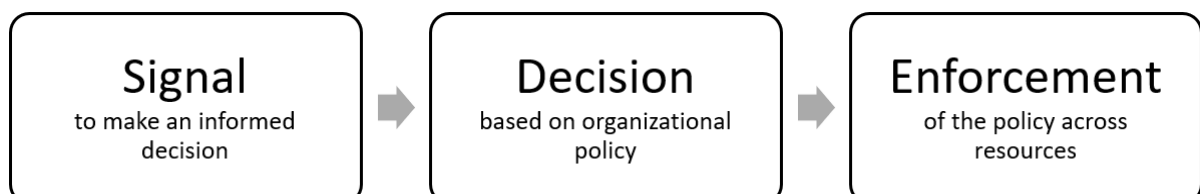
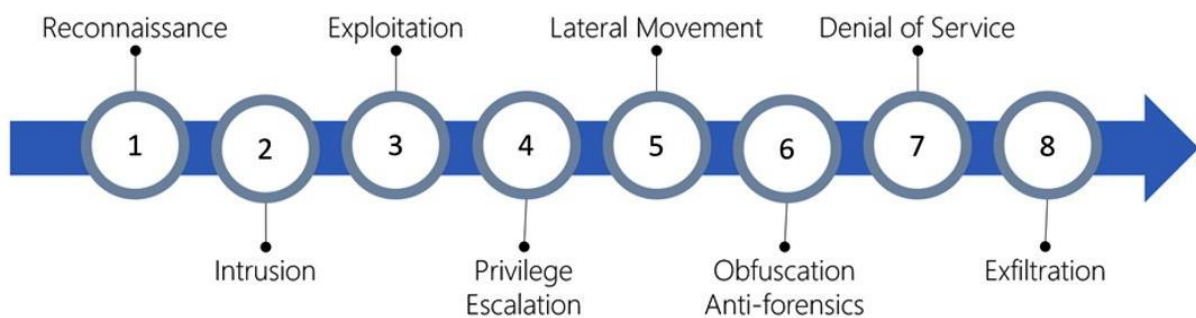
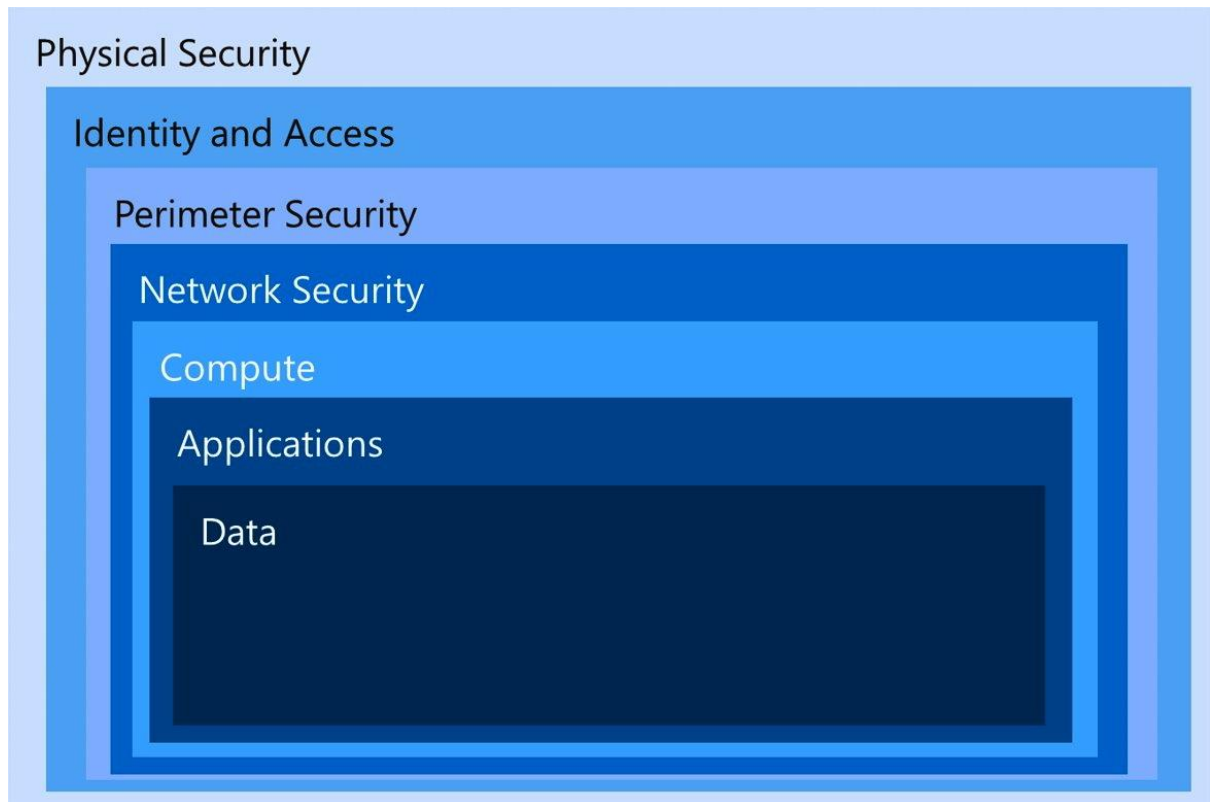
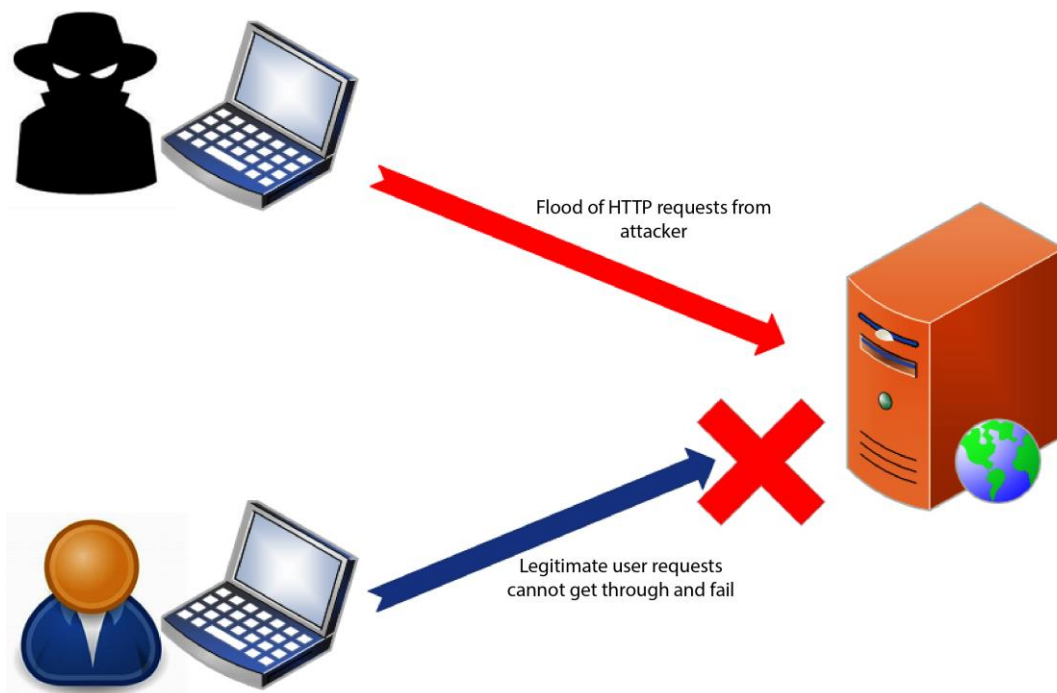
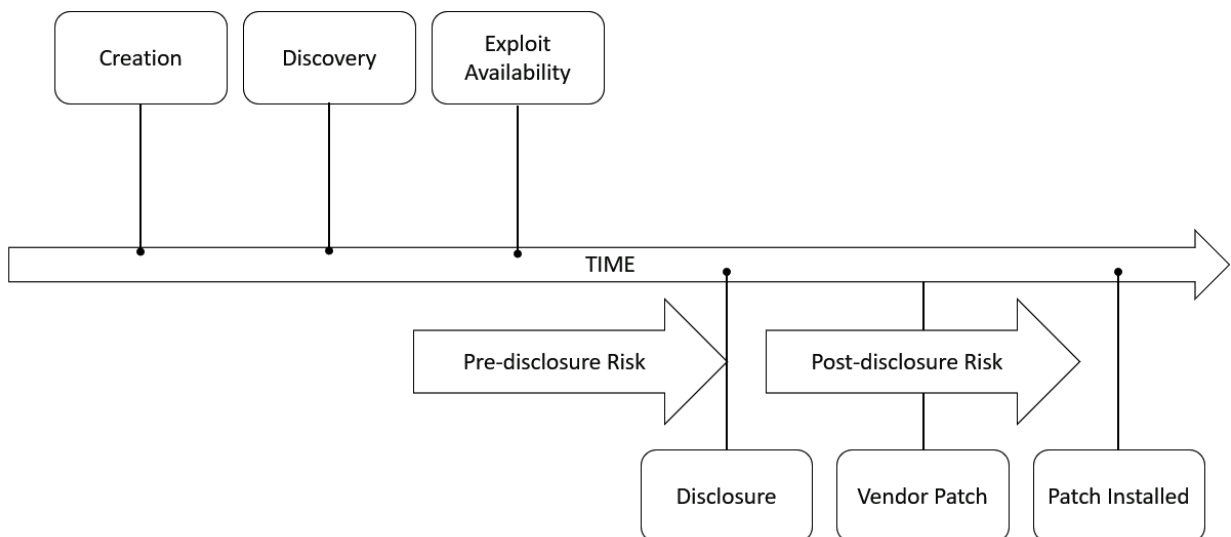
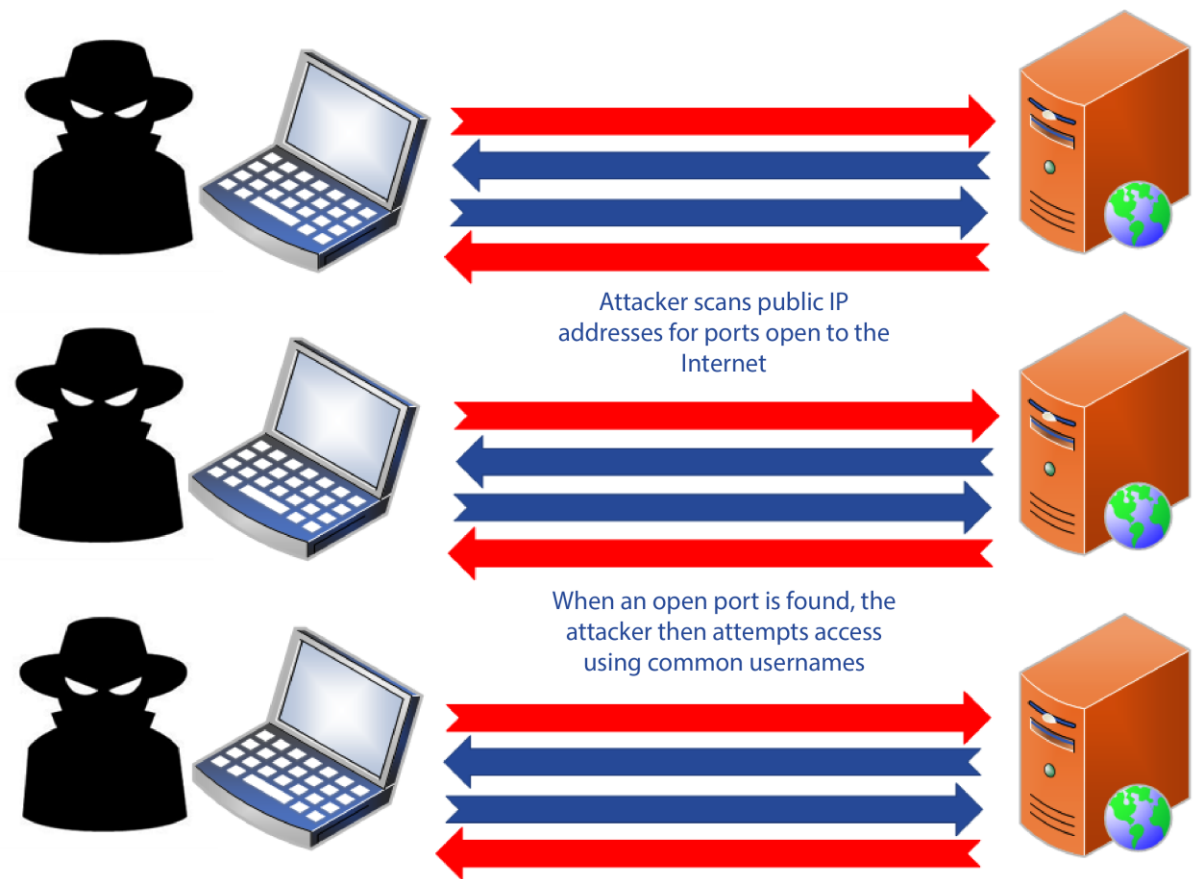
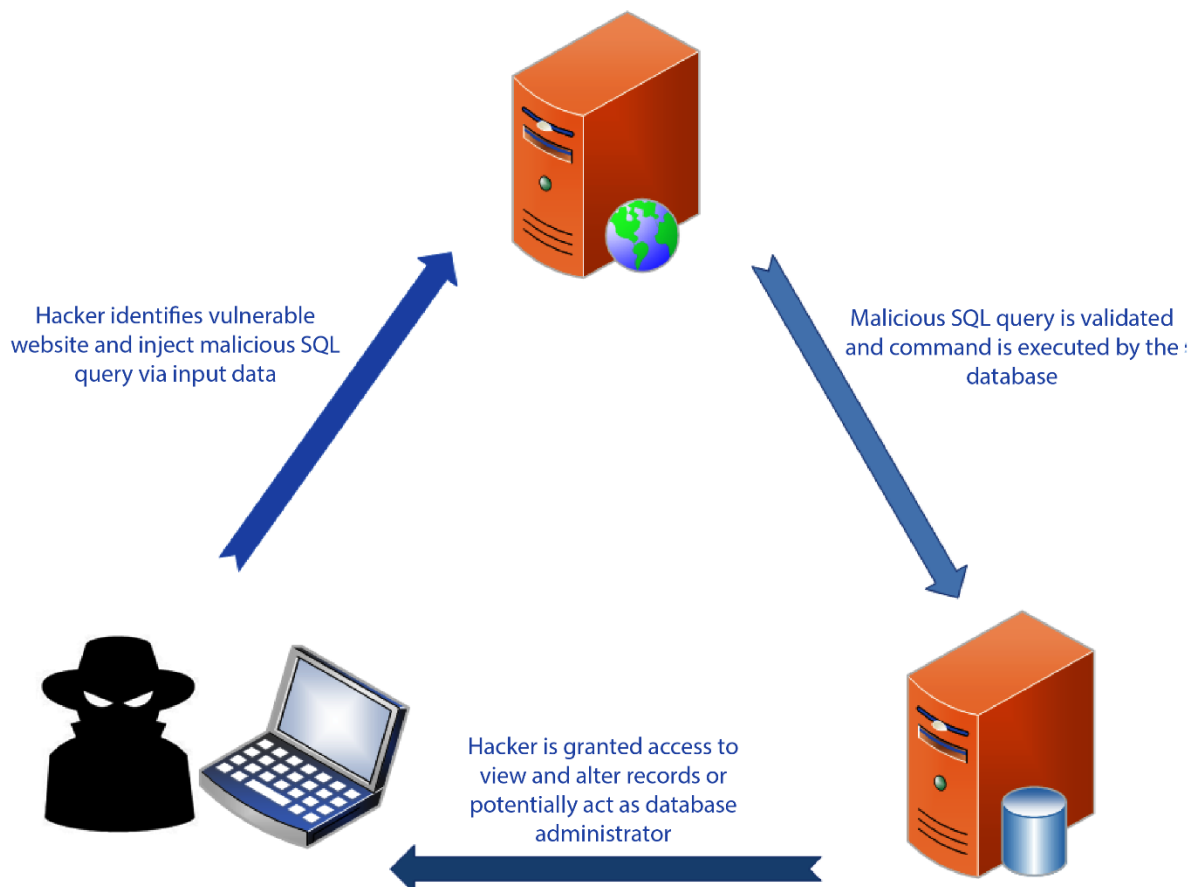
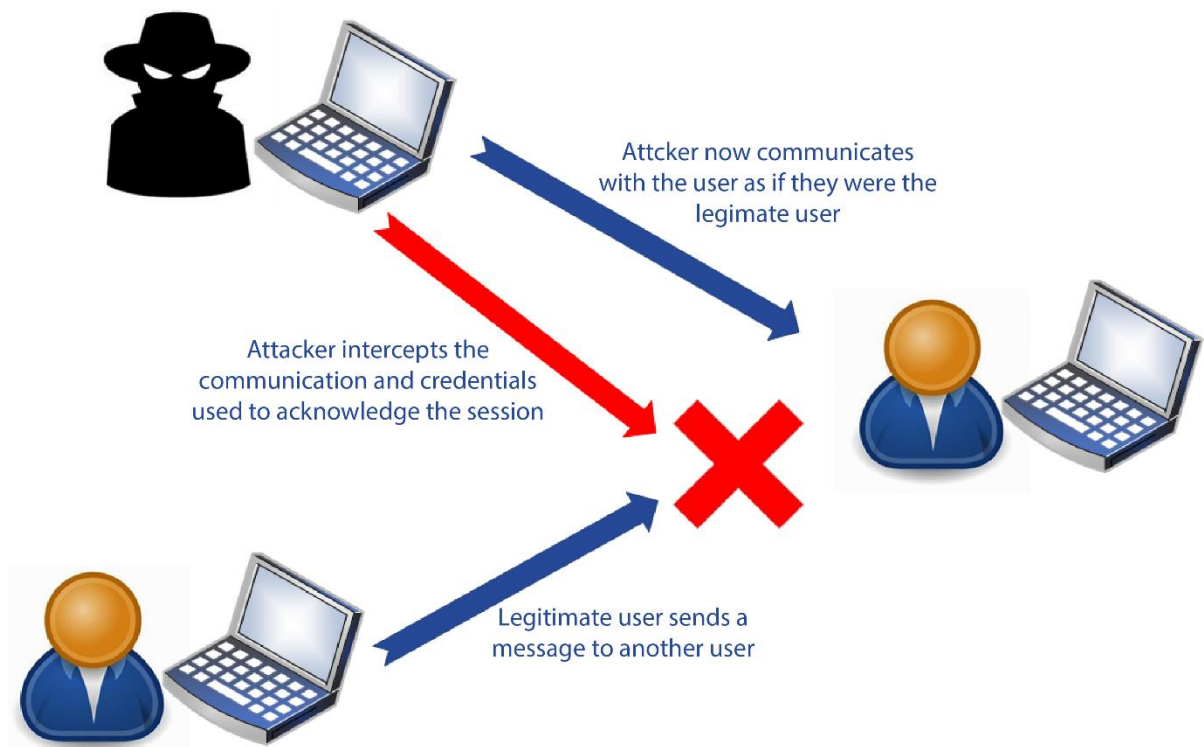


## Chapter 1: Cybersecurity in the Cloud

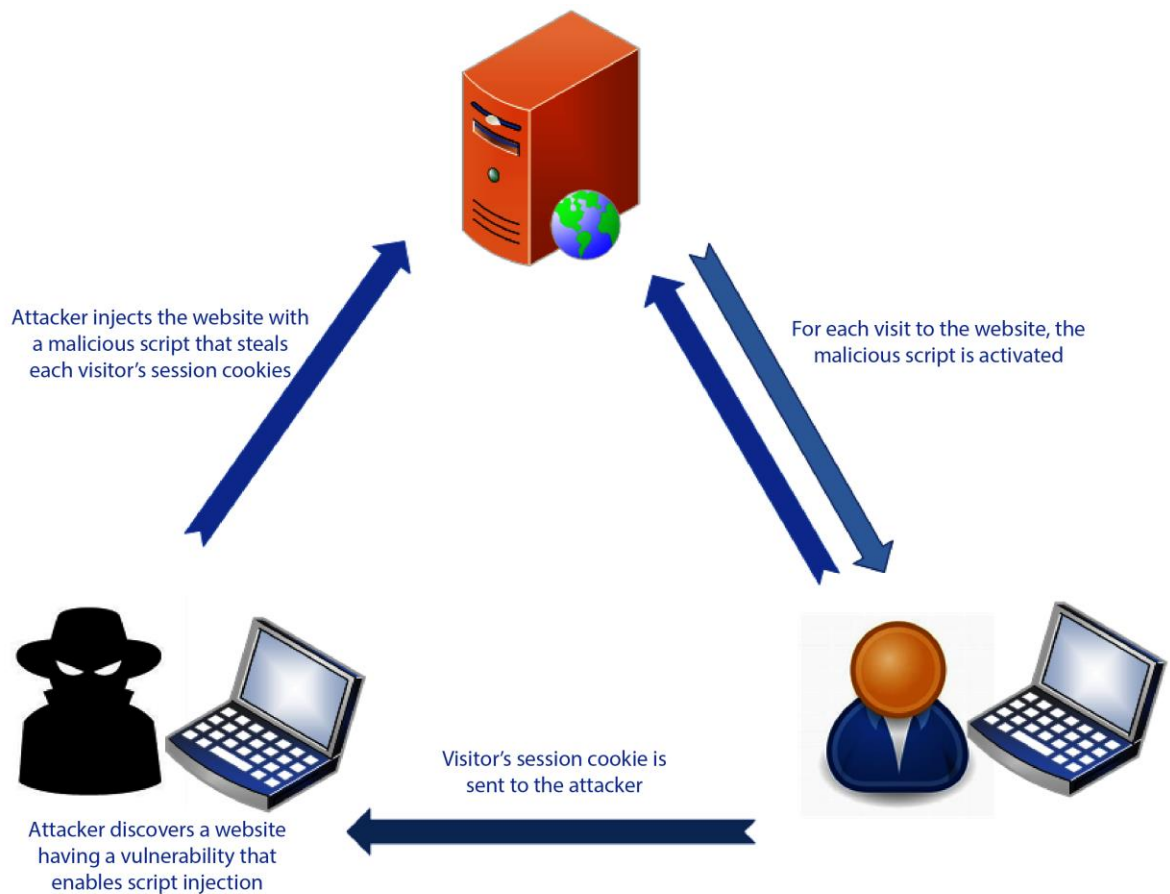












|   |   |                             |                             |                                |
|---|---|-----------------------------|-----------------------------|--------------------------------|
| Likelihood<br>↑                         | Very Likely                             | Acceptable risk<br>Medium 2 | Unacceptable risk<br>High 3 | Unacceptable risk<br>Extreme 5 |
|   | Likely                                  | Acceptable risk<br>Low 1    | Acceptable risk<br>Medium 2 | Unacceptable risk<br>High 3    |
|   | Unlikely                                | Acceptable risk<br>Low 1    | Acceptable risk<br>Low 1    | Acceptable risk<br>Medium 2    |
|   | What is the chance that it will happen? | Minor                       | Moderate                    | Major                          |
| Impact<br>→<br>How serious is the risk? |   |                             |                             |                                |

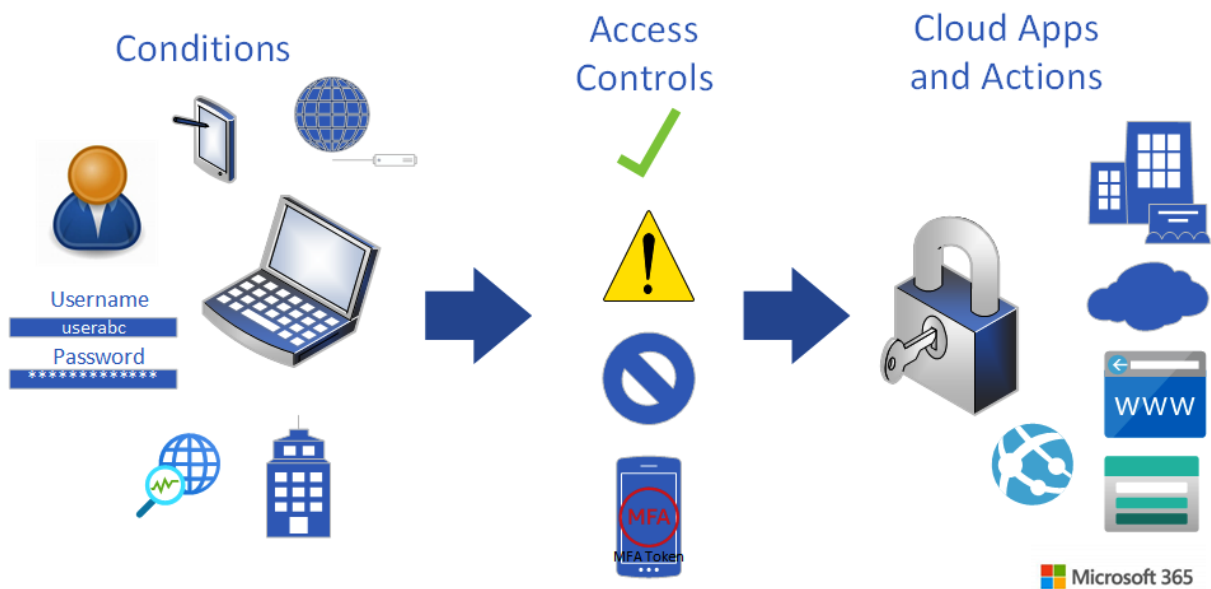
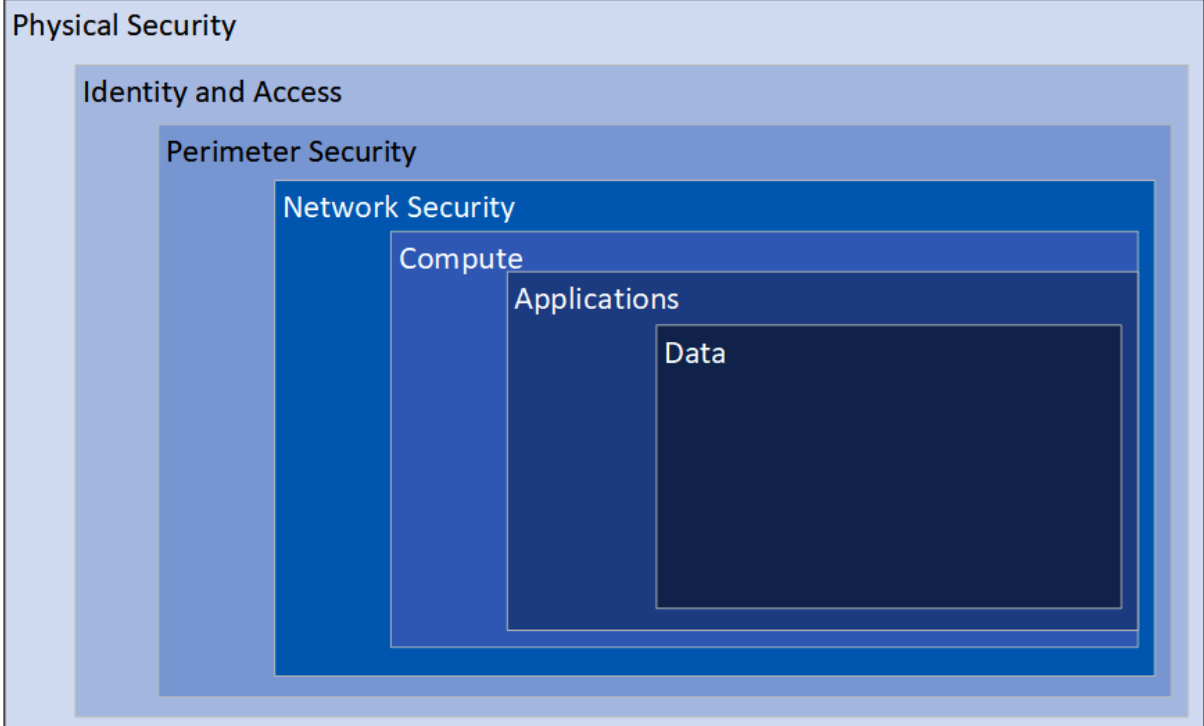
## Chapter 2: Building an Overall Security Strategy and Architecture

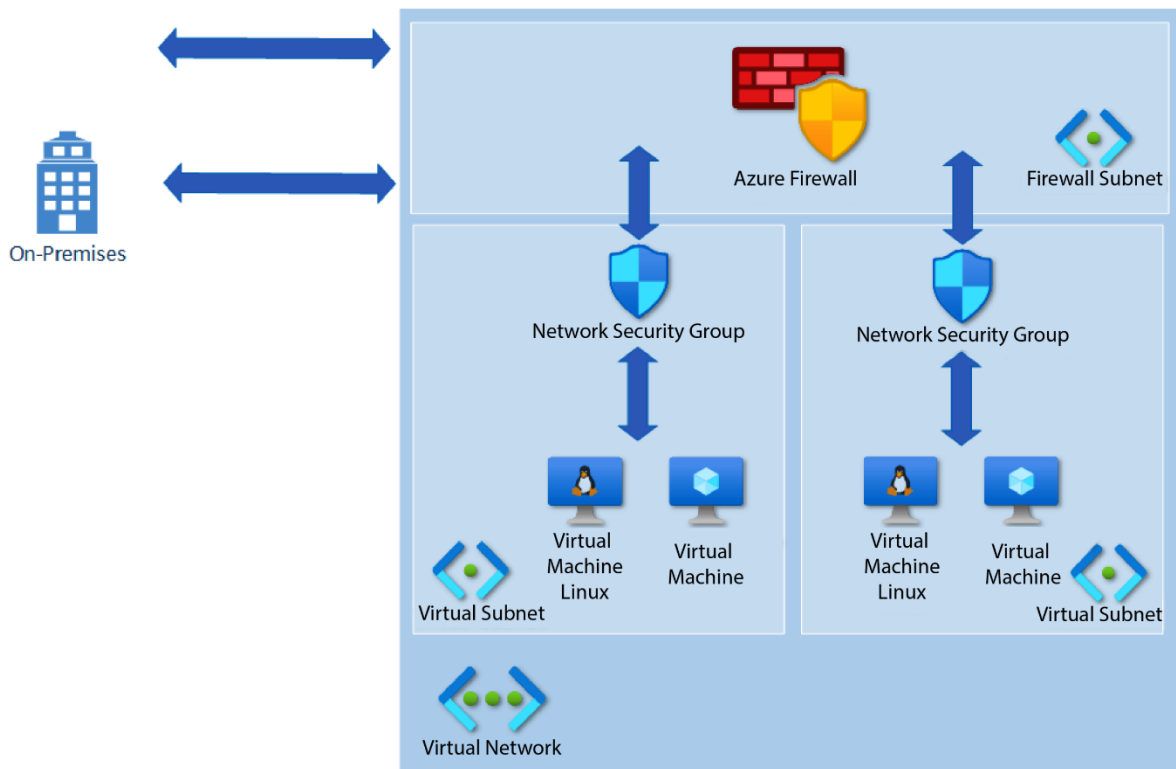
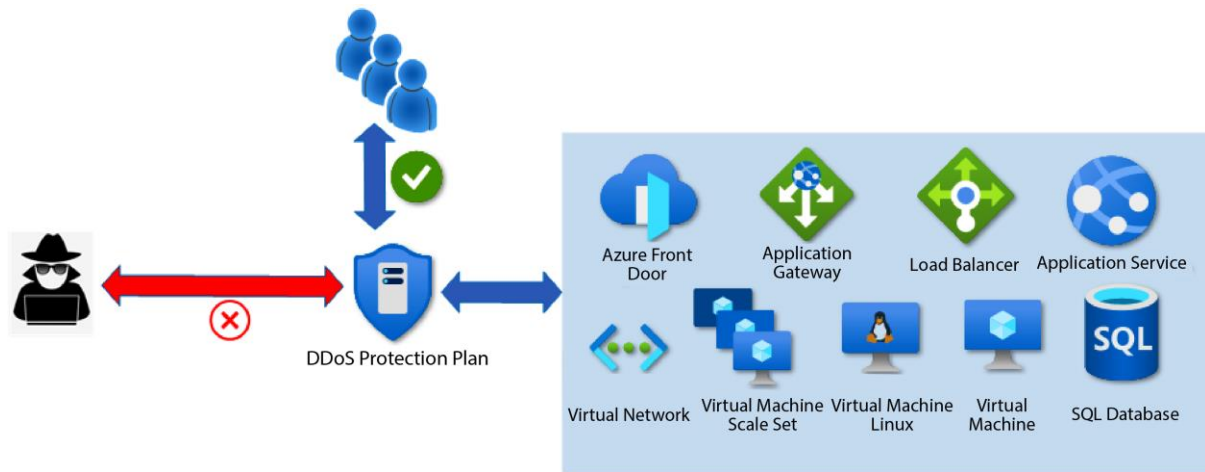
### Microsoft Cybersecurity Reference Architecture (MCRA)

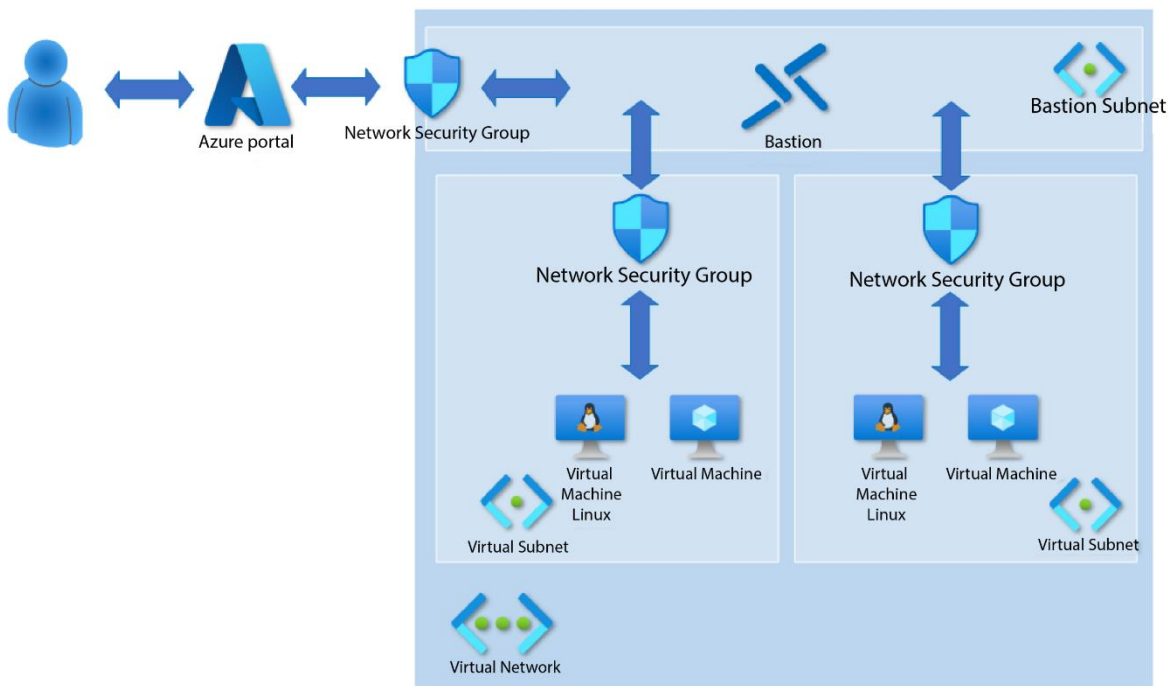
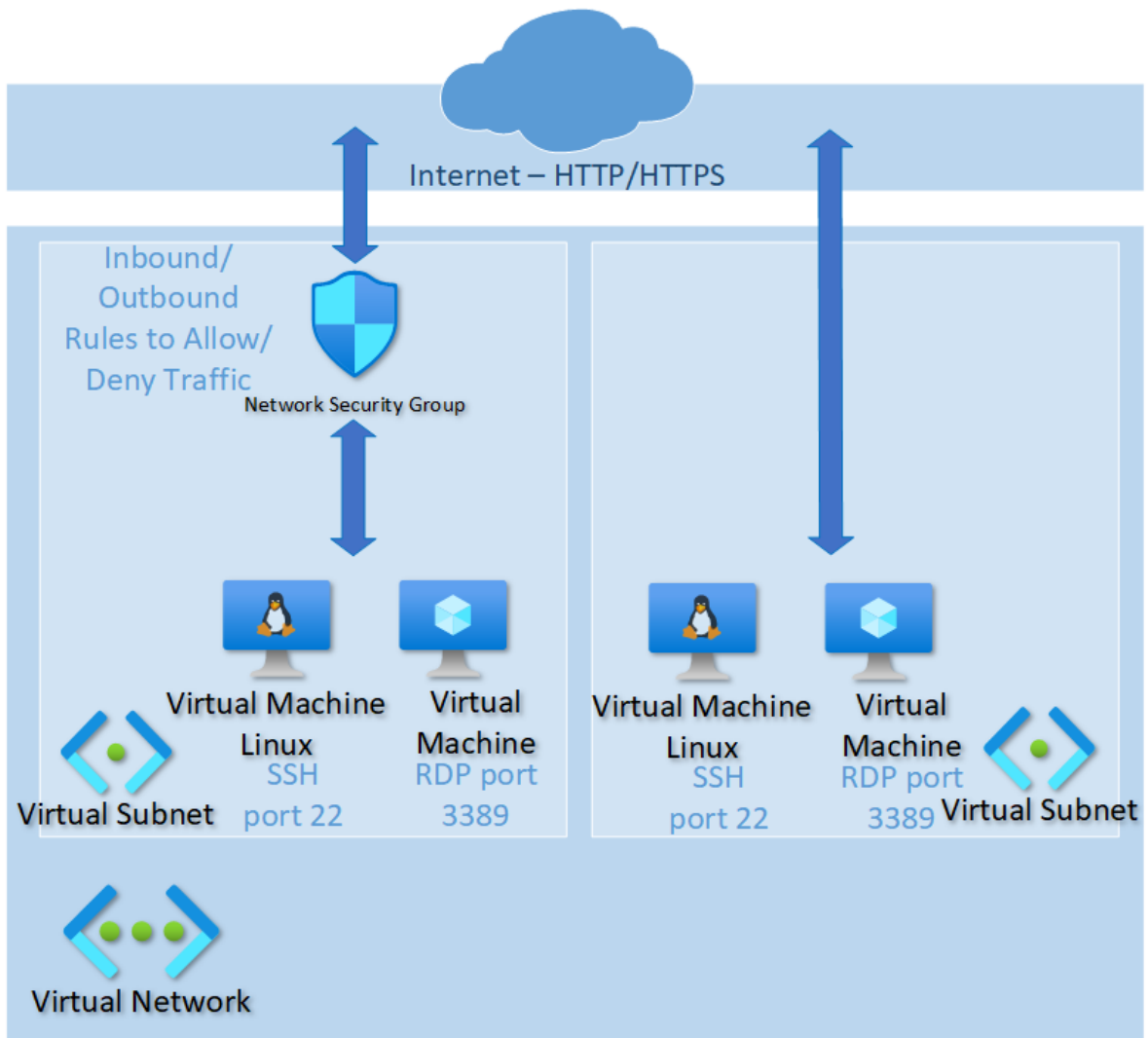
|                                   |                       |                                |
|-----------------------------------|-----------------------|--------------------------------|
| Capabilities                      | Azure Native Controls | People                         |
| Zero Trust User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

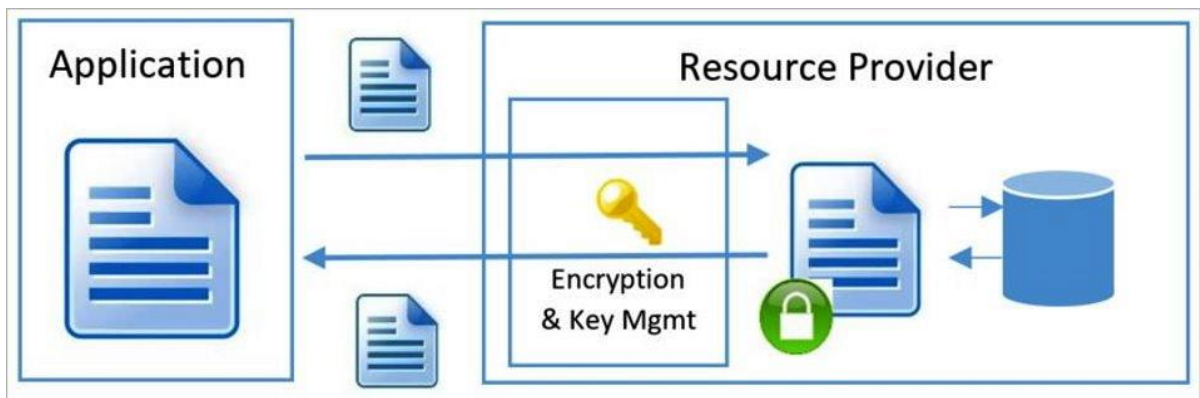
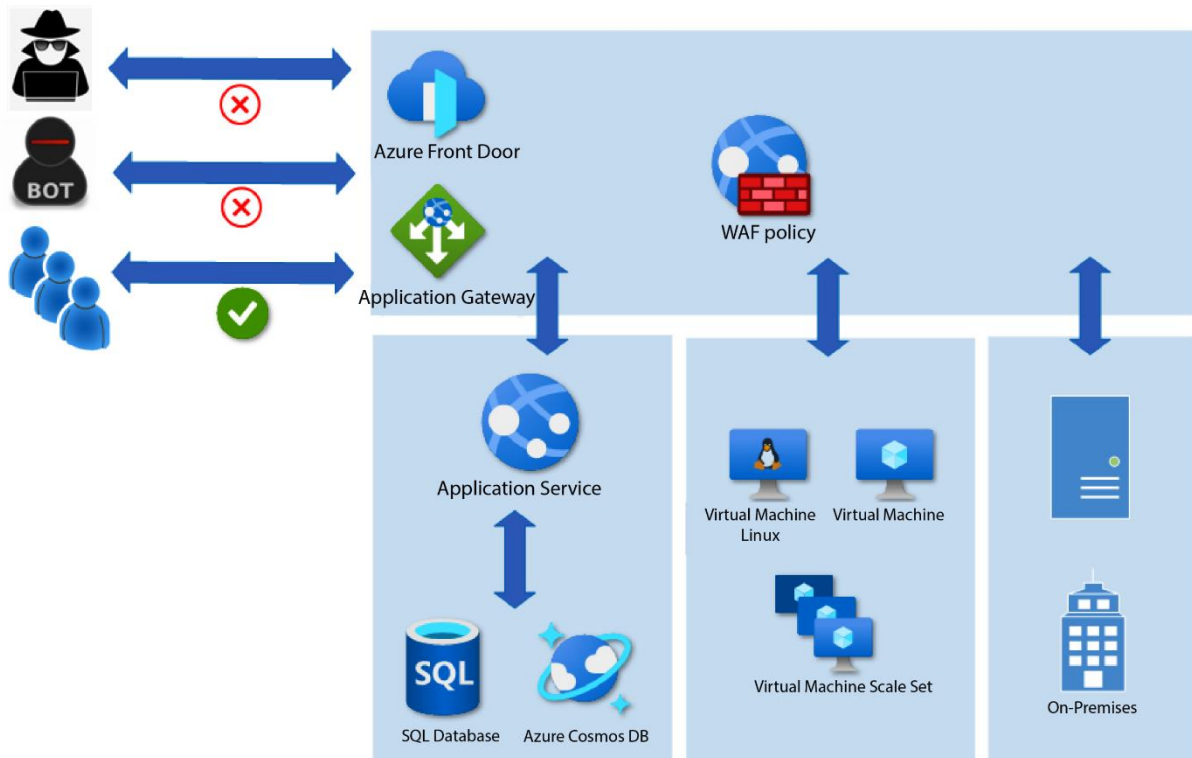
The diagram illustrates a risk assessment matrix. A vertical blue arrow on the left points upwards and is labeled 'Likelihood'. A horizontal blue arrow at the bottom points to the right and is labeled 'Impact' and 'How serious is the risk?'. The matrix itself is a 4x4 grid. The first column contains likelihood levels: 'Very Likely', 'Likely', 'Unlikely', and 'What is the chance that it will happen?'. The first row contains impact levels: 'Acceptable risk Medium 2', 'Unacceptable risk High 3', and 'Unacceptable risk Extreme 5'. The remaining cells contain risk levels categorized as 'Acceptable risk' (Low 1, Medium 2, or High 3) or 'Unacceptable risk' (High 3 or Extreme 5). The colors of the cells indicate the risk level: green for acceptable low risk, yellow for acceptable medium/high risk, orange for unacceptable high risk, and red for unacceptable extreme risk.

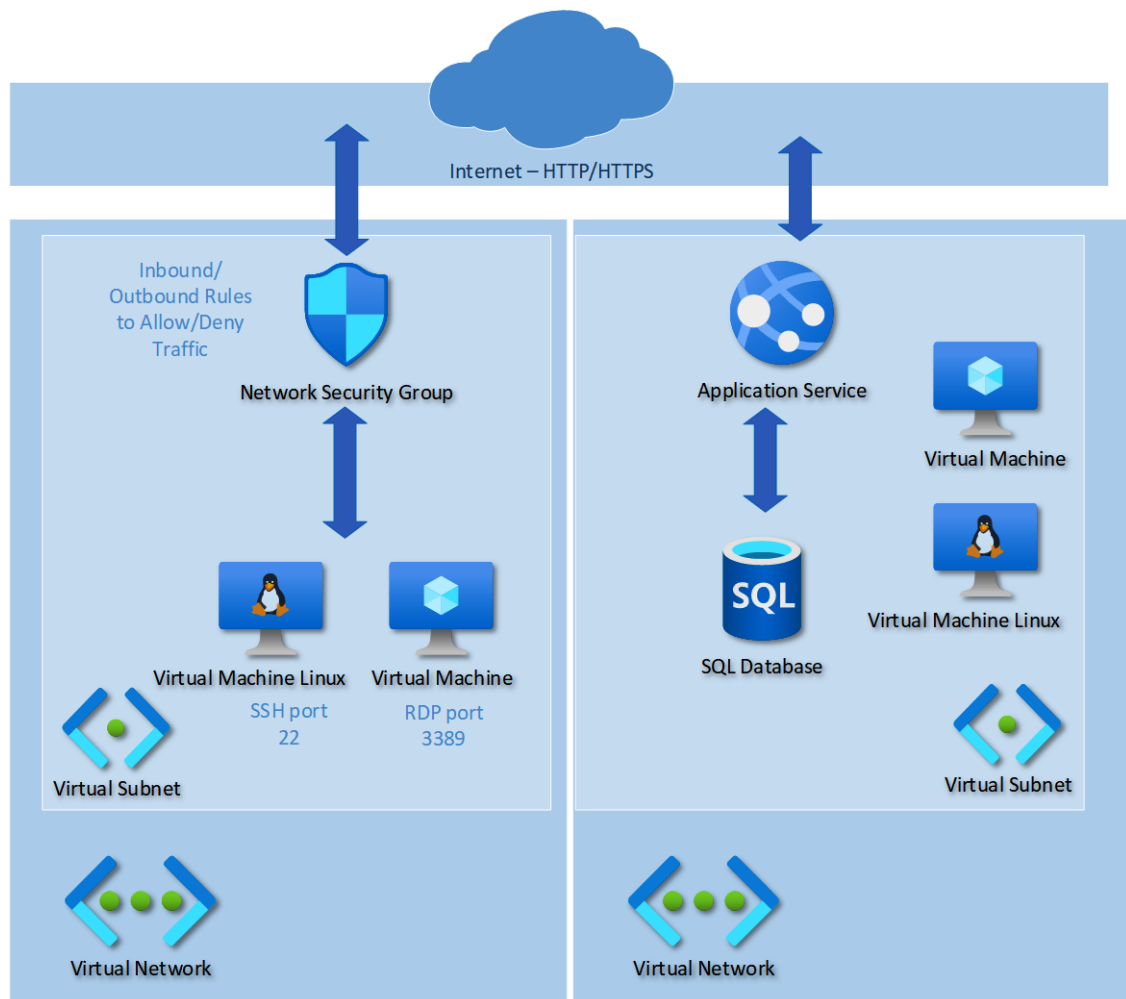
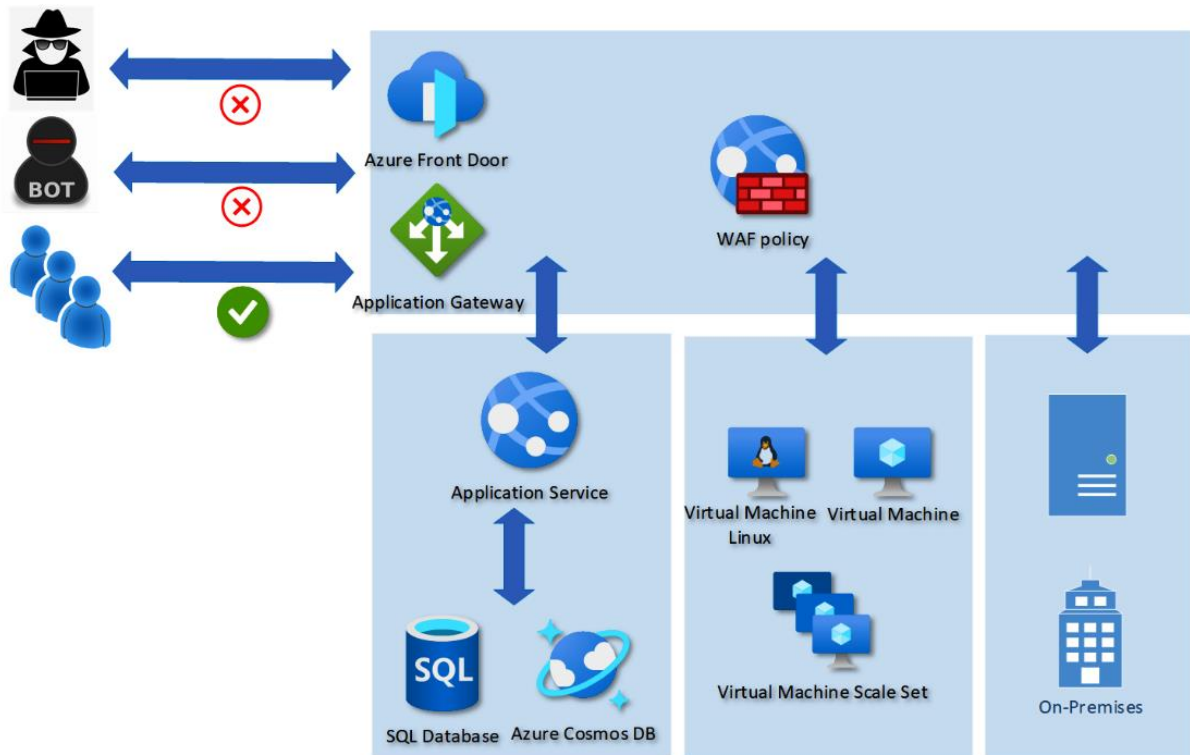
|   |                             |                             |                                |
|---|-----------------------------|-----------------------------|--------------------------------|
| Very Likely                                   | Acceptable risk<br>Medium 2 | Unacceptable risk<br>High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



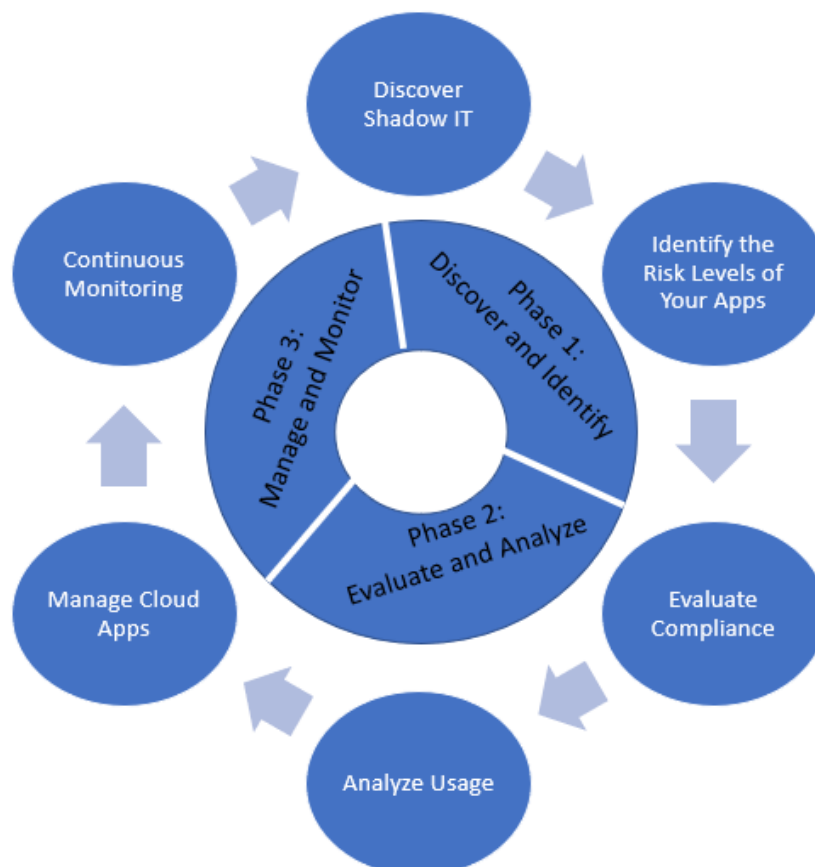




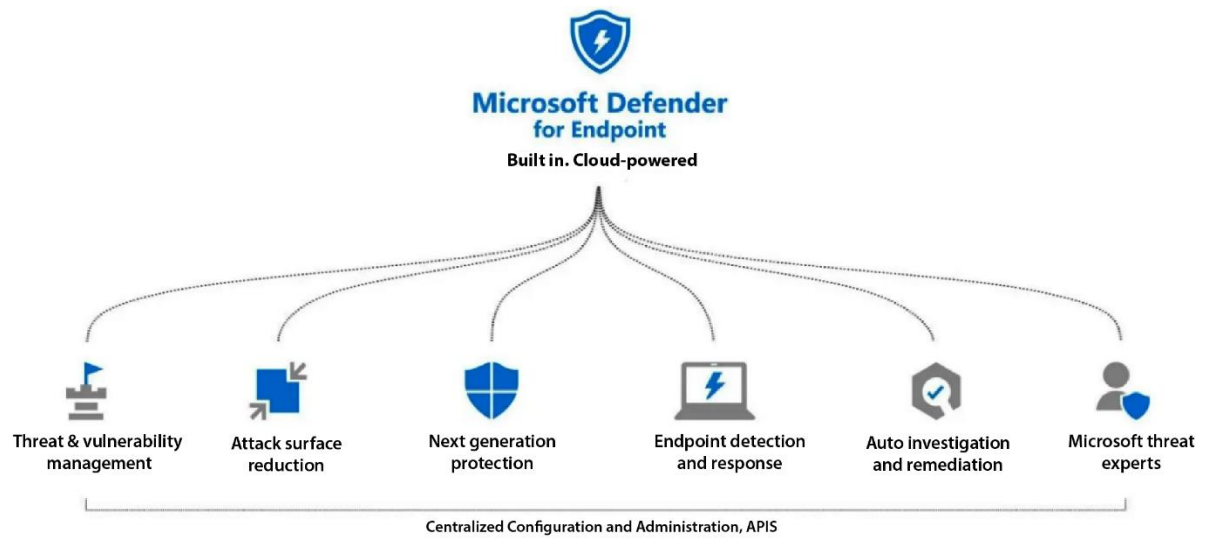
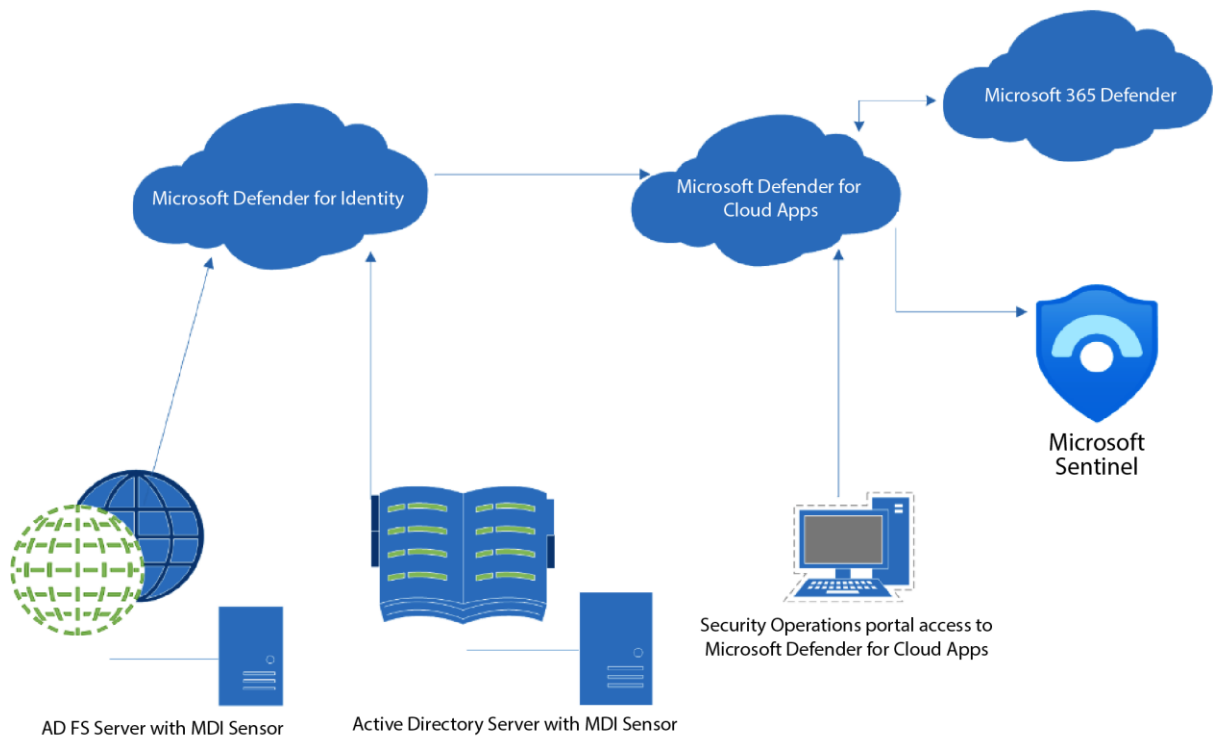


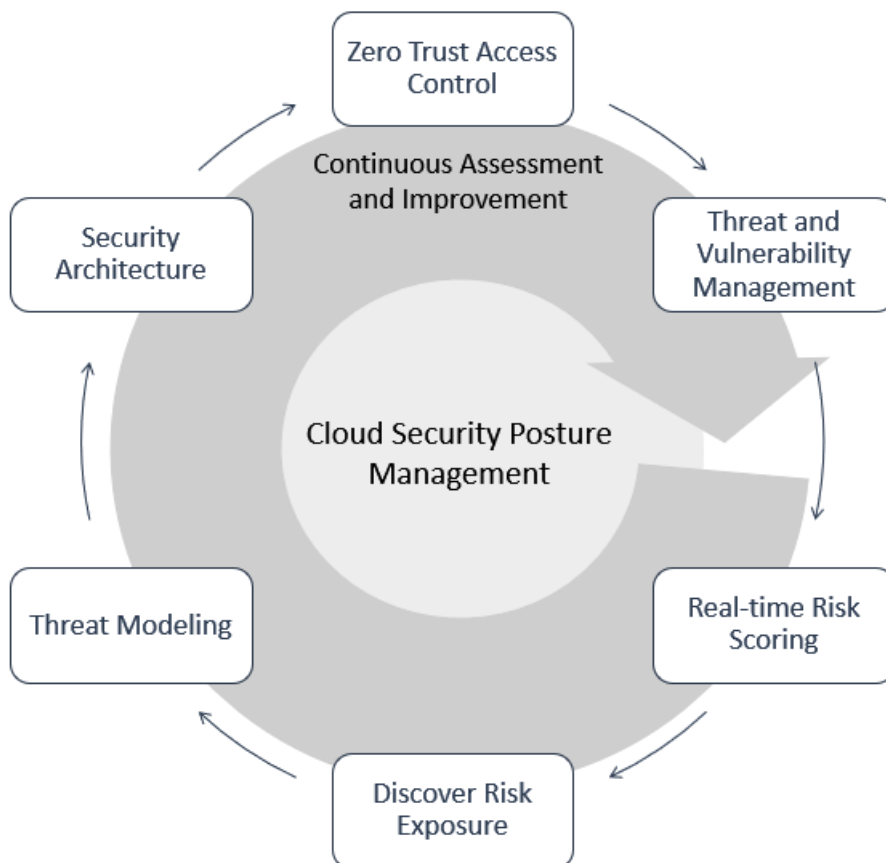


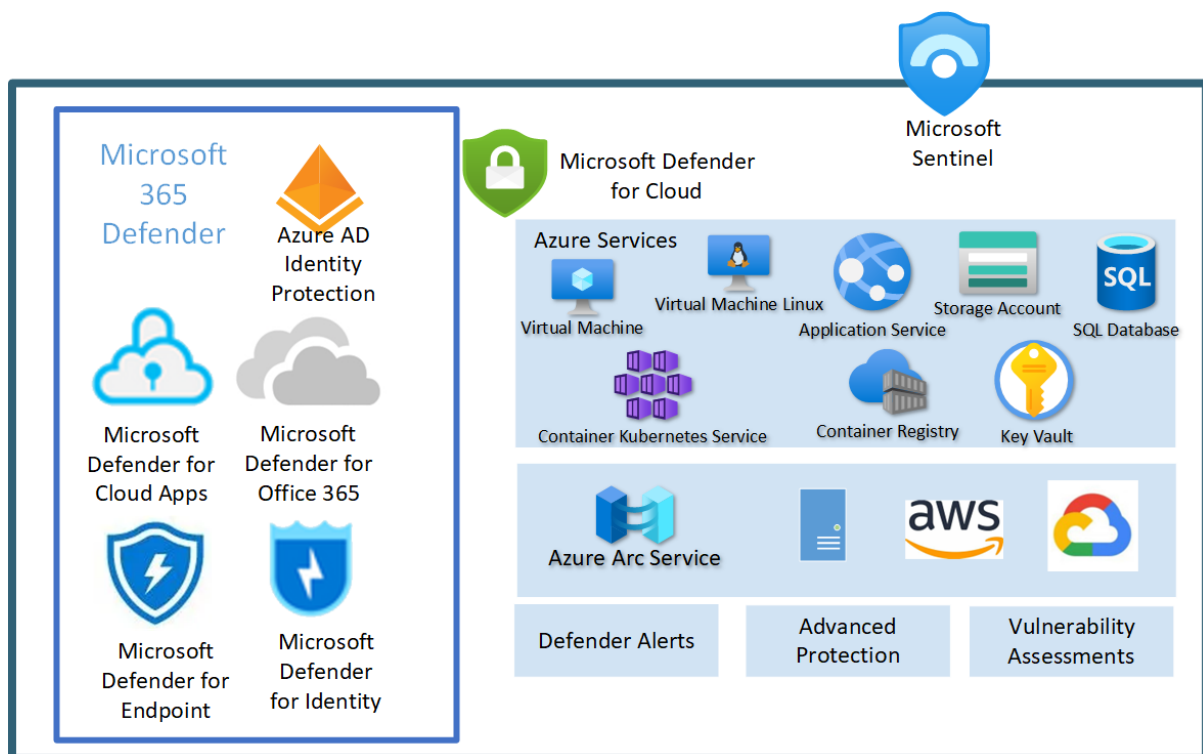
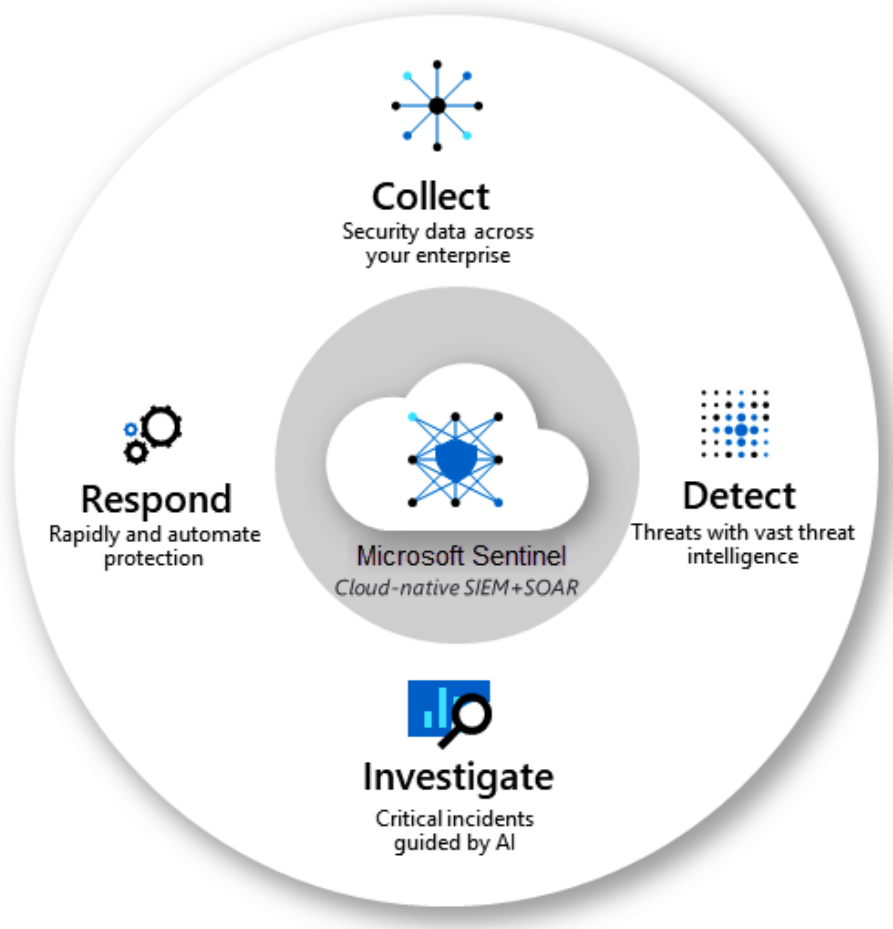
## Chapter 3: Designing a Security Operations Strategy

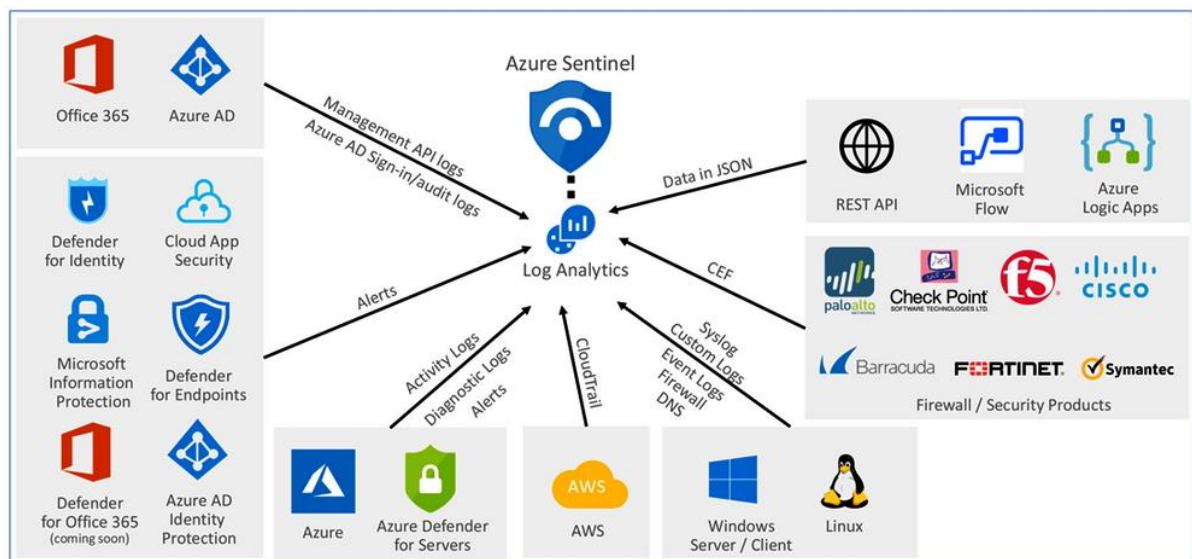
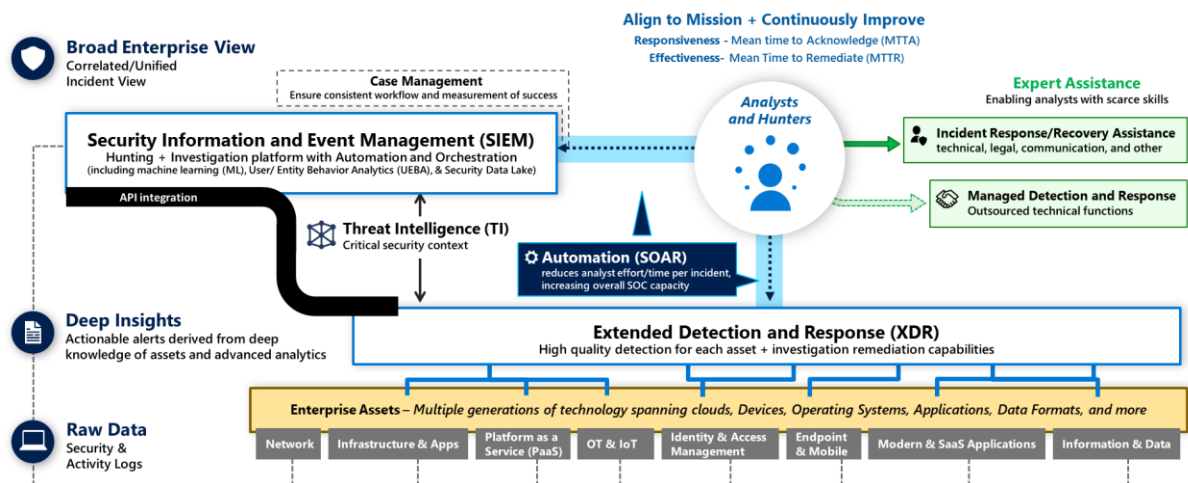
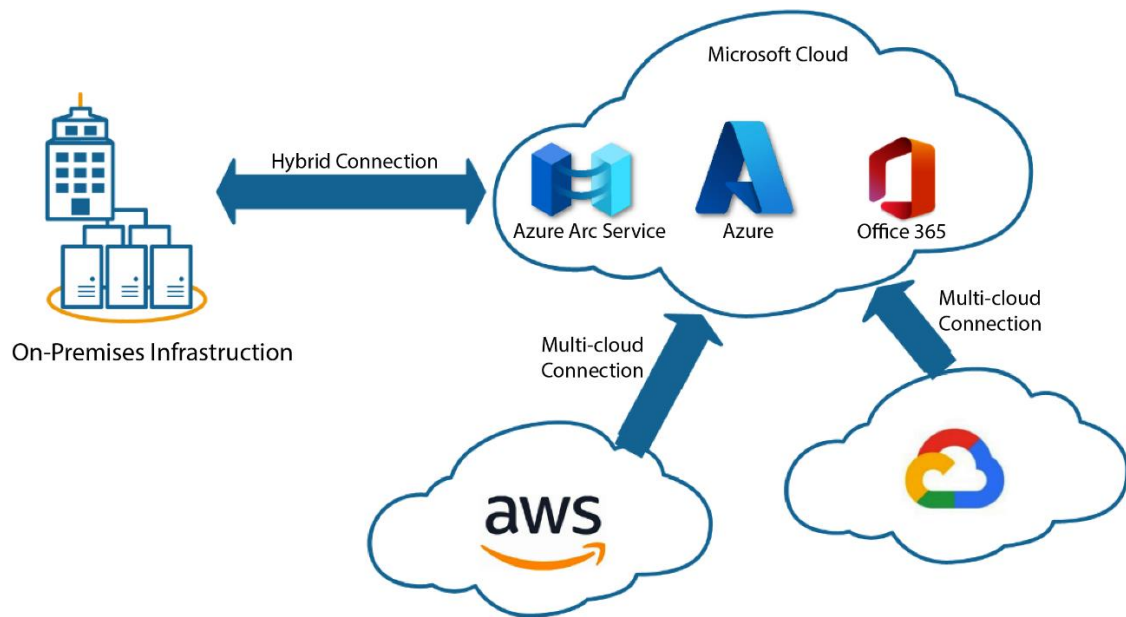


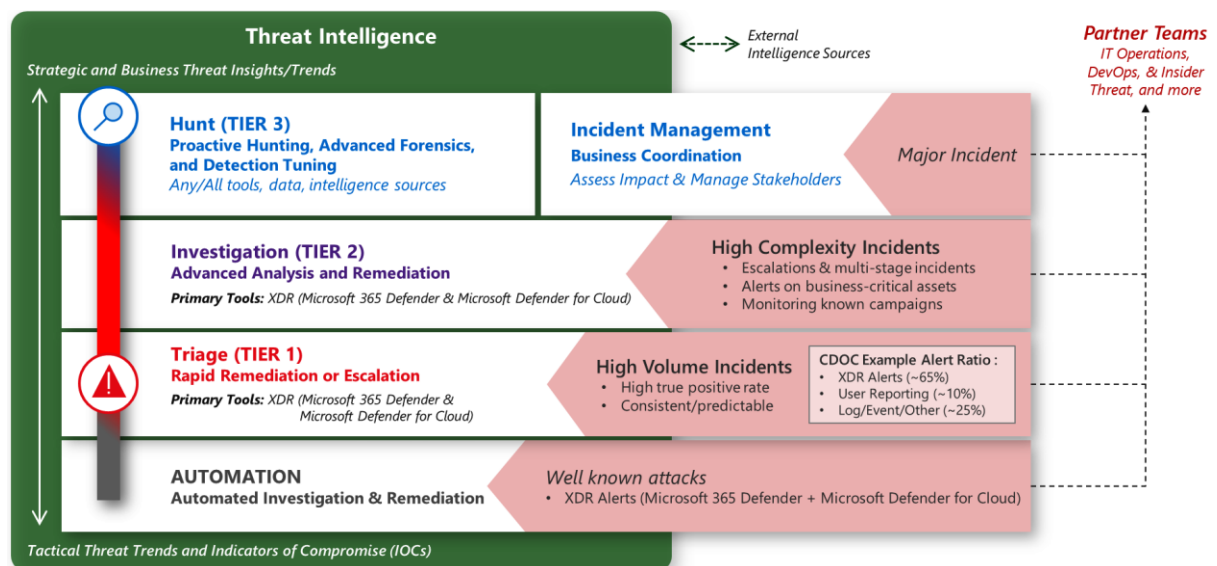
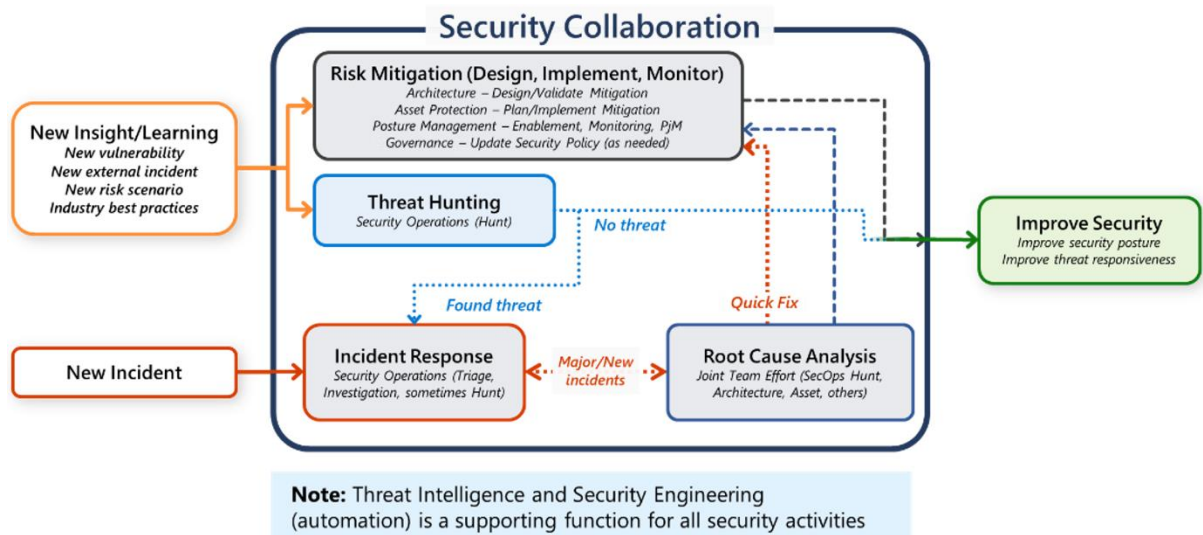




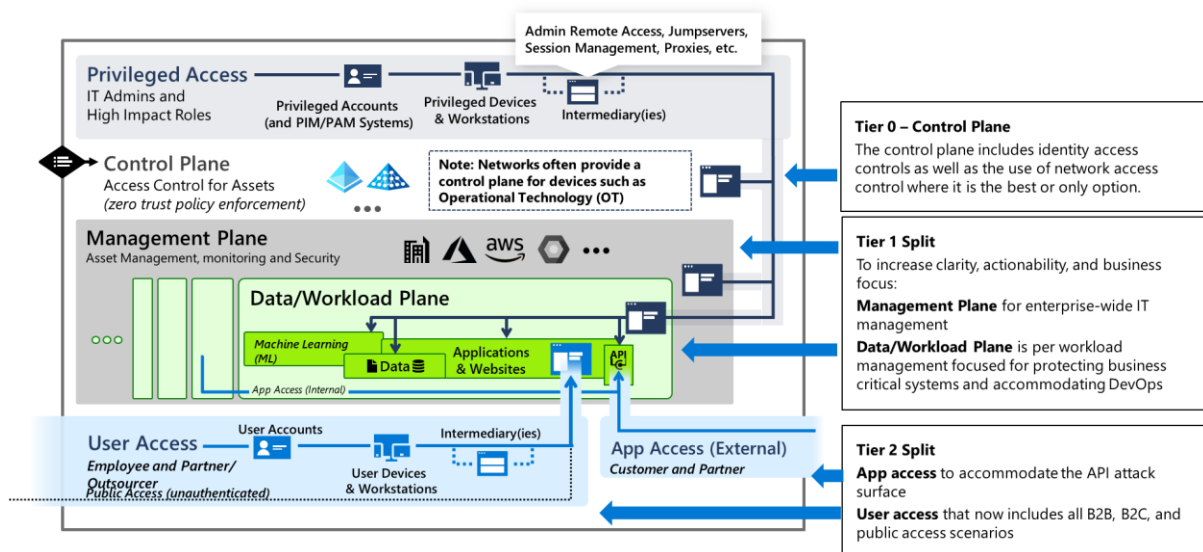
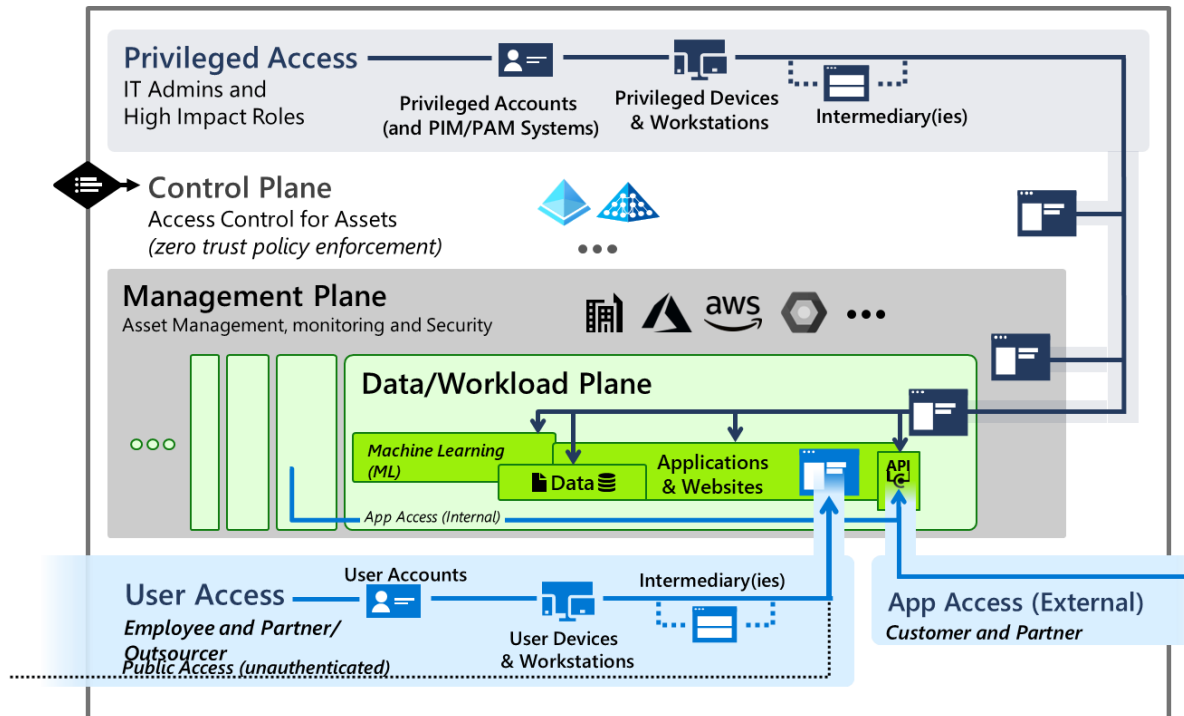


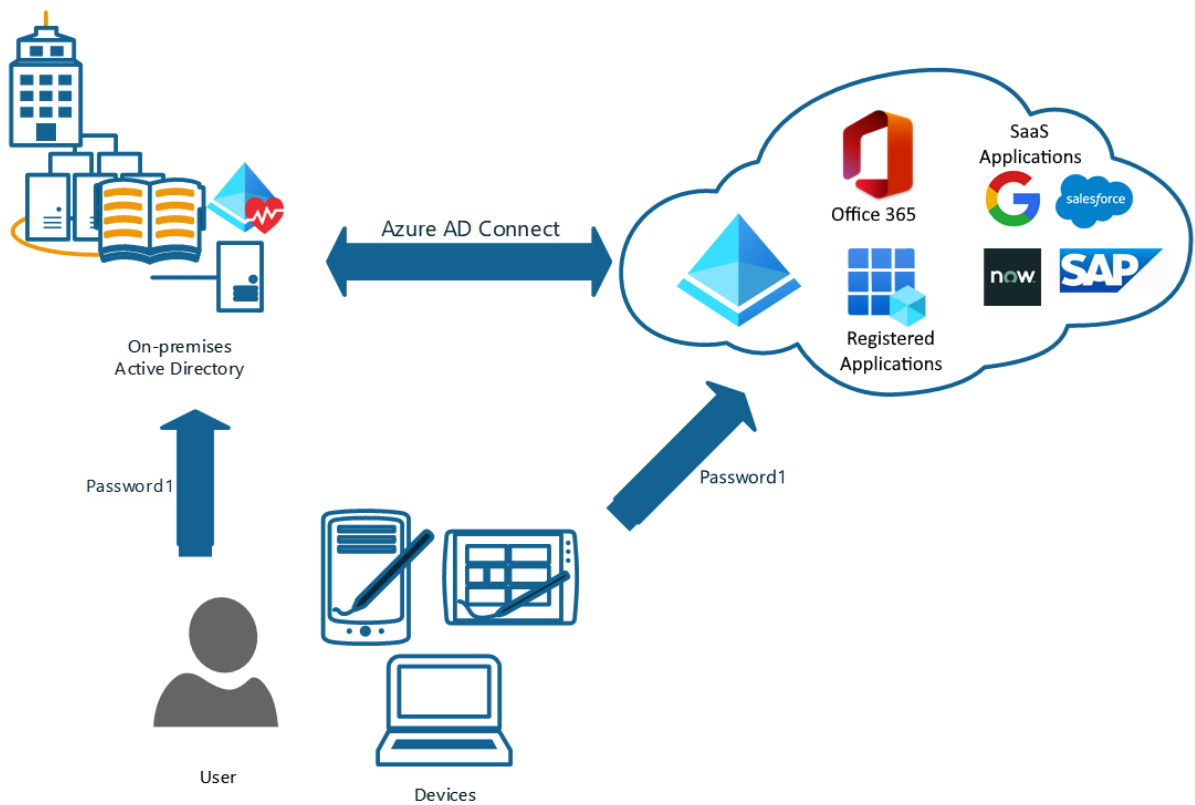
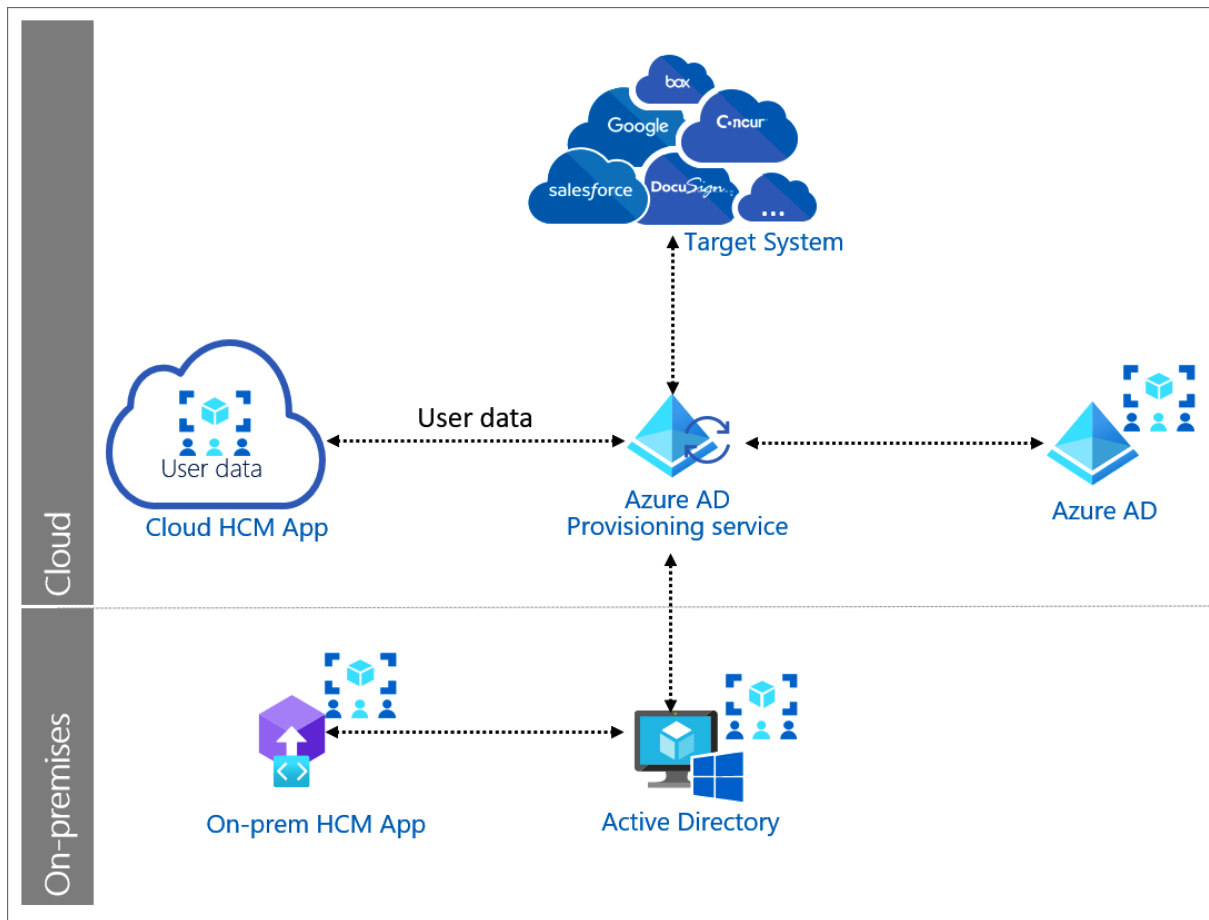


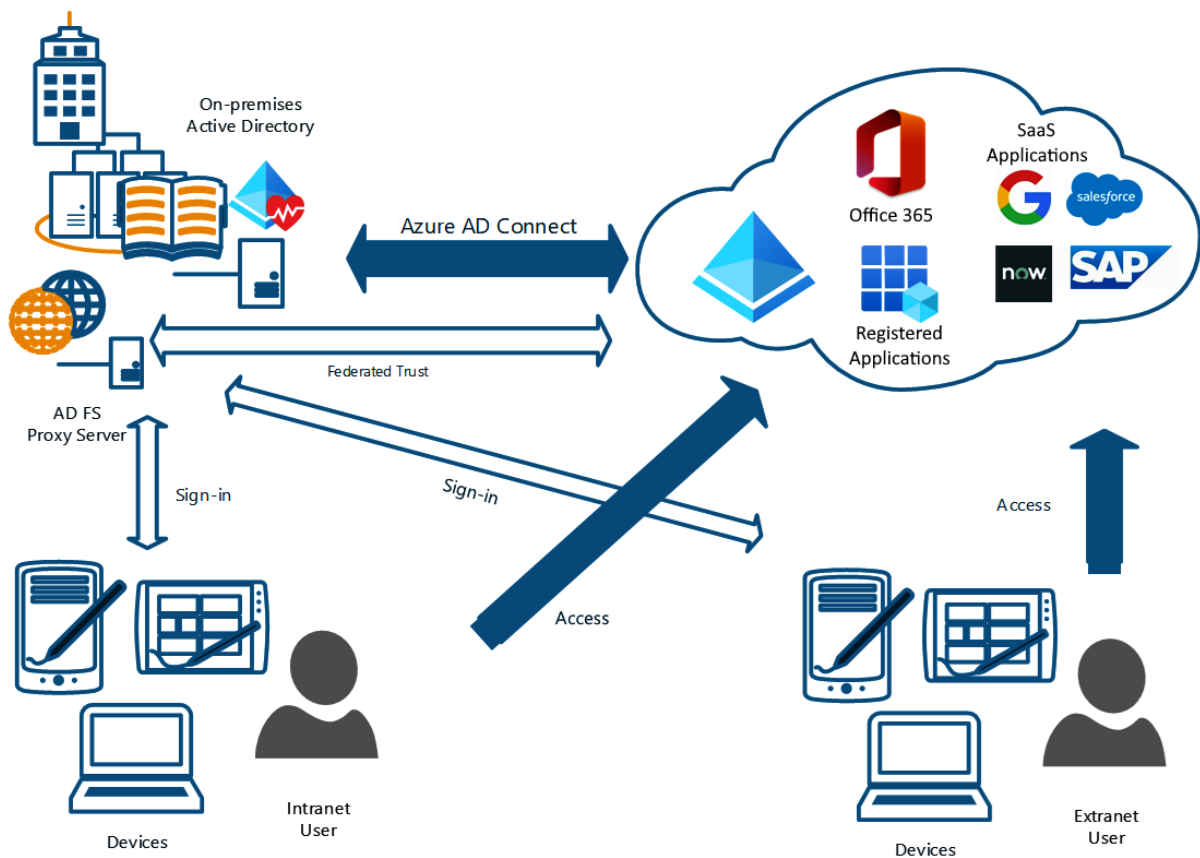
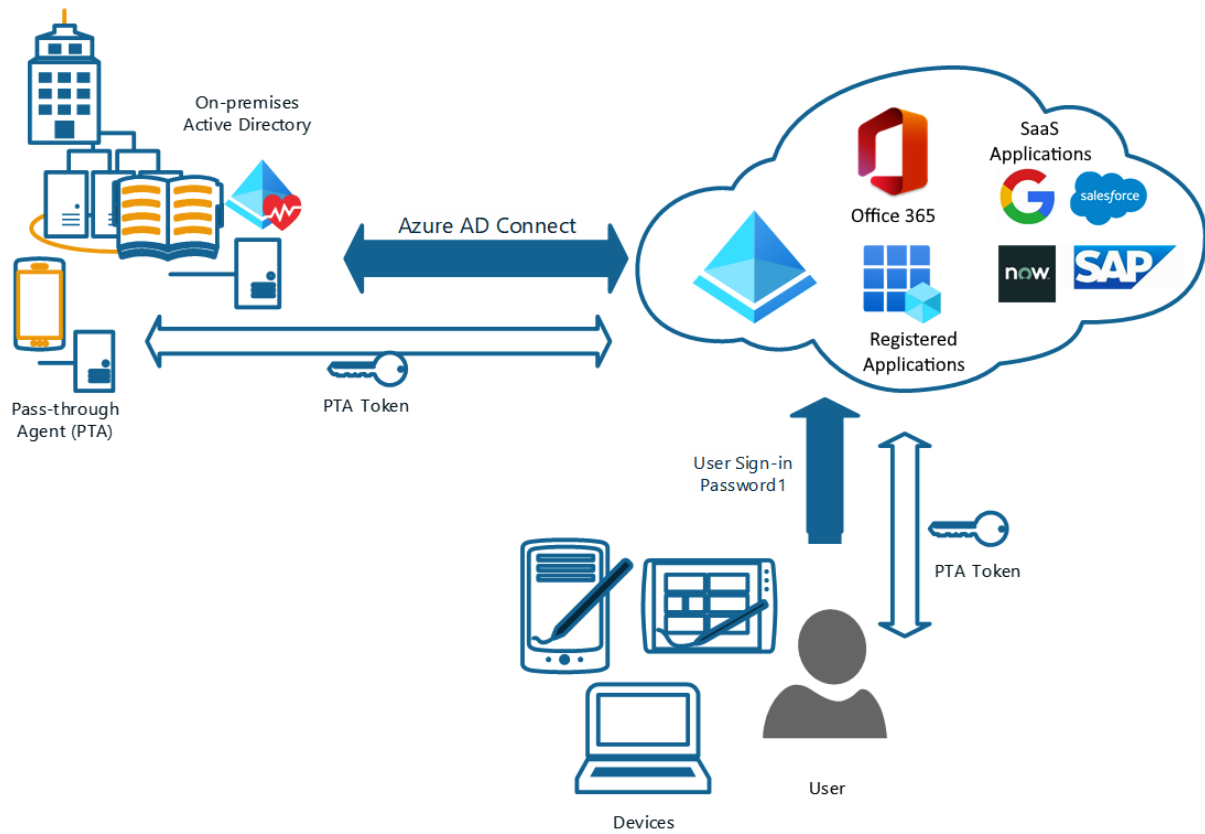




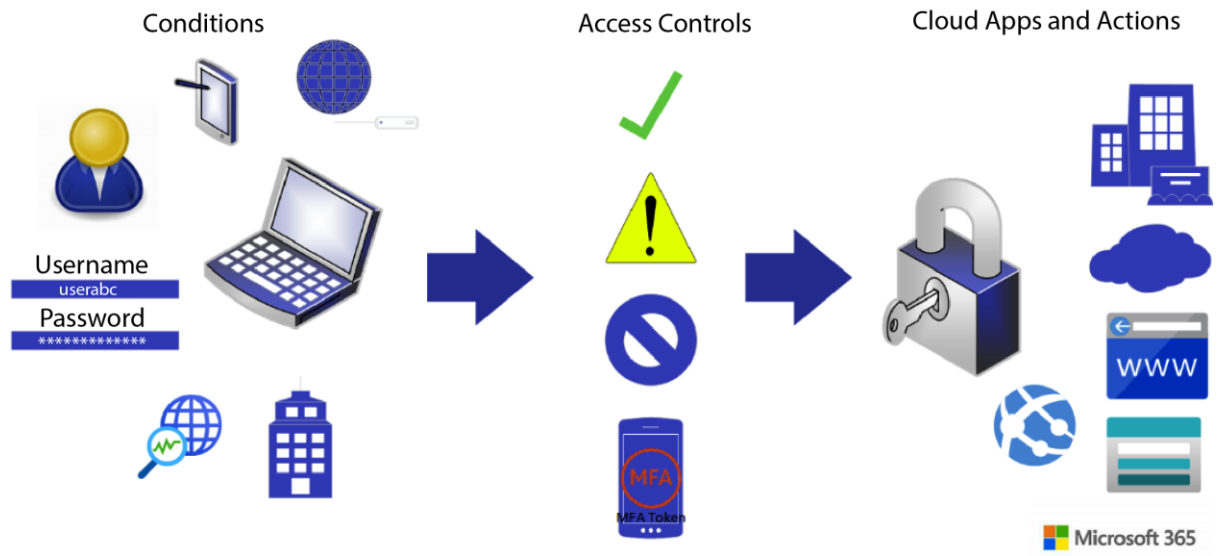
## Chapter 4: Designing an Identity Security Strategy











## Chapter 5: Designing a Regulatory Compliance Strategy

**Settings | Defender plans** Microsoft Azure Sponsorship ×

Search « Save Settings & monitoring

**Settings**

- Defender plans
- Email notifications
- Workflow automation
- Integrations
- Continuous export

**Policy settings**

- Security policy
- Governance rules (preview)

**Select Defender plan** **Enable all**

| Plan          | Pricing   | Resource quantity       | Monitoring coverage                      | Status   |
|---------------|---|-------------------------|--|--|
| Defender CSPM | Free (preview)<br><a href="#">Details &gt;</a>              | N/A                     | Full<br><a href="#">Settings &gt;</a>    | <input checked="" type="checkbox"/> On<br><input type="checkbox"/> Off |
| Servers       | Plan 2 (\$15/Server/Mo)<br><a href="#">Change plan &gt;</a> | 6 servers               | Partial<br><a href="#">Settings &gt;</a> | <input checked="" type="checkbox"/> On<br><input type="checkbox"/> Off |
| App Service   | \$15/Instance/Month<br><a href="#">Details &gt;</a>         | 0 instances             | Full                                     | <input checked="" type="checkbox"/> On<br><input type="checkbox"/> Off |
| Databases     | Selected: 4/4<br><a href="#">Select types &gt;</a>          | Protected: 1/1 instance | Full<br><a href="#">Settings &gt;</a>    | <input checked="" type="checkbox"/> On<br><input type="checkbox"/> Off |

**Recommendations** ×

[Refresh](#) [Download CSV report](#) [Open query](#) [Governance report \(preview\)](#) [Guides & Feedback](#)

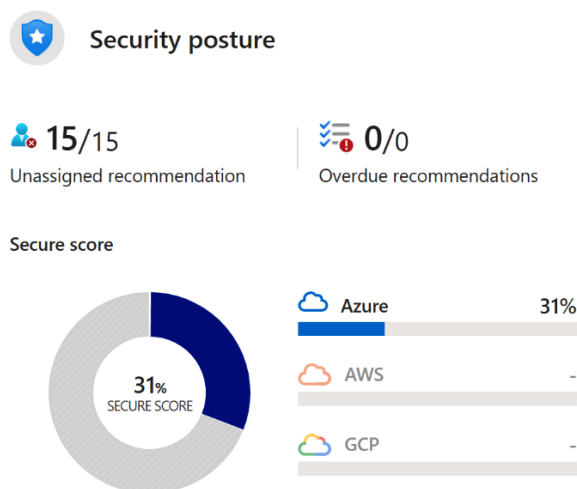
**Secure score recommendations** **All recommendations**

**Secure score** **Active items** **Resource health** **Governance (preview)**

**30%** **Controls 11/15** **Recommendations 15/45** **Unhealthy (11)** **Healthy (4)** **Not applicable (3)** **Overdue recommendations 0/0** **Unassigned recommendations 15/15**

Search recommendations **Environment == Azure** **Recommendation status == None** [Add filter](#) **More (4)** **Show my items only:** ☐ Off

| Name                         | Max score | Current score | Potential score increase | Status     | Unhealthy resources | Insights |
|------------------------------|-----------|---------------|--------------------------|------------|---------------------|----------|
| Enable MFA                   | 10        | 0.00          | +18%                     | Unassigned | 1 of 1 resources    |          |
| Secure management ports      | 8         | 1.60          | +11%                     | Unassigned | 4 of 5 resources    |          |
| Apply system updates         | 6         | 6.00          | +0%                      | Completed  | 0 of 5 resources    |          |
| Remediate vulnerabilities    | 6         | 0.00          | +11%                     | Unassigned | 5 of 5 resources    |          |
| Encrypt data in transit      | 4         | 2.67          | +2%                      | Unassigned | 1 of 3 resources    |          |
| Restrict unauthorized net... | 4         | 0.80          | +6%                      | Unassigned | 4 of 11 resources   |          |



[Explore your security posture >](#)



## 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 >](#)



### 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
- Environment settings
- Security solutions
- Workflow automation

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. →

Microsoft cloud security benchmark PCI DSS 3.2.1 SOC TSP NIST SP 800 53 R4 Azure CIS 1.1.0 ISO 27001:2013

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 Microsoft Azure Sponsorship

☐ Expand all compliance controls

#### NS. Network Security

- NS-1. Establish network segmentation boundaries [Control details](#) MS C
- NS-2. Secure cloud services with network controls [Control details](#) MS C
- NS-3. Deploy firewall at the edge of enterprise network [Control details](#) MS C
- NS-4. Deploy intrusion detection/intrusion prevention systems (IDS/IPS) [Control details](#) MS C
- NS-5. Deploy DDOS protection [Control details](#) MS C

[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](#) MS C
- PV-2. Audit and enforce secure configurations [Control details](#) MS C
- PV-3. Define and establish secure configurations for compute resources [Control details](#) MS C
- PV-4. Audit and enforce secure configurations for compute resources [Control details](#) MS C
- PV-5. Perform vulnerability assessments [Control details](#) MS C
- PV-6. Rapidly and automatically remediate vulnerabilities [Control details](#) MS C
- PV-7. Conduct regular red team operations [Control details](#) MS C

## ^ x PV. Posture and Vulnerability Management

- ✓ PV-1. Define and establish secure configurations [Control details](#) MS C
- ✓ PV-2. Audit and enforce secure configurations [Control details](#) MS C
- ✓ PV-3. Define and establish secure configurations for compute resources [Control details](#) MS C
- ✓ x PV-4. Audit and enforce secure configurations for compute resources [Control details](#) MS C
- ✓ PV-5. Perform vulnerability assessments [Control details](#) MS C
- ^ x PV-6. Rapidly and automatically remediate vulnerabilities [Control details](#) MS C

| Customer responsibility   | Resource type    | Failed resources | Resource compliance status |
|---|------------------|------------------|----------------------------|
| <a href="#">Machines should be configured securely</a>                              | Virtual machines | 3 of 5           | <div><div></div></div>     |
| <a href="#">SQL databases should have vulnerability findings resolved</a>           | SQL servers      | 1 of 1           | <div><div></div></div>     |
| <a href="#">SQL servers on machines should have vulnerability findings resolved</a> | Azure resources  | 0 of 0           | <div><div></div></div>     |

## SQL databases should have vulnerability findings resolved ...

[Exempt](#) [Disable rule](#) [View policy definition](#) [Open query](#) ▼

i 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

Tightly define  
your policy

Audit your  
existing resources

Audit new or  
updated resource  
requests

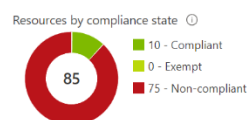
Deploy your  
policy to  
resources

Continuous  
monitoring

## Policy ...

- 
- Overview
  - Getting started
  - Compliance
  - Remediation
  - Events
  - Authoring
    - Definitions
    - Assignments
    - Exemptions











Overall resource compliance i  
**12%**  
10 out of 85



**LEARN MORE**  
[Learn about Policy](#) i  
[Onboarding tutorial](#)

Non-compliant initiatives i  
**4**  
out of 6

Non-compliant policies i  
**153**  
out of 1587

| Name  | Scope                  | Compliance state  | Resource compli... | Non-Compliant Res... | Non-compliant poli... |
|---|------------------------|---|--------------------|----------------------|-----------------------|
|  ISO 27001:2013              | Microsoft Azure Spo... |  Non-compliant | 0% (0 out of 44)   | 44                   | 20                    |
|  NIST SP 800-53 R4           | Microsoft Azure Spo... |  Non-compliant | 16% (7 out of 44)  | 37                   | 55                    |
|  CIS Microsoft Azure Fou...  | Microsoft Azure Spo... |  Non-compliant | 30% (14 out of 47) | 33                   | 34                    |
|  ASC Default (subscriptio... | Microsoft Azure Spo... |  Non-compliant | 27% (7 out of 26)  | 19                   | 43                    |
|  Windows machines sho...     | Microsoft Azure Spo... |  Non-compliant | 0% (0 out of 1)    | 1                    | 1                     |

Policy | Definitions

Search

Policy definition

Initiative definition

Export definitions

Refresh

Overview

Events

Authoring

Definitions

Assignments

Exemptions

Microsoft Azure Sponsor...

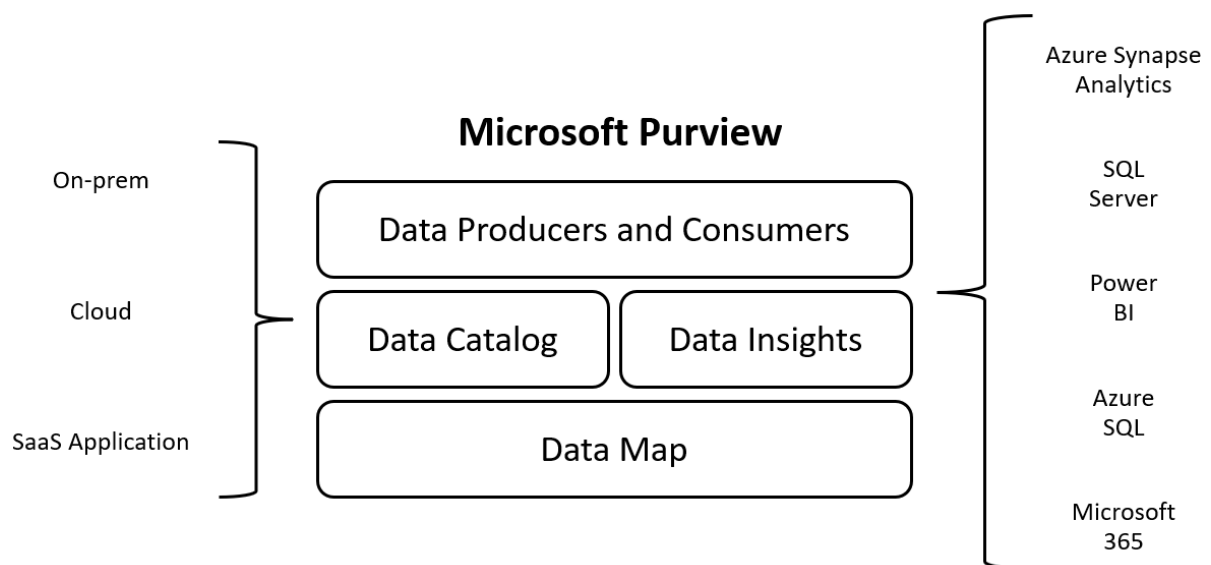
All definition types

All categories

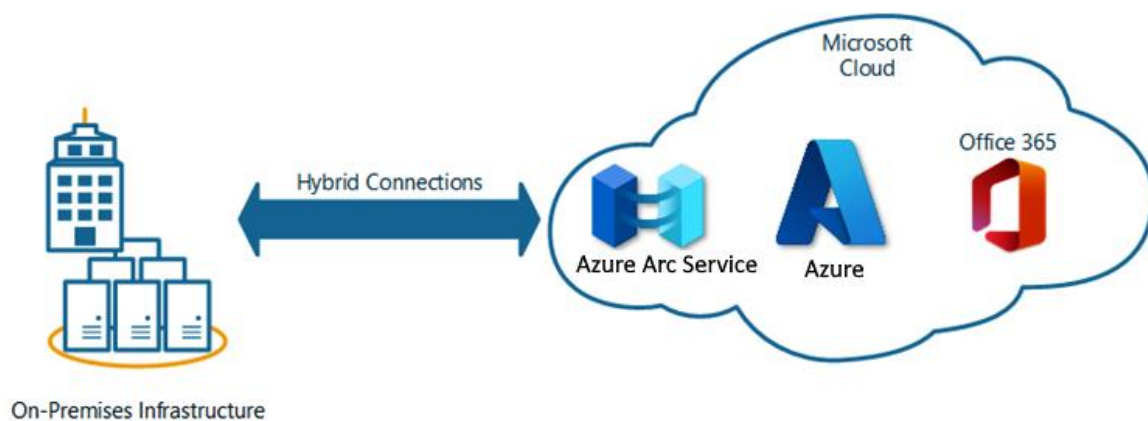
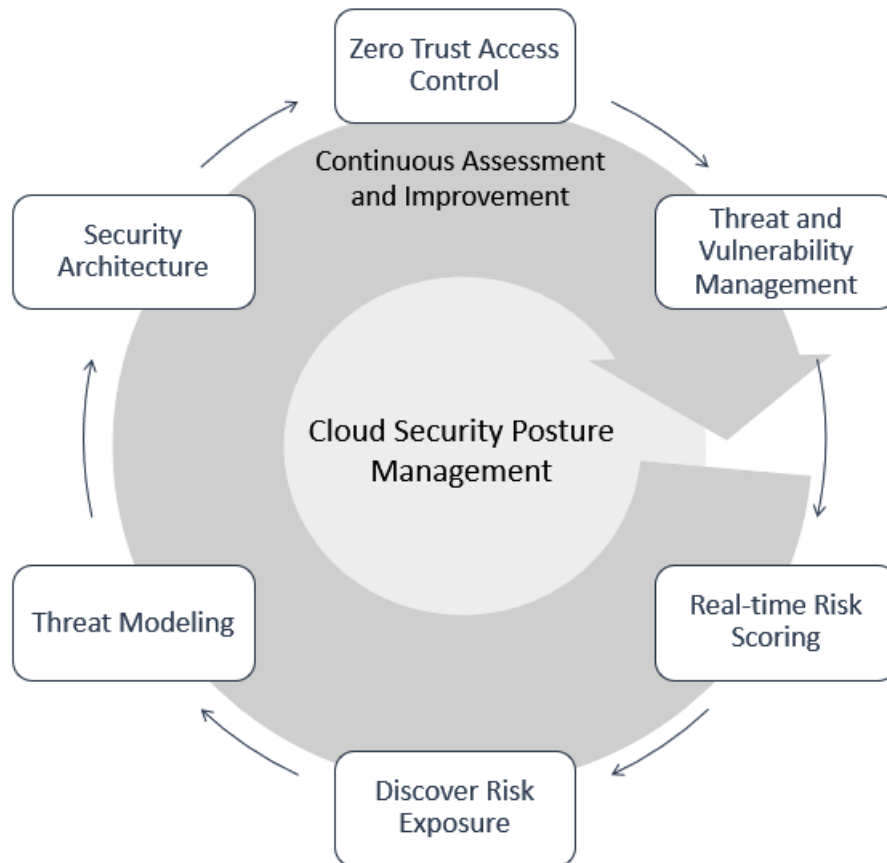
Filter by name or ID...

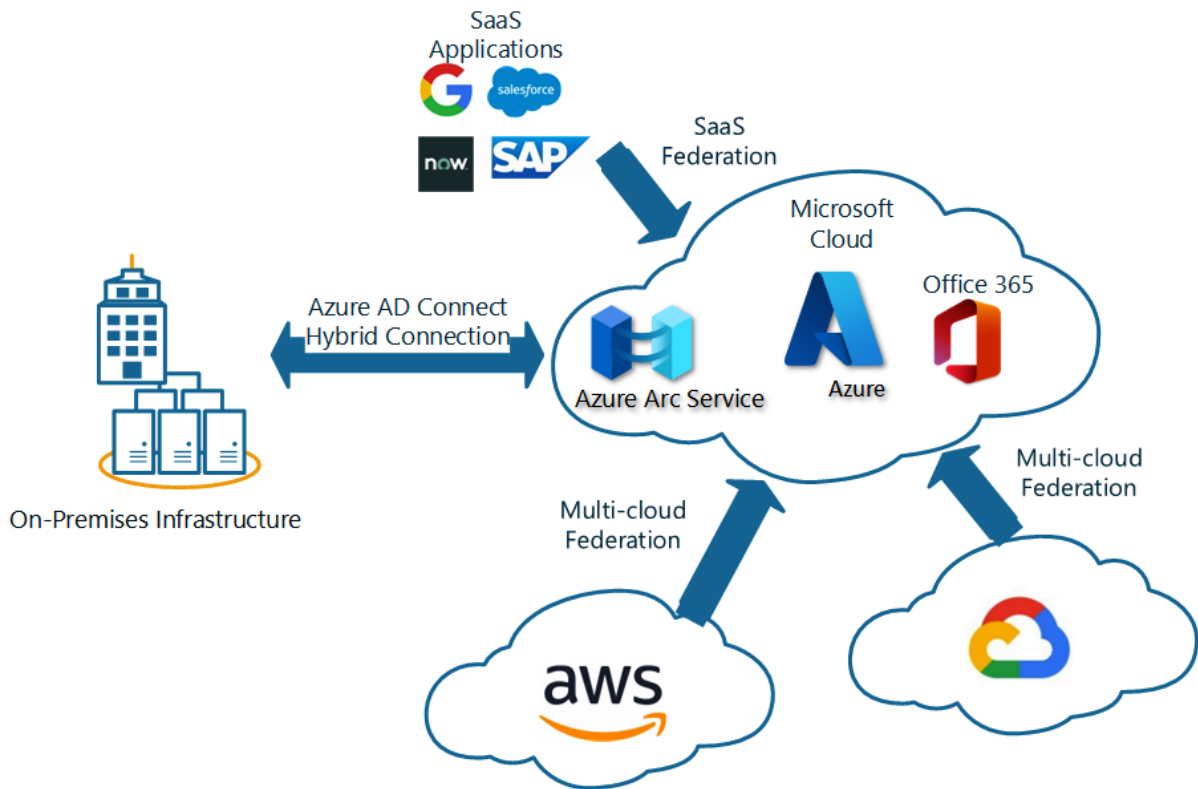
| Name  | Type       | De...      | Category              |
|---|------------|------------|-----------------------|
| Separately store backup information                                     | BuiltIn    | Policy     | Regulatory Compliance |
| Enforce appropriate usage of all accounts                               | BuiltIn    | Policy     | Regulatory Compliance |
| Notify users of system logon or access                                  | BuiltIn    | Policy     | Regulatory Compliance |
| Observe and report security weaknesses                                  | BuiltIn    | Policy     | Regulatory Compliance |
| Secure the interface to external systems                                | BuiltIn    | Policy     | Regulatory Compliance |
| Establish usage restrictions for mobile code technologies               | BuiltIn    | Policy     | Regulatory Compliance |
| Review cloud service provider's compliance with policies and agreements | BuiltIn    | Policy     | Regulatory Compliance |
| NIST SP 800-171 Rev. 2  | 4. BuiltIn | Initiative | Regulatory Compliance |
| IRS1075 September 2016  | 6. BuiltIn | Initiative | Regulatory Compliance |
| NIST SP 800-53 Rev. 5   | 7. BuiltIn | Initiative | Regulatory Compliance |

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



## Chapter 6: Evaluating Security Posture and Recommending Technical Strategies to Manage Risk





## Microsoft Defender for Cloud | Regulatory compliance

Showing subscription 'Microsoft Azure Sponsorship'

Search

Download report Manage compliance policies Open query

You can now fully customize the standards you track in the dashboard. Update your dashboard by selecting 'Manage compliance policies' above.

**Cloud Security**

- Security posture
- Regulatory compliance**
- Workload protections

**Management**

- Environment settings
- Security solutions

**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 'Microsoft Azure Sponsorship'

Search

Download reportManage compliance policiesOpen queryCompliance over time workbook

Recommendations

Security alerts

Inventory

Workbooks

Community

Diagnose and solve problems

Cloud Security

Security posture

Regulatory compliance

Workload protections

You can now fully customize the standards you track in the dashboard. Update your dashboard by selecting 'Manage compliance policies' above.

Azure Security Benchmark V3

PCI DSS 3.2.1

SOC TSP

NIST SP 800 53 R4

Azure CIS 1.1.0

Under each applicable compliance control is the set of assessments run by Defender for Cloud that are associated with that control. If they are all green, it means those assessments are currently passing; this does not ensure you are fully compliant with that control. Furthermore, not all controls for any particular regulation are covered by Defender for Cloud assessments, and therefore this report is only a partial view of your overall compliance status.

Azure Security Benchmark is applied to the subscription Microsoft Azure Sponsorship

☐ 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

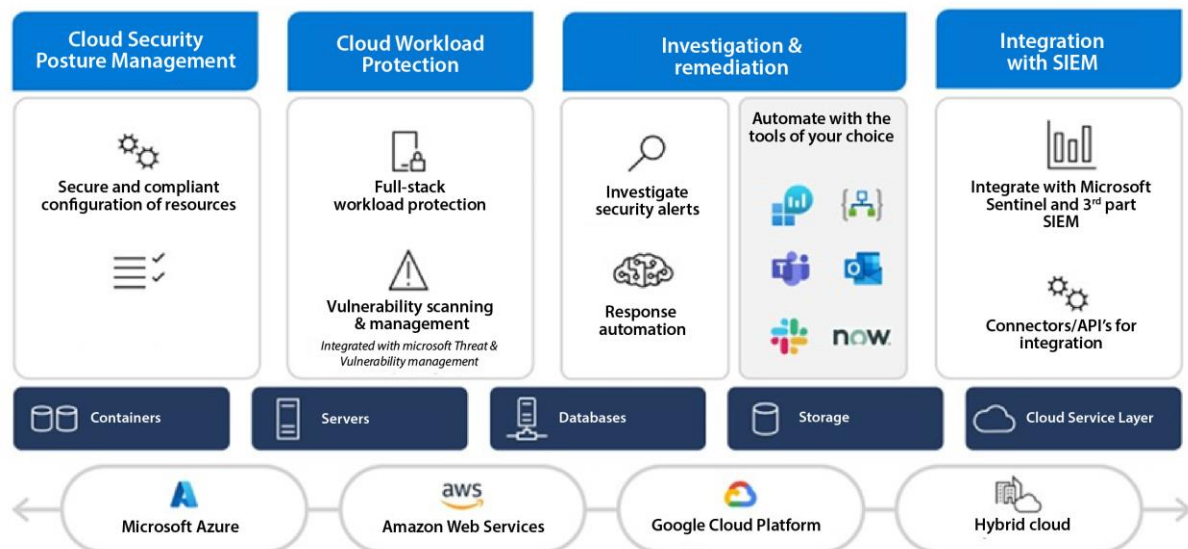
## ^ ❌ NS. Network Security

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

| Customer responsibility                                     | Resource type  | Failed resources | Resource complianc...  |
|---|--|------------------|------------------------|
| <a href="#">Adaptive network hardening recommenda</a>       |  Virtual machines | 4 of 5           | <div><div></div></div> |
| <a href="#">All network ports should be restricted on i</a> |  Virtual machines | 4 of 5           | <div><div></div></div> |
| <a href="#">Subnets should be associated with a netw</a>    |  Subnets          | 2 of 3           | <div><div></div></div> |
| <a href="#">Non-internet-facing virtual machines shou</a>   |  Virtual machines | 0 of 5           | <div><div></div></div> |
| <a href="#">Internet-facing virtual machines should be</a>  |  Virtual machines | 0 of 5           | <div><div></div></div> |

- ✓ ✗ 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'

[Secure score over time](#) [Governance report \(preview\)](#) [Guides & Feedback](#)

### General

- Overview
- Getting started
- Recommendations
- Security alerts
- Inventory
- Workbooks
- Community
- Diagnose and solve problems

### Cloud Security

- Security posture**
- Regulatory compliance
- Workload protections

### All environments

☒ Azure ☒ AWS ☐ GCP

#### Secure score



|       |     |
|-------|-----|
| Azure | 31% |
| AWS   | N/A |
| GCP   | N/A |

#### Environment

2 Total

Subscriptions 1 Accounts 1

#### Governance (preview)

No data to display

## Microsoft Defender for Cloud | Security posture

Showing subscription 'Microsoft Azure Sponsorship'

[Secure score over time](#) [Governance report \(preview\)](#) [Guides & Feedback](#)

### General

- Overview
- Getting started
- Recommendations
- Security alerts
- Inventory
- Workbooks
- Community
- Diagnose and solve problems

### Cloud Security

- Security posture**
- Regulatory compliance
- Workload protections

Subscriptions 1 Accounts 1

11/18  
Unhealthy resources

45  
Recommendations

#### Environment Owner (preview)

Environment == Azure, AWS

☐ Group by environment

Name ↑↓ Secure score ↑↓ Unhealthy resourc... ↑↓ Recommendations

|   |     |          |  |
|---|-----|----------|--|
| Microsoft Azure Sponsorship<br>Azure subscription | 31% | 11 of 15 | <a href="#">View recommendation...</a> |
| 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 ⓘ

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 <div></div> | + 18%                       | Unassigned | 1 of 1 resources <div></div> |
| Secure manage...     | 8            | 1.60 <div></div> | + 11%                       | Unassigned | 4 of 5 resources <div></div> |
| Remediate vuln...    | 6            | 0.00 <div></div> | + 11%                       | Unassigned | 5 of 5 resources <div></div> |
| Apply system u...    | 6            | 6.00 <div></div> | + 0%                        | Completed  | 0 of 5 resources <div></div> |
| Encrypt data in t... | 4            | 2.67 <div></div> | + 2%                        | Unassigned | 1 of 3 resources <div></div> |

| Name ↑↓    | Max score ↑↓ | Current score ↑↓ | Potential score increase ↑↓ |
|------------|--------------|------------------|-----------------------------|
| Enable MFA | 10           | 0.00 <div></div> | + 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:

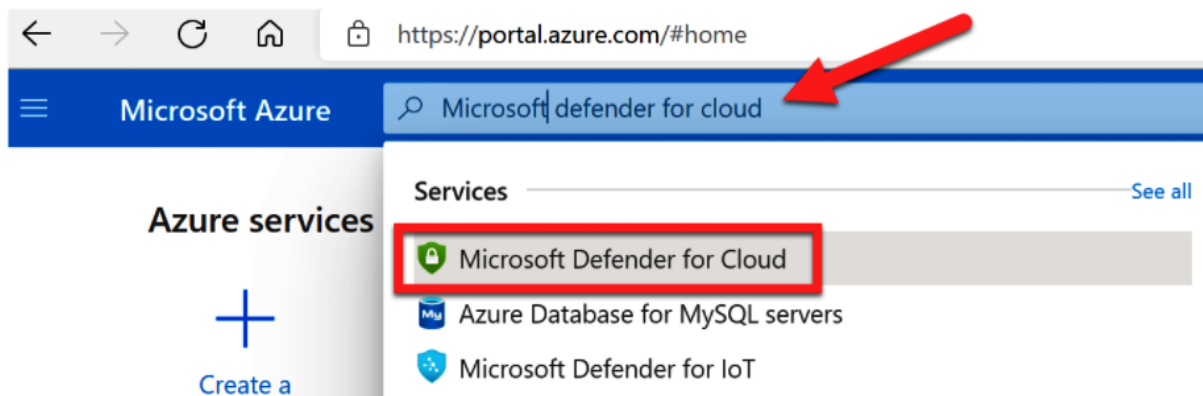
To enable MFA using conditional access you must have an Azure AD Premium license and have AD tenant admin permissions.

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



## Hybrid Cloud Protection



**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

| Standard       | 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

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 plan

Enable all

| Plan                      | Pricing  | Resource quantity       | Monitoring coverage                   | Status    |
|---------------------------|--|-------------------------|---------------------------------------|-----------|
| Cloud Security Posture Ma | Free   |                         |                                       | On<br>Off |
| Servers                   | Plan 2 (\$15/Server/Mo<br><a href="#">Change plan &gt;</a> ) | 5 servers               |                                       | On<br>Off |
| App Service               | \$15/Instance/Month  | 0 instances             |                                       | On<br>Off |
| Databases                 | Selected: 4/4<br><a href="#">Select types &gt;</a>           | Protected: 1/1 instance | Full<br><a href="#">Settings &gt;</a> | On<br>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%)

Azure SQL database servers 1/1

Upgrade

Key Vault 1/1

Upgrade

Servers 5/5

Upgrade

DNS subscriptions 1/1

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

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

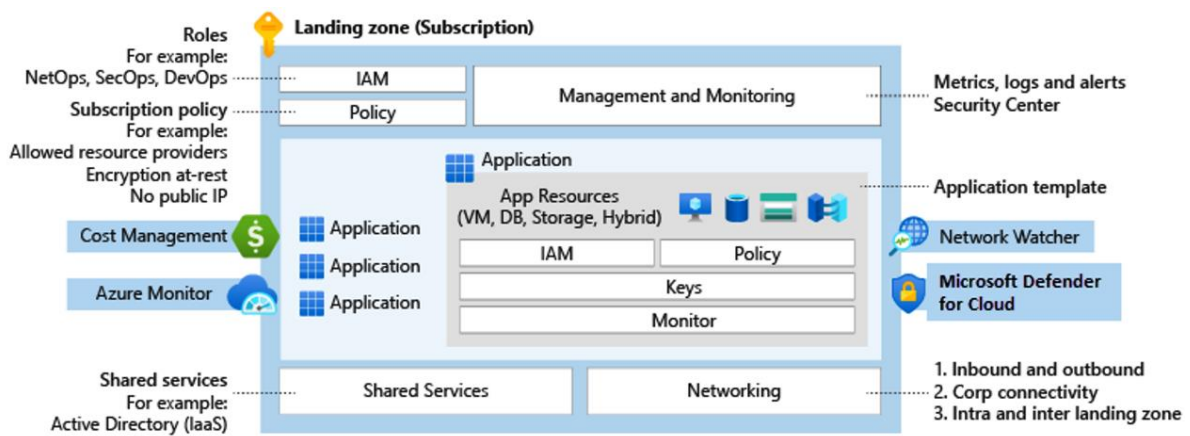
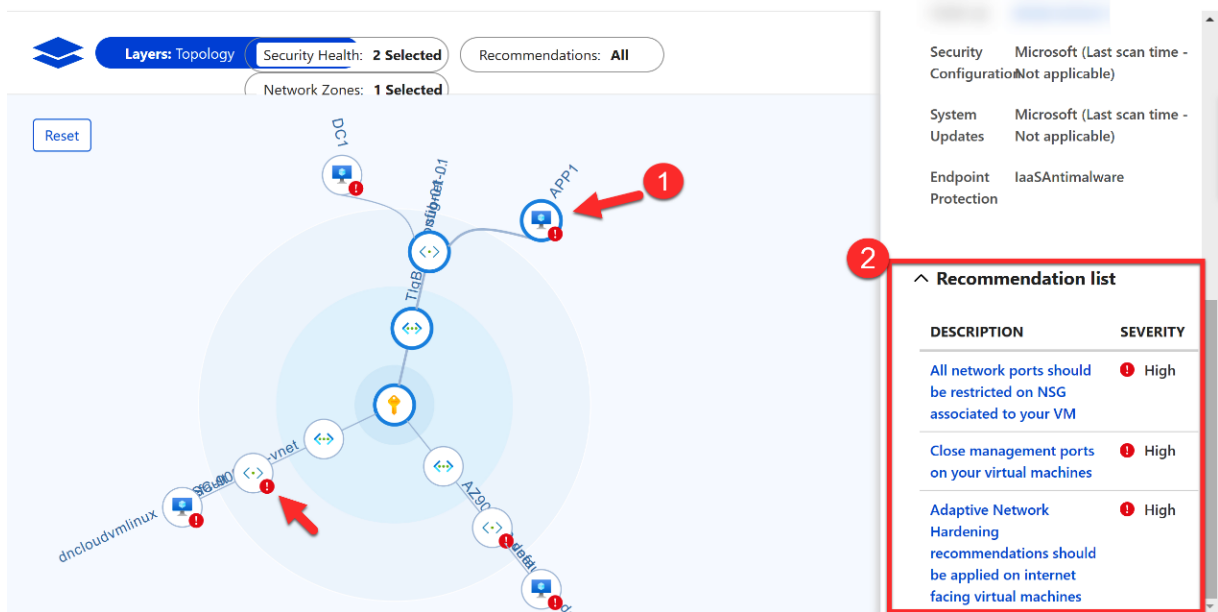
File integrity monitoring

Network map

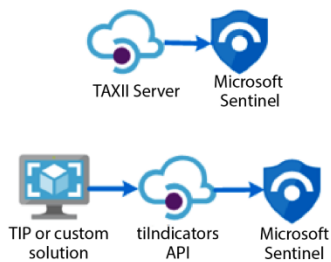
IoT security

## Network Map ...

Showing subscription 'Microsoft Azure Sponsorship'



## Microsoft Sentinel Data connectors



## Microsoft Sentinel Logs

| ThreatIntelligenceIndicator                                   |                       |        |                 |                   |   |
|---|-----------------------|--------|-----------------|-------------------|---|
| where TimeGenerated > ago(24h)                                |                       |        |                 |                   |   |
| limit 10  |                       |        |                 |                   |   |
| Results Chart Columns Add bookmark Display time (UTC+00:00)   |                       |        |                 |                   |   |
| Completed   |                       |        |                 |                   |   |
| Drag a column header and drop it here to group by that column |                       |        |                 |                   |   |
| <input type="checkbox"/>                                      | TimeGenerated...      | Action | ApplicationId   | AzureTenantId     | Description                                   |
| >   | 4/7/2020, 7:21:02.... | alert  | 7E7BB8EC-916... | 72f988bf-86f1-... | TS ID: 55475482452; iType: suspicious_dom...  |
| >   | 4/7/2020, 7:21:03.... | alert  | 7E7BB8EC-916... | 72f988bf-86f1-... | TS ID: 55474479406; iType: suspicious_dom...  |
| >   | 4/7/2020, 7:21:03.... | alert  | 7E7BB8EC-916... | 72f988bf-86f1-... | TS ID: 55478096090; iType: phish_domain; S... |

## Microsoft Sentinel Analytics

**Incidents**

**Playbooks**

**TI map IP entity to AzureActivity**

Medium Severity Scheduled Rule Type

Description  
Identifies a match in AzureActivity from any IP IOC from TI

Data sources  
Threat Intelligence Platforms (Preview)  
ThreatIntelligenceIndicator --

Azure Activity  
AzureActivity --

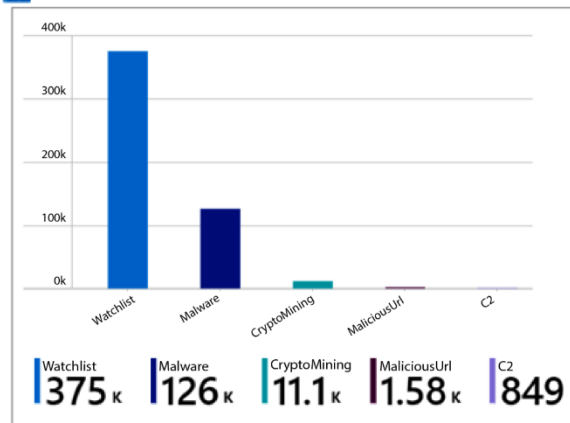
Tactics  
Impact

Rule query

```

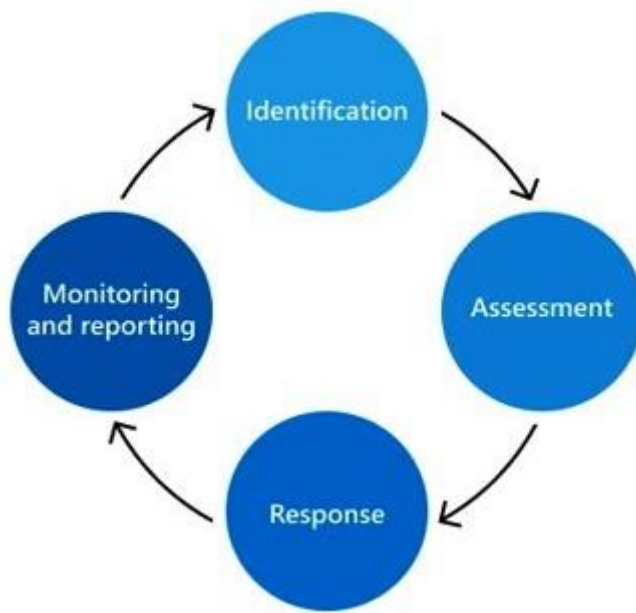
let dt_lookBack = 1h;
let ioc_lookBack = 14d;
ThreatIntelligenceIndicator
| where TimeGenerated >= ago(ioc_lookBack) and Exp
| where Active == true
// Picking up only IOC's that contain the entities
  
```

## Microsoft Sentinel Workbooks

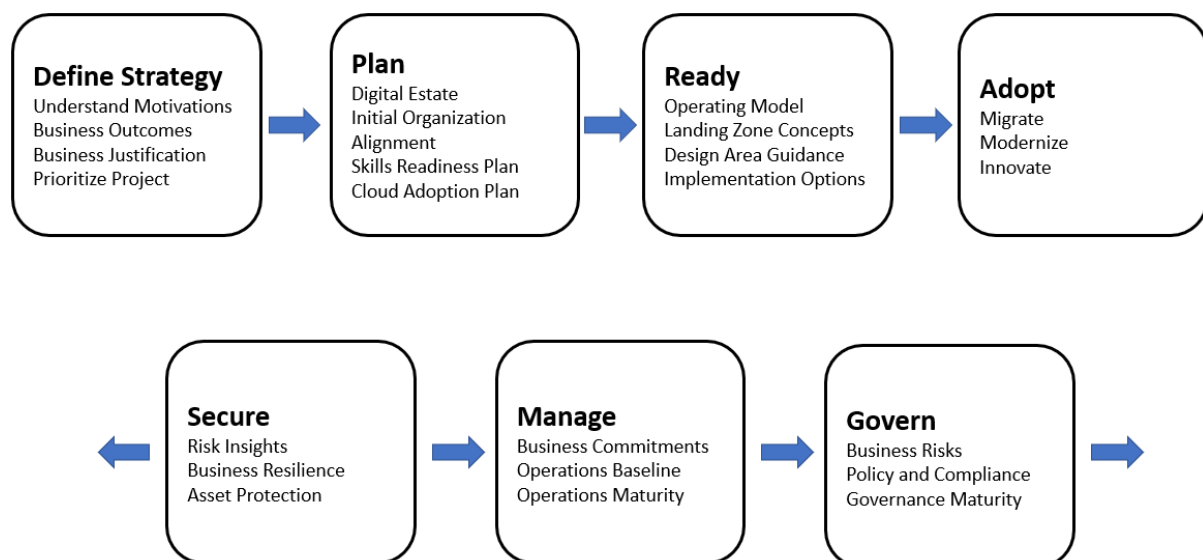
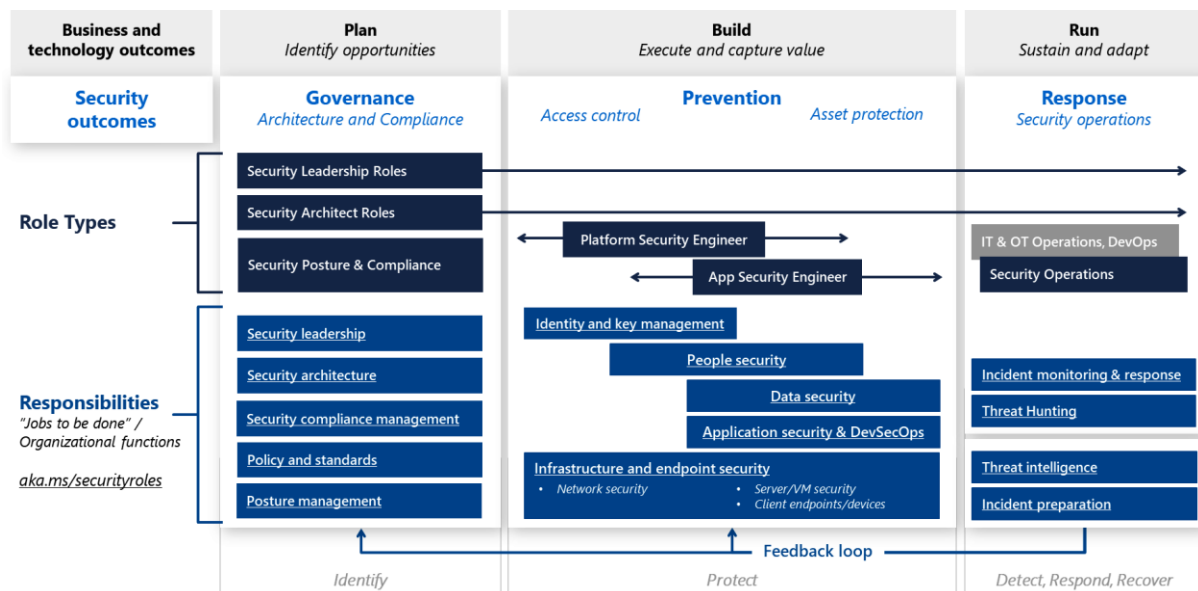


|   |   |                             |                             |                                |
|---|---|-----------------------------|-----------------------------|--------------------------------|
| Likelihood<br>↑                         | Very Likely                             | Acceptable risk<br>Medium 2 | Unacceptable risk<br>High 3 | Unacceptable risk<br>Extreme 5 |
|   | Likely                                  | Acceptable risk<br>Low 1    | Acceptable risk<br>Medium 2 | Unacceptable risk<br>High 3    |
|   | Unlikely                                | Acceptable risk<br>Low 1    | Acceptable risk<br>Low 1    | Acceptable risk<br>Medium 2    |
|   | What is the chance that it will happen? | Minor                       | Moderate                    | Major                          |
| Impact<br>→<br>How serious is the risk? |   |                             |                             |                                |





# Chapter 7: Designing a Strategy for Securing Server and Client Endpoints



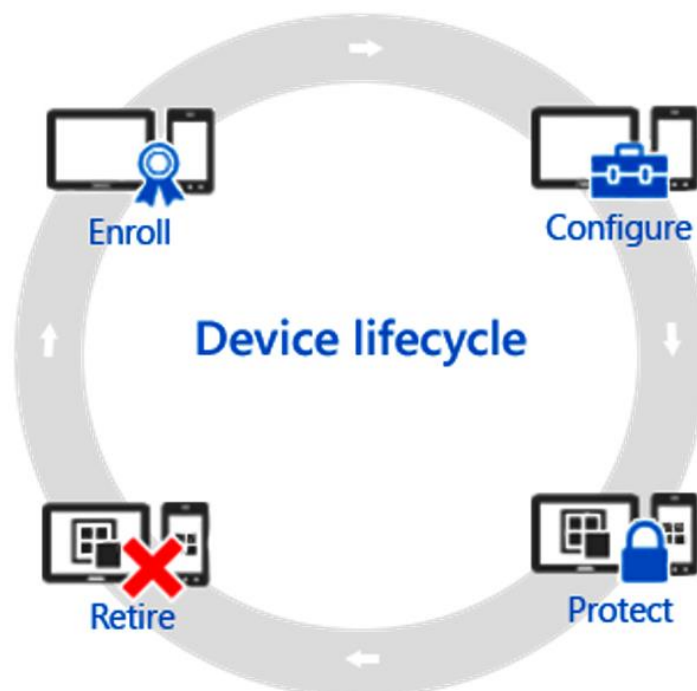
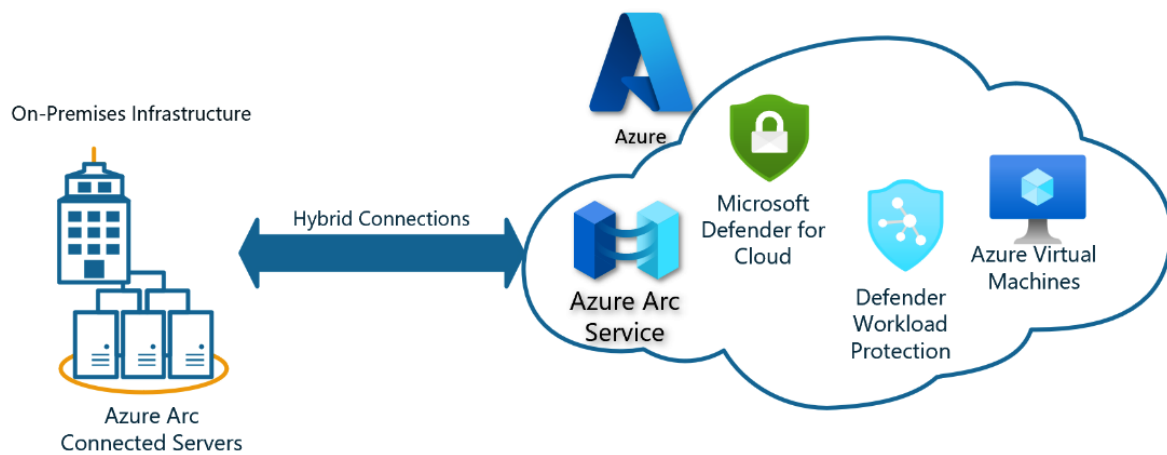
Microsoft Endpoint Manager admin center

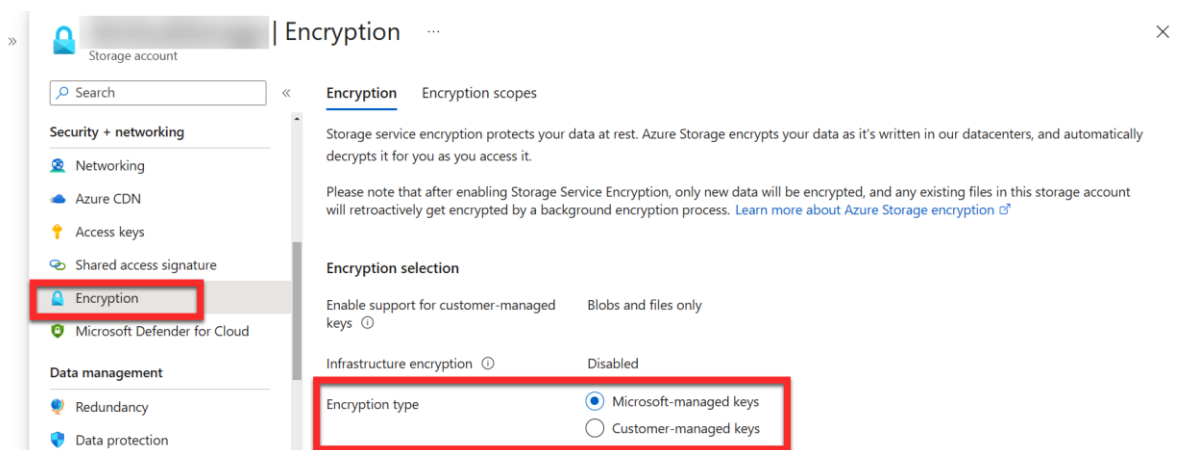
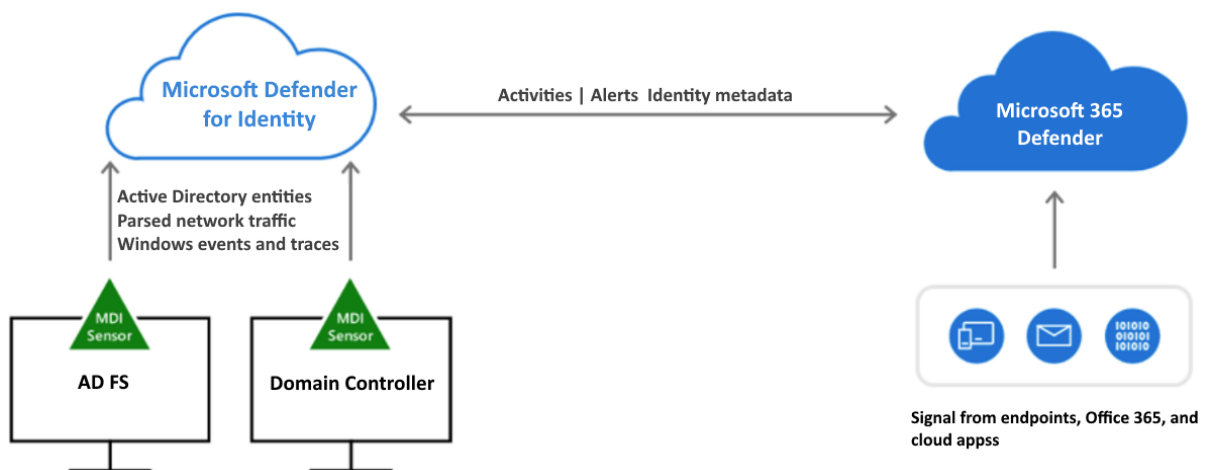
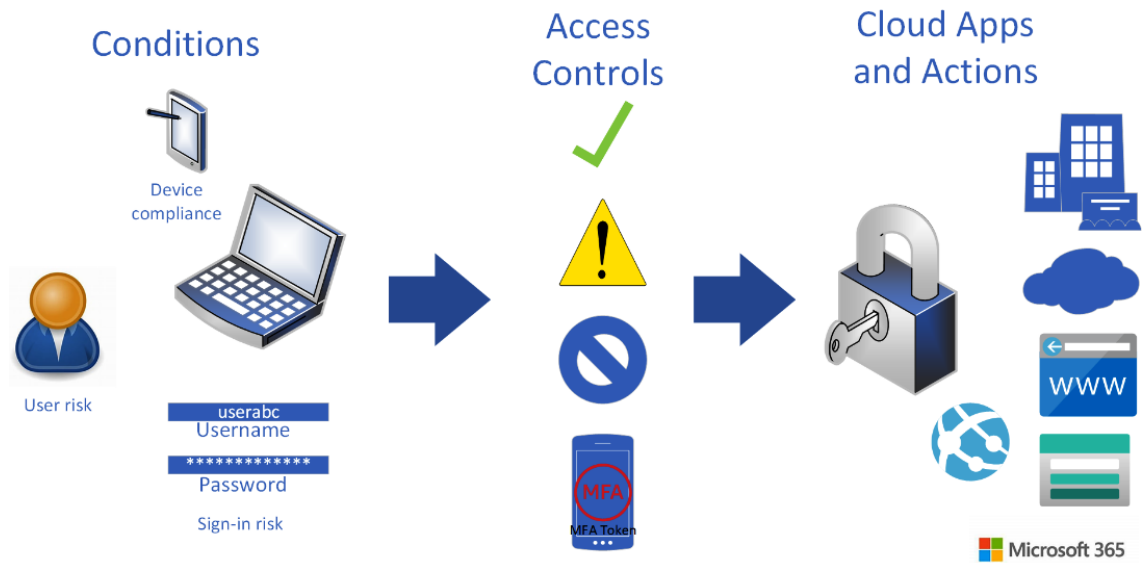
Home > Endpoint security | Overview > Endpoint security

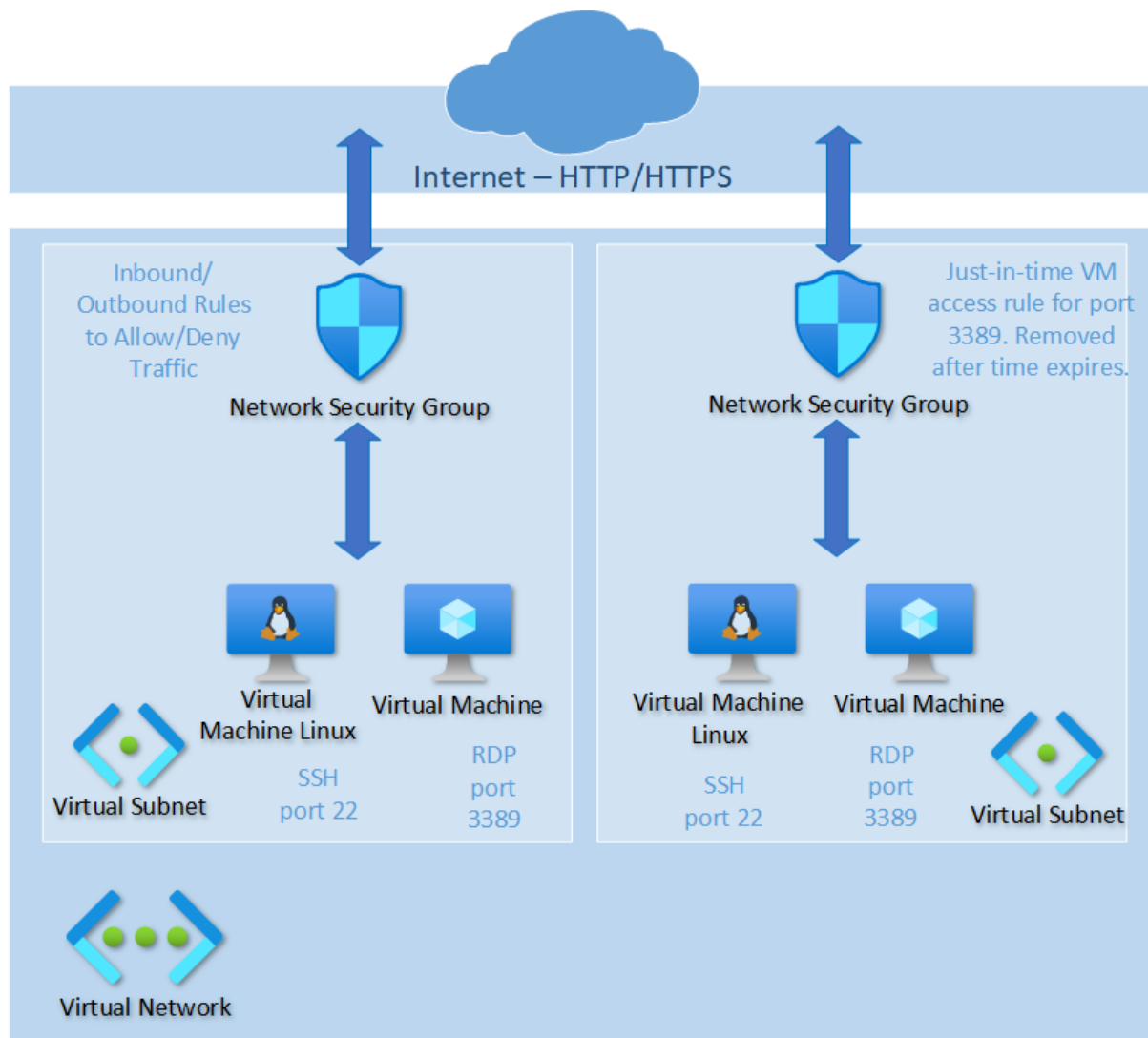
## Endpoint security | Security baselines

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        |

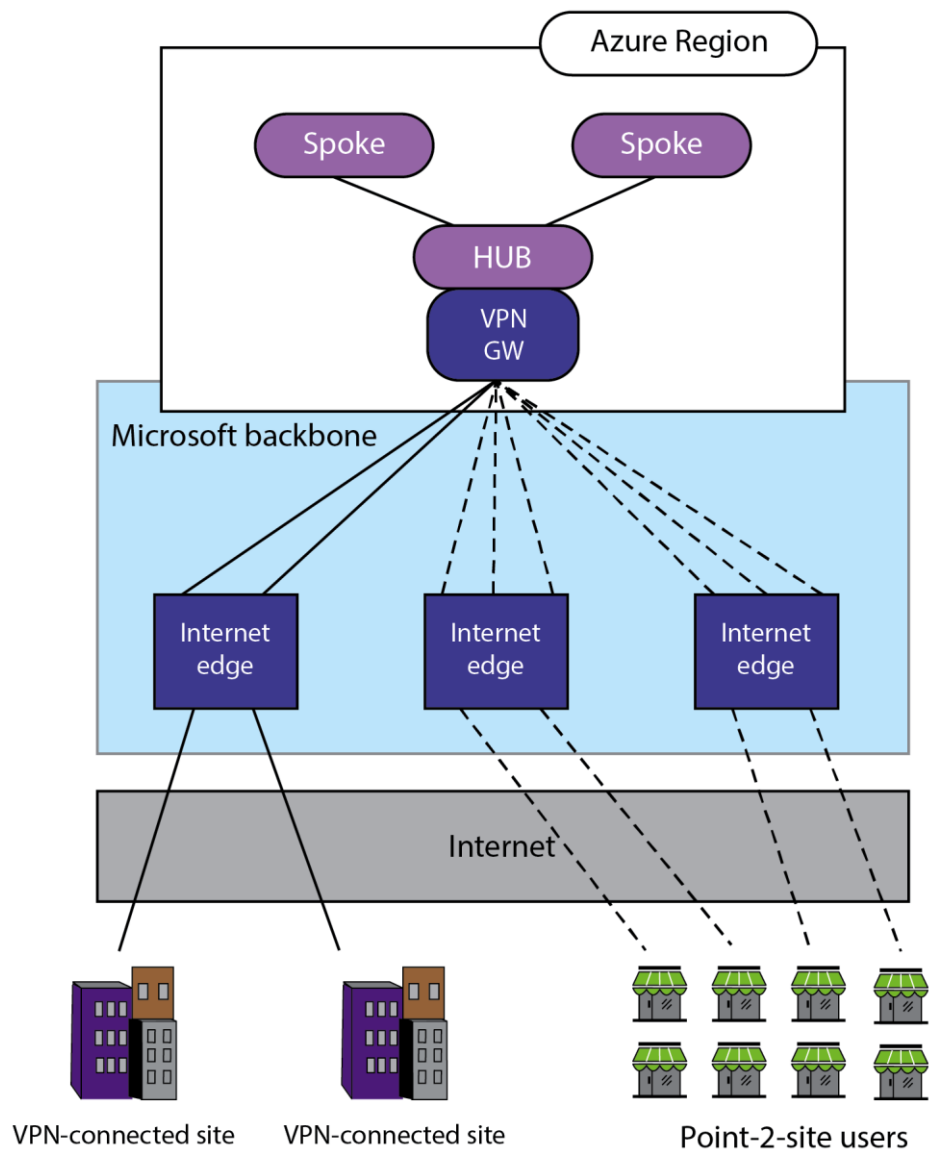




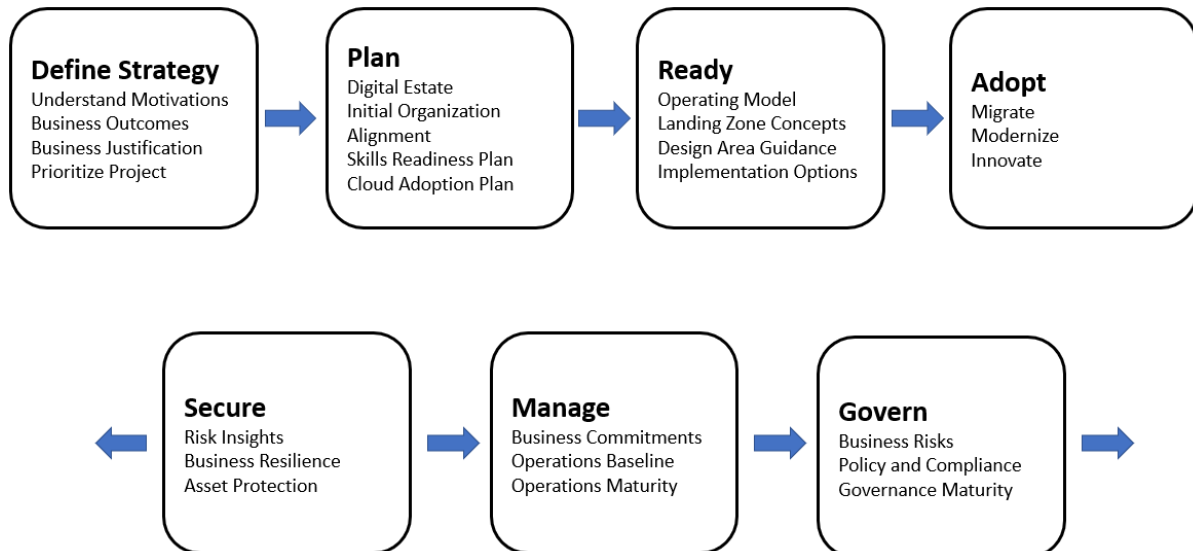




# Bastion Subnet



## Chapter 8: Designing 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 datacenter                   | Customer    | Microsoft | Microsoft          | Microsoft          |

Apps 138 IP addresses 8 Users 4 Devices 3 Traffic 91.7 GB ↑ 1.4 GB ↓ 90.3 GB

Cloud Discovery open alerts [+ Create policy](#)

0 Cloud Discovery alerts 0 Suspicious use alerts

#### App categories

◀ 1-5 of 38 ▶

Traffic

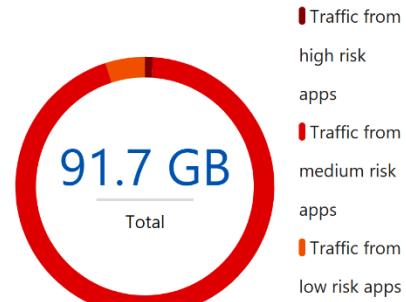
☒ Sanctioned ☒ Unsanctioned ☒ Other

|                          |                        |         |
|--------------------------|------------------------|---------|
| Development tools        | <div><div></div></div> | 55.7 GB |
| Security                 | <div><div></div></div> | 29.6 GB |
| Productivity             | <div><div></div></div> | 2.0 GB  |
| IT services              | <div><div></div></div> | 1.0 GB  |
| Cloud computing platf... | <div><div></div></div> | 925 MB  |

Risk I...

All categories

by Traffic



#### Secure score recommendations

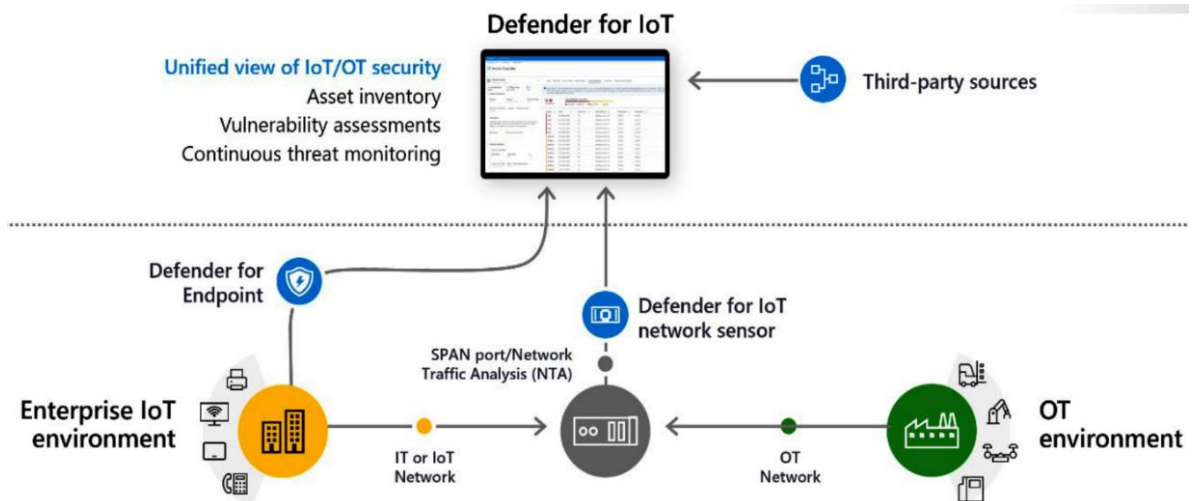
All recommendations

Unassigned recommendations  16/16 ⓘ

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

| Responsibility                      | On-prem | PaaS                     |  |                                       |   |
|-------------------------------------|---------|--------------------------|--|---------------------------------------|---|
| Data governance & rights management |         |                          |  |                                       | Application data – Depends on key/data management   |
| Client endpoints                    |         |                          |  |                                       | User/endpoints – Depends on least privilege design  |
| Account & access management         |         |                          |  |                                       | Admin access – One account → access to all apps / data / infra  |
| Identity & directory infrastructure |         |                          |  |                                       | Directory – Depends on identity system / app authentication   |
| Application                         |         |                          |  |                                       | Application code – One exploit can lead to access of all data   |
| Network controls                    |         |                          |  |                                       | Network configuration – Depends on TLS usage  |
| Operating system                    |         |                          |  |                                       | <b>Attack Azure Infrastructure</b> – Extremely low attack return on investment (ROI) for a single tenant <ul style="list-style-type: none"><li>Active security monitoring &amp; engineering make attack very expensive</li><li>Expense limits potential attackers to small pool with larger budgets</li></ul> |
| Physical hosts                      |         |                          |  |                                       |   |
| Physical network                    |         |                          |  |                                       |   |
| Physical datacenter                 |         |                          |  |                                       |   |
|                                     |         | Always attractive target |  | App design can quickly deter attacker |   |





## Defender for IoT | Getting started

Showing subscription 'Microsoft Azure Sponsorship'

- Search
- General
- Getting started
  - Device inventory (Preview)
  - Alerts (Preview)
  - Recommendations (Preview)
  - Workbooks (Preview)
  - Diagnose and solve problems (Preview)
- Management
- Sites and sensors
  - Pricing

## 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.

[Set up OT/ICS Security](#)



### Enterprise networks (IoT)

Gain full visibility into unmanaged IoT devices across your enterprise networks.

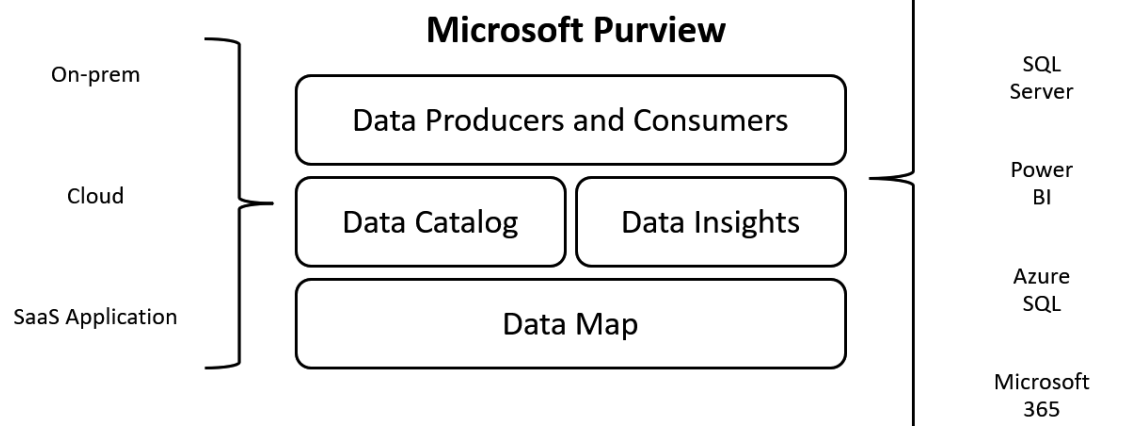
Using Microsoft Defender for Endpoint? Integrate it to improve network discovery.

[Set up Enterprise IoT Security](#)



### What else?

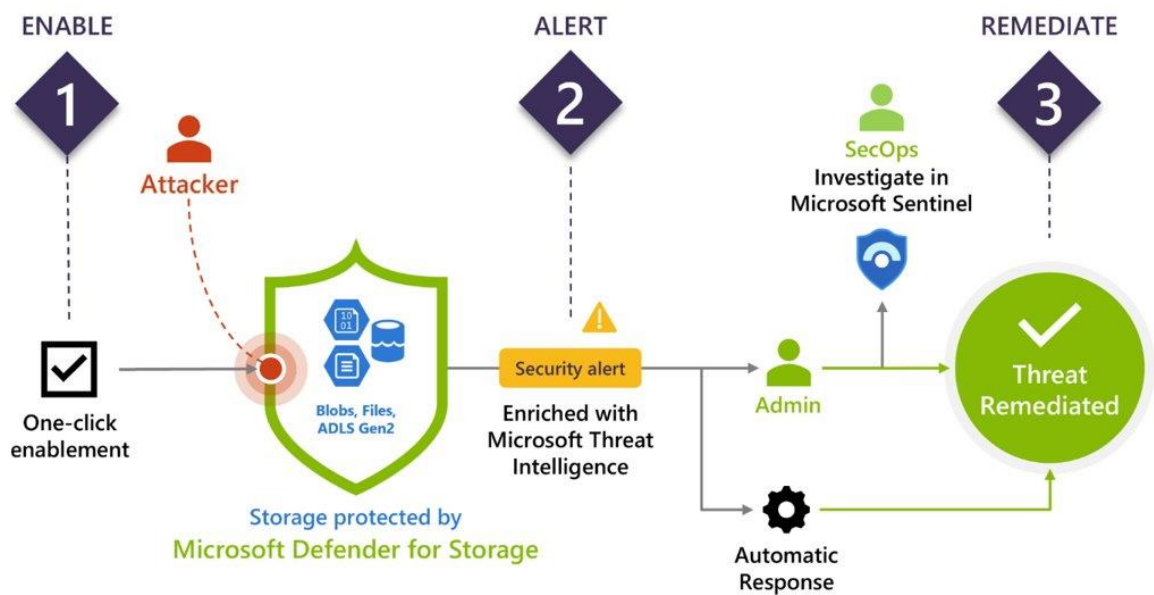
[Deploy an on-premises management console](#)  
[Connect to Microsoft Sentinel](#)  
[Join the community](#)

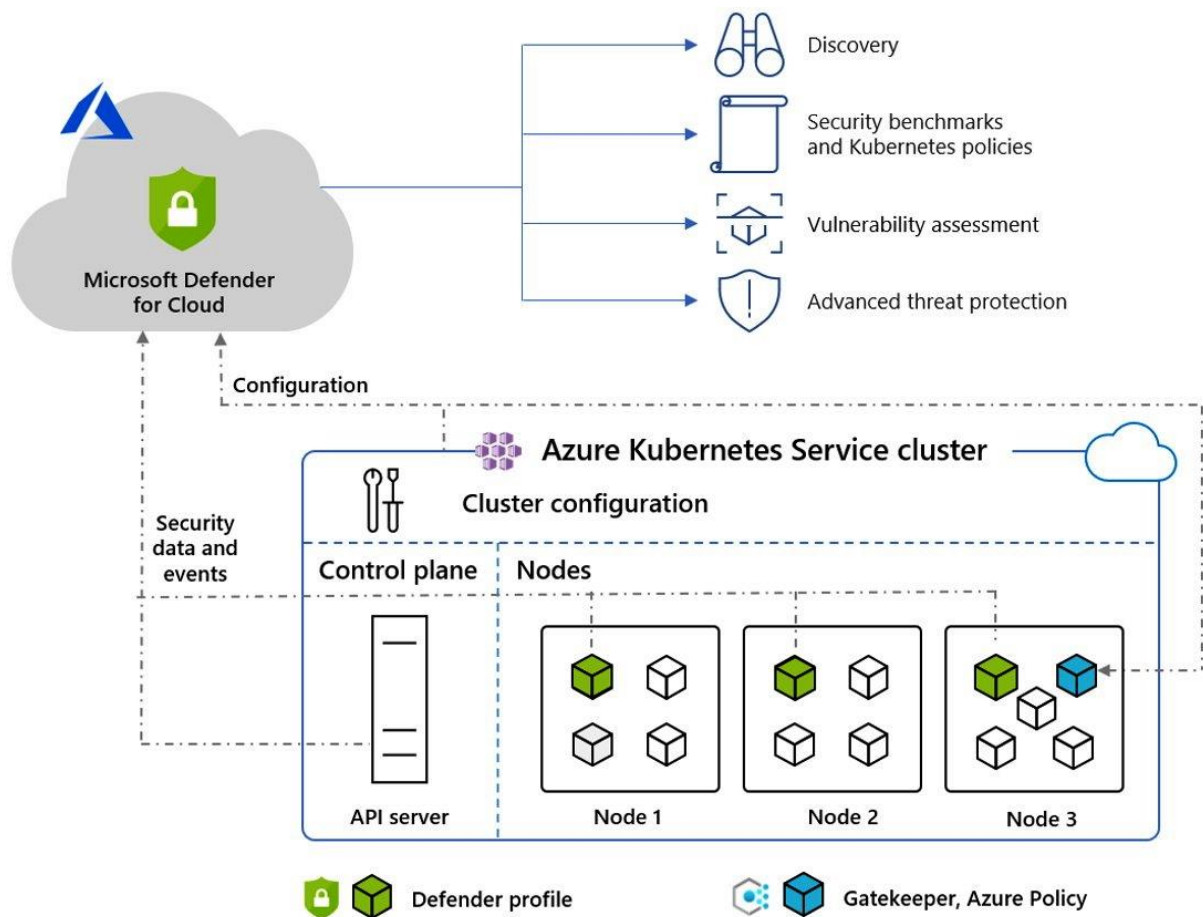


Secure score recommendations    All recommendations

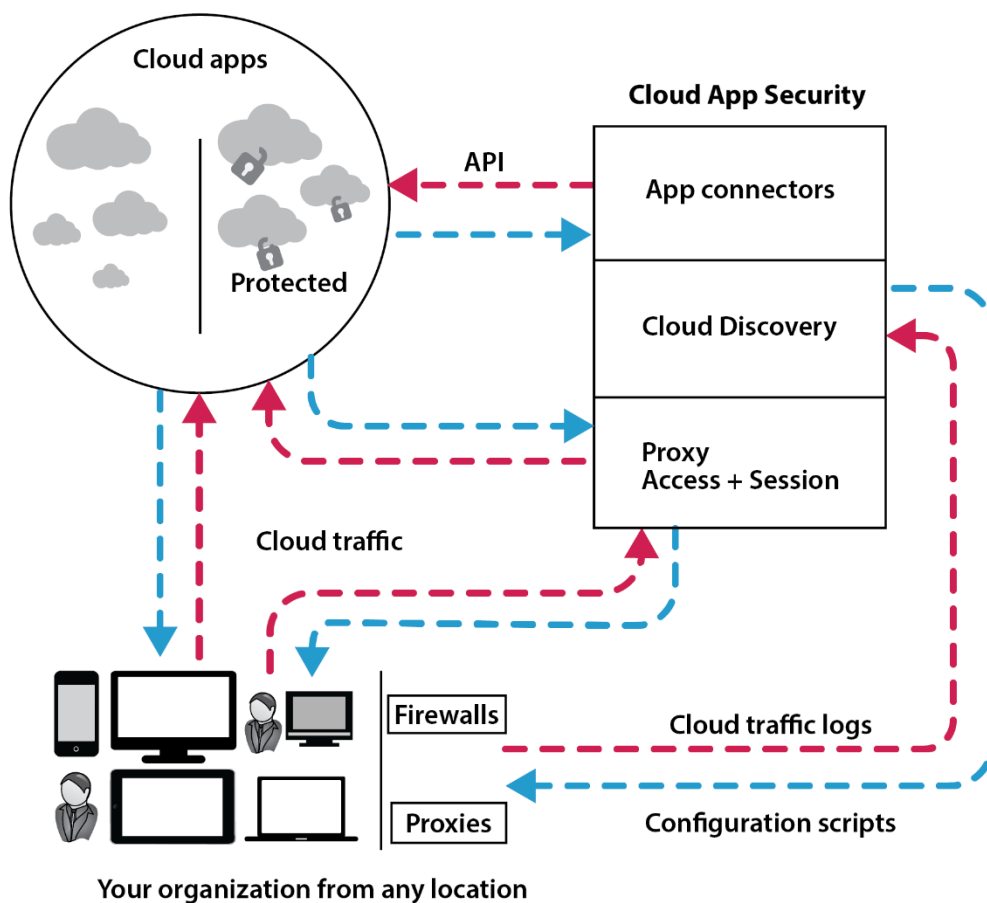
Unassigned recommendations    **16/16**

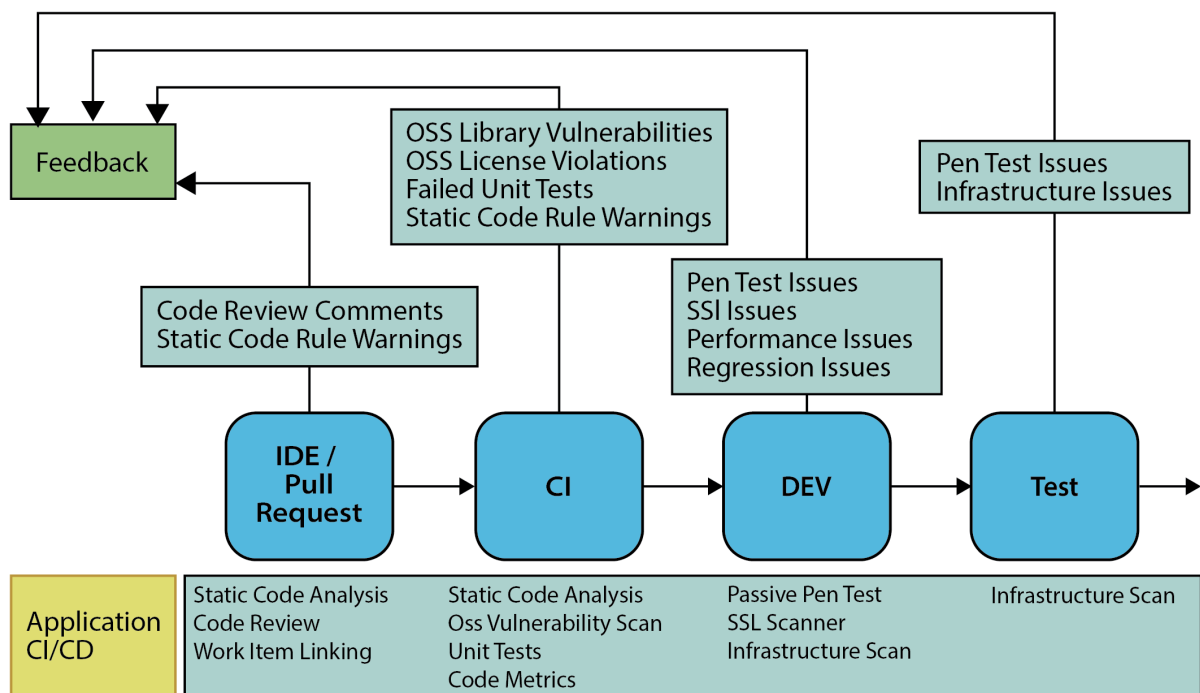
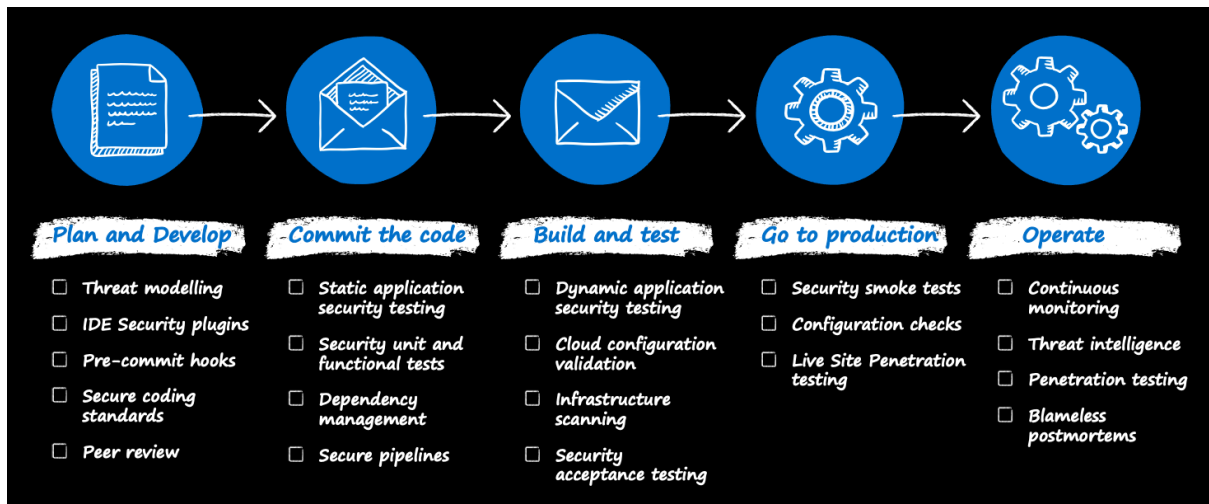
| Name ↑↓   | Max score ↑↓ | Current score ↑↓ | P... ↑↓ | Status ↑↓  | Unhealthy resources |
|---|--------------|------------------|---------|------------|---------------------|
| Transparent Data Encryption on SQL databases should be ena...     |              |                  |         | Completed  | 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         |              |                  |         |            |                     |

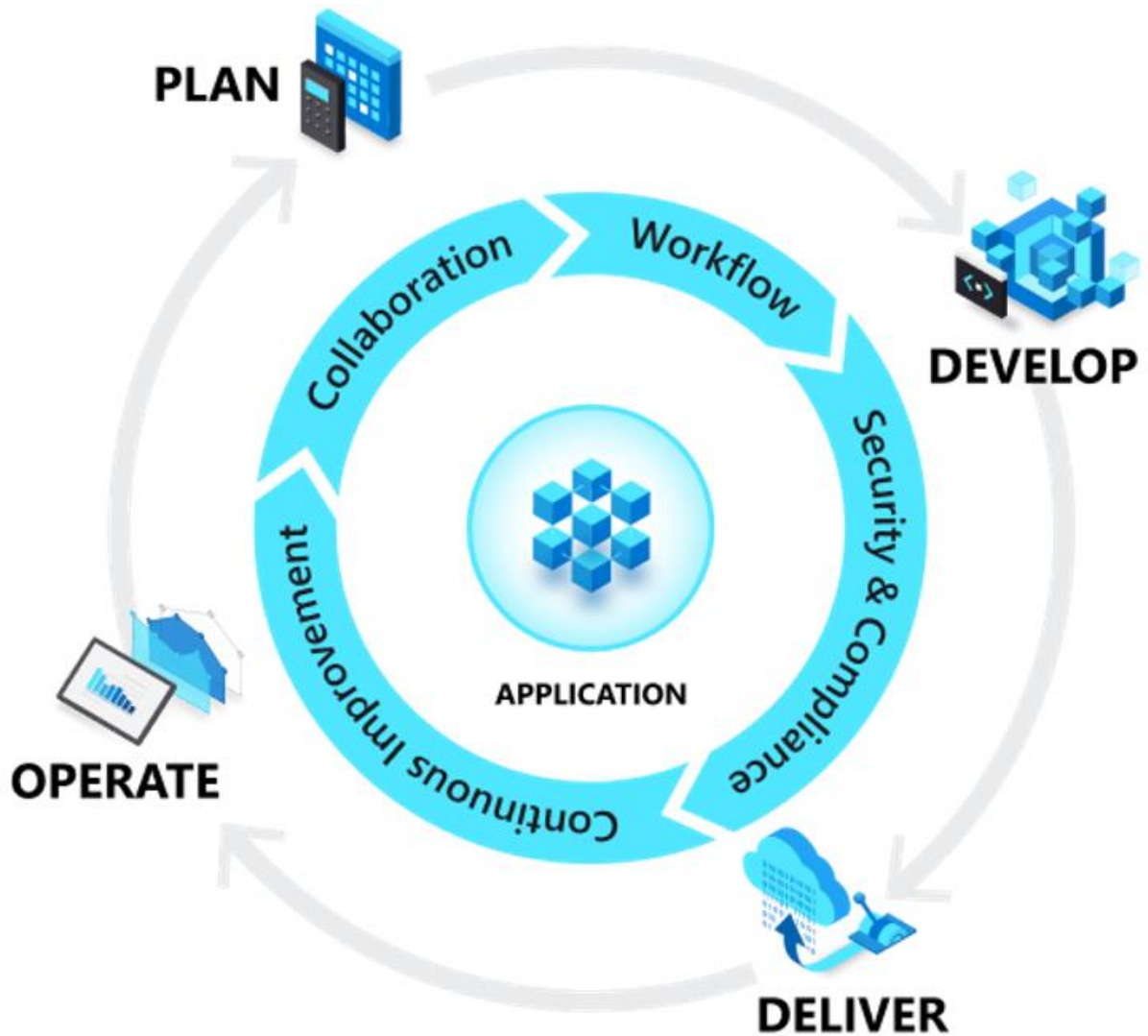




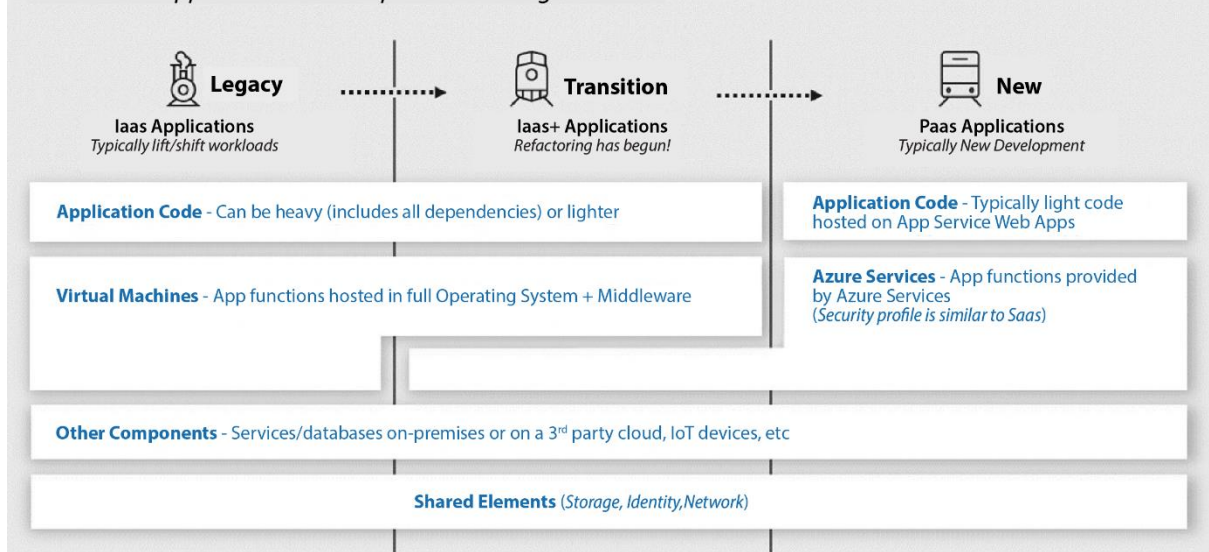
## Chapter 9: Specifying Security Requirements for Applications







### Standalone Applications or Components of Larger Solutions

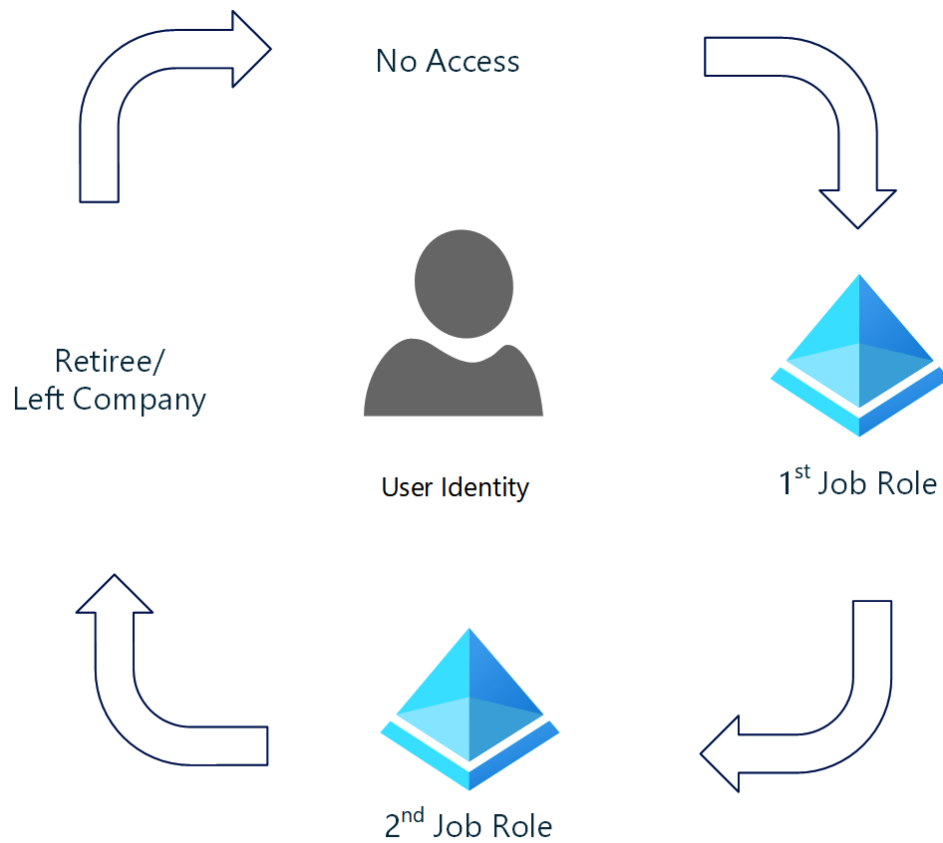


## Chapter 10: Designing a Strategy for Securing Data

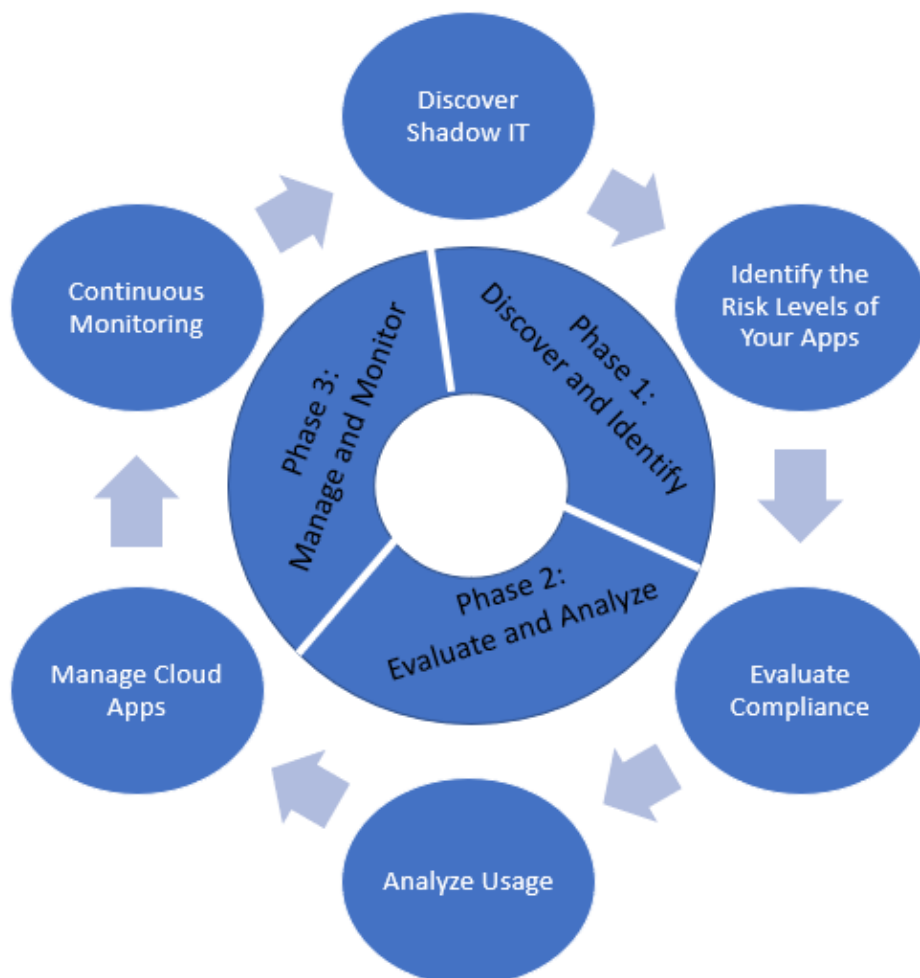
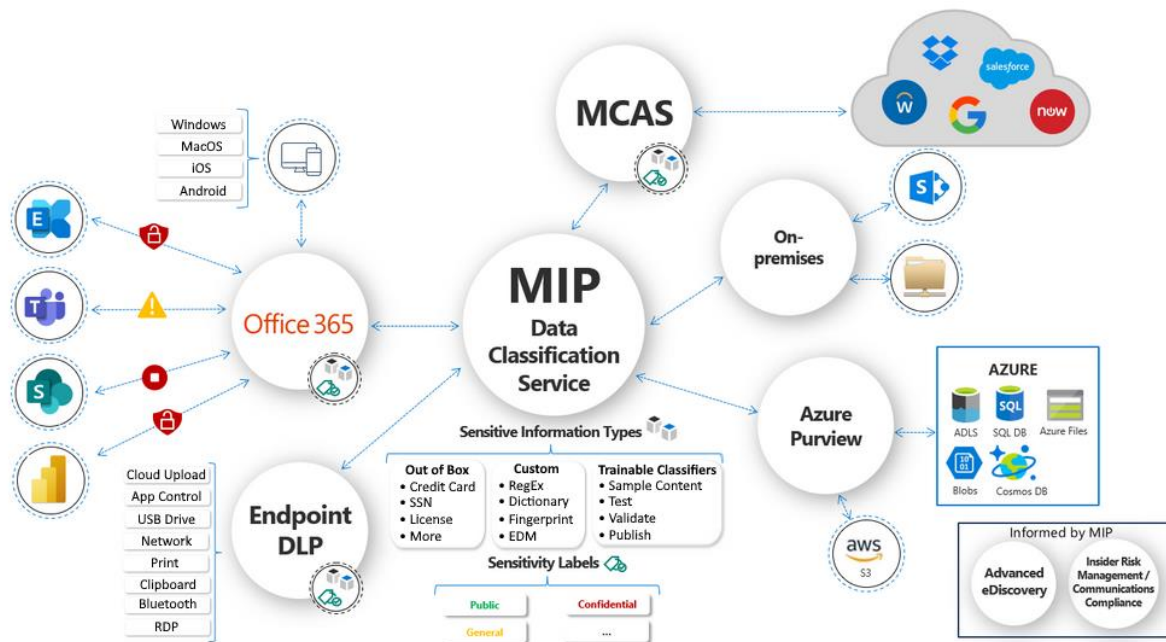


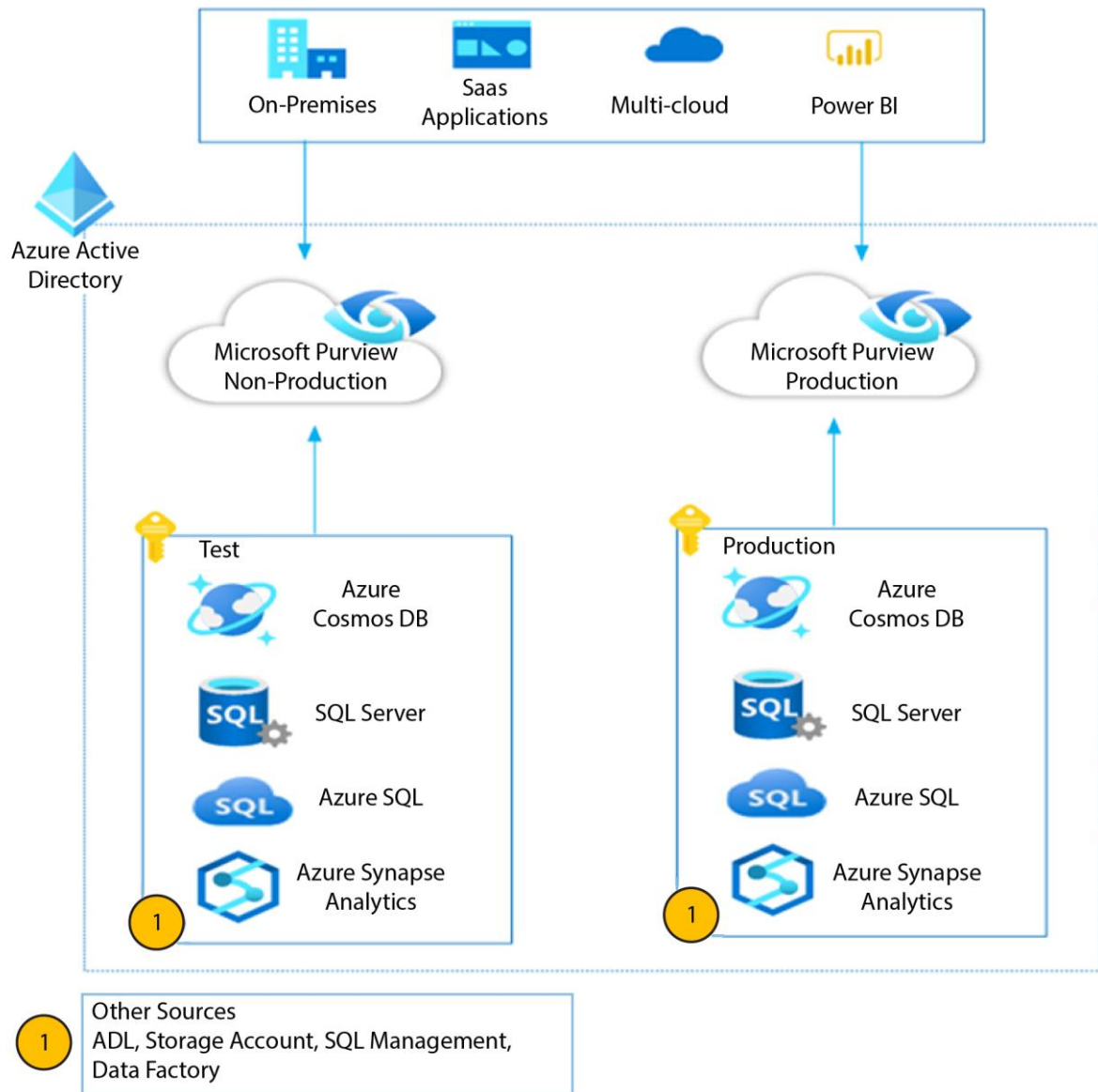
|   |   |                             |                             |                                |
|---|---|-----------------------------|-----------------------------|--------------------------------|
| Likelihood<br>↑                         | Very Likely                                   | Acceptable risk<br>Medium 2 | Unacceptable risk<br>High 3 | Unacceptable risk<br>Extreme 5 |
|   | Likely  | Acceptable risk<br>Low 1    | Acceptable risk<br>Medium 2 | Unacceptable risk<br>High 3    |
|   | Unlikely                                      | Acceptable risk<br>Low 1    | Acceptable risk<br>Low 1    | Acceptable risk<br>Medium 2    |
|   | What is the chance<br>that it will<br>happen? | Minor                       | Moderate                    | Major                          |
| Impact<br>→<br>How serious is the risk? |   |                             |                             |                                |

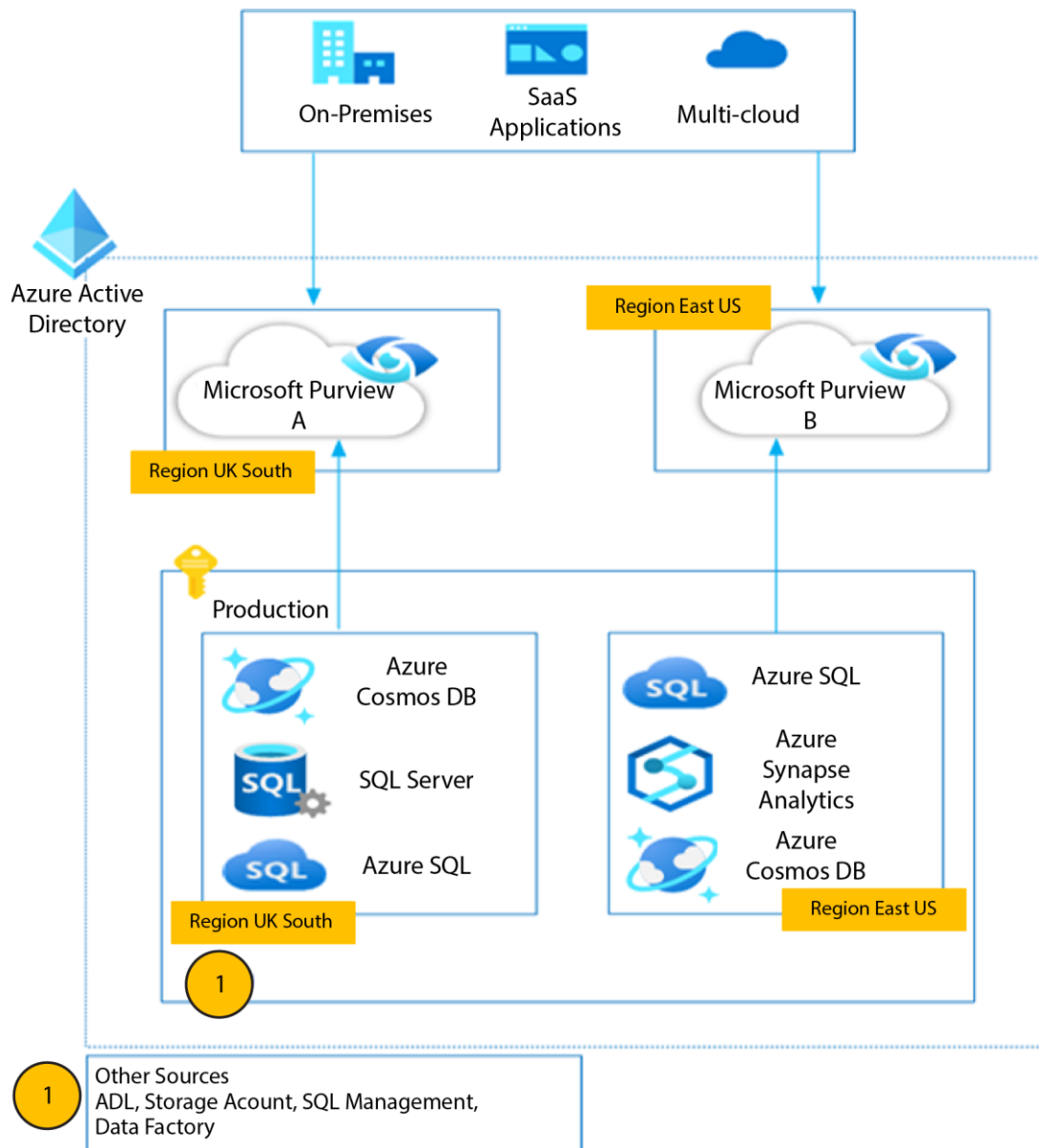


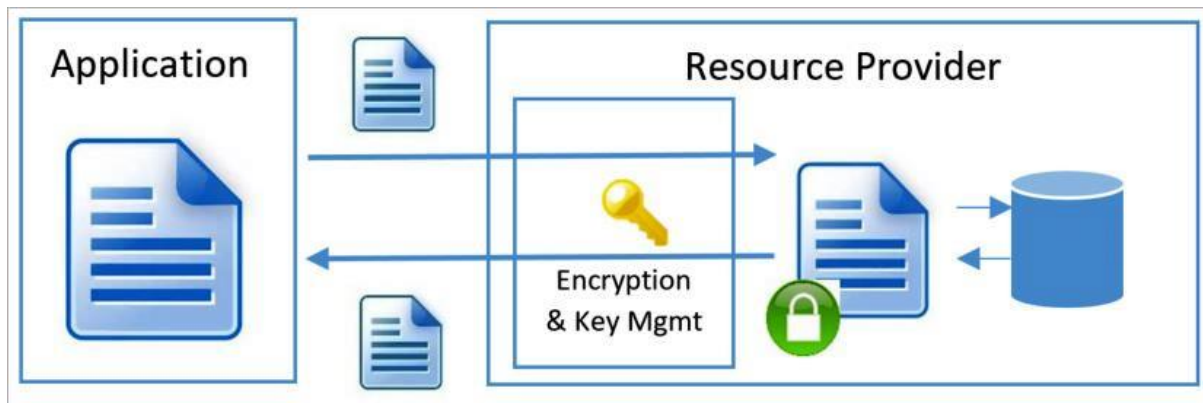












## az900ondemand

Storage account



Data migration



Events



Storage browser (preview)

### Data storage



Containers



File shares



Queues



Tables

### Security + networking



Networking



Azure CDN



Access keys



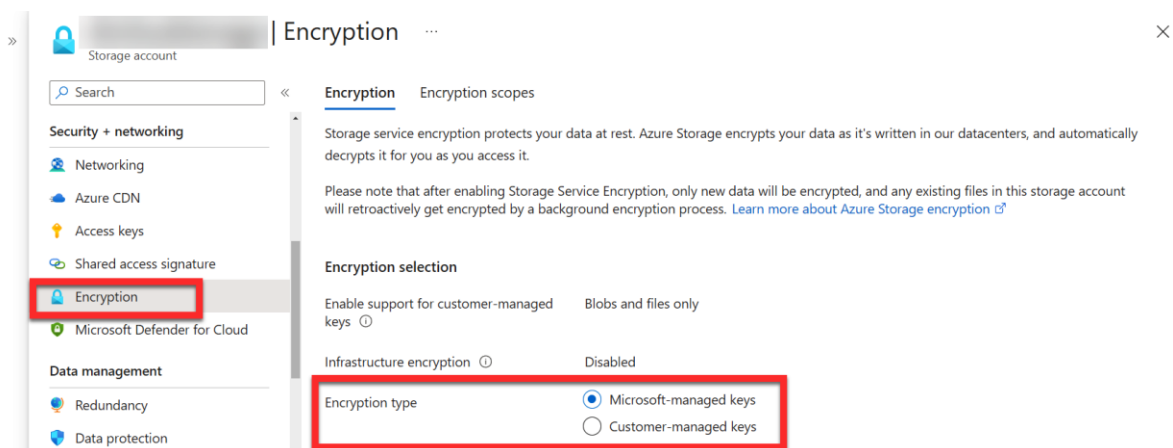
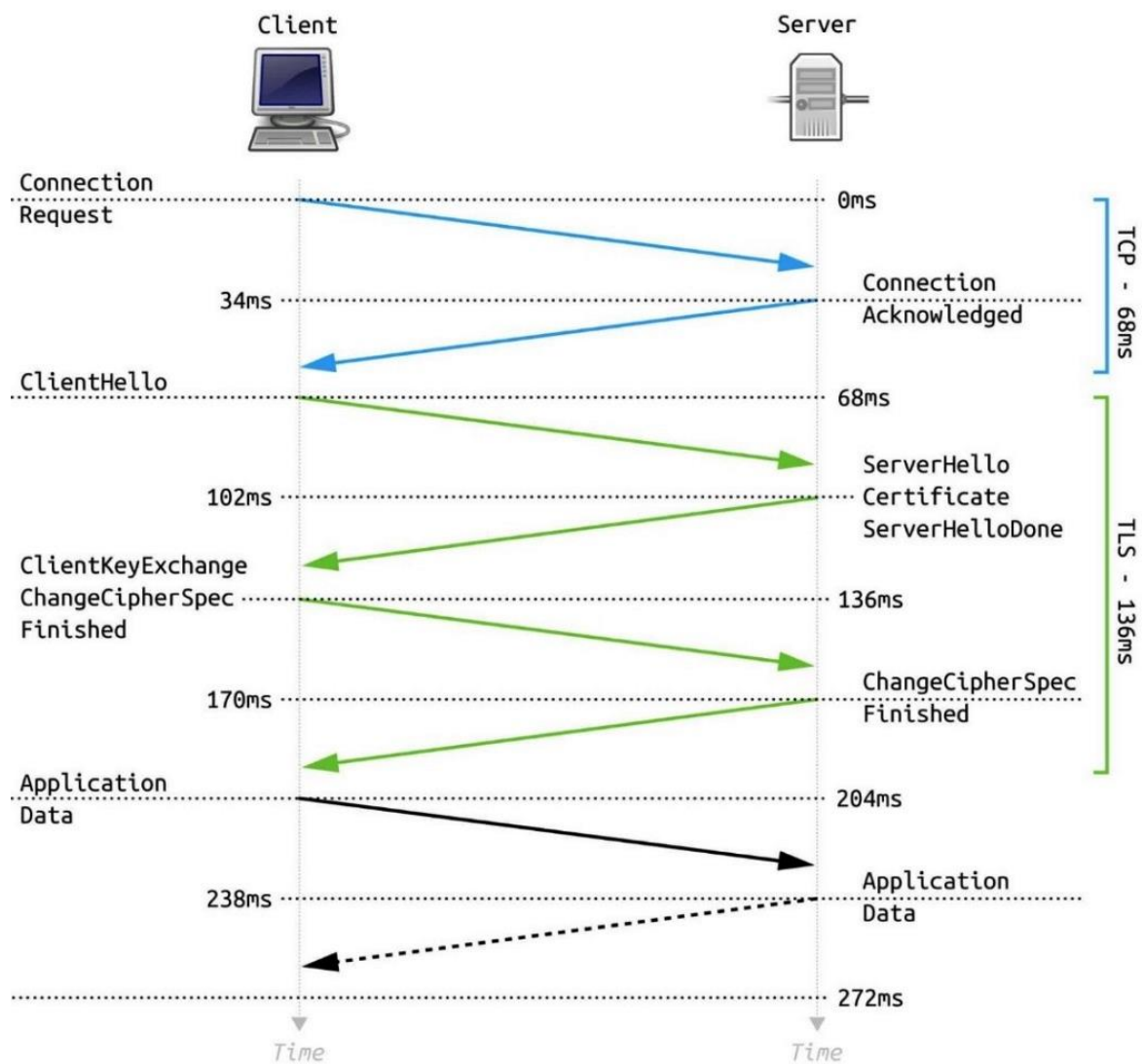
Shared access signature



Encryption



Security



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

*No images...*

## Appendix: Preparing for Your Microsoft Exam

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

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



### Sign in

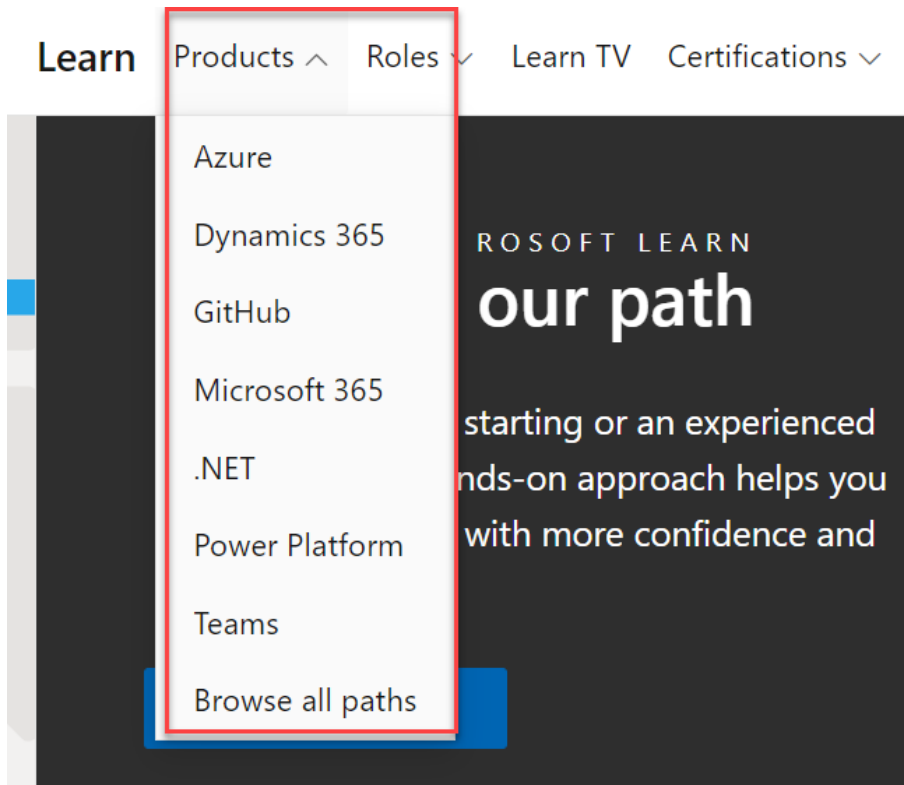
Email, phone, or Skype

No account? [Create one!](#)

[Can't access your account?](#)

Back

Next



Microsoft

Learn

Documentation

Training

Certifications

Q&A

Code Samples

Shows

Events

Search

Sign in

Training

Products

Roles

Learning Paths

Courses

Educator Center

Student Hub

FAQ & Help

Browse all learning paths and modules

Learn new skills and discover the power of Microsoft products with step-by-step guidance. Start your journey today by exploring our learning paths and modules.

Filter

Types

☐ Learning Path

☐ Module

Levels

☐ Advanced

☐ Beginner

☐ Intermediate

Subjects

Find a subject

☒ Business applications

☐ Data and AI

☐ Digital and application innovation

☐ Infrastructure

☐ Modern life

☐ Modern work

☐ Search, ads, and news

☐ Security

Search

Search

4,314 results

MODULE

Describe cloud service types

12 min

★★★★★ 4.8 (23K)

Azure • Administrator • Beginner

Save

MODULE

Describe the benefits of using cloud services

17 min

★★★★★ 4.8 (23K)

Azure • Administrator • Beginner

Save

MODULE

Describe cloud computing

23 min

★★★★★ 4.8 (30K)

Azure • Administrator • Beginner

Save

LEARNING PATH

Microsoft Azure Fundamentals: Describe cloud concepts

52 min

Azure • Administrator • Beginner

Save

MODULE

Describe the core architectural components of Azure

48 min

★★★★★ 4.8 (9.1K)

Azure • Administrator • Beginner

Save

MODULE

Describe Azure compute and networking services

1 hr 8 min

★★★★★ 4.6 (7.6K)

Azure • Administrator • Beginner

Save

MODULE

Describe Azure identity, access, and security

Save

MODULE

Get started building with Power BI

Save

MODULE

Describe Azure storage services

Save



# Browse Certifications and Exams

Learn new skills to boost your productivity and enable your organization to accomplish more with Microsoft Certifications.

## Filter

### Products


- ☐ Azure
- ☐ Microsoft 365

### Roles

- ☐ Administrator
- ☐ Security Engineer
- ☐ Security Operations Analyst
- ☐ Solution Architect

[Search](#)

2 results for "sc-100"




EXAM

**Exam SC-100: Microsoft Cybersecurity Architect (beta)**

Azure Administrator Advanced

[Save](#)



CERTIFICATION

**Microsoft Certified: Cybersecurity Architect Expert**

ExamSC-100

Azure Administrator Intermediate

[Save](#)

[Learn](#) / [Certifications](#) / [Browse Certifications](#) /



EXAMS

## Exam SC-100: Microsoft Cybersecurity Architect

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

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

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

### Exam SC-100: Microsoft Cybersecurity Architect

United States 

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

**Retirement date:** none

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

[Schedule exam](#) >

**\$165 USD\***

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

[Official practice test](#) for Microsoft Cybersecurity Architect

All objectives of the exam are covered in depth so you'll be ready for any question on the exam.

## Skills measured

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

# Office 365 E5

All the features of Office 365 E3 plus advanced security, analytics, and voice capabilities<sup>1</sup>.

**\$35.00** user/month  
(annual commitment)

Buy now

Try for free >

Contact sales >

Learn more >



## Office 365 E5 Trial

One month free with payment details

○ About you      ○ Sign-in details      ○ Payment info and finish

### Let's get you started

Enter your work or school email address, we'll check if you need to create a new account for Office 365 E5 Trial.

Email

This is required

Next

### What is Office 365 E5 Trial?

Fully installed Office apps for PC and Mac



Premium services



**\$14.80**  
user/month  
(annual commitment)

## Enterprise Mobility + Security E5

Try now >

Buy E5

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

①

Let's set up your account

Enter your work or school email address, we'll check if you need to create a new account for Enterprise Mobility + Security E5.

Next

②

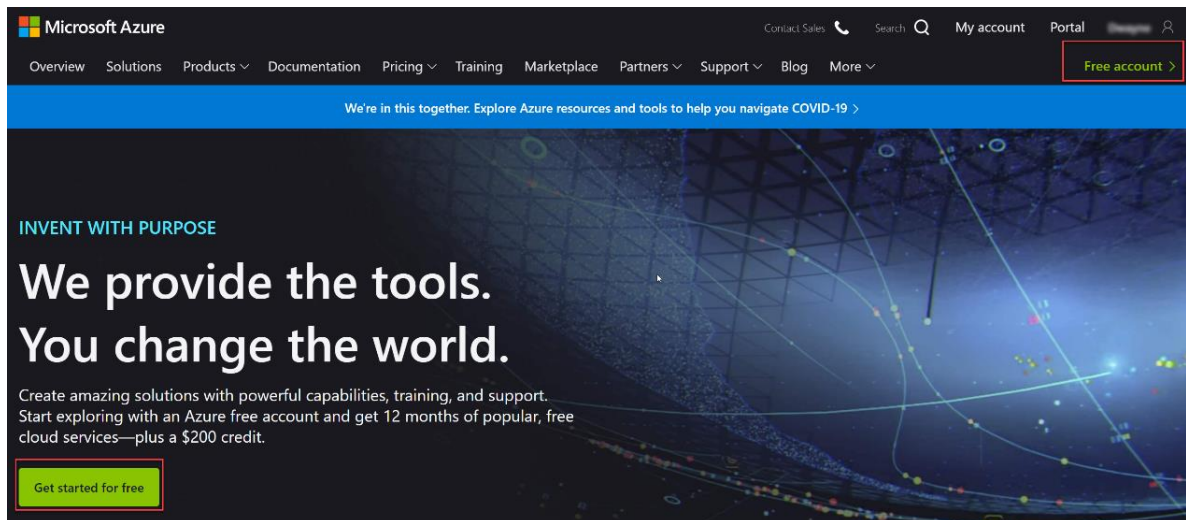
Tell us about yourself

③

Create your business identity

④

You're all set



## Certification details

Complete one prerequisite

