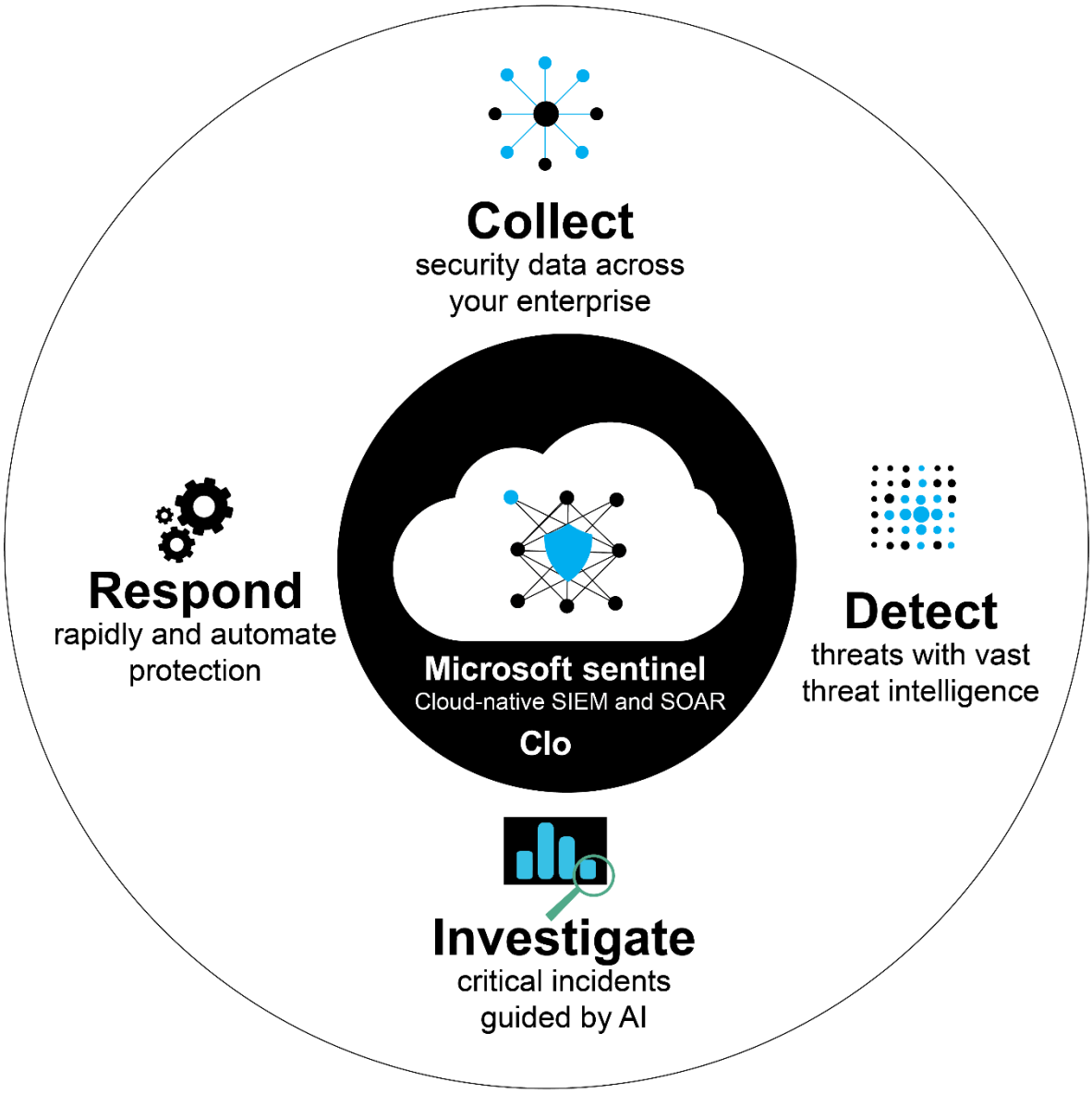


Figure 3.7 – Microsoft Sentinel SIEM and SOAR

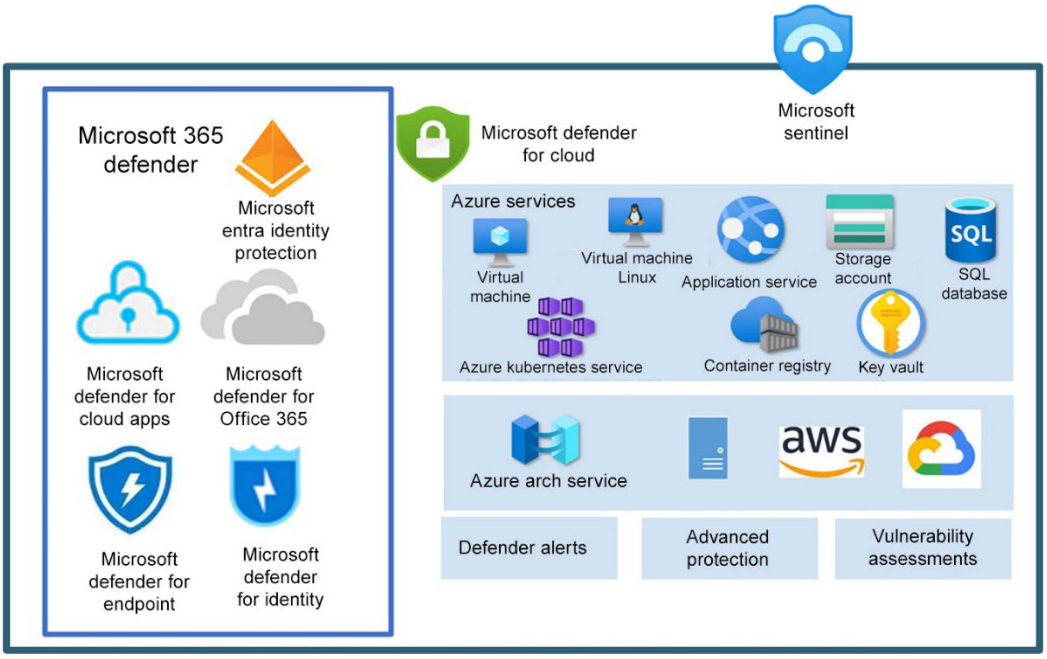


Figure 3.8 – Microsoft Defender for Office 365 and Microsoft Sentinel

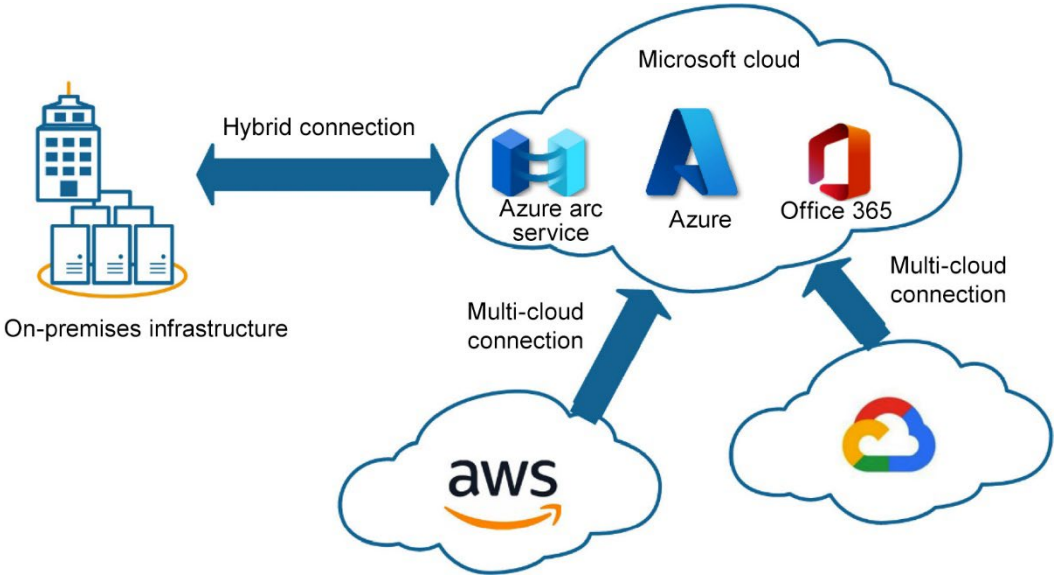


Figure 3.9 – Hybrid and multi-cloud architecture

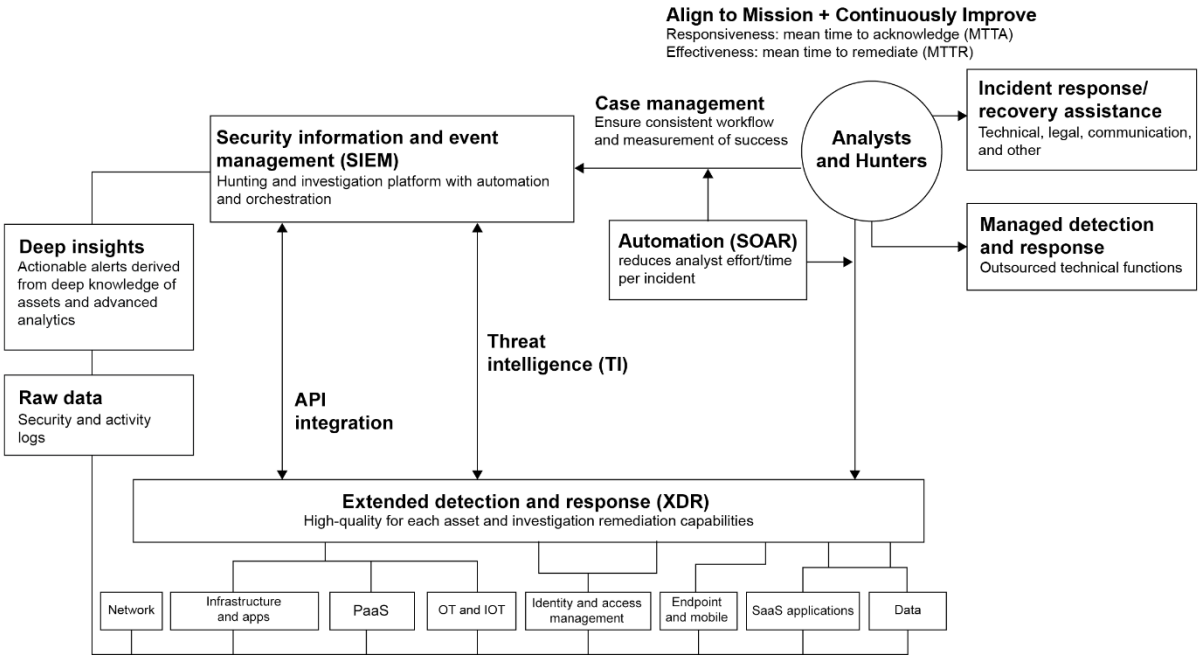


Figure 3.10 – Security operations technology usage

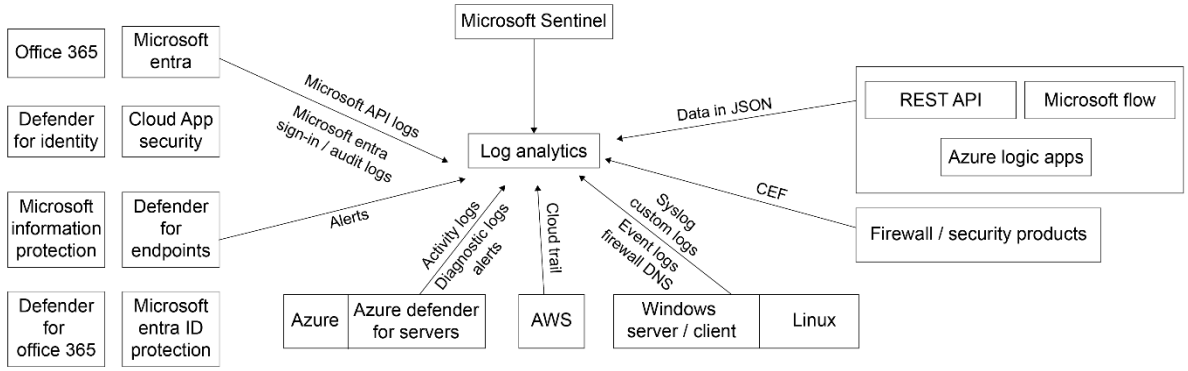


Figure 3.11 – Microsoft Sentinel architecture

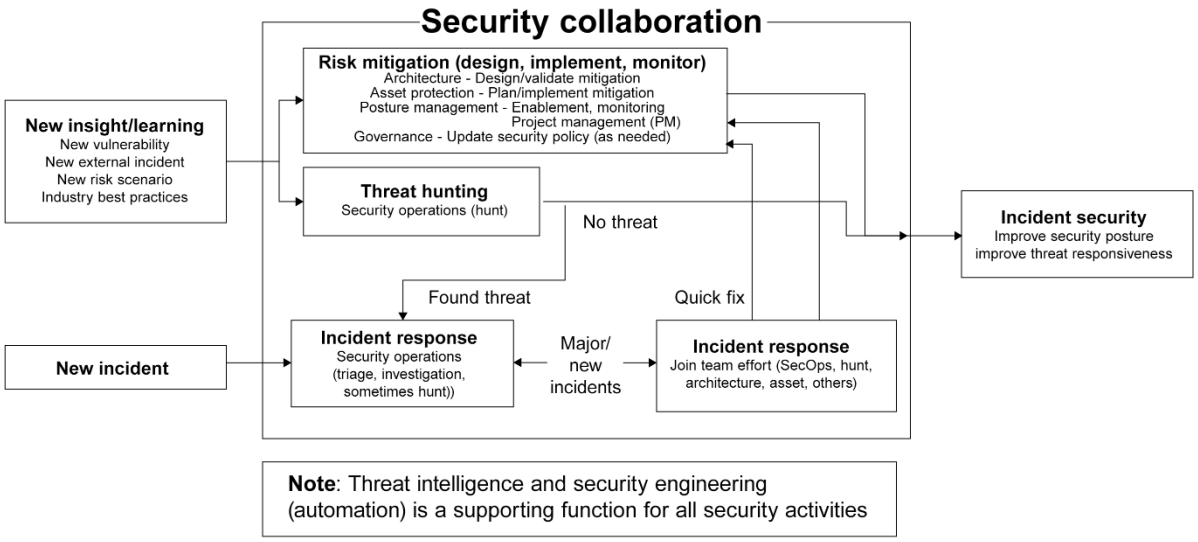


Figure 3.12 – The security operations continuous improvement process

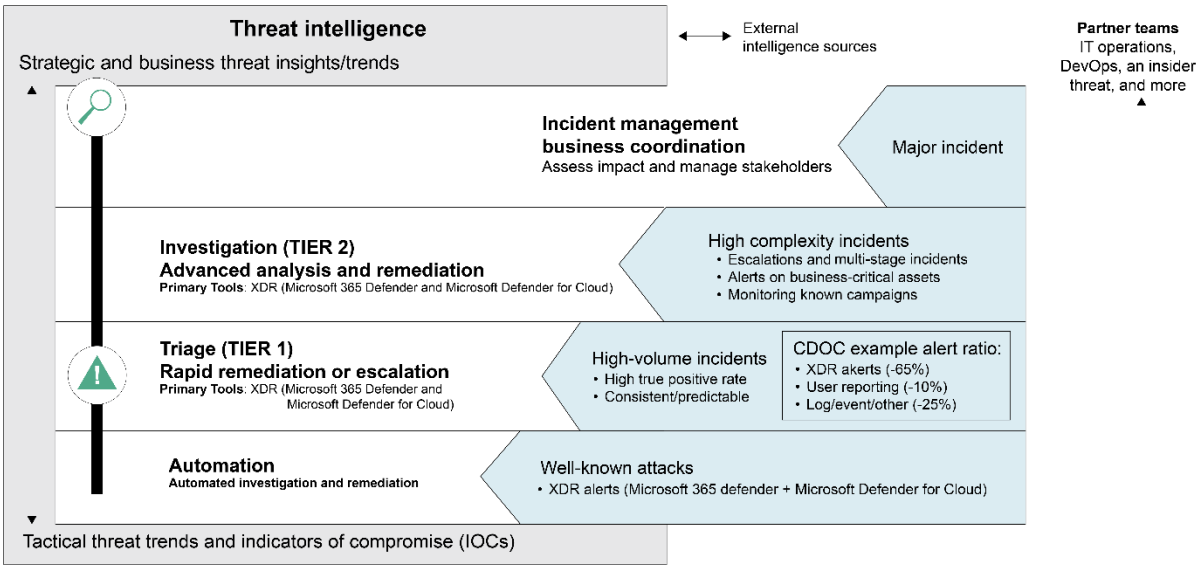


Figure 3.13 – The security operations functional tiers

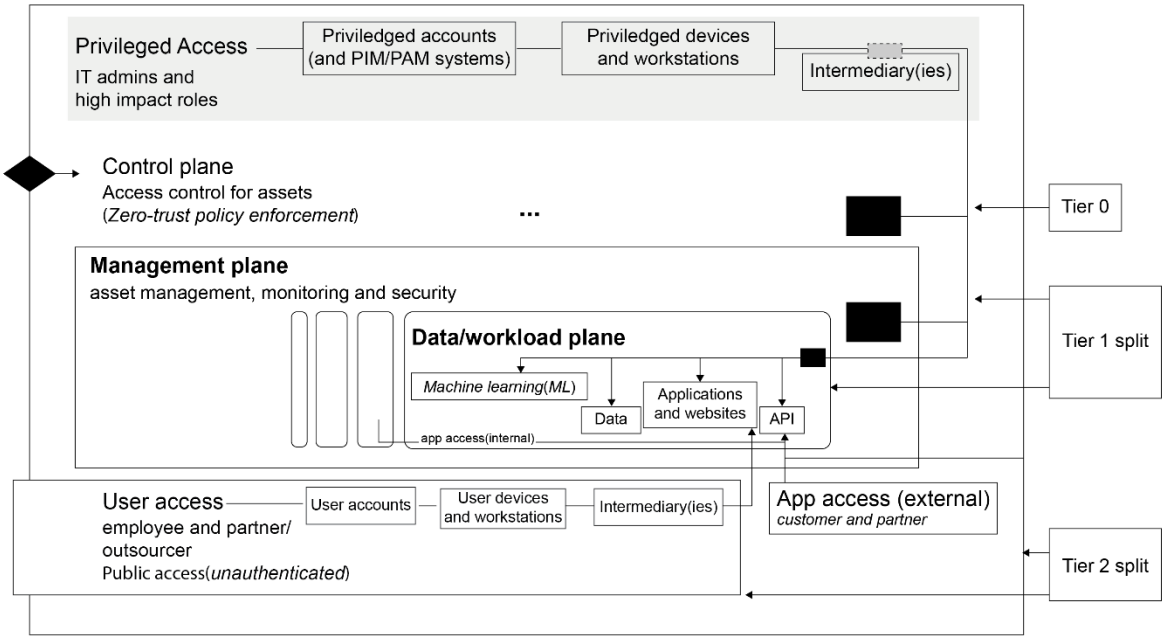


Figure 4.1: Expanded visualization of identity and access controls for secure access

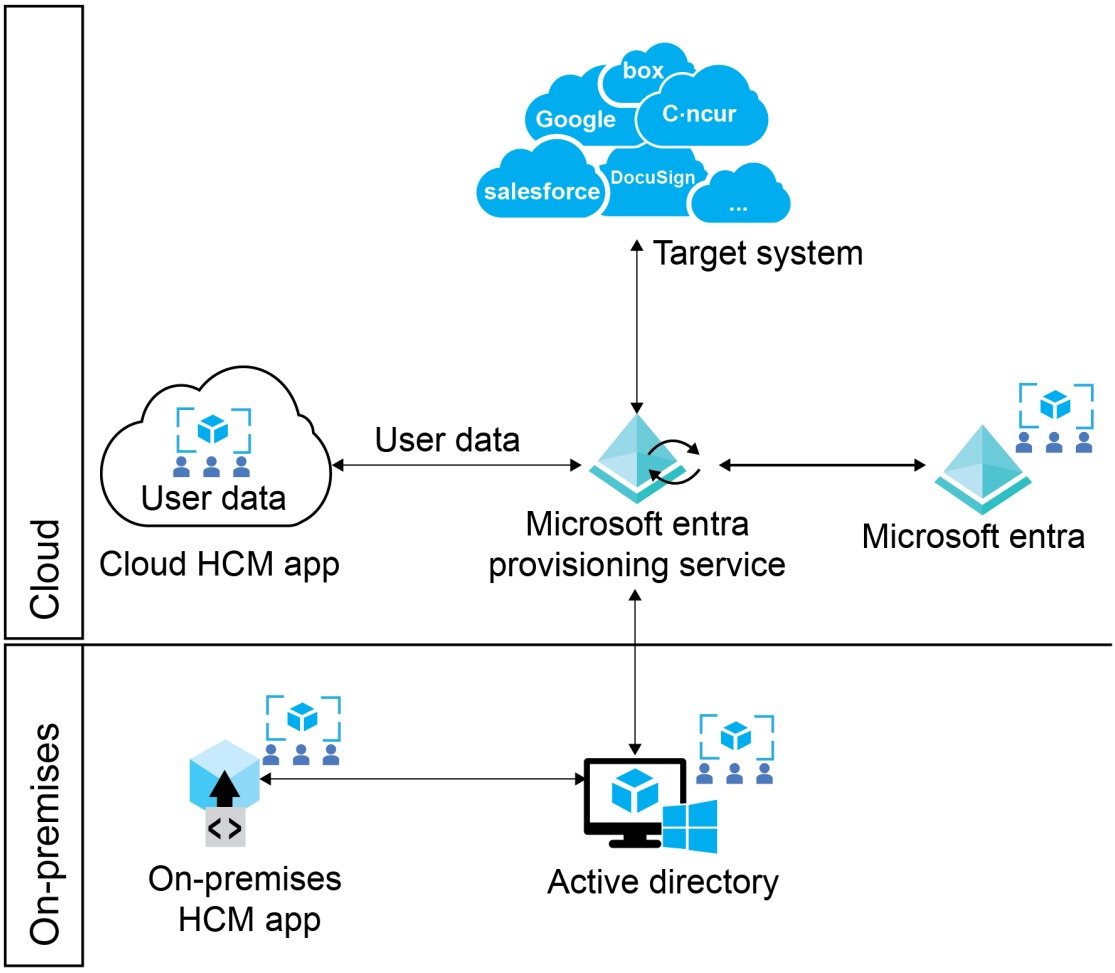


Figure 4.2: SCIM Microsoft Entra provisioning diagram

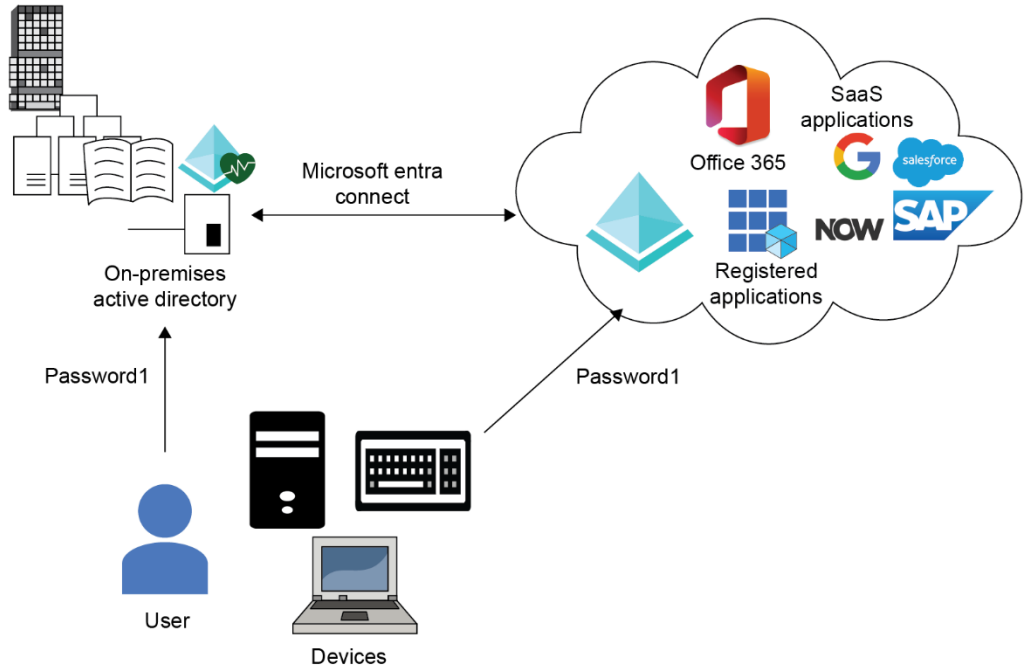


Figure 4.3: Overview of PHS, showing the flow from user devices to on-premises Active Directory and Microsoft Entra Connect

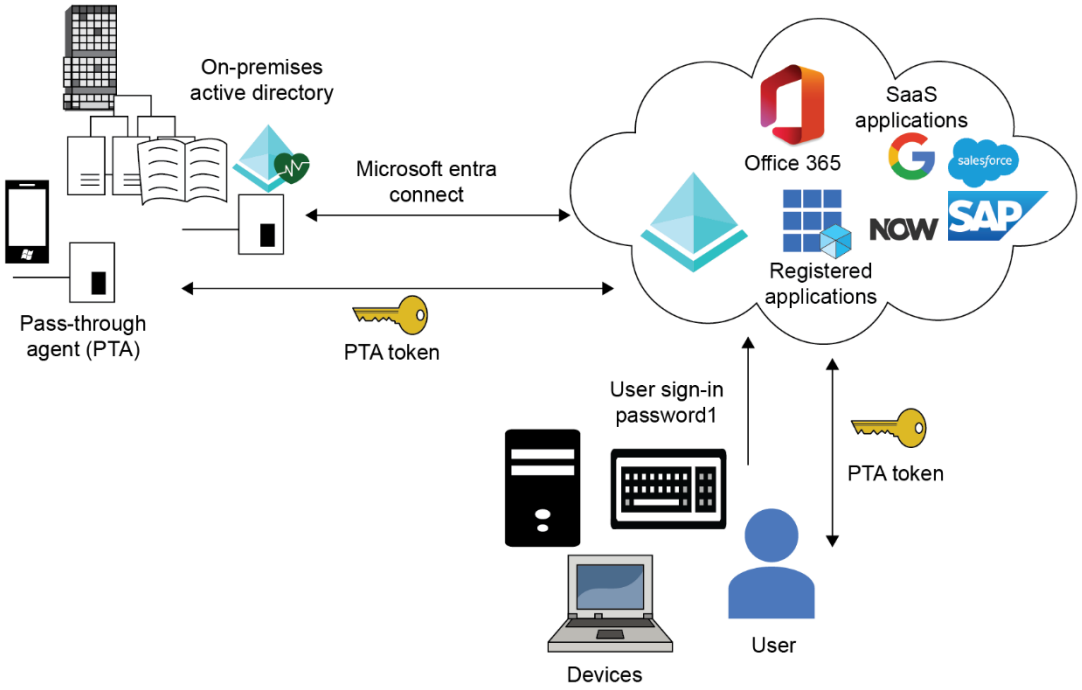


Figure 4.4: An overview of PTS, with the key difference from PHS being the dependency on communication between on-premises Active Directory and Microsoft Entra

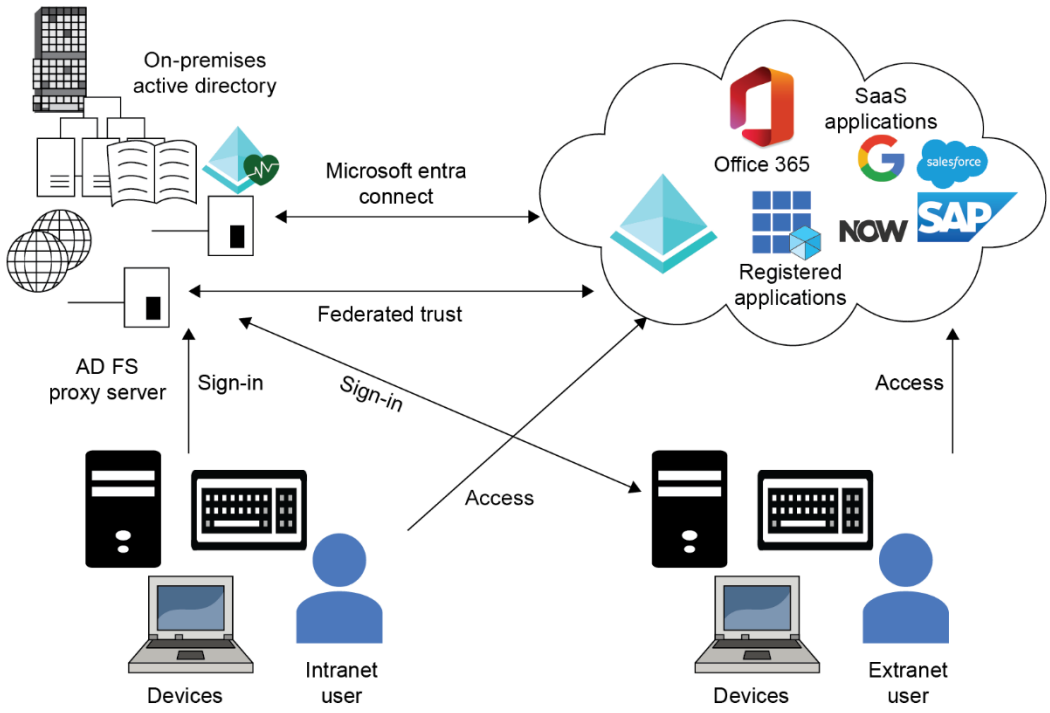


Figure 4.5: An overview of AD FS synchronization flows

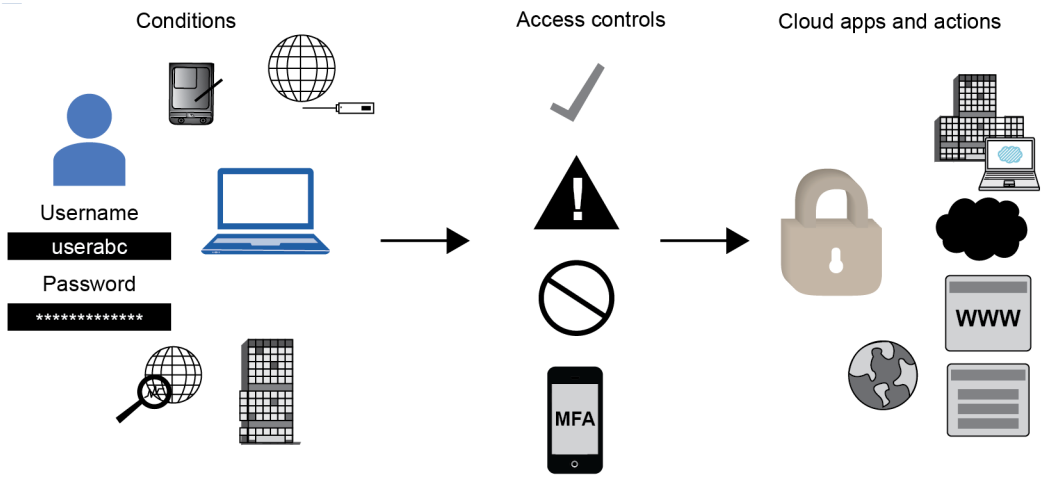


Figure 4.6: A CA workflow showing the flow of evaluation of user access, from left to right

Chapter 5: Design a Regulatory Compliance Strategy

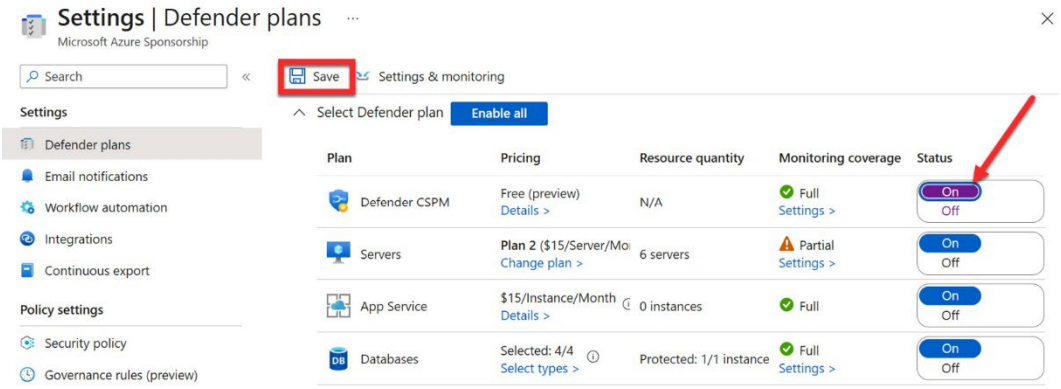


Figure 5.1: Turning on and saving Defender plans settings

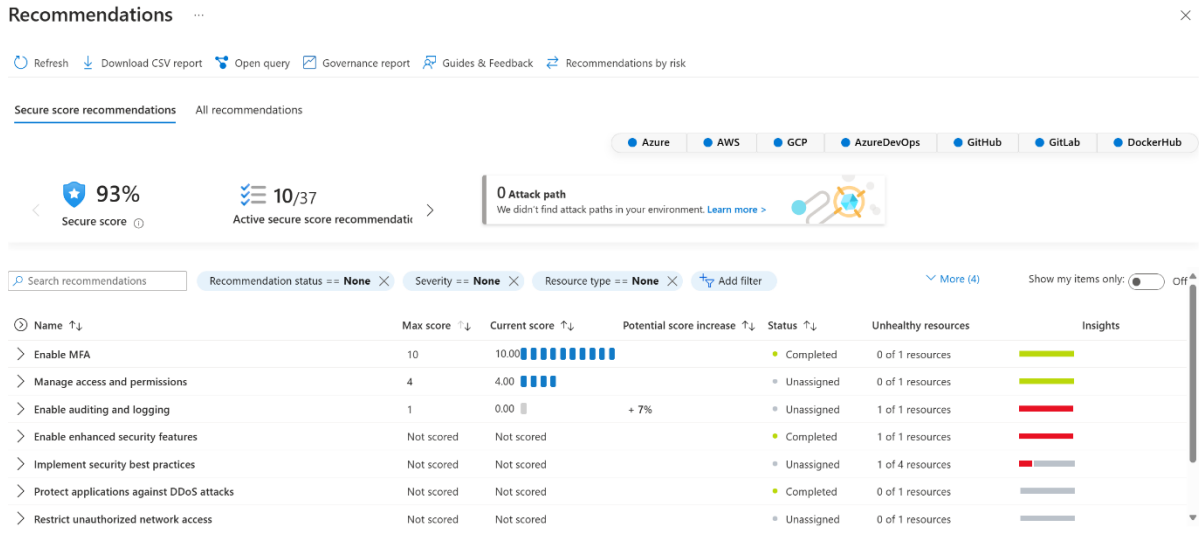


Figure 5.2: Security posture recommendations

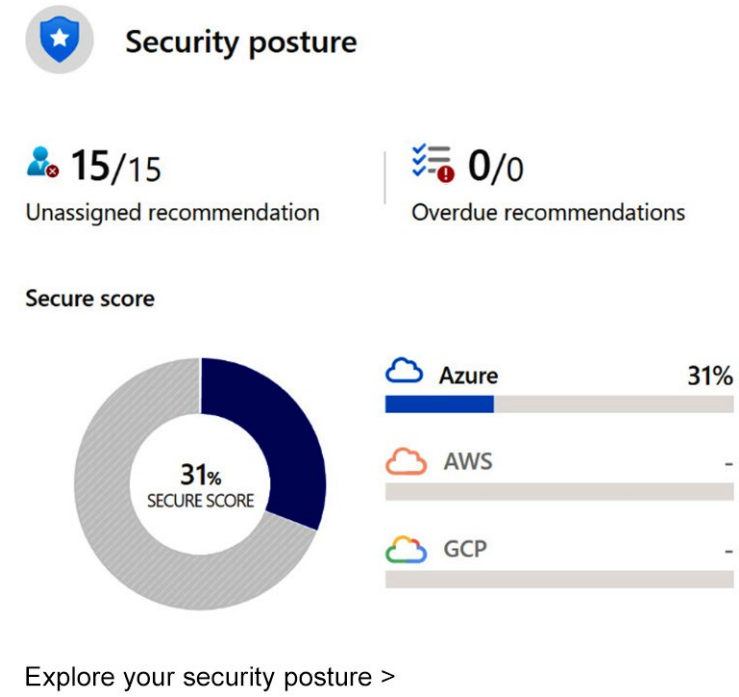


Figure 5.3: The Security posture overview tile

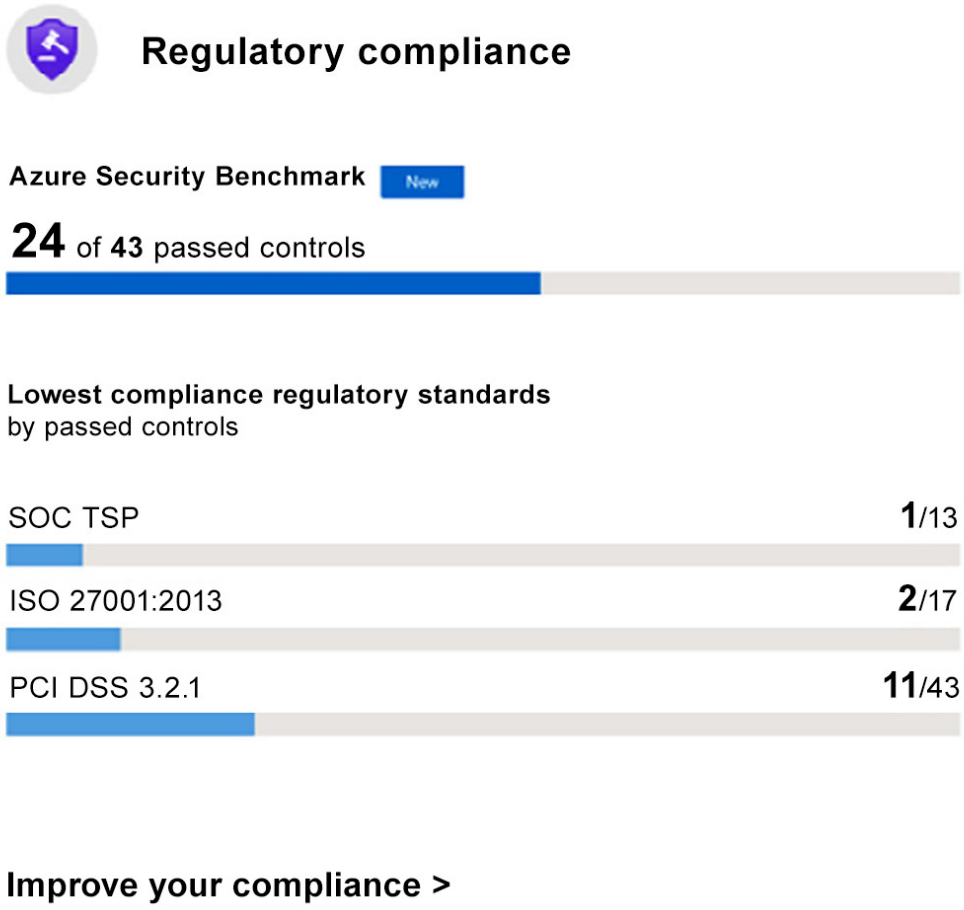


Figure 5.4: The Regulatory compliance overview tile

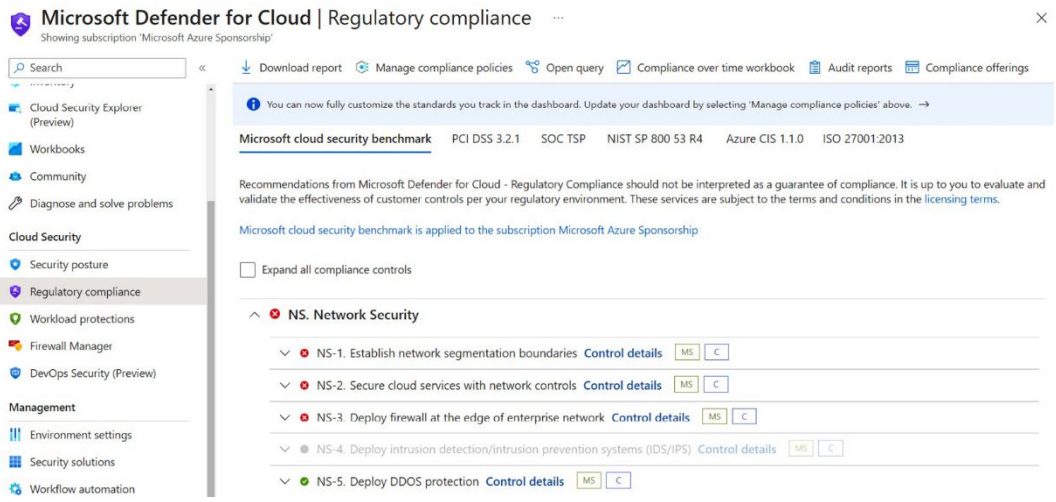


Figure 5.5: The Azure Security Benchmark compliance controls

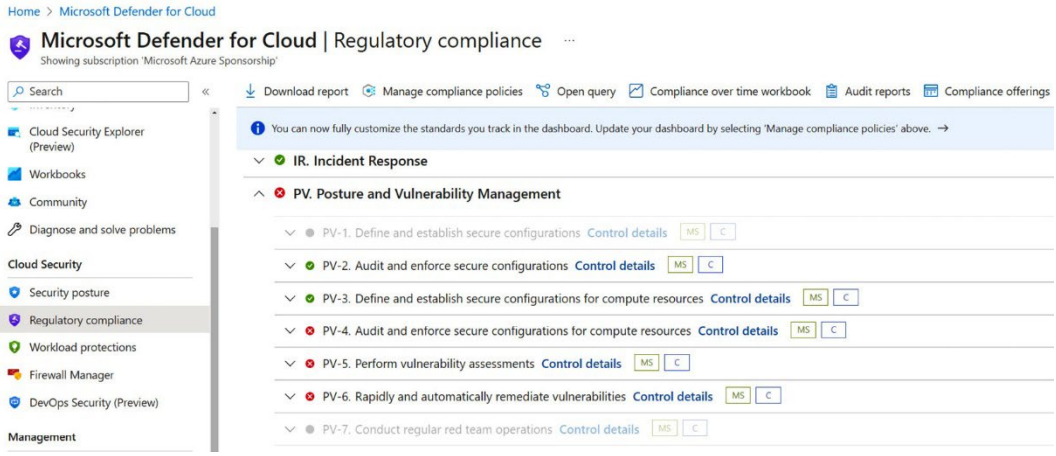


Figure 5.6: Regulatory compliance color representation

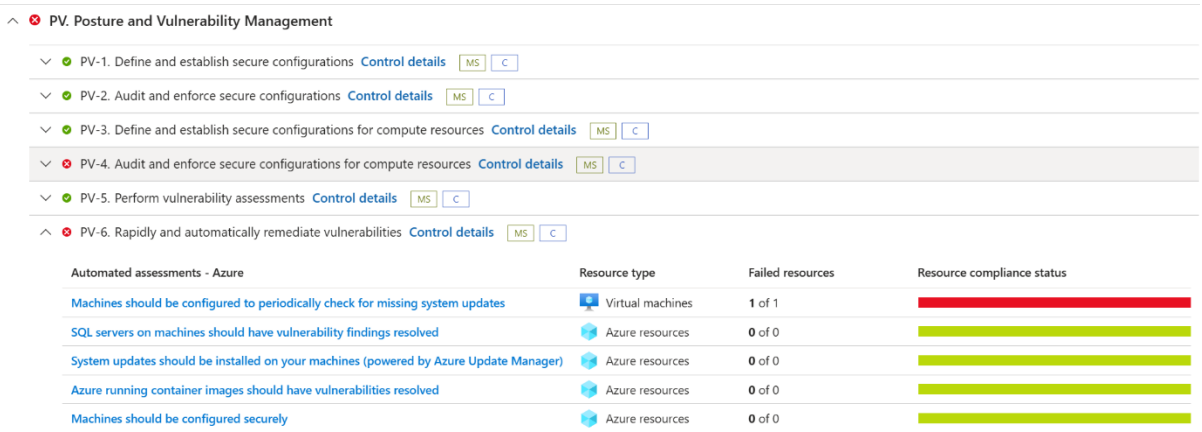


Figure 5.7: Security control recommendations

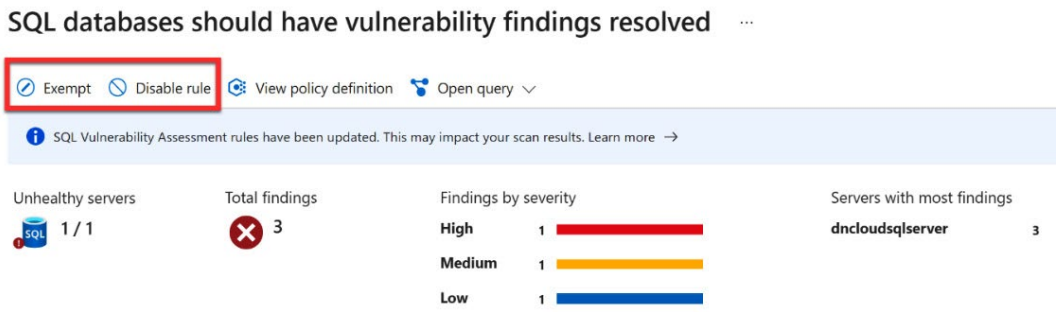


Figure 5.8: Recommendation resolution

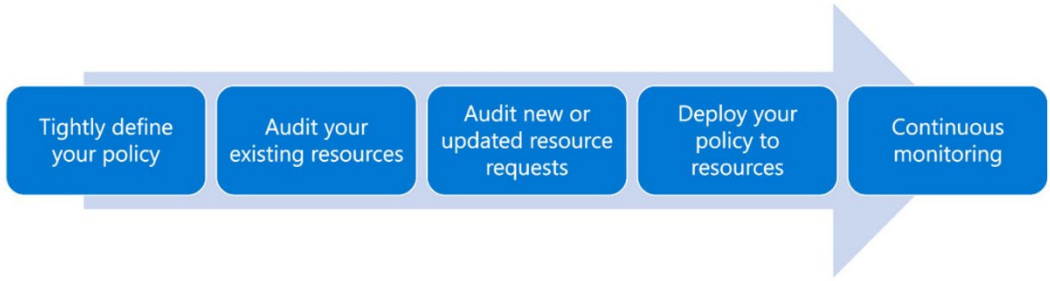


Figure 5.9: Azure Policy workflow

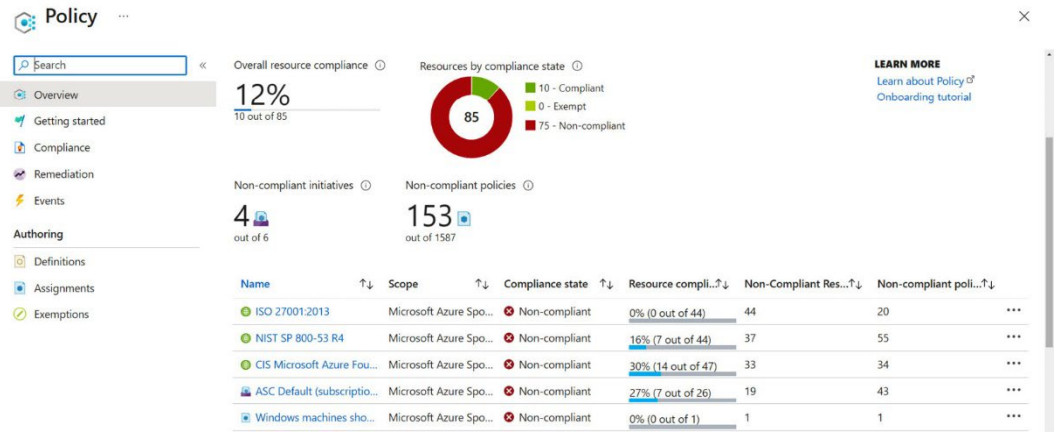


Figure 5.10: Policy compliance overview

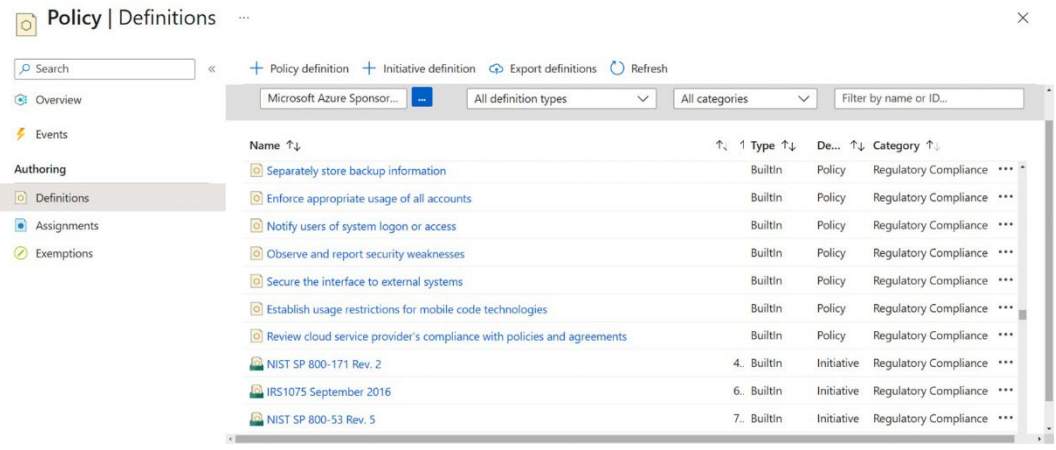


Figure 5.11: Built-in policies and + Policy definition and + Initiative definition

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

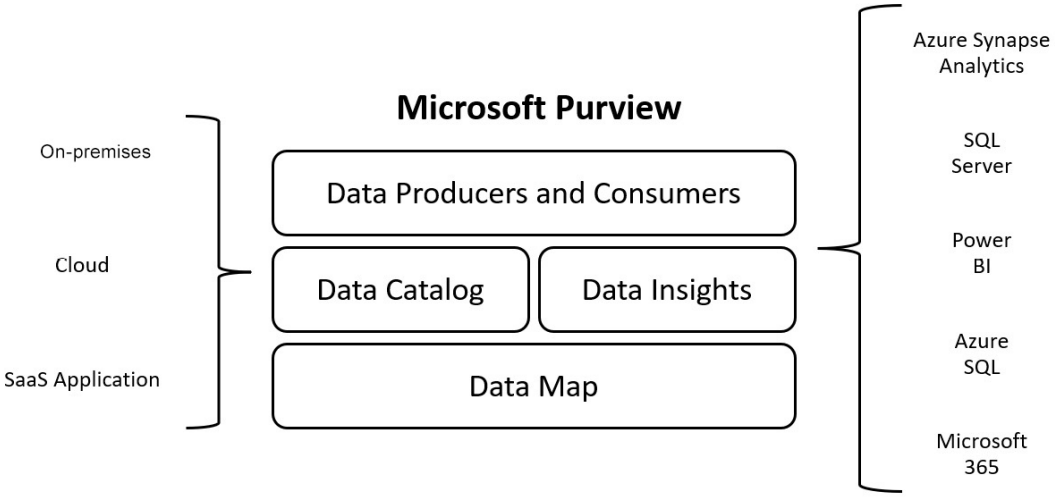


Figure 5.13: Microsoft Purview for data privacy governance

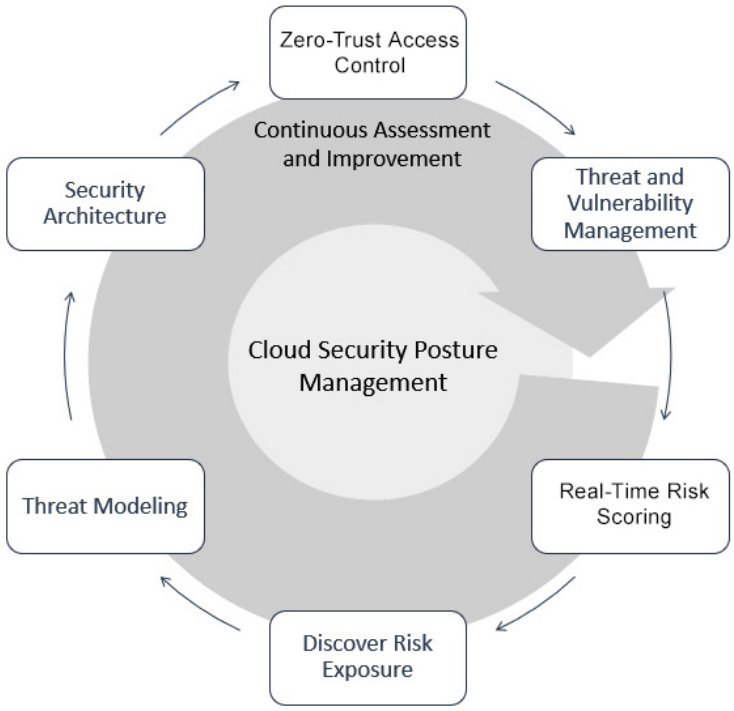


Figure 6.1: CSPM – continuous assessment and improvement

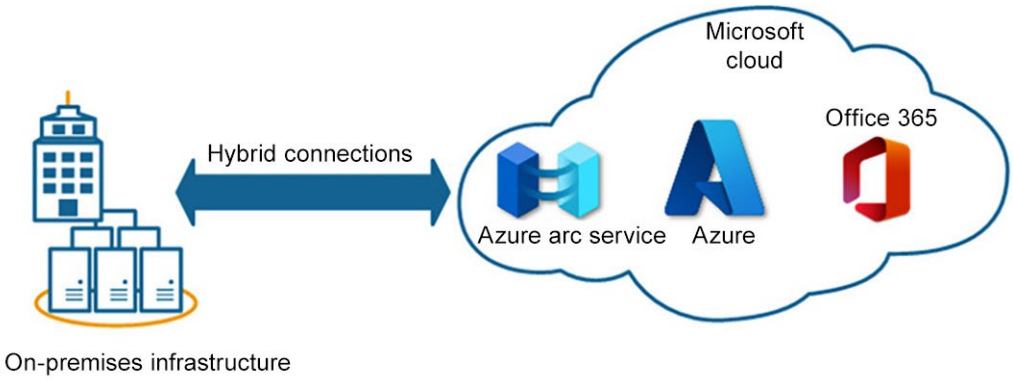


Figure 6.2: Hybrid infrastructure diagram

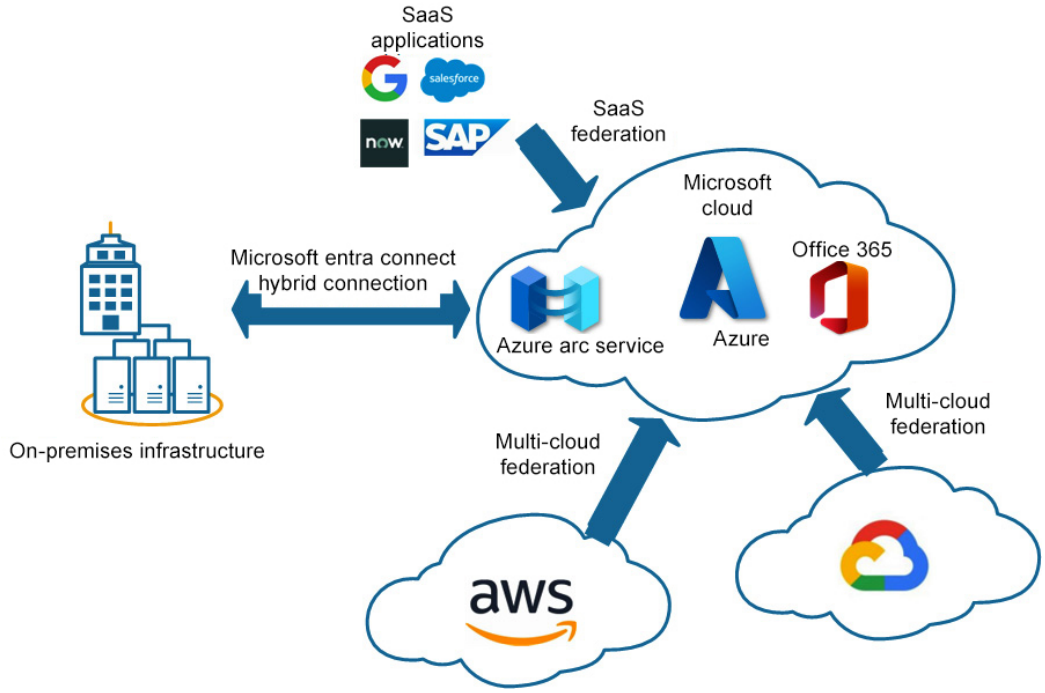


Figure 6.3: Multi-cloud infrastructure diagram

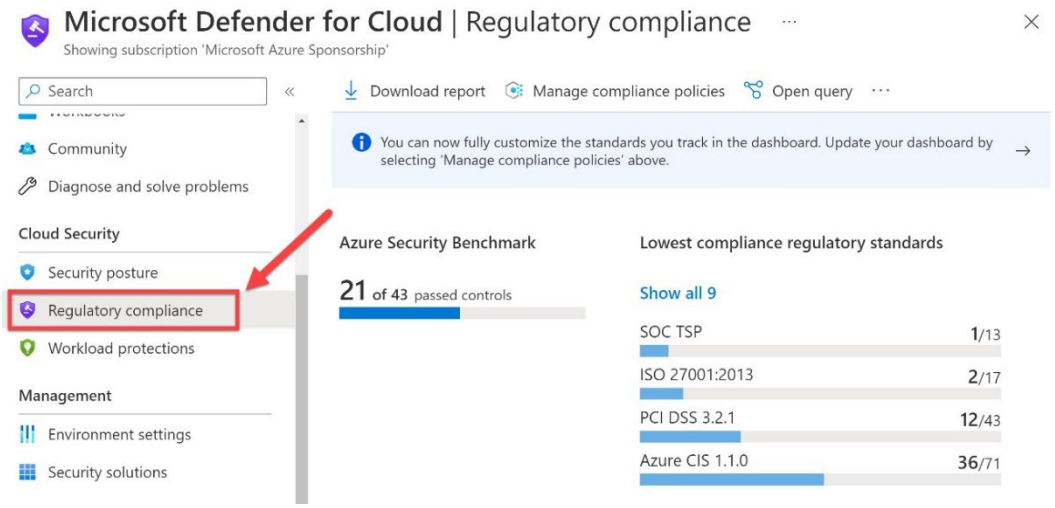


Figure 6.4: Regulatory compliance in the Cloud Security menu

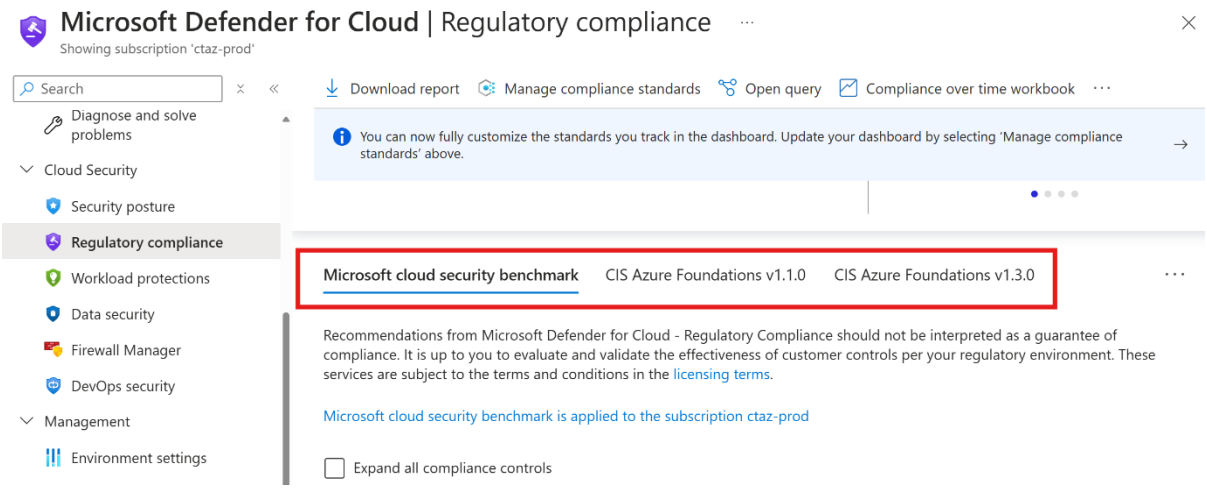


Figure 6.5: List of regulatory compliance options

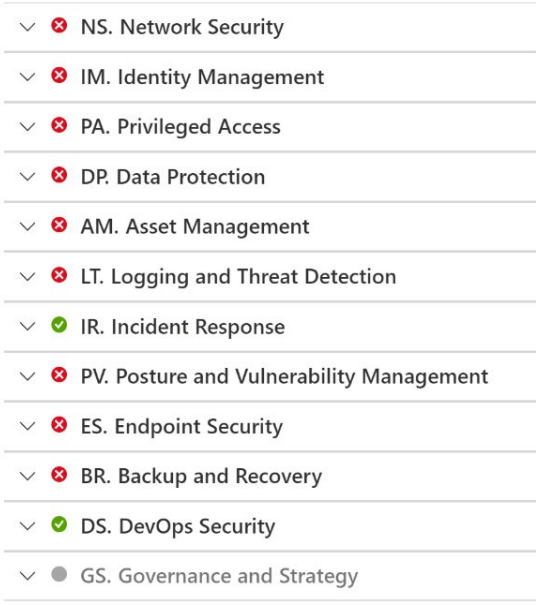


Figure 6.6: List of Azure Security Benchmark controls

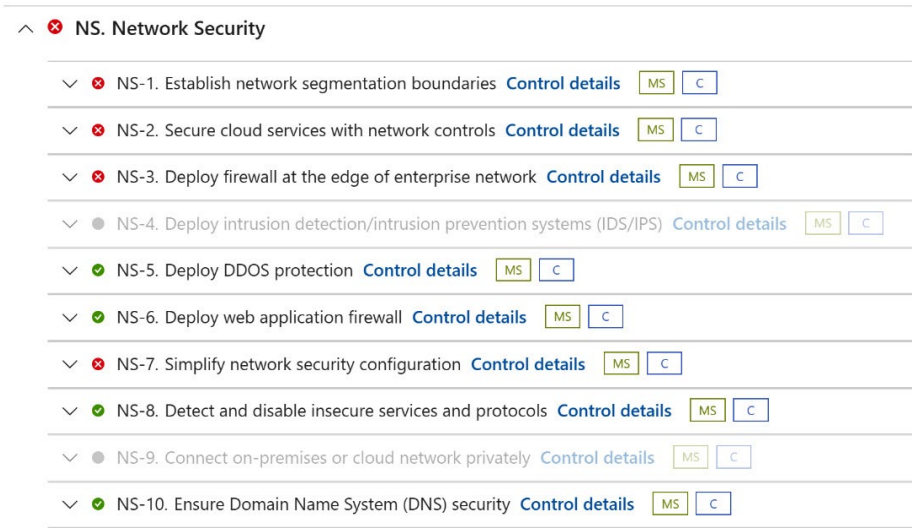


Figure 6.7: Network security controls

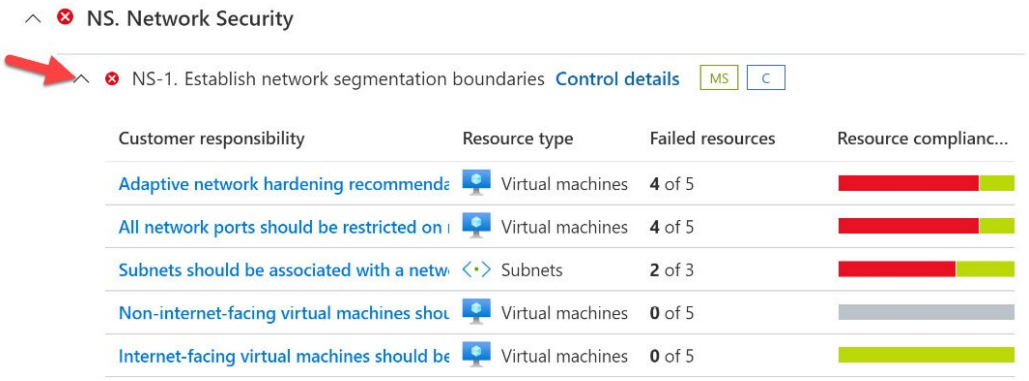


Figure 6.8: Recommended security controls to increase security posture

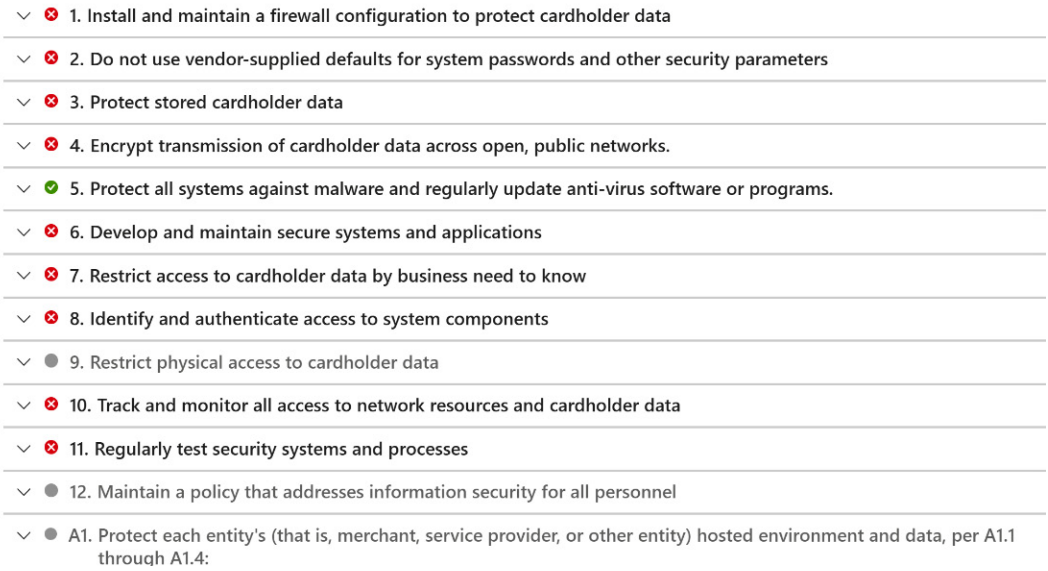


Figure 6.9: PCI-DSS 3.2.1 list of security control requirements

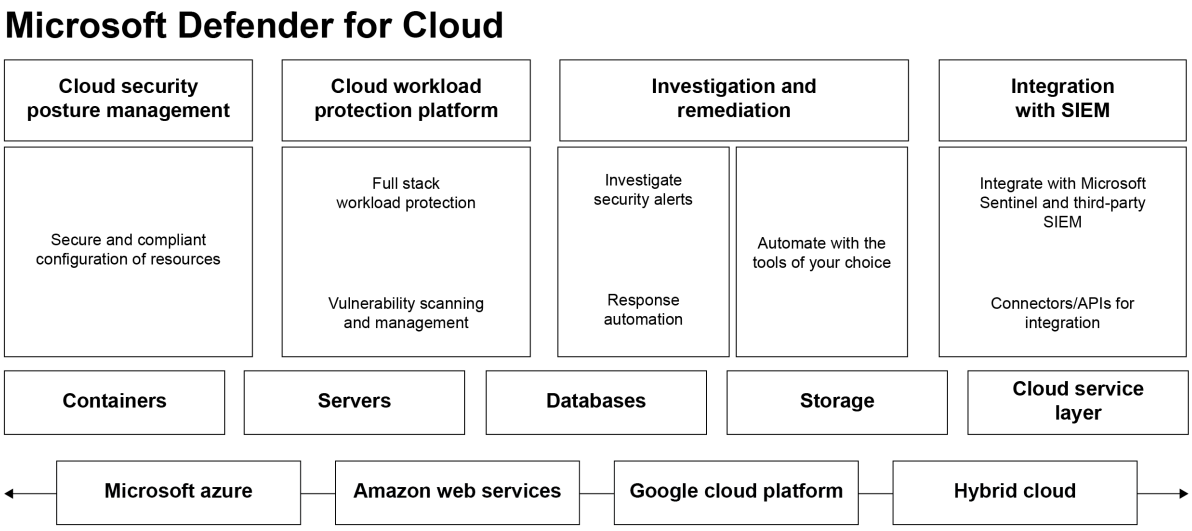


Figure 6.10: Microsoft Defender for Cloud capabilities

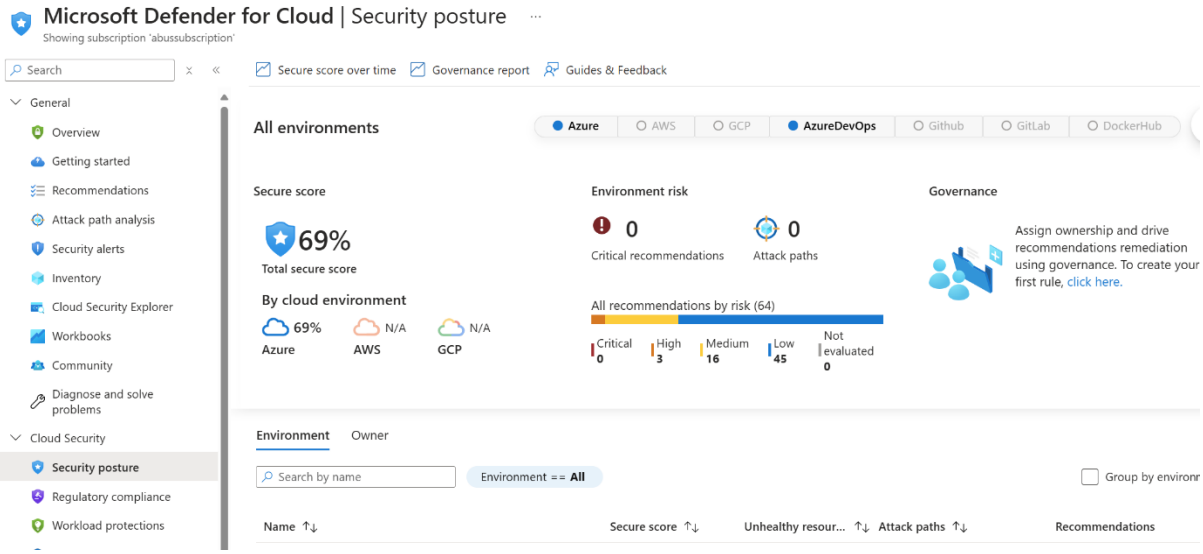


Figure 6.11: Security posture in the Cloud Security menu

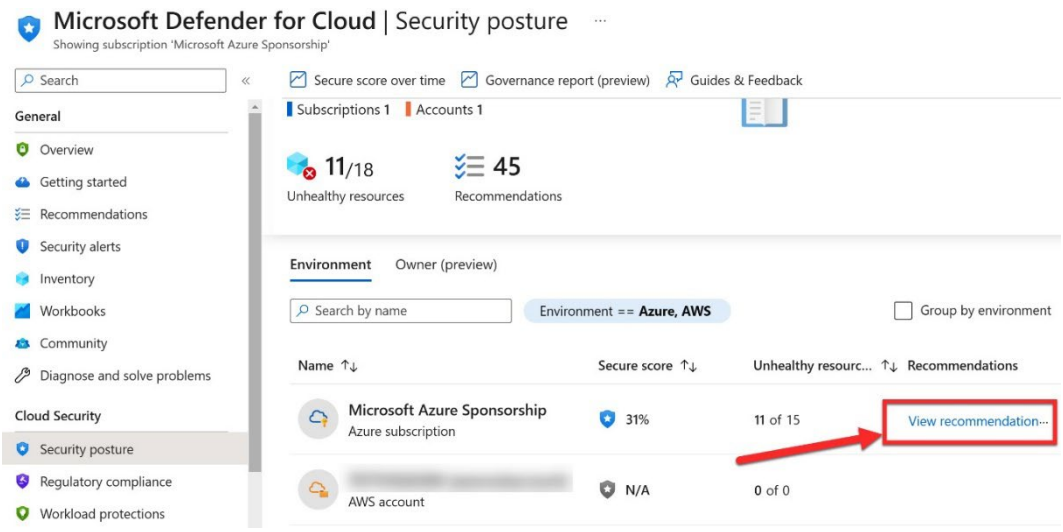


Figure 6.12: Subscription security posture recommendations

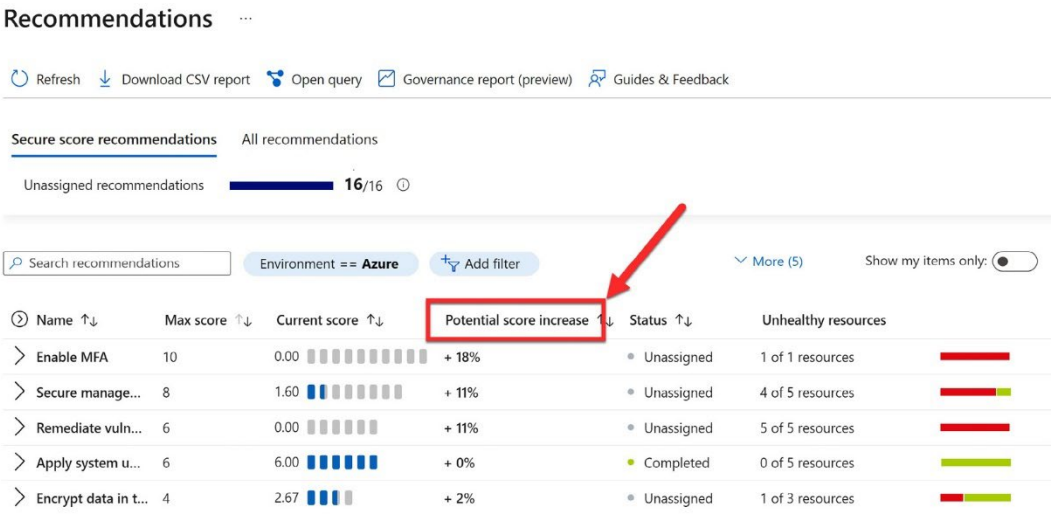


Figure 6.13: Potential score increase

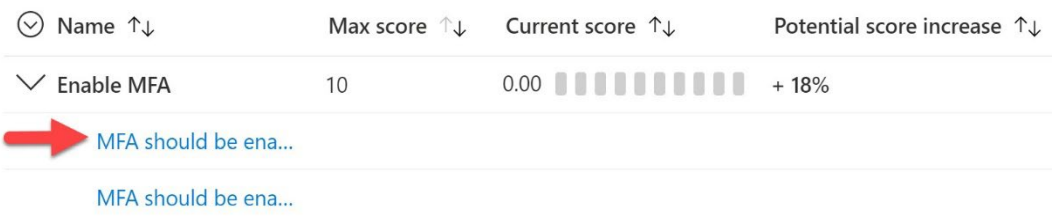


Figure 6.14: Enable MFA recommendations list

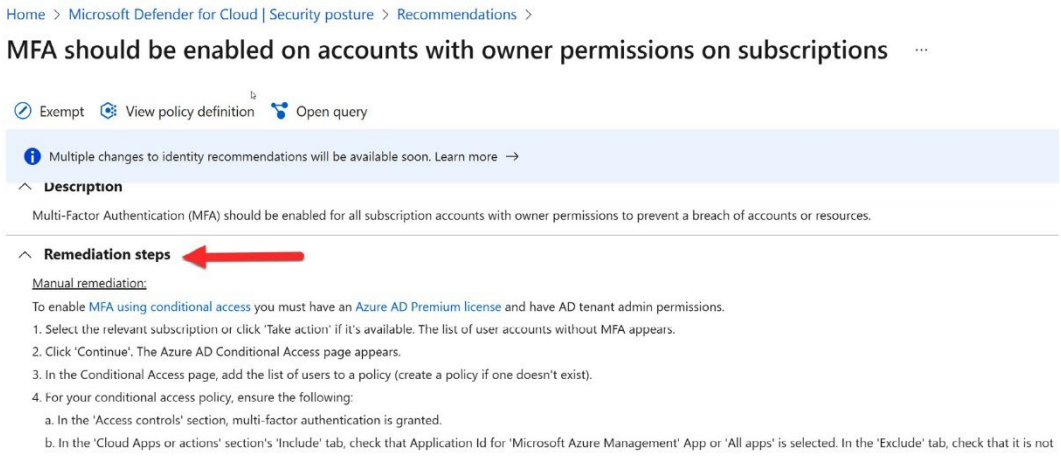


Figure 6.15: Remediation steps within the security posture recommendations

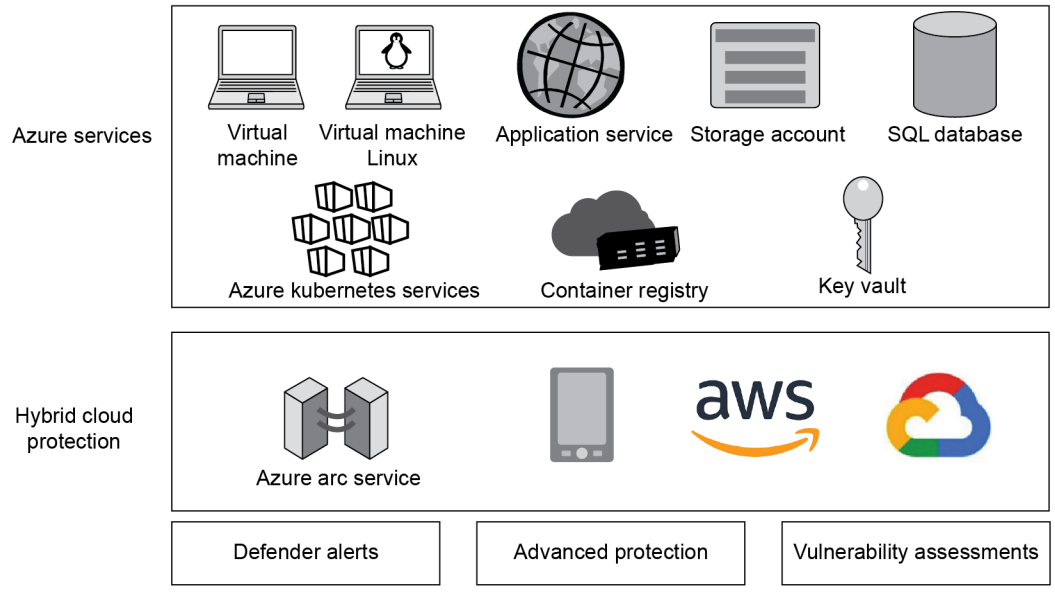


Figure 6.16: Microsoft Defender for Cloud enhanced security protection

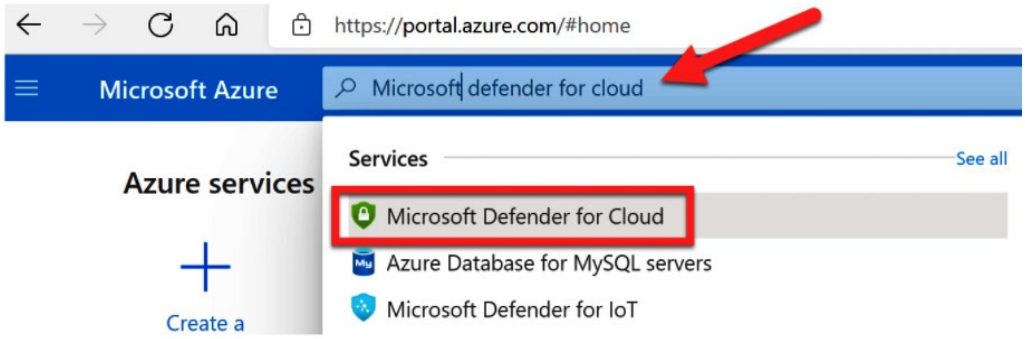


Figure 6.17: Navigating to Microsoft Defender for Cloud

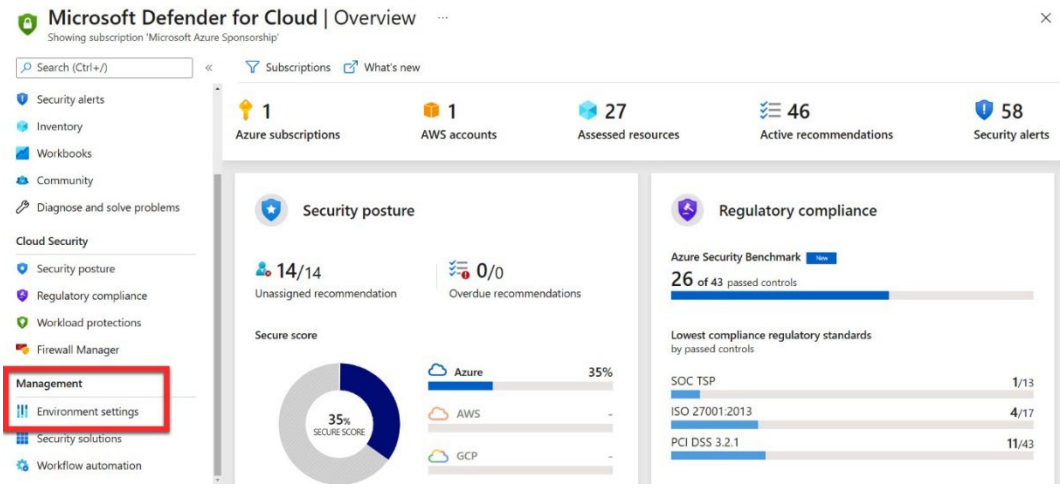


Figure 6.18: Environment settings in Microsoft Defender for Cloud

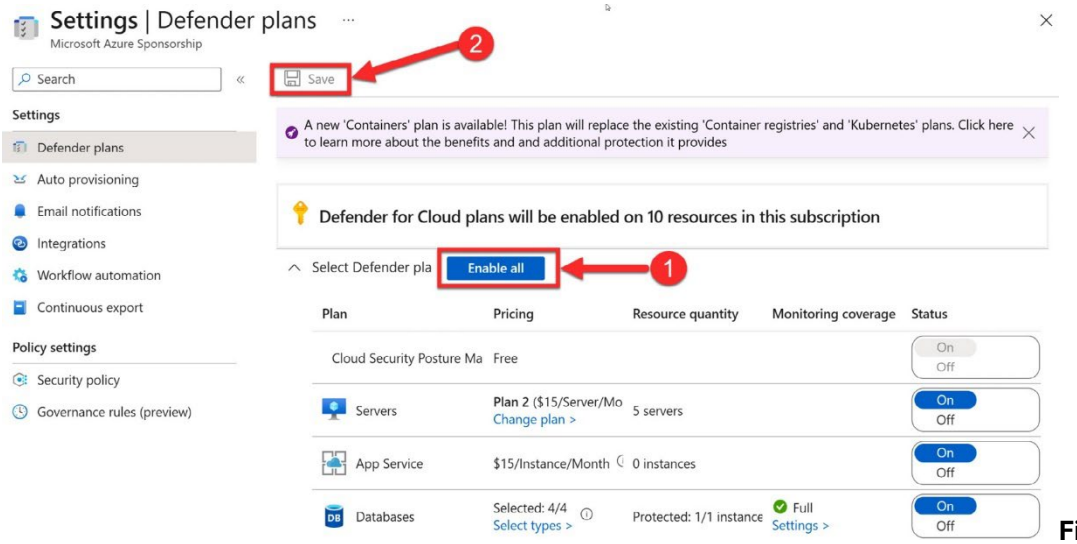


Figure 6.19: Enabling Defender for Cloud enhanced security plans

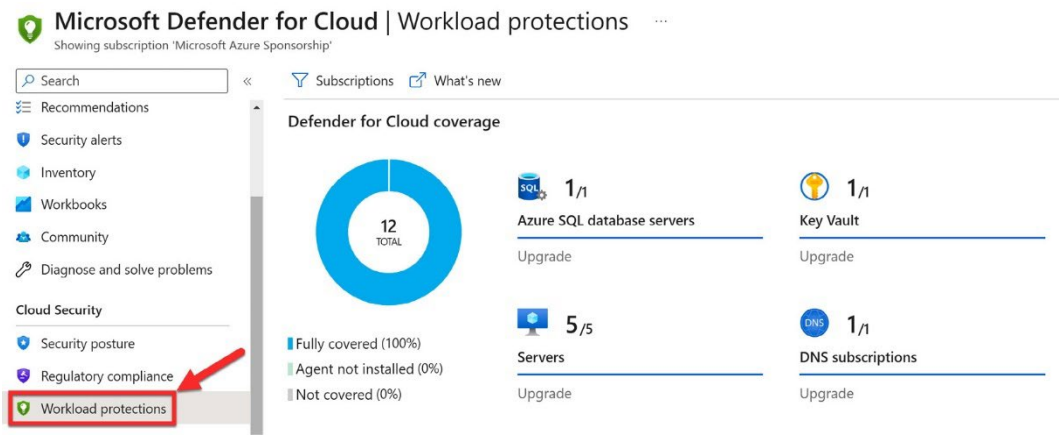


Figure 6.20: Workload protections in the Cloud Security menu

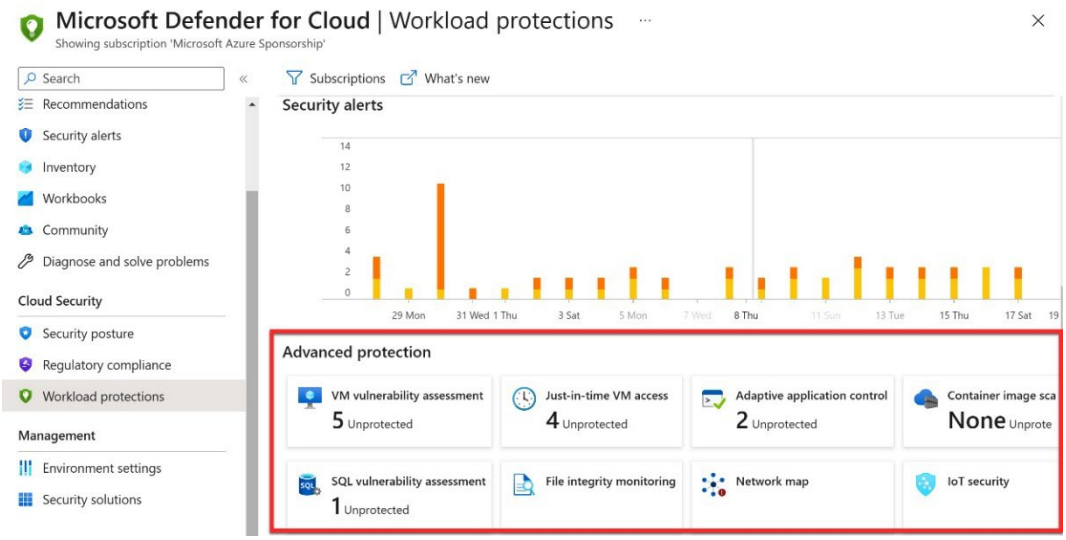


Figure 6.21: Advanced protection for Defender plans

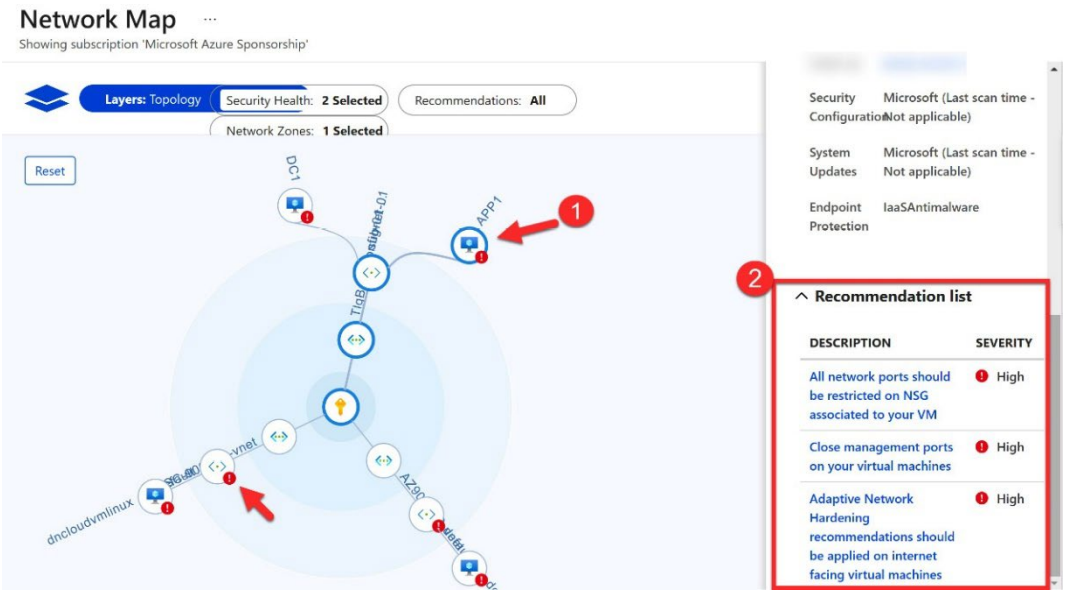


Figure 6.22: Network map and security posture recommendations

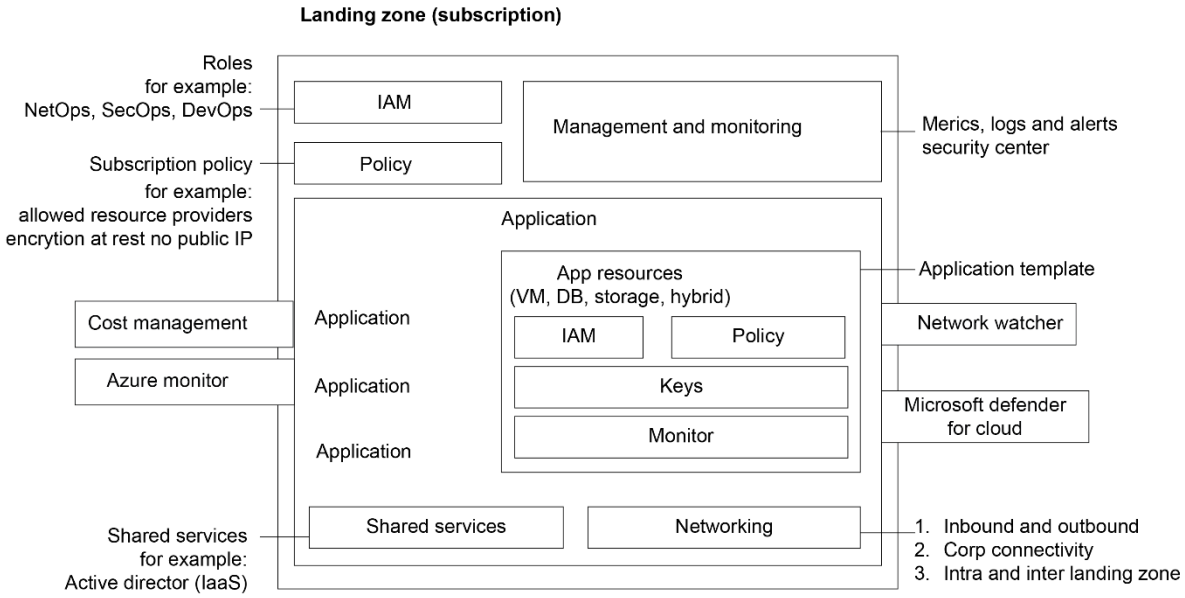


Figure 6.23: Diagram of the components of an Azure landing zone

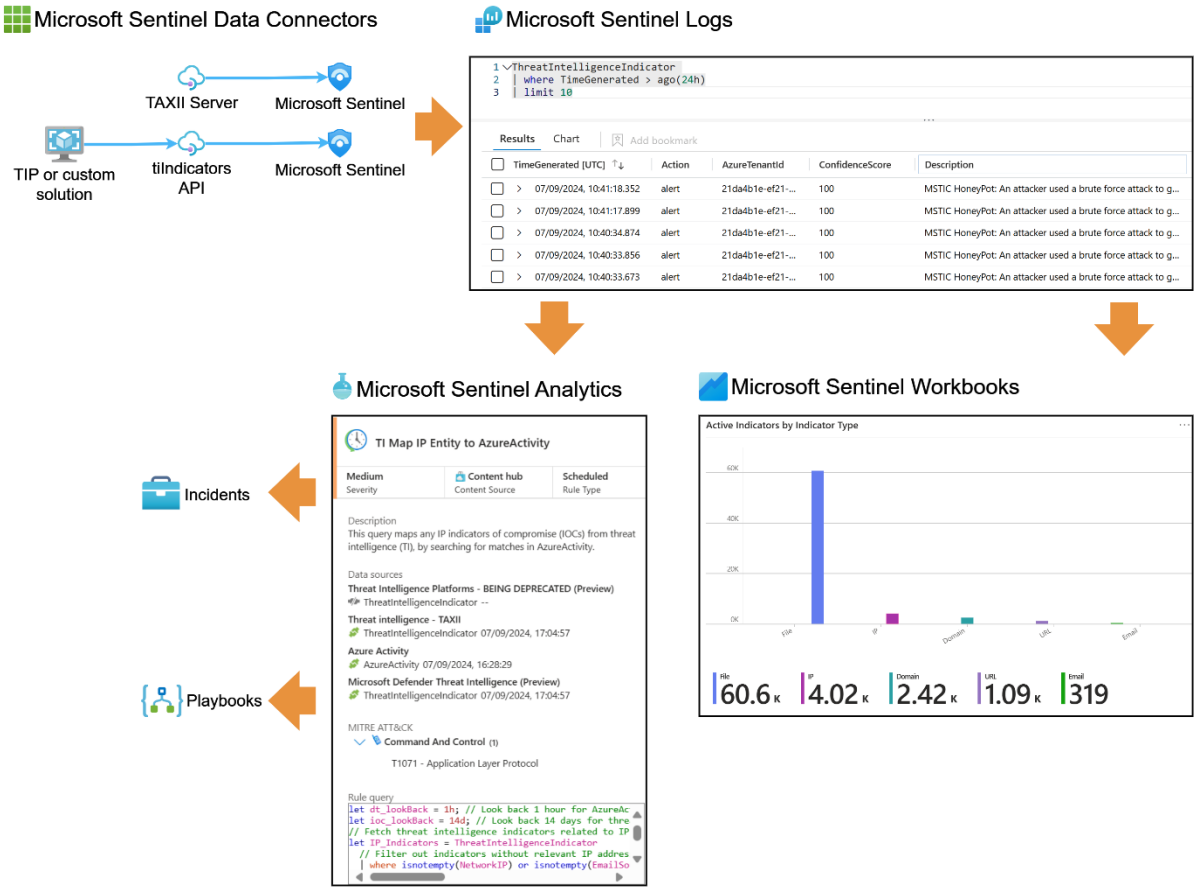


Figure 6.24: Microsoft Sentinel tools for threat intelligence

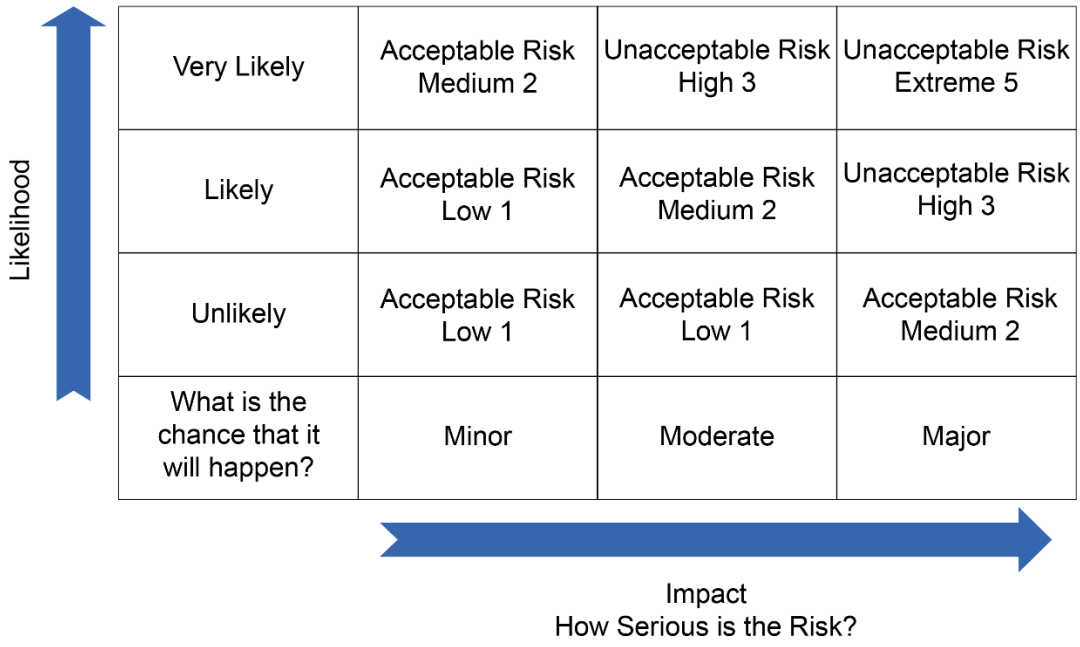


Figure 6.25: Risk assessment matrix

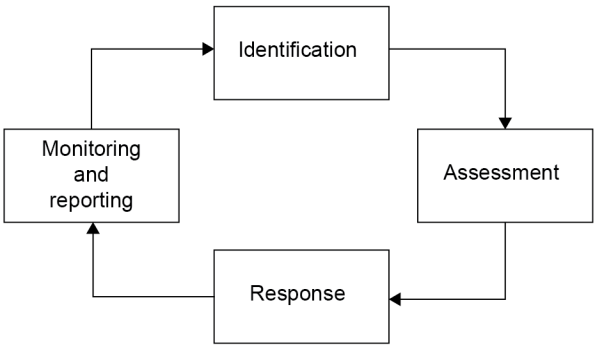


Figure 6.26: Risk assessment and mitigation life cycle

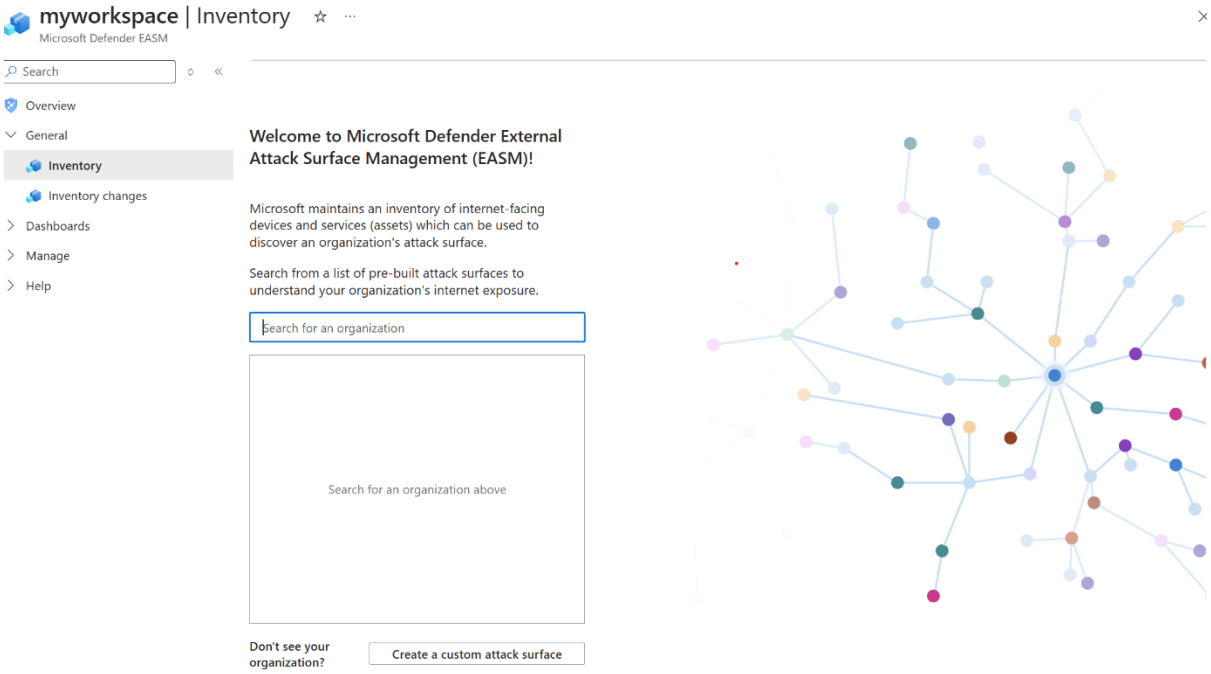


Figure 6.27: Screenshot of Defender for EASM in Azure portal

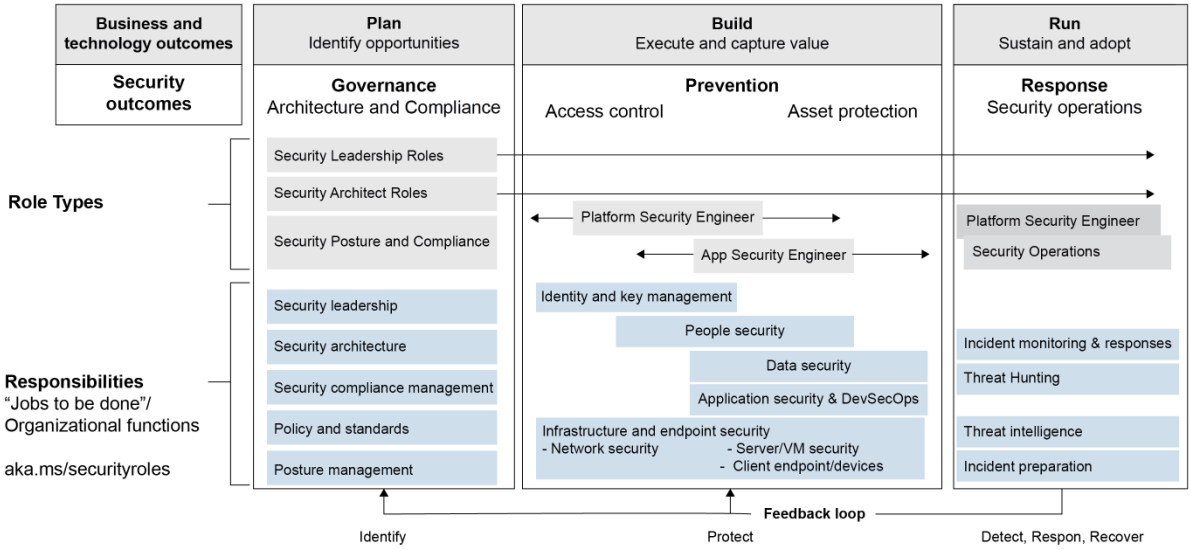


Figure 7.1: A flowchart that outlines a structured approach to cybersecurity, divided into five phases: Govern, Plan, Build, Operate, and Sustain

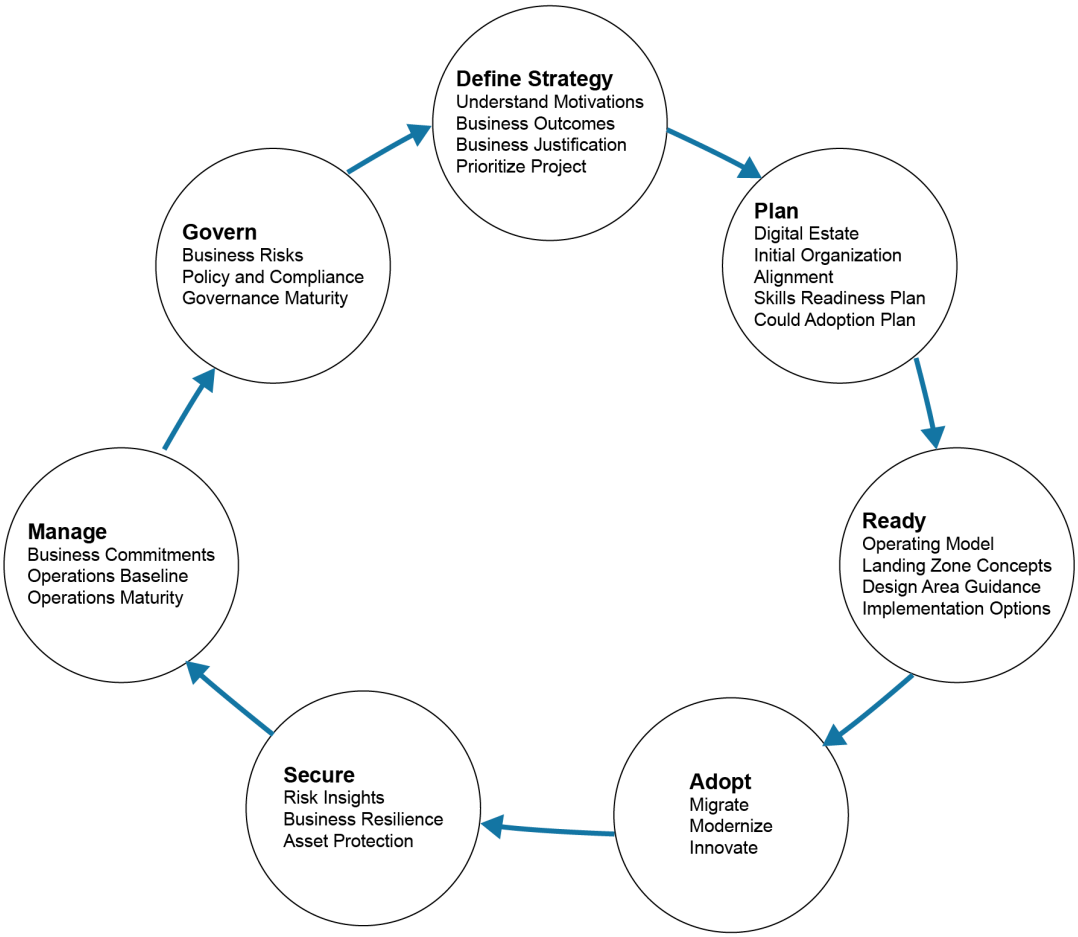


Figure 7.2: CAF depicted as a cyclical lifecycle: Define Strategy, Plan, Ready, Adopt, Secure, Manage, Govern, and then start again

Figure 7.3: Microsoft Endpoint Manager admin center on the "Endpoint security | Security baselines" pages

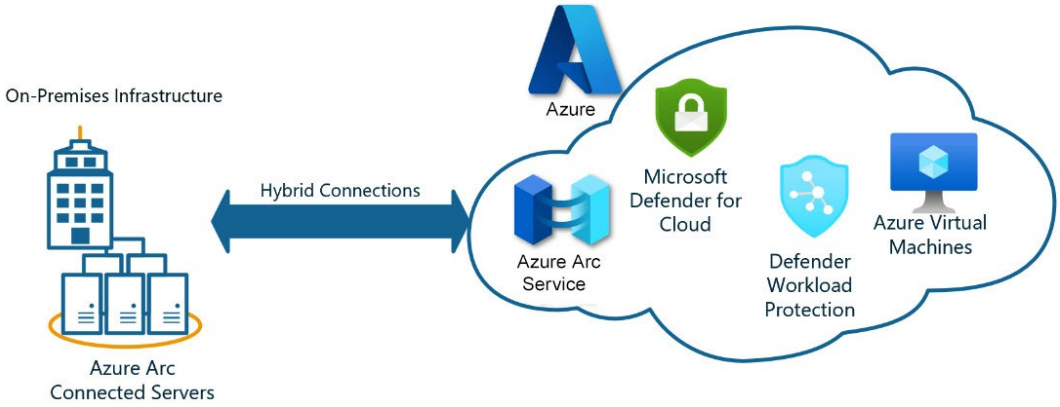


Figure 7.4: Hybrid server infrastructures

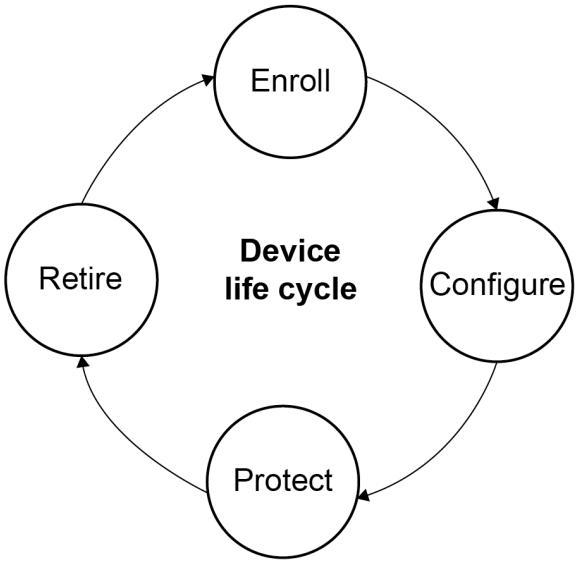


Figure 7.5: Mobile device life cycle – from Enrol, through Configure, Protect, and then Retire

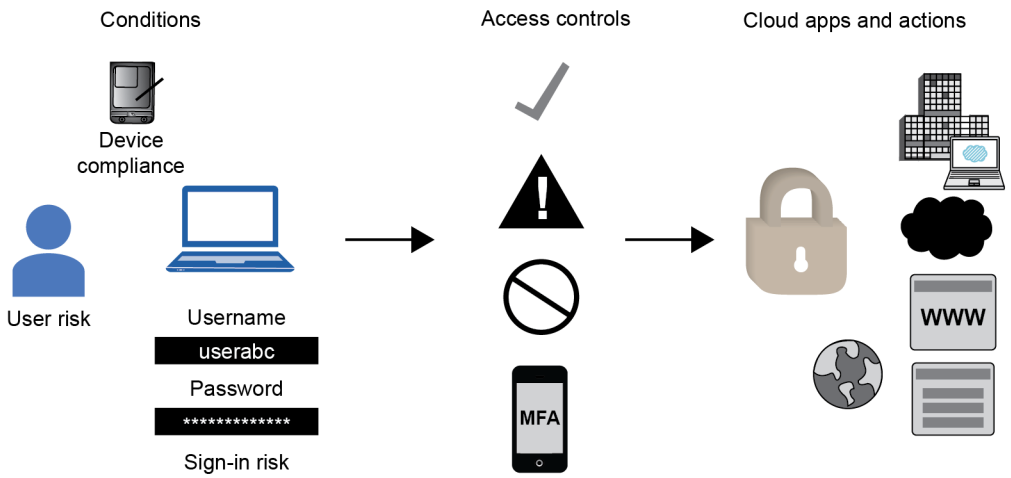


Figure 7.6: Conditional Access policies for MDM-compliant devices, highlighting the various conditions that can be evaluated

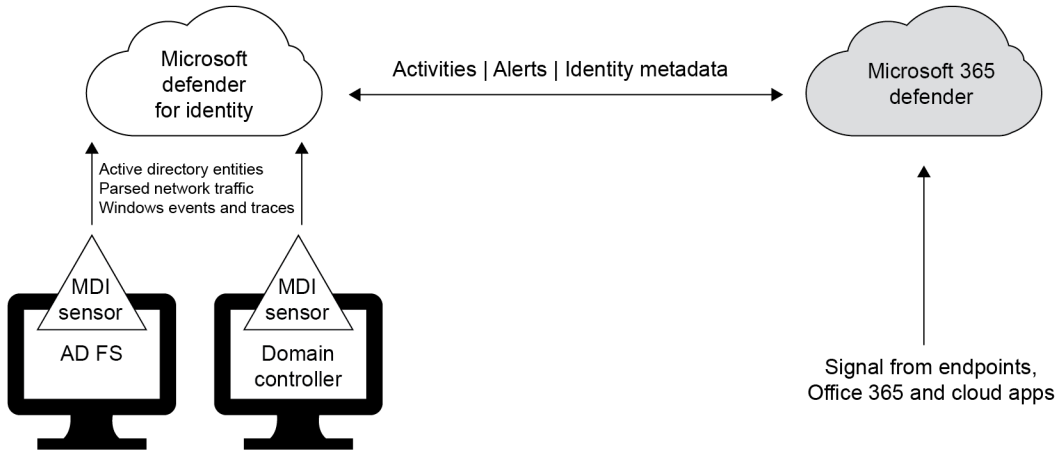


Figure 7.7: Microsoft Defender for Identity (MDI) integrating with Microsoft 365 Defender

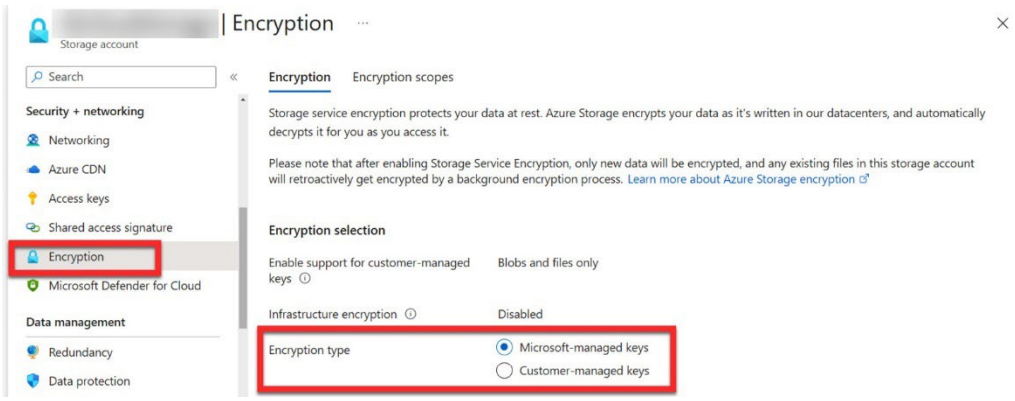


Figure 7.8: Configuring customer-managed keys with Azure Key Vault – a screenshot from the Azure portal

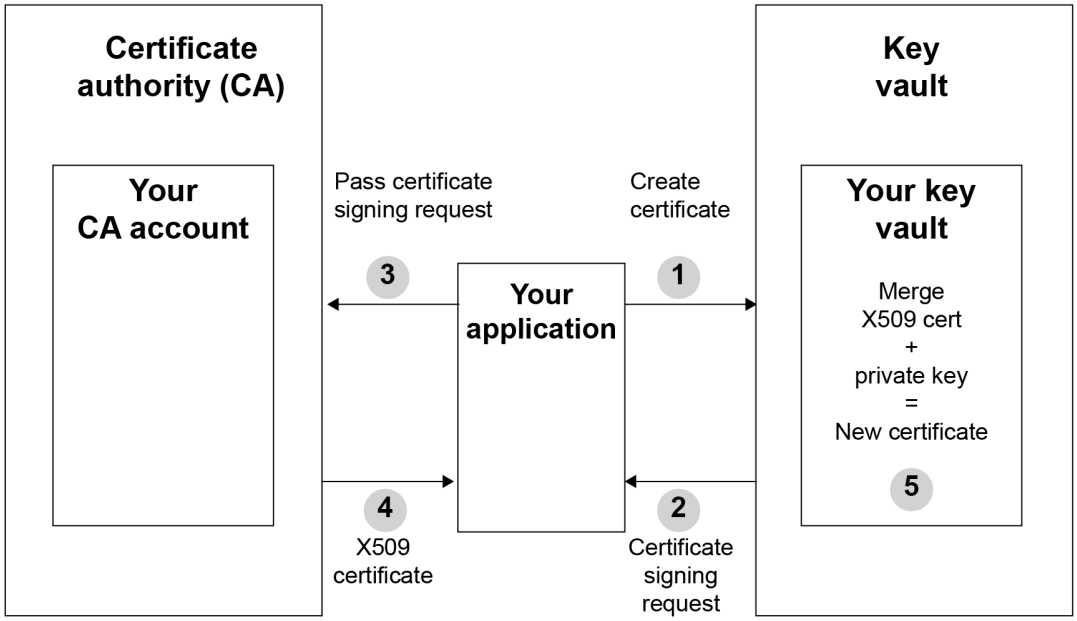


Figure 7.9: CA validation process with Azure Key Vault

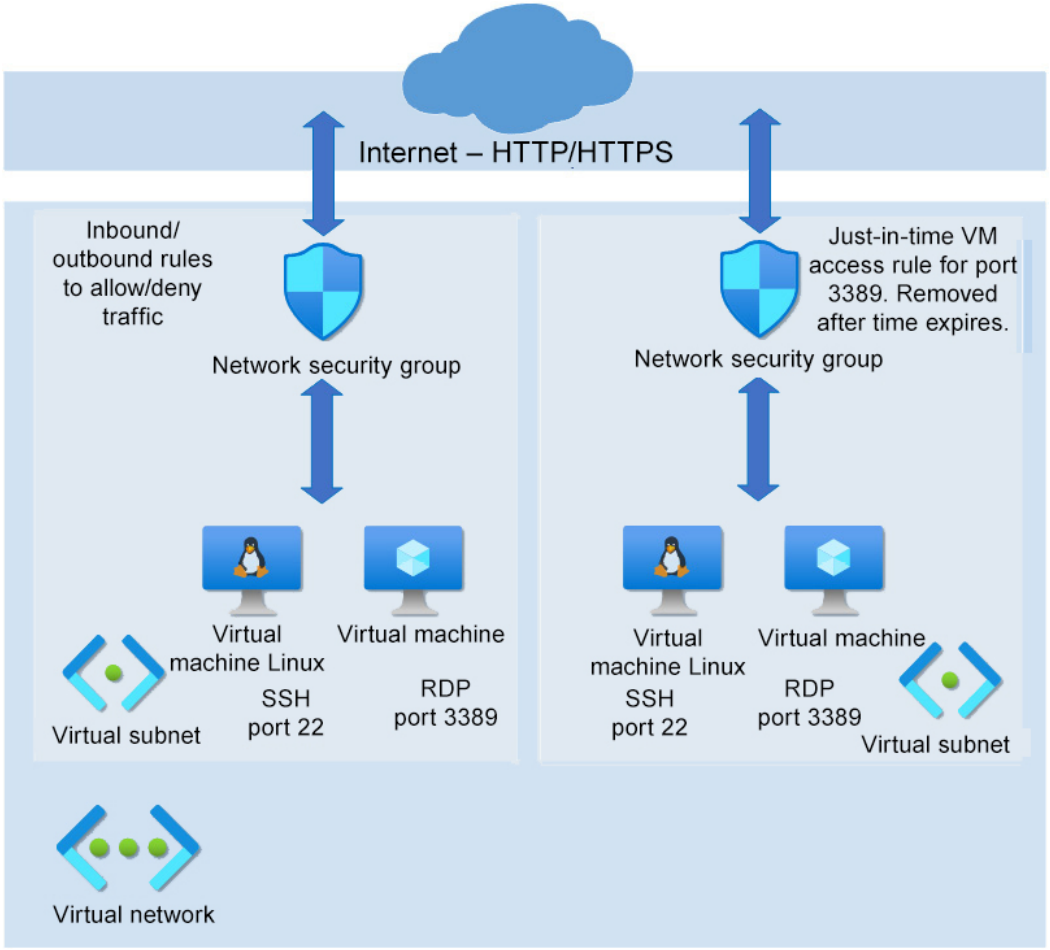


Figure 7.10: NSG with a JIT virtual machine access inbound rule

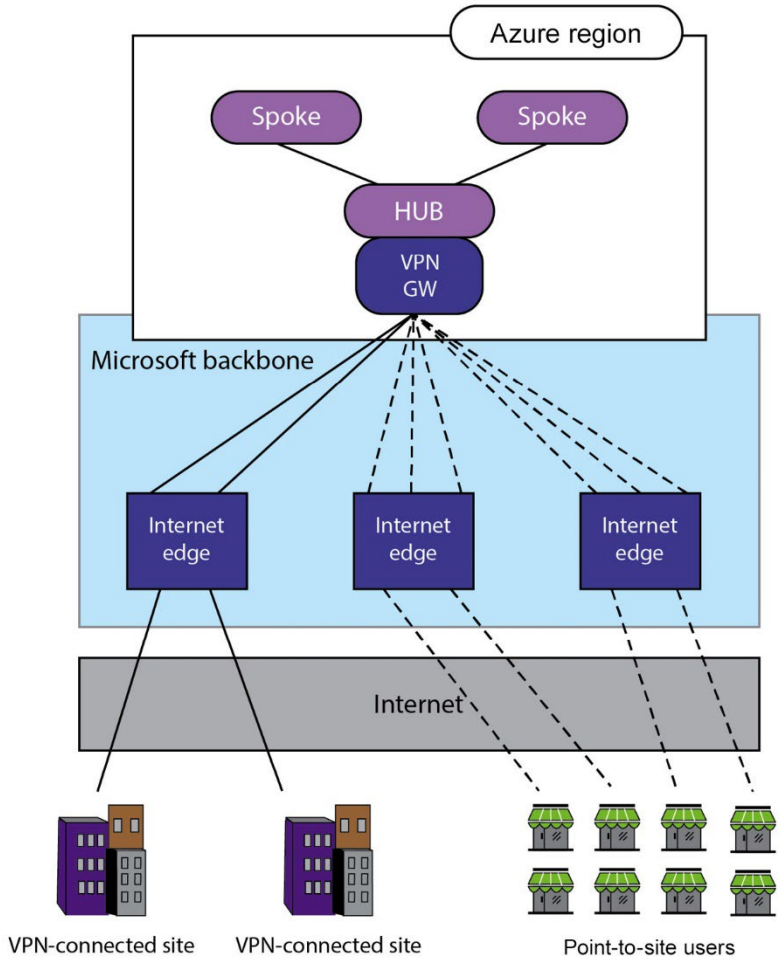


Figure 7.11: Secure connectivity from Azure to on-premises sites

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

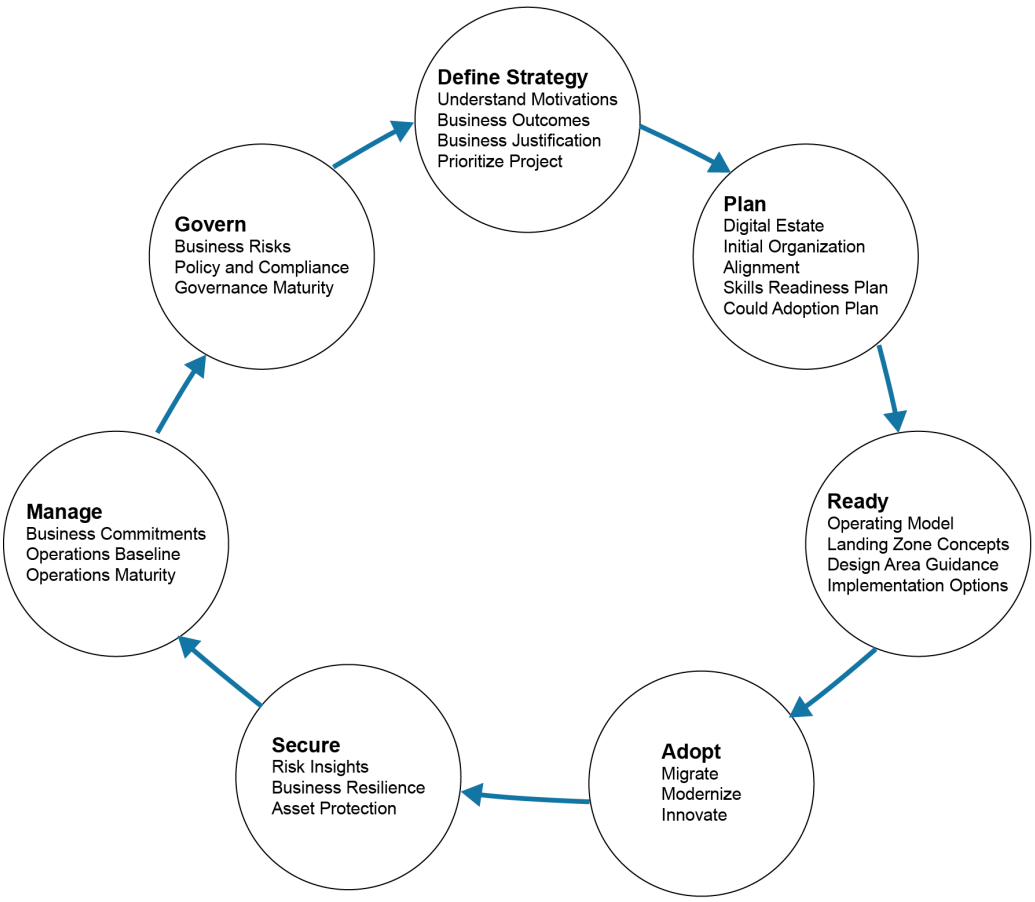


Figure 8.1 – CAF

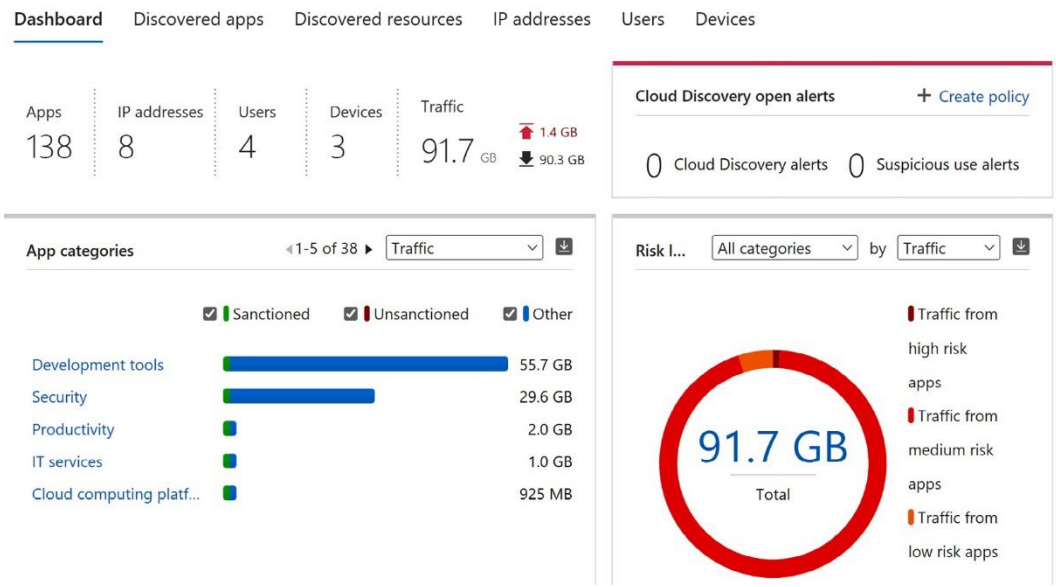


Figure 8.2 – The Microsoft Defender for Cloud Apps discovery dashboard

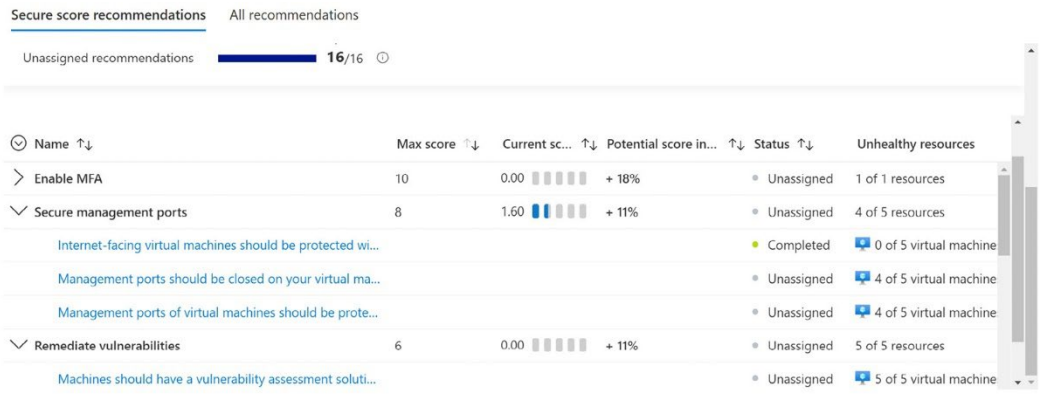


Figure 8.3 – Microsoft Defender for Cloud virtual machine security recommendations

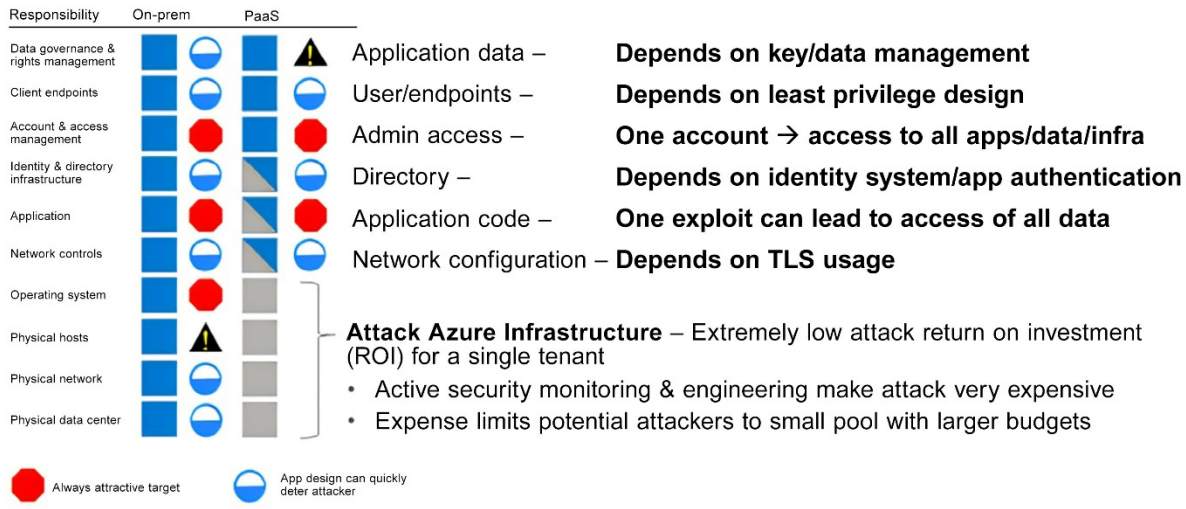


Figure 8.4 – Security controls for PaaS

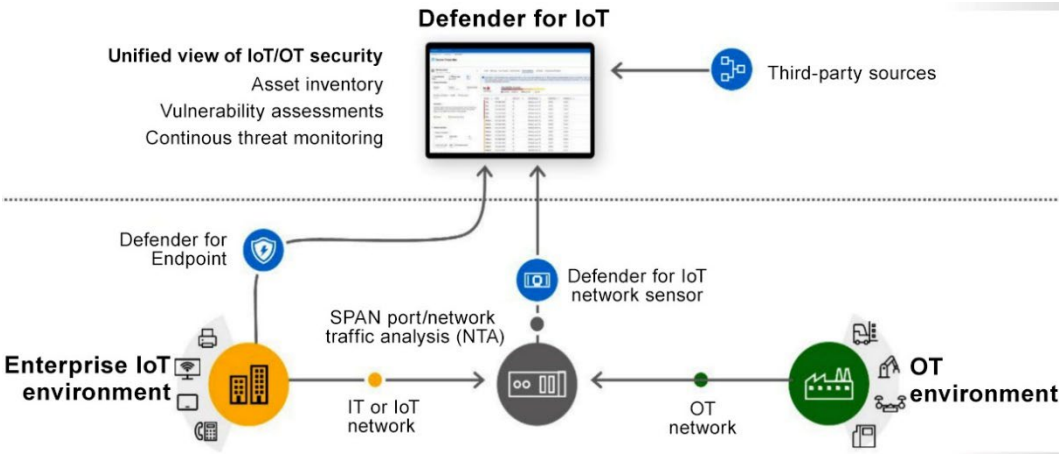


Figure 8.5 – Defender for IoT threat detection diagram

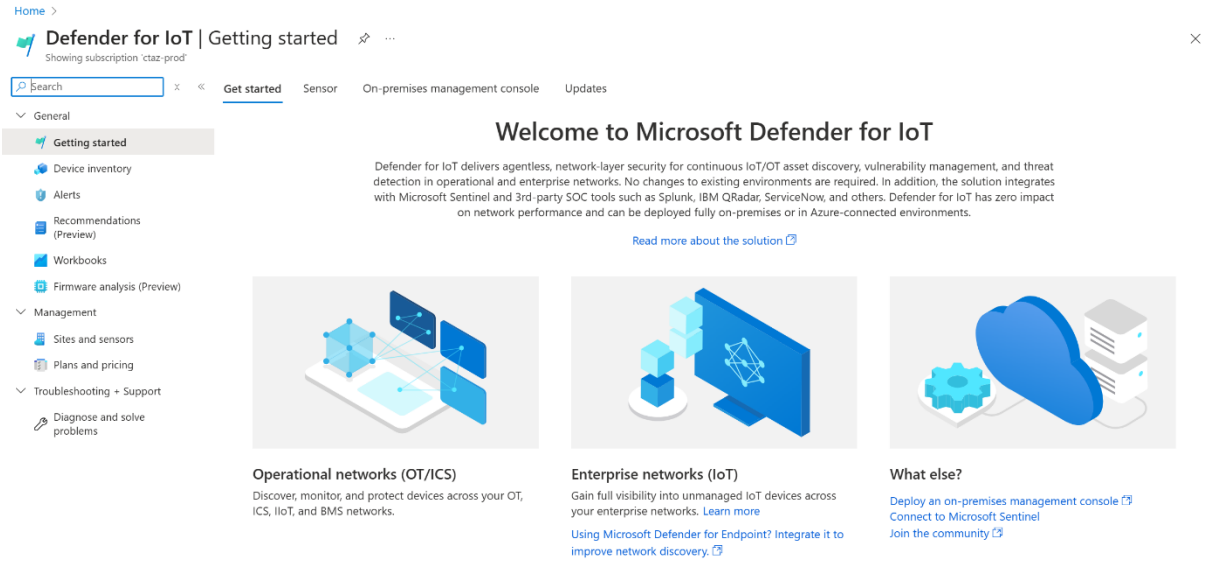


Figure 8.6 – Microsoft Defender for IoT getting started

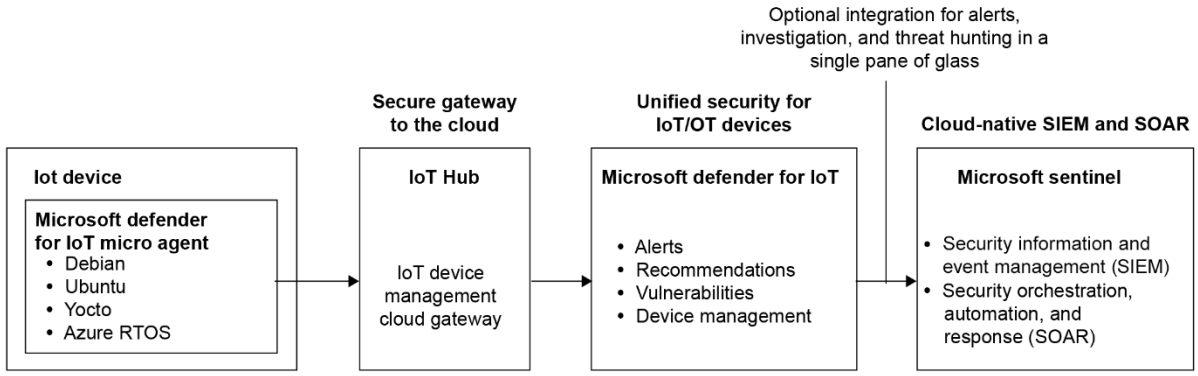


Figure 8.7 – Microsoft Defender for IoT micro agent architecture

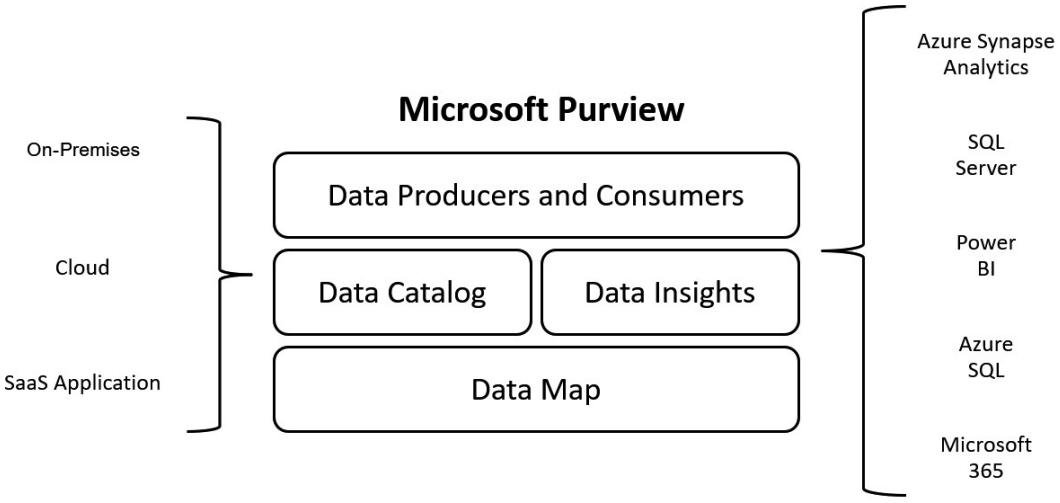


Figure 8.8 – Microsoft Purview data sources

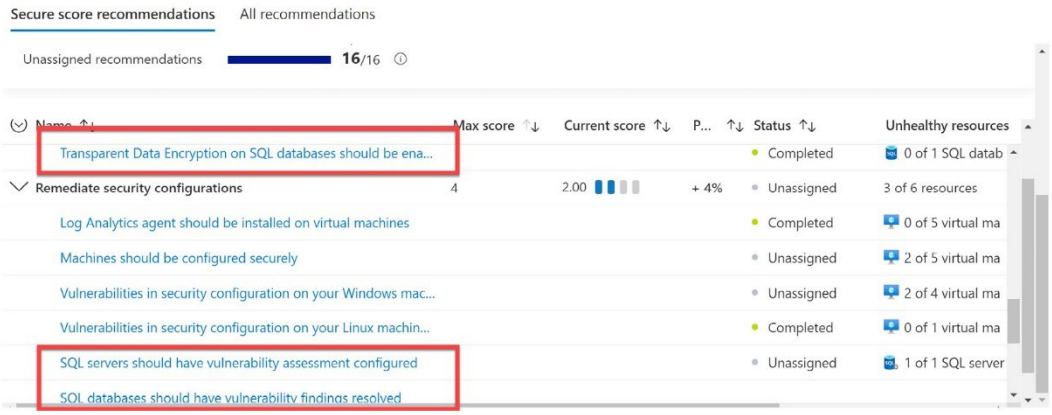


Figure 8.9 – Microsoft Defender for Cloud SQL security recommendations

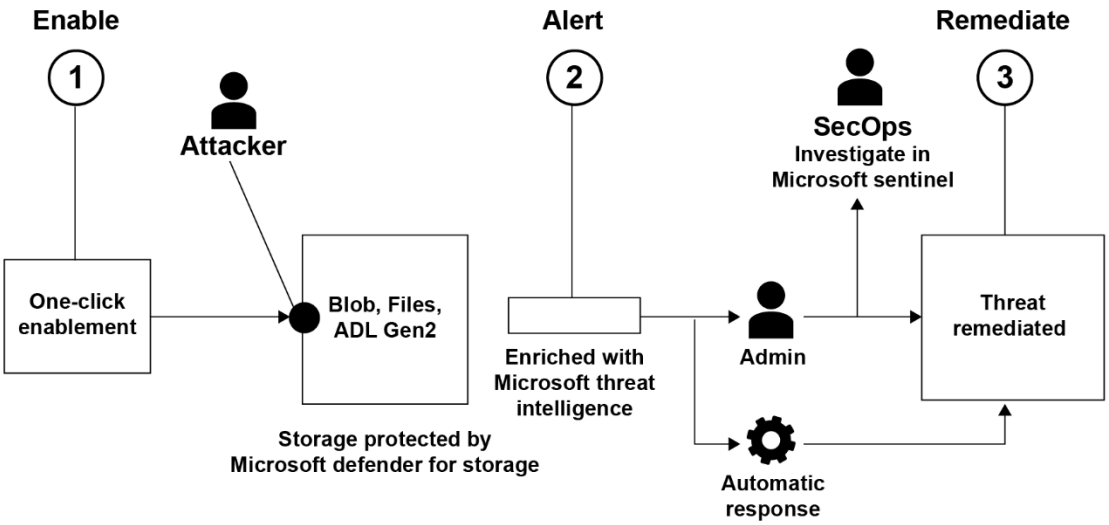


Figure 8.10 – Microsoft Defender for Storage threat protection

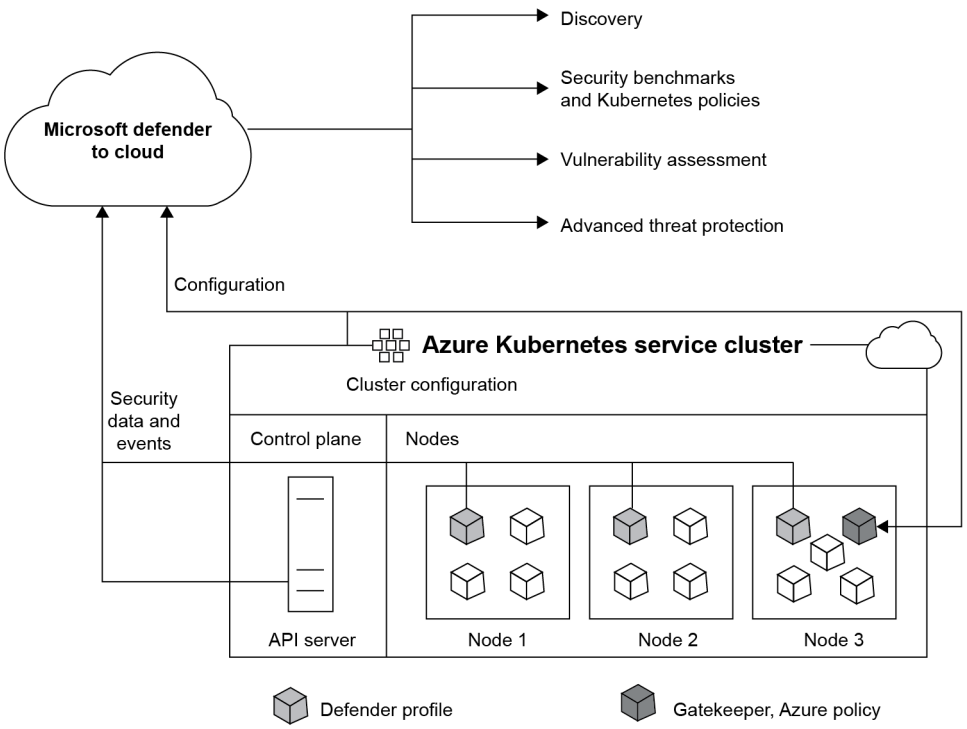


Figure 8.11 – Diagram illustrating the architecture of a cloud computing security system, specifically focusing on Microsoft Defender for Cloud integrated with an Azure Kubernetes Service (AKS) cluster

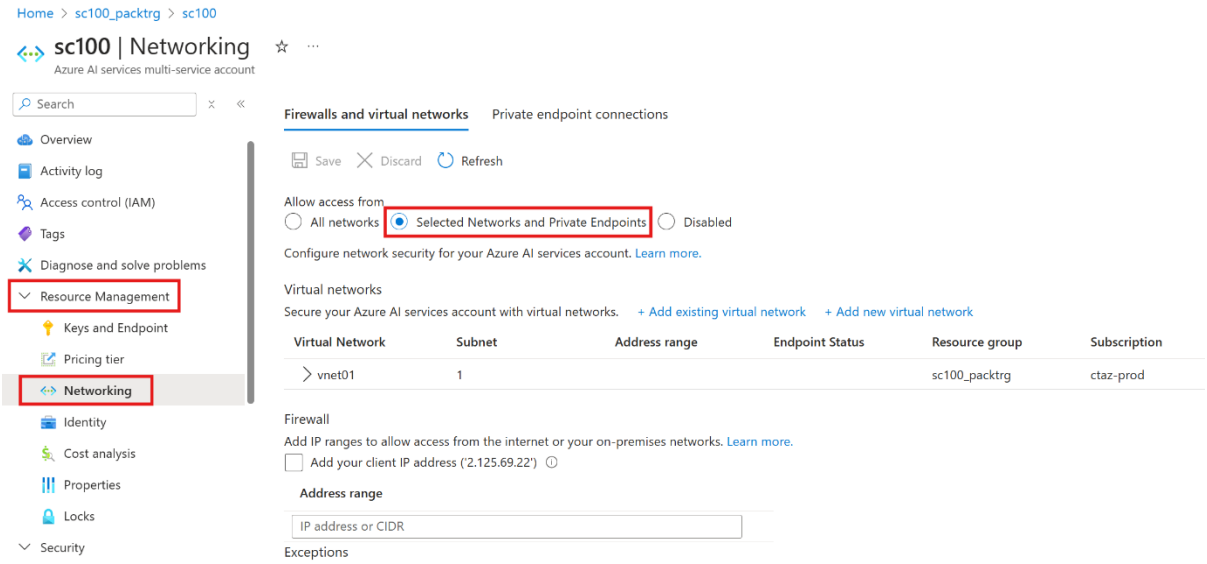


Figure 8.12 – Configuring network access for an Azure AI service in the Azure portal

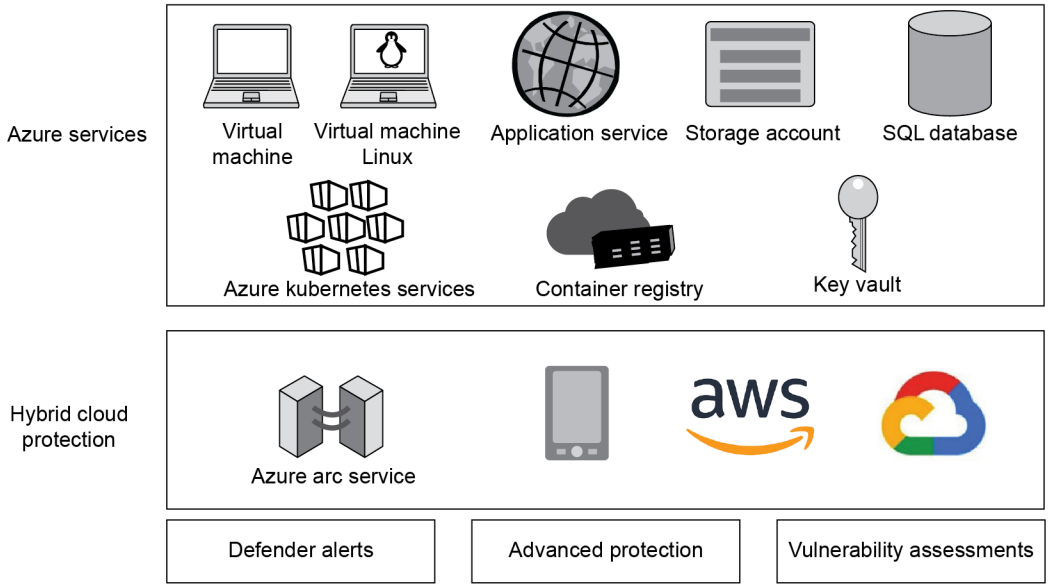


Figure 9.1: Microsoft Defender for Cloud workload protection plans

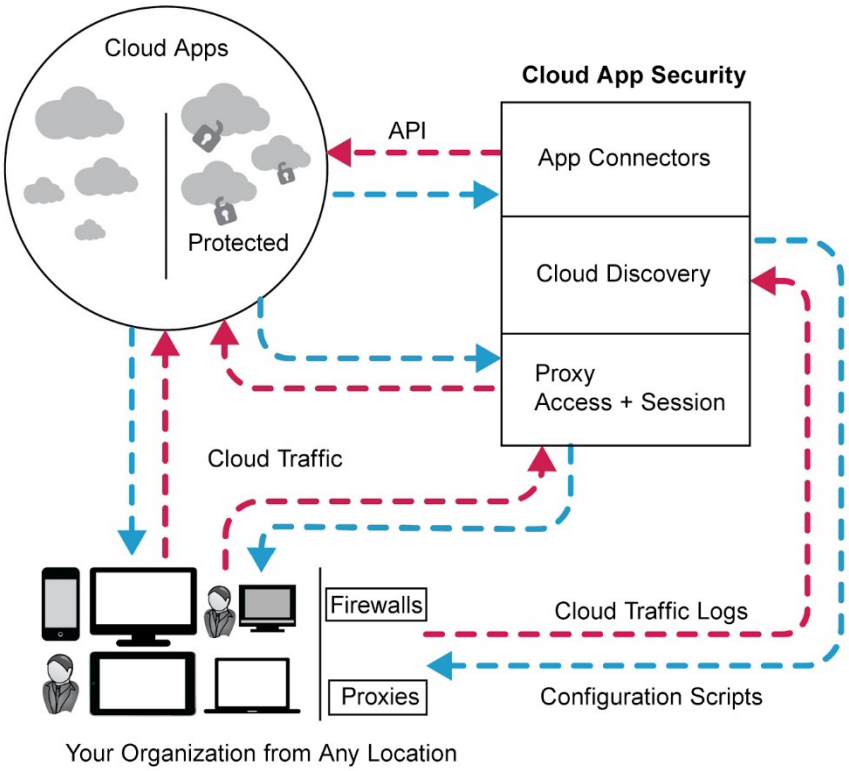


Figure 9.2: Microsoft Defender for Cloud Apps protection workflow

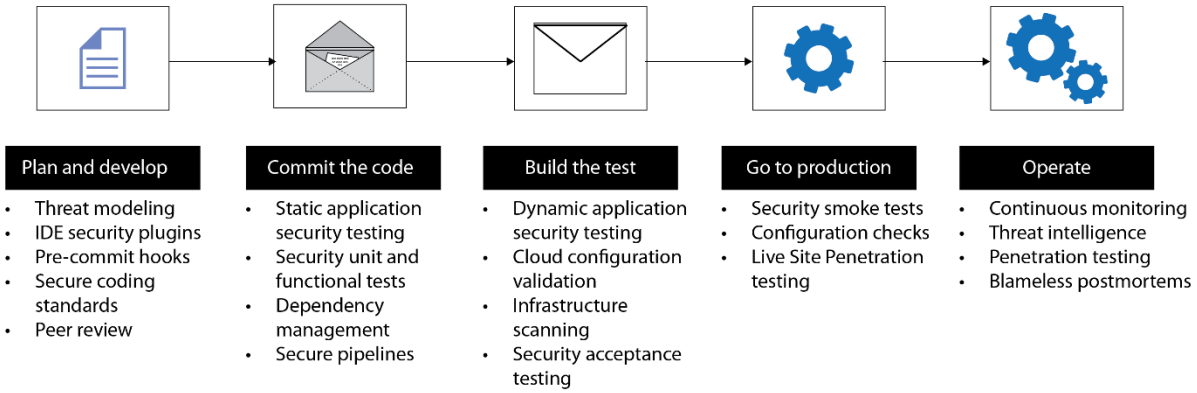


Figure 9.3: DevSecOps and the CAF

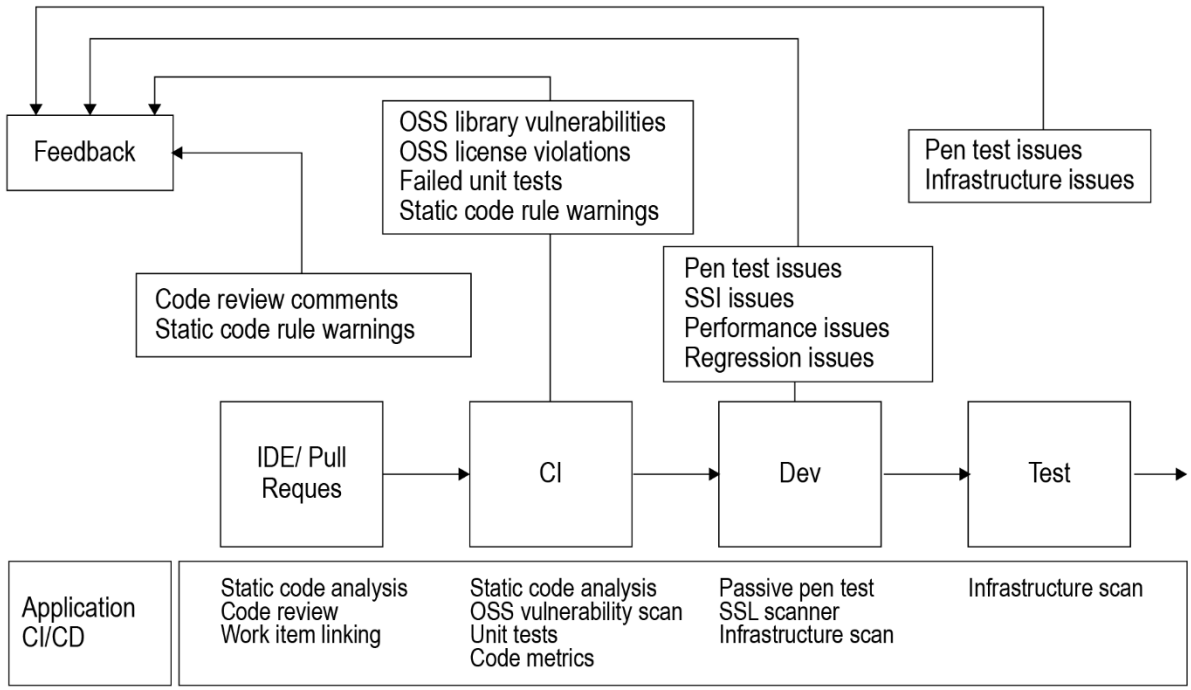


Figure 9.4: Continuous feedback loop

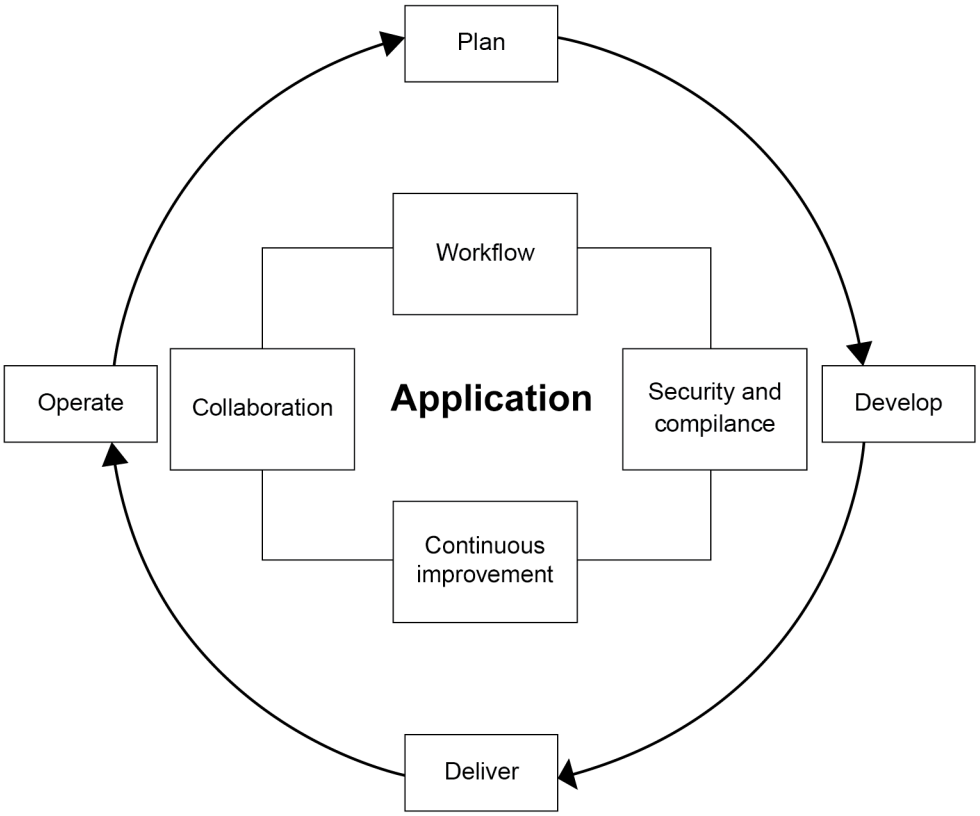


Figure 9.5: Continuous life cycle of DevSecOps

Figure 9.6: Devices sending data to data sources through APIs

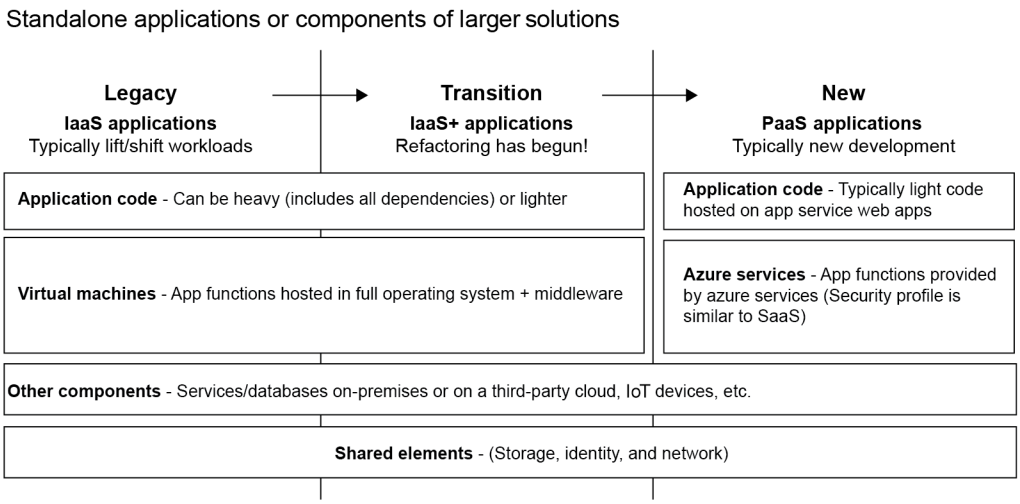


Figure 9.7: Application evolution to PaaS

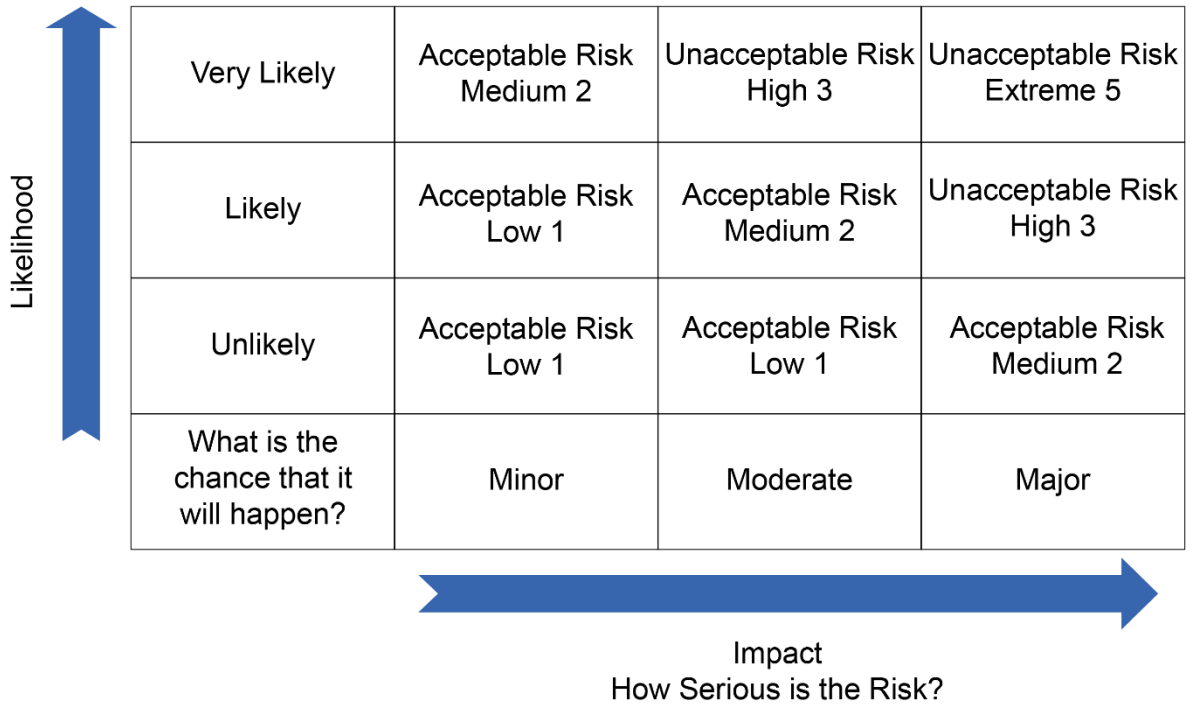


Figure 10.1: Risk assessment categorization

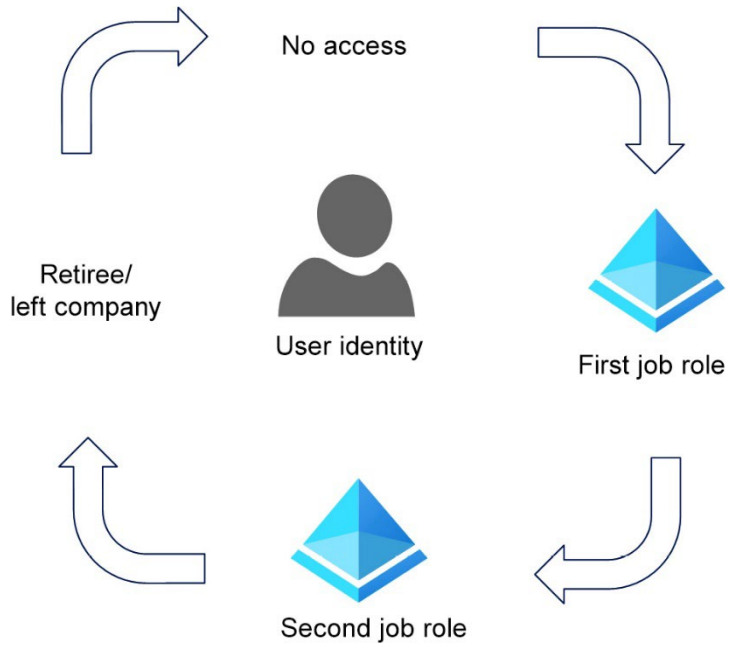


Figure 10.2: Identity governance life cycle

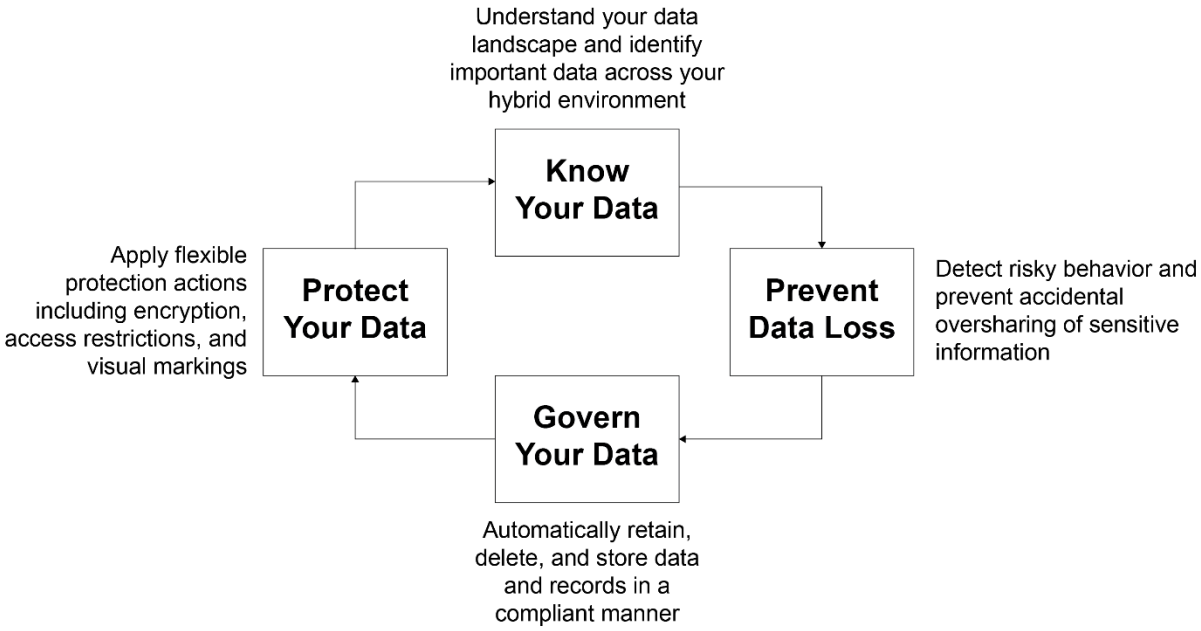


Figure 10.3: Zero-trust framework for data protection

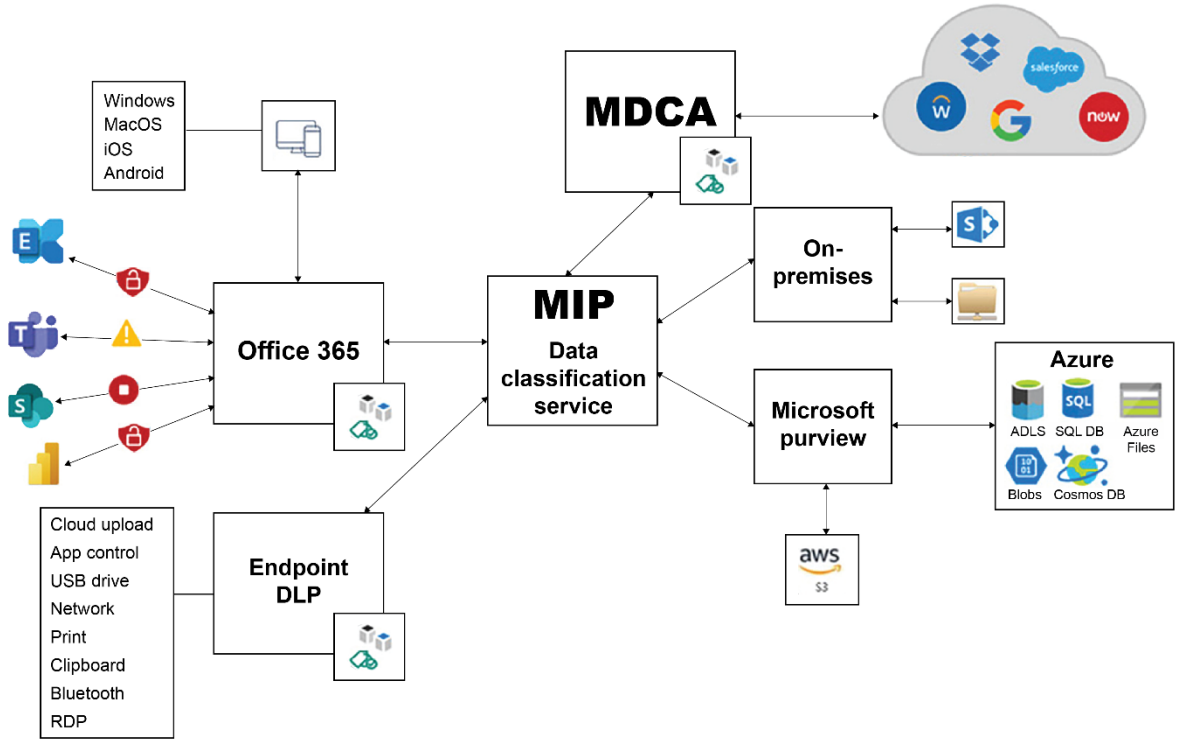


Figure 10.4: Microsoft Information Protection (MIP) workflow

Figure 10.5: Microsoft Defender for Cloud Apps workflow

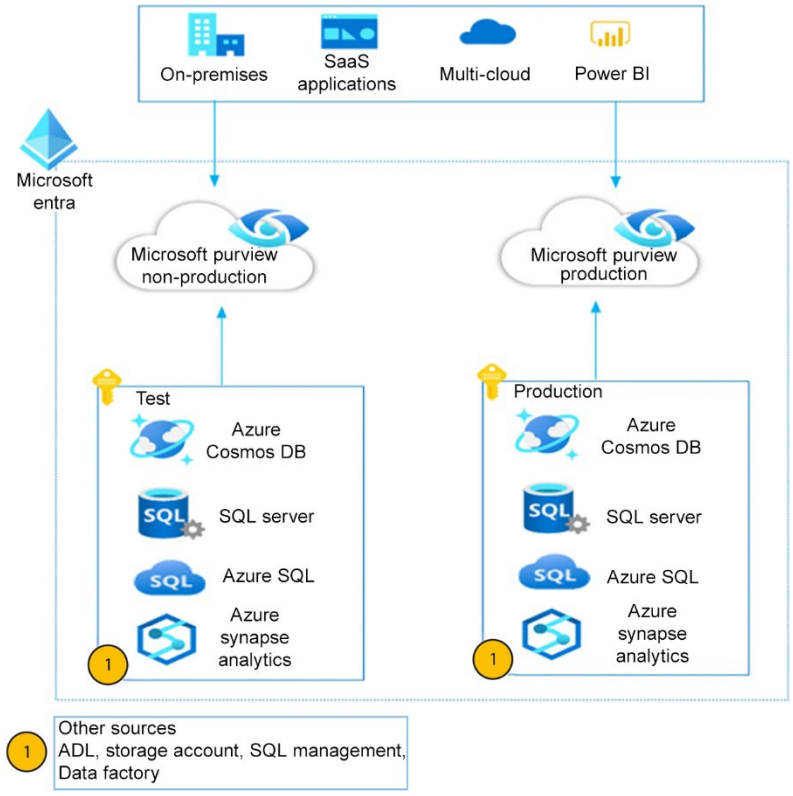


Figure 10.6: Database segmentation for production and non-production

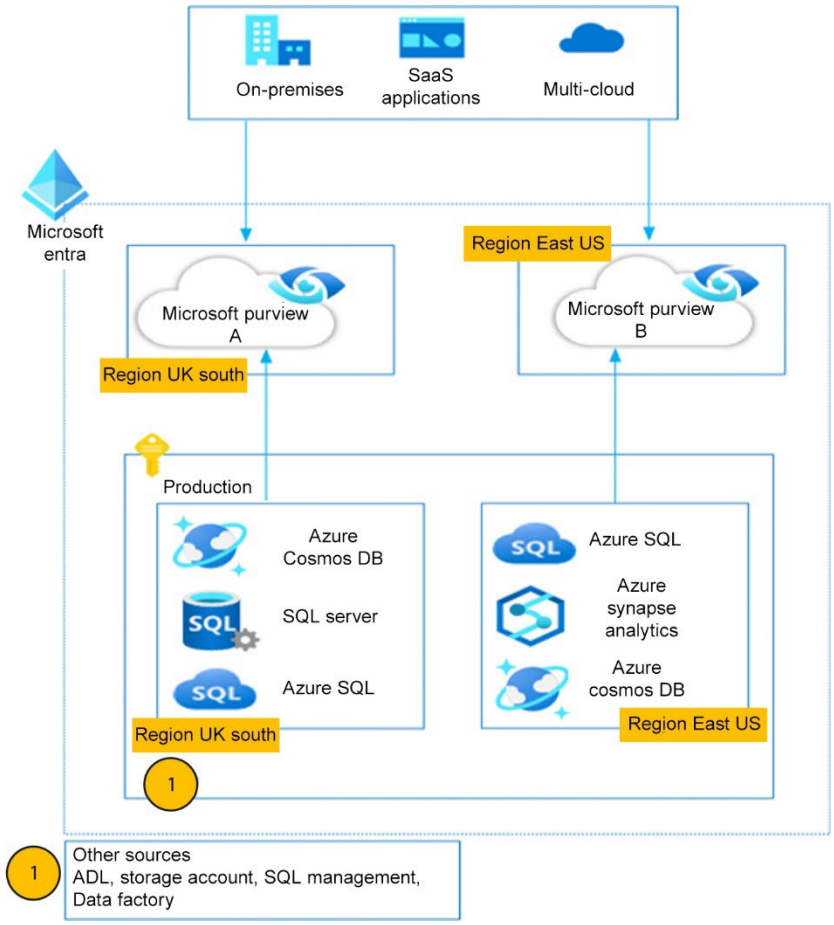


Figure 10.7: Using Microsoft Purview for data sovereignty

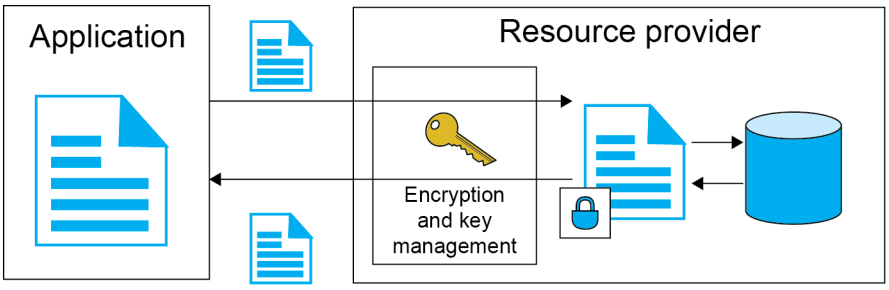


Figure 10.8: Accessing data encrypted at rest

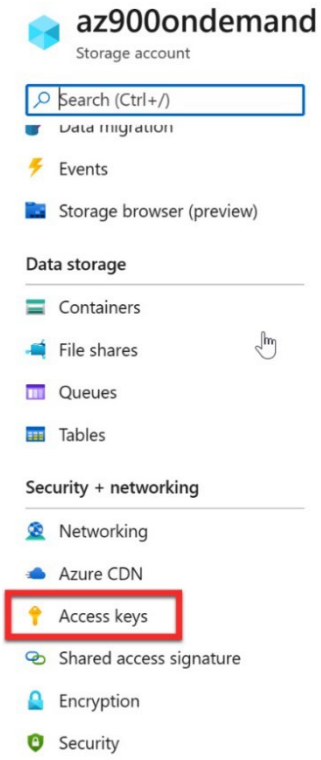


Figure 10.9: Storage account access keys

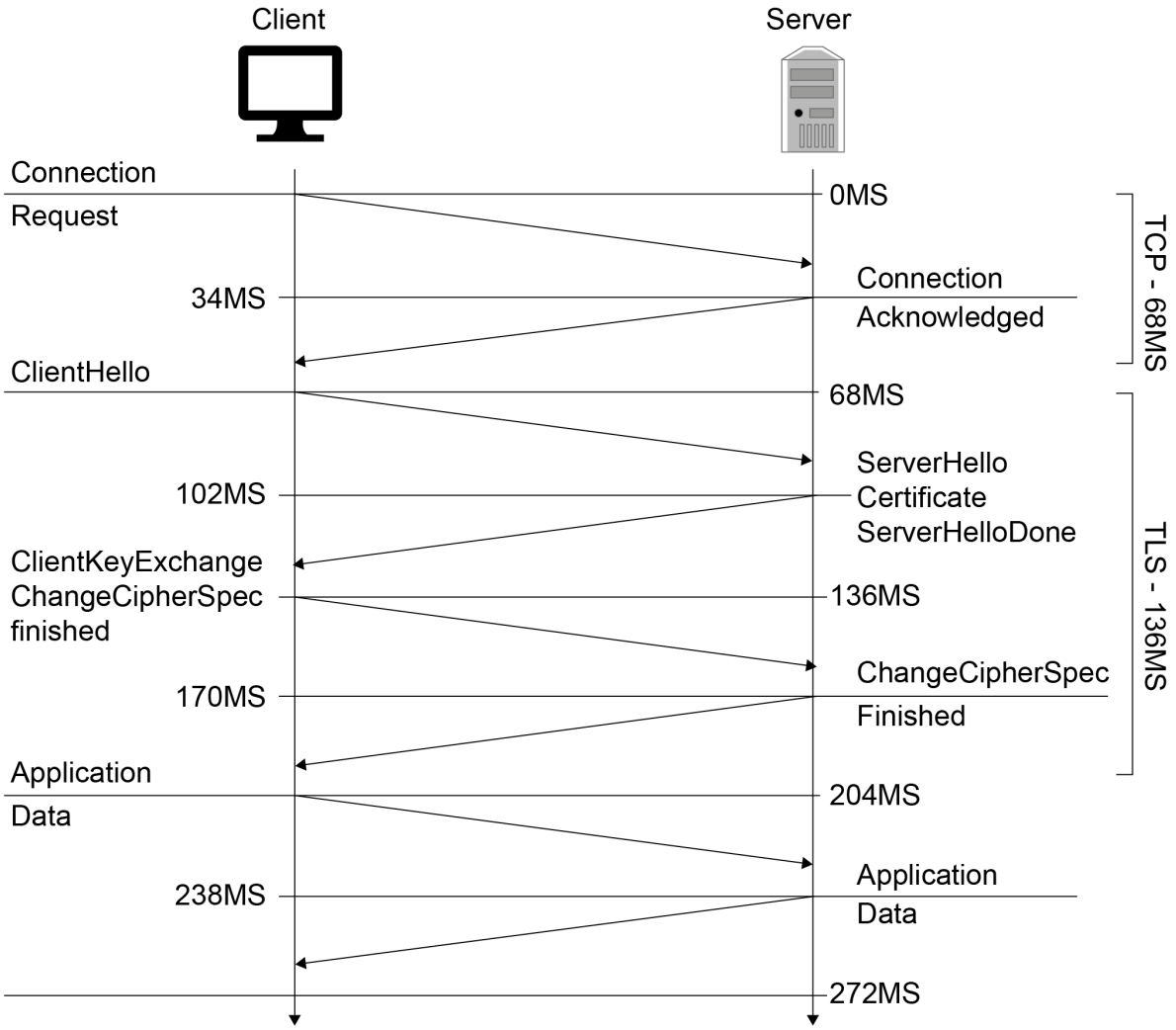


Figure 10.10: TLS 1.2 handshake process

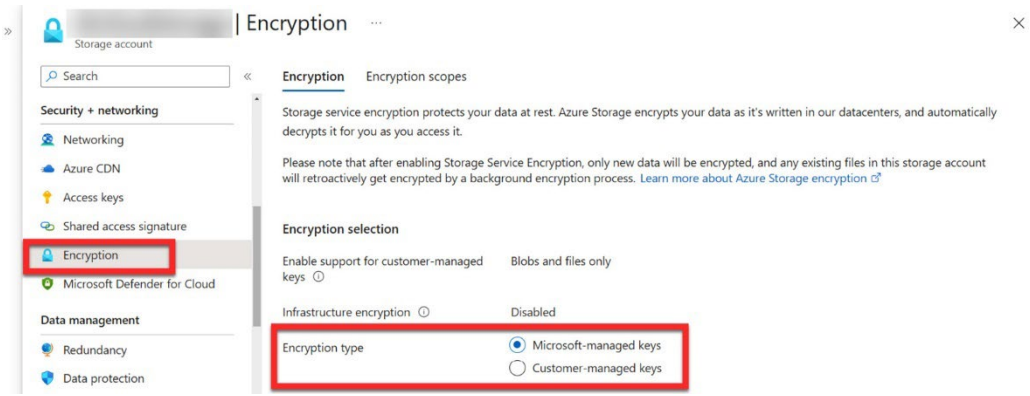


Figure 10.11: Configuring customer-managed keys with Azure Key Vault

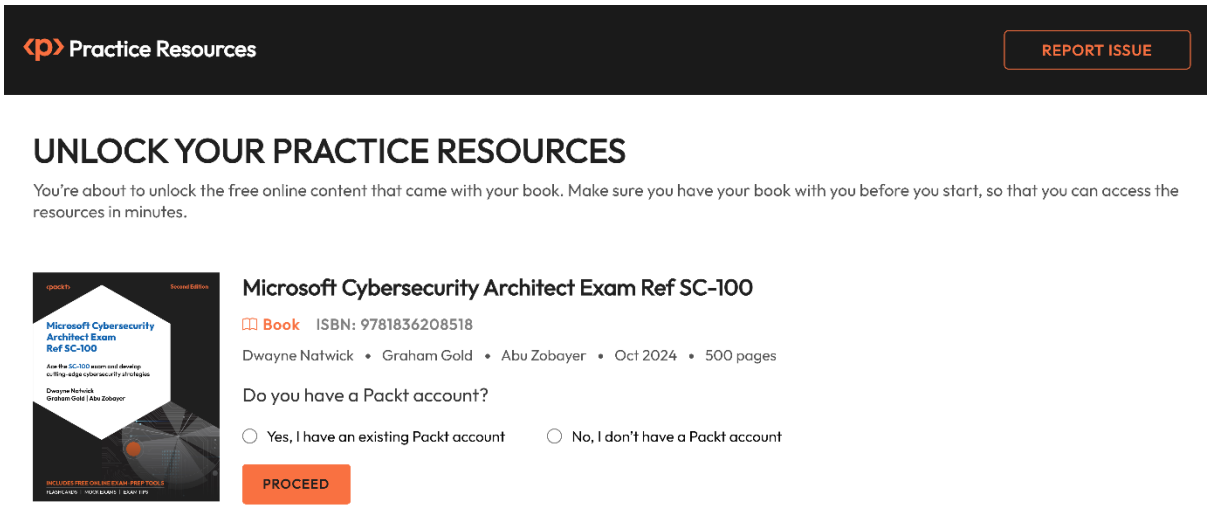


Figure 11.2: Unlock page for the online practice resources

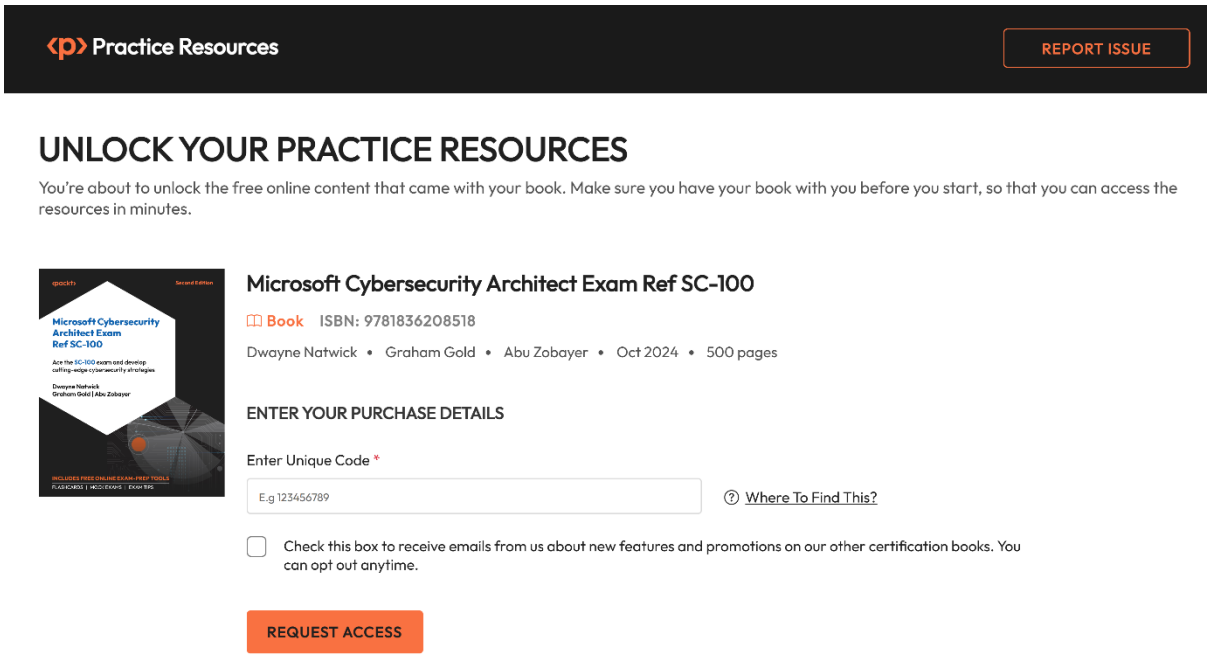


Figure 11.3: Enter your unique sign-up code to unlock the resources

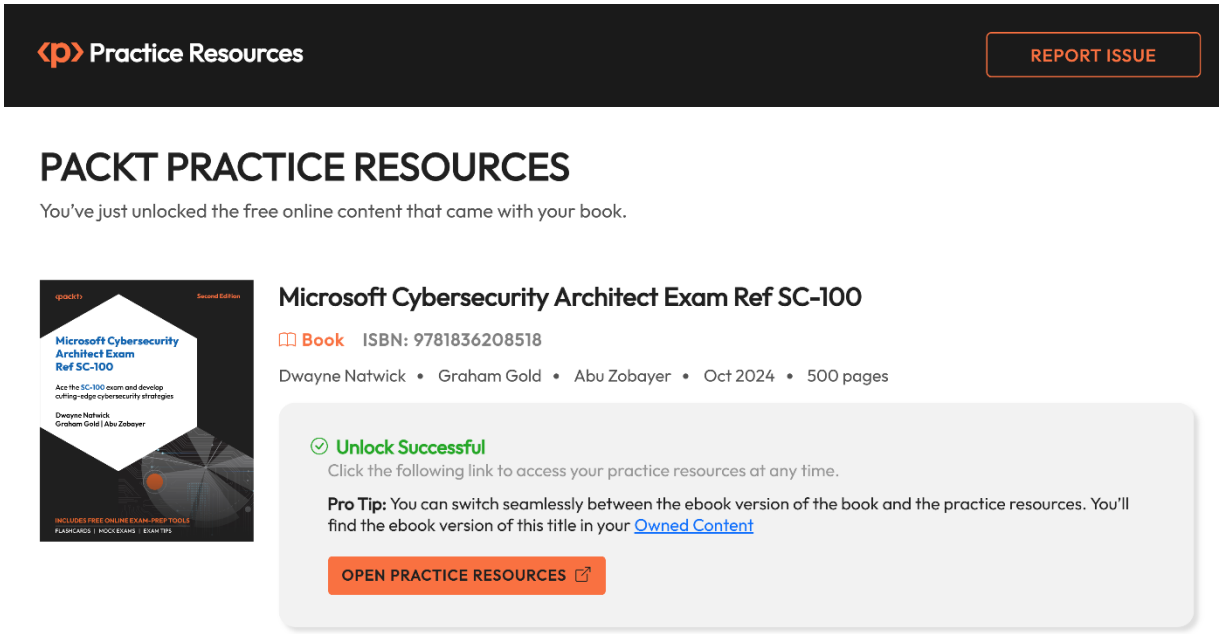


Figure 11.4: Page that shows up after a successful unlock

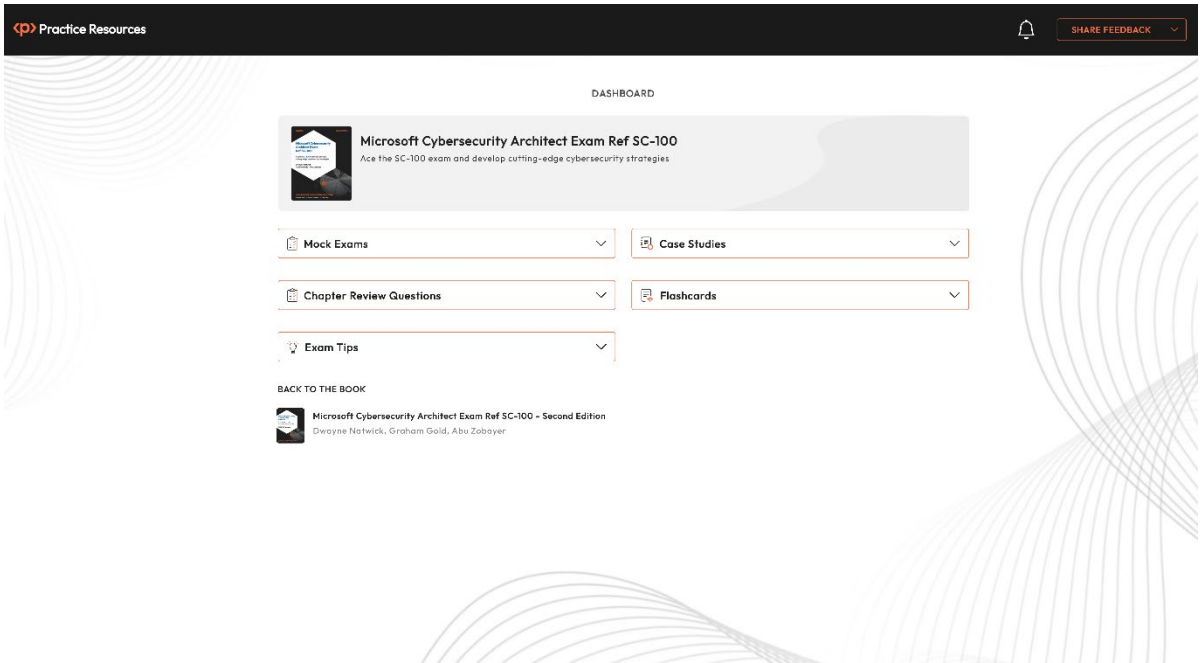


Figure 11.5: Dashboard page for SC-100 practice resources

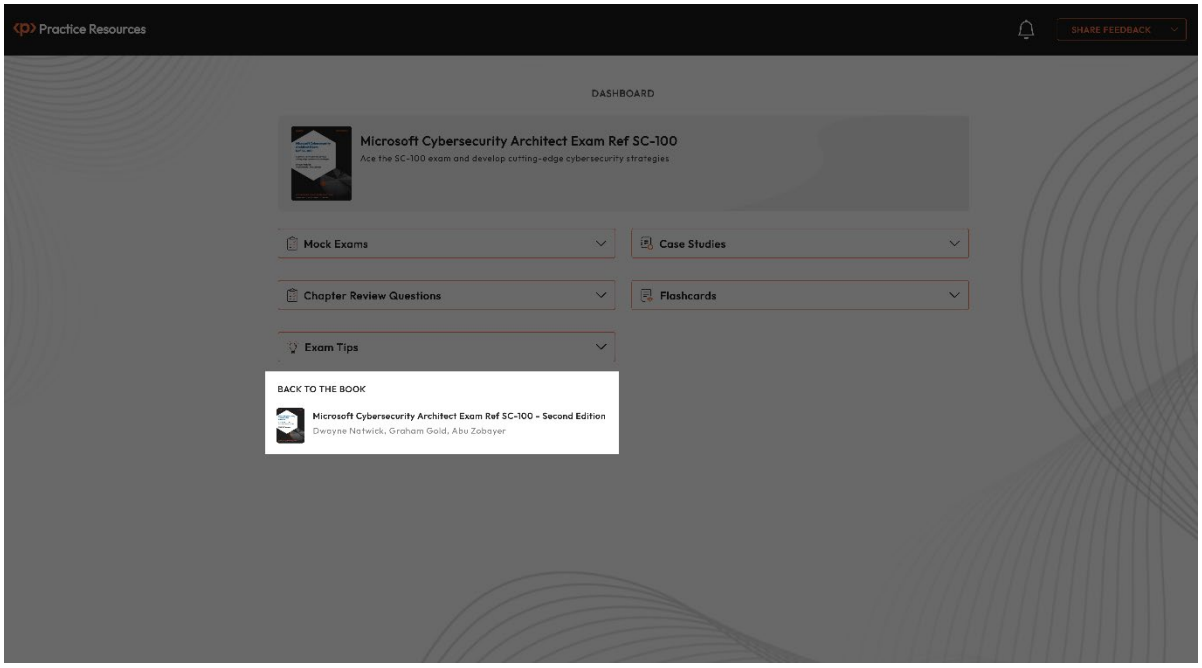


Figure 11.7: Dashboard page for SC-100 practice resources