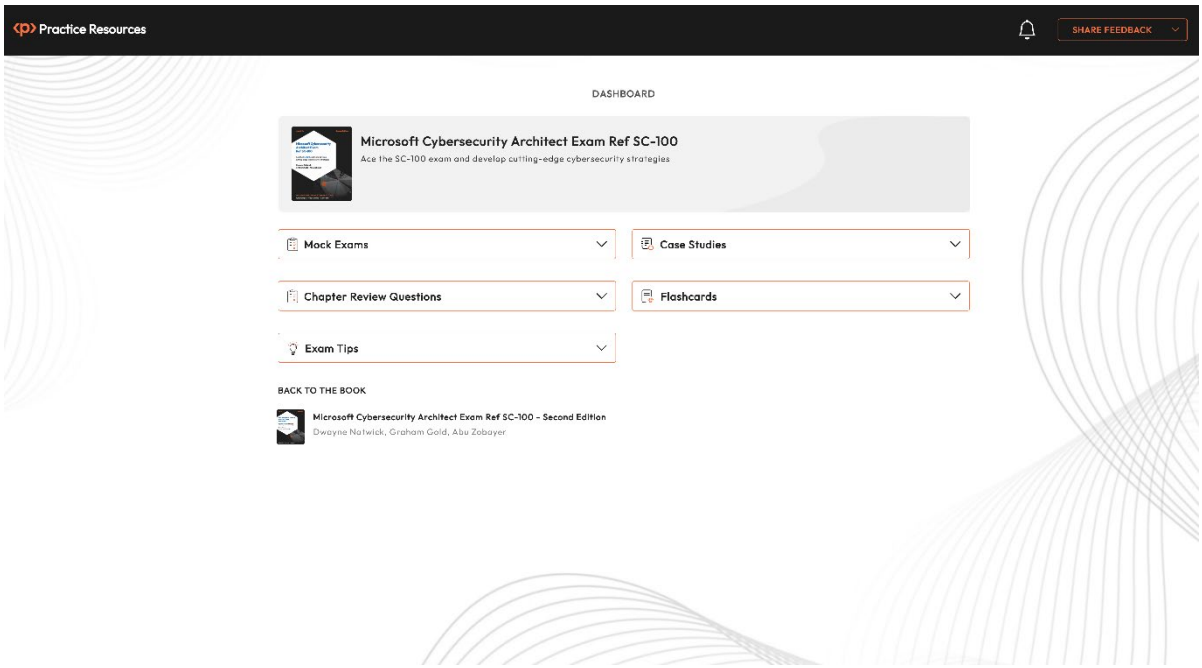
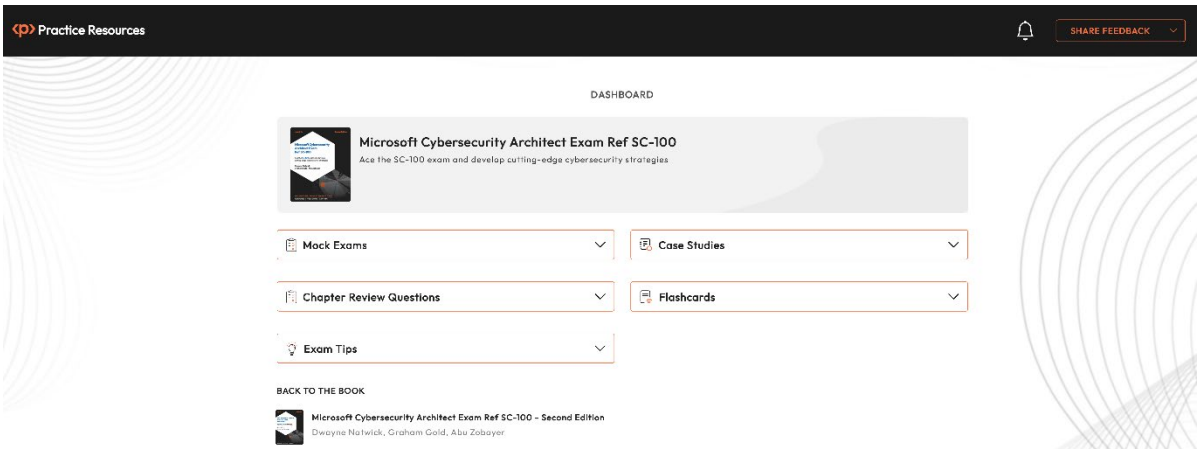
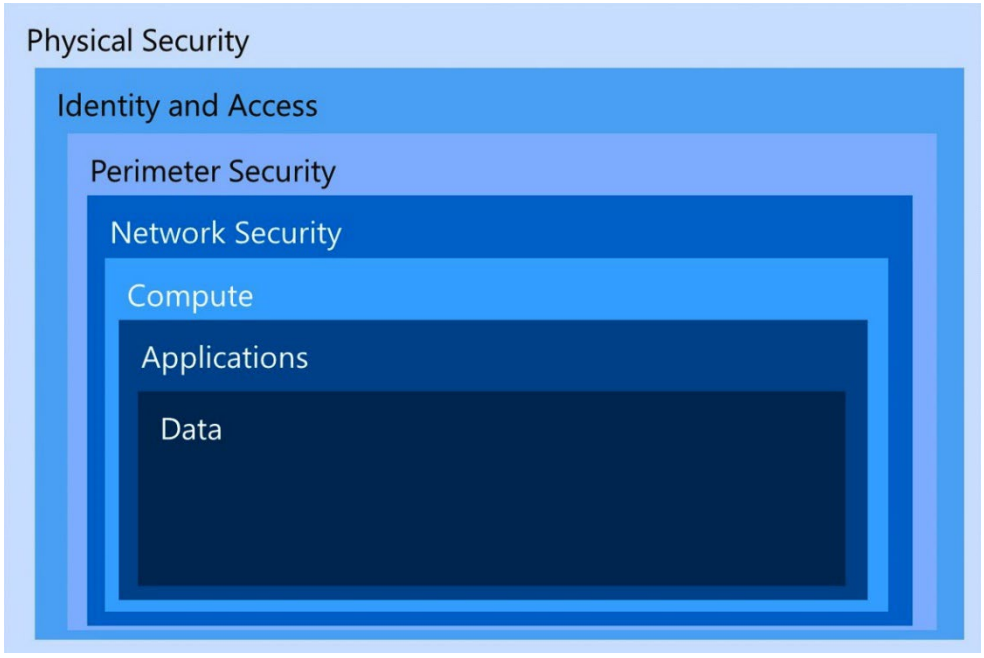
Microsoft Cybersecurity Architect Exam Ref SC-100, Second Edition

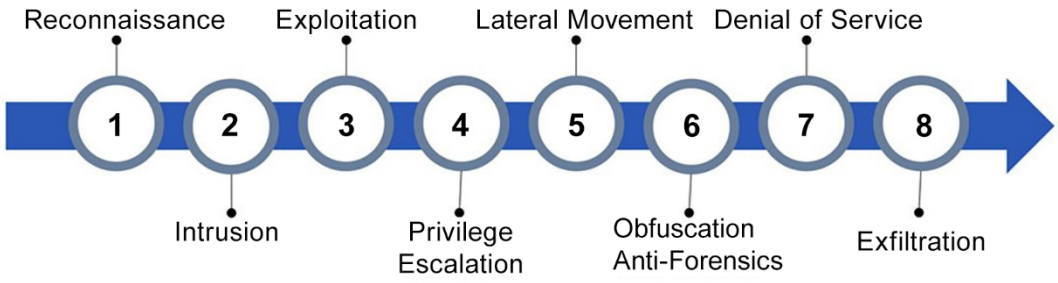
Preface:



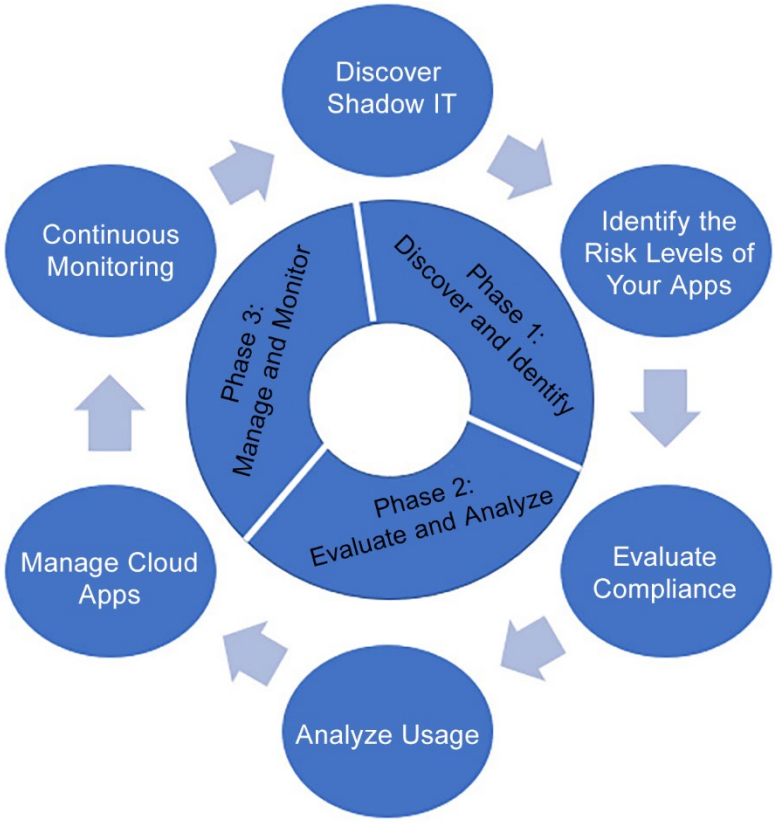
Chapter 1: Cybersecurity in the Cloud

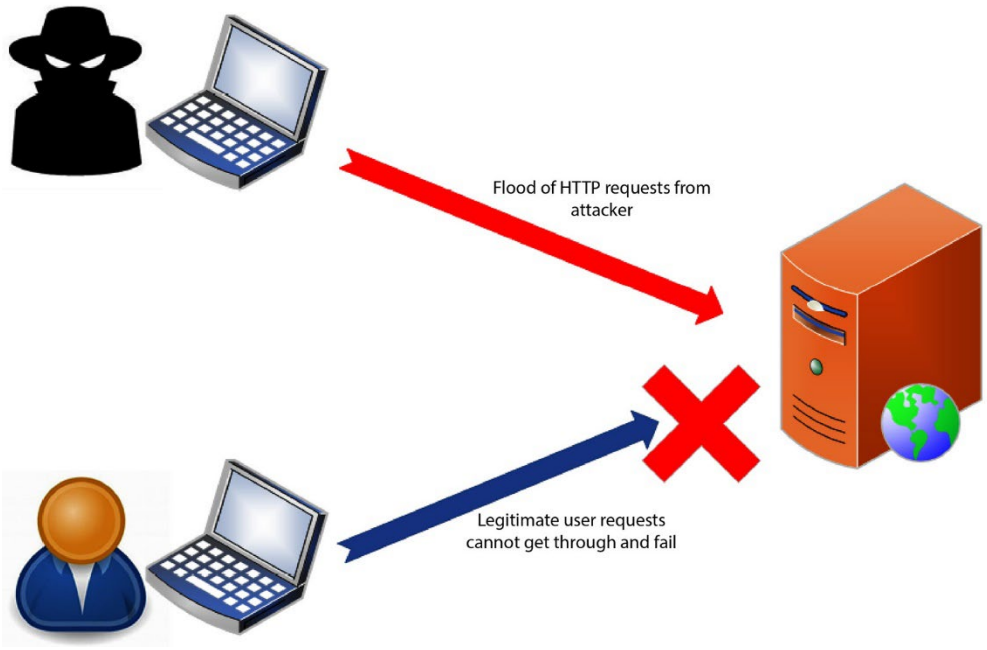


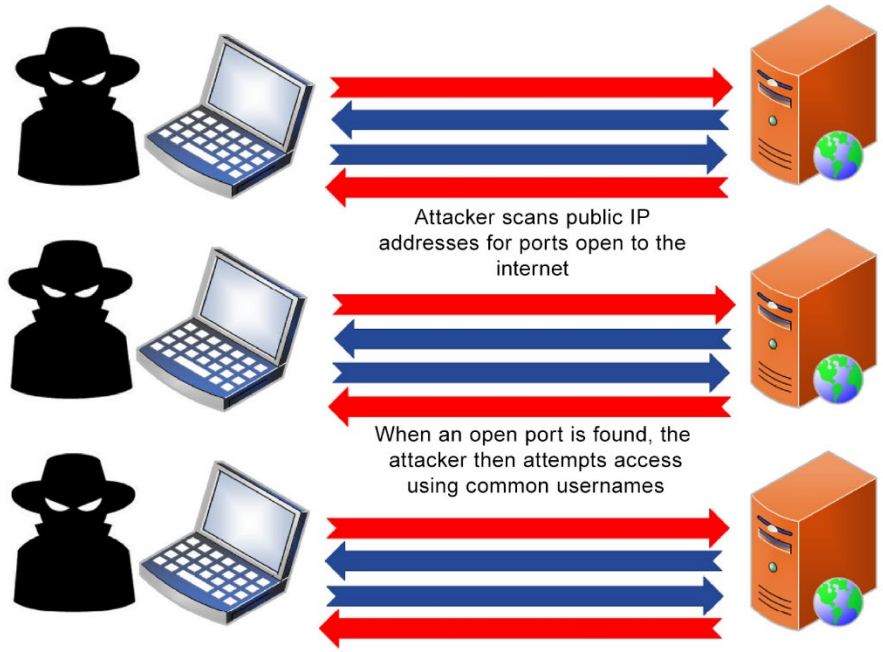


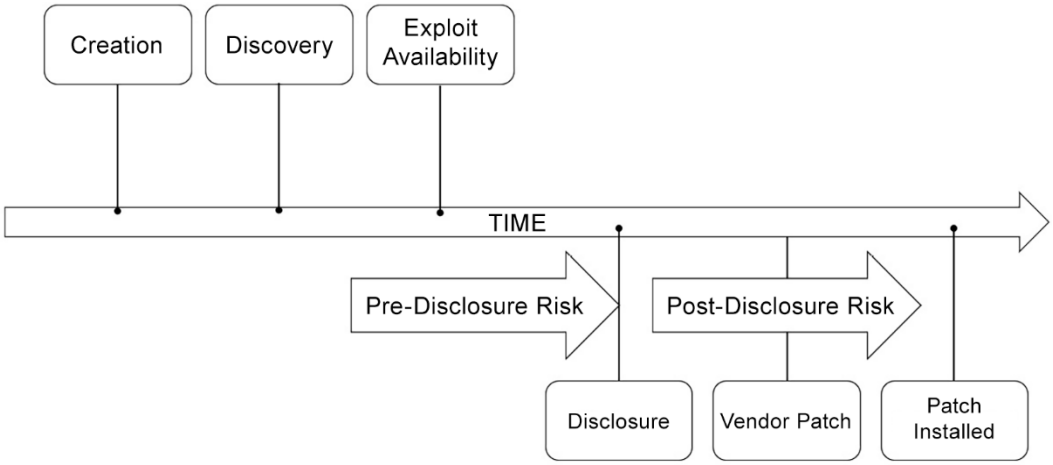


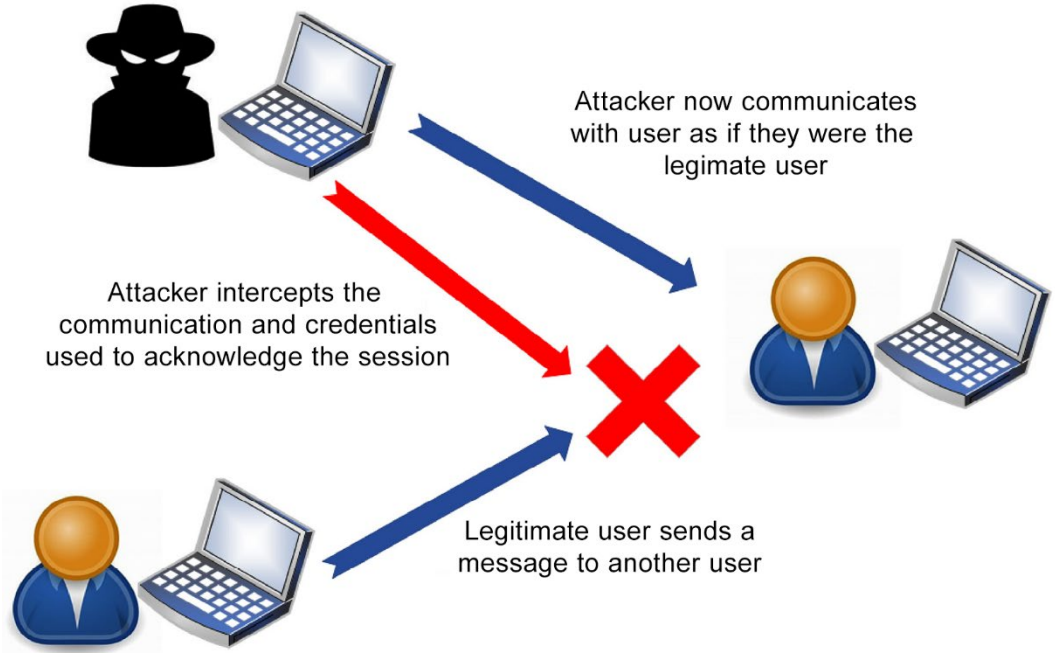

Signal
to make an informed decision
Decision
based on organizational policy
Enforcement
of the policy across resources

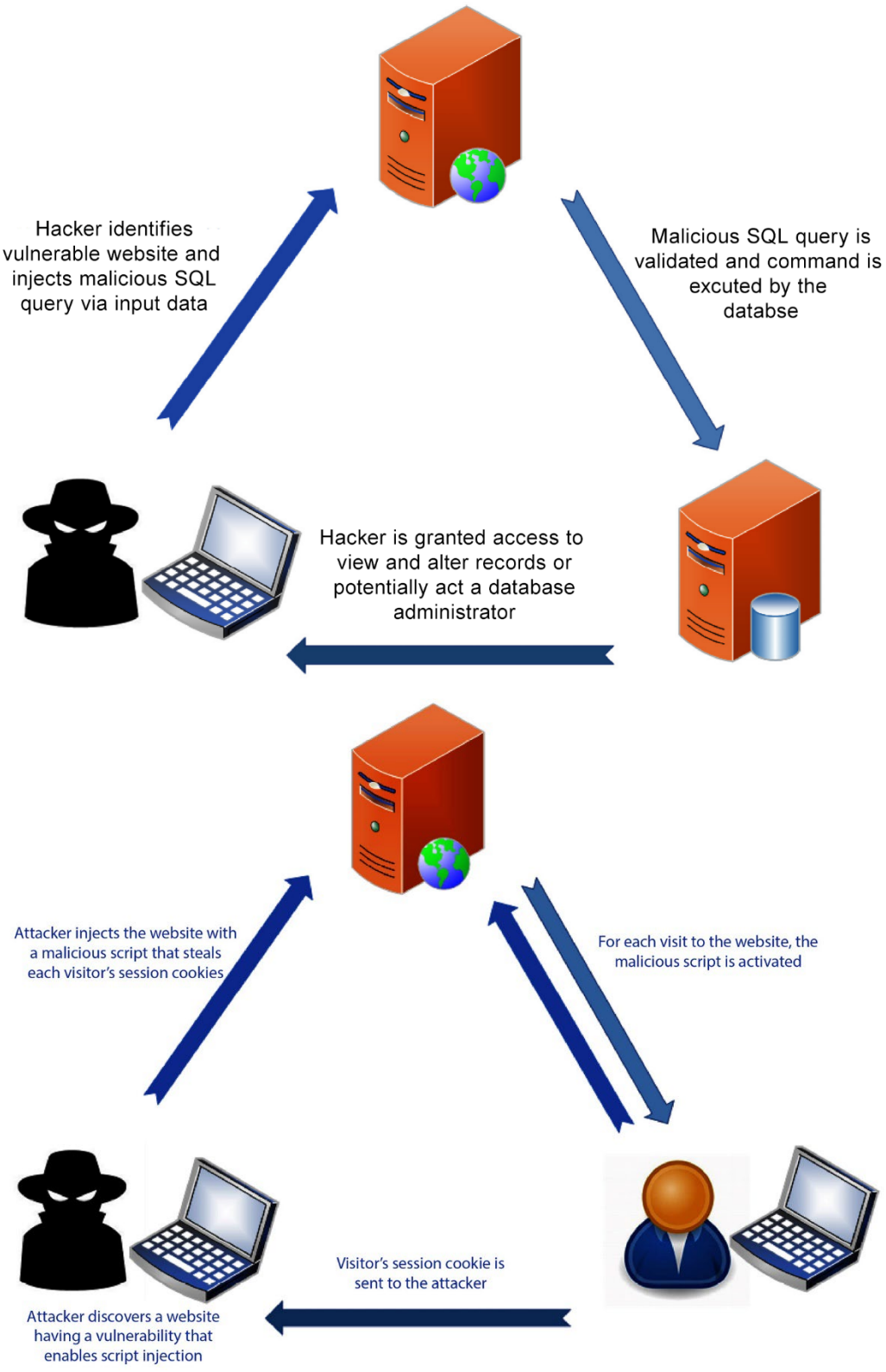

Discover Shadow IT
Identify the Risk Levels of Your Apps
Evaluate Compliance
Analyze Usage
Manage Cloud Apps
Continuous Monitoring
Phase 1: Discover and Identify
Phase 2: Evaluate and Analyze
Phase 3: Manage and Monitor

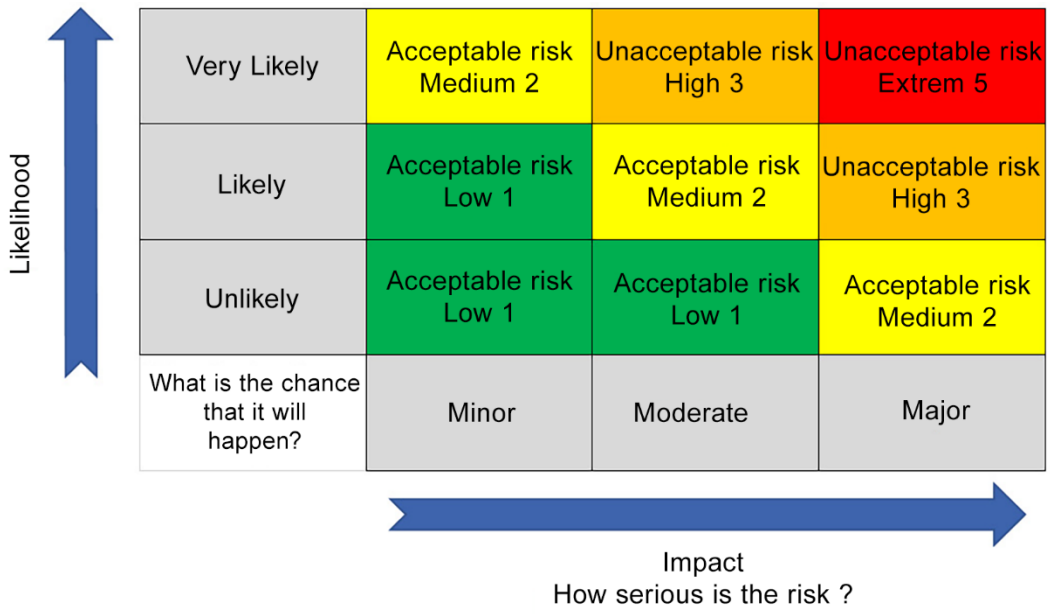

Flood of HTTP requests from attacker
Legitimate user requests cannot get through and fail


Attacker scans public IP addresses for ports open to the internet
When an open port is found, the attacker then attempts access using common usernames


Creation
Discovery
Exploit Availability
TIME
Pre-Disclosure Risk
Post-Disclosure Risk
Disclosure
Vendor Patch
Patch Installed


Attacker now communicates with user as if they were the legimate user
Attacker intercepts the communication and credentials used to acknowledge the session
Legitimate user sends a message to another user

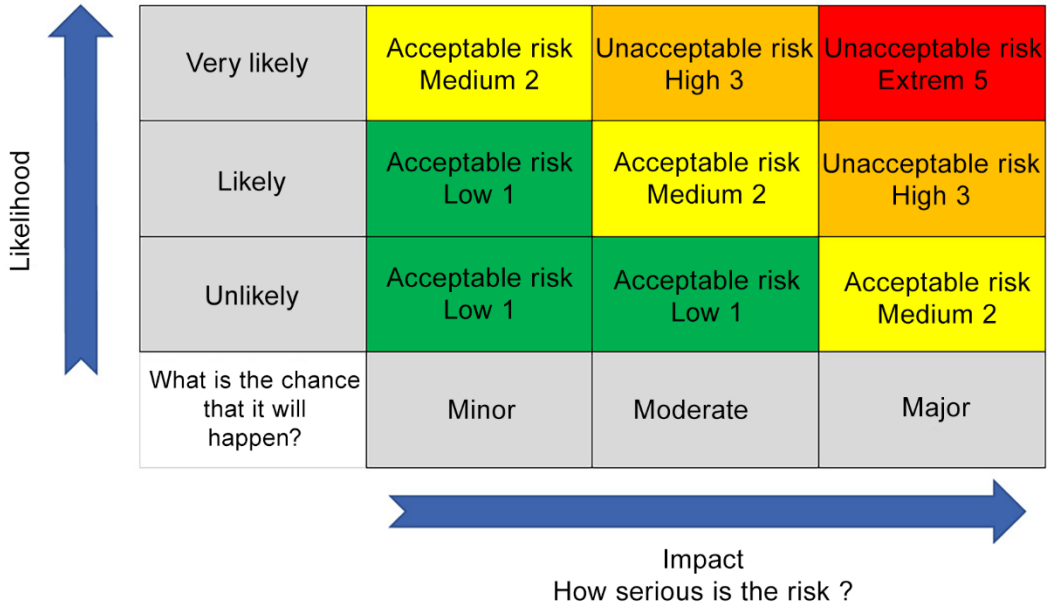

Hacker identifies vulnerable website and injects malicious SQL query via input data
Malicious SQL query is validated and command is excuted by the databse
Hacker is granted access to view and alter records or potentially act a database administrator
Attacker injects the website with a malicious script that steals each visitor's session cookies
For each visit to the website, the malicious script is activated
Visitor's session cookie is sent to the attacker
Attacker discovers a website having a vulnerability that enables script injection

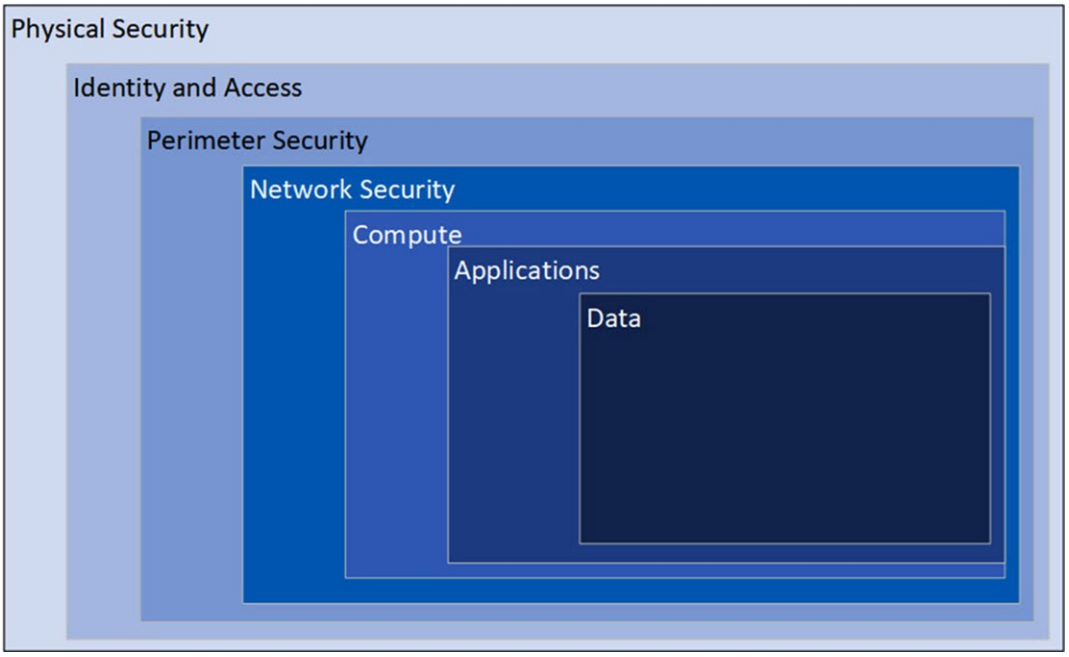

Likelihood
Very Likely
Acceptable risk Medium 2
Unacceptable risk High 3
Unacceptable risk Extrem 5
Likely
Acceptable risk Low 1
Acceptable risk Medium 2
Unacceptable risk High 3
Unlikely
Acceptable risk Low 1
Acceptable risk Low 1
Acceptable risk Medium 2
What is the chance that it will happen?
Minor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

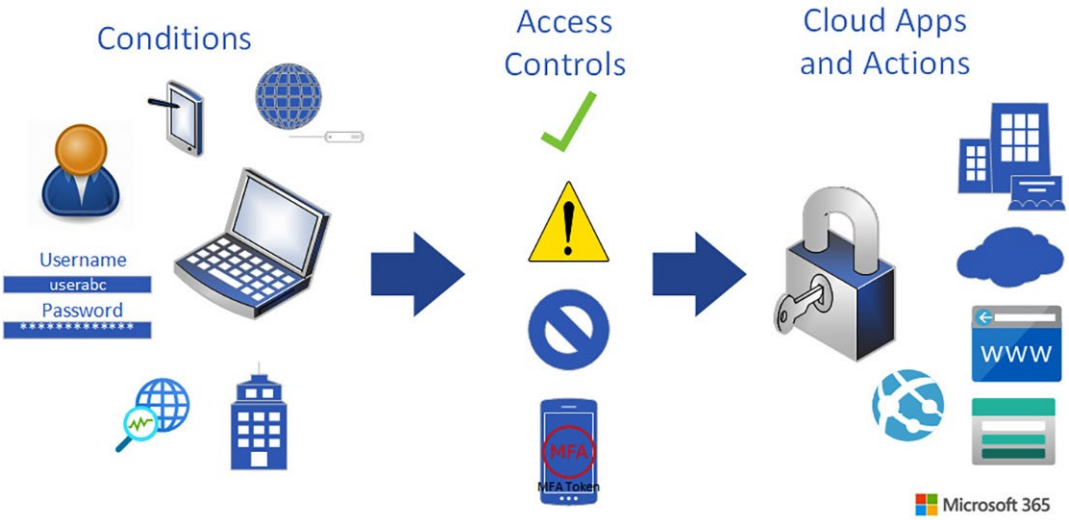
Chapter 2: Build an Overall Security Strategy and Architecture

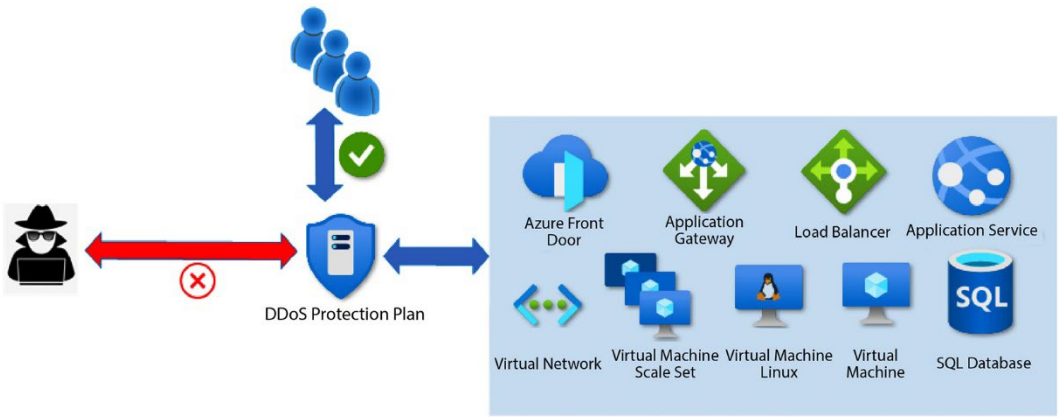
Microsoft Cybersecurity Reference Architecture (MCRA)

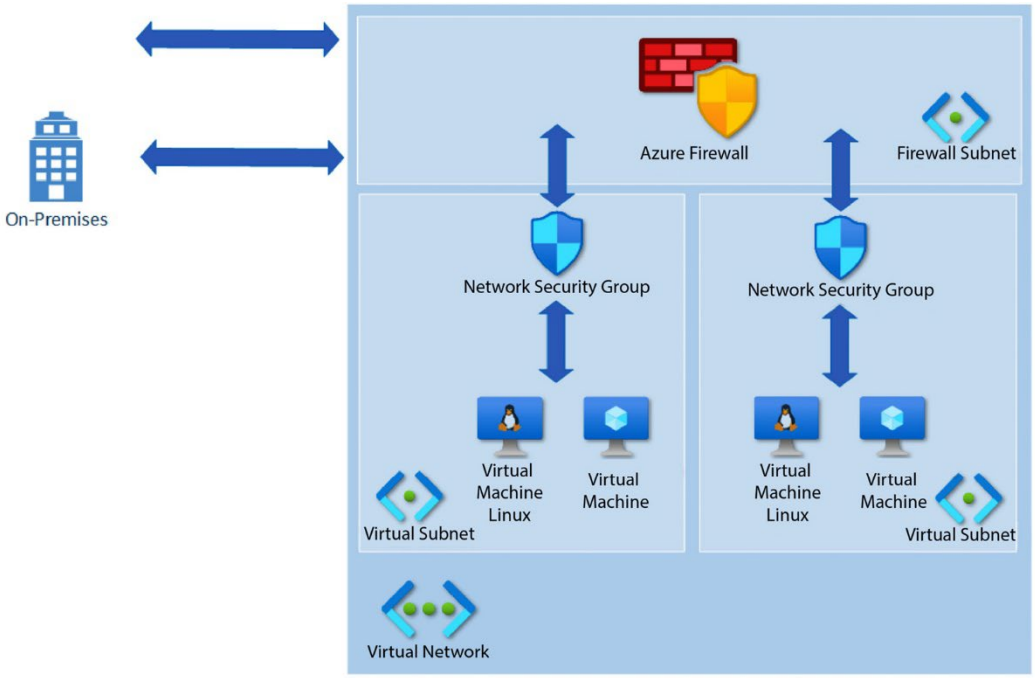
Capabilities	Azure Native Controls	People
Zero-Trust User Access	Security Operations	Multi-Cloud and Cross-Platform
Secure Access Service Edge (SASE)	Attack Chain Coverage	Operational Technology

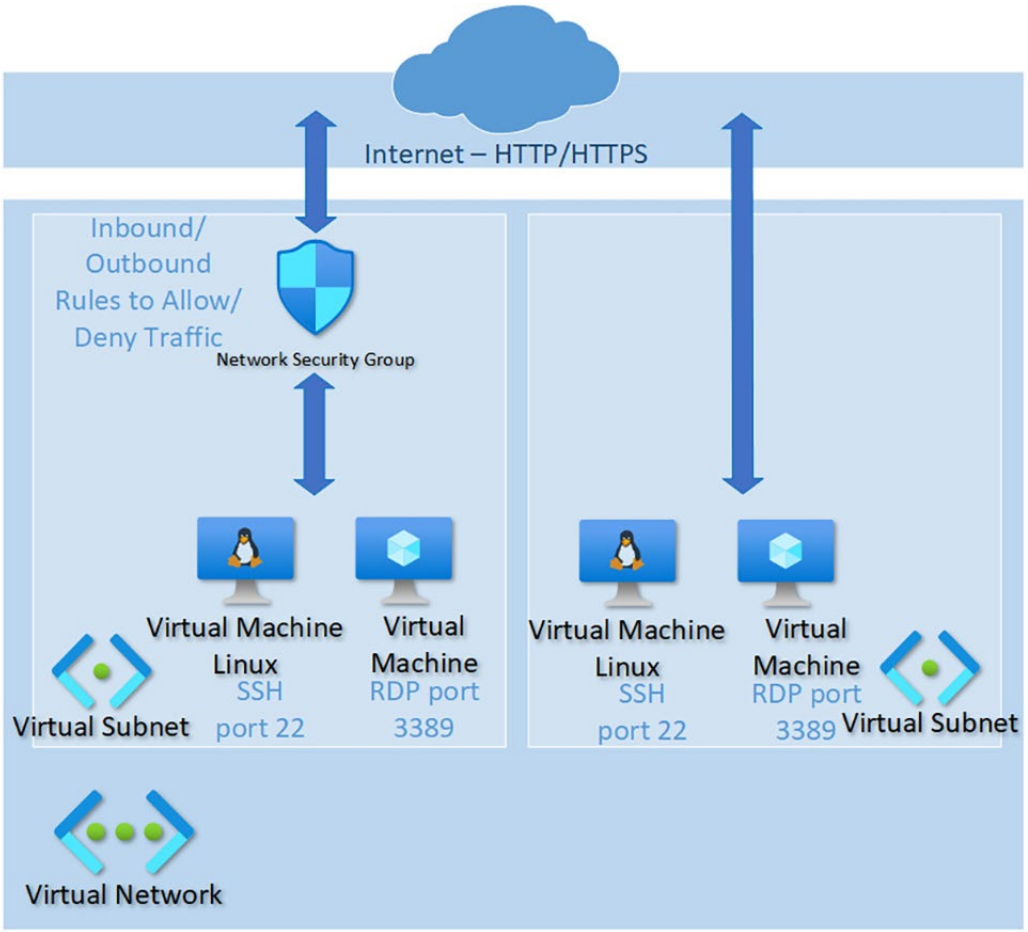


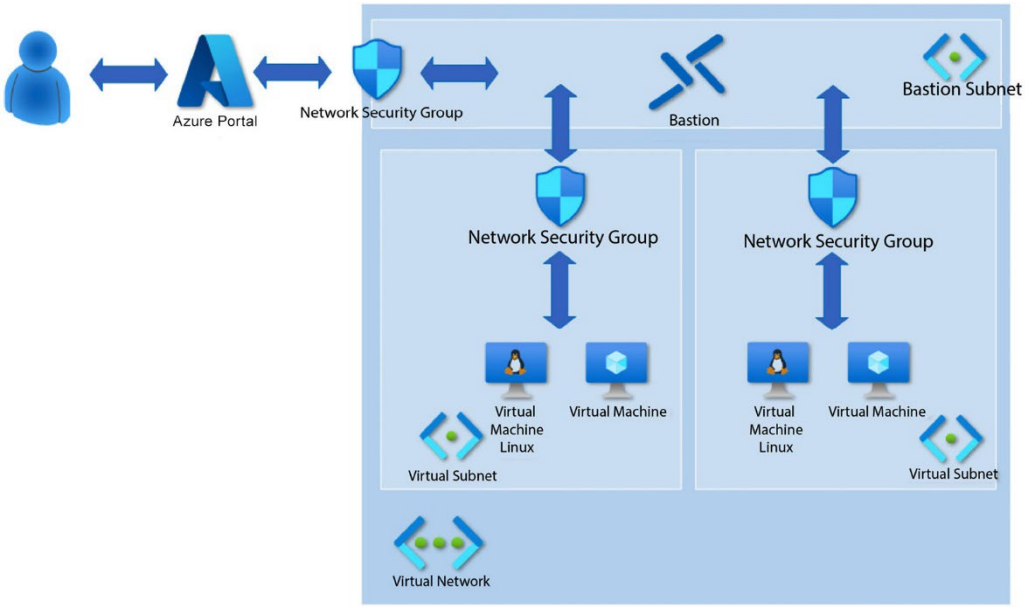

Physical Security
Identity and Access
Perimeter Security
Network Security
Compute
Applications
Data

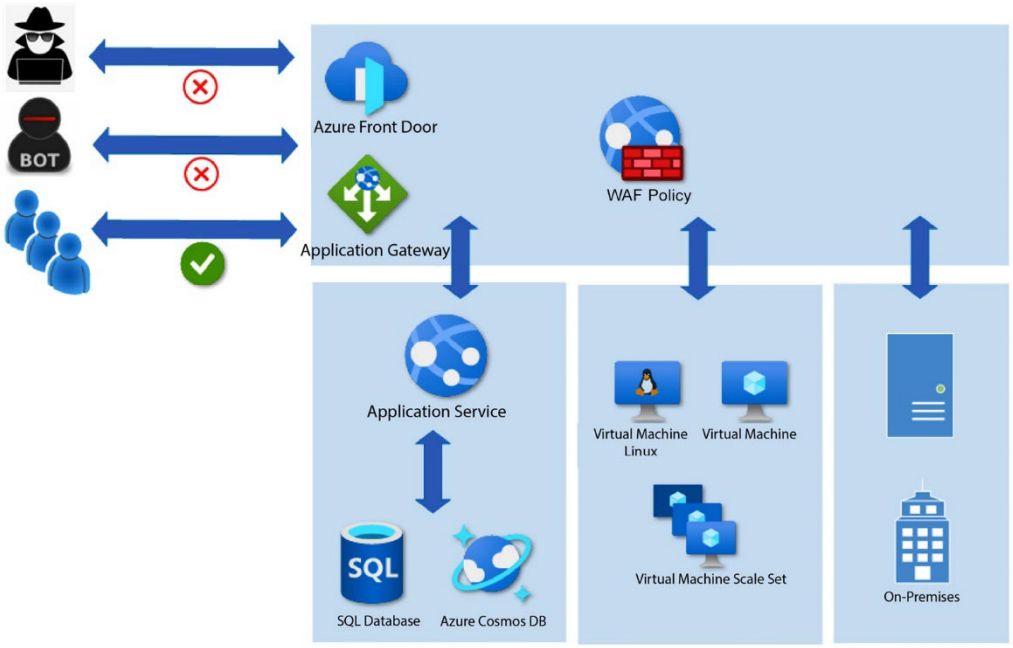

Conditions
Access Controls
Cloud Apps and Actions
Username
userabc
Password
MFA
MFA Token
WWW
Microsoft 365

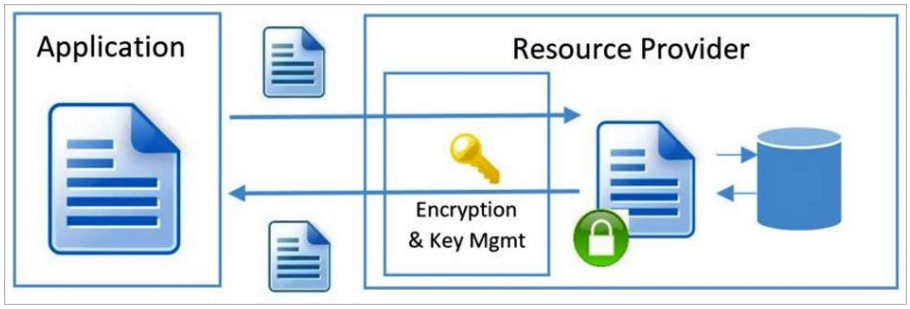

DDoS Protection Plan
Azure Front Door
Application Gateway
Load Balancer
Application Service
Virtual Network
Virtual Machine Scale Set
Virtual Machine Linux
Virtual Machine
SQL
SQL Database

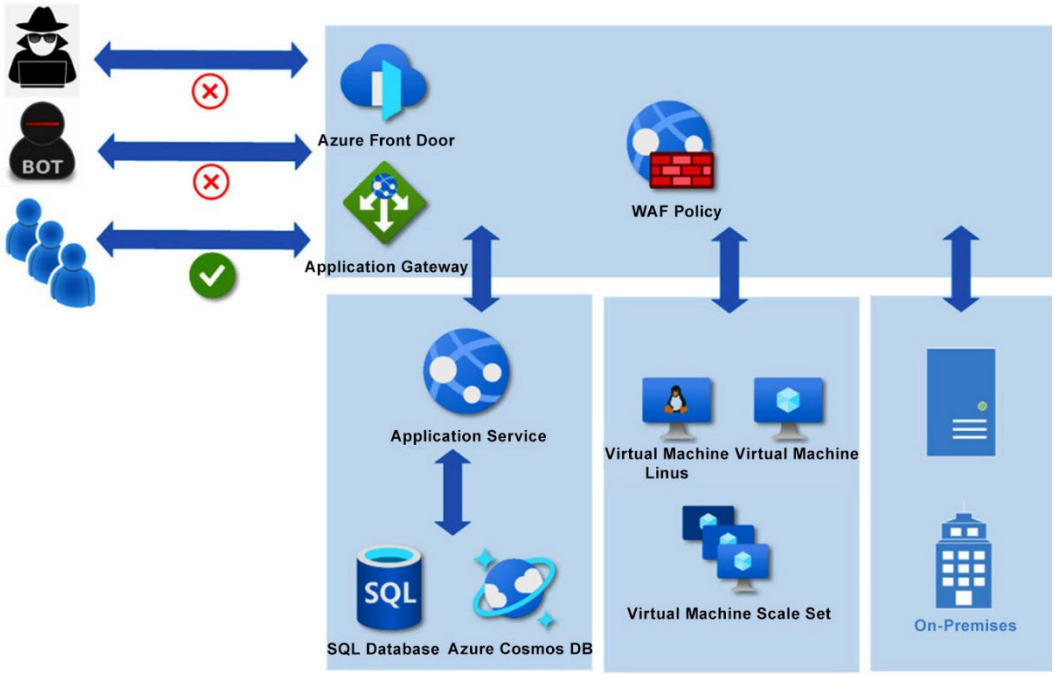

On-Premises
Azure Firewall
Firewall Subnet
Network Security Group
Network Security Group
Virtual Machine Linux
Virtual Machine
Virtual Machine Linux
Virtual Machine
Virtual Subnet
Virtual Subnet
Virtual Network

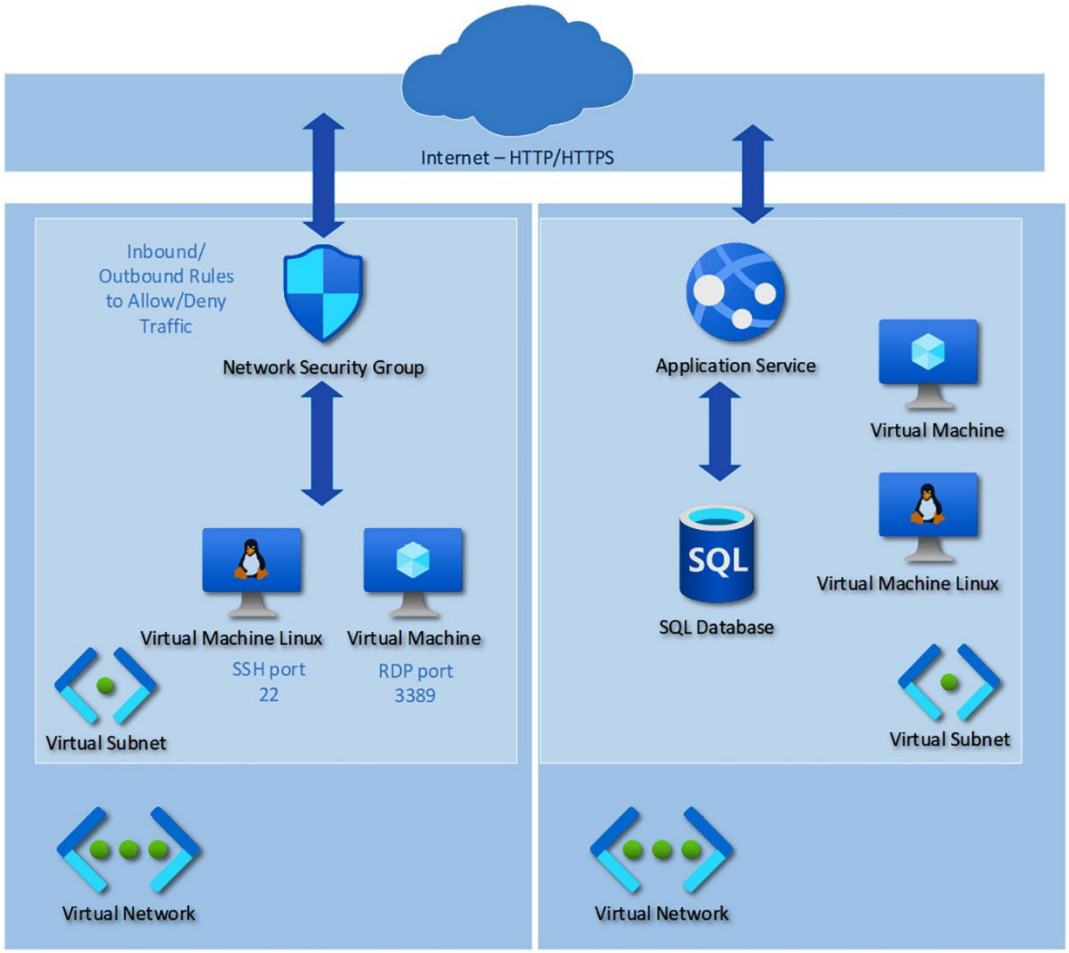

Internet – HTTP/HTTPS
Inbound/ Outbound Rules to Allow/ Deny Traffic
Network Security Group
Virtual Machine Linux
SSH port 22
Virtual Machine
RDP port 3389
Virtual Machine Linux
SSH port 22
Virtual Machine
RDP port 3389
Virtual Subnet
Virtual Subnet
Virtual Network


Azure Portal
Network Security Group
Bastion
Bastion Subnet
Network Security Group
Network Security Group
Virtual Machine Linux
Virtual Machine
Virtual Machine Linux
Virtual Machine
Virtual Subnet
Virtual Subnet
Virtual Network

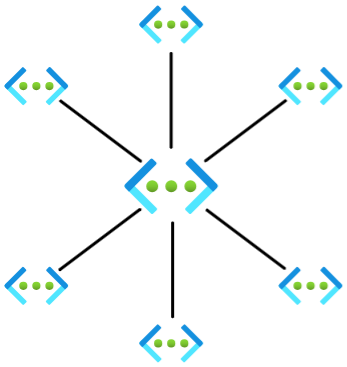

BOT
Azure Front Door
WAF Policy
Application Gateway
Application Service
Virtual Machine Linux
Virtual Machine
Virtual Machine Scale Set
SQL
SQL Database
Azure Cosmos DB
On-Premises


Application
Resource Provider
Encryption
& Key Mgmt

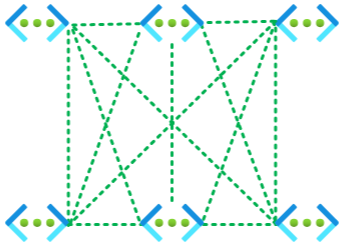

BOT
Azure Front Door
WAF Policy
Application Gateway
Application Service
Virtual Machine
Linus
Virtual Machine
Virtual Machine Scale Set
SQL
SQL Database
Azure Cosmos DB
On-Premises


Internet – HTTP/HTTPS
Inbound/
Outbound Rules
to Allow/Deny
Traffic
Network Security Group
Application Service
Virtual Machine
Virtual Machine Linux
SQL
SQL Database
Virtual Machine Linux
Virtual Machine
SSH port
22
RDP port
3389
Virtual Subnet
Virtual Subnet
Virtual Network
Virtual Network

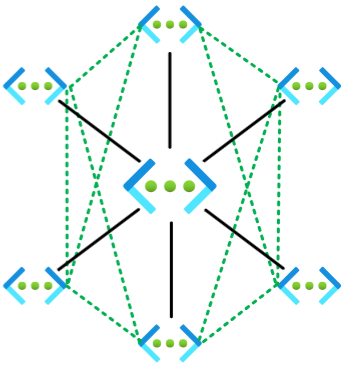
Hub and spoke



Mesh

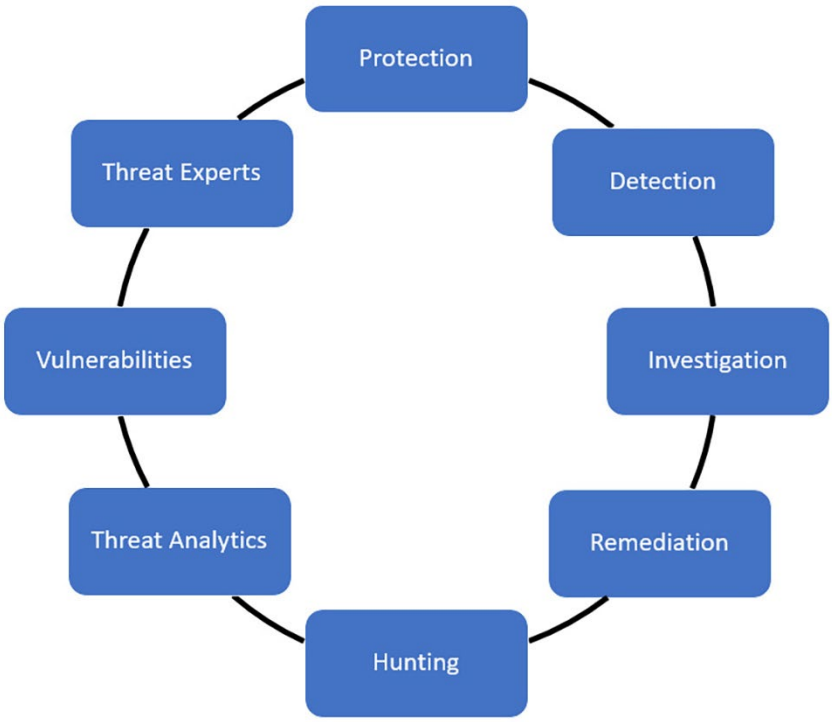


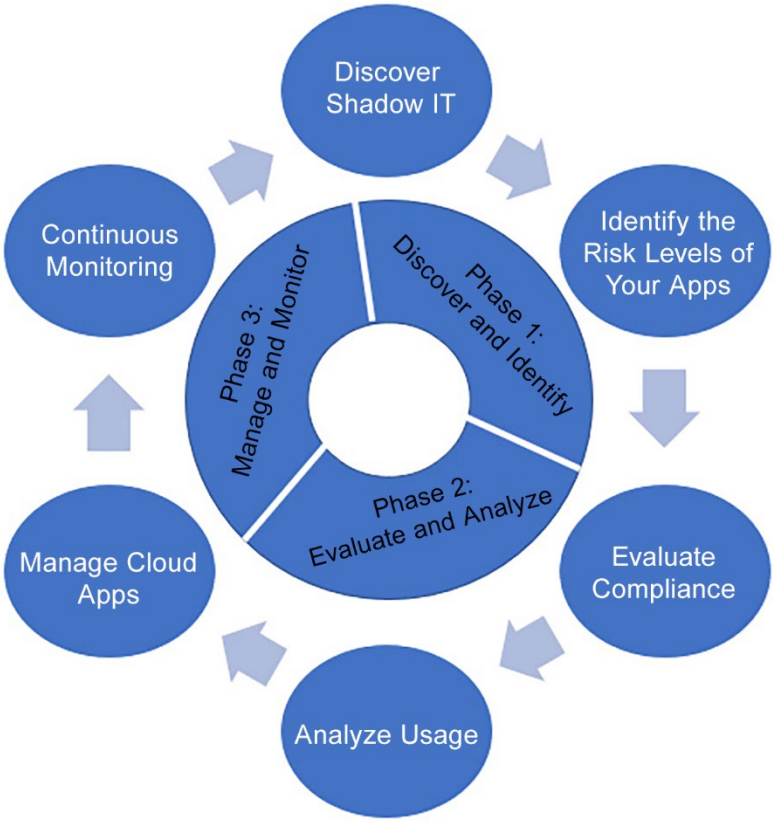
Hub and spoke with direct connectivity between spokes

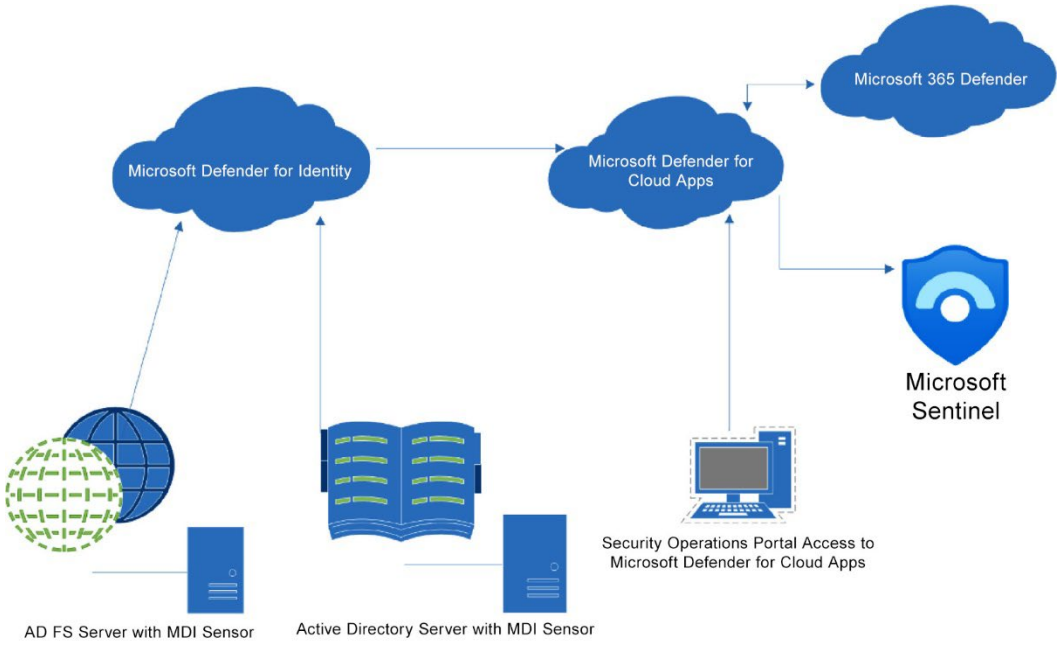


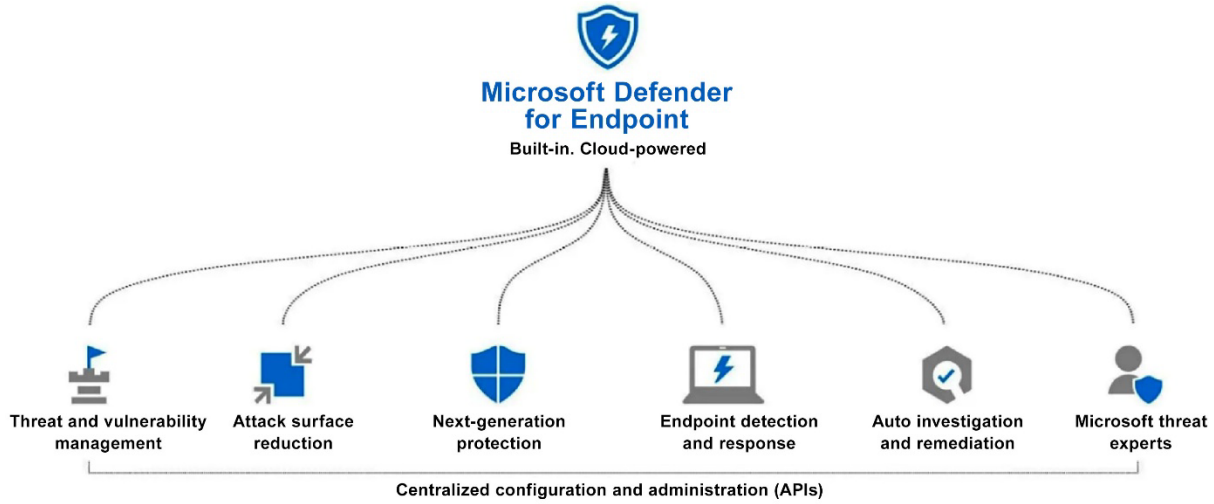
Microsoft Azure

Chapter 3: Design a Security Operations Strategy

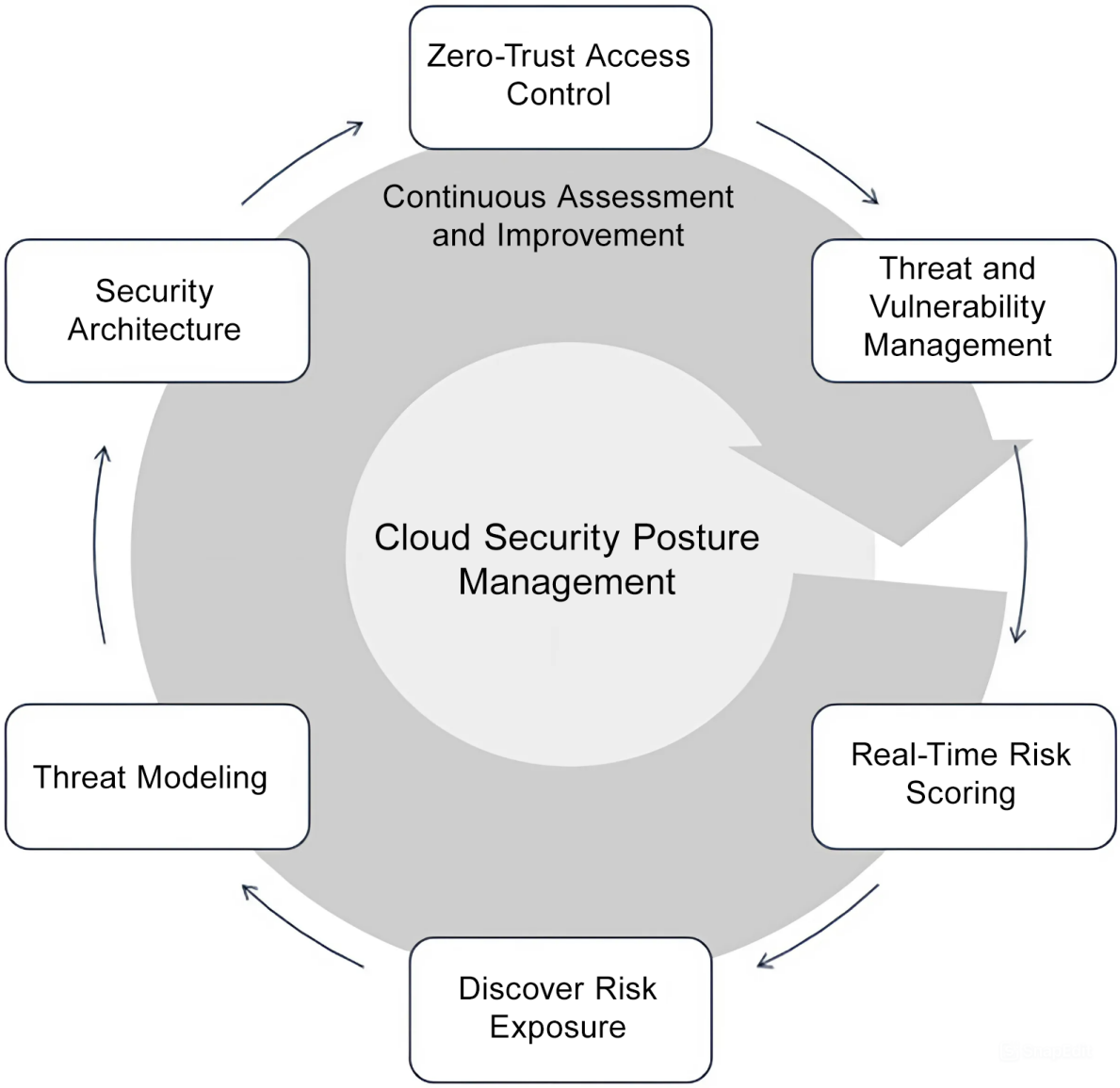


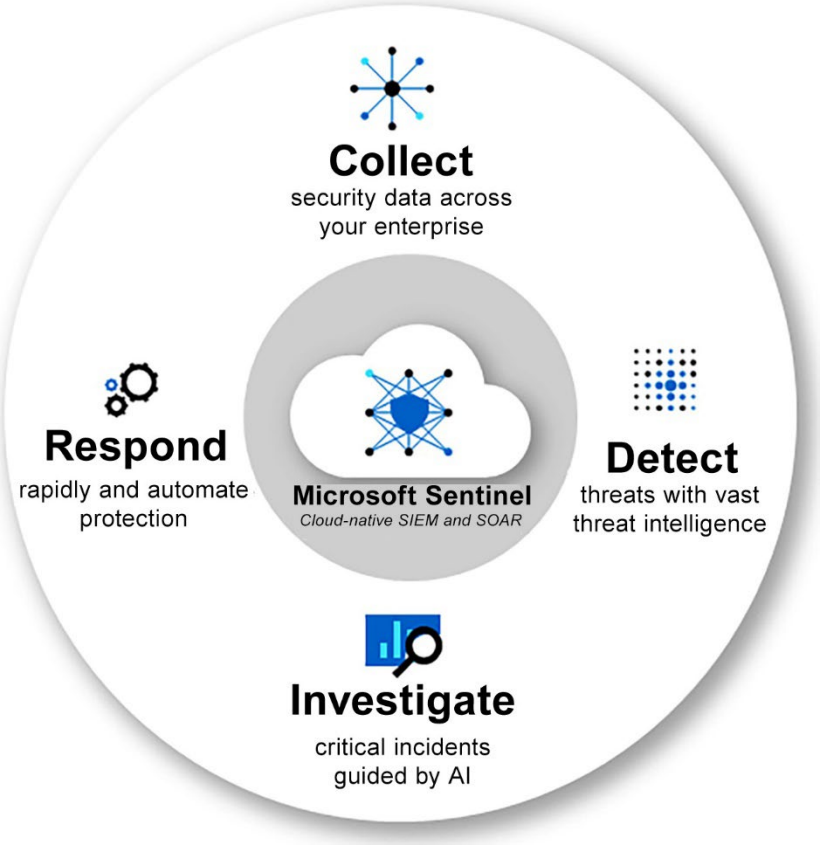


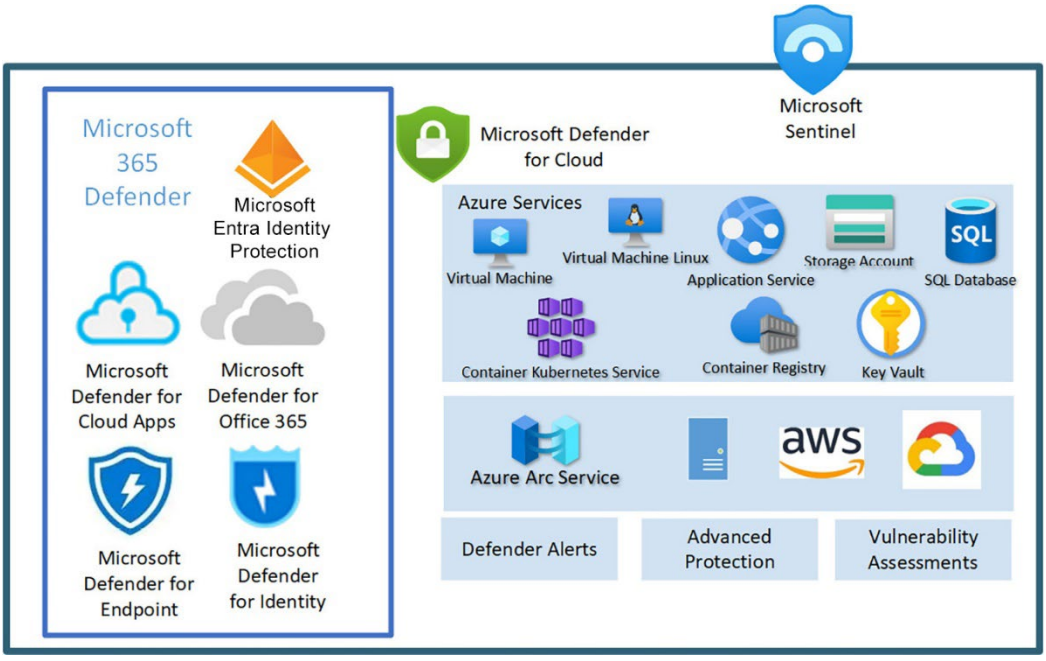

Microsoft 365 Defender
Microsoft Defender for Identity
Microsoft Defender for Cloud Apps
Microsoft Sentinel
Security Operations Portal Access to Microsoft Defender for Cloud Apps
AD FS Server with MDI Sensor
Active Directory Server with MDI Sensor

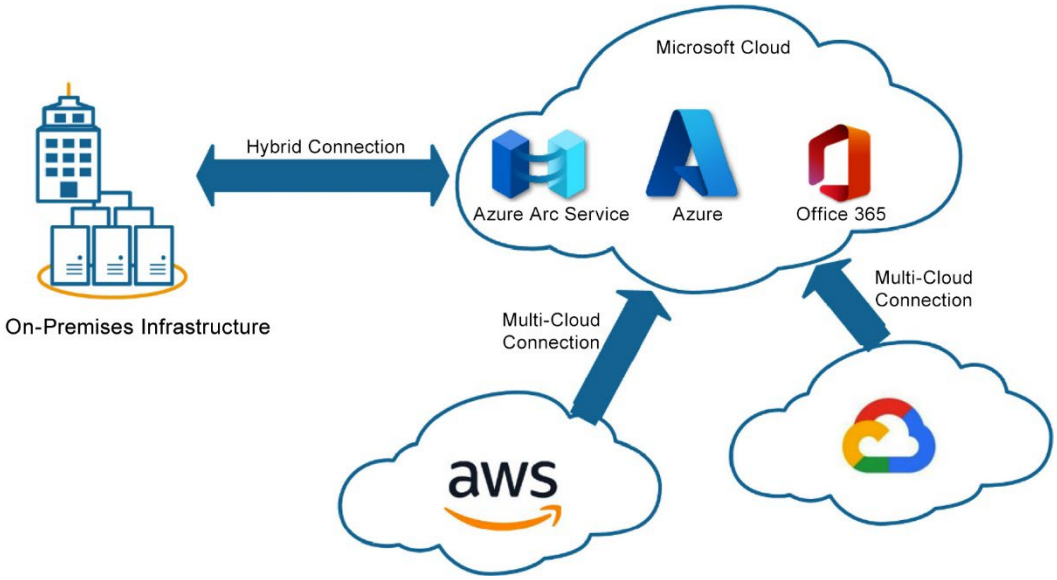

Microsoft Defender for Endpoint
Built-in. Cloud-powered
Threat and vulnerability management
Attack surface reduction
Next-generation protection
Endpoint detection and response
Auto investigation and remediation
Microsoft threat experts
Centralized configuration and administration (APIs)

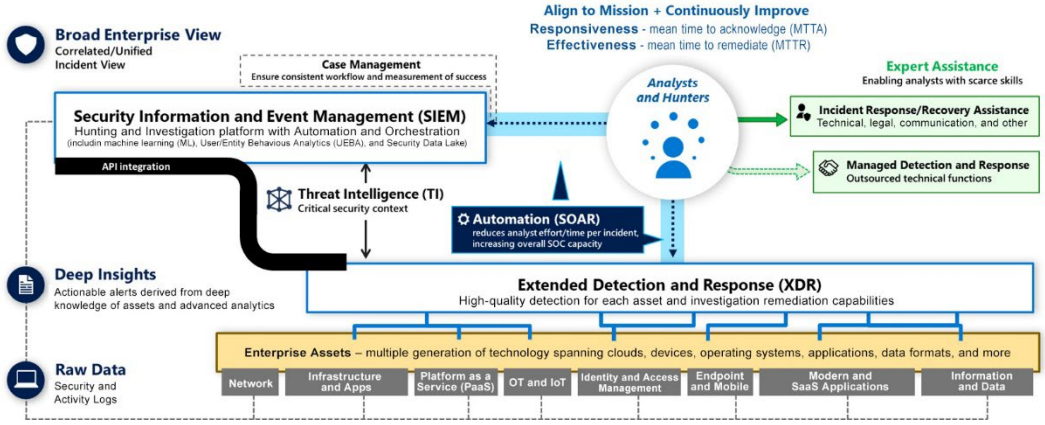

Secure Posture
Prevention
Detection
Investigation and Hunting
Response and Remediation
Awareness and Training
Office 365

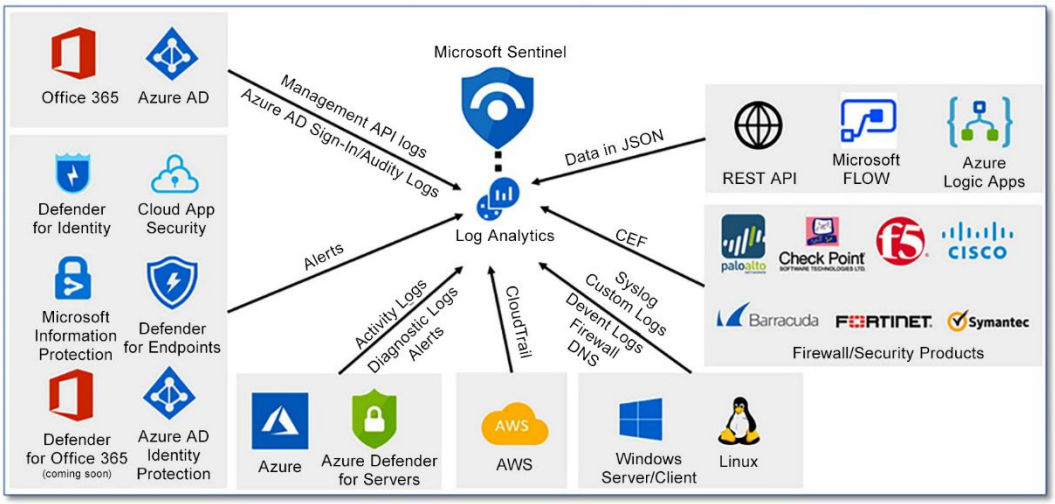

Zero-Trust Access Control
Threat and Vulnerability Management
Real-Time Risk Scoring
Discover Risk Exposure
Threat Modeling
Security Architecture
Continuous Assessment and Improvement
Cloud Security Posture Management

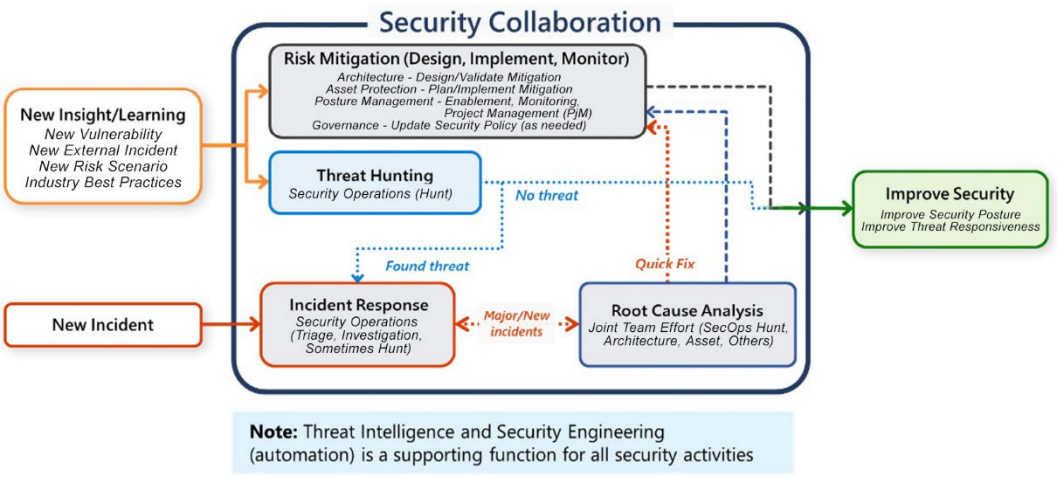

Collect
security data across your enterprise
Respond
rapidly and automate protection
Microsoft Sentinel
Cloud-native SIEM and SOAR
Detect
threats with vast threat intelligence
Investigate
critical incidents guided by AI


Microsoft 365 Defender
Microsoft Entra Identity Protection
Microsoft Defender for Cloud Apps
Microsoft Defender for Office 365
Microsoft Defender for Endpoint
Microsoft Defender for Identity
Microsoft Defender for Cloud
Microsoft Sentinel
Azure Services
Virtual Machine
Virtual Machine Linux
Application Service
Storage Account
SQL Database
Container Kubernetes Service
Container Registry
Key Vault
Azure Arc Service
aws
Defender Alerts
Advanced Protection
Vulnerability Assessments

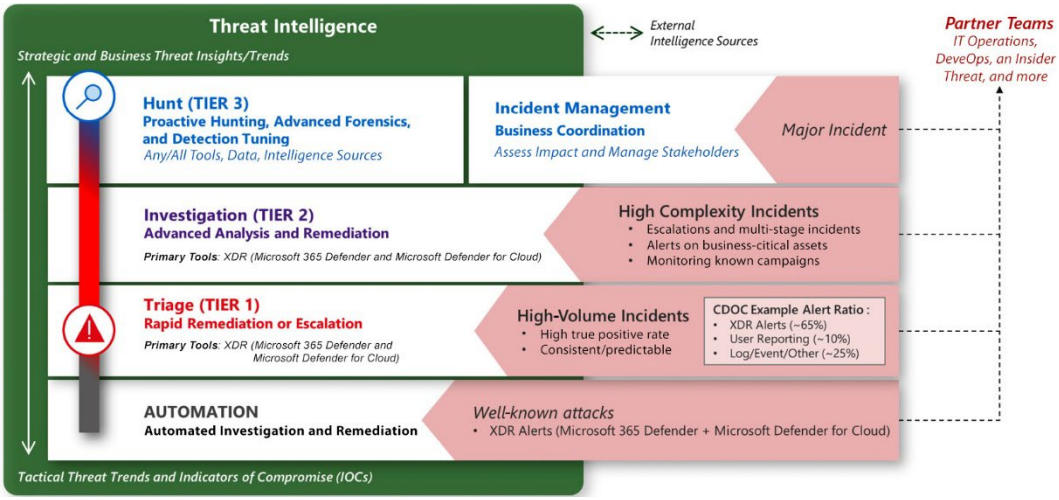

Microsoft Cloud
Hybrid Connection
Azure Arc Service
Azure
Office 365
On-Premises Infrastructure
Multi-Cloud Connection
Multi-Cloud Connection
aws


Align to Mission + Continuously Improve
Responsiveness - mean time to acknowledge (MTTA)
Effectiveness - mean time to remediate (MTTR)
Broad Enterprise View
Correlated/Unified Incident View
Case Management
Ensure consistent workflow and measurement of success
Security Information and Event Management (SIEM)
Hunting and Investigation platform with Automation and Orchestration
(includin machine learning (ML), User/Entity Behavious Analytics (UEBA), and Security Data Lake)
API integration
Threat Intelligence (TI)
Critical security context
Analysts and Hunters
Expert Assistance
Enabling analysts with scarce skills
Incident Response/Recovery Assistance
Technical, legal, communication, and other
Managed Detection and Response
Outsourced technical functions
Automation (SOAR)
reduces analyst effort/time per incident, increasing overall SOC capacity
Deep Insights
Actionable alerts derived from deep knowledge of assets and advanced analytics
Extended Detection and Response (XDR)
High-quality detection for each asset and investigation remediation capabilities
Raw Data
Security and Activity Logs
Enterprise Assets – multiple generation of technology spanning clouds, devices, operating systems, applications, data formats, and more
Network
Infrastructure and Apps
Platform as a Service (PaaS)
OT and IoT
Identity and Access Management
Endpoint and Mobile
Modern and SaaS Applications
Information and Data

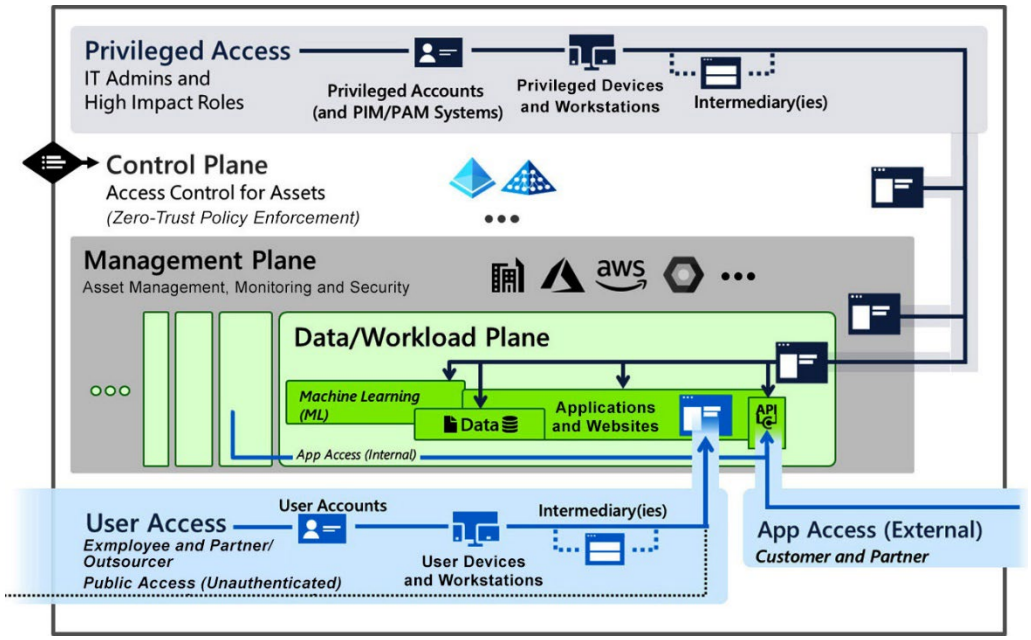

Office 365
Azure AD
Defender for Identity
Cloud App Security
Microsoft Information Protection
Defender for Endpoints
Defender for Office 365
(coming soon)
Azure AD Identity Protection
Microsoft Sentinel
Management API logs
Azure AD Sign-In/Audity Logs
Data in JSON
Alerts
Log Analytics
CEF
Activity Logs
Diagnostic Logs
Alerts
CloudTrail
Syslog
Custom Logs
Devent Logs
Firewall
DNS
REST API
Microsoft FLOW
Azure Logic Apps
paloalto
Check Point
f5
CISCO
Barracuda
FORTINET
Symantec
Firewall/Security Products
Azure
Azure Defender for Servers
AWS
AWS
Windows Server/Client
Linux

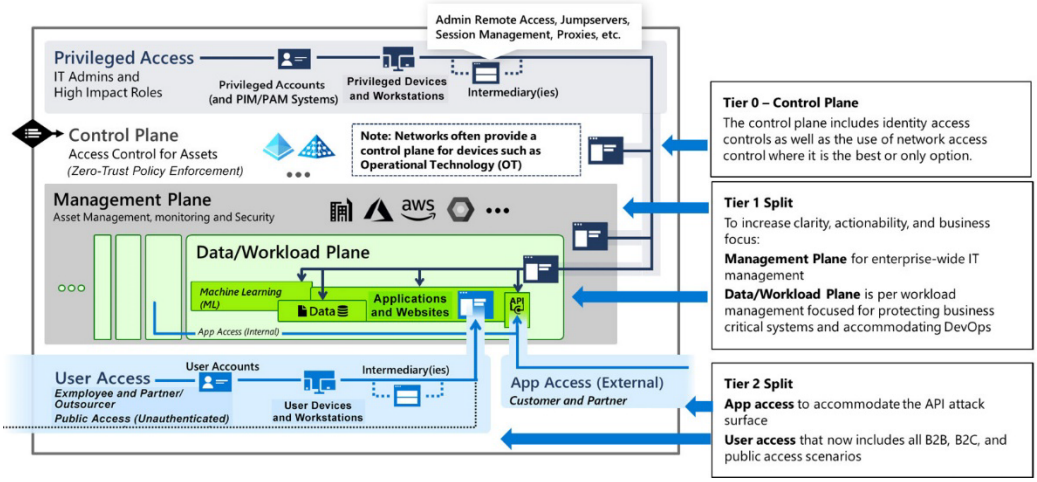


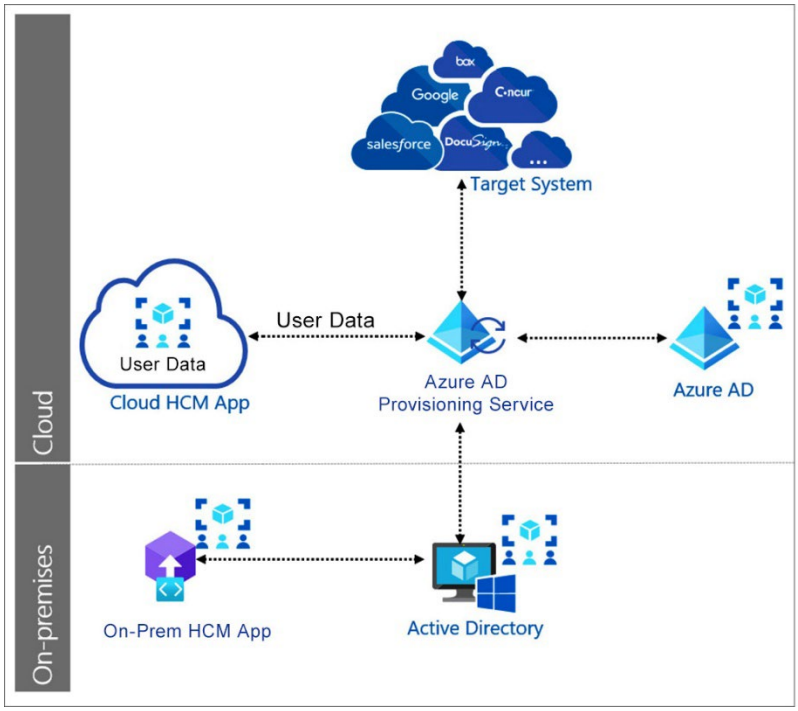
Note: Threat Intelligence and Security Engineering (automation) is a supporting function for all security activities

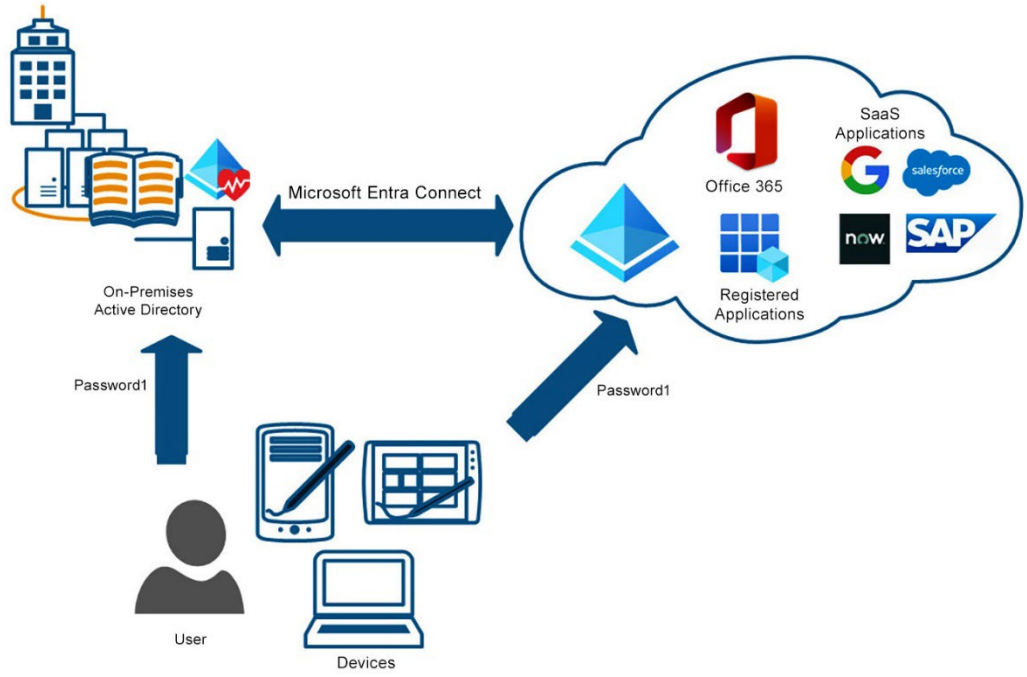


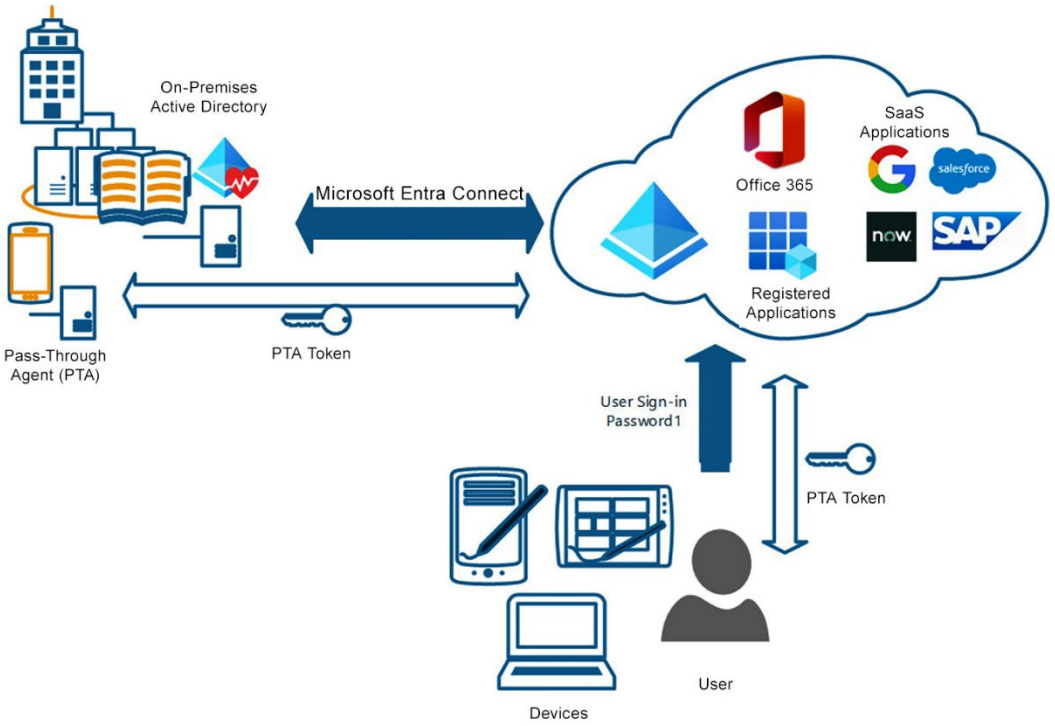
Chapter 4: Design an Identity Security Strategy

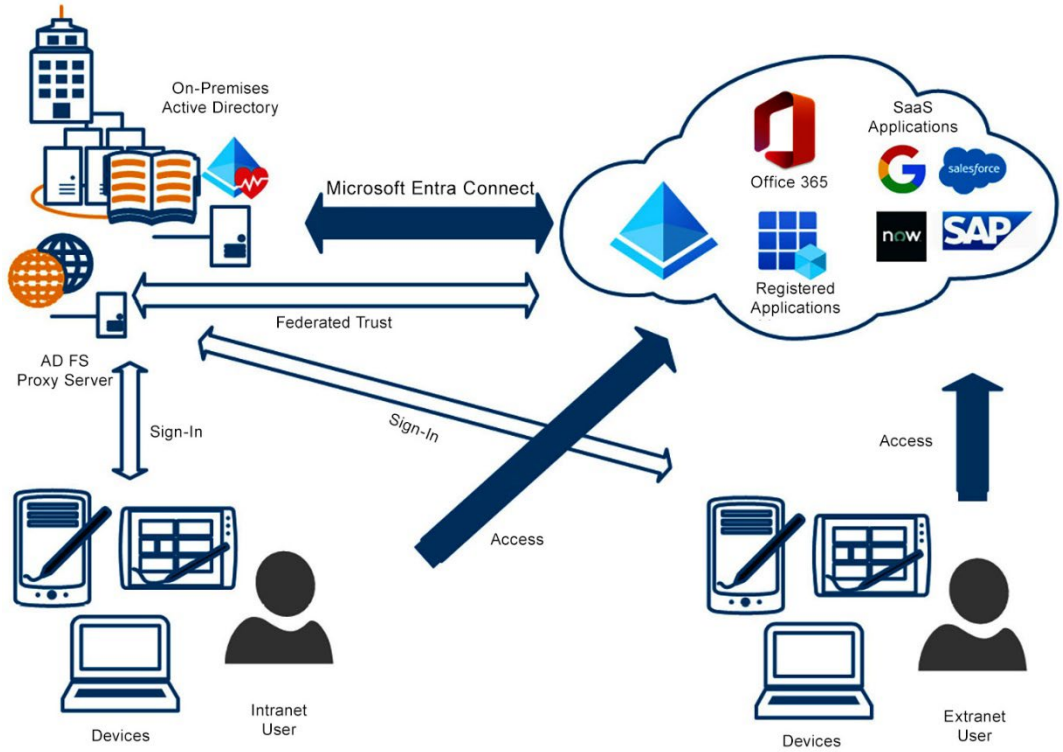


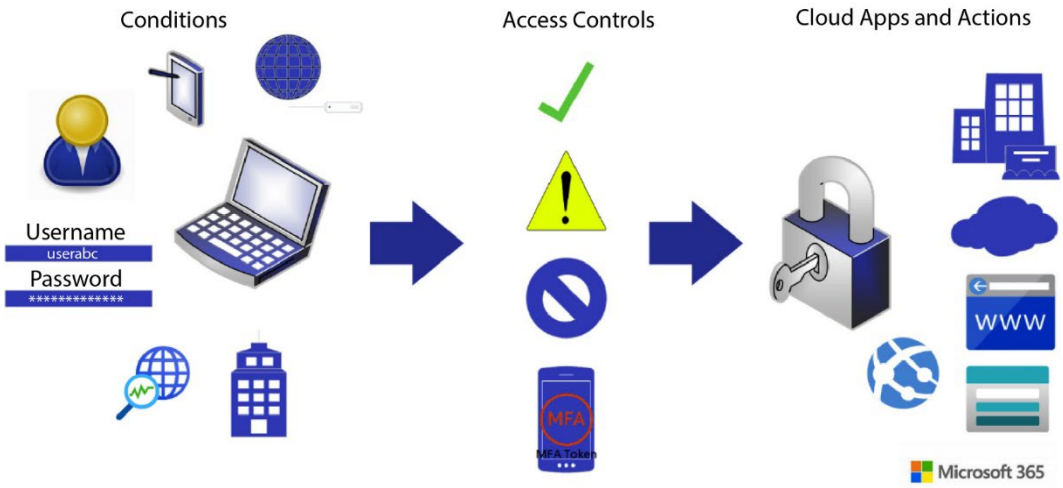



Cloud
On-premises
Target System
User Data
User Data
Cloud HCM App
Azure AD
Provisioning Service
Azure AD
On-Prem HCM App
Active Directory

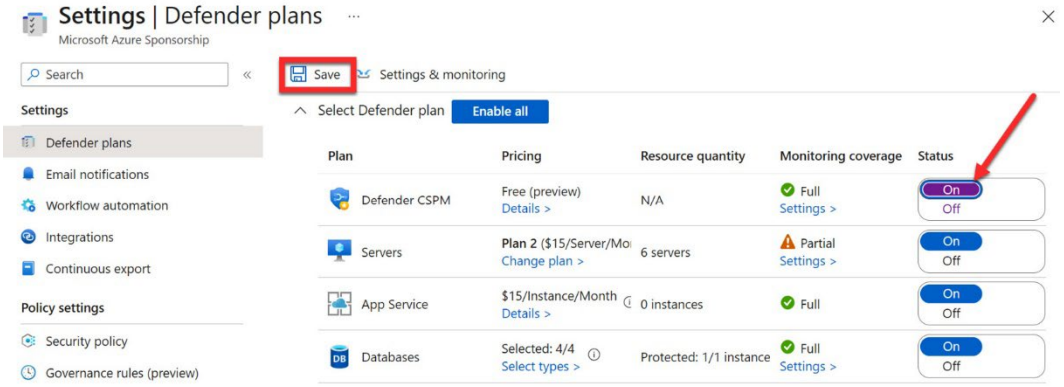

Microsoft Entra Connect
On-Premises
Active Directory
Office 365
SaaS
Applications
Registered
Applications
Password1
Password1
User
Devices

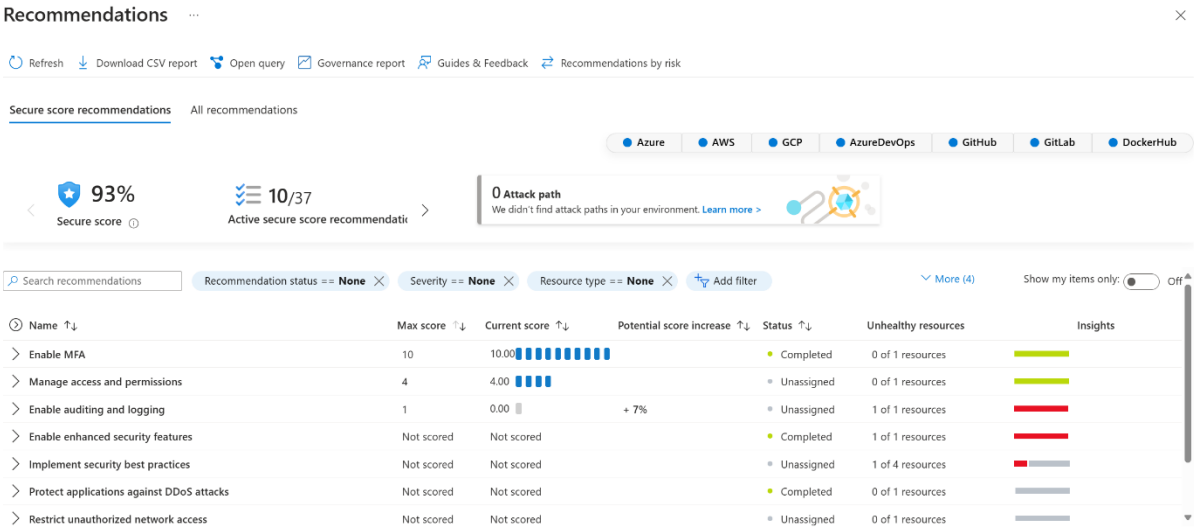

On-Premises
Active Directory
Microsoft Entra Connect
Office 365
SaaS
Applications
Registered
Applications
Pass-Through
Agent (PTA)
PTA Token
User Sign-in
Password1
PTA Token
Devices
User

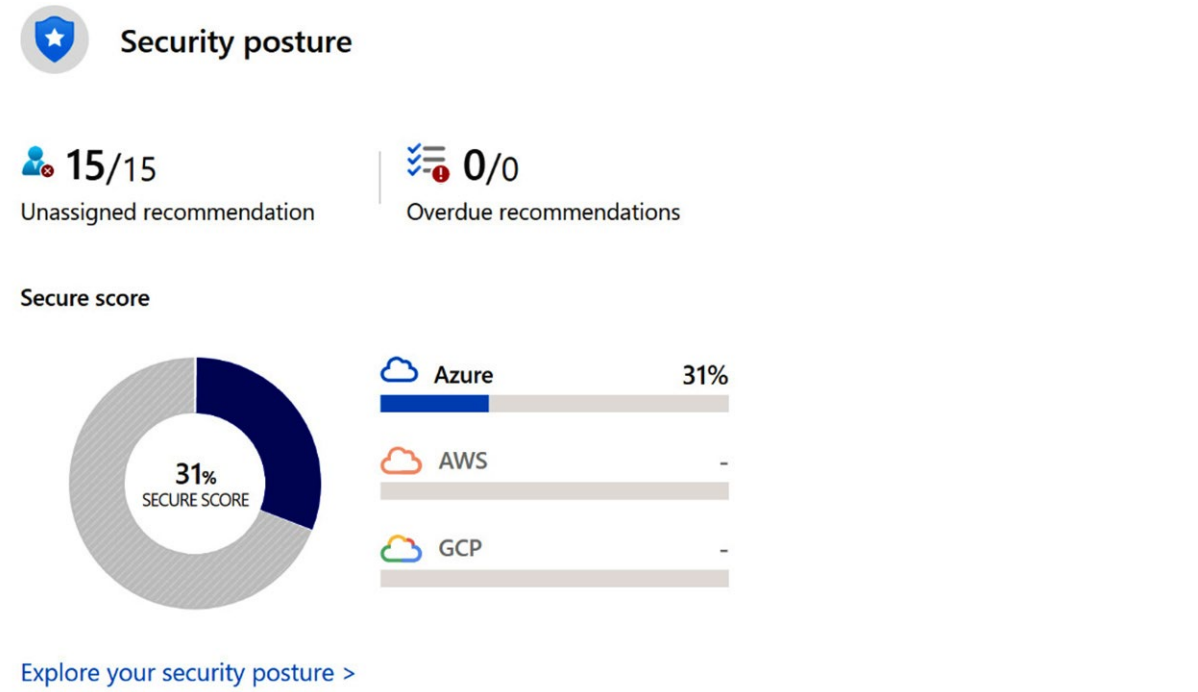

On-Premises
Active Directory
Microsoft Entra Connect
Office 365
SaaS
Applications
Registered
Applications
Federated Trust
AD FS
Proxy Server
Sign-In
Sign-In
Access
Access
Devices
Intranet
User
Devices
Extranet
User


Conditions
Access Controls
Cloud Apps and Actions
Username
userabc
Password
****
MFA
MFA Token
WWW
Microsoft 365

Chapter 5: Design a Regulatory Compliance Strategy







Regulatory compliance

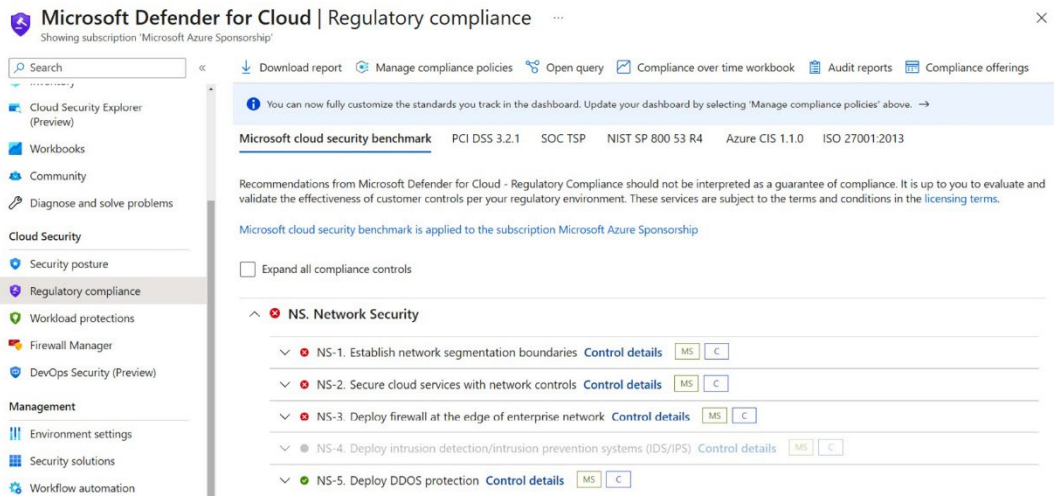
Azure Security Benchmark New

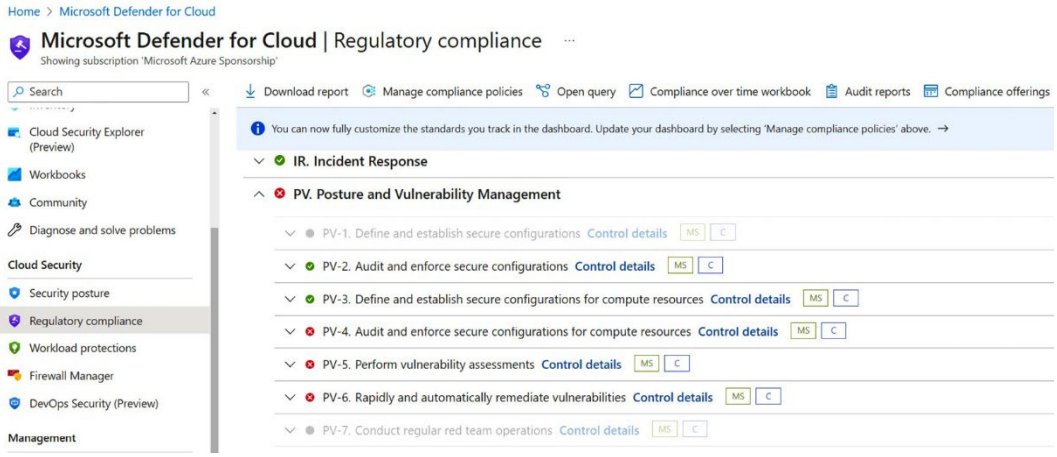
24 of **43** passed controls

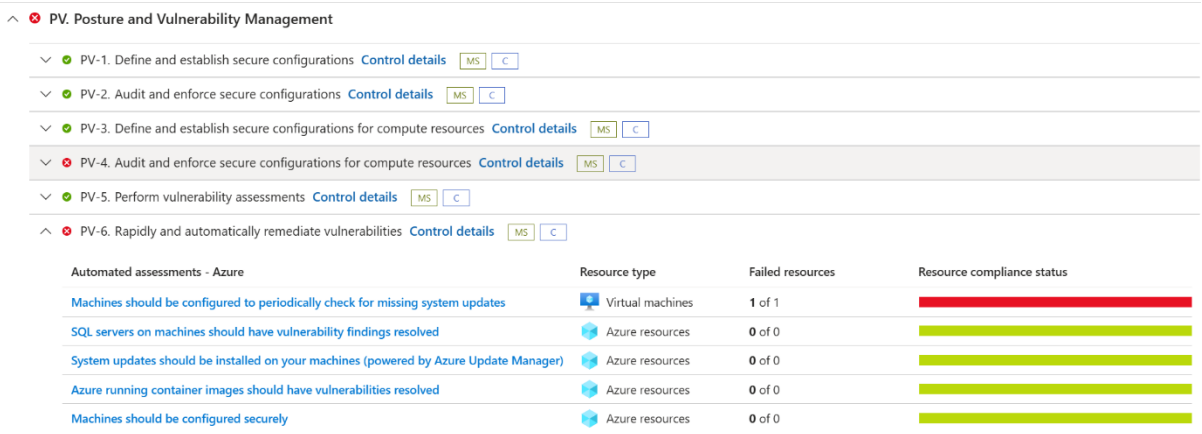
Lowest compliance regulatory standards
by passed controls

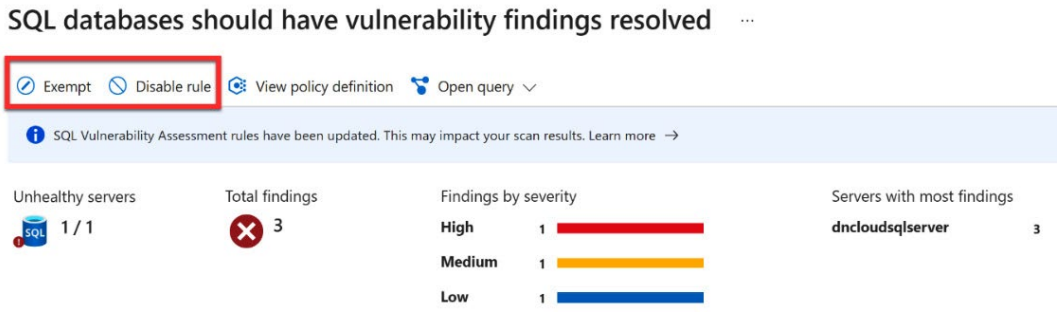
SOC TSP	**1**/13
ISO 27001:2013	**2**/17
PCI DSS 3.2.1	**11**/43

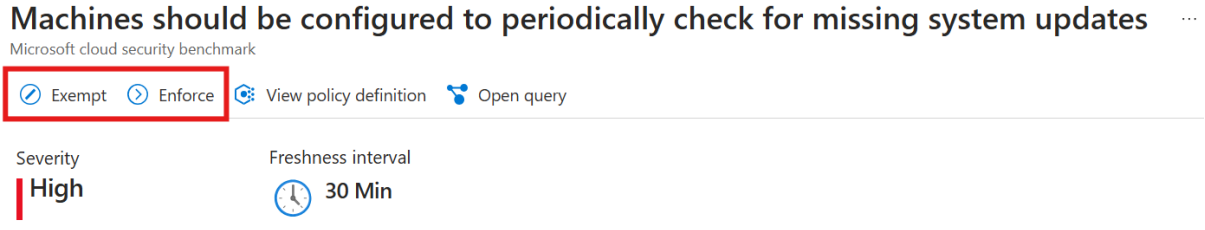
Improve your compliance >



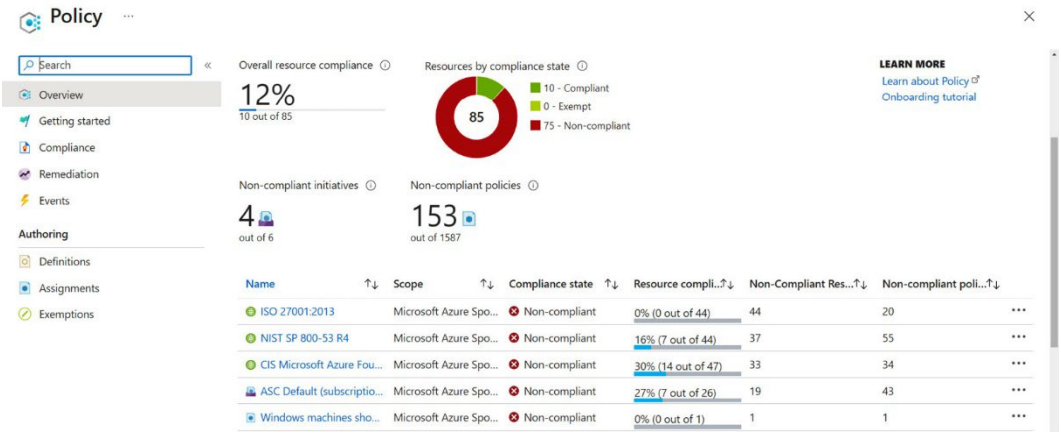

Home > Microsoft Defender for Cloud
Microsoft Defender for Cloud | Regulatory compliance
Showing subscription 'Microsoft Azure Sponsorship'
Search
Cloud Security Explorer (Preview)
Workbooks
Community
Diagnose and solve problems
Cloud Security
Security posture
Regulatory compliance
Workload protections
Firewall Manager
DevOps Security (Preview)
Management
Download report
Manage compliance policies
Open query
Compliance over time workbook
Audit reports
Compliance offerings
You can now fully customize the standards you track in the dashboard. Update your dashboard by selecting 'Manage compliance policies' above.
IR. Incident Response
PV. Posture and Vulnerability Management
PV-1. Define and establish secure configurations Control details
PV-2. Audit and enforce secure configurations Control details
PV-3. Define and establish secure configurations for compute resources Control details
PV-4. Audit and enforce secure configurations for compute resources Control details
PV-5. Perform vulnerability assessments Control details
PV-6. Rapidly and automatically remediate vulnerabilities Control details
PV-7. Conduct regular red team operations Control details

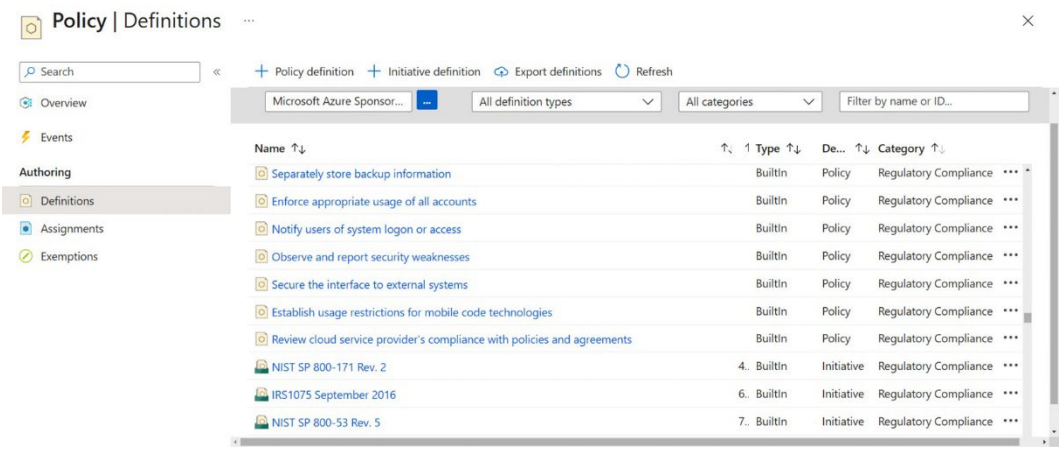

PV. Posture and Vulnerability Management
PV-1. Define and establish secure configurations Control details
PV-2. Audit and enforce secure configurations Control details
PV-3. Define and establish secure configurations for compute resources Control details
PV-4. Audit and enforce secure configurations for compute resources Control details
PV-5. Perform vulnerability assessments Control details
PV-6. Rapidly and automatically remediate vulnerabilities Control details
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
SQL servers on machines should have vulnerability findings resolved
Azure resources
0 of 0
System updates should be installed on your machines (powered by Azure Update Manager)
Azure resources
0 of 0
Azure running container images should have vulnerabilities resolved
Azure resources
0 of 0
Machines should be configured securely
Azure resources
0 of 0


SQL databases should have vulnerability findings resolved
Exempt
Disable rule
View policy definition
Open query
SQL Vulnerability Assessment rules have been updated. This may impact your scan results. Learn more
Unhealthy servers
1 / 1
Total findings
3
Findings by severity
High 1
Medium 1
Low 1
Servers with most findings
dncloudsqlserver 3

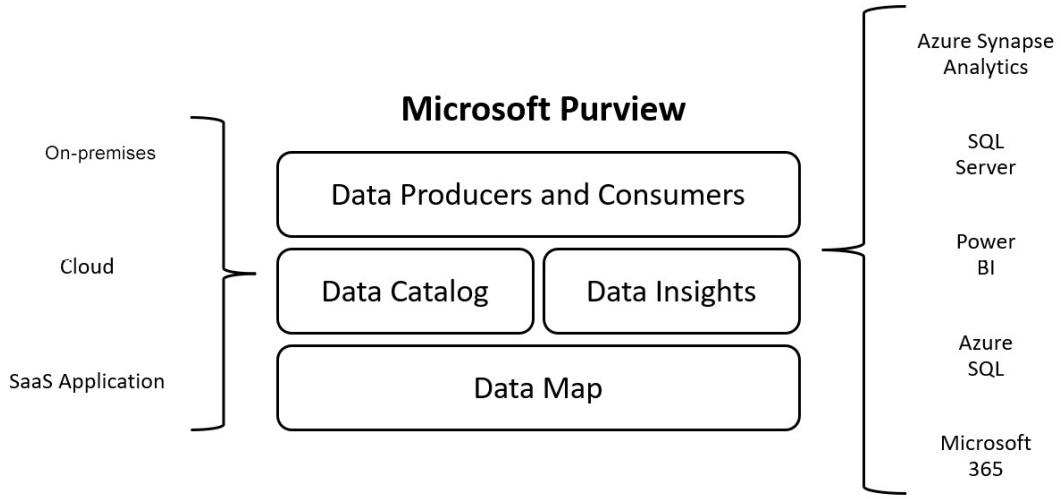

Machines should be configured to periodically check for missing system updates
Microsoft cloud security benchmark
Exempt
Enforce
View policy definition
Open query
Severity
High
Freshness interval
30 Min


Tightly define your policy
Audit your existing resources
Audit new or updated resource requests
Deploy your policy to resources
Continuous monitoring

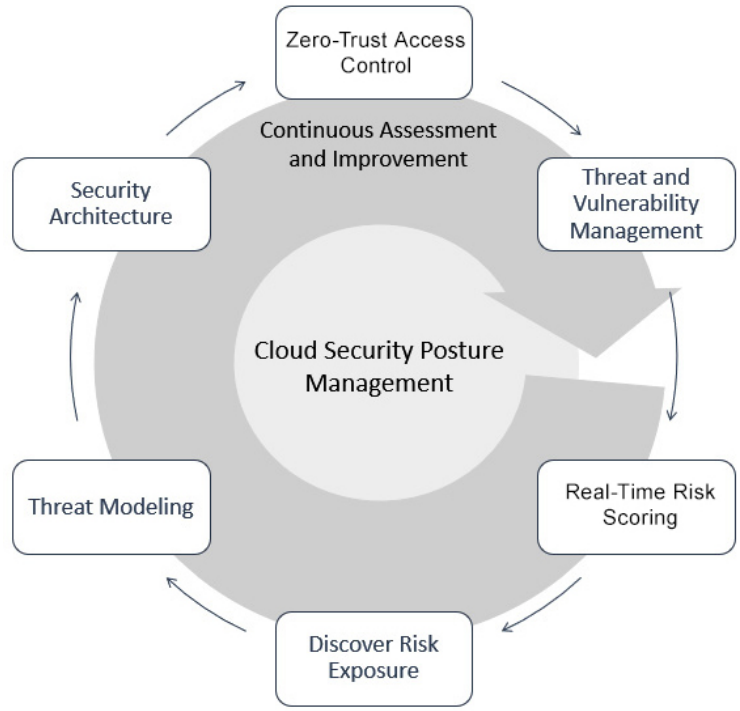


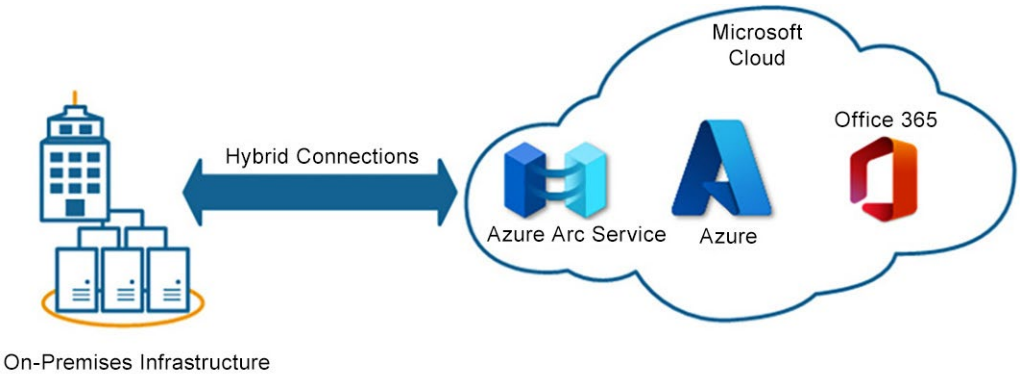


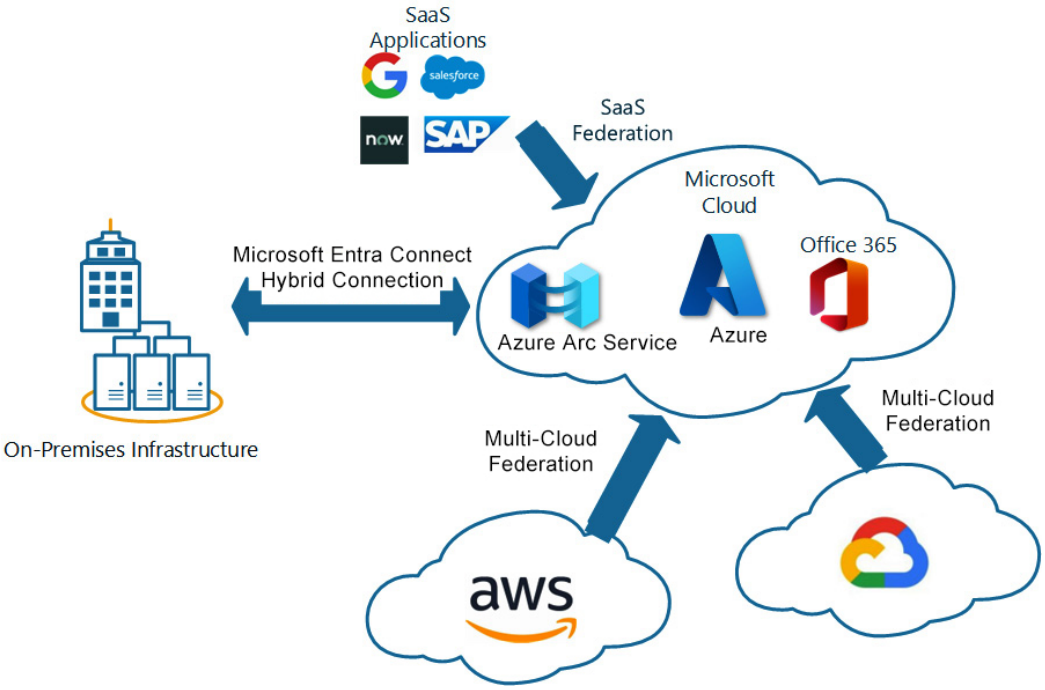
Name	Latest version (preview)	Definition location	Policies	Type	Definition type	Category
Allowed locations for resource groups	1.0.0			BuiltIn	Policy	General
Configure subscriptions to set up preview features	1.0.1			BuiltIn	Policy	General
Allowed locations	1.0.0			BuiltIn	Policy	General
Audit usage 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



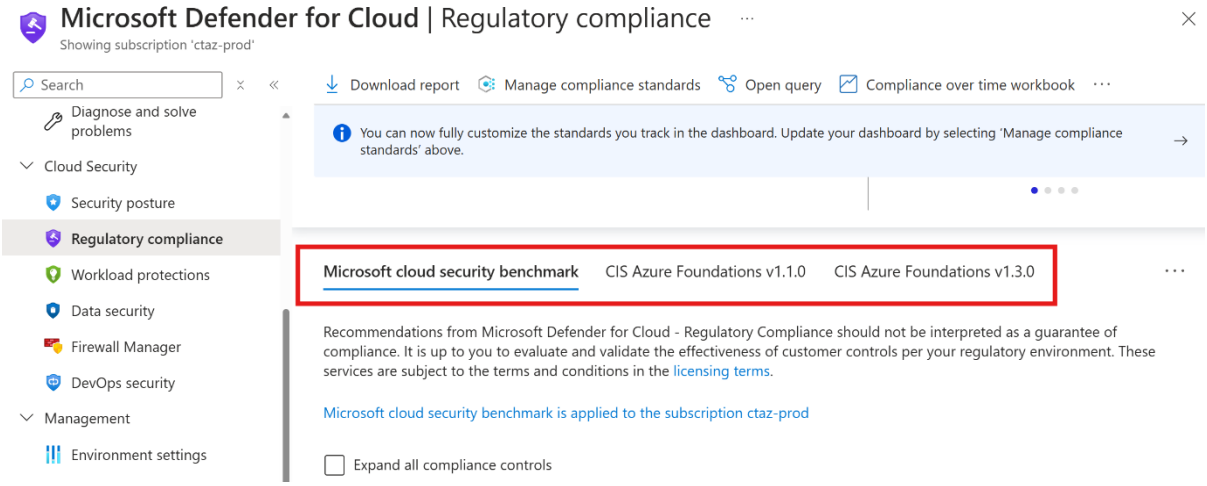
Chapter 6: Evaluate Security Posture and Recommend Technical Strategies to Manage Risk






SaaS
Applications
SaaS
Federation
Microsoft
Cloud
Office 365
Microsoft Entra Connect
Hybrid Connection
Azure Arc Service
Azure
On-Premises Infrastructure
Multi-Cloud
Federation
Multi-Cloud
Federation
aws


Microsoft Defender for Cloud | Regulatory compliance
Showing subscription 'Microsoft Azure Sponsorship'
Search
Download report
Manage compliance policies
Open query
Community
Diagnose and solve problems
Cloud Security
Security posture
Regulatory compliance
Workload protections
Management
Environment settings
Security solutions
You can now fully customize the standards you track in the dashboard. Update your dashboard by selecting 'Manage compliance policies' above.
Azure Security Benchmark
21 of 43 passed controls
Lowest compliance regulatory standards
Show all 9
SOC TSP 1/13
ISO 27001:2013 2/17
PCI DSS 3.2.1 12/43
Azure CIS 1.1.0 36/71


Microsoft Defender for Cloud | Regulatory compliance
Showing subscription 'ctaz-prod'
Search
Download report
Manage compliance standards
Open query
Compliance over time workbook
Diagnose and solve problems
Cloud Security
Security posture
Regulatory compliance
Workload protections
Data security
Firewall Manager
DevOps security
Management
Environment settings
You can now fully customize the standards you track in the dashboard. Update your dashboard by selecting 'Manage compliance standards' above.
Microsoft cloud security benchmark
CIS Azure Foundations v1.1.0
CIS Azure Foundations v1.3.0
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.
Microsoft cloud security benchmark is applied to the subscription ctaz-prod
Expand all compliance controls

- 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

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

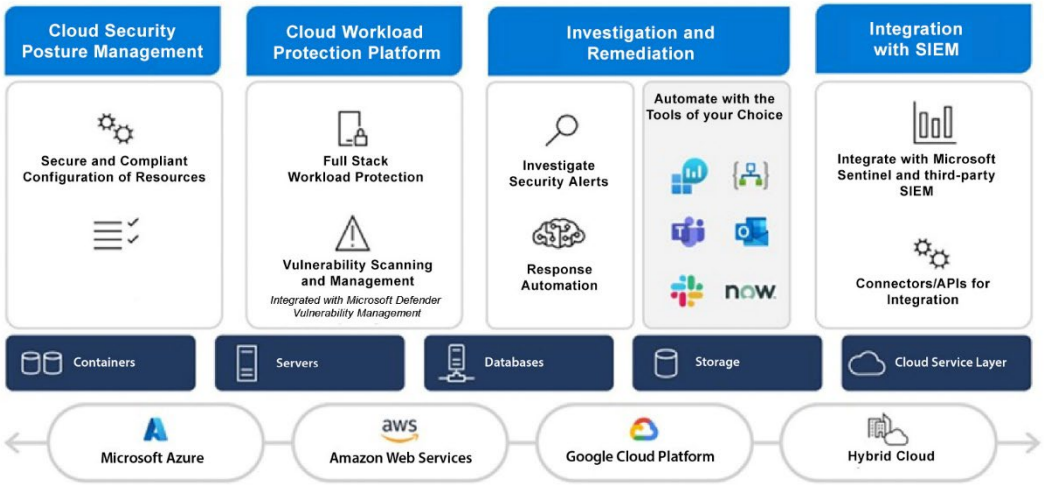
NS. Network Security

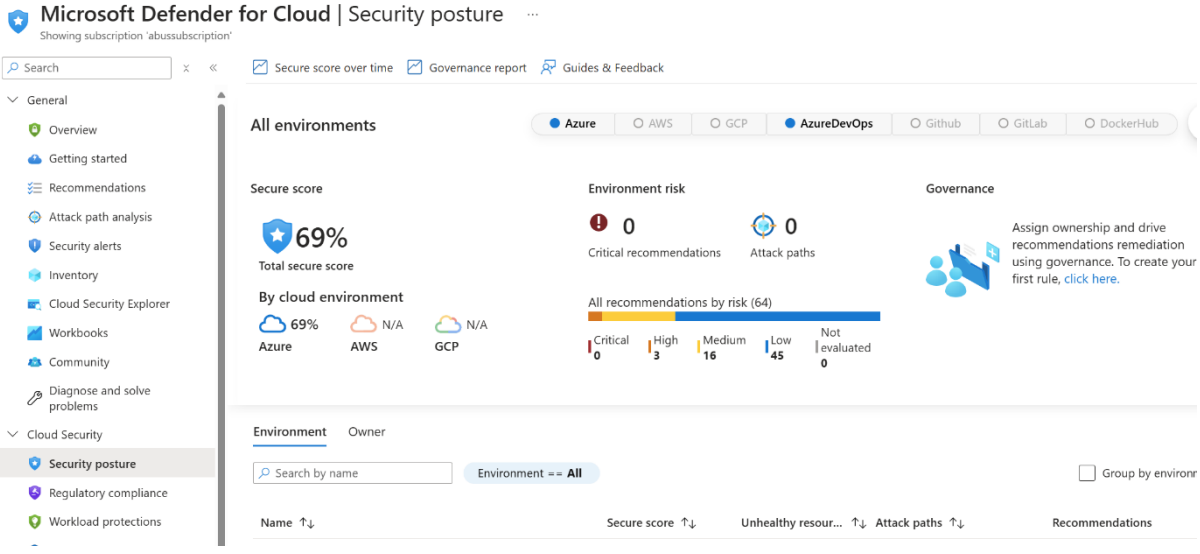
NS-1. Establish network segmentation boundaries **Control details** MS C

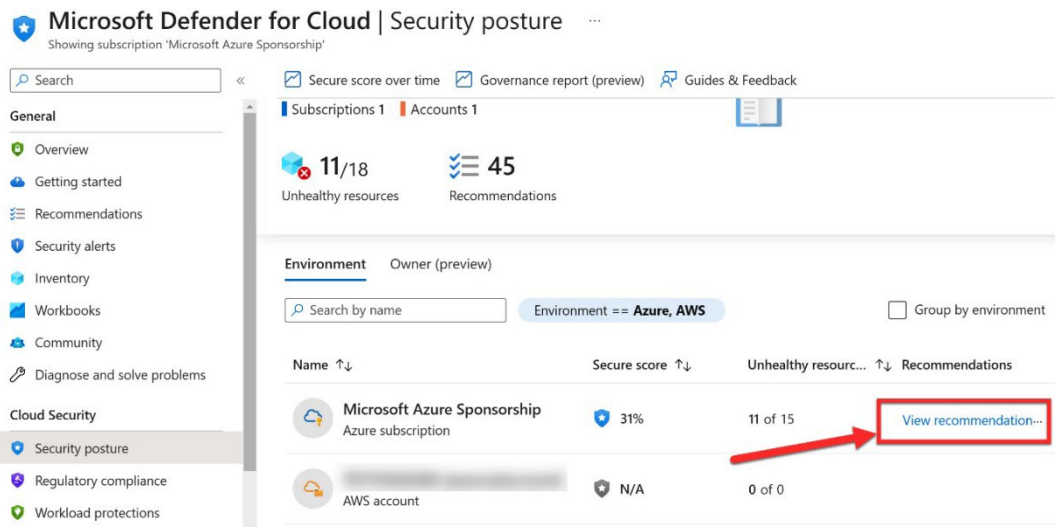
Customer responsibility	Resource type	Failed resources	Resource compliance...
Adaptive network hardening recommenda	Virtual machines	**4** of 5	
All network ports should be restricted on	Virtual machines	**4** of 5	
Subnets should be associated with a netw	Subnets	**2** of 3	
Non-internet-facing virtual machines shou	Virtual machines	**0** of 5	
Internet-facing virtual machines should be	Virtual machines	**0** of 5	

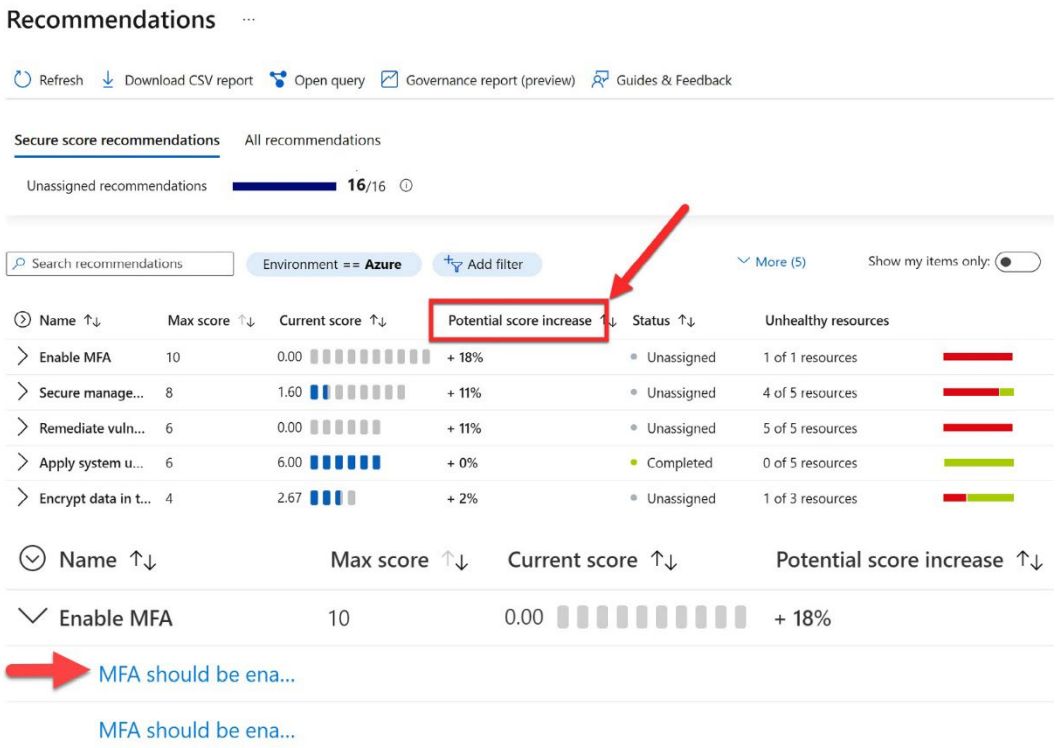
- 1. Install and maintain a firewall configuration to protect cardholder data
- 2. Do not use vendor-supplied defaults for system passwords and other security parameters
- 3. Protect stored cardholder data
- 4. Encrypt transmission of cardholder data across open, public networks.
- 5. Protect all systems 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:

Microsoft Defender for Cloud

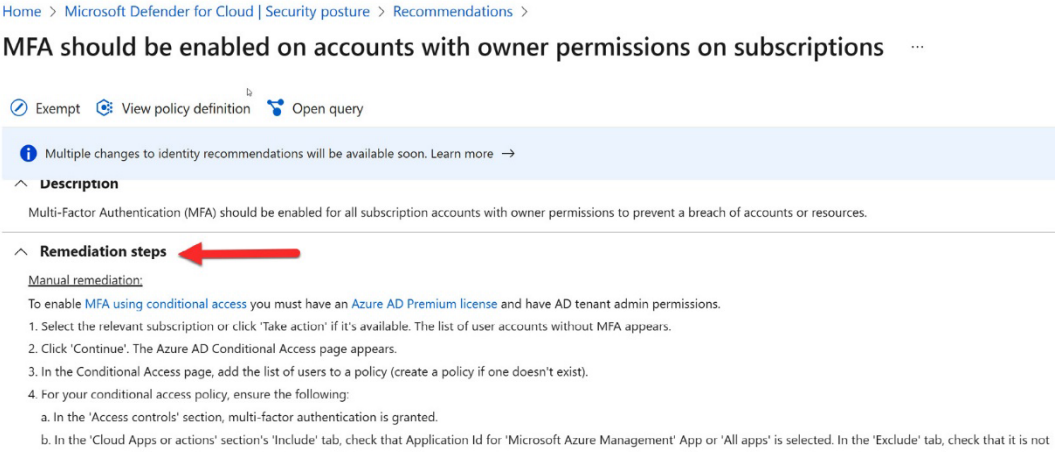


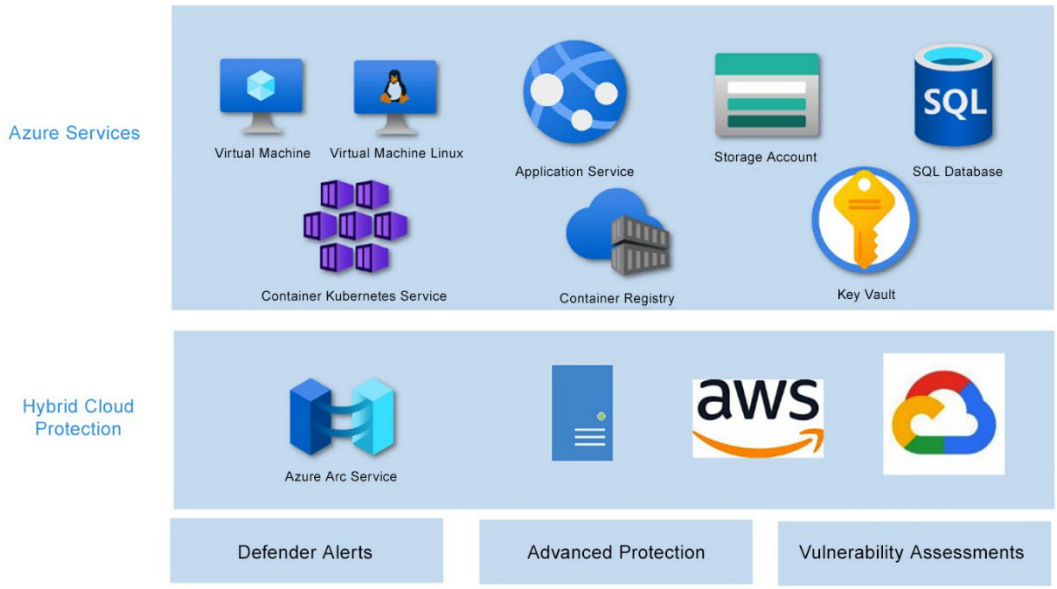


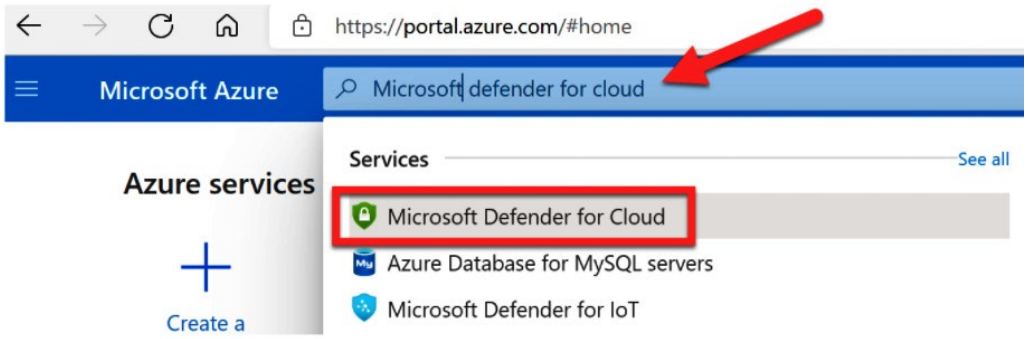

Microsoft Defender for Cloud | Security posture
Showing subscription 'Microsoft Azure Sponsorship'
Search
General
Overview
Getting started
Recommendations
Security alerts
Inventory
Workbooks
Community
Diagnose and solve problems
Cloud Security
Security posture
Regulatory compliance
Workload protections
Secure score over time
Governance report (preview)
Guides & Feedback
Subscriptions 1
Accounts 1
11/18
Unhealthy resources
45
Recommendations
Environment
Owner (preview)
Search by name
Environment == Azure, AWS
Group by environment
Name
Secure score
Unhealthy resourc...
Recommendations
Microsoft Azure Sponsorship
Azure subscription
31%
11 of 15
View recommendation
AWS account
N/A
0 of 0

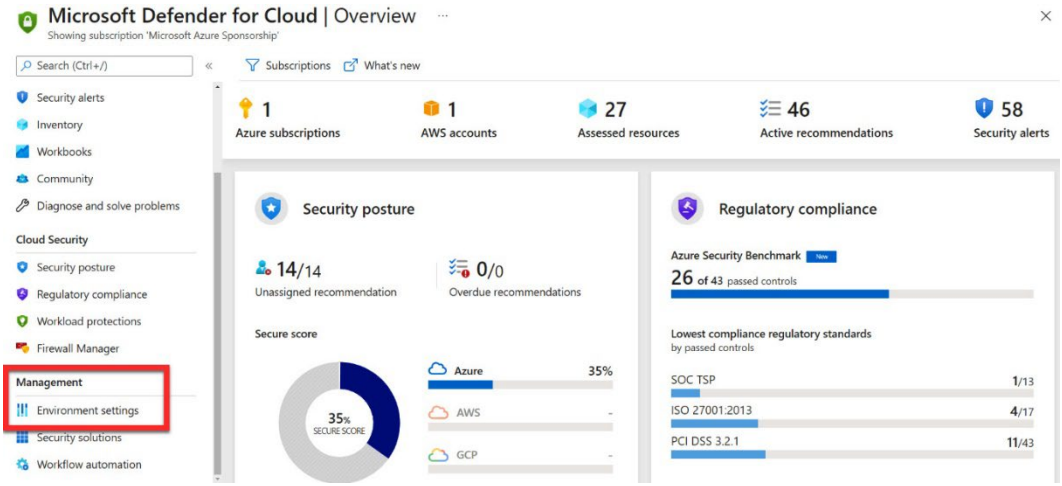

Recommendations
Refresh
Download CSV report
Open query
Governance report (preview)
Guides & Feedback
Secure score recommendations
All recommendations
Unassigned recommendations
16/16
Search recommendations
Environment == Azure
Add filter
More (5)
Show my items only:
Name
Max score
Current score
Potential score increase
Status
Unhealthy resources
Enable MFA 10 0.00 + 18% Unassigned 1 of 1 resources
Secure manage... 8 1.60 + 11% Unassigned 4 of 5 resources
Remediate vuln... 6 0.00 + 11% Unassigned 5 of 5 resources
Apply system u... 6 6.00 + 0% Completed 0 of 5 resources
Encrypt data in t... 4 2.67 + 2% Unassigned 1 of 3 resources

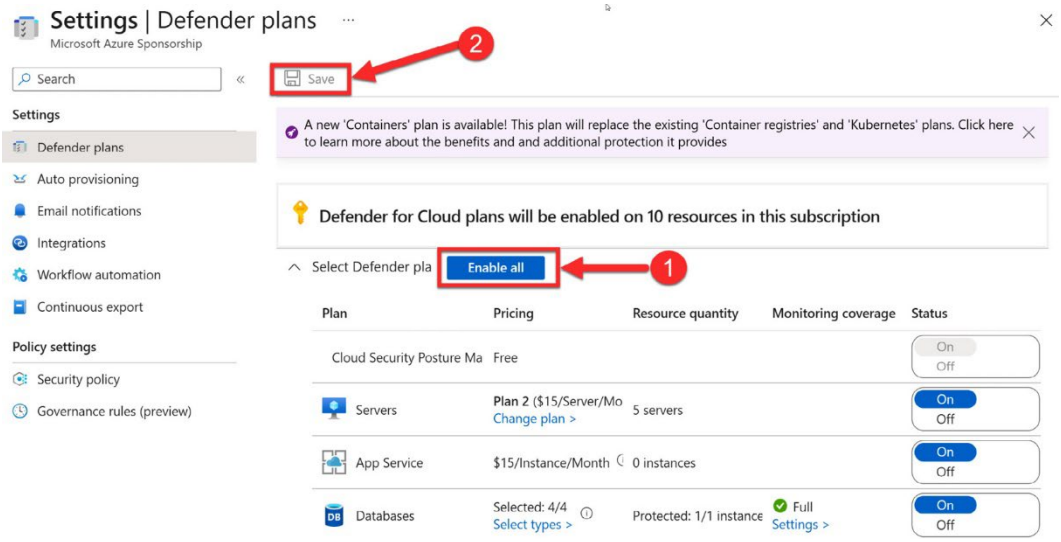
Name
Max score
Current score
Potential score increase
Enable MFA
10
0.00
+ 18%
MFA should be ena...
MFA should be ena...

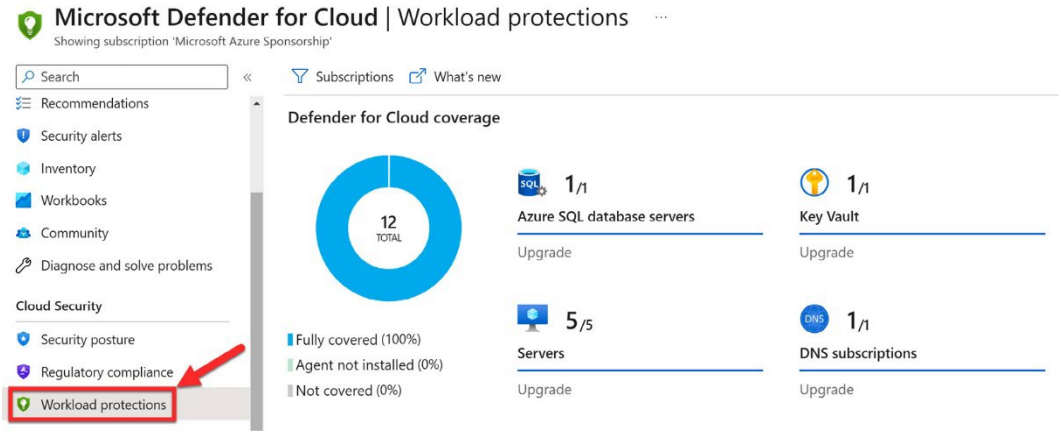

Home > Microsoft Defender for Cloud | Security posture > Recommendations >
MFA should be enabled on accounts with owner permissions on subscriptions
Exempt
View policy definition
Open query
Multiple changes to identity recommendations will be available soon. Learn more
Description
Multi-Factor Authentication (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

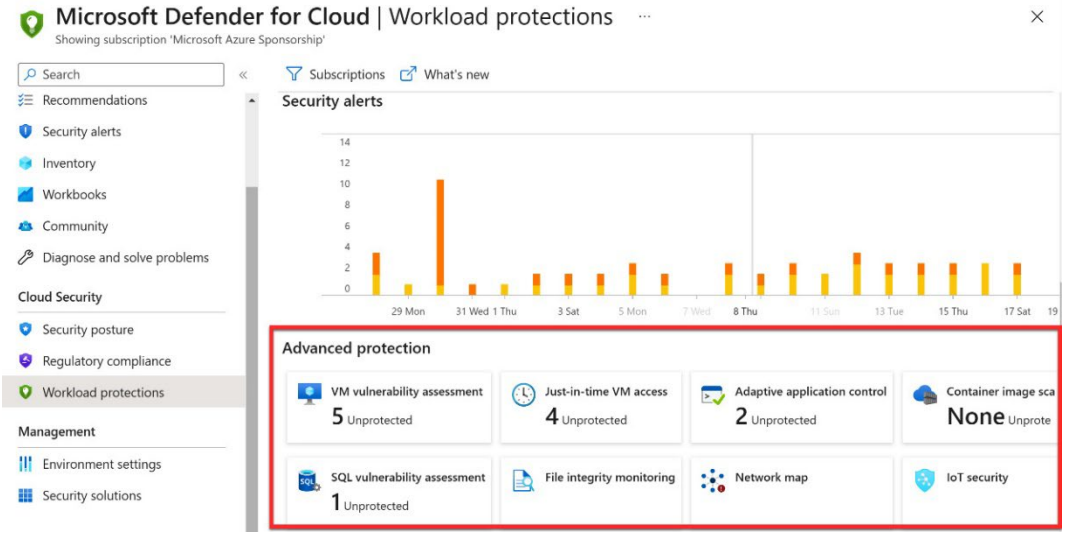

Azure Services
Virtual Machine
Virtual Machine Linux
Application Service
Storage Account
SQL
SQL Database
Container Kubernetes Service
Container Registry
Key Vault
Hybrid Cloud Protection
Azure Arc Service
aws
Defender Alerts
Advanced Protection
Vulnerability Assessments

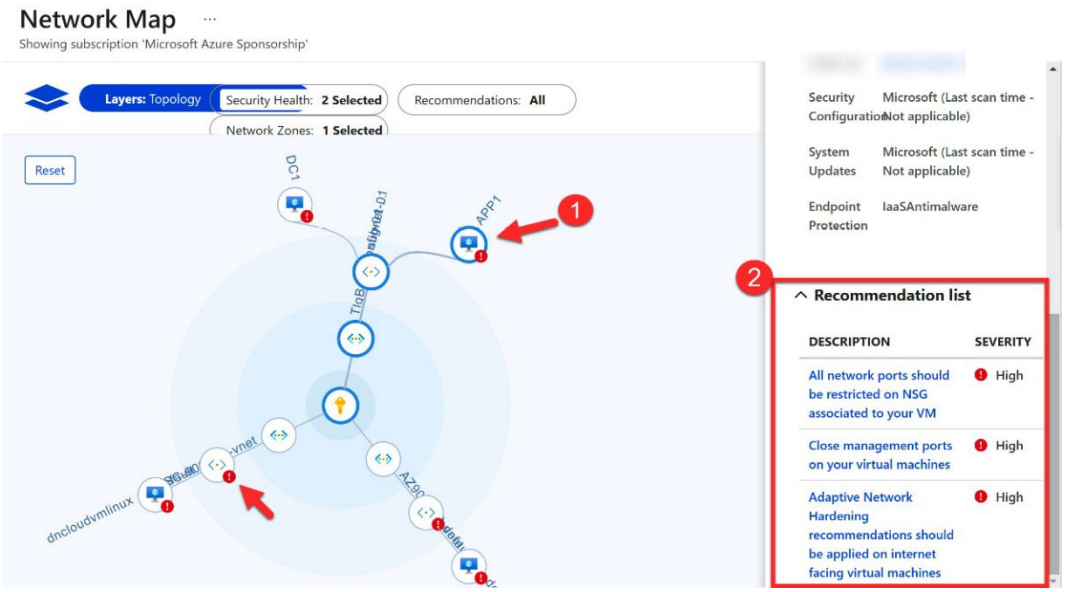

https://portal.azure.com/#home
Microsoft Azure
Microsoft defender for cloud
Azure services
Create a
Services
See all
Microsoft Defender for Cloud
Azure Database for MySQL servers
Microsoft Defender for IoT

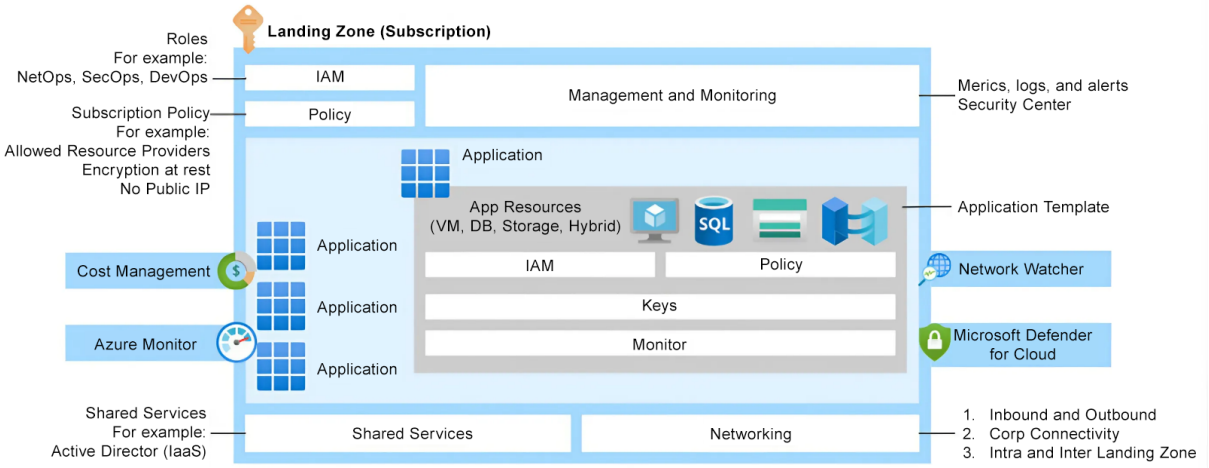

Microsoft Defender for Cloud | Overview
Showing subscription 'Microsoft Azure Sponsorship'
Search (Ctrl+/)
Subscriptions
What's new
Security alerts
Inventory
Workbooks
Community
Diagnose and solve problems
Cloud Security
Security posture
Regulatory compliance
Workload protections
Firewall Manager
Management
Environment settings
Security solutions
Workflow automation
1
Azure subscriptions
1
AWS accounts
27
Assessed resources
46
Active recommendations
58
Security alerts
Security posture
14/14
Unassigned recommendation
0/0
Overdue recommendations
Secure score
35%
SECURE SCORE
Azure
35%
AWS
GCP
Regulatory compliance
Azure Security Benchmark
26 of 43 passed controls
Lowest compliance regulatory standards
by passed controls
SOC TSP
1/13
ISO 27001:2013
4/17
PCI DSS 3.2.1
11/43

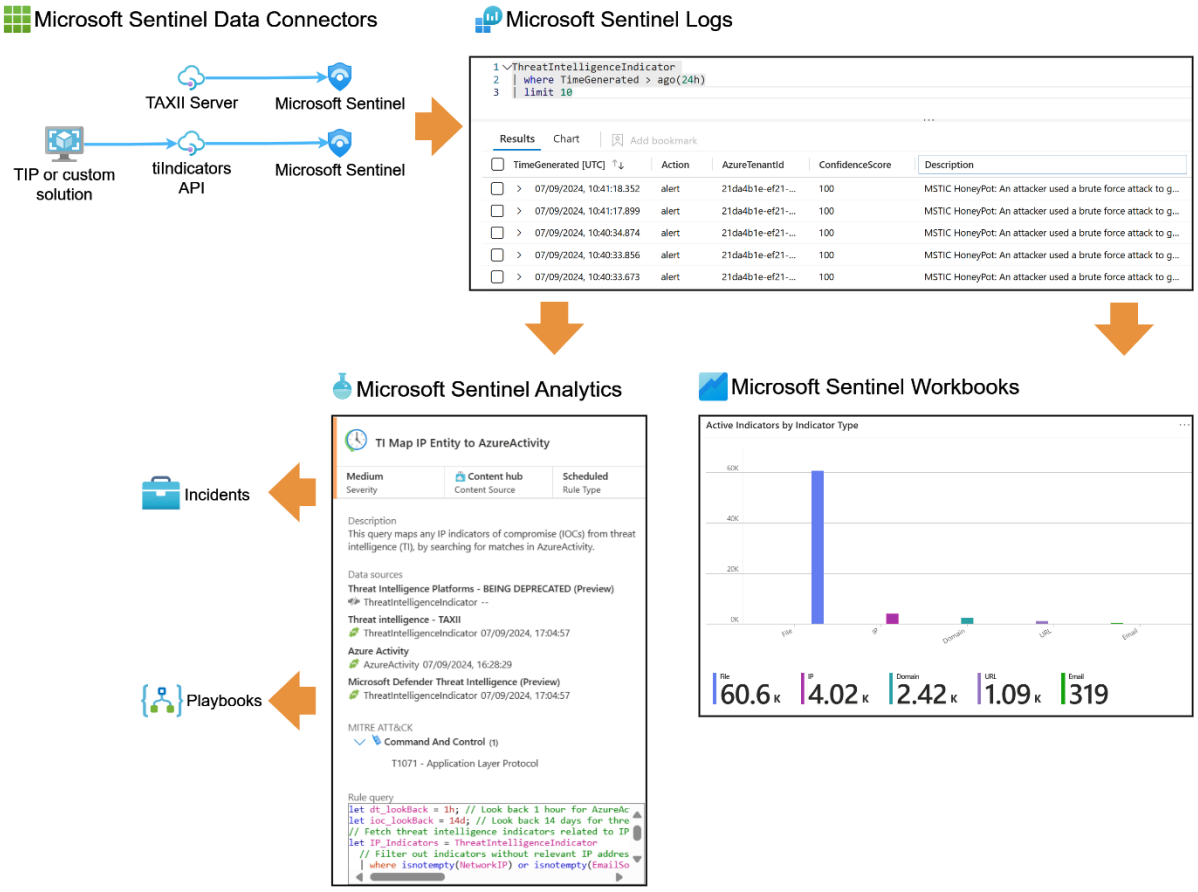

Settings | Defender plans
Microsoft Azure Sponsorship
Search
Save
2
Settings
Defender plans
Auto provisioning
Email notifications
Integrations
Workflow automation
Continuous export
Policy settings
Security policy
Governance rules (preview)
A new 'Containers' plan is available! This plan will replace the existing 'Container registries' and 'Kubernetes' plans. Click here to learn more about the benefits and and additional protection it provides
Defender for Cloud plans will be enabled on 10 resources in this subscription
Select Defender pla
Enable all
1
Plan
Pricing
Resource quantity
Monitoring coverage
Status
Cloud Security Posture Ma
Free
On
Off
Servers
Plan 2 ($15/Server/Mo
Change plan >
5 servers
On
Off
App Service
$15/Instance/Month
0 instances
On
Off
Databases
Selected: 4/4
Select types >
Protected: 1/1 instance
Full
Settings >
On
Off


Microsoft Defender for Cloud | Workload protections
Showing subscription 'Microsoft Azure Sponsorship'
Search
Subscriptions
What's new
Recommendations
Security alerts
Inventory
Workbooks
Community
Diagnose and solve problems
Cloud Security
Security posture
Regulatory compliance
Workload protections
Defender for Cloud coverage
12
TOTAL
Fully covered (100%)
Agent not installed (0%)
Not covered (0%)
1/1
Azure SQL database servers
Upgrade
1/1
Key Vault
Upgrade
5/5
Servers
Upgrade
1/1
DNS subscriptions
Upgrade


Microsoft Defender for Cloud | Workload protections
Showing subscription 'Microsoft Azure Sponsorship'
Search
Subscriptions
What's new
Recommendations
Security alerts
Inventory
Workbooks
Community
Diagnose and solve problems
Cloud Security
Security posture
Regulatory compliance
Workload protections
Management
Environment settings
Security solutions
Security alerts
14
12
10
8
6
4
2
0
29 Mon
31 Wed 1 Thu
3 Sat
5 Mon
8 Thu
13 Tue
15 Thu
17 Sat
Advanced protection
VM vulnerability assessment
5 Unprotected
Just-in-time VM access
4 Unprotected
Adaptive application control
2 Unprotected
Container image sca
None Unprote
SQL vulnerability assessment
1 Unprotected
File integrity monitoring
Network map
IoT security


Network Map
Showing subscription 'Microsoft Azure Sponsorship'
Layers: Topology
Security Health: 2 Selected
Recommendations: All
Network Zones: 1 Selected
Reset
DC1
APP1
1
dncloudvmlinux
Security Configuration
Microsoft (Last scan time - Not applicable)
System Updates
Microsoft (Last scan time - Not applicable)
Endpoint Protection
IaaSAntimalware
2
Recommendation list
DESCRIPTION
SEVERITY
All network ports should be restricted on NSG associated to your VM
High
Close management ports on your virtual machines
High
Adaptive Network Hardening recommendations should be applied on internet facing virtual machines
High

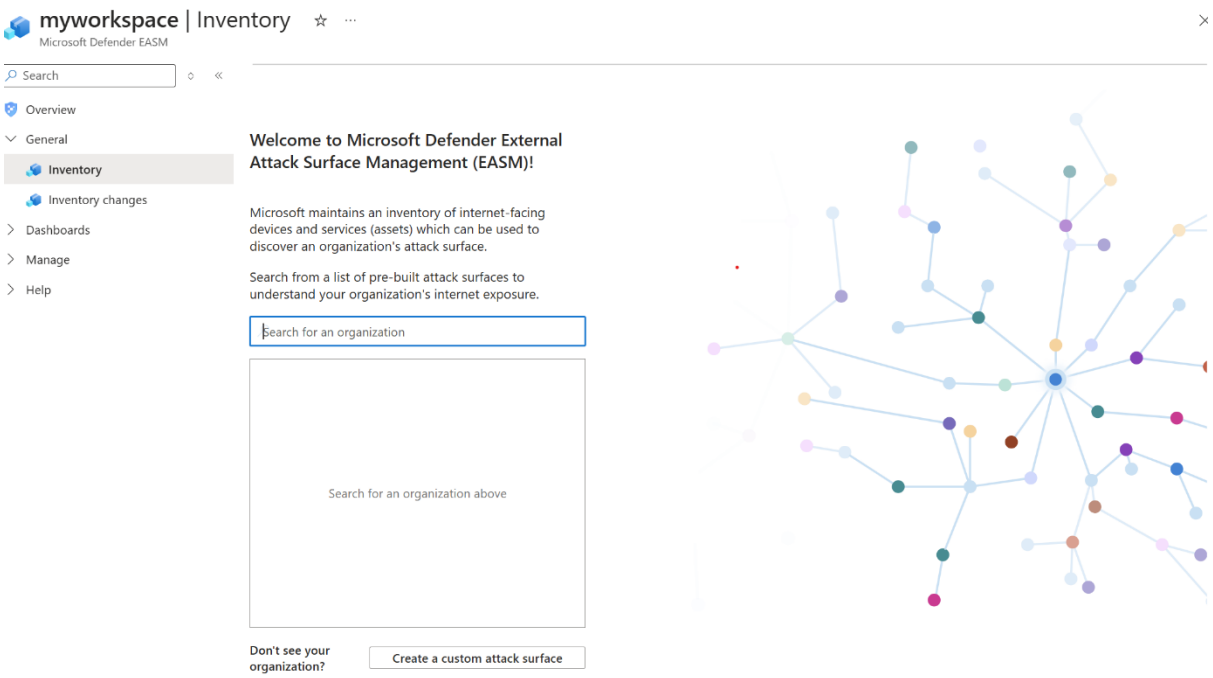

Landing Zone (Subscription)
Roles
For example:
NetOps, SecOps, DevOps
IAM
Management and Monitoring
Merics, logs, and alerts
Security Center
Subscription Policy
For example:
Allowed Resource Providers
Encryption at rest
No Public IP
Policy
Application
App Resources
(VM, DB, Storage, Hybrid)
SQL
Application Template
Application
IAM
Policy
Cost Management
Network Watcher
Application
Keys
Azure Monitor
Application
Monitor
Microsoft Defender for Cloud
Shared Services
For example:
Active Director (IaaS)
Shared Services
Networking
1. Inbound and Outbound
2. Corp Connectivity
3. Intra and Inter Landing Zone



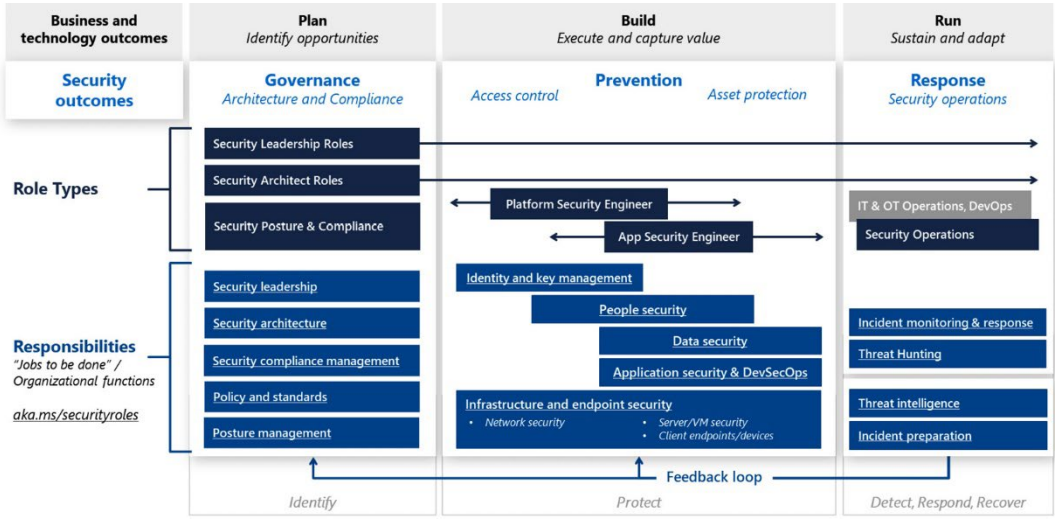
Likelihood			
Very Likely	Acceptable risk Medium 2	Unacceptable risk High 3	Unacceptable risk Extreme 5
Likely	Acceptable risk Low 1	Acceptable risk Medium 2	Unacceptable risk High 3
Unlikely	Acceptable risk Low 1	Acceptable risk Low 1	Acceptable risk Medium 2
What is the chance that it will happen?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

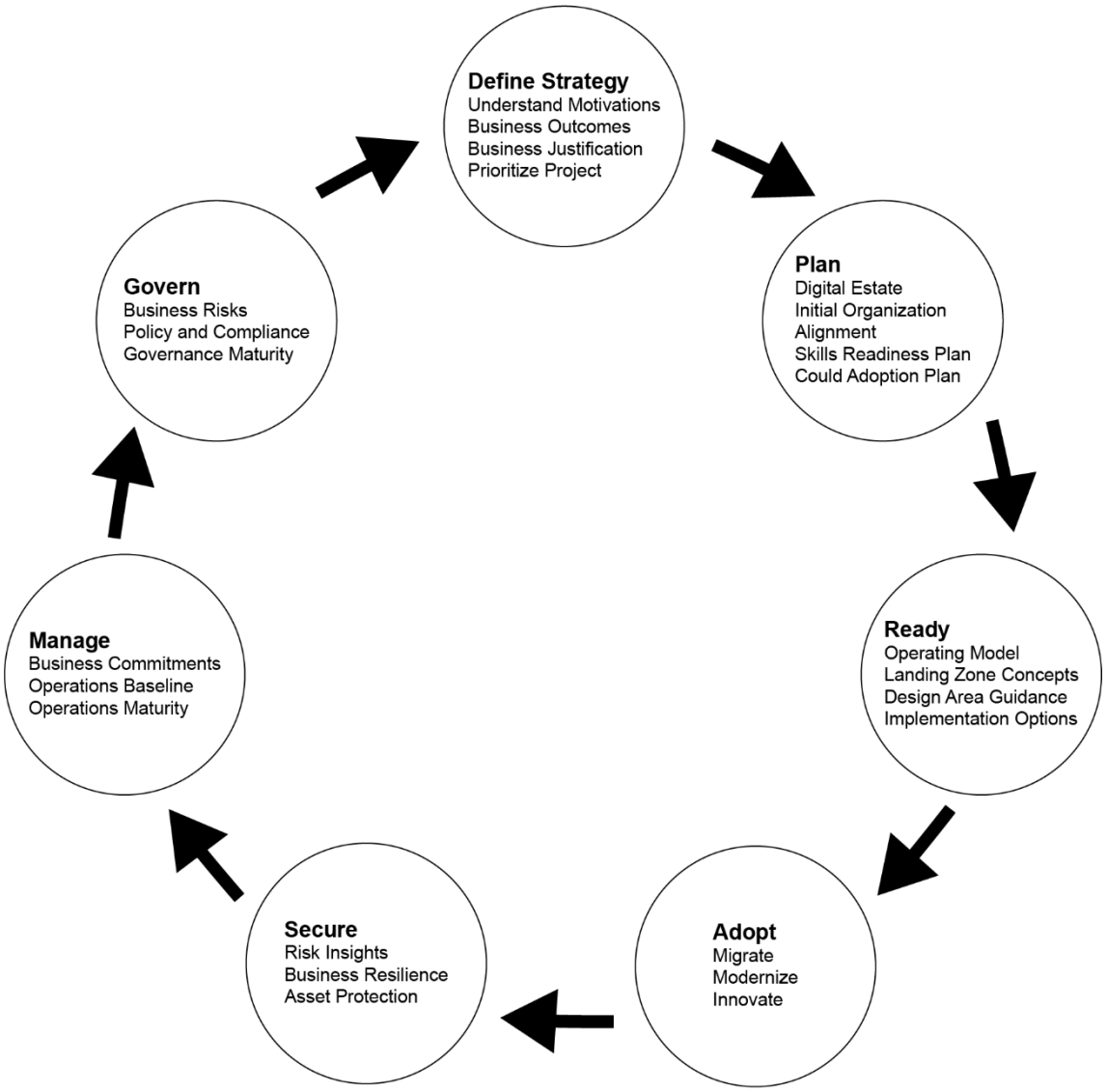
Impact
How serious is the risk?


Identification
Assessment
Response
Monitoring and reporting

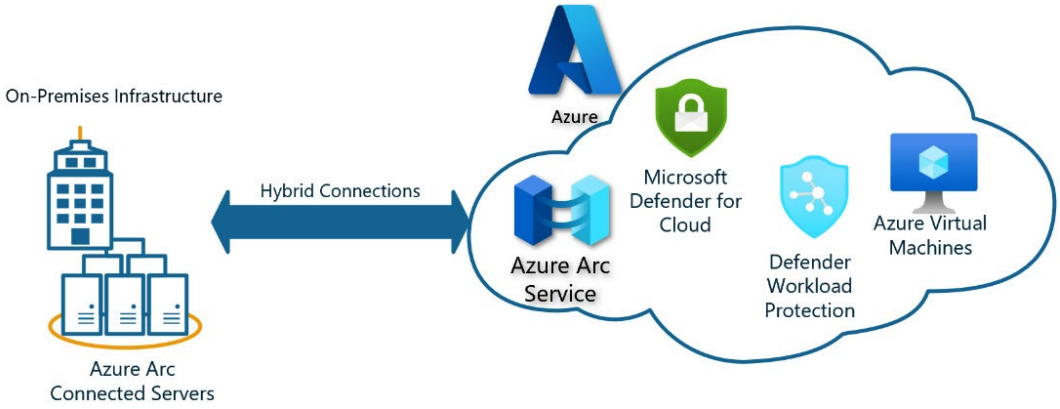

myworkspace | Inventory
Microsoft Defender EASM
Search
Overview
General
Inventory
Inventory changes
Dashboards
Manage
Help
Welcome to Microsoft Defender External Attack Surface Management (EASM)!
Microsoft maintains an inventory of internet-facing devices and services (assets) which can be used to discover an organization's attack surface.
Search from a list of pre-built attack surfaces to understand your organization's internet exposure.
Search for an organization
Search for an organization above
Don't see your organization?
Create a custom attack surface

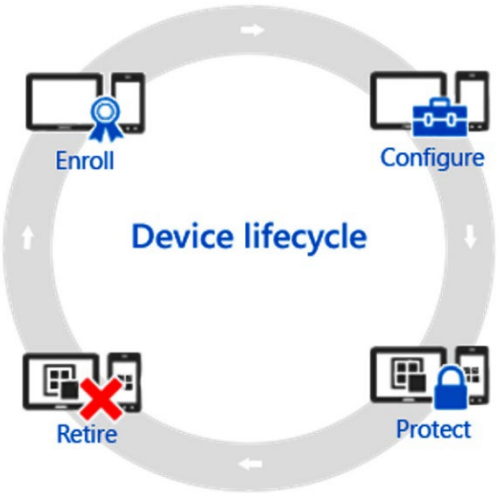
Chapter 7: Design a Strategy for Securing Server and Client Endpoints

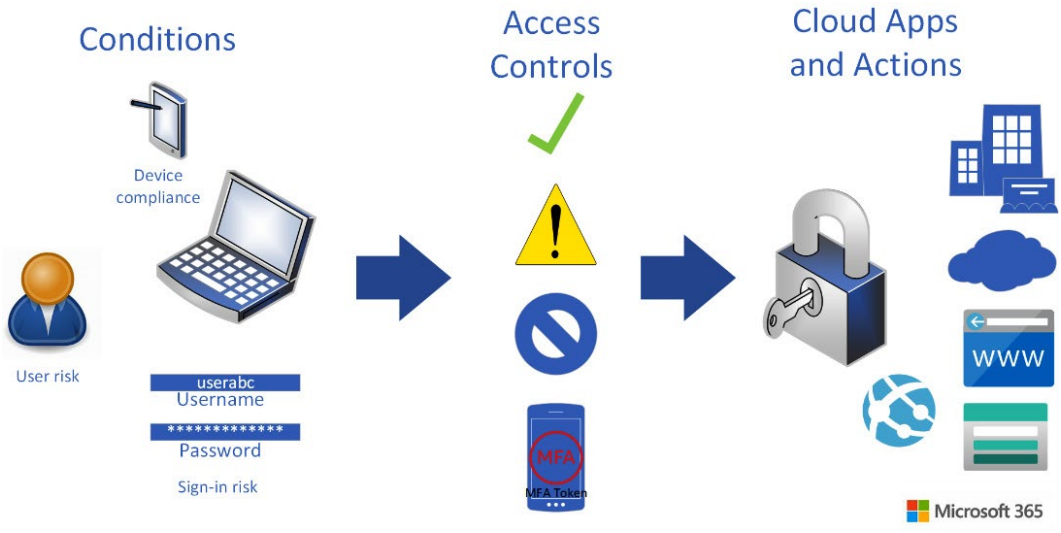


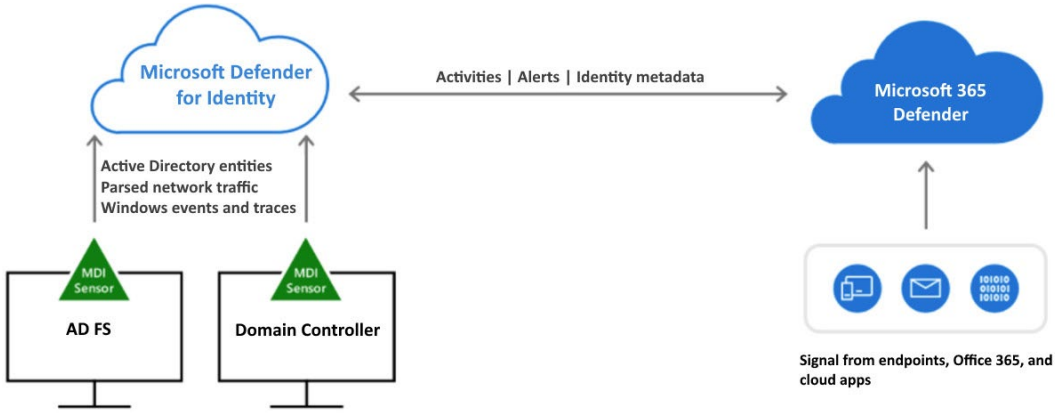


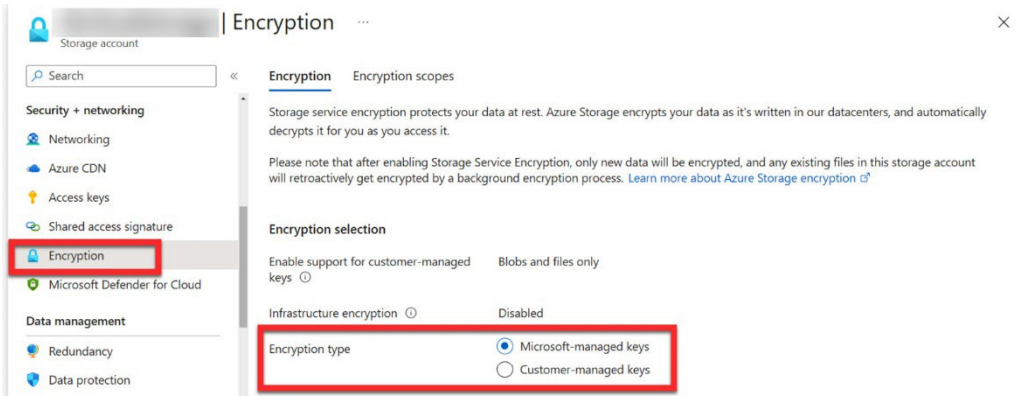

Microsoft Endpoint Manager admin center
Home > Endpoint security | Overview > Endpoint security
Endpoint security | Security baselines
Search
Overview
Overview
All devices
Security baselines
Security tasks
Manage
Manage and monitor the baseline security status of all your enrolled devices. For more information 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

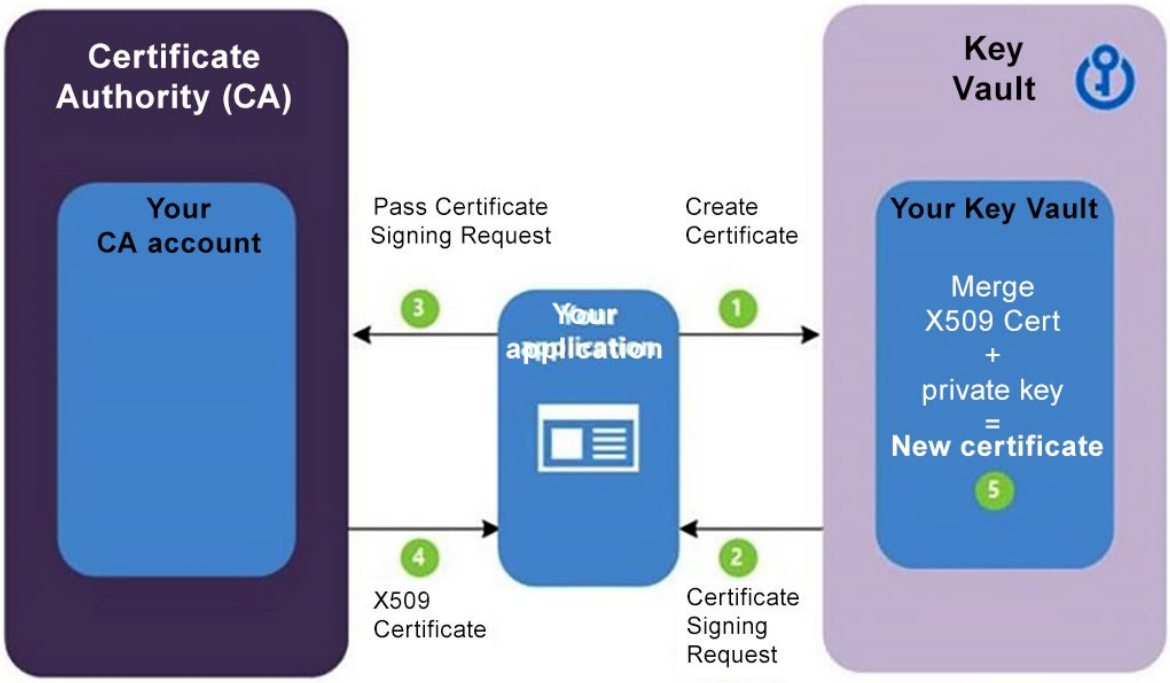

On-Premises Infrastructure
Azure
Hybrid Connections
Microsoft Defender for Cloud
Azure Virtual Machines
Azure Arc Service
Defender Workload Protection
Azure Arc Connected Servers

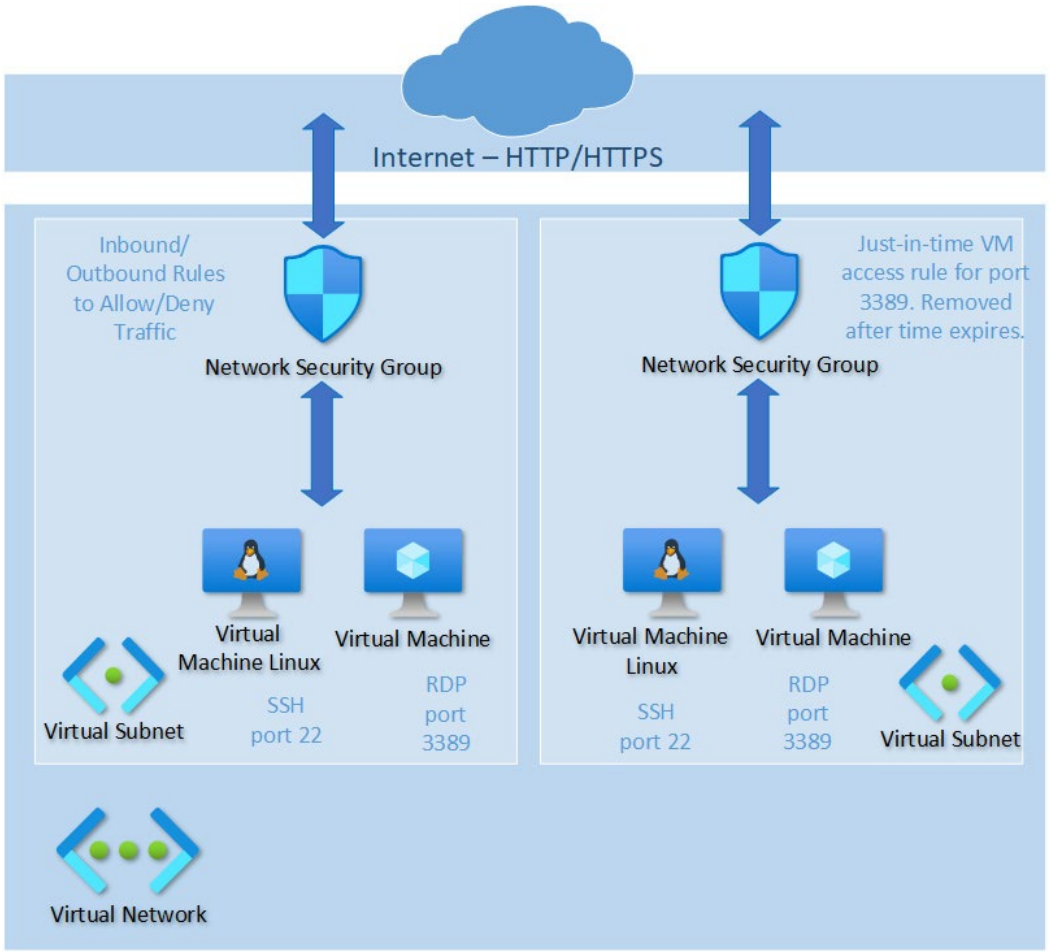

Enroll
Configure
Device lifecycle
Retire
Protect

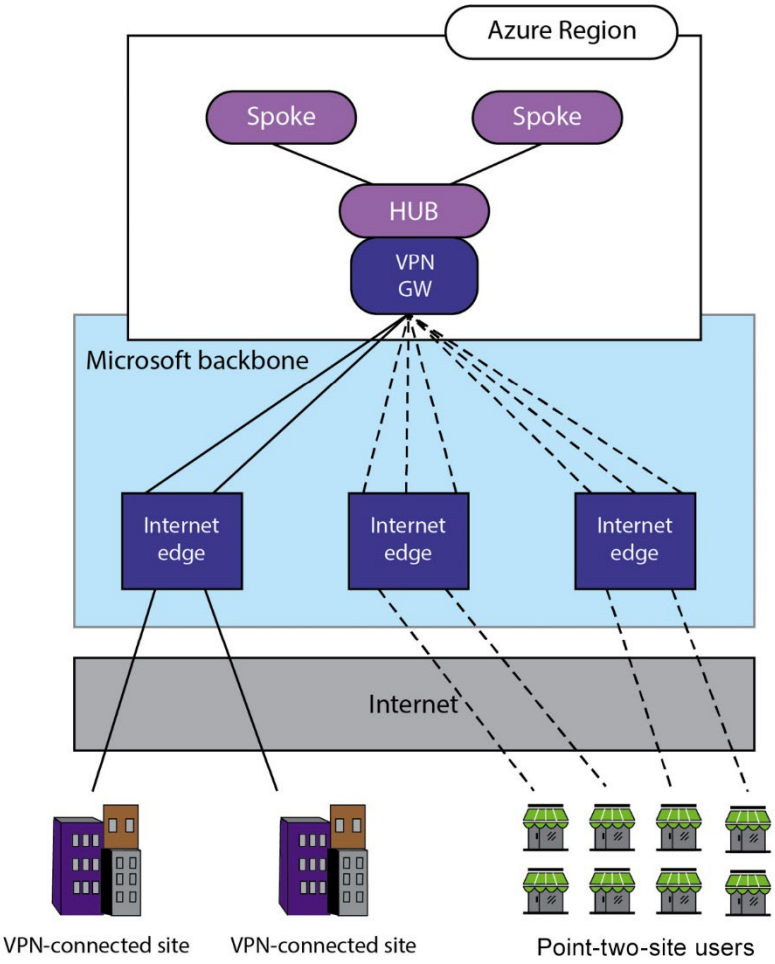

Conditions
Access Controls
Cloud Apps and Actions
Device compliance
User risk
userabc
Username
****
Password
Sign-in risk
MFA
MFA Token
WWW
Microsoft 365


Microsoft Defender for Identity
Activities | Alerts | Identity metadata
Microsoft 365 Defender
Active Directory entities
Parsed network traffic
Windows events and traces
MDI Sensor
AD FS
MDI Sensor
Domain Controller
Signal from endpoints, Office 365, and cloud apps

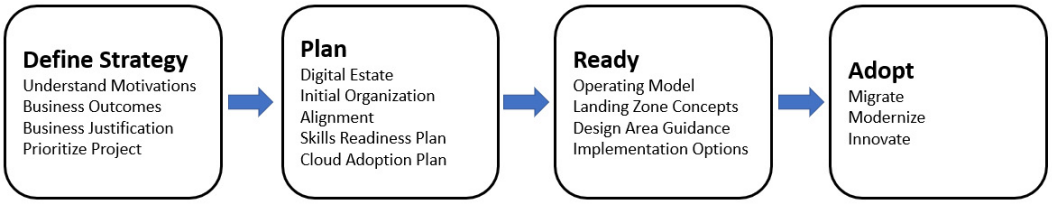

| Encryption
Storage account
Search
Encryption
Encryption scopes
Security + networking
Networking
Azure CDN
Access keys
Shared access signature
Encryption
Microsoft Defender for Cloud
Data management
Redundancy
Data protection
Storage service encryption protects your data at rest. Azure Storage encrypts your data as it's written in our datacenters, and automatically decrypts it for you as you access it.
Please note that after enabling Storage Service Encryption, only new data will be encrypted, and any existing files in this storage account will retroactively get encrypted by a background encryption process. Learn more about Azure Storage encryption
Encryption selection
Enable support for customer-managed keys
Blobs and files only
Infrastructure encryption
Disabled
Encryption type
Microsoft-managed keys
Customer-managed keys


Certificate Authority (CA)
Your CA account
Key Vault
Your Key Vault
Merge X509 Cert + private key = New certificate
5
Pass Certificate Signing Request
Create Certificate
3
Your application
1
4
X509 Certificate
2
Certificate Signing Request

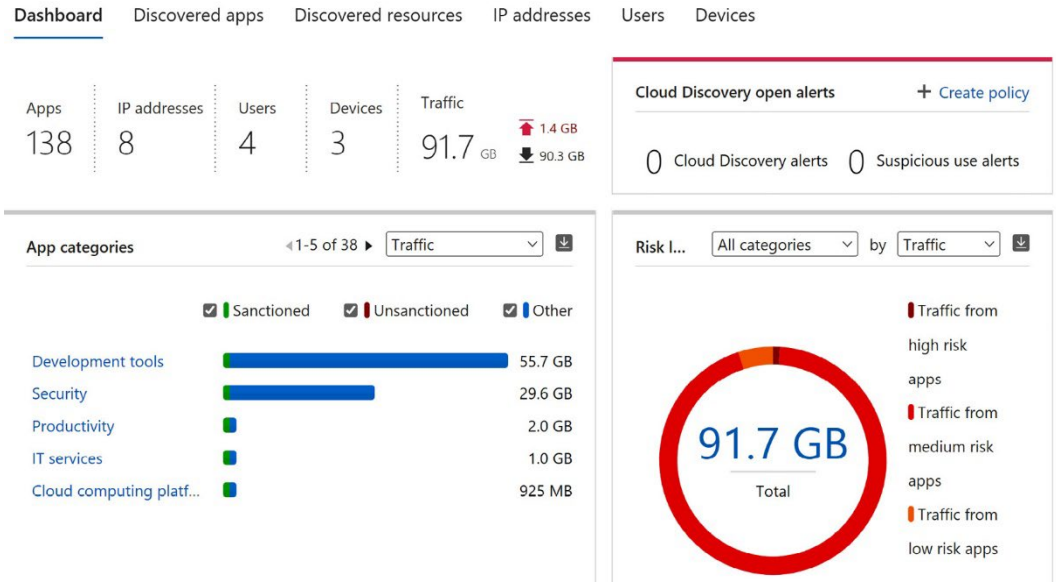

Internet – HTTP/HTTPS
Inbound/ Outbound Rules to Allow/Deny Traffic
Network Security Group
Just-in-time VM access rule for port 3389. Removed after time expires.
Network Security Group
Virtual Machine Linux
SSH port 22
Virtual Machine
RDP port 3389
Virtual Subnet
Virtual Machine Linux
SSH port 22
Virtual Machine
RDP port 3389
Virtual Subnet
Virtual Network

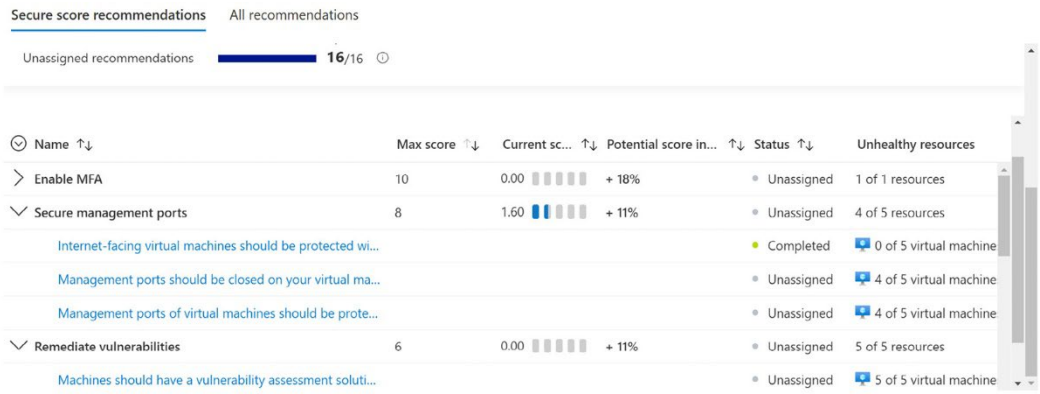

Azure Region
Spoke
Spoke
HUB
VPN
GW
Microsoft backbone
Internet
edge
Internet
edge
Internet
edge
Internet
VPN-connected site
VPN-connected site
Point-two-site users

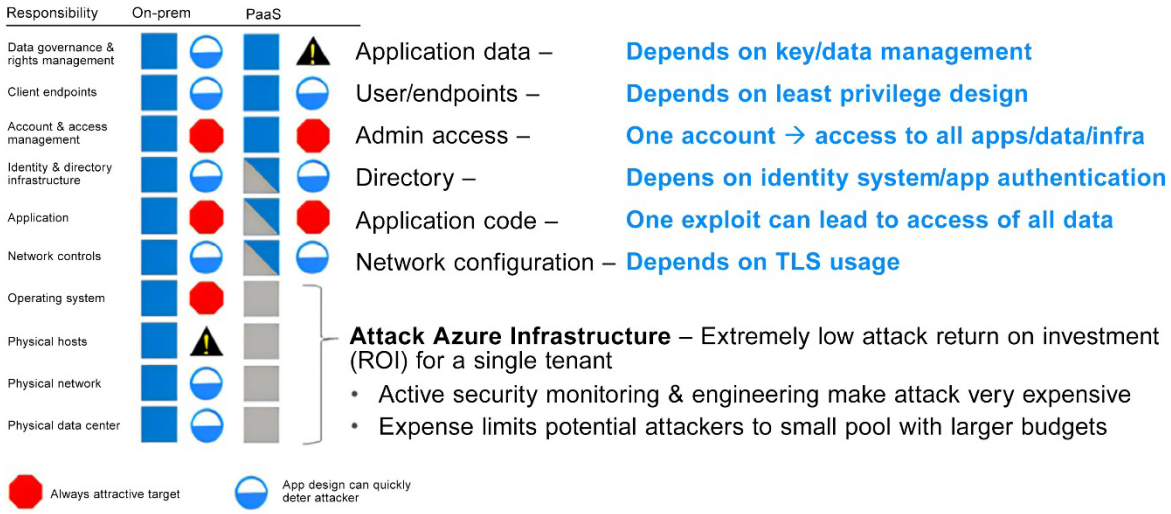
Chapter 8: Design a Strategy for Securing SaaS, PaaS, and IaaS

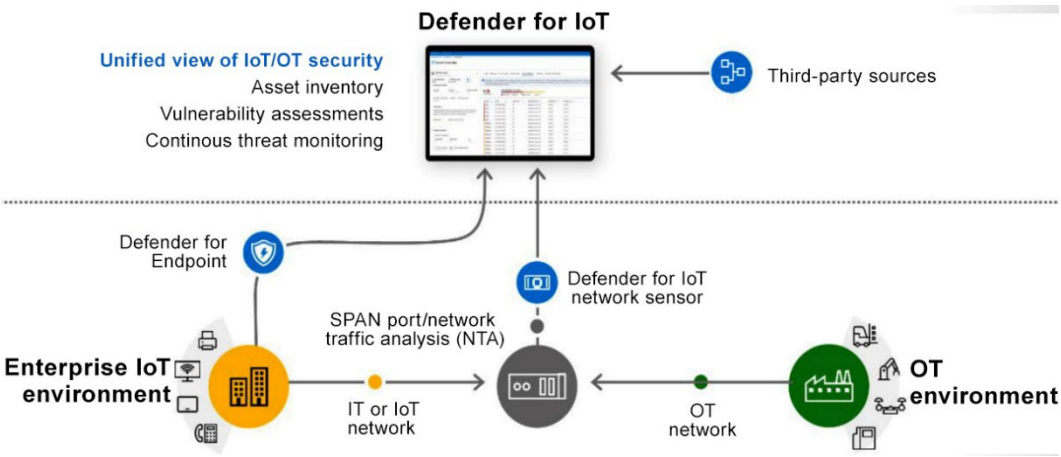


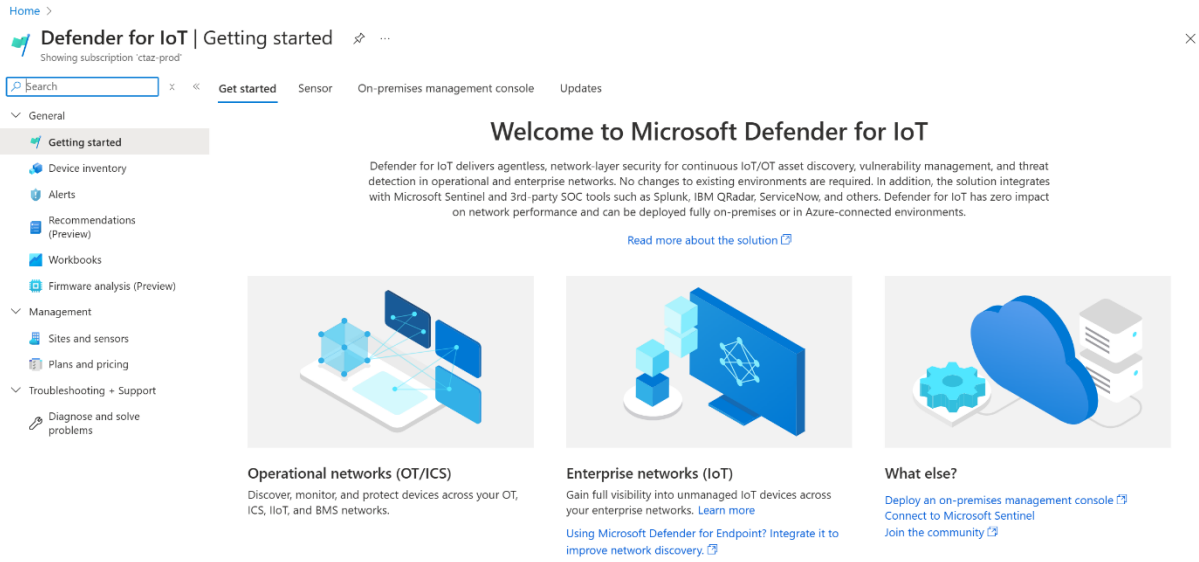
Responsibility	On-premises	IaaS	PaaS	SaaS
Data governance and rights management	Customer	Customer	Customer	Customer
Client endpoints	Customer	Customer	Customer	Customer
Account and access management	Customer	Customer	Customer	Customer
Identity and directory infrastructure	Customer	Customer	Microsoft/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

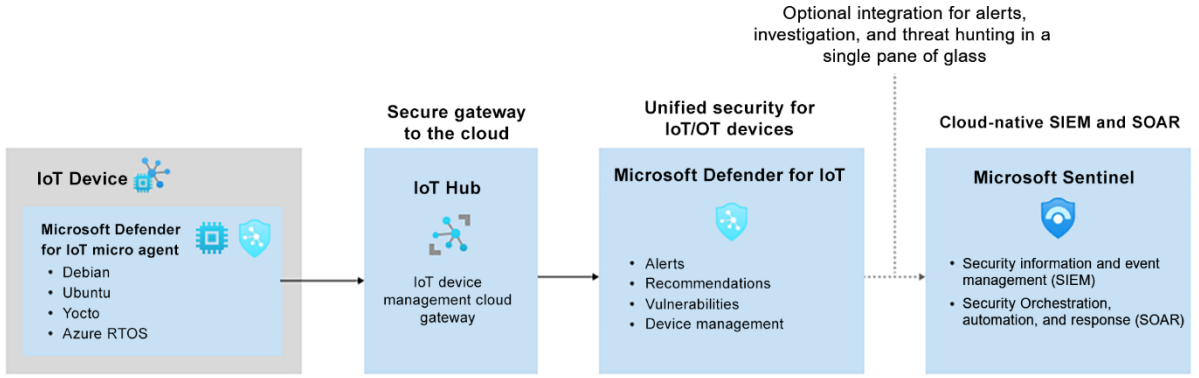


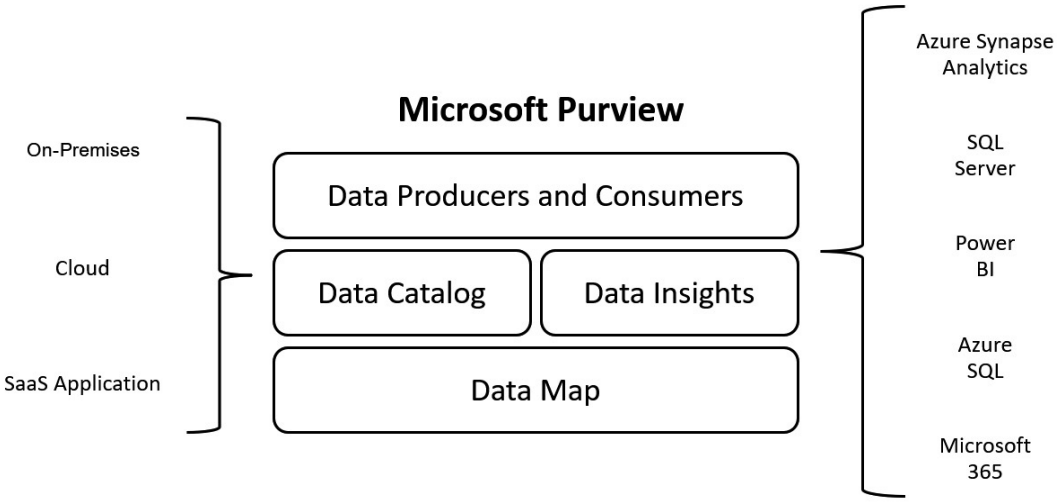

Secure score recommendations
All recommendations
Unassigned recommendations
16/16
Name
Max score
Current sc...
Potential score in...
Status
Unhealthy resources
Enable MFA
10
0.00
+ 18%
Unassigned
1 of 1 resources
Secure management ports
8
1.60
+ 11%
Unassigned
4 of 5 resources
Internet-facing virtual machines should be protected wi...
Completed
0 of 5 virtual machine
Management ports should be closed on your virtual ma...
Unassigned
4 of 5 virtual machine
Management ports of virtual machines should be prote...
Unassigned
4 of 5 virtual machine
Remediate vulnerabilities
6
0.00
+ 11%
Unassigned
5 of 5 resources
Machines should have a vulnerability assessment soluti...
Unassigned
5 of 5 virtual machine

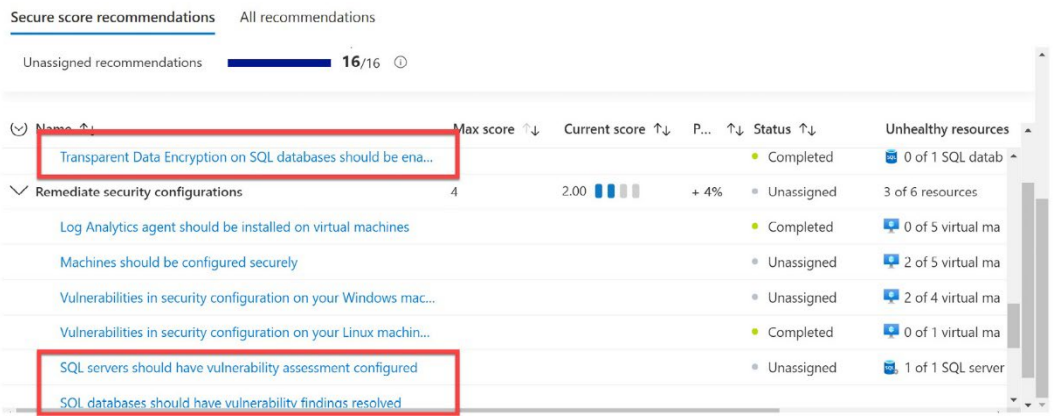

Responsibility
On-prem
PaaS
Data governance & rights management
Client endpoints
Account & access management
Identity & directory infrastructure
Application
Network controls
Operating system
Physical hosts
Physical network
Physical data center
Application data – Depends on key/data management
User/endpoints – Depends on least privilege design
Admin access – One account → access to all apps/data/infra
Directory – Depens on identity system/app authentication
Application code – One exploit can lead to access of all data
Network configuration – Depends on TLS usage
Attack Azure Infrastructure – Extremely low attack return on investment (ROI) for a single tenant
Active security monitoring & engineering make attack very expensive
Expense limits potential attackers to small pool with larger budgets
Always attractive target
App design can quickly deter attacker

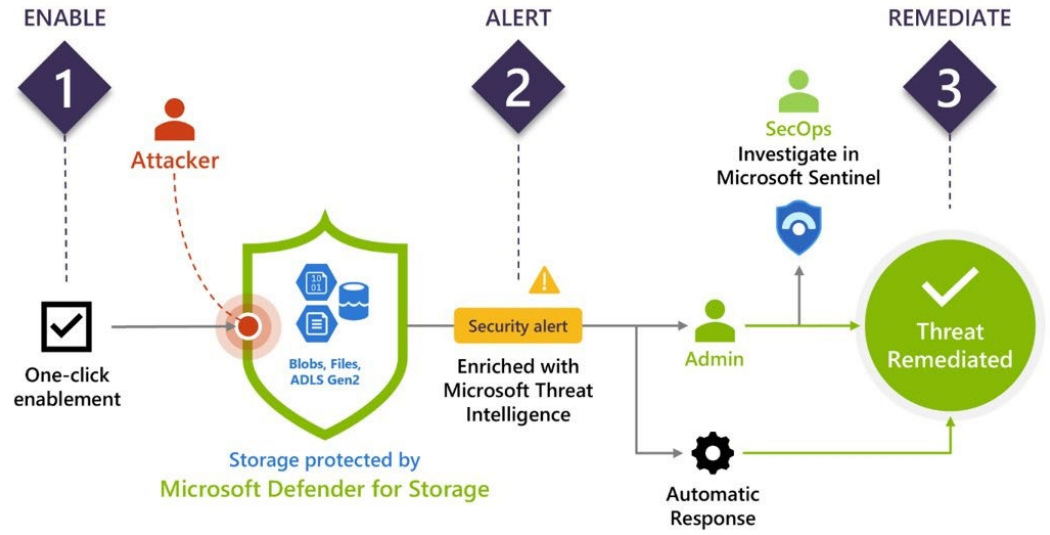

Defender for IoT
Unified view of IoT/OT security
Asset inventory
Vulnerability assessments
Continous threat monitoring
Third-party sources
Defender for Endpoint
Defender for IoT network sensor
SPAN port/network traffic analysis (NTA)
Enterprise IoT environment
IT or IoT network
OT network
OT environment

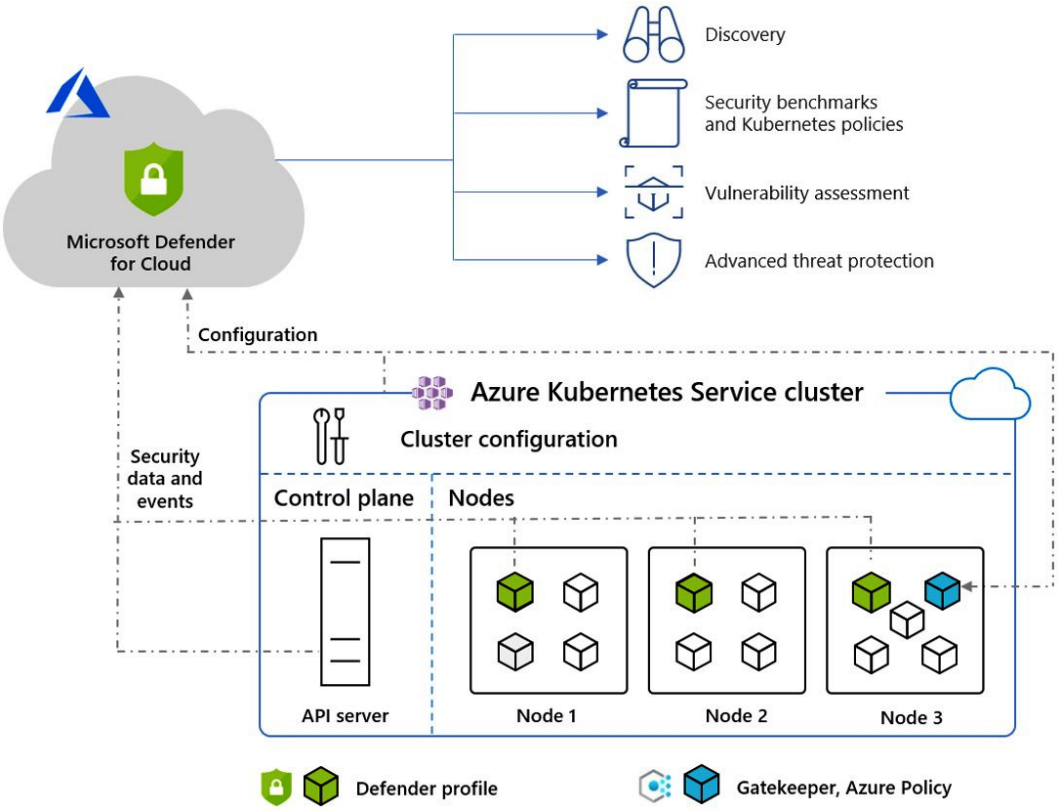

Home
Defender for IoT | Getting started
Showing subscription 'ctaz-prod'
Search
Get started
Sensor
On-premises management console
Updates
General
Getting started
Device inventory
Alerts
Recommendations (Preview)
Workbooks
Firmware analysis (Preview)
Management
Sites and sensors
Plans and pricing
Troubleshooting + 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
Using Microsoft Defender for Endpoint? Integrate it to improve network discovery.
What else?
Deploy an on-premises management console
Connect to Microsoft Sentinel
Join the community

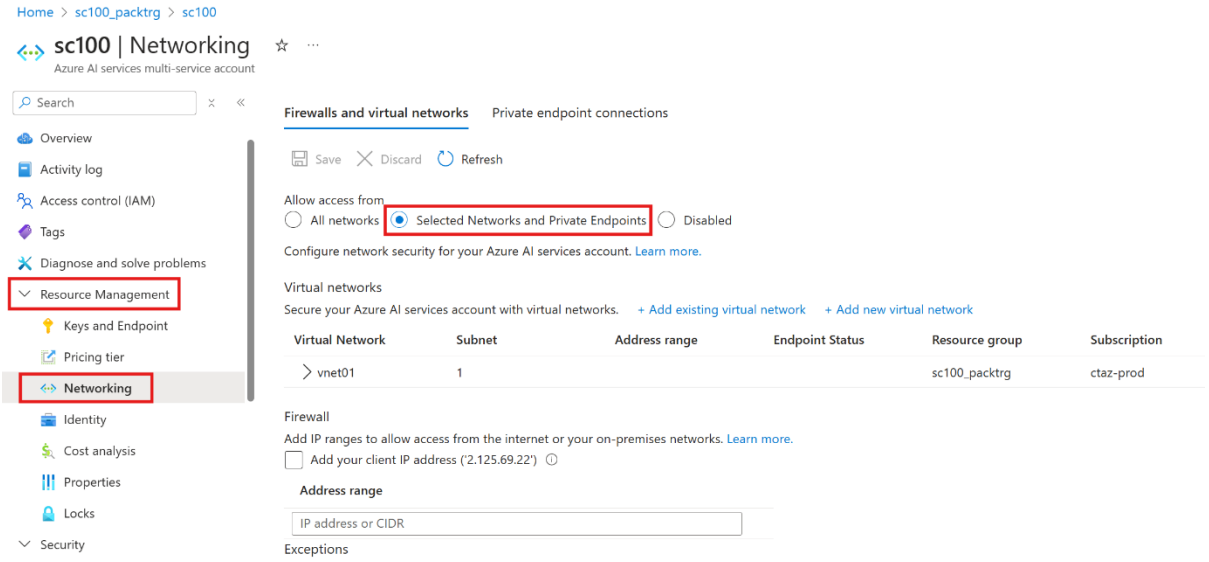

Optional integration for alerts, investigation, and threat hunting in a single pane of glass
IoT Device
Microsoft Defender for IoT micro agent
Debian
Ubuntu
Yocto
Azure RTOS
Secure gateway to the cloud
IoT Hub
IoT device management cloud gateway
Unified security for IoT/OT devices
Microsoft Defender for IoT
Alerts
Recommendations
Vulnerabilities
Device management
Cloud-native SIEM and SOAR
Microsoft Sentinel
Security information and event management (SIEM)
Security Orchestration, automation, and response (SOAR)


Microsoft Purview
On-Premises
Cloud
SaaS Application
Data Producers and Consumers
Data Catalog
Data Insights
Data Map
Azure Synapse Analytics
SQL Server
Power BI
Azure SQL
Microsoft 365

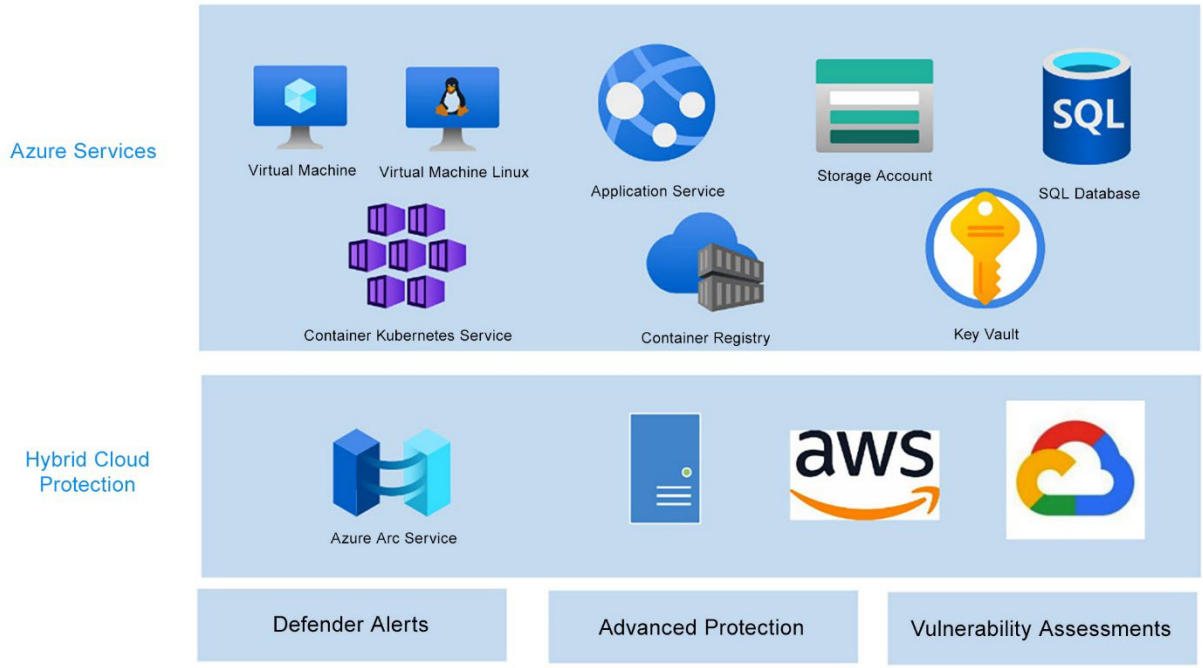

Secure score recommendations
All recommendations
Unassigned recommendations
16/16
Name
Max score
Current score
P...
Status
Unhealthy resources
Transparent Data Encryption on SQL databases should be ena...
Completed
0 of 1 SQL datab
Remediate security configurations
4
2.00
+ 4%
Unassigned
3 of 6 resources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

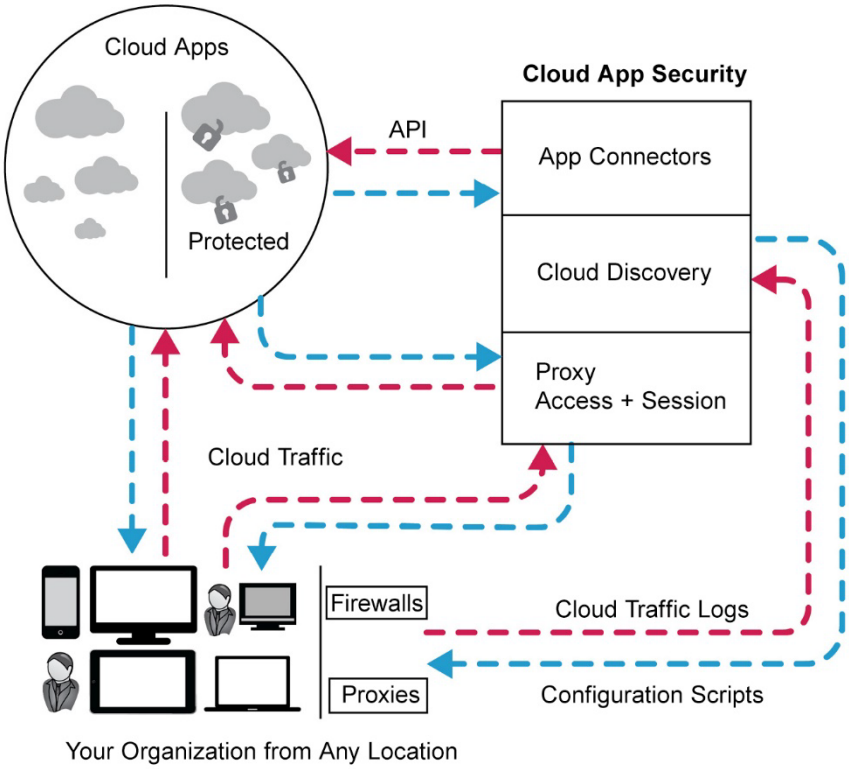

ENABLE
ALERT
REMEDIATE
1
2
3
Attacker
SecOps
Investigate in
Microsoft Sentinel
One-click
enablement
Blobs, Files,
ADLS Gen2
Storage protected by
Microsoft Defender for Storage
Security alert
Enriched with
Microsoft Threat
Intelligence
Admin
Threat
Remediated
Automatic
Response

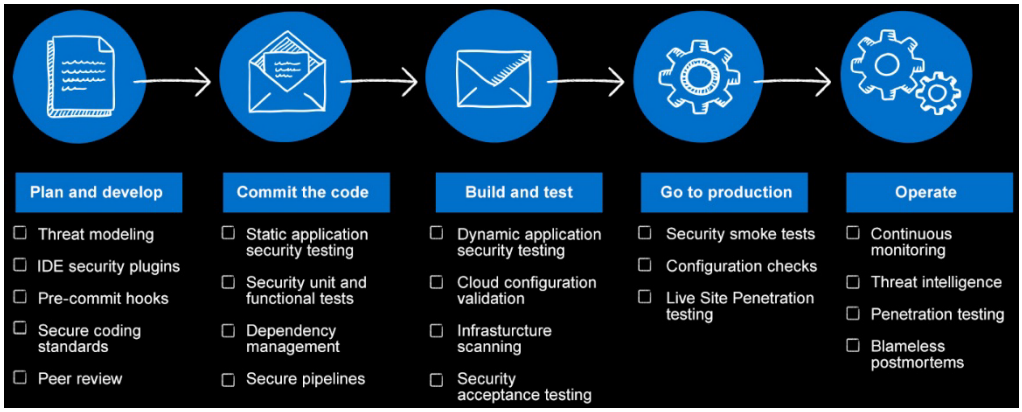

Discovery
Security benchmarks
and Kubernetes policies
Vulnerability assessment
Advanced threat protection
Microsoft Defender
for Cloud
Configuration
Azure Kubernetes Service cluster
Cluster configuration
Security
data and
events
Control plane
Nodes
API server
Node 1
Node 2
Node 3
Defender profile
Gatekeeper, Azure Policy

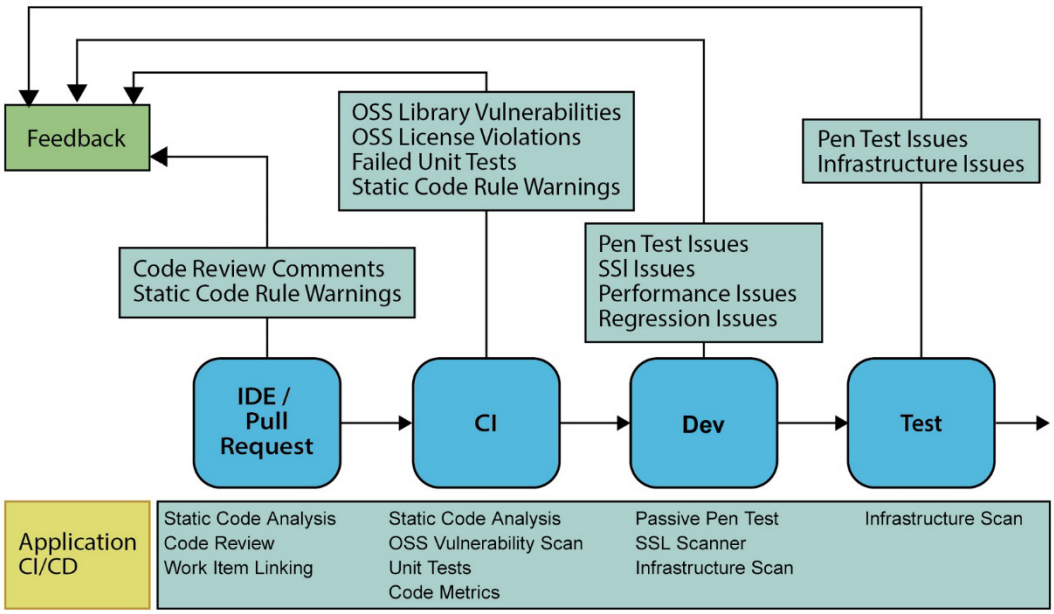

Home > sc100_packtrg > sc100
sc100 | Networking
Azure AI services multi-service account
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Resource Management
Keys and Endpoint
Pricing tier
Networking
Identity
Cost analysis
Properties
Locks
Security
Firewalls and virtual networks
Private endpoint connections
Save
Discard
Refresh
Allow access from
All networks
Selected Networks and Private Endpoints
Disabled
Configure network security for your Azure AI services account. Learn more.
Virtual networks
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
Add IP ranges to allow access from the internet or your on-premises networks. Learn more.
Add your client IP address ('2.125.69.22')
Address range
IP address or CIDR
Exceptions

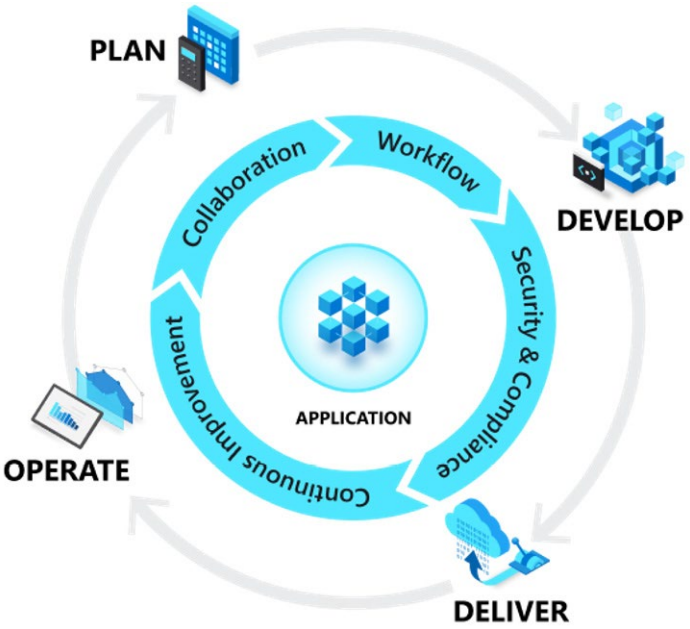
Chapter 9: Specify Security Requirements for Applications



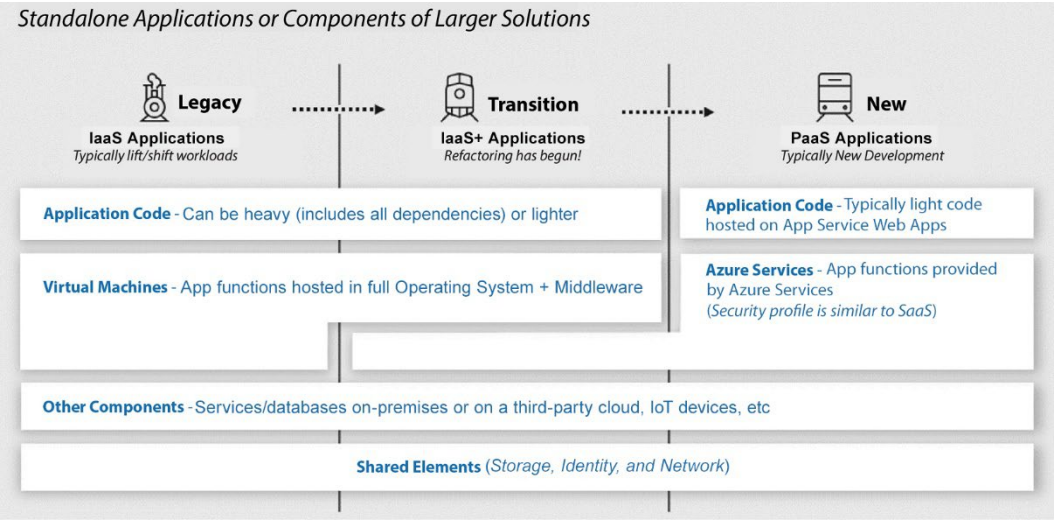



Plan and develop
Threat modeling
IDE security plugins
Pre-commit hooks
Secure coding standards
Peer review
Commit the code
Static application security testing
Security unit and functional tests
Dependency management
Secure pipelines
Build and test
Dynamic application security testing
Cloud configuration validation
Infrastructure scanning
Security acceptance testing
Go to production
Security smoke tests
Configuration checks
Live Site Penetration testing
Operate
Continuous monitoring
Threat intelligence
Penetration testing
Blameless postmortems


Feedback
OSS Library Vulnerabilities
OSS License Violations
Failed Unit Tests
Static Code Rule Warnings
Pen Test Issues
Infrastructure Issues
Code Review Comments
Static Code Rule Warnings
Pen Test Issues
SSl Issues
Performance Issues
Regression Issues
IDE / Pull Request
CI
Dev
Test
Application CI/CD
Static Code Analysis
Code Review
Work Item Linking
Static Code Analysis
OSS Vulnerability Scan
Unit Tests
Code Metrics
Passive Pen Test
SSL Scanner
Infrastructure Scan
Infrastructure Scan


PLAN
DEVELOP
DELIVER
OPERATE
Collaboration
Workflow
Security & Compliance
Continuous Improvement
APPLICATION


Devices
APIs
Data sources

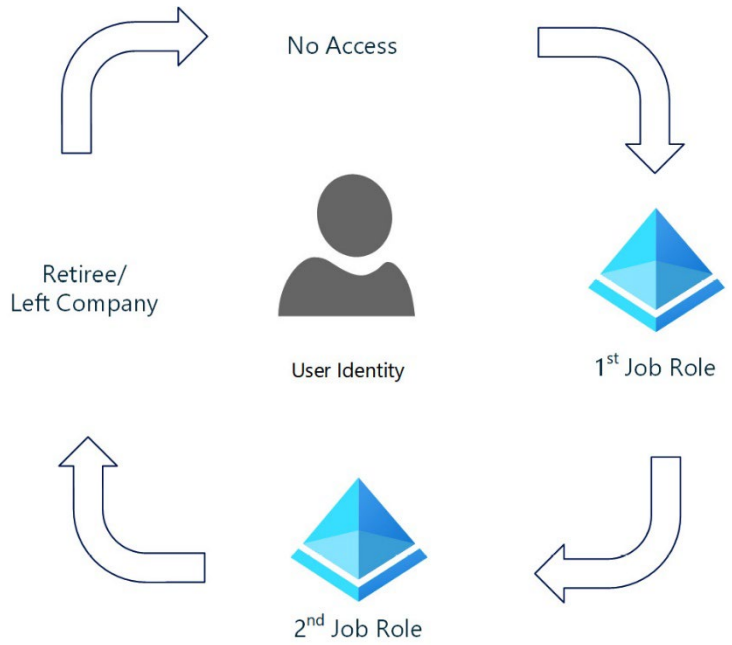

Standalone Applications or Components of Larger Solutions
Legacy
IaaS Applications
Typically lift/shift workloads
Transition
IaaS+ Applications
Refactoring has begun!
New
PaaS Applications
Typically New Development
Application Code - Can be heavy (includes all dependencies) or lighter
Application Code - Typically light code hosted on App Service Web Apps
Virtual Machines - App functions hosted in full Operating System + Middleware
Azure Services - App functions provided by Azure Services
(Security profile is similar to SaaS)
Other Components - Services/databases on-premises or on a third-party cloud, IoT devices, etc
Shared Elements (Storage, Identity, and Network)

Chapter 10: Design a Strategy for Securing Data

Likelihood

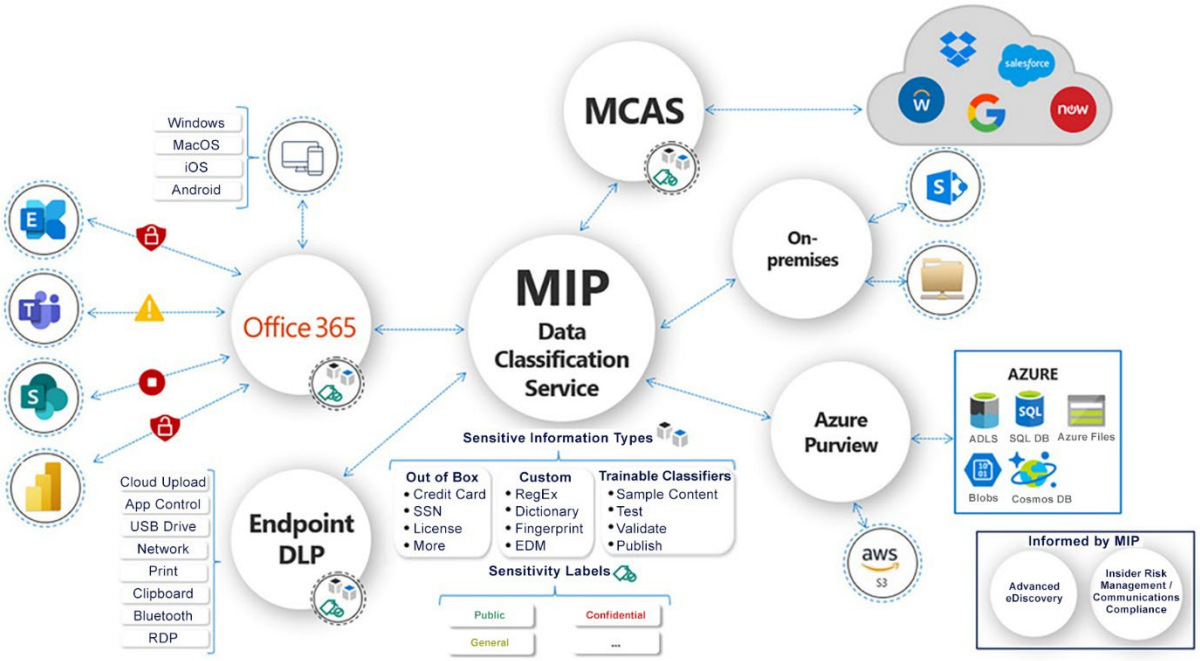
Very Likely	Acceptable risk Medium 2	Unacceptable risk High 3	Unacceptable risk Extreme 5
Likely	Acceptable risk Low 1	Acceptable risk Medium 2	Unacceptable risk High 3
Unlikely	Acceptable risk Low 1	Acceptable risk Low 1	Acceptable risk Medium 2
What is the chance that it will happen?	Minor	Moderate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

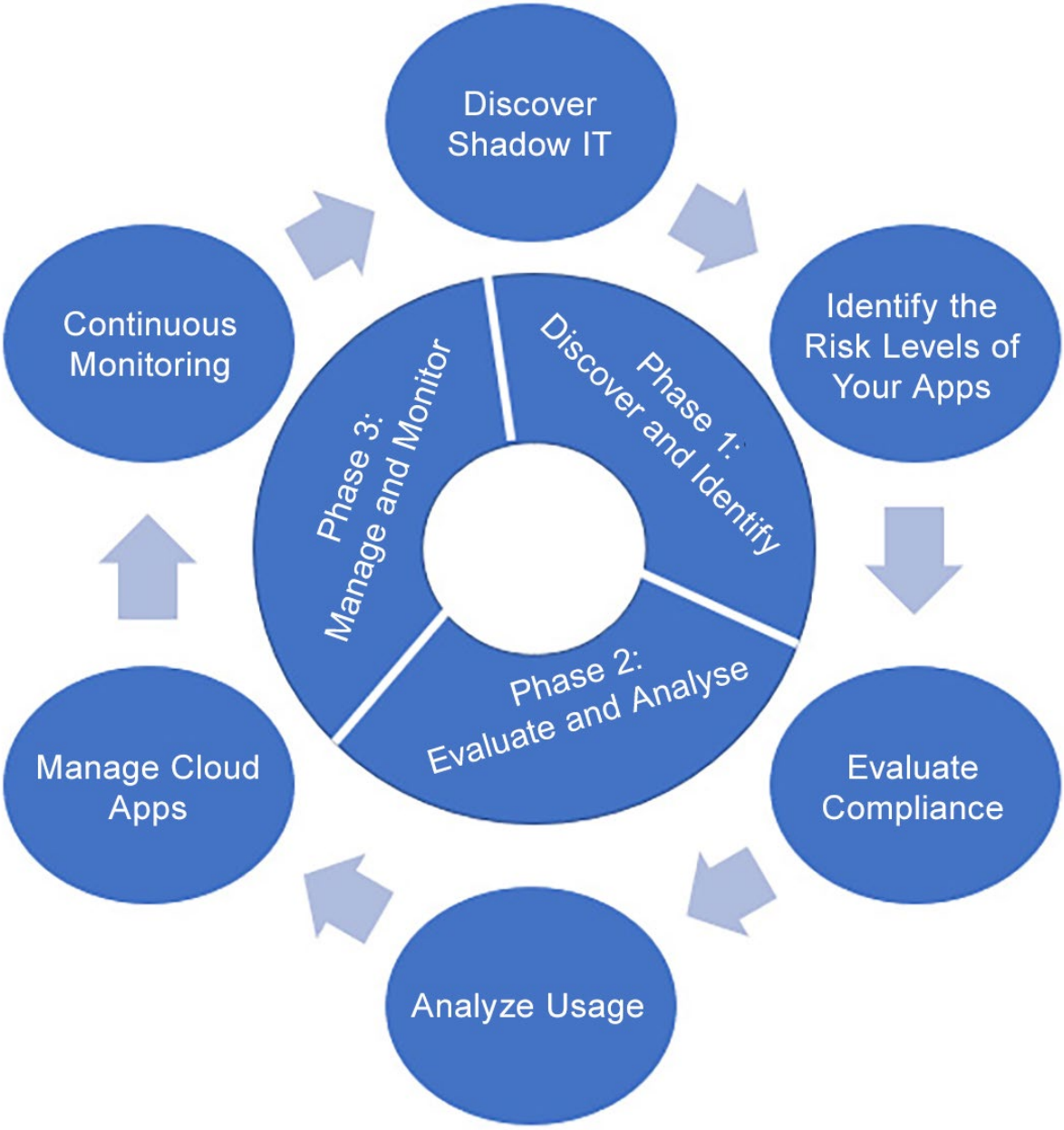
Impact
How serious is the risk?

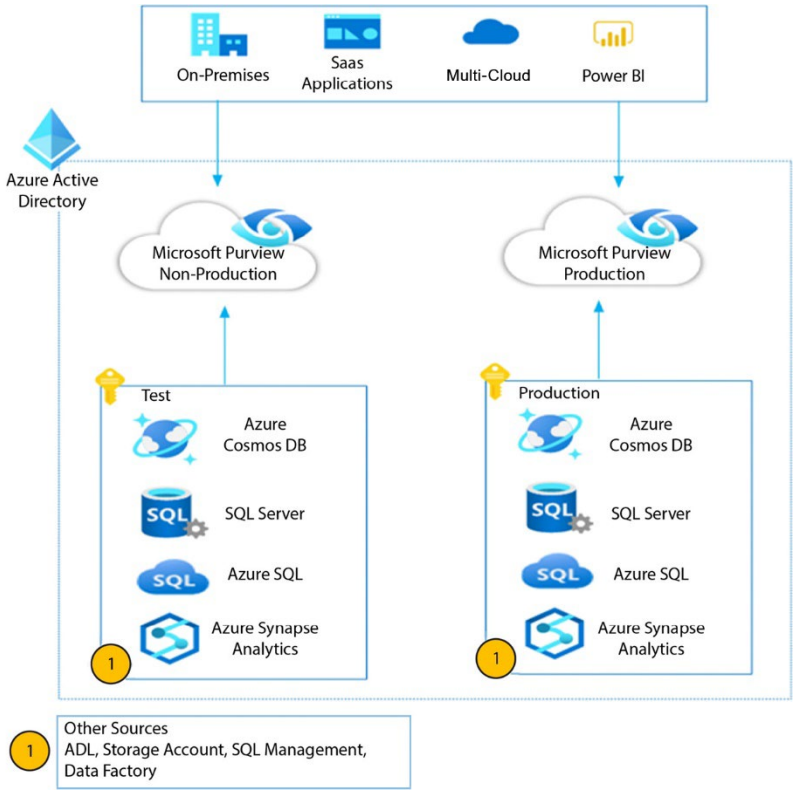

No Access
Retiree/
Left Company
User Identity
1st Job Role
2nd Job Role

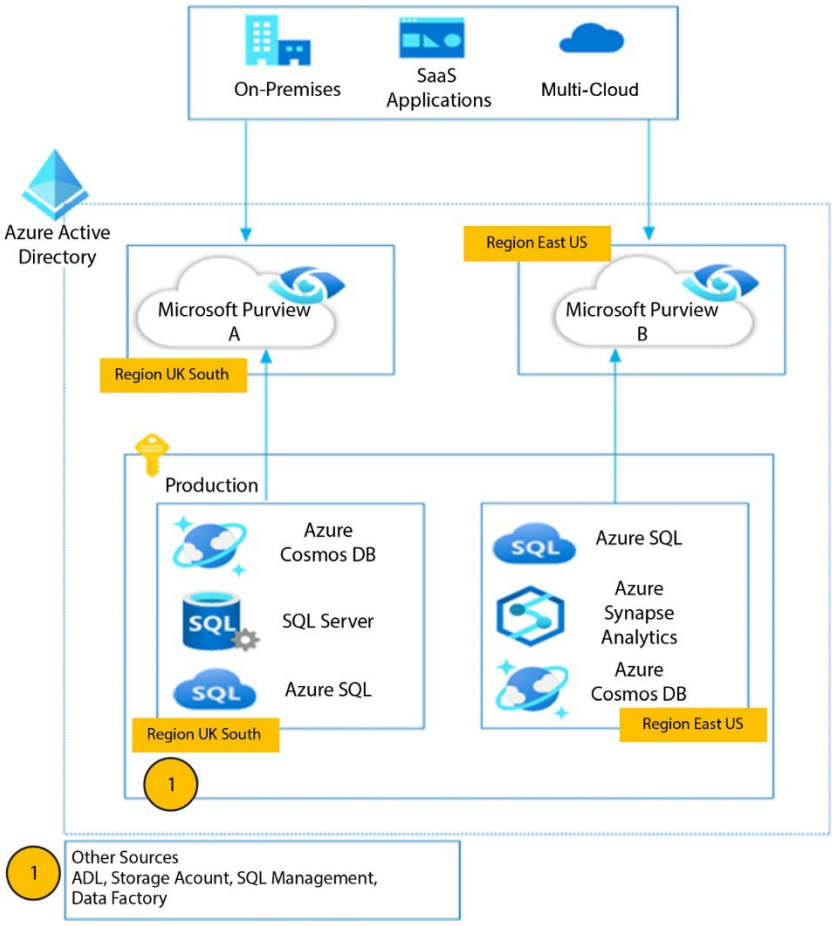

Understand your data landscape and identify important data across your hybrid environment
KNOW YOUR DATA
PREVENT DATA LOSS
Detect risky behavior and prevent accidental oversharing of sensitive information
Apply flexible protection actions including encryption, access restrictions and visual markings
PROTECT YOUR DATA
GOVERN YOUR DATA
Automatically retain, delete, and store data and records in a compliant manner

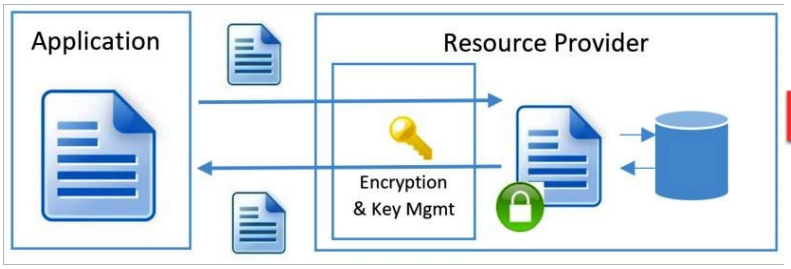

Understand your data landscape and identity important data across your hybrid environment
Know Your Data
Prevent Data Loss
Detect risky behavior and prevent accidental oversharing of sensitive information
Apply flexible protection actions including encryption, access restrictions, and visual markings
Protect Your Data
Govern Your Data
Automatically retain, delete, and store data and records in a compliant manner

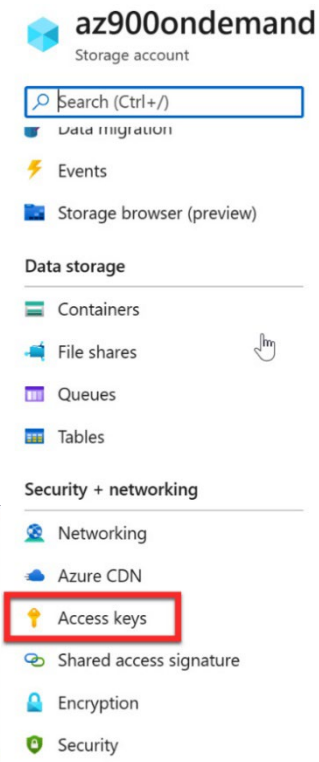

MCAS
Windows
MacOS
iOS
Android
Office 365
MIP
Data
Classification
Service
On-
premises
Azure
Purview
AZURE
ADLS
SQL DB
Azure Files
Blobs
Cosmos DB
Endpoint
DLP
Cloud Upload
App Control
USB Drive
Network
Print
Clipboard
Bluetooth
RDP
Sensitive Information Types
Out of Box
• Credit Card
• SSN
• License
• More
Custom
• RegEx
• Dictionary
• Fingerprint
• EDM
Trainable Classifiers
• Sample Content
• Test
• Validate
• Publish
Sensitivity Labels
Public
General
Confidential
...
Informed by MIP
Advanced
eDiscovery
Insider Risk
Management /
Communications
Compliance

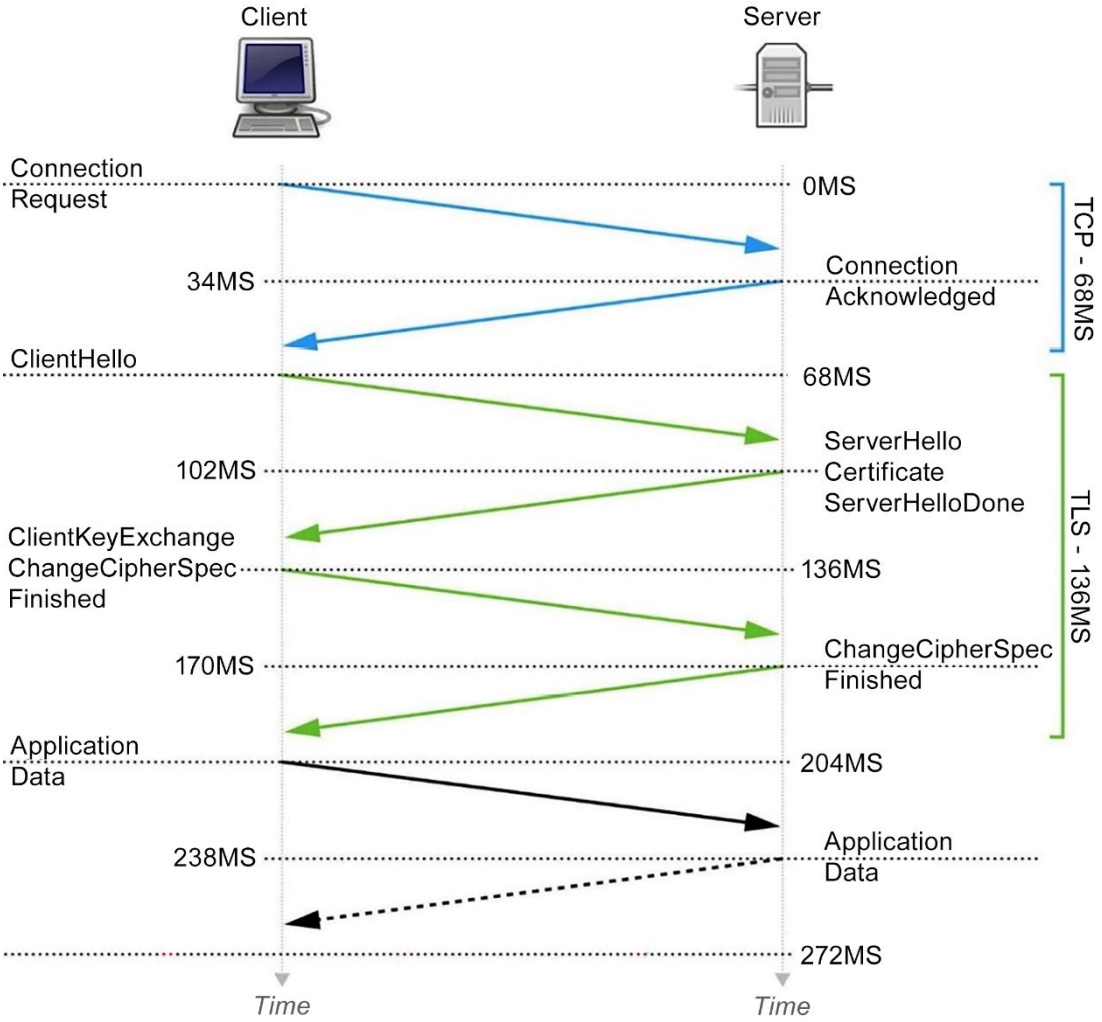

Discover Shadow IT
Identify the Risk Levels of Your Apps
Evaluate Compliance
Analyze Usage
Manage Cloud Apps
Continuous Monitoring
Phase 1: Discover and Identify
Phase 2: Evaluate and Analyse
Phase 3: Manage and Monitor

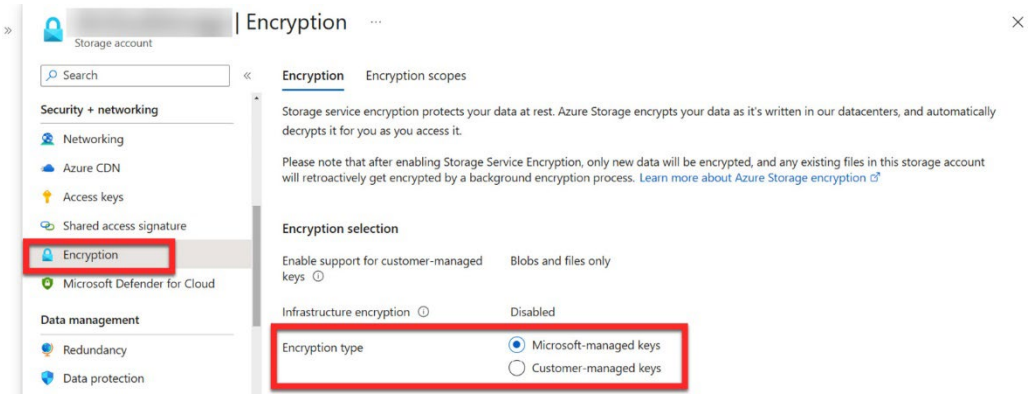

On-Premises
Saas Applications
Multi-Cloud
Power BI
Azure Active Directory
Microsoft Purview Non-Production
Microsoft Purview Production
Test
Azure Cosmos DB
SQL Server
Azure SQL
Azure Synapse Analytics
1
Production
Azure Cosmos DB
SQL Server
Azure SQL
Azure Synapse Analytics
1
1
Other Sources
ADL, Storage Account, SQL Management, Data Factory


On-Premises
SaaS Applications
Multi-Cloud
Azure Active Directory
Region East US
Microsoft Purview A
Microsoft Purview B
Region UK South
Production
Azure Cosmos DB
SQL Server
Azure SQL
Region UK South
1
Azure SQL
Azure Synapse Analytics
Azure Cosmos DB
Region East US
1
Other Sources
ADL, Storage Acount, SQL Management, Data Factory


Application
Resource Provider
Encryption
& Key Mgmt


az900ondemand
Storage account
Search (Ctrl+/)
Events
Storage browser (preview)
Data storage
Containers
File shares
Queues
Tables
Security + networking
Networking
Azure CDN
Access keys
Shared access signature
Encryption
Security


Client
Server
Connection
Request
0MS
34MS
Connection
Acknowledged
TCP - 68MS
ClientHello
68MS
ServerHello
Certificate
ServerHelloDone
102MS
ClientKeyExchange
ChangeCipherSpec
Finished
136MS
170MS
ChangeCipherSpec
Finished
TLS - 136MS
Application
Data
204MS
238MS
Application
Data
272MS
Time
Time


Storage account
| Encryption
Search
Security + networking
Networking
Azure CDN
Access keys
Shared access signature
Encryption
Microsoft Defender for Cloud
Data management
Redundancy
Data protection
Encryption
Encryption scopes
Storage service encryption protects your data at rest. Azure Storage encrypts your data as it's written in our datacenters, and automatically decrypts it for you as you access it.
Please note that after enabling Storage Service Encryption, only new data will be encrypted, and any existing files in this storage account will retroactively get encrypted by a background encryption process. Learn more about Azure Storage encryption
Encryption selection
Enable support for customer-managed keys
Blobs and files only
Infrastructure encryption
Disabled
Encryption type
Microsoft-managed keys
Customer-managed keys

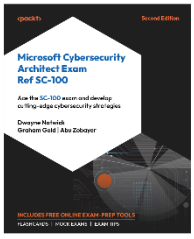
Chapter 11: Accessing the Online Practice Resources

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

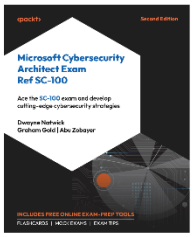
PROCEED

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 *

E.g 123456789 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.

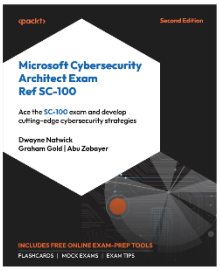
REQUEST ACCESS

Practice Resources

REPORT ISSUE

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

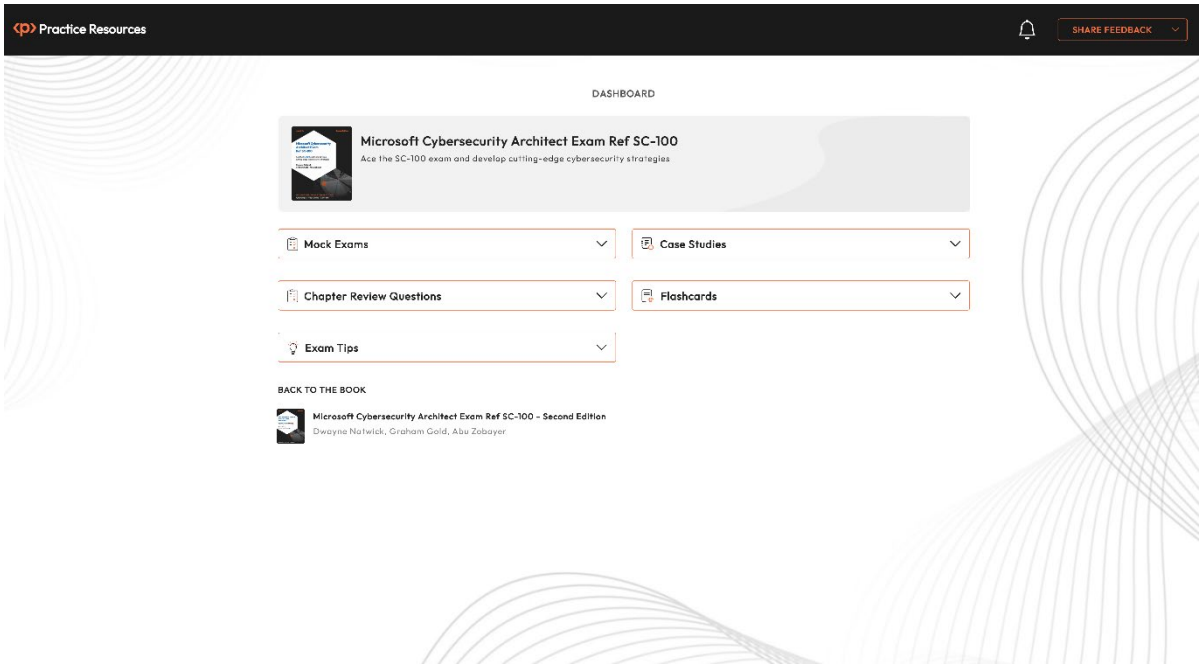
Dwayne Natwick • Graham Gold • Abu Zobayer • Oct 2024 • 500 pages

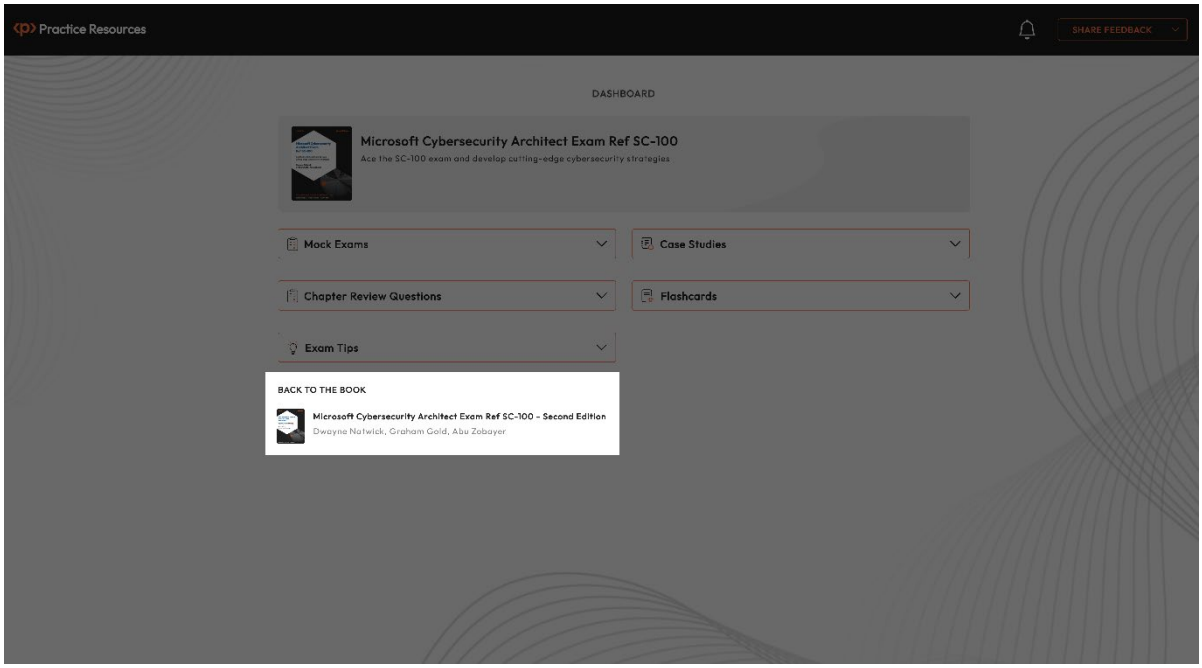
Unlock Successful

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




Practice Resources
SHARE FEEDBACK
DASHBOARD
Microsoft Cybersecurity Architect Exam Ref SC-100
Ace the SC-100 exam and develop cutting-edge cybersecurity strategies
Mock Exams
Case Studies
Chapter Review Questions
Flashcards
Exam Tips
BACK TO THE BOOK
Microsoft Cybersecurity Architect Exam Ref SC-100 - Second Edition
Dwayne Natwick, Graham Gold, Abu Zobayer