Microsoft Security

Steve Scholz
Security Solution Specialist
Steve.scholz@microsoft.com
https://aka.ms/meetwithme

# Industry-leading security from Microsoft

Monitoring

**140+**[3]

Threat groups

**40+**[3]

Nation state-groups

Serving billions of global customers, learning and predicting what's next

**43T**[1]

Analyzing

Threat signals daily

**32B**[1]

Blocking

email threats annually

**$20B**[1]

in the next 5 years

Investing to improve **and share** knowledge, gain insights, and combat cybercrime

Keeping you secure, while saving you time and resources

**60%**

Up to **savings**, on average, over multi-vendor security solutions

**15K**[1]

partners in security ecosystem

**785K**[2]

customers rely on Microsoft for their multicloud, multiplatform infrastructure security

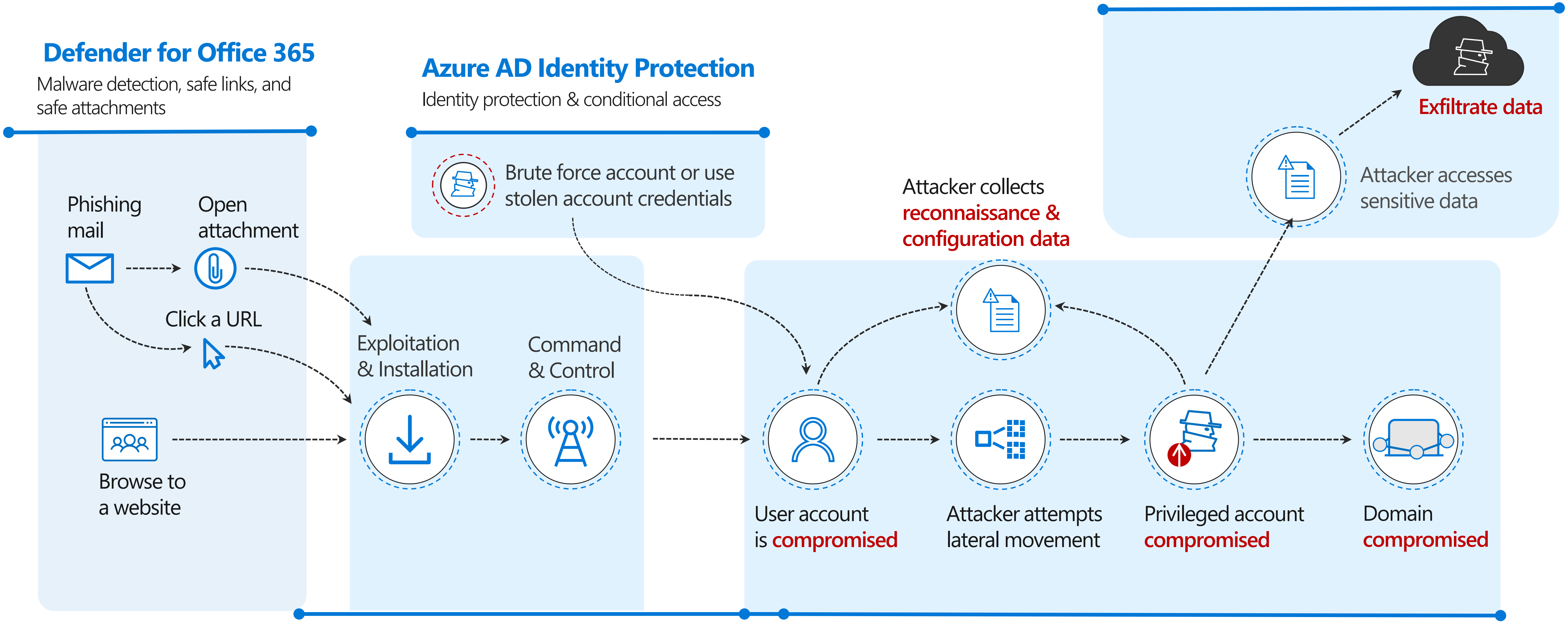
Trusted globally, protecting organizations' multi-Cloud and multi-platform infrastructures

[1] Earnings Press Release, FY22 Q4. July 26, 2022, Microsoft Investor Relations

[2] "Microsoft Digital Defense Report". October 2021, Microsoft Security

[3] Earnings Press Release, FY22 Q2. December 16, 2021,  Microsoft Investor Relations

# Microsoft 365 Defender –End User



## Defender for Cloud Apps

Extends protection & conditional access to other cloud apps

## Defender for Office 365

Malware detection, safe links, and safe attachments

## Azure AD Identity Protection

Identity protection & conditional access

Phishing mail

Open attachment

Click a URL

Browse to a website

Brute force account or use stolen account credentials

Exploitation & Installation

Command & Control

Attacker collects reconnaissance & configuration data

User account is compromised

Attacker attempts lateral movement

Privileged account compromised

Domain compromised

Attacker accesses sensitive data

Exfiltrate data

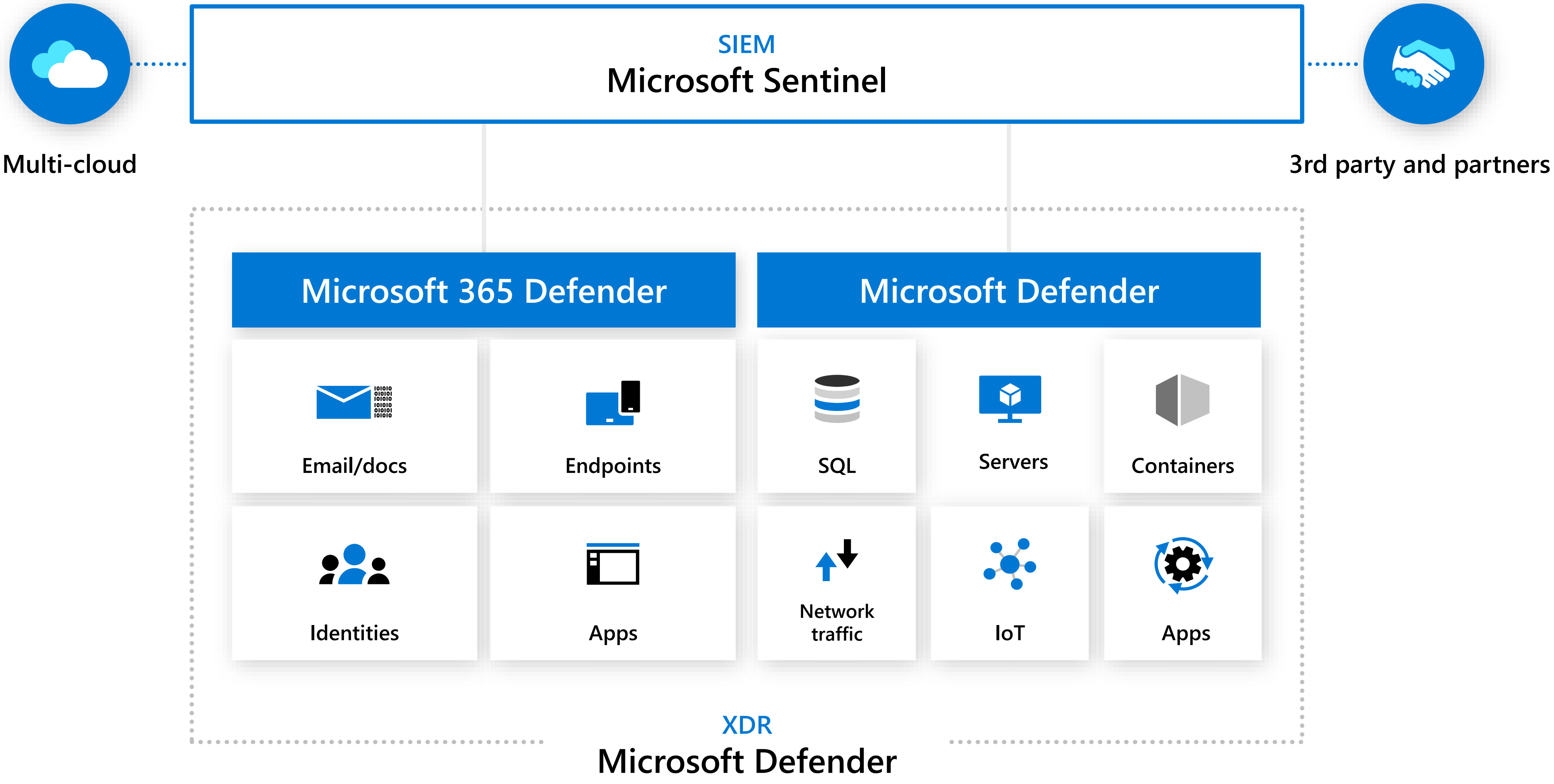
## Defender for Endpoint

Endpoint Detection and Response (EDR)
End-point Protection (EPP)
Threat & Vulnerability Management
Web Content Filtering

## Defender for Identity

Identity protection

# Integrated threat protection for your enterprise



Multi-cloud

SIEM
Microsoft Sentinel

3rd party and partners

Microsoft 365 Defender

Email/docs

Endpoints

Identities

Apps

Microsoft Defender

SQL

Servers

Containers

Network traffic

IoT

Apps

XDR
Microsoft Defender

©Microsoft Corporation
Azure

# Microsoft 365- End User Protection

Feature Matrix

## Microsoft 365 A3

**Productivity Solutions**

- Microsoft 365 Apps for Enterprise
- Teams Live Events
- Bookings
- Windows Virtual Desktop in Azure

+

**Security Solutions**

- Azure Active Directory Premium P1
- Information Protection P1
- Defender for Endpoint P1
- Cloud App Security for Office 365
- Windows Enterprise/Education

+

**Management Solutions**

- Microsoft Endpoint Management (w/Intune for Education)

+

**Minecraft: Education Edition**

+

**Windows/Productivity CALs**

- All customers get Enterprise CALs

**Productivity Server Licenses**

- Includes Productivity Server Licenses

## Microsoft 365 A5

**All Microsoft 365 A3 Features**

+

**Productivity Solutions**

- *Power BI Pro*
- *My Analytics*
- *Audio Conferencing*
- *Phone System*

+

**Security Solutions**

- *Azure Active Directory Premium P2*
- *Defender for Office 365 P2*
- *Defender for Endpoint P2*
- *Defender for Identity*
- *Defender for Cloud Apps (CASB)*

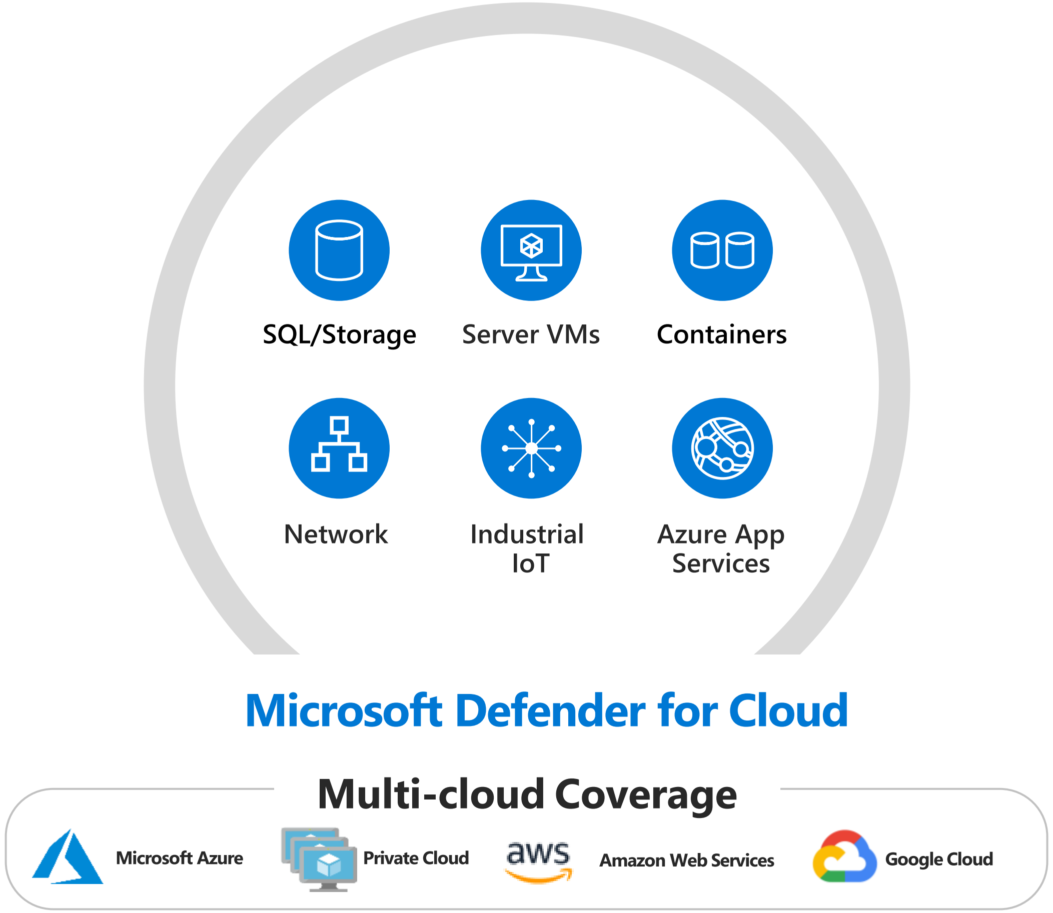
+

**Compliance Solutions**

- *Information Protection and Governance*
- *Insider Risk Management*
- *eDiscovery & Audit*

Microsoft Defender for Cloud

## Secure your critical cloud workloads running in Azure, AWS, Google, and Private Cloud (onprem)



SQL/Storage

Server VMs

Containers

Network

Industrial IoT

Azure App Services

**Microsoft Defender for Cloud**

**Multi-cloud Coverage**

Microsoft Azure

Private Cloud

aws

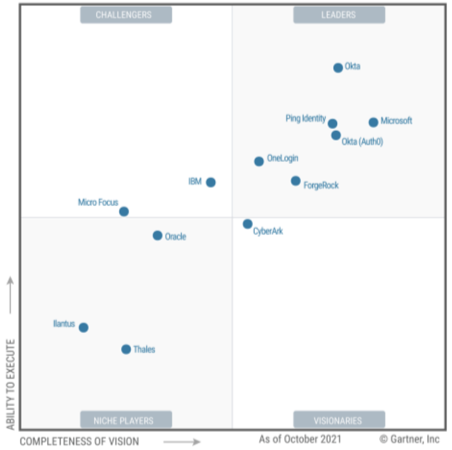
Amazon Web Services

Google Cloud

- Easy onboarding of AWS and GCP accounts and native support for Azure
- Get a bird’s-eye view of your security posture and vulnerabilities across clouds with secure score
- Assess and implement best practices for compliance and security in the cloud
- Protect Amazon EKS clusters and AWS EC2 workloads
- Detect and block advanced malware and threats for Linux and Windows servers running in the cloud or on-premises

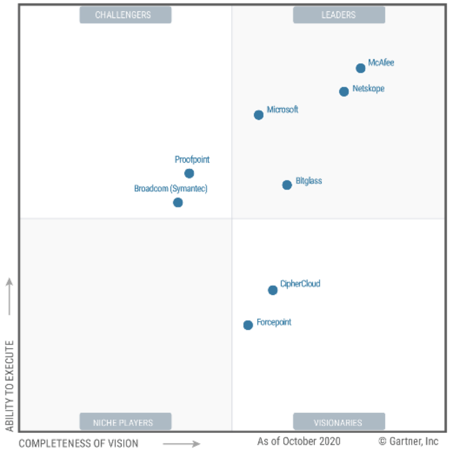
Gartner®

# Microsoft Security: Leader in 6 Gartner Magic Quadrant reports

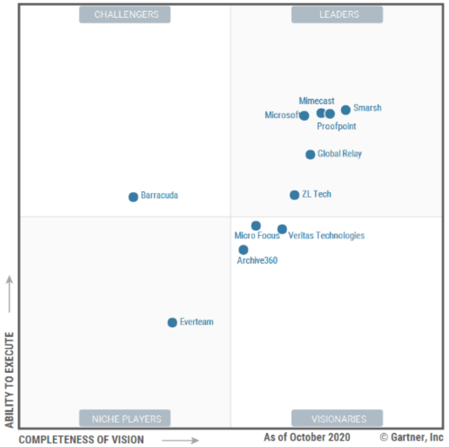


Source: Gartner (November 2021)

Access Management

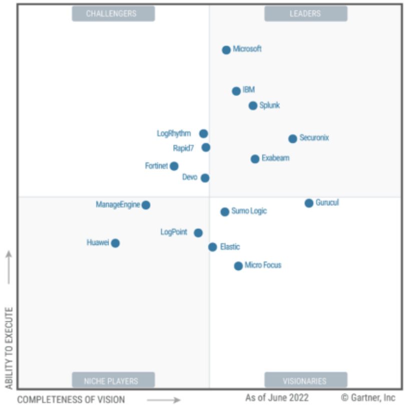


Cloud Access Security Brokers

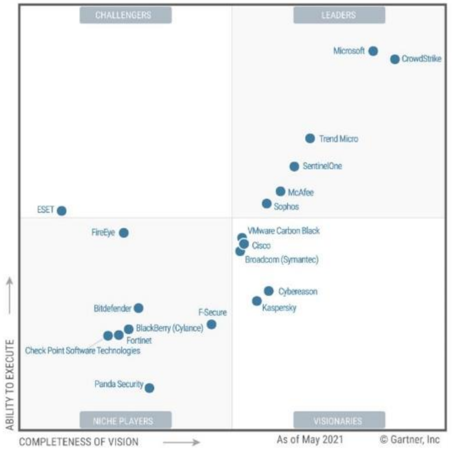


Enterprise Information Archiving

Figure 1: Magic Quadrant for Security Information and Event Management

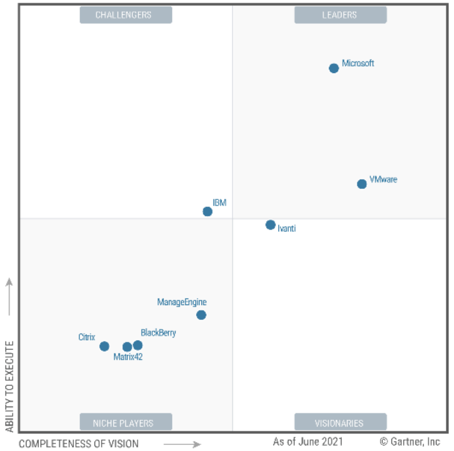


Security Information Event Management



Source: Gartner (May 2021)

Endpoint Protection Platforms



Source: Gartner (August 2021)

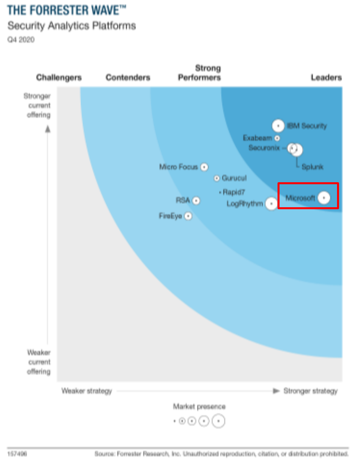
Unified Endpoint Management

*Gartner "Magic Quadrant for Access Management," by Henrique Teixeira, Abhyuday Data, Michael Kelley, November 2021
*Gartner "Magic Quadrant for Cloud Access Security Brokers," by Craig Lawson, Steve Riley, October 2020
*Gartner "Magic Quadrant for Enterprise Information Archiving," by Michael Hoech, Jeff Vogel, October 2020
*Gartner "Magic Quadrant for Endpoint Protection Platforms," by Paul Webber, Rob Smith, Prateek Bhajanka, Mark Harris, Peter Firstbrook, May 2021
*Gartner "Magic Quadrant for Unified Endpoint Management," by Dan Wilson, Chris Silva, Tom Cipolla, August 2021

*These graphics were published by Gartner, Inc. as part of larger research documents and should be evaluated in the context of the entire documents. The Gartner documents are available upon request from Microsoft. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, express or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally, and is used herein with permission. All rights reserved.*

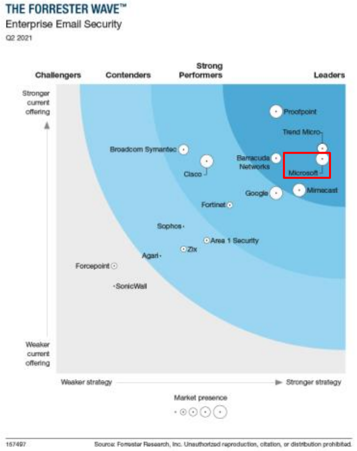
FORRESTER®

# Microsoft Security—a Leader in 7 Forrester Wave reports


THE FORRESTER WAVE™
Security Analytics Platforms
Q4 2020

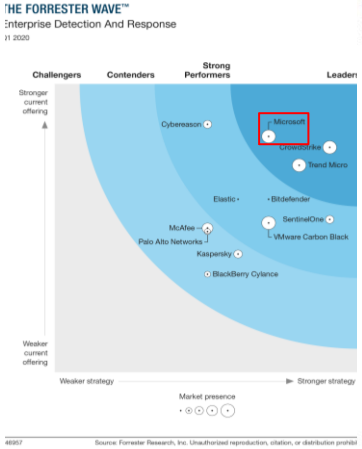
157496 Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

Security Analytics Platform


THE FORRESTER WAVE™
Enterprise Email Security
Q2 2021

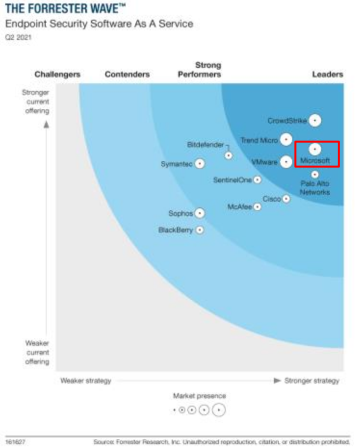
157497 Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

Enterprise Email Security


THE FORRESTER WAVE™
Enterprise Detection And Response
Q1 2020

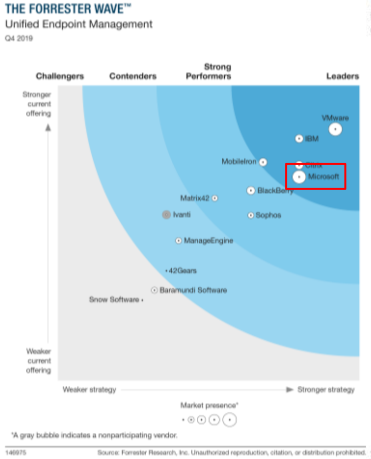
46957 Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

Enterprise Detection & Response


THE FORRESTER WAVE™
Endpoint Security Software As A Service
Q2 2021

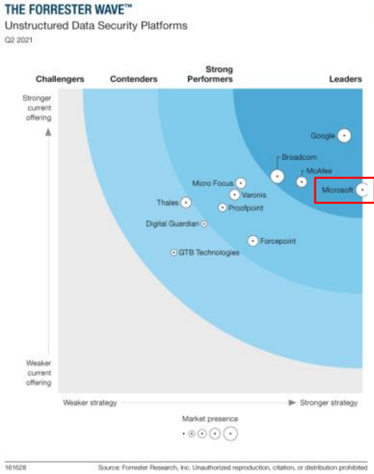
161627 Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

Endpoint Security Software as a Service


THE FORRESTER WAVE™
Unified Endpoint Management
Q4 2019

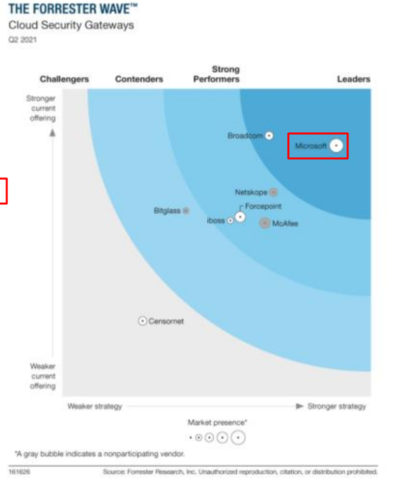
*A gray bubble indicates a nonparticipating vendor.
146975 Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

Unified Endpoint Management


THE FORRESTER WAVE™
Unstructured Data Security Platforms
Q2 2021

161628 Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

Unstructured Data Security Platforms


THE FORRESTER WAVE™
Cloud Security Gateways
Q2 2021

*A gray bubble indicates a nonparticipating vendor.
161626 Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

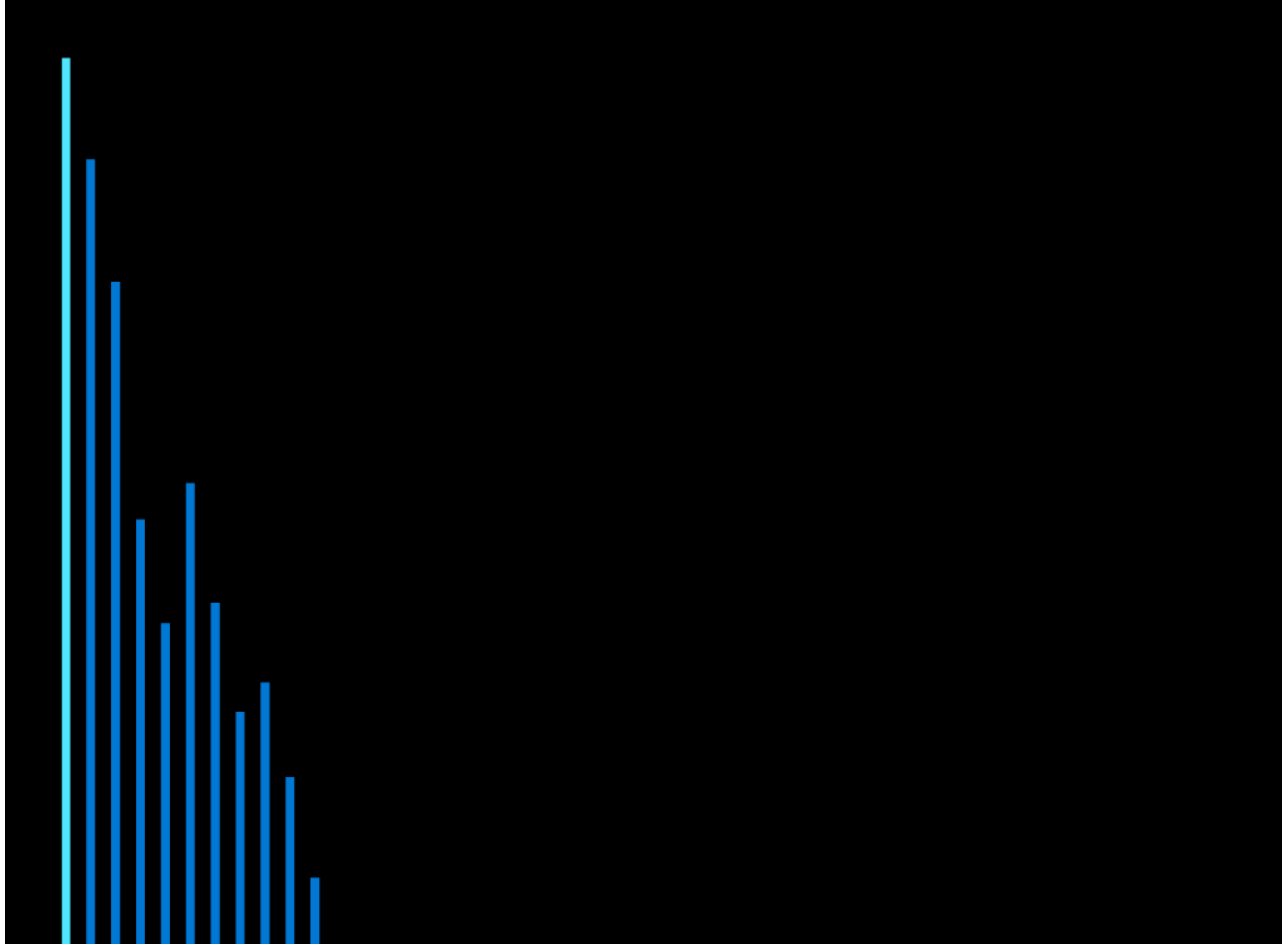
Cloud Security Gateways

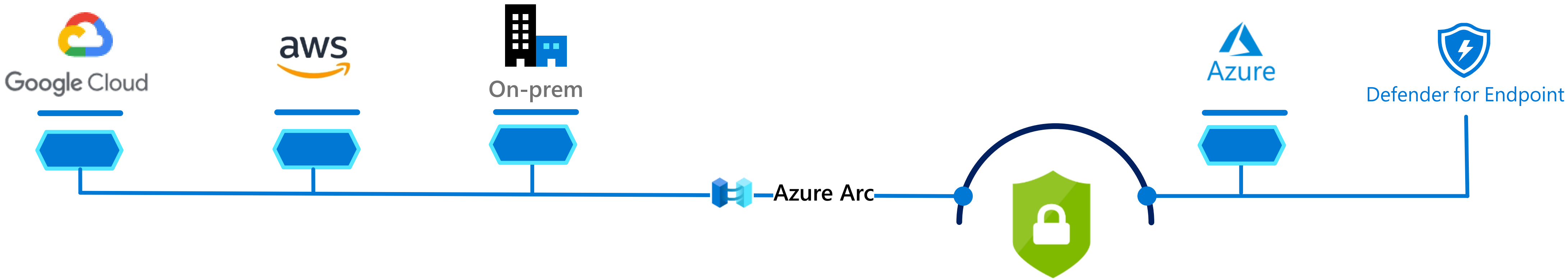
1. The Forrester Wave™: Security Analytics Platforms, Q4 2020, Joseph Blankenship, Claire O'Malley, December 2020
2. The Forrester Wave™: Enterprise Email Security Q2 2021 Joseph Blankenship, Claire O'Malley, April 2021
3. The Forrester Wave™: Enterprise Detection And Response, Q1 2020, Josh Zelonis, March 2020
4. The Forrester Wave™: Endpoint Security Software as a Service, Q2 2021, Chris Sherman, May 2021
5. The Forrester Wave™: Unified Endpoint Management, Q4 2019, Andrew Hewitt, November 2019
6. The Forrester Wave™: Unstructured Data Security Platforms, Q2 2021, Heidi Shey, May 2021
7. The Forrester Wave™: Cloud Security Gateways, Q2 2021, Andras Cser, May 2021

The Forrester Wave™ is copyrighted by Forrester Research, Inc. Forrester and Forrester Wave™ are trademarks of Forrester Research, Inc.
The Forrester Wave™ is a graphical representation of Forrester's call on a market and is plotted using a detailed spreadsheet with exposed scores, weightings, and comments. Forrester does not endorse any vendor, product, or service depicted in the Forrester Wave™.
Information is based on best available resources. Opinions reflect judgment at the time and are subject to change.

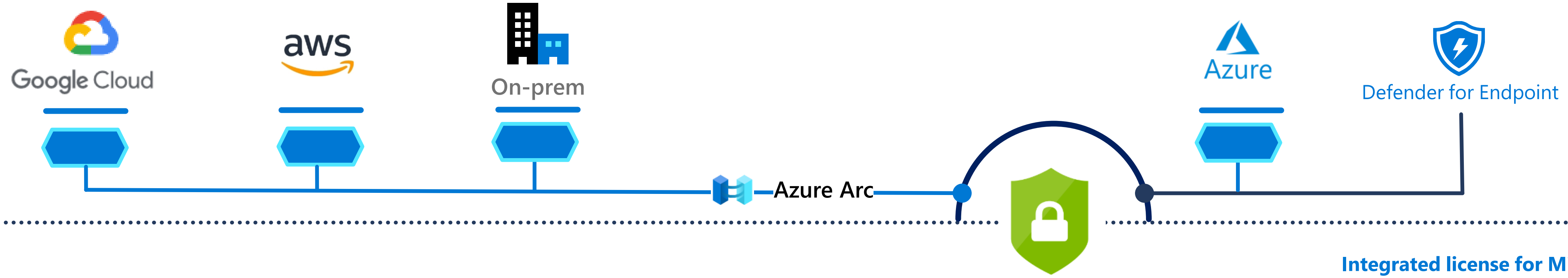
Microsoft Azure

# Defender for Server





# Protect Server Workloads – Key Features



**Integrated license for Microsoft Defender for Endpoint**

| | | | | | |
|---|---|---|---|---|---|
| Server Hygiene | Secure score | Visibility | Regulatory Compliance | Vulnerability Assessment | |
| Advanced Protection | Adaptive Application Control | *Just-in-time VM Access | *Adaptive Network Hardening | File Integrity Monitoring | Docker Host Hardening |
| Detection & Response | Threat Detection (MDE) | *Fileless Attack Detection | Linux auditd ML | Export & Automation | |

Microsoft Security

# Pricing

# Feature comparison

| | Defender for Endpoint-Servers ($5) | Defender for Servers P1 ($5) | Defender for Servers P2 ($15) |
|---|---|---|---|
| Hardening recommendations | | ✓ | ✓ |
| Asset discovery | | ✓ | ✓ |
| Vulnerability assessment using Microsoft Threat & Vulnerability Management | ✓ | ✓ | ✓ |
| Attack surface reduction | ✓ | ✓ | ✓ |
| Next generation antivirus protection | ✓ | ✓ | ✓ |
| Endpoint detection & response | ✓ | ✓ | ✓ |
| Automated self-healing | ✓ | ✓ | ✓ |
| Log-analytics (500MB free) | | | ✓ |
| Regulatory compliance assessment | | | ✓ |
| Vulnerability assessment using Qualys | | | ✓ |
| Network layer threat detection | | | ✓ |
| Adaptive application controls | | | ✓ |
| File integrity monitoring | | | ✓ |
| Just-in-time VM access for management ports | | | ✓ |
| Adaptive network hardening | | | ✓ |

Microsoft Defender for Endpoint

# SUNY Negotiated Pricing

**Microsoft Defender for Endpoint (MDE) Client-Side** Per user Per Month every user has 5 devices included.

| | |
|---|---|
| MDE P2 List Price | $2.65 |
| MDE P2 Discount Percentage | 25% |
| MDE P2 Price After Discount | $2.00 |

**Microsoft Defender for Endpoint Server (MDES)** Per Month Per OSE (Operating System Environment)

| | |
|---|---|
| MDES P2 List Price | $5.00 |
| MDES P2 Discount Percentage | 25% |
| MDES P2 Price After Discount | $3.75 |

**Microsoft Defender for Servers (DfS)** Part of Microsoft Defender for Cloud Per Server

| | |
|---|---|
| DfS P1 List Price | $5.00 |
| DfS P1 Discount Percentage | 25% |
| DfS P1 Price After Discount | $3.75 |
| DfS P2 List Price | $15.00 |
| DfS P2 Discount Percentage | 50% |
| DfS P2 Price After Discount | $7.50 |

M365 A5 per EQU Per Month

| | |
|---|---|
| List price | $8.76 |
| Discounted price | $7.65 |

M365 A5 Security* per EQU per Month

| | |
|---|---|
| List Price | $3.30 |
| Discounted Price | $2.35 |

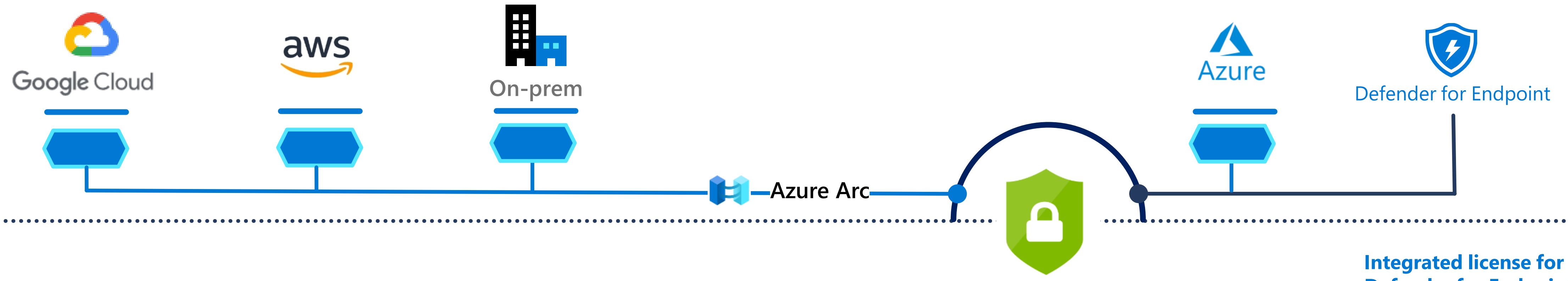
*Step up from M365 A3

Microsoft Security

# Questions?

Steve Scholz
Security Solution Specialist
Steve.scholz@microsoft.com
https://aka.ms/meetwithme

# Hygiene and Visbility



**Integrated license for Microsoft Defender for Endpoint**

| | | | | | |
|---|---|---|---|---|---|
| Server Hygiene | Secure score | Visibility | Regulatory Compliance | Vulnerability Assessment | |
| Advanced Protection | Adaptive Application Control | *Just-in-time VM Access | *Adaptive Network Hardening | File Integrity Monitoring | Docker Host Hardening |
| Detection & Response | Threat Detection (MDE) | Fileless Attack Detection | Linux auditd ML | Export & Automation | |

# Security posture management with Secure Score

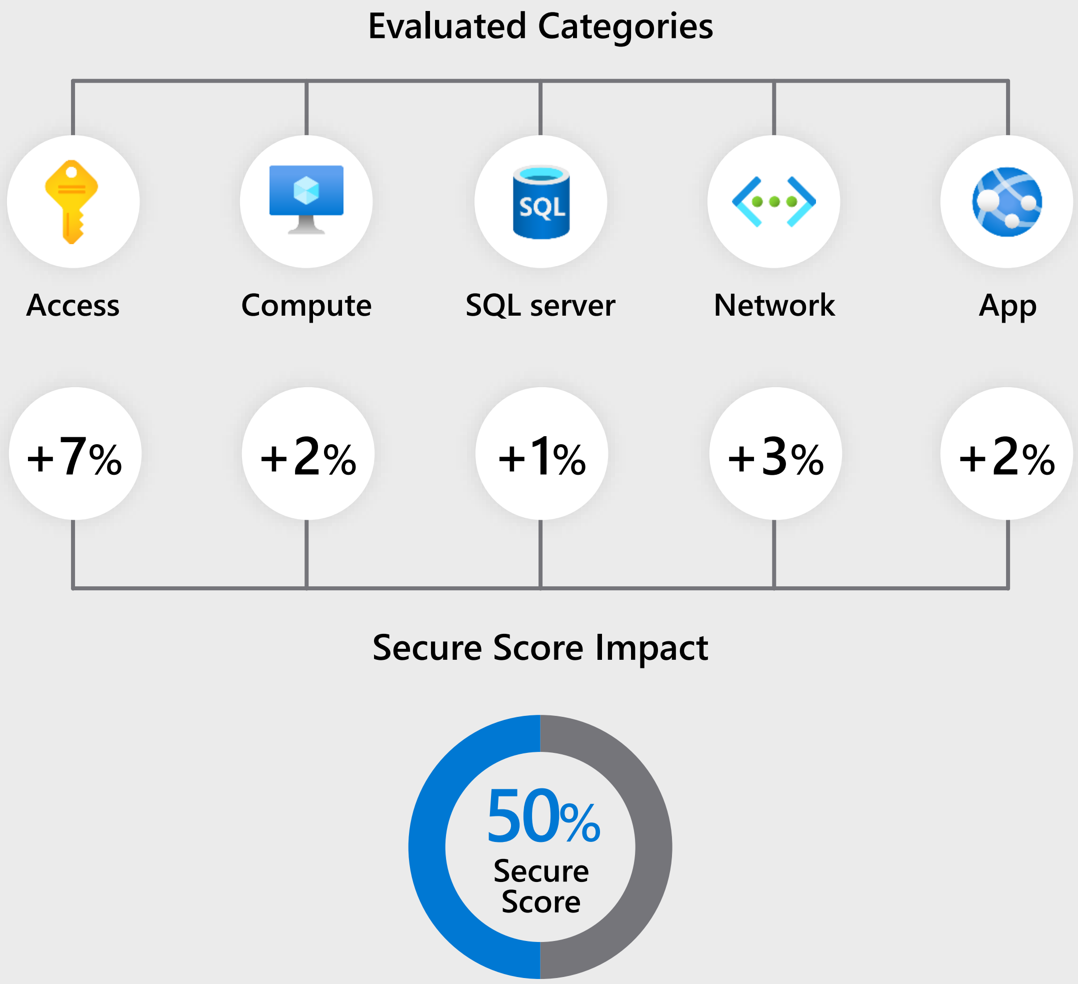
Gain instant insight into the security state of your cloud workloads

Address security vulnerabilities with prioritized recommendations

Improve your Secure Score and overall security posture in minutes

Speed up regulatory compliance

Granular control of Secure Score



©Microsoft Corporation
Azure

# Inventory View

## Improved visibility across the entire estate

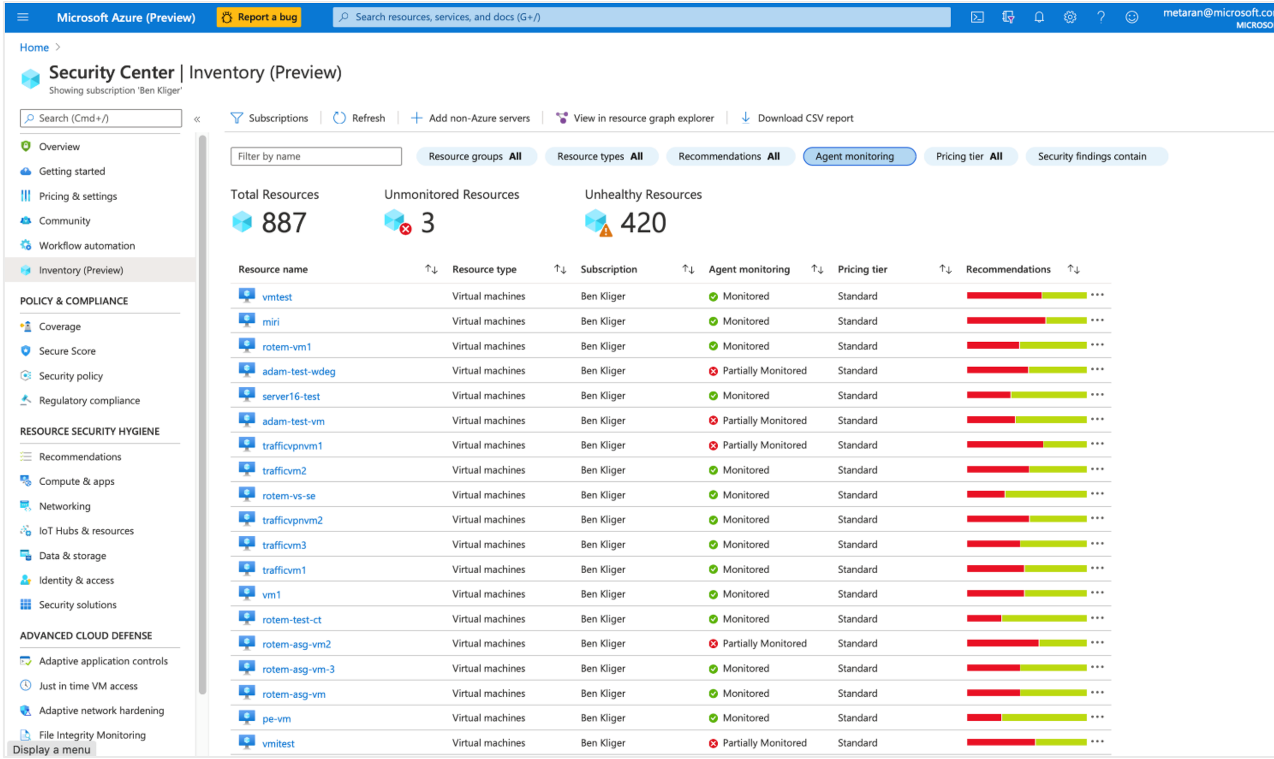
Single view of all monitored resources

Easy filtering, sorting and cross-referencing experience

Continue exploration in Azure Resource Graph & export to CSV

Management of resources

Review applications and software installed on your machines (integration with MDE)



Security Center | Inventory (Preview)

Showing subscription 'Ben Kliger'

Total Resources 887

Unmonitored Resources 3

Unhealthy Resources 420

| Resource name ↑↓ | Resource type ↑↓ | Subscription ↑↓ | Agent monitoring ↑↓ | Pricing tier ↑↓ | Recommendations ↑↓ |
|---|---|---|---|---|---|
| vmtest | Virtual machines | Ben Kliger | ✓ Monitored | Standard | 🟥🟩 ··· |
| miri | Virtual machines | Ben Kliger | ✓ Monitored | Standard | 🟥🟩 ··· |
| rotem-vm1 | Virtual machines | Ben Kliger | ✓ Monitored | Standard | 🟥🟩 ··· |
| adam-test-wdeg | Virtual machines | Ben Kliger | ☒ Partially Monitored | Standard | 🟥🟩 ··· |
| server16-test | Virtual machines | Ben Kliger | ✓ Monitored | Standard | 🟥🟩 ··· |
| adam-test-vm | Virtual machines | Ben Kliger | ☒ Partially Monitored | Standard | 🟥🟩 ··· |
| trafficvpnvm1 | Virtual machines | Ben Kliger | ☒ Partially Monitored | Standard | 🟥🟩 ··· |
| trafficvm2 | Virtual machines | Ben Kliger | ✓ Monitored | Standard | 🟥🟩 ··· |
| rotem-vs-se | Virtual machines | Ben Kliger | ✓ Monitored | Standard | 🟥🟩 ··· |
| trafficvpnvm2 | Virtual machines | Ben Kliger | ✓ Monitored | Standard | 🟥🟩 ··· |
| trafficvm3 | Virtual machines | Ben Kliger | ✓ Monitored | Standard | 🟥🟩 ··· |
| trafficvm1 | Virtual machines | Ben Kliger | ✓ Monitored | Standard | 🟥🟩 ··· |
| vm1 | Virtual machines | Ben Kliger | ✓ Monitored | Standard | 🟥🟩 ··· |
| rotem-test-ct | Virtual machines | Ben Kliger | ✓ Monitored | Standard | 🟥🟩 ··· |
| rotem-asg-vm2 | Virtual machines | Ben Kliger | ☒ Partially Monitored | Standard | 🟥🟩 ··· |
| rotem-asg-vm-3 | Virtual machines | Ben Kliger | ✓ Monitored | Standard | 🟥🟩 ··· |
| rotem-asg-vm | Virtual machines | Ben Kliger | ✓ Monitored | Standard | 🟥🟩 ··· |
| pe-vm | Virtual machines | Ben Kliger | ✓ Monitored | Standard | 🟥🟩 ··· |
| vmitest | Virtual machines | Ben Kliger | ☒ Partially Monitored | Standard | 🟥🟩 ··· |

©Microsoft Corporation
Azure

# Regulatory Compliance

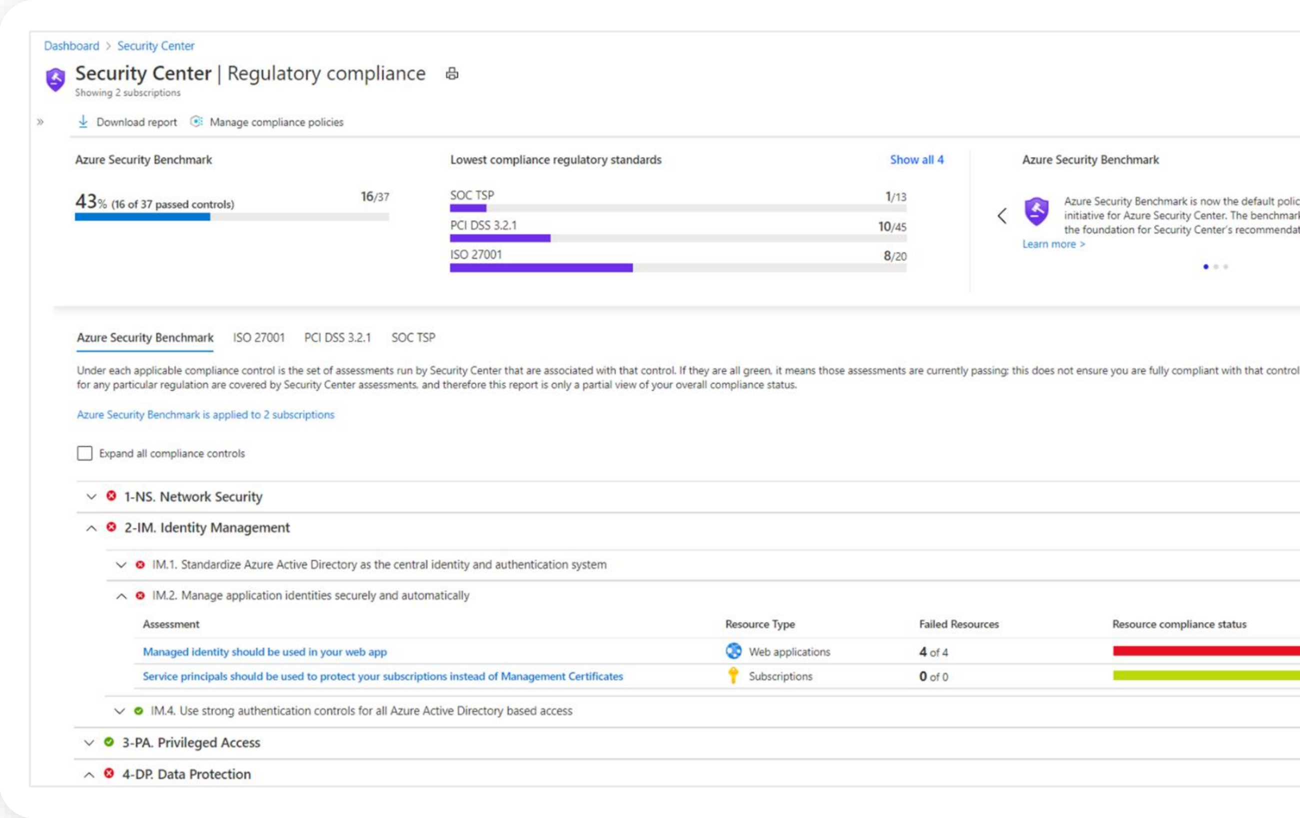
Demonstrate compliance status, based on continuous assessments of Azure and Hybrid resources

Monitor AWS and GCP resources with multi-cloud support

**Azure Security Benchmark** monitoring enabled by default, fully aligned with Secure Score

Support common industry standards, as well as custom initiatives based on Azure Policy

Overview of compliance status and report download



Dashboard > Security Center

Security Center | Regulatory compliance

Showing 2 subscriptions

Azure Security Benchmark

43% (16 of 37 passed controls) 16/37

Lowest compliance regulatory standards

| | |
|---|---|
| SOC TSP | 1/13 |
| PCI DSS 3.2.1 | 10/45 |
| ISO 27001 | 8/20 |

Azure Security Benchmark

Azure Security Benchmark is now the default polic
initiative for Azure Security Center. The benchmar
the foundation for Security Center's recommendat

Under each applicable compliance control is the set of assessments run by Security Center 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
for any particular regulation are covered by Security Center assessments, and therefore this report is only a partial view of your overall compliance status.

Azure Security Benchmark is applied to 2 subscriptions

☐ Expand all compliance controls

- ✗ 1-NS. Network Security
- ✗ 2-IM. Identity Management
  - ✗ IM.1. Standardize Azure Active Directory as the central identity and authentication system
  - ✗ IM.2. Manage application identities securely and automatically

| Assessment | Resource Type | Failed Resources | Resource compliance status |
|---|---|---|---|
| Managed identity should be used in your web app | Web applications | 4 of 4 | 🟥 |
| Service principals should be used to protect your subscriptions instead of Management Certificates | Subscriptions | 0 of 0 | 🟩 |

  - ✓ IM.4. Use strong authentication controls for all Azure Active Directory based access
- ✓ 3-PA. Privileged Access
- ✗ 4-DP. Data Protection

©Microsoft Corporation
Azure

# Vulnerability Assessment

## Available as part of Microsoft Defender for Servers

Google Cloud aws Azure

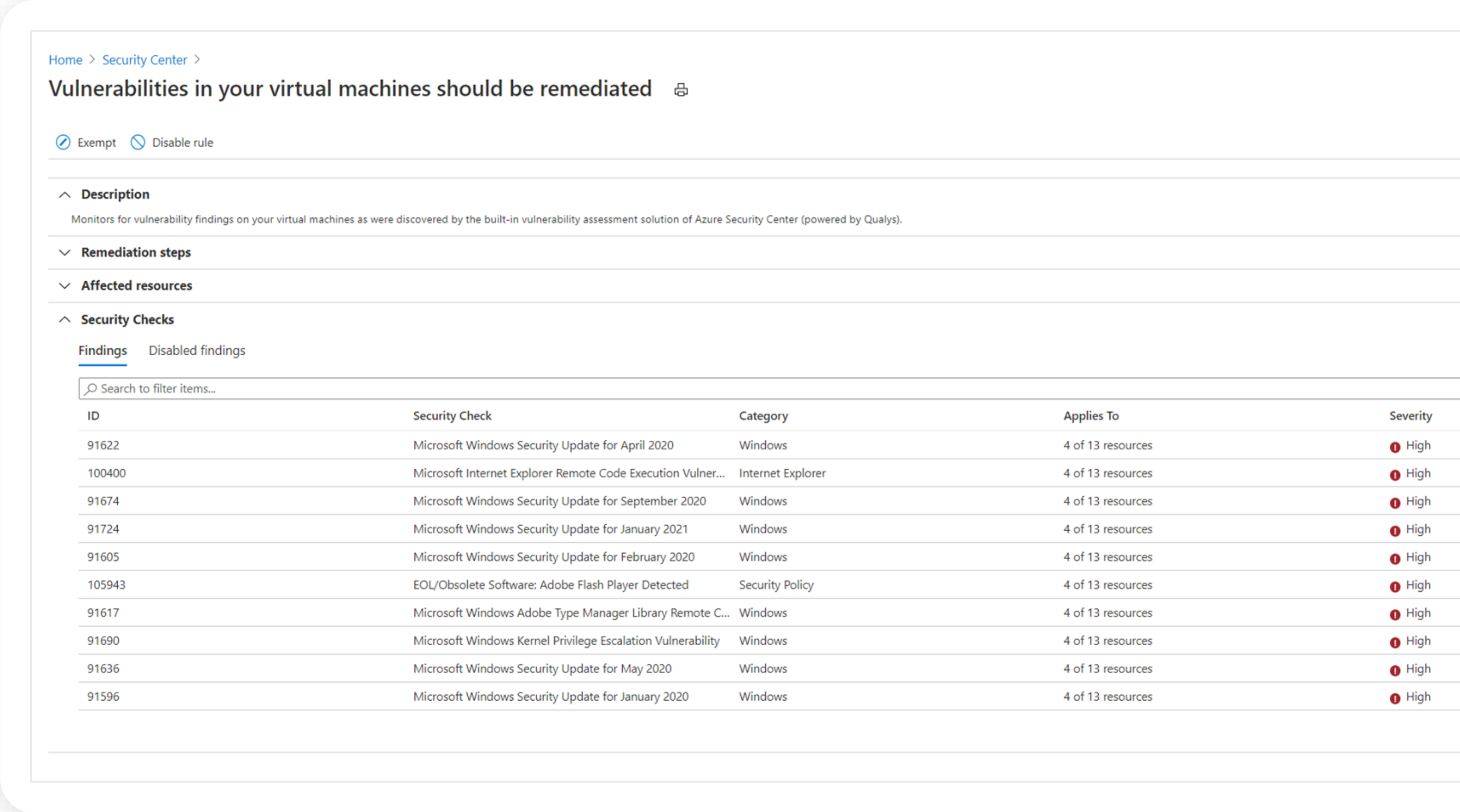
Automated deployment of the vulnerability scanner

Continuously scans installed applications to find vulnerabilities for Linux & Windows VMs

Visibility to the vulnerability findings in Security Center portal and APIs

Powered by Qualys or Microsoft Defender for Endpoint

Bring your own license (BYOL) solutions for (Qualys or Rapid 7)



Vulnerabilities in your virtual machines should be remediated

**Description**

Monitors for vulnerability findings on your virtual machines as were discovered by the built-in vulnerability assessment solution of Azure Security Center (powered by Qualys).

**Remediation steps**

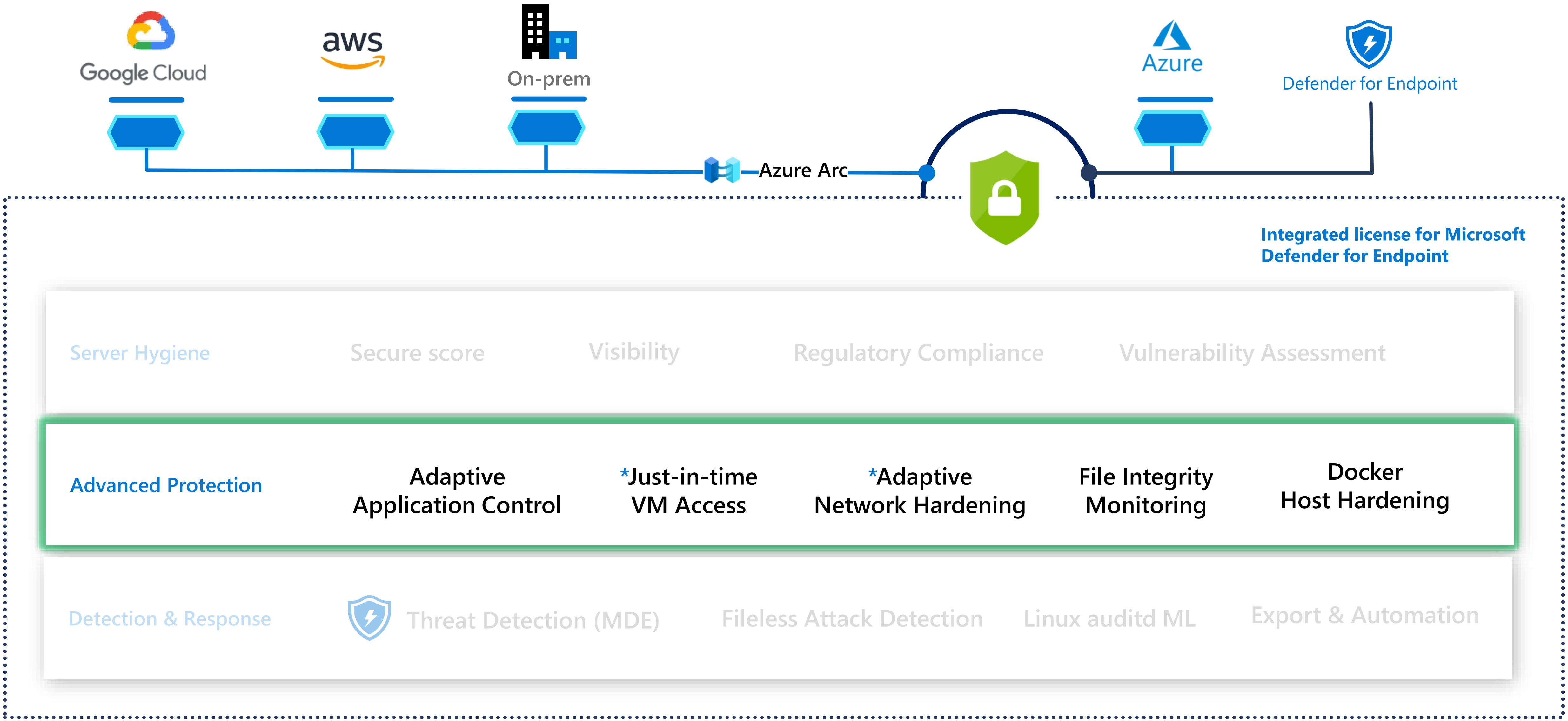
**Affected resources**

**Security Checks**

| ID | Security Check | Category | Applies To | Severity |
|---|---|---|---|---|
| 91622 | Microsoft Windows Security Update for April 2020 | Windows | 4 of 13 resources | ● High |
| 100400 | Microsoft Internet Explorer Remote Code Execution Vulner... | Internet Explorer | 4 of 13 resources | ● High |
| 91674 | Microsoft Windows Security Update for September 2020 | Windows | 4 of 13 resources | ● High |
| 91724 | Microsoft Windows Security Update for January 2021 | Windows | 4 of 13 resources | ● High |
| 91605 | Microsoft Windows Security Update for February 2020 | Windows | 4 of 13 resources | ● High |
| 105943 | EOL/Obsolete Software: Adobe Flash Player Detected | Security Policy | 4 of 13 resources | ● High |
| 91617 | Microsoft Windows Adobe Type Manager Library Remote C... | Windows | 4 of 13 resources | ● High |
| 91690 | Microsoft Windows Kernel Privilege Escalation Vulnerability | Windows | 4 of 13 resources | ● High |
| 91636 | Microsoft Windows Security Update for May 2020 | Windows | 4 of 13 resources | ● High |
| 91596 | Microsoft Windows Security Update for January 2020 | Windows | 4 of 13 resources | ● High |

©Microsoft Corporation
Azure

# Advanced Protection



**Integrated license for Microsoft Defender for Endpoint**

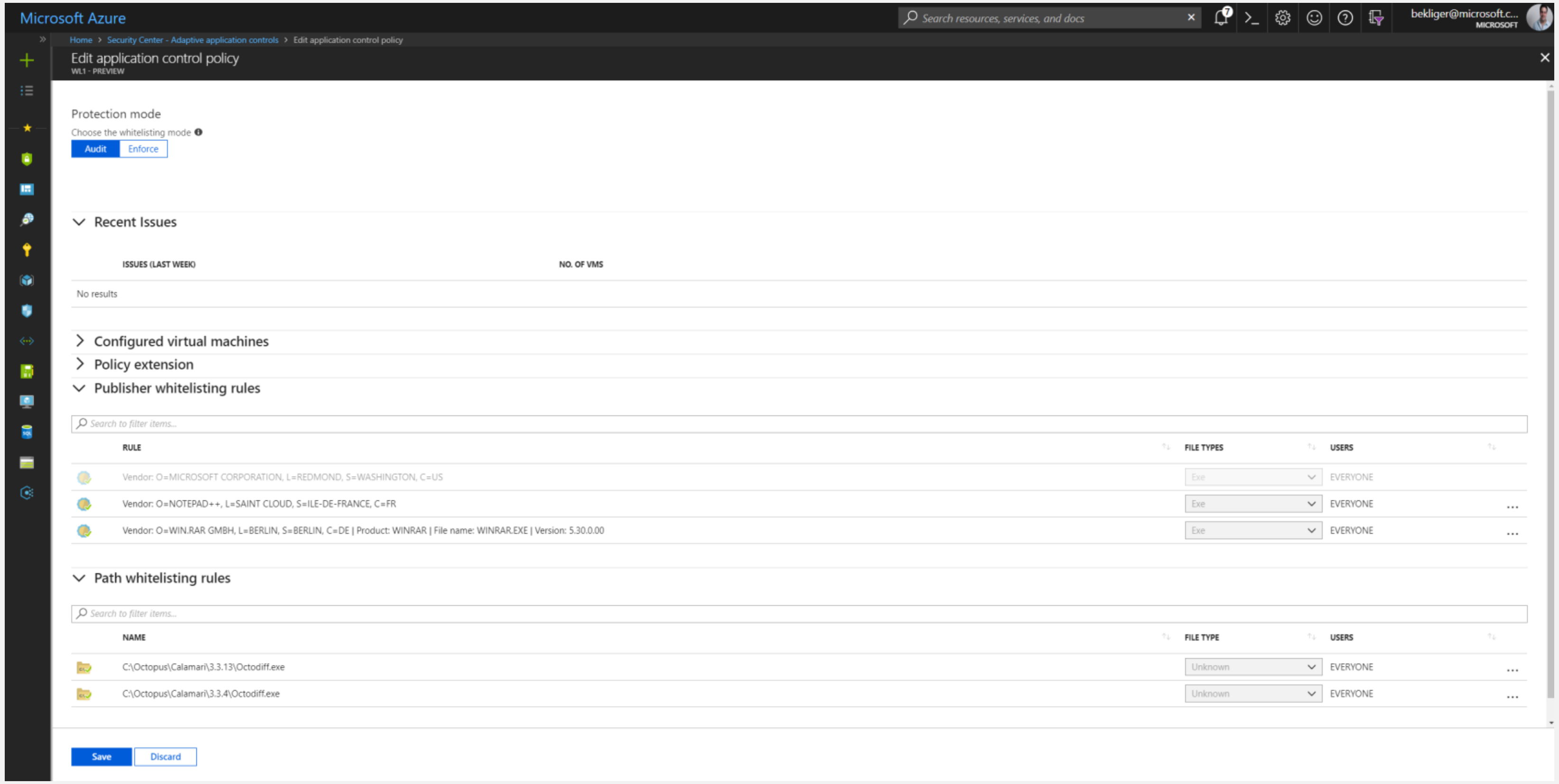
Server Hygiene — Secure score — Visibility — Regulatory Compliance — Vulnerability Assessment

Advanced Protection — Adaptive Application Control — *Just-in-time VM Access — *Adaptive Network Hardening — File Integrity Monitoring — Docker Host Hardening

Detection & Response — Threat Detection (MDE) — Fileless Attack Detection — Linux auditd ML — Export & Automation

# Adaptive Application Controls

- Identify potential malware, even any that might be missed by antimalware solutions
- Improve compliance with local security policies that dictate the use of only licensed software
- Identify outdated or unsupported versions of applications
- Identify software that's banned by your organization
- Increase oversight of apps that access sensitive data


Microsoft Azure
Search resources, services, and docs
bekliger@microsoft.c...
MICROSOFT
Home > Security Center - Adaptive application controls > Edit application control policy

Edit application control policy
WL1 - PREVIEW

Protection mode

Choose the whitelisting mode

[✓ Audit] Enforce

Recent Issues

| ISSUES (LAST WEEK) | NO. OF VMS |
|---|---|
| No results | |

Configured virtual machines

Policy extension

Publisher whitelisting rules

Search to filter items...

| RULE | FILE TYPES | USERS |
|---|---|---|
| Vendor: O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US | Exe | EVERYONE |
| Vendor: O=NOTEPAD++, L=SAINT CLOUD, S=ILE-DE-FRANCE, C=FR | Exe | EVERYONE |
| Vendor: O=WIN.RAR GMBH, L=BERLIN, S=BERLIN, C=DE \| Product: WINRAR \| File name: WINRAR.EXE \| Version: 5.30.0.00 | Exe | EVERYONE |

Path whitelisting rules

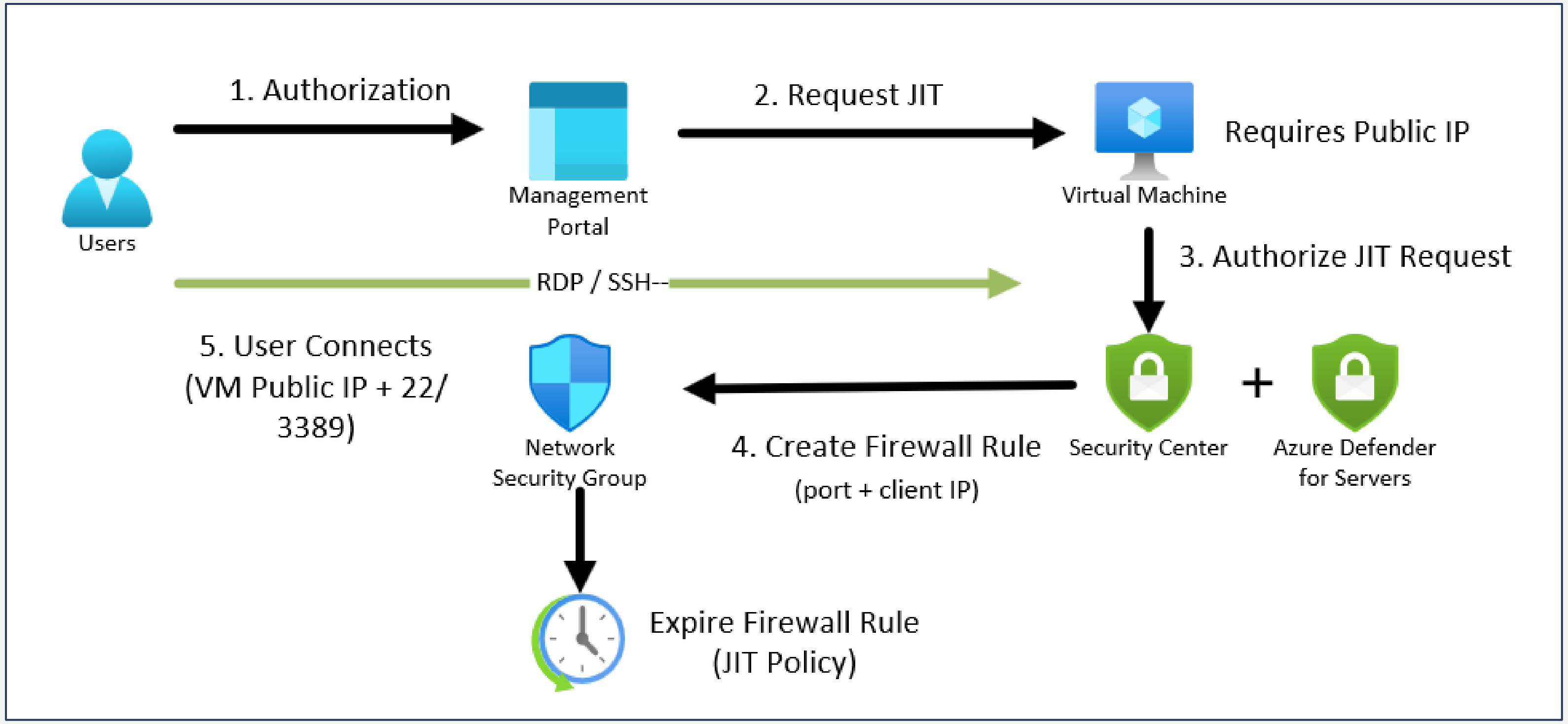
Search to filter items...

| NAME | FILE TYPE | USERS |
|---|---|---|
| C:\Octopus\Calamari\3.3.13\Octodiff.exe | Unknown | EVERYONE |
| C:\Octopus\Calamari\3.3.4\Octodiff.exe | Unknown | EVERYONE |

# Just in Time Virtual Machine Access

## Azure Virtual Machines Only

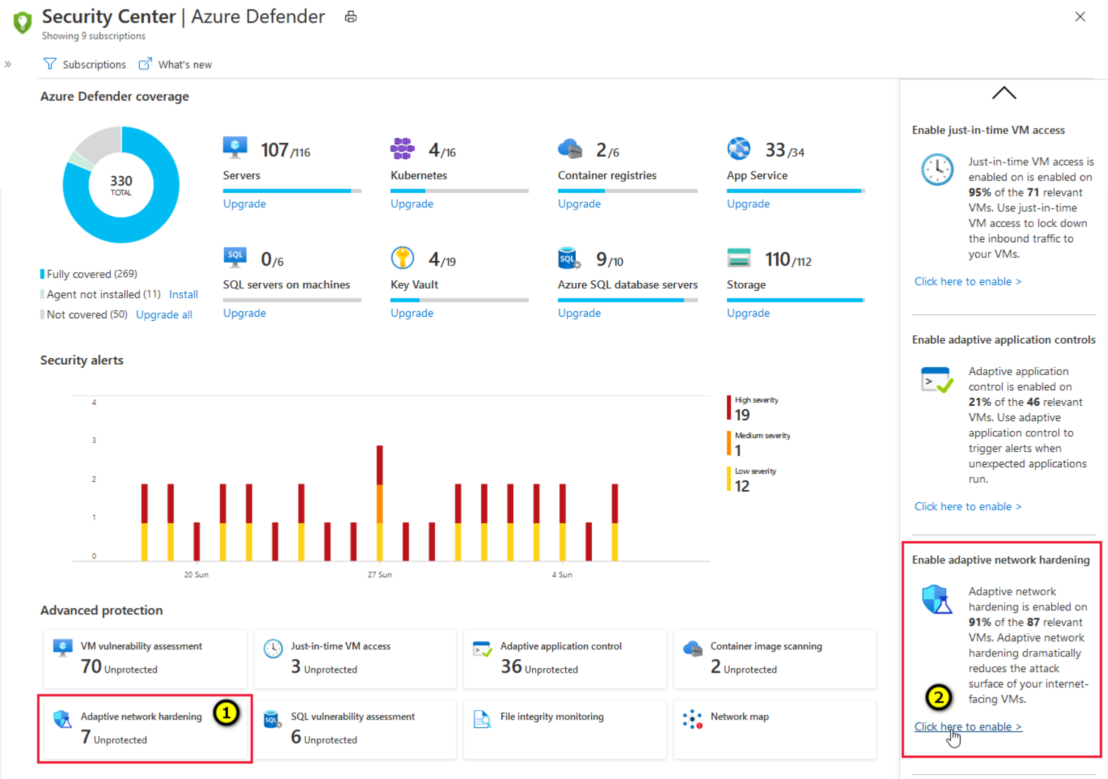
- Lock down the inbound traffic to your VMs, reducing exposure to attacks while providing easy access to connect to VMs when needed
- Provide Just in Time Access to RDP and SSH
- Security Center configures the NSGs and Azure Firewall to allow inbound traffic to the selected ports from the relevant IP address (or range)



# Adaptive Network Hardening

## Azure Virtual Machines Only

- Provides recommendations to further harden the NSG rules
- Uses machine learning that factors in actual traffic, known trusted configuration, threat intelligence, and other indicators of compromise



Security Center | Azure Defender

Showing 9 subscriptions

Subscriptions · What's new

**Azure Defender coverage**

330 TOTAL

Fully covered (269)
Agent not installed (11) Install
Not covered (50) Upgrade all

| | | | |
|---|---|---|---|
| 107/116<br>Servers<br>Upgrade | 4/16<br>Kubernetes<br>Upgrade | 2/6<br>Container registries<br>Upgrade | 33/34<br>App Service<br>Upgrade |
| 0/6<br>SQL servers on machines<br>Upgrade | 4/19<br>Key Vault<br>Upgrade | 9/10<br>Azure SQL database servers<br>Upgrade | 110/112<br>Storage<br>Upgrade |

**Security alerts**

**Advanced protection**

| | | | |
|---|---|---|---|
| VM vulnerability assessment<br>70 Unprotected | Just-in-time VM access<br>3 Unprotected | Adaptive application control<br>36 Unprotected | Container image scanning<br>2 Unprotected |
| Adaptive network hardening (1)<br>7 Unprotected | SQL vulnerability assessment<br>6 Unprotected | File integrity monitoring | Network map |

**Enable just-in-time VM access**

Just-in-time VM access is enabled on is enabled on **95%** of the **71** relevant VMs. Use just-in-time VM access to lock down the inbound traffic to your VMs.

Click here to enable >

**Enable adaptive application controls**

Adaptive application control is enabled on **21%** of the **46** relevant VMs. Use adaptive application control to trigger alerts when unexpected applications run.

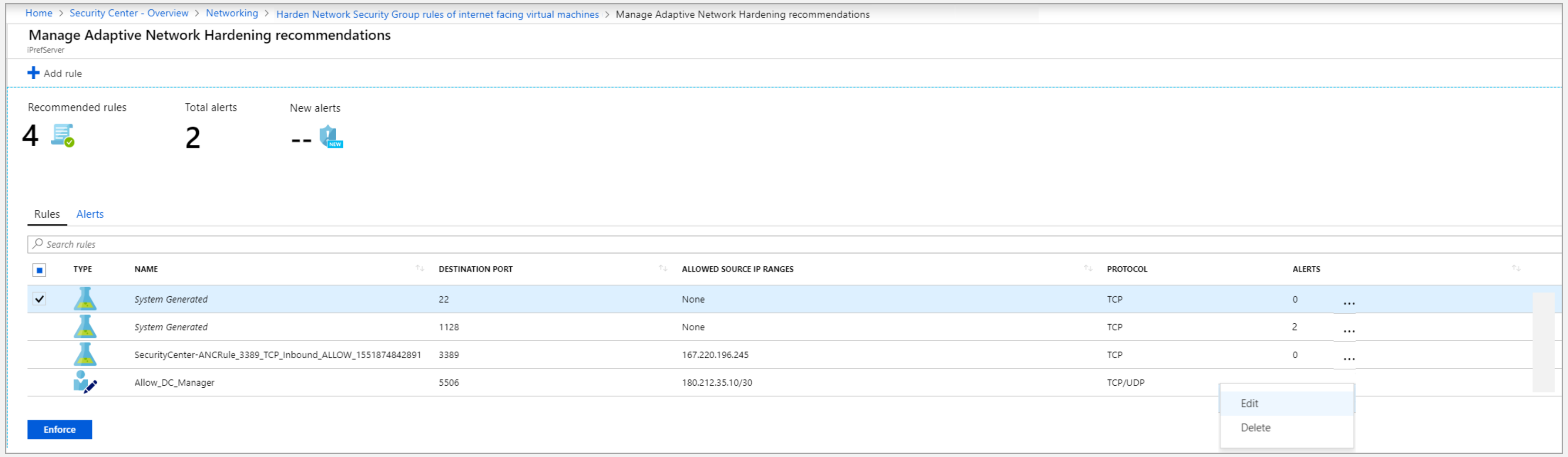
Click here to enable >

**Enable adaptive network hardening**

Adaptive network hardening is enabled on **91%** of the **87** relevant VMs. Adaptive network hardening dramatically reduces the attack surface of your internet-facing VMs.

(2)

Click here to enable >



Home > Security Center - Overview > Networking > Harden Network Security Group rules of internet facing virtual machines > Manage Adaptive Network Hardening recommendations

Manage Adaptive Network Hardening recommendations

iPrefServer

Add rule

Recommended rules 4 · Total alerts 2 · New alerts --

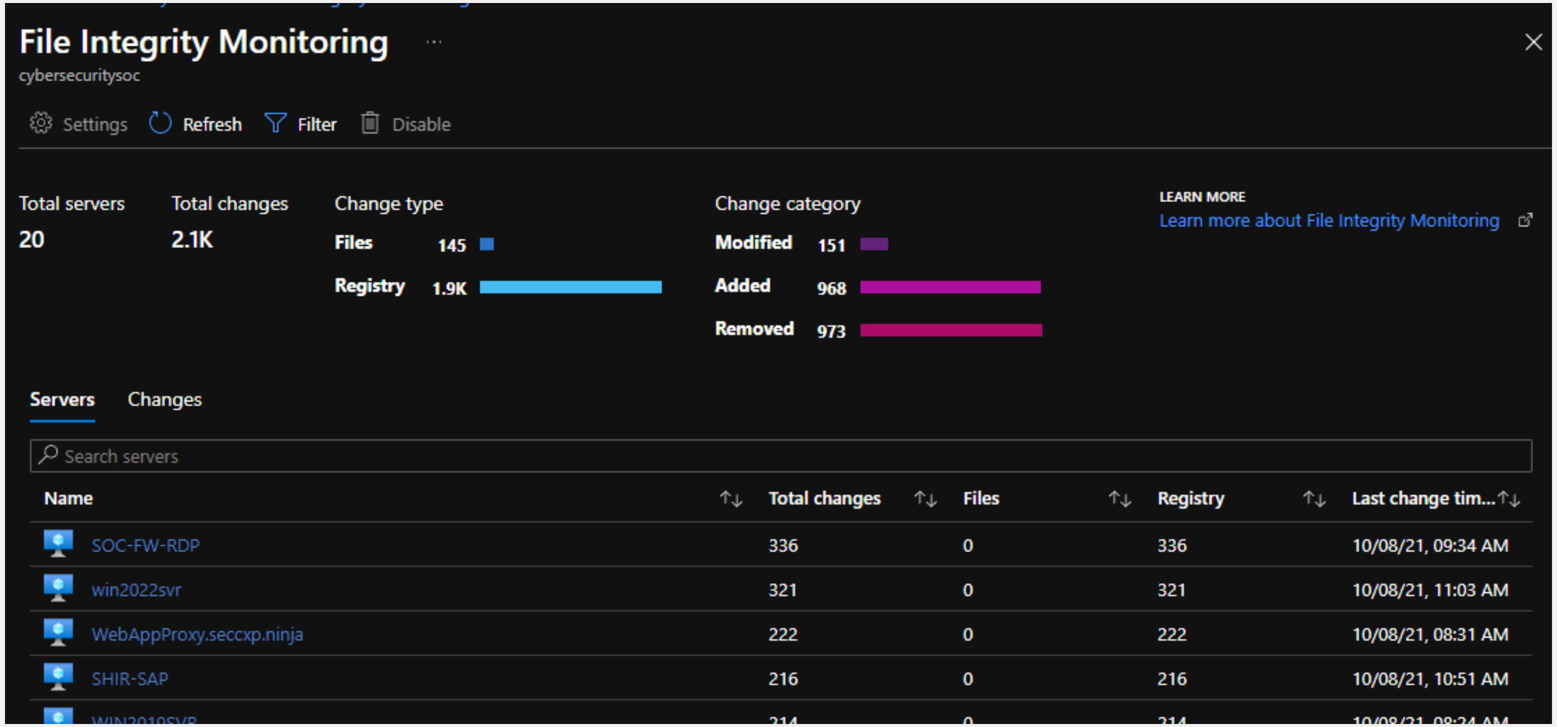
Rules · Alerts

Search rules

| ■ | TYPE | NAME | DESTINATION PORT | ALLOWED SOURCE IP RANGES | PROTOCOL | ALERTS |
|---|---|---|---|---|---|---|
| ✓ | | *System Generated* | 22 | None | TCP | 0 |
| | | *System Generated* | 1128 | None | TCP | 2 |
| | | SecurityCenter-ANCRule_3389_TCP_Inbound_ALLOW_1551874842891 | 3389 | 167.220.196.245 | TCP | 0 |
| | | Allow_DC_Manager | 5506 | 180.212.35.10/30 | TCP/UDP | |

# File integrity monitoring

- Examines files and registries of the operating system, application software, and others for changes that might indicate an attack
- Validates the integrity of Windows files, Windows registry, and Linux files.
- Select the files that you want to be monitored by enabling File Integration Monitoring (FIM)



File Integrity Monitoring

cybersecuritysoc

Total servers 20

Total changes 2.1K

Change type

| | |
|---|---|
| Files | 145 |
| Registry | 1.9K |

Change category

| | |
|---|---|
| Modified | 151 |
| Added | 968 |
| Removed | 973 |

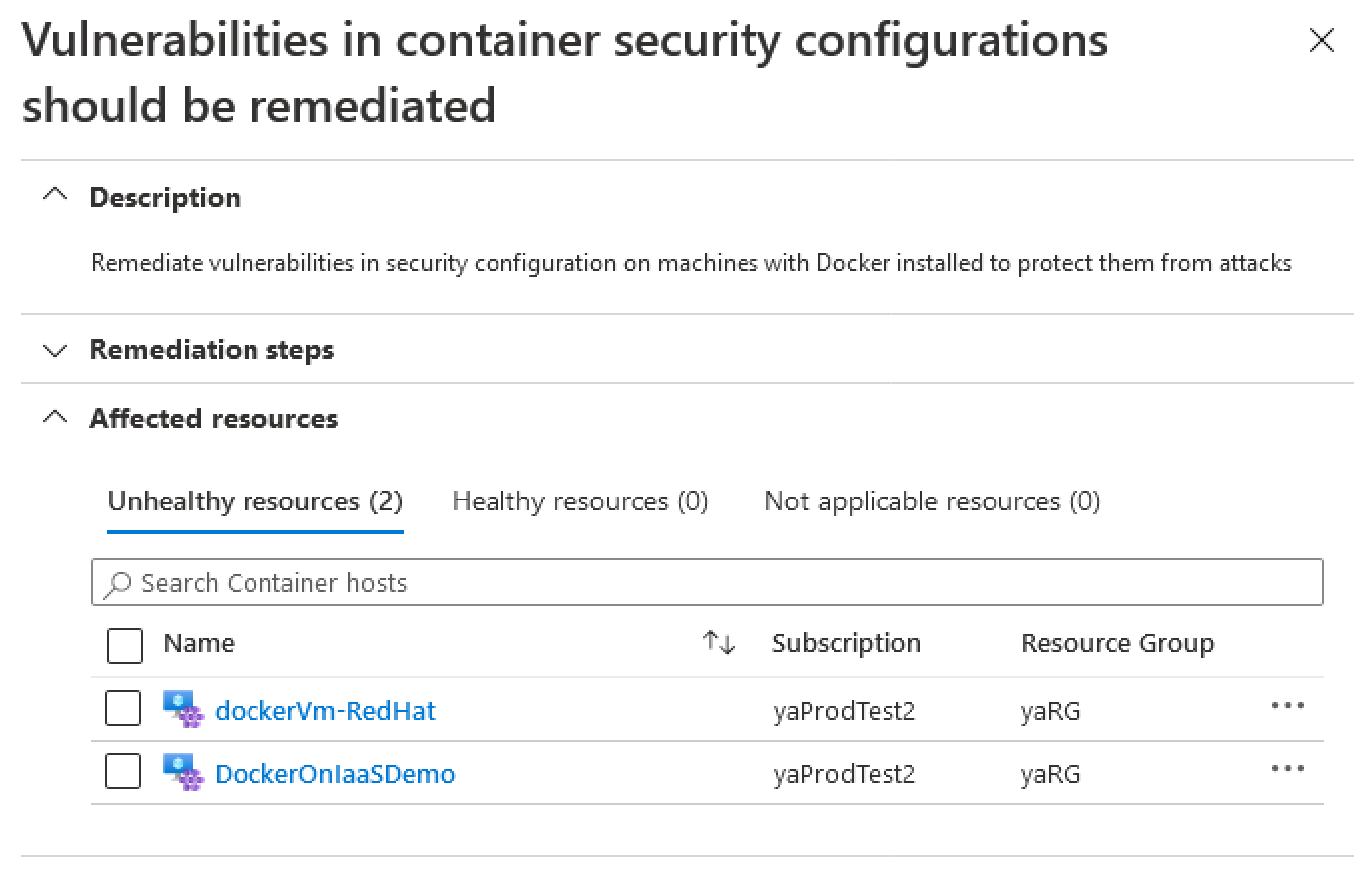
LEARN MORE

Learn more about File Integrity Monitoring

| Name | Total changes | Files | Registry | Last change tim... |
|---|---|---|---|---|
| SOC-FW-RDP | 336 | 0 | 336 | 10/08/21, 09:34 AM |
| win2022svr | 321 | 0 | 321 | 10/08/21, 11:03 AM |
| WebAppProxy.seccxp.ninja | 222 | 0 | 222 | 10/08/21, 08:31 AM |
| SHIR-SAP | 216 | 0 | 216 | 10/08/21, 10:51 AM |
| WIN2019SVR | 214 | 0 | 214 | 10/08/21, 08:24 AM |

# Docker Host Hardening

- Identifies unmanaged containers hosted on IaaS Linux VMs, or other Linux machines running Docker containers
- Continuously assesses the configurations of containers
- Generates security recommendations based on vulnerabilities and the CIS benchmark



## Vulnerabilities in container security configurations should be remediated

**Description**

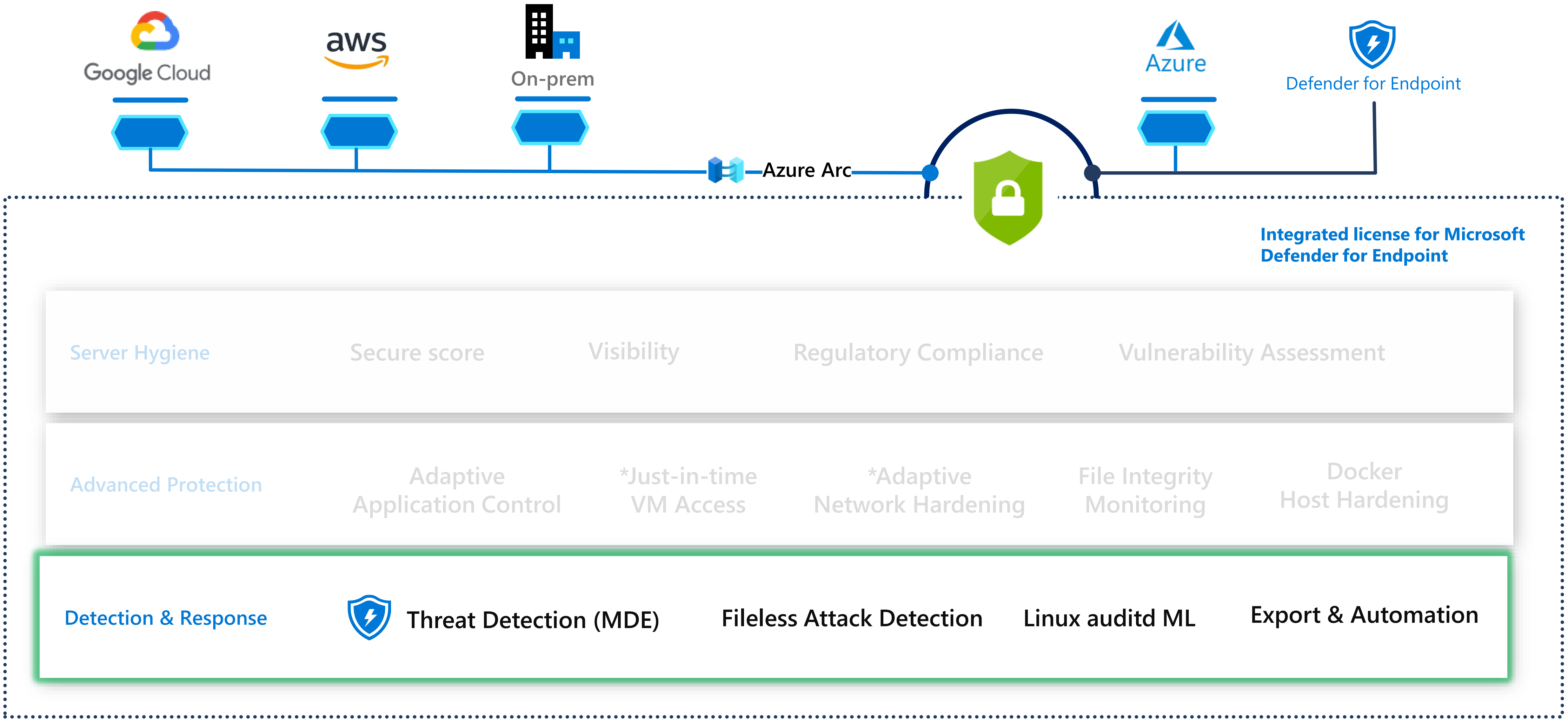
Remediate vulnerabilities in security configuration on machines with Docker installed to protect them from attacks

**Remediation steps**

**Affected resources**

| □ | Name ↑↓ | Subscription | Resource Group | |
|---|---|---|---|---|
| □ | dockerVm-RedHat | yaProdTest2 | yaRG | ··· |
| □ | DockerOnIaaSDemo | yaProdTest2 | yaRG | ··· |

# Detection and Response



Integrated license for Microsoft Defender for Endpoint

| | | | | | |
|---|---|---|---|---|---|
| Server Hygiene | Secure score | Visibility | Regulatory Compliance | Vulnerability Assessment | |
| Advanced Protection | Adaptive Application Control | *Just-in-time VM Access | *Adaptive Network Hardening | File Integrity Monitoring | Docker Host Hardening |
| Detection & Response | Threat Detection (MDE) | Fileless Attack Detection | Linux auditd ML | Export & Automation | |

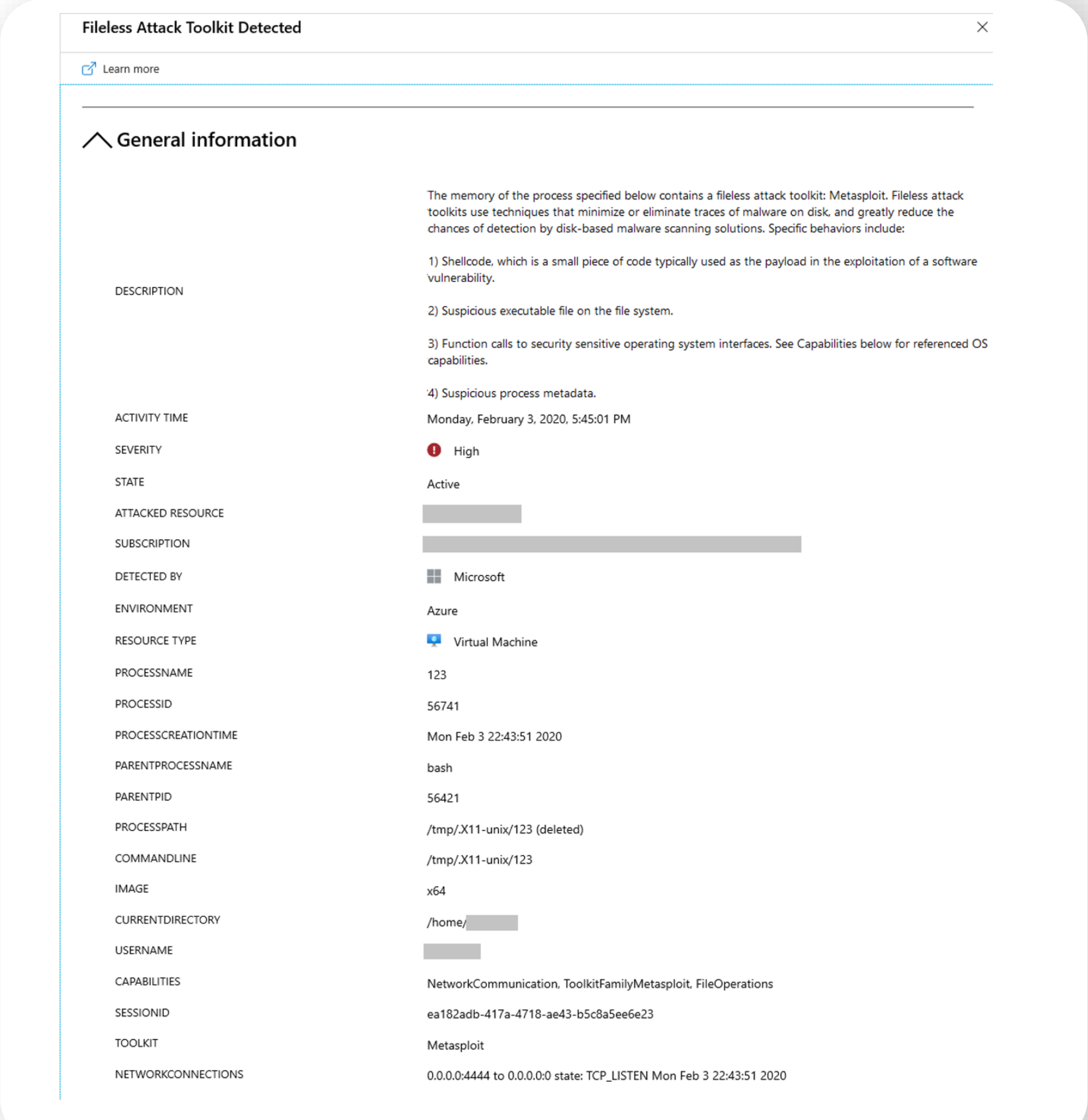
# Fileless Attack Detection

## Complement EDR with increased detection coverage

Automated memory forensic techniques identify fileless attack toolkits, techniques, and behaviors

Periodically scans your machine at runtime, and extracts insights directly from the memory of processes to detect:

- Well-known toolkits and crypto mining software
- Shellcode, which is a small piece of code typically used as the payload in the exploitation of a software vulnerability.
- Injected malicious executable in process memory, LD_PRELOAD based rootkits to preload malicious libraries.
- Elevation of privilege of a process from non-root to root.
- Remote control of another process using ptrace.



Fileless Attack Toolkit Detected

General information

| | |
|---|---|
| DESCRIPTION | The memory of the process specified below contains a fileless attack toolkit: Metasploit. Fileless attack toolkits use techniques that minimize or eliminate traces of malware on disk, and greatly reduce the chances of detection by disk-based malware scanning solutions. Specific behaviors include:<br>1) Shellcode, which is a small piece of code typically used as the payload in the exploitation of a software vulnerability.<br>2) Suspicious executable file on the file system.<br>3) Function calls to security sensitive operating system interfaces. See Capabilities below for referenced OS capabilities.<br>4) Suspicious process metadata. |
| ACTIVITY TIME | Monday, February 3, 2020, 5:45:01 PM |
| SEVERITY | ● High |
| STATE | Active |
| ATTACKED RESOURCE | [redacted] |
| SUBSCRIPTION | [redacted] |
| DETECTED BY | Microsoft |
| ENVIRONMENT | Azure |
| RESOURCE TYPE | Virtual Machine |
| PROCESSNAME | 123 |
| PROCESSID | 56741 |
| PROCESSCREATIONTIME | Mon Feb 3 22:43:51 2020 |
| PARENTPROCESSNAME | bash |
| PARENTPID | 56421 |
| PROCESSPATH | /tmp/.X11-unix/123 (deleted) |
| COMMANDLINE | /tmp/.X11-unix/123 |
| IMAGE | x64 |
| CURRENTDIRECTORY | /home/[redacted] |
| USERNAME | [redacted] |
| CAPABILITIES | NetworkCommunication, ToolkitFamilyMetasploit, FileOperations |
| SESSIONID | ea182adb-417a-4718-ae43-b5c8a5ee6e23 |
| TOOLKIT | Metasploit |
| NETWORKCONNECTIONS | 0.0.0.0:4444 to 0.0.0.0:0 state: TCP_LISTEN Mon Feb 3 22:43:51 2020 |

©Microsoft Corporation
Azure

# Linux auditd

## Detect MITRE Attacks across servers

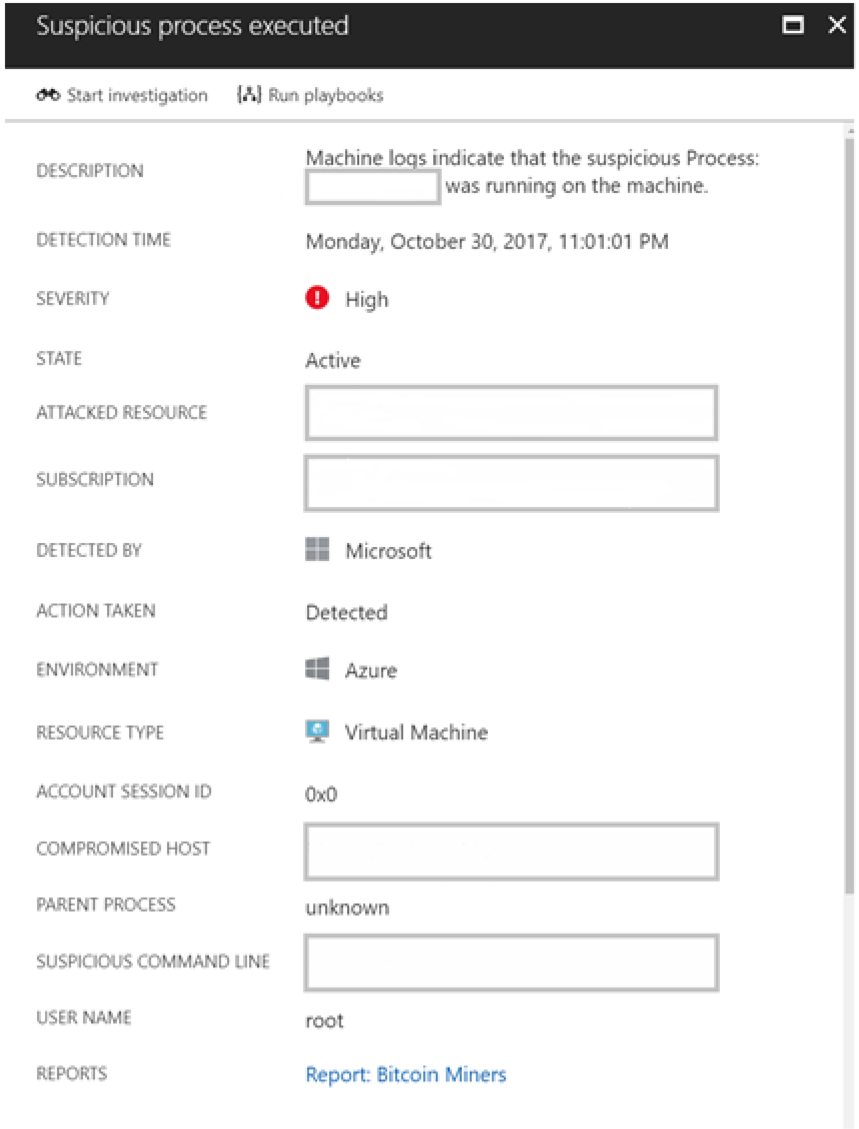
Google Cloud aws Azure

Enables collection of auditd events in all supported Linux distributions, without any prerequisites.

Collects auditd records and enriches and aggregates them into events

Continuously adds new analytics that use Linux signals to detect malicious behaviors on cloud and on-premises Linux machines.

Analytics span across suspicious processes, dubious sign-in attempts, kernel module loading, and other activities



Suspicious process executed

| | |
|---|---|
| DESCRIPTION | Machine logs indicate that the suspicious Process: [redacted] was running on the machine. |
| DETECTION TIME | Monday, October 30, 2017, 11:01:01 PM |
| SEVERITY | ❗ High |
| STATE | Active |
| ATTACKED RESOURCE | [redacted] |
| SUBSCRIPTION | [redacted] |
| DETECTED BY | Microsoft |
| ACTION TAKEN | Detected |
| ENVIRONMENT | Azure |
| RESOURCE TYPE | Virtual Machine |
| ACCOUNT SESSION ID | 0x0 |
| COMPROMISED HOST | [redacted] |
| PARENT PROCESS | unknown |
| SUSPICIOUS COMMAND LINE | [redacted] |
| USER NAME | root |
| REPORTS | Report: Bitcoin Miners |

©Microsoft Corporation
Azure

# Reporting and Exporting

## Create rich, interactive reports of Security Center data

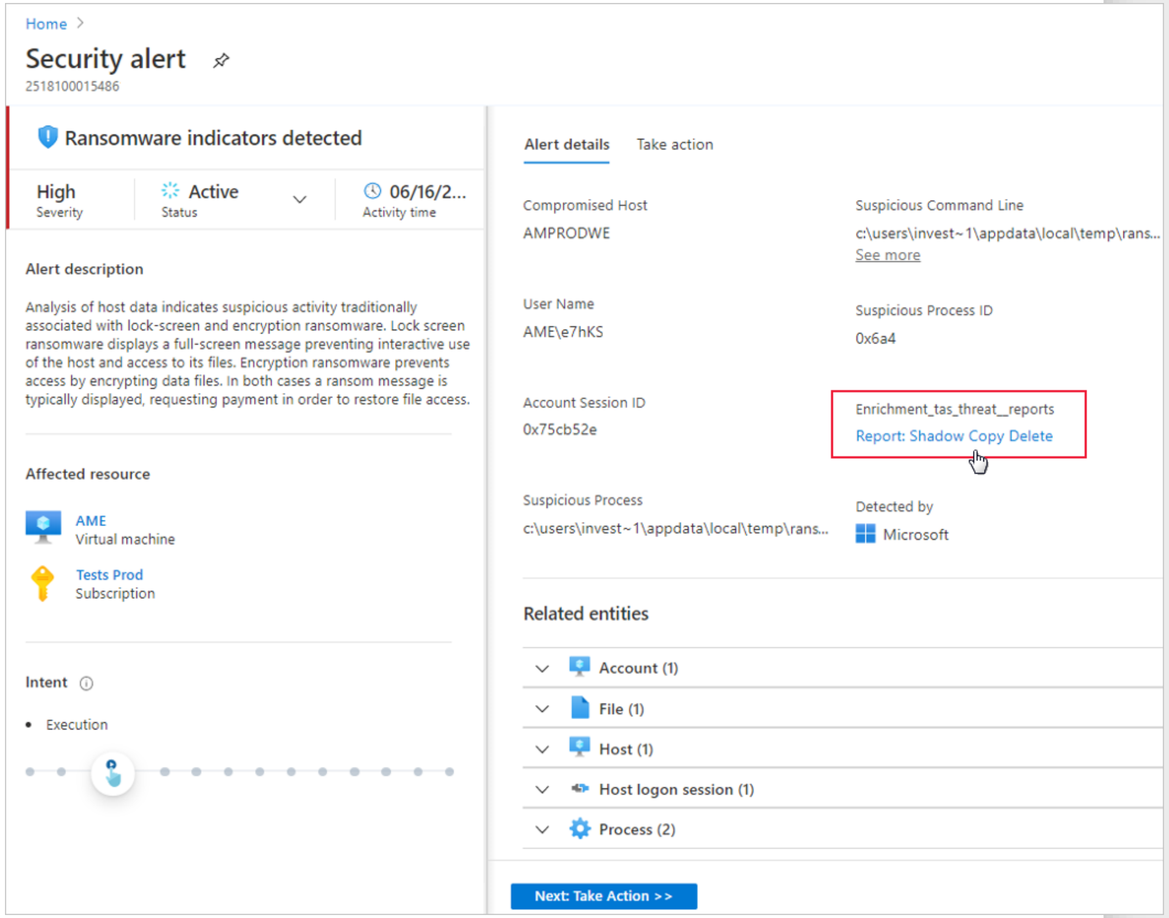
Generate Threat Intelligence Reports

Export Alerts and Recommendations

- SIEM, SOAR, ITSM
- Log Analytics
- CSV

Workbooks to Analyze:

- Secure Score
- Vulnerabilities
- Compliance
- System Updates
- Recommendations



Security alert

2518100015486

Ransomware indicators detected

High
Severity

Active
Status

06/16/2...
Activity time

Alert description

Analysis of host data indicates suspicious activity traditionally associated with lock-screen and encryption ransomware. Lock screen ransomware displays a full-screen message preventing interactive use of the host and access to its files. Encryption ransomware prevents access by encrypting data files. In both cases a ransom message is typically displayed, requesting payment in order to restore file access.

Affected resource

AME
Virtual machine

Tests Prod
Subscription

Intent

- Execution

Compromised Host
AMPRODWE

Suspicious Command Line
c:\users\invest~1\appdata\local\temp\rans...
See more

User Name
AME\e7hKS

Suspicious Process ID
0x6a4

Account Session ID
0x75cb52e

Enrichment_tas_threat__reports
Report: Shadow Copy Delete

Suspicious Process
c:\users\invest~1\appdata\local\temp\rans...

Detected by
Microsoft

Related entities

- Account (1)
- File (1)
- Host (1)
- Host logon session (1)
- Process (2)

©Microsoft Corporation
Azure

# Automation and Response

## Complement EDR and provides increased detection coverage

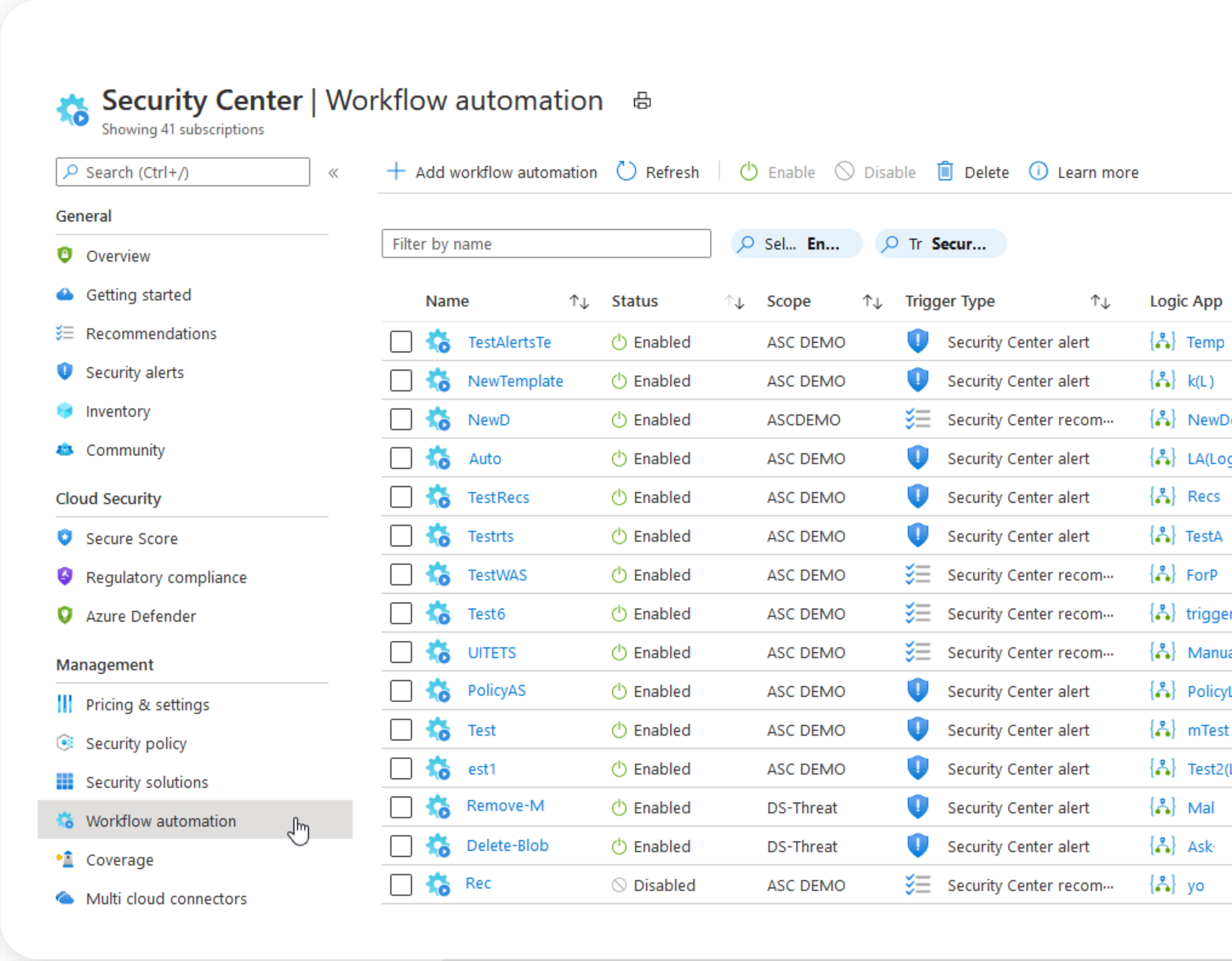
Google Cloud aws Azure

Logic Apps provide an open ecosystem and flexible automation engine

Take action on Security Center Recommendations

Take action on Security Center Alerts

Take action on Security Center regulatory compliance assessment



Security Center | Workflow automation

Showing 41 subscriptions

| | Name | Status | Scope | Trigger Type | Logic App |
|---|---|---|---|---|---|
| □ | TestAlertsTe | Enabled | ASC DEMO | Security Center alert | Temp |
| □ | NewTemplate | Enabled | ASC DEMO | Security Center alert | k(L) |
| □ | NewD | Enabled | ASCDEMO | Security Center recom... | NewD |
| □ | Auto | Enabled | ASC DEMO | Security Center alert | LA(Log |
| □ | TestRecs | Enabled | ASC DEMO | Security Center alert | Recs |
| □ | Testrts | Enabled | ASC DEMO | Security Center alert | TestA |
| □ | TestWAS | Enabled | ASC DEMO | Security Center recom... | ForP |
| □ | Test6 | Enabled | ASC DEMO | Security Center recom... | trigge |
| □ | UITETS | Enabled | ASC DEMO | Security Center recom... | Manua |
| □ | PolicyAS | Enabled | ASC DEMO | Security Center alert | Policy |
| □ | Test | Enabled | ASC DEMO | Security Center alert | mTest |
| □ | est1 | Enabled | ASC DEMO | Security Center alert | Test2( |
| □ | Remove-M | Enabled | DS-Threat | Security Center alert | Mal |
| □ | Delete-Blob | Enabled | DS-Threat | Security Center alert | Ask |
| □ | Rec | Disabled | ASC DEMO | Security Center recom... | yo |

©Microsoft Corporation
Azure

# Azure Policy Reference – By Name

- **Vulnerability Assessment Agent**
  - [Preview]: Configure machines to receive a vulnerability assessment provider
    - Above Policy currently doesn't support vm scale sets
- **Microsoft Dependency Agent**
  - Deploy Dependency agent for Linux virtual machines
  - Deploy - Configure Dependency agent to be enabled on Windows virtual machines
  - Configure Dependency agent on Azure Arc enabled Windows servers
  - Configure Dependency agent on Azure Arc enabled Linux servers
  - Deploy - Configure Dependency agent to be enabled on Windows virtual machine scale sets
  - Deploy Dependency agent for Linux virtual machine scale sets
- **Guest Configuration Agent**
  - Deploy the Linux Guest Configuration extension to enable Guest Configuration assignments on Linux VMs
  - Deploy the Windows Guest Configuration extension to enable Guest Configuration assignments on Windows VMs
  - [Preview]: Configure supported Linux virtual machine scale sets to automatically install the Guest Attestation extension
  - [Preview]: Configure supported Windows virtual machine scale sets to automatically install the Guest Attestation extension
  - [Preview]: Configure system-assigned managed identity to enable Azure Monitor assignments on VMs
  - No out of the box policies for ARC
- **Log Analytics Agent**
  - Deploy Log Analytics extension for Linux VMs
  - Deploy - Configure Log Analytics extension to be enabled on Windows virtual machines
  - Deploy - Configure Log Analytics extension to be enabled on Windows virtual machine scale sets
  - Deploy Log Analytics extension for Linux virtual machine scale sets
  - Configure Log Analytics extension on Azure Arc enabled Linux servers
  - Configure Log Analytics extension on Azure Arc enabled Windows servers
- **Log Analytics Workspace Settings**
  - Enable Security Center's auto provisioning of the Log Analytics agent on your subscriptions with custom workspace
  - Enable Security Center's auto provisioning of the Log Analytics agent on your subscriptions with default workspace
- **Enable Defender for Servers Plan**
  - Configure Microsoft Defender for servers to be enabled
  - No out of the box policies for enabling on the workspace

# Azure Policy Reference – Out of the Box Policies

## Agent Policies

| | Linux | Windows | Linux VMSS | Windows VMSS | Linux Arc | Windows Arc |
|---|---|---|---|---|---|---|
| Log Analytics | Deploy Policy | Deploy Policy | Deploy Policy | Deploy Policy | Deploy Policy | Deploy Policy |
| Dependency Agent | Deploy Policy | Deploy Policy | Deploy Policy | Deploy Policy | Deploy Policy | Deploy Policy |
| Guest Configuration | Deploy Policy | Deploy Policy | Deploy Policy | Deploy Policy | ✗ | ✗ |
| System Assigned Identity | Deploy Policy → | → | → | → | → | → |
| Vulnerability Agent | Deploy Policy → | → | ✗ | ✗ | → | → |

* **Vulnerability Agent:** Depends on your deployment, Assumes Integrated Qualys or Defender for Endpoint
* **System Assigned Identity:** A system Managed Identity is required for the Guest Configuration Agent
* **Arc Agent** must be manually installed on non-Azure machines first

## Defender for Servers Enablement Policies

| | Subscription | Log Analytics Workspace |
|---|---|---|
| Enable Defender for Servers | Deploy Policy | ✗ |
| Configure Security Events | ✗ | ✗ |

# References

## Adoption and Deployment

- Microsoft Defender for Cloud PoC Series - Defender for Servers - Microsoft Tech Community
- Microsoft Defender for Cloud — Price Estimation Dashboard

## Features and FAQ

- Microsoft Defender for servers - the benefits and features | Microsoft Docs
- Defender for Cloud FAQ - data collection and agents | Microsoft Docs
- Defender for Cloud FAQ - questions about existing Log Analytics agents | Microsoft Docs
- Release notes for Defender for Cloud | Microsoft Docs