

Microsoft Defender for Endpoint & (ASC) Azure Defender





ASC – Azure Defender

Introduction to Azure Security Center

Azure Security Center's features cover the two broad pillars of cloud security

Cloud Security Posture Management (CSPM)

*Free Experience Features

- Secure Score
- Security Misconfigurations in Azure VM's
- Asset inventory

Cloud Workload Protection (CWP)

Azure Defender enablement brings advanced intelligent & protection of Azure + Hybrid resources/workloads

- Additional security features
- Built-in policies & Custom policies
- Regulatory standards - such as NIST and Azure CIS (Azure Security Benchmark)





ASC – Azure Defender

Introduction to Azure Security Center

Azure Security Center's features cover the two broad pillars of cloud security

Cloud Security Posture Management (CSPM)

Cloud Workload Protection (CWP)

| Azure Defender off | Azure Defender on |
|--|--|
| ✓ Continuous assessment and security recommendations | ✓ Continuous assessment and security recommendations |
| ✓ Azure Secure Score | ✓ Azure Secure Score |
| ✗ Just in time VM Access | ✓ Just in time VM Access |
| ✗ Adaptive application controls and network hardening | ✓ Adaptive application controls and network hardening |
| ✗ Regulatory compliance dashboard and reports | ✓ Regulatory compliance dashboard and reports |
| ✗ Threat protection for Azure VMs and non-Azure servers (including Server EDR) | ✓ Threat protection for Azure VMs and non-Azure servers (including Server EDR) |
| ✗ Threat protection for supported PaaS services | ✓ Threat protection for supported PaaS services |

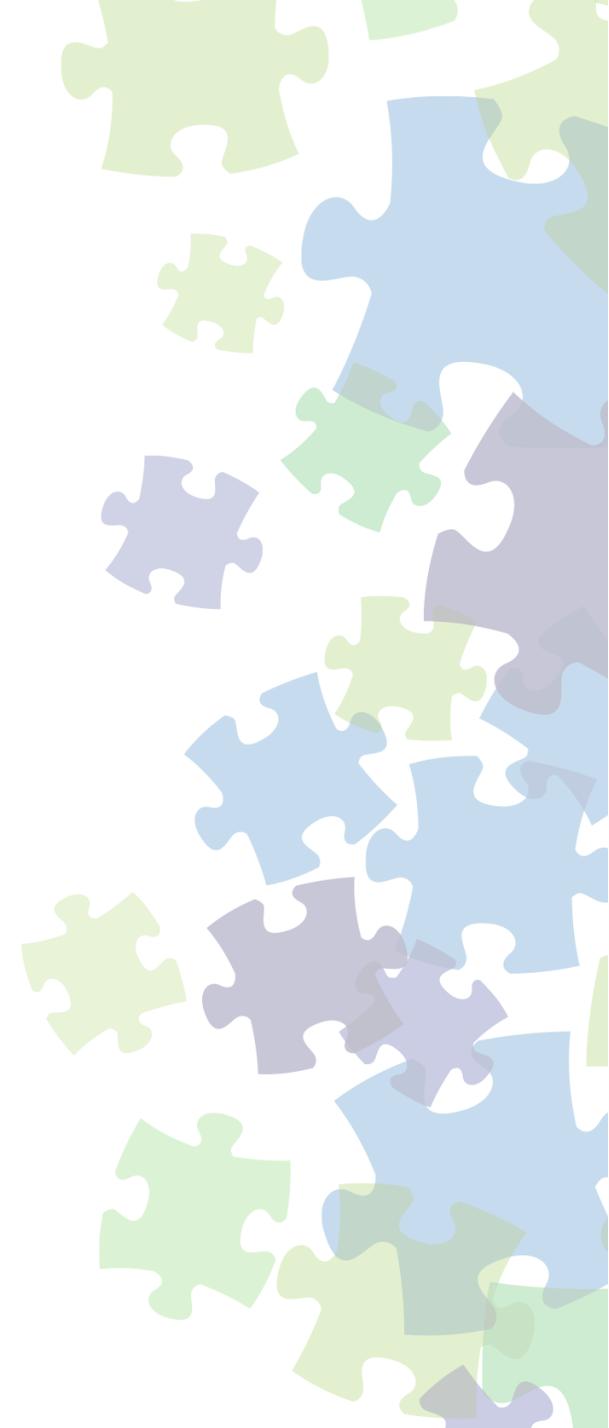


Azure Security Center

Azure Security Center Tiers

- **Azure Security Center Free Tier (OFF)**
- **Azure Defender (ON)**

| FEATURES | AZURE SECURITY CENTER FREE TIER | AZURE DEFENDER |
|---|---------------------------------|----------------|
| Continuous assessment and security recommendations | ✓ | ✓ |
| Azure secure score | ✓ | ✓ |
| Just in time VM Access | -- | ✓ |
| Adaptive application controls and network hardening | -- | ✓ |
| Regulatory compliance dashboard and reports | -- | ✓ |
| Threat protection for Azure VMs and non-Azure servers (including Server EDR) | -- | ✓ |
| Threat protection for PaaS services | -- | ✓ |
| Microsoft Defender for Endpoint (servers) | -- | ✓ |





ASC – Azure Defender

Supported Platforms

ASC – Azure Defender supports virtual machines & servers on different types of hybrid environments:

- Only Azure
- Azure and on-premises
- Azure and other clouds
- Azure, other clouds, and on-premises

NOTE: For an Azure environment activated on an Azure subscription, Azure Security Center will automatically discover IaaS resources that are deployed within the subscription





ASC – Azure Defender

Supported Operating Systems (Windows)

| Operations system | Azure Monitor agent | Log Analytics agent | Dependency agent | Diagnostics extension |
|---|---------------------|---------------------|------------------|-----------------------|
| Windows Server 2019 | X | X | X | X |
| Windows Server 2016 | X | X | X | X |
| Windows Server 2016 Core | | | | X |
| Windows Server 2012 R2 | X | X | X | X |
| Windows Server 2012 | X | X | X | X |
| Windows Server 2008 R2 | | X | X | X |
| Windows 10 Enterprise (including multi-session) and Pro (Server scenarios only) | X | X | X | X |
| Windows 8 Enterprise and Pro (Server scenarios only) | | X | X | |
| Windows 7 SP1 (Server scenarios only) | | X | X | |

ASC – Azure Defender

Security Alerts



The alerts shown in customer's environment depend on the resources and services protected, as well as customized configuration

Types of Security Alerts

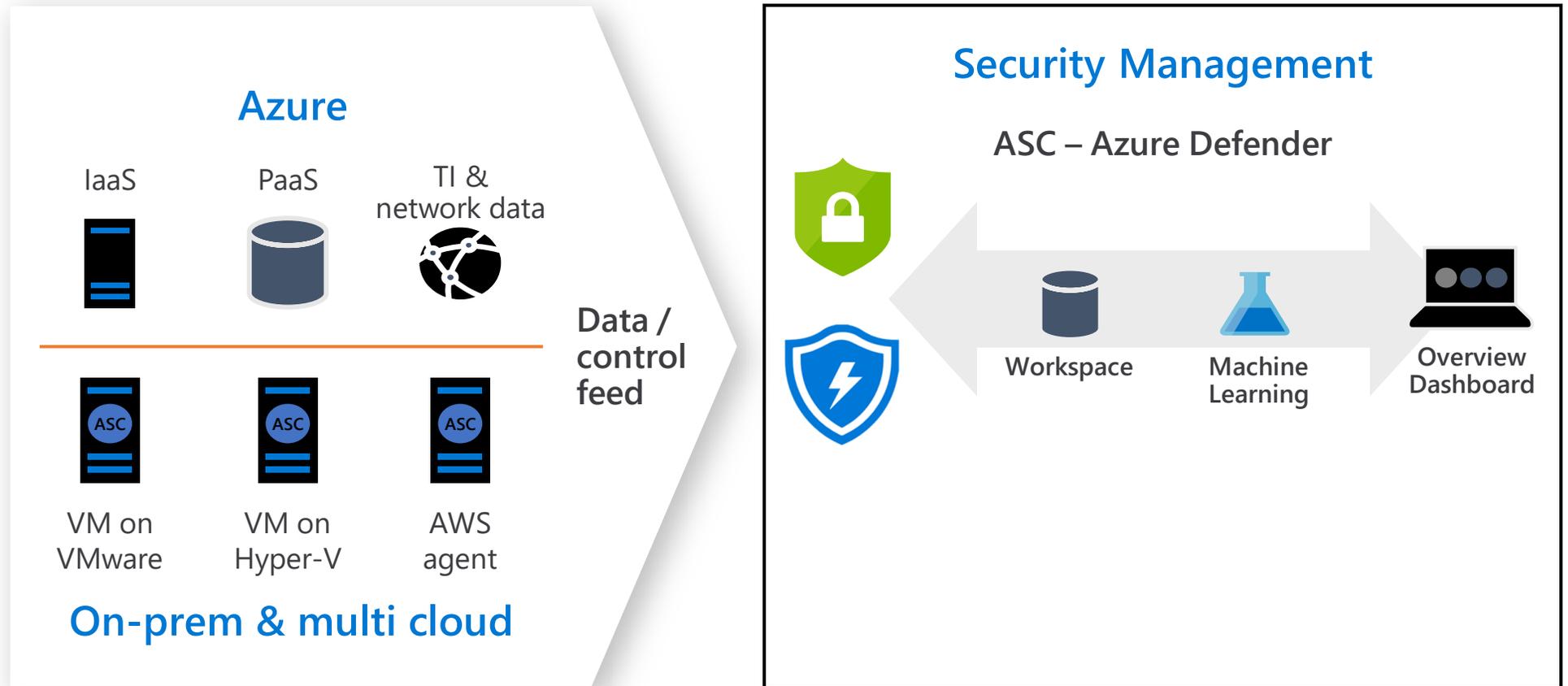
- Alerts for Windows machines
- Alerts for Linux machines
- Alerts for Azure App Service
- Alerts for containers - Azure Kubernetes Service clusters
- Alerts for containers - host level
- Alerts for SQL Database and Azure Synapse Analytics
- Alerts for Azure Storage
- Alerts for Azure Cosmos DB (Preview)
- Alerts for Azure network layer
- Alerts for Azure Resource Manager (Preview)
- Alerts for Azure Key Vault
- Alerts for Azure DDoS Protection
- Security incident alerts

*Full List of Alerts can be found [HERE](#)

Defender for Endpoint & ASC



High-Level Architecture





ASC – Azure Defender

Azure Defender - Overview

Hybrid cloud protection

- Protects non-Azure Servers
- Protection to AWS & GCP VM's
- SQL databases
 - (Other clouds or on-premises with [Azure Arc](#))

Azure Defender Alerts & Insights

- Affected Resources
- Suggested Remediation Steps
- Trigger a logic App in Response

Advanced Protection Capabilities

- Just-in-time access
- Adaptive application control

Vulnerability Assessment & Management

- Vulnerability scanning
 - VM's
 - Container Registries

Security Center alerts can be exported

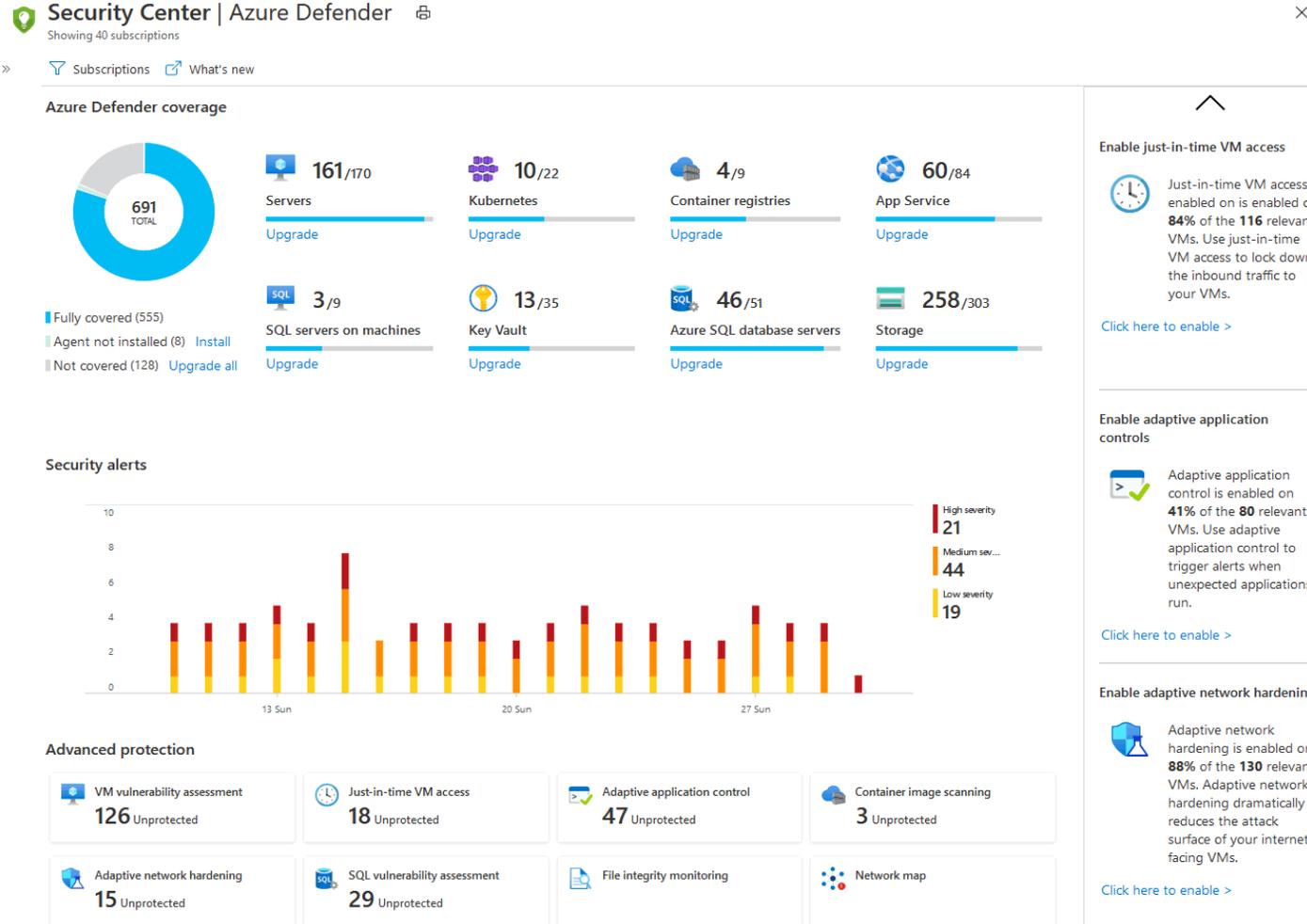
- Azure Sentinel
- Any third-party SIEM
- External tool



ASC – Azure Defender

Azure Defender Dashboard

Cloud Workload Protection (CWP)





ASC – Azure Defender

Azure Defender Workloads

- **Azure Defender for Servers**
- Azure Defender for App Service
- Azure Defender for Storage
- Azure Defender for SQL
- Azure Defender for Kubernetes
- Azure Defender for container registries
- Azure Defender for Key Vault

Resource Types

- Virtual machines
- SQL databases
- Containers
- Web applications
- Network



Azure Defender for Servers

Introduction Azure Defender for Servers

Threat detection & advanced defenses for Windows and Linux machines – presented as alerts and remediation suggestions

Azure Defender For Servers Capabilities

- **Integrated license for Microsoft Defender for Endpoint (Windows only)**
- Vulnerability assessment scanning for VMs
- Just-in-time (JIT) virtual machine (VM) access
- File integrity monitoring (FIM)
- Adaptive application controls (AAC)
- Adaptive network hardening (ANH)
- Docker host hardening
- Fileless attack detection (Windows only)
- Linux auditd alerts and Log Analytics agent integration (Linux only)



Azure Defender for Servers

Integrated License for Microsoft Defender for Endpoint (Windows only)

Main Features

- Risk-based vulnerability management and assessment
- Attack surface reduction
- Behavioral based and cloud-powered protection
- Endpoint detection and response (EDR)
- Automatic investigation and remediation
- Managed hunting services



Azure Defender for Servers

Integrated License for Microsoft Defender for Endpoint (Windows only)

Availability

| Aspect | Details |
|--------------------------------|---|
| Release state | Generally available (GA) |
| Pricing | Requires Azure Defender for servers |
| Supported platforms: | Azure machines running Windows Azure Arc machines running Windows |
| Supported versions of Windows: | Defender for Endpoint is built into Windows 10 1703 (and newer) and Windows Server 2019 Security Center supports detection on Windows Server 2016, 2012 R2, and 2008 R2 SP1. |



Azure Defender for Servers

Integrated License for Microsoft Defender for Endpoint (Windows only) (Cont.)

Availability

| Aspect | Details |
|--------------------------------|--|
| Required roles and permissions | To enable/disable the integration: Security admin or Owner To view MDATP alerts in Security Center: Security reader, Reader, Resource Group Contributor, Resource Group Owner, Security admin, Subscription owner, or Subscription Contributor |
| Clouds | Commercial Clouds US Gov |



Azure Defender for Servers

Microsoft Defender for Endpoint features in Security Center

- Advanced post-breach detection sensors
- Analytics-based, cloud-powered, post-breach detection
- Threat intelligence
- Automated onboarding
- Single pane of glass

Microsoft Defender Security Center Machine Search Microsoft Defender ATP

Threat & Vulnerability Management dashboard

Organization exposure score

Exposure score
This score reflects the current exposure associated with machines in your organization

36/100

Low 0-29 Medium 30-69 High 70-100

Organization configuration score

Configuration score: 292 / 578

This score reflects the collective security configuration posture of your machines across OS, Application, Network, Accounts and Security Controls

| Category | Score |
|-------------------|-----------|
| Application | 13 / 63 |
| OS | 45 / 175 |
| Network | 32 / 62 |
| Accounts | 7 / 12 |
| Security controls | 195 / 266 |

Machine exposure distribution

Exposure distribution

Exposed machines are easy targets for cybersecurity attacks. Ensure that these machines can receive security updates, have critical security controls, and are properly configured.

2 Total

Low Medium High

Top security recommendations 4/51
Based on highest organizational exposure impact

- Update Chrome**
2 Exposed machines
25.20 Software patch
- Update Windows 10**
1 Exposed machines
24.00 Software patch
- Turn on PUA protection**
2 Exposed machines
3.00 | + 9.00 Configuration change
- Turn on Attack Surface Reduction rules**
2 Exposed machines
3.00 | + 9.00 Configuration change

Show more Show exceptions

Exposure score over time 36 Last 30 days

Configuration score over time 12 Last 30 days



Azure Defender for Servers

Enabling the Microsoft Defender for Endpoint integration

1. Enable **Azure Defender for servers**
2. From Security Center's menu, select **Pricing & settings**
3. Select **Threat detection**
4. Select **Allow Microsoft Defender for Endpoint to access my data** Save

Settings | Threat detection 
Contoso Hotels

Search (Ctrl+/) <<  Save

Settings

-  Azure Defender plans
-  Data Collection
-  Email notifications
-  **Threat detection**
-  Workflow automation
-  Continuous export
-  Cloud connectors (Preview)

Enable integrations

To enable Security Center to integrate with other Microsoft security services, allow those services to access your data.

- Allow Microsoft Cloud App Security to access my data. [Learn more >](#)
- Allow Microsoft Defender for Endpoint to access my data. [Learn more >](#)**



Azure Defender for Servers

Microsoft Defender Security Center

Microsoft Defender Security Center

Device | Search Microsoft Defender ATP

Security operations

Microsoft Threat Protection

Experience Microsoft Threat Protection

Unify your security operations through a single pane of glass across Office 365 ATP, Microsoft Defender ATP, Azure ATP, and Microsoft Cloud App Security. Get incident management, automated investigations, and advanced hunting on Office 365, your endpoints, and your identities.

Available in the Microsoft 365 security center with a Microsoft 365 E5 or equivalent license. [Learn more.](#)

[Try it now](#)

[Hide this card](#)

Active alerts

| Severity | Count |
|---------------|-------|
| High | 98 |
| Medium | 1.79k |
| Low | 4.33k |
| Informational | 5.26k |

6.21k New

4 In progress

MicrosoftDefenderATP | Medium | 4/10/20, 8:20 PM

Active automated investigations

30 days

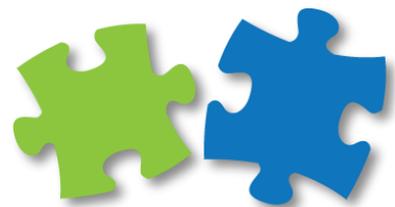
| Status | Count |
|--------------------|-------|
| Pending action | 0 |
| Waiting for device | 1.68k |
| Running | 122 |

1.81k Active

Automated investigations statistics

7 days

| | | |
|------------------------------|-----------------------------|-------------------------|
| 333 Automated investigations | 2d ↑ Average pending time | 384 Alerts investigated |
| 0 Remediated investigations | 0 Average time to remediate | 4.1625 Hours automated |



SYNERGY

ADVISORS