Microsoft 365 Defender – Things you should go do

- Stefan Schörling, Onevinn
- Twitter @stefanschorling
- Microsoft MVP

- Mattias Borg, Onevinn
- Twitter @mattiasborg82
- Microsoft MVP

NORDIC – VIRTUAL SUMMIT –

But first – No sessions this year without ChatGPT

Yes, we asked ChatGPT for the top 5 must do things
as a SecOp and SecAdmin with Microsoft 365 Defender

5 Sec Ops must do things according to ChatGPT

As a security operator with Microsoft 365 Defender, here are five essential tasks you should do:

1. Investigate security incidents
2. Respond to threats
3. Monitor and maintain security
4. Stay informed: Keep up-to-date with the latest cybersecurity threats and trends
5. Report and document incidents

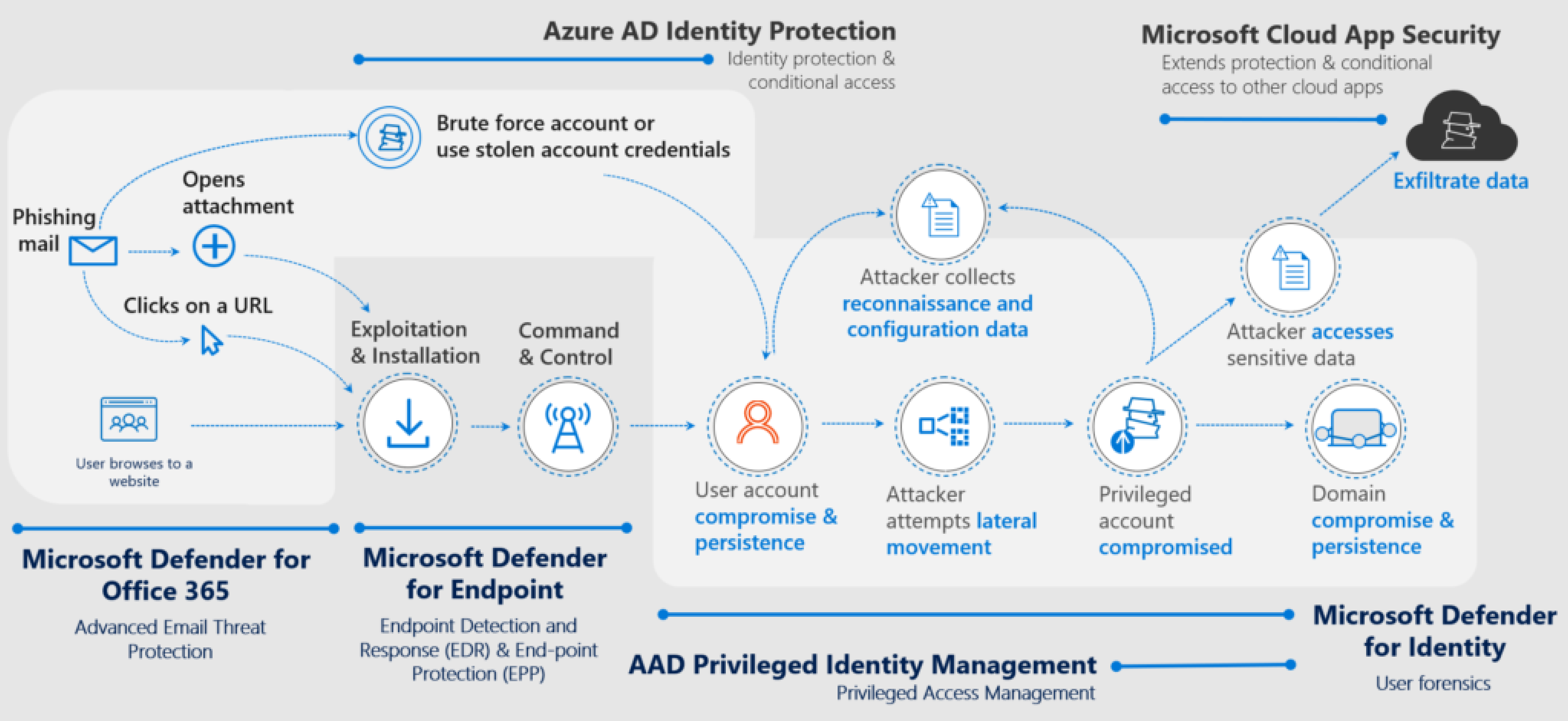
Introduction – M365Defender

Defender Overview

- **M365D – Microsoft 365 Defender**
  - *MDI – Microsoft Defender for Identity*
  - *MDCA – Microsoft Defender for Clous Apps*
  - *MDO – Microsoft Defender for Office*
  - MDE – Microsoft Defender for Endpoint
    - TVM Add-on

- MDC - Defender for Cloud
- *MDTI*
- *MD4IoT - Microsoft Defender for IoT*

XDR coverage



Azure AD Identity Protection
Identity protection & conditional access

Microsoft Cloud App Security
Extends protection & conditional access to other cloud apps

Brute force account or use stolen account credentials

Phishing mail

Opens attachment

Clicks on a URL

User browses to a website

Exploitation & Installation

Command & Control

User account compromise & persistence

Attacker collects reconnaissance and configuration data

Attacker attempts lateral movement

Privileged account compromised

Attacker accesses sensitive data

Exfiltrate data

Domain compromise & persistence

Microsoft Defender for Office 365
Advanced Email Threat Protection

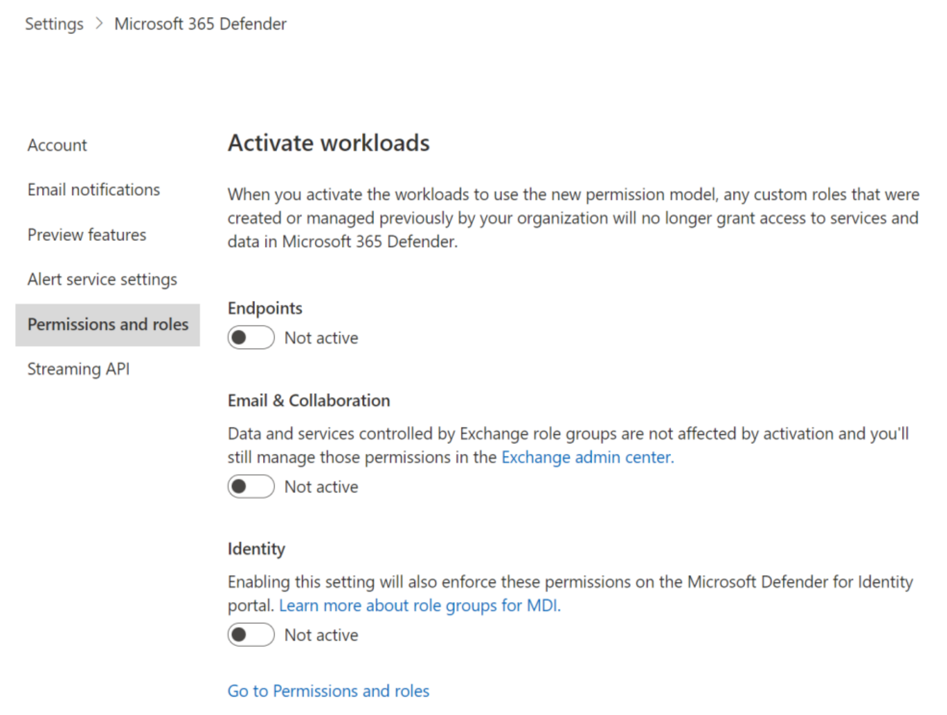
Microsoft Defender for Endpoint
Endpoint Detection and Response (EDR) & End-point Protection (EPP)

AAD Privileged Identity Management
Privileged Access Management

Microsoft Defender for Identity
User forensics

Things to do

M365D Unified RBAC



Settings > Microsoft 365 Defender

- Account
- Email notifications
- Preview features
- Alert service settings
- Permissions and roles
- Streaming API

Activate workloads

When you activate the workloads to use the new permission model, any custom roles that were created or managed previously by your organization will no longer grant access to services and data in Microsoft 365 Defender.

Endpoints

○ Not active

Email & Collaboration

Data and services controlled by Exchange role groups are not affected by activation and you'll still manage those permissions in the Exchange admin center.

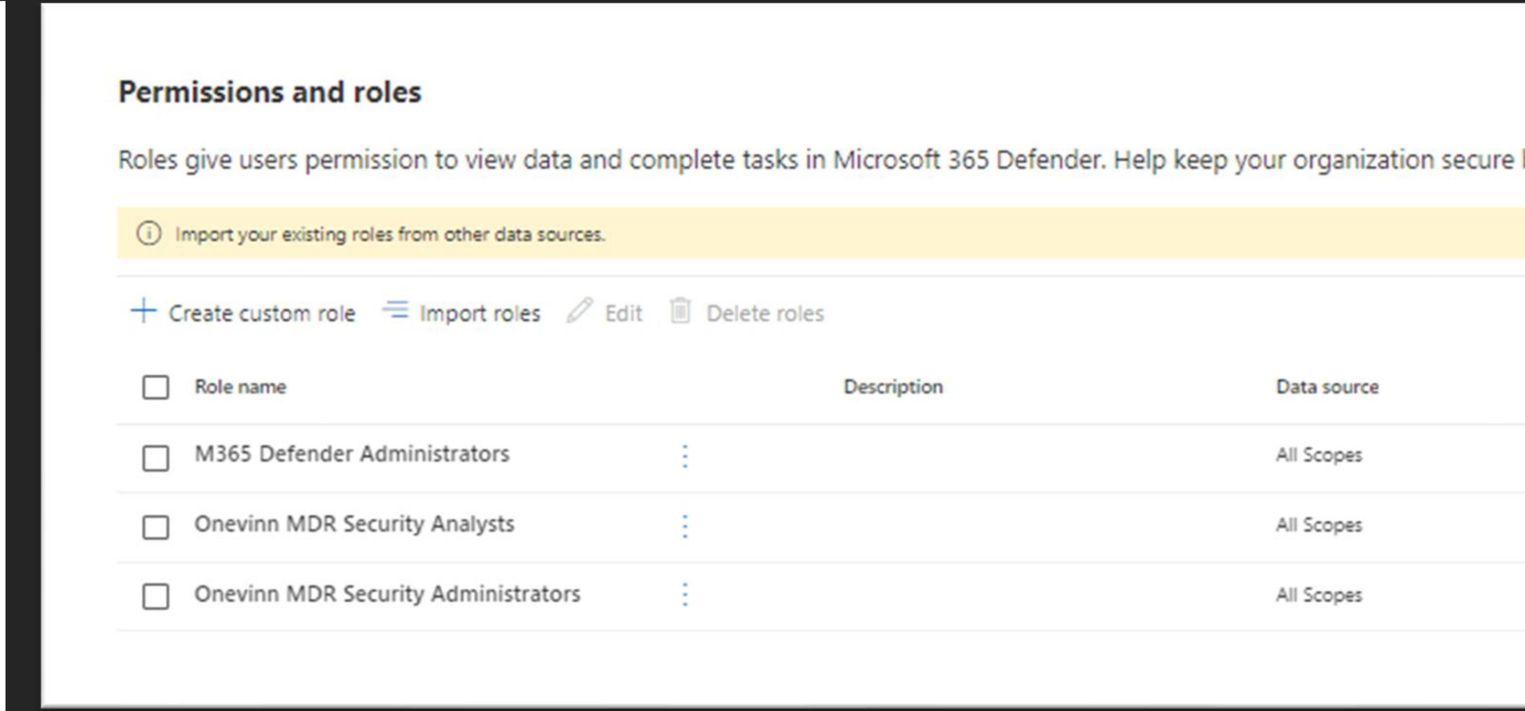
○ Not active

Identity

Enabling this setting will also enforce these permissions on the Microsoft Defender for Identity portal. Learn more about role groups for MDI.

○ Not active

Go to Permissions and roles



Permissions and roles

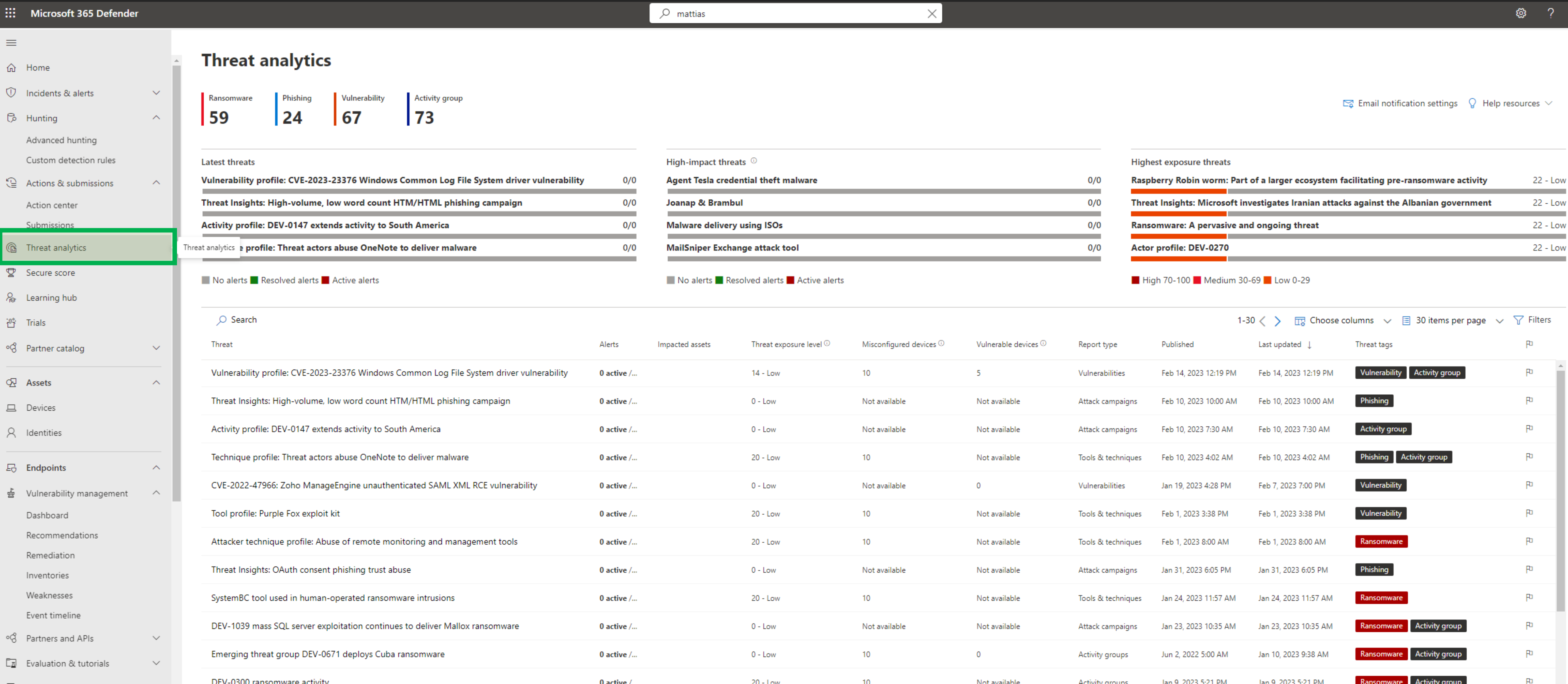
Roles give users permission to view data and complete tasks in Microsoft 365 Defender. Help keep your organization secure

ⓘ Import your existing roles from other data sources.

□	Role name	Description	Data source
□	M365 Defender Administrators		All Scopes
□	Onevinn MDR Security Analysts		All Scopes
□	Onevinn MDR Security Administrators		All Scopes

Use Threat Analytics

NORDIC
— VIRTUAL SUMMIT —



Threat analytics

Ransomware	Phishing	Vulnerability	Activity group
59	24	67	73

Latest threats

Vulnerability profile: CVE-2023-23376 Windows Common Log File System driver vulnerability	0/0
Threat Insights: High-volume, low word count HTM/HTML phishing campaign	0/0
Activity profile: DEV-0147 extends activity to South America	0/0
e profile: Threat actors abuse OneNote to deliver malware	0/0

■ No alerts ■ Resolved alerts ■ Active alerts

High-impact threats

Agent Tesla credential theft malware	0/0
Joanap & Brambul	0/0
Malware delivery using ISOs	0/0
MailSniper Exchange attack tool	0/0

■ No alerts ■ Resolved alerts ■ Active alerts

Highest exposure threats

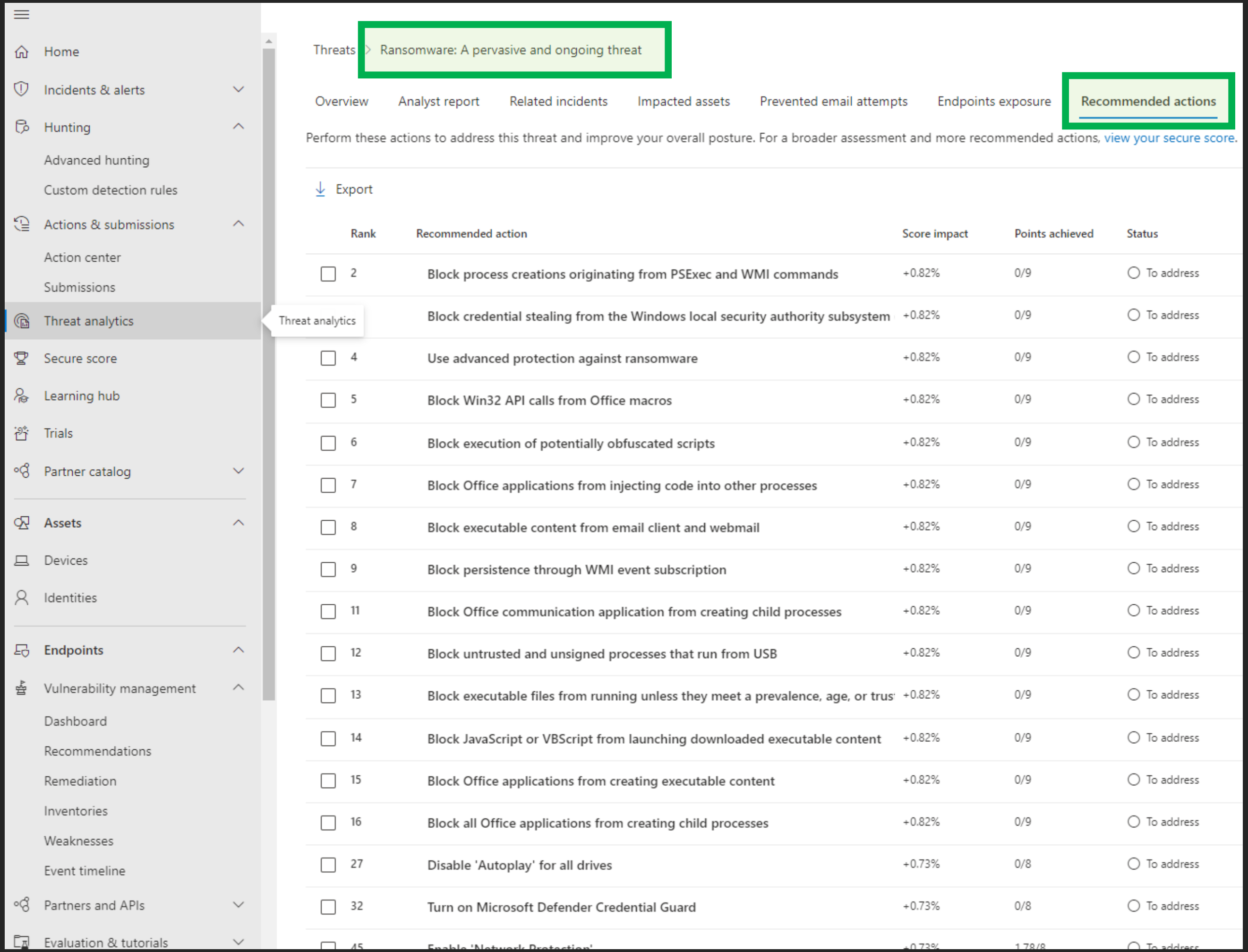
Raspberry Robin worm: Part of a larger ecosystem facilitating pre-ransomware activity	22 - Low
Threat Insights: Microsoft investigates Iranian attacks against the Albanian government	22 - Low
Ransomware: A pervasive and ongoing threat	22 - Low
Actor profile: DEV-0270	22 - Low

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

Threat	Alerts	Impacted assets	Threat exposure level	Misconfigured devices	Vulnerable devices	Report type	Published	Last updated ↓	Threat tags
Vulnerability profile: CVE-2023-23376 Windows Common Log File System driver vulnerability	**0 active** /...		14 - Low	10	5	Vulnerabilities	Feb 14, 2023 12:19 PM	Feb 14, 2023 12:19 PM	Vulnerability Activity group
Threat Insights: High-volume, low word count HTM/HTML phishing campaign	**0 active** /...		0 - Low	Not available	Not available	Attack campaigns	Feb 10, 2023 10:00 AM	Feb 10, 2023 10:00 AM	Phishing
Activity profile: DEV-0147 extends activity to South America	**0 active** /...		0 - Low	Not available	Not available	Attack campaigns	Feb 10, 2023 7:30 AM	Feb 10, 2023 7:30 AM	Activity group
Technique profile: Threat actors abuse OneNote to deliver malware	**0 active** /...		20 - Low	10	Not available	Tools & techniques	Feb 10, 2023 4:02 AM	Feb 10, 2023 4:02 AM	Phishing Activity group
CVE-2022-47966: Zoho ManageEngine unauthenticated SAML XML RCE vulnerability	**0 active** /...		0 - Low	Not available	0	Vulnerabilities	Jan 19, 2023 4:28 PM	Feb 7, 2023 7:00 PM	Vulnerability
Tool profile: Purple Fox exploit kit	**0 active** /...		20 - Low	10	Not available	Tools & techniques	Feb 1, 2023 3:38 PM	Feb 1, 2023 3:38 PM	Vulnerability
Attacker technique profile: Abuse of remote monitoring and management tools	**0 active** /...		20 - Low	10	Not available	Tools & techniques	Feb 1, 2023 8:00 AM	Feb 1, 2023 8:00 AM	Ransomware
Threat Insights: OAuth consent phishing trust abuse	**0 active** /...		0 - Low	Not available	Not available	Attack campaigns	Jan 31, 2023 6:05 PM	Jan 31, 2023 6:05 PM	Phishing
SystemBC tool used in human-operated ransomware intrusions	**0 active** /...		20 - Low	10	Not available	Tools & techniques	Jan 24, 2023 11:57 AM	Jan 24, 2023 11:57 AM	Ransomware
DEV-1039 mass SQL server exploitation continues to deliver Mallox ransomware	**0 active** /...		0 - Low	Not available	Not available	Attack campaigns	Jan 23, 2023 10:35 AM	Jan 23, 2023 10:35 AM	Ransomware Activity group
Emerging threat group DEV-0671 deploys Cuba ransomware	**0 active** /...		0 - Low	10	0	Activity groups	Jun 2, 2022 5:00 AM	Jan 10, 2023 9:38 AM	Ransomware Activity group
DEV-0300 ransomware activity	**0 active** /...		20 - Low	10	Not available	Activity groups	Jan 9, 2023 5:21 PM	Jan 9, 2023 5:21 PM	Ransomware Activity group

Use Threat Analytics

- Human operated ransomware



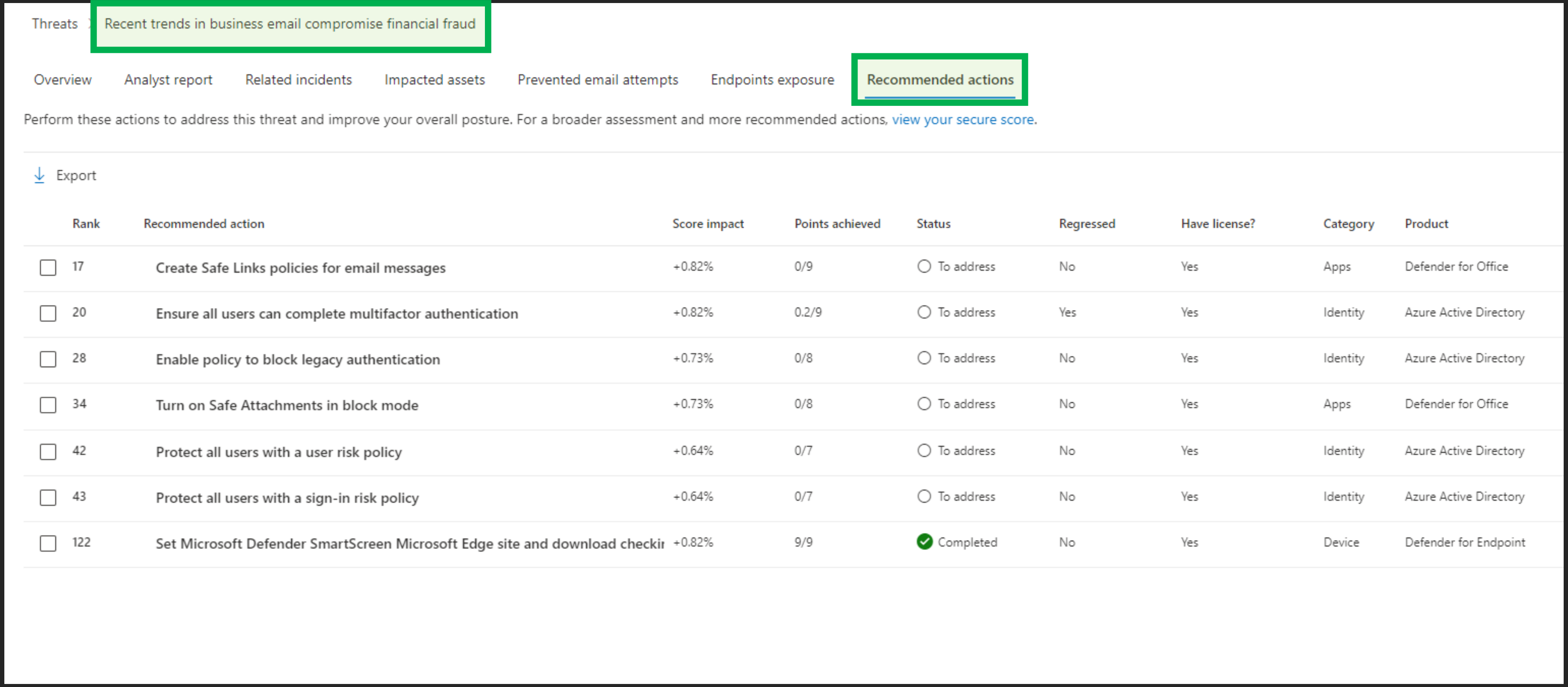
Perform these actions to address this threat and improve your overall posture. For a broader assessment and more recommended actions, view your secure score.

	Rank	Recommended action	Score impact	Points achieved	Status
□	2	Block process creations originating from PSExec and WMI commands	+0.82%	0/9	○ To address
		Block credential stealing from the Windows local security authority subsystem	+0.82%	0/9	○ To address
□	4	Use advanced protection against ransomware	+0.82%	0/9	○ To address
□	5	Block Win32 API calls from Office macros	+0.82%	0/9	○ To address
□	6	Block execution of potentially obfuscated scripts	+0.82%	0/9	○ To address
□	7	Block Office applications from injecting code into other processes	+0.82%	0/9	○ To address
□	8	Block executable content from email client and webmail	+0.82%	0/9	○ To address
□	9	Block persistence through WMI event subscription	+0.82%	0/9	○ To address
□	11	Block Office communication application from creating child processes	+0.82%	0/9	○ To address
□	12	Block untrusted and unsigned processes that run from USB	+0.82%	0/9	○ To address
□	13	Block executable files from running unless they meet a prevalence, age, or trus	+0.82%	0/9	○ To address
□	14	Block JavaScript or VBScript from launching downloaded executable content	+0.82%	0/9	○ To address
□	15	Block Office applications from creating executable content	+0.82%	0/9	○ To address
□	16	Block all Office applications from creating child processes	+0.82%	0/9	○ To address
□	27	Disable 'Autoplay' for all drives	+0.73%	0/8	○ To address
□	32	Turn on Microsoft Defender Credential Guard	+0.73%	0/8	○ To address
□	45	Enable 'Network Protection'	+0.73%	1.78/8	○ To address

https://security.microsoft.com/threatanalytics3/05658b6c-dc62-496d-ad3c-c6a795a33c27/recommendedActions

Use Threat Analytics

- Business email compromise



Threats > Recent trends in business email compromise financial fraud

Perform these actions to address this threat and improve your overall posture. For a broader assessment and more recommended actions, view your secure score.

	Rank	Recommended action	Score impact	Points achieved	Status	Regressed	Have license?	Category	Product
□	17	Create Safe Links policies for email messages	+0.82%	0/9	○ To address	No	Yes	Apps	Defender for Office
□	20	Ensure all users can complete multifactor authentication	+0.82%	0.2/9	○ To address	Yes	Yes	Identity	Azure Active Directory
□	28	Enable policy to block legacy authentication	+0.73%	0/8	○ To address	No	Yes	Identity	Azure Active Directory
□	34	Turn on Safe Attachments in block mode	+0.73%	0/8	○ To address	No	Yes	Apps	Defender for Office
□	42	Protect all users with a user risk policy	+0.64%	0/7	○ To address	No	Yes	Identity	Azure Active Directory
□	43	Protect all users with a sign-in risk policy	+0.64%	0/7	○ To address	No	Yes	Identity	Azure Active Directory
□	122	Set Microsoft Defender SmartScreen Microsoft Edge site and download checkir	+0.82%	9/9	✓ Completed	No	Yes	Device	Defender for Endpoint

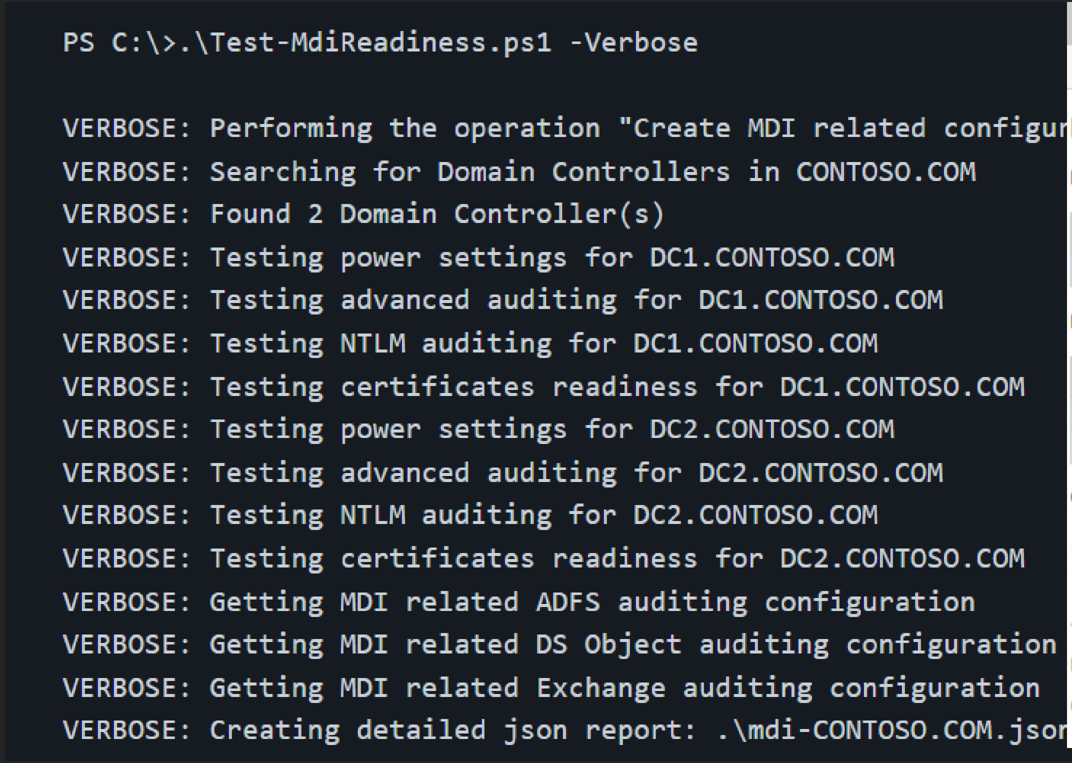
https://security.microsoft.com/threatanalytics3/eedf4df4-df1e-410f-a063-071ab75d2c68/recommendedActions

MDI

Microsoft Defender for Identity

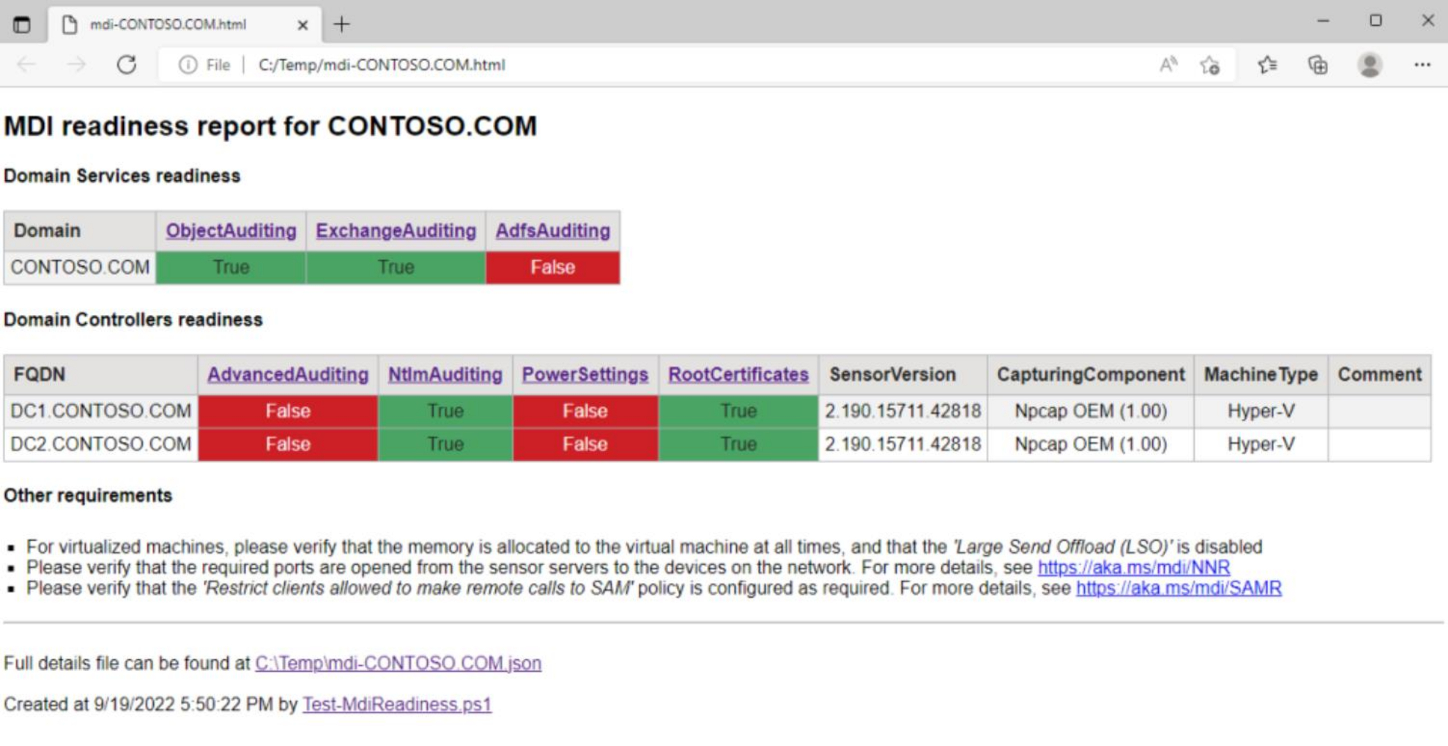
MDI Readiness

NORDIC
— VIRTUAL SUMMIT —



```
PS C:\>.\Test-MdiReadiness.ps1 -Verbose

VERBOSE: Performing the operation "Create MDI related configur
VERBOSE: Searching for Domain Controllers in CONTOSO.COM
VERBOSE: Found 2 Domain Controller(s)
VERBOSE: Testing power settings for DC1.CONTOSO.COM
VERBOSE: Testing advanced auditing for DC1.CONTOSO.COM
VERBOSE: Testing NTLM auditing for DC1.CONTOSO.COM
VERBOSE: Testing certificates readiness for DC1.CONTOSO.COM
VERBOSE: Testing power settings for DC2.CONTOSO.COM
VERBOSE: Testing advanced auditing for DC2.CONTOSO.COM
VERBOSE: Testing NTLM auditing for DC2.CONTOSO.COM
VERBOSE: Testing certificates readiness for DC2.CONTOSO.COM
VERBOSE: Getting MDI related ADFS auditing configuration
VERBOSE: Getting MDI related DS Object auditing configuration
VERBOSE: Getting MDI related Exchange auditing configuration
VERBOSE: Creating detailed json report: .\mdi-CONTOSO.COM.jsor
```



MDI readiness report for CONTOSO.COM

Domain Services readiness

Domain	ObjectAuditing	ExchangeAuditing	AdfsAuditing
CONTOSO.COM	True	True	False

Domain Controllers readiness

FQDN	AdvancedAuditing	NtlmAuditing	PowerSettings	RootCertificates	SensorVersion	CapturingComponent	MachineType	Comment
DC1.CONTOSO.COM	False	True	False	True	2.190.15711.42818	Npcap OEM (1.00)	Hyper-V	
DC2.CONTOSO.COM	False	True	False	True	2.190.15711.42818	Npcap OEM (1.00)	Hyper-V	

Other requirements

- For virtualized machines, please verify that the memory is allocated to the virtual machine at all times, and that the *'Large Send Offload (LSO)'* is disabled
- Please verify that the required ports are opened from the sensor servers to the devices on the network. For more details, see https://aka.ms/mdi/NNR
- Please verify that the *'Restrict clients allowed to make remote calls to SAM'* policy is configured as required. For more details, see https://aka.ms/mdi/SAMR

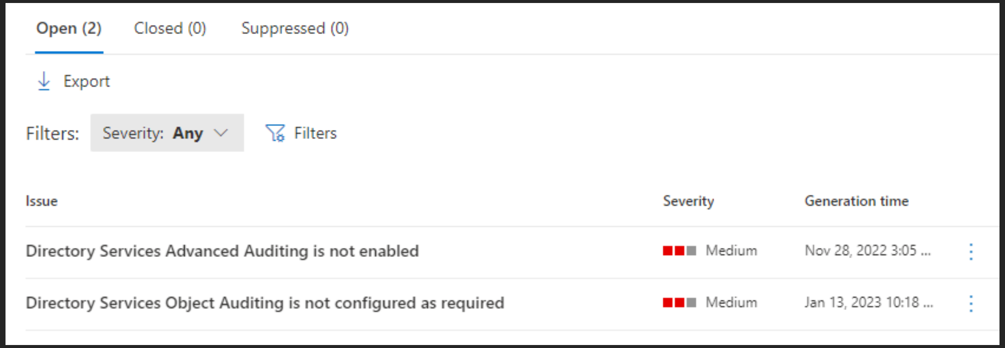
Full details file can be found at C:\Temp\mdi-CONTOSO.COM.json

Created at 9/19/2022 5:50:22 PM by Test-MdiReadiness.ps1

https://github.com/microsoft/Microsoft-Defender-for-Identity/tree/main/Test-MdiReadiness

MDI – Health alerts

- NTLM Auditing is not enabled
- Directory Services Advanced Auditing is not enabled as required
- Directory Services Object Auditing is not enabled as required
- Power mode is not configured for optimal processor performance



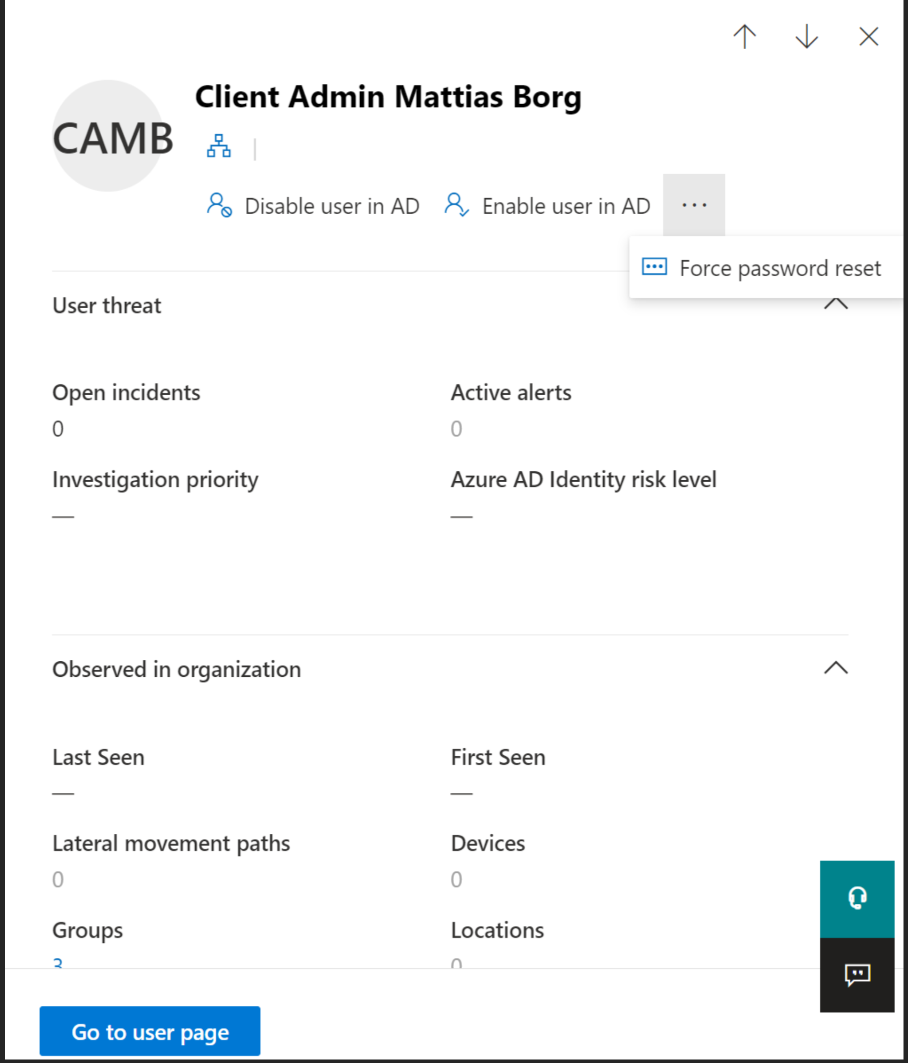
Issue	Severity	Generation time
Directory Services Advanced Auditing is not enabled	■■■ Medium	Nov 28, 2022 3:05 ...
Directory Services Object Auditing is not configured as required	■■■ Medium	Jan 13, 2023 10:18 ...

https://learn.microsoft.com/en-us/defender-for-identity/health-alerts

MDI Actions

- Disable user in AD
- Enable user in AD
- Force Password reset

- Requires gMSA account for custom delegation of permissions



Client Admin Mattias Borg

Open incidents: 0

Active alerts: 0

Investigation priority: —

Azure AD Identity risk level: —

Last Seen: —

First Seen: —

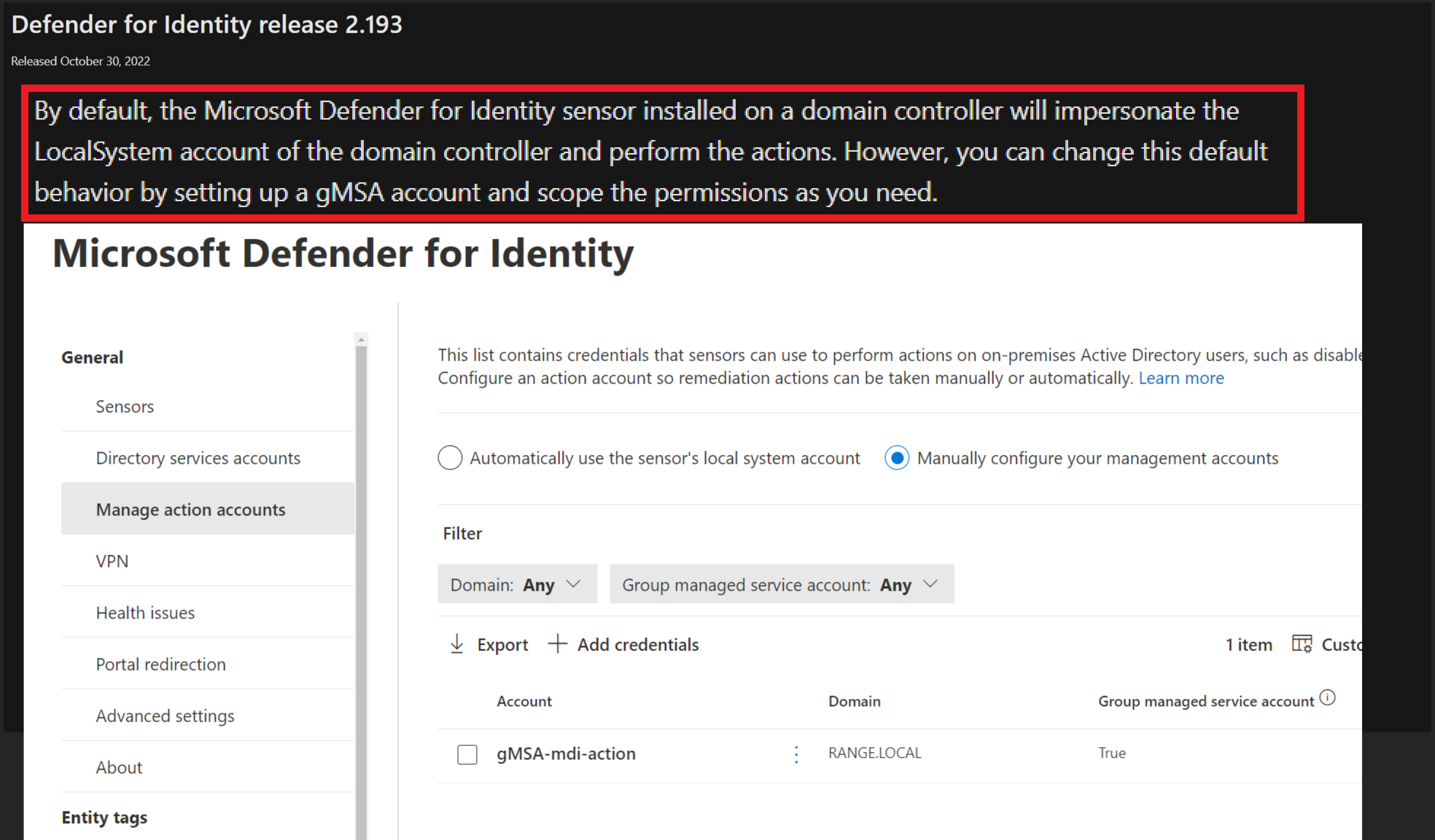
Lateral movement paths: 0

Devices: 0

Groups: 3

Locations: 0

MDI Action Account



Defender for Identity release 2.193

Released October 30, 2022

By default, the Microsoft Defender for Identity sensor installed on a domain controller will impersonate the LocalSystem account of the domain controller and perform the actions. However, you can change this default behavior by setting up a gMSA account and scope the permissions as you need.

Microsoft Defender for Identity

This list contains credentials that sensors can use to perform actions on on-premises Active Directory users, such as disable
Configure an action account so remediation actions can be taken manually or automatically. Learn more

○ Automatically use the sensor's local system account ● Manually configure your management accounts

	Account	Domain	Group managed service account
□	gMSA-mdi-action	RANGE.LOCAL	True

MDI Action Account Troubleshooting

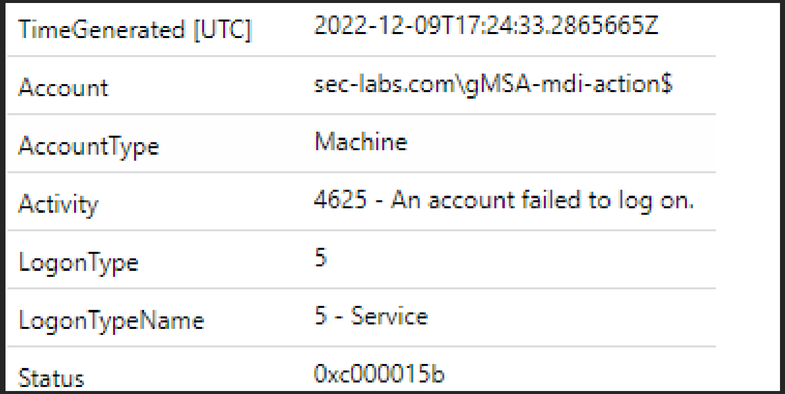
- Wrong Account Type
- Not allowed to logon as service
- Permissions

Events with the configured MDI account (Requires central logging)

```
SecurityEvent
| where Account has "gMSA-MDIAction$“
```

Portal action events by the configured MDI account (Requires central logging)

```
SecurityEvent
| where EventID in(4738,4725,4722)
| where Account has "gMSA-mdi-action$" //mdi account account name
| where TargetAccount contains "test" //the user you want to take action on
```



TimeGenerated [UTC]	2022-12-09T17:24:33.2865665Z
Account	sec-labs.com\gMSA-mdi-action$
AccountType	Machine
Activity	4625 - An account failed to log on.
LogonType	5
LogonTypeName	5 - Service
Status	0xc000015b

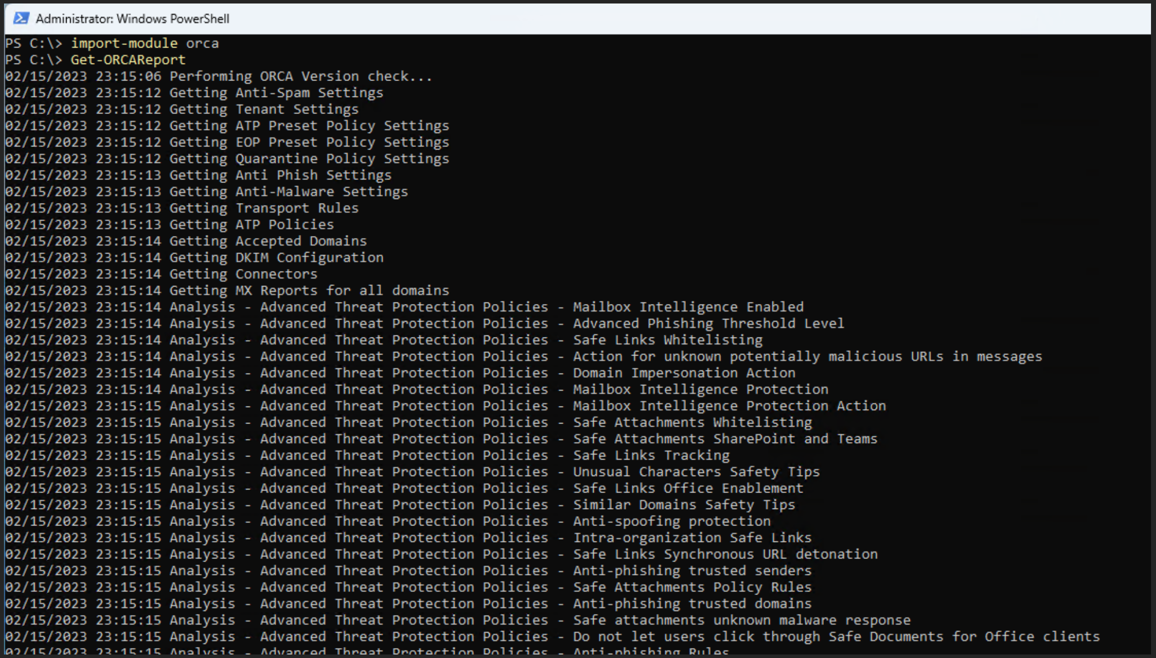
https://blog.sec-labs.com/2023/01/taking-actions-on-on-prem-accounts-with-mdi-action-account-troubleshooting

MDO

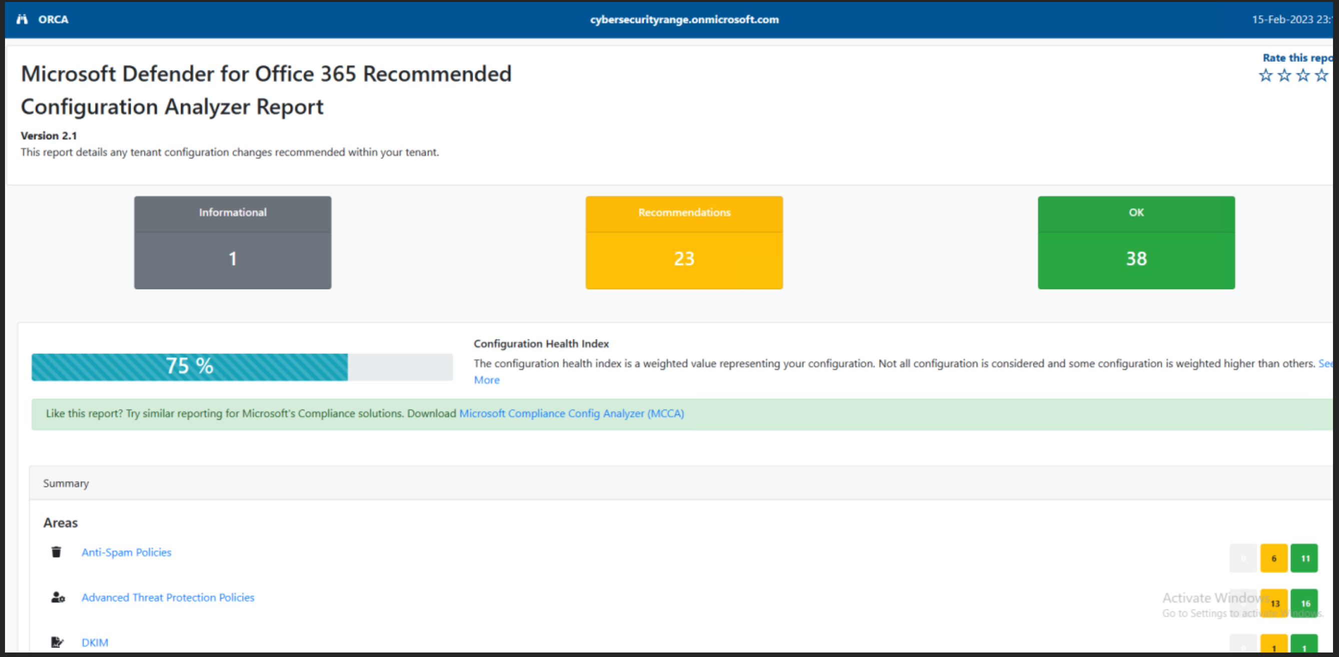
Microsoft Defender for Office

Old School - ORCA

- **Install-Module -Name ORCA**
- **Get-ORCAReport**



```
PS C:\> import-module orca
PS C:\> Get-ORCAReport
02/15/2023 23:15:06 Performing ORCA Version check...
02/15/2023 23:15:12 Getting Anti-Spam Settings
02/15/2023 23:15:12 Getting Tenant Settings
02/15/2023 23:15:12 Getting ATP Preset Policy Settings
02/15/2023 23:15:12 Getting EOP Preset Policy Settings
02/15/2023 23:15:12 Getting Quarantine Policy Settings
02/15/2023 23:15:13 Getting Anti Phish Settings
02/15/2023 23:15:13 Getting Anti-Malware Settings
02/15/2023 23:15:13 Getting Transport Rules
02/15/2023 23:15:13 Getting ATP Policies
02/15/2023 23:15:14 Getting Accepted Domains
02/15/2023 23:15:14 Getting DKIM Configuration
02/15/2023 23:15:14 Getting Connectors
02/15/2023 23:15:14 Getting MX Reports for all domains
02/15/2023 23:15:14 Analysis - Advanced Threat Protection Policies - Mailbox Intelligence Enabled
02/15/2023 23:15:14 Analysis - Advanced Threat Protection Policies - Advanced Phishing Threshold Level
02/15/2023 23:15:14 Analysis - Advanced Threat Protection Policies - Safe Links Whitelisting
02/15/2023 23:15:14 Analysis - Advanced Threat Protection Policies - Action for unknown potentially malicious URLs in messages
02/15/2023 23:15:14 Analysis - Advanced Threat Protection Policies - Domain Impersonation Action
02/15/2023 23:15:14 Analysis - Advanced Threat Protection Policies - Mailbox Intelligence Protection
02/15/2023 23:15:15 Analysis - Advanced Threat Protection Policies - Mailbox Intelligence Protection Action
02/15/2023 23:15:15 Analysis - Advanced Threat Protection Policies - Safe Attachments Whitelisting
02/15/2023 23:15:15 Analysis - Advanced Threat Protection Policies - Safe Attachments SharePoint and Teams
02/15/2023 23:15:15 Analysis - Advanced Threat Protection Policies - Safe Links Tracking
02/15/2023 23:15:15 Analysis - Advanced Threat Protection Policies - Unusual Characters Safety Tips
02/15/2023 23:15:15 Analysis - Advanced Threat Protection Policies - Safe Links Office Enablement
02/15/2023 23:15:15 Analysis - Advanced Threat Protection Policies - Similar Domains Safety Tips
02/15/2023 23:15:15 Analysis - Advanced Threat Protection Policies - Anti-spoofing protection
02/15/2023 23:15:15 Analysis - Advanced Threat Protection Policies - Intra-organization Safe Links
02/15/2023 23:15:15 Analysis - Advanced Threat Protection Policies - Safe Links Synchronous URL detonation
02/15/2023 23:15:15 Analysis - Advanced Threat Protection Policies - Anti-phishing trusted senders
02/15/2023 23:15:15 Analysis - Advanced Threat Protection Policies - Safe Attachments Policy Rules
02/15/2023 23:15:15 Analysis - Advanced Threat Protection Policies - Anti-phishing trusted domains
02/15/2023 23:15:15 Analysis - Advanced Threat Protection Policies - Safe attachments unknown malware response
02/15/2023 23:15:15 Analysis - Advanced Threat Protection Policies - Do not let users click through Safe Documents for Office clients
02/15/2023 23:15:15 Analysis - Advanced Threat Protection Policies - Anti-phishing Rules
```



Microsoft Defender for Office 365 Recommended Configuration Analyzer Report

Version 2.1

This report details any tenant configuration changes recommended within your tenant.

Informational	Recommendations	OK
1	23	38

75 %

Configuration Health Index

The configuration health index is a weighted value representing your configuration. Not all configuration is considered and some configuration is weighted higher than others. See More

Like this report? Try similar reporting for Microsoft's Compliance solutions. Download Microsoft Compliance Config Analyzer (MCCA)

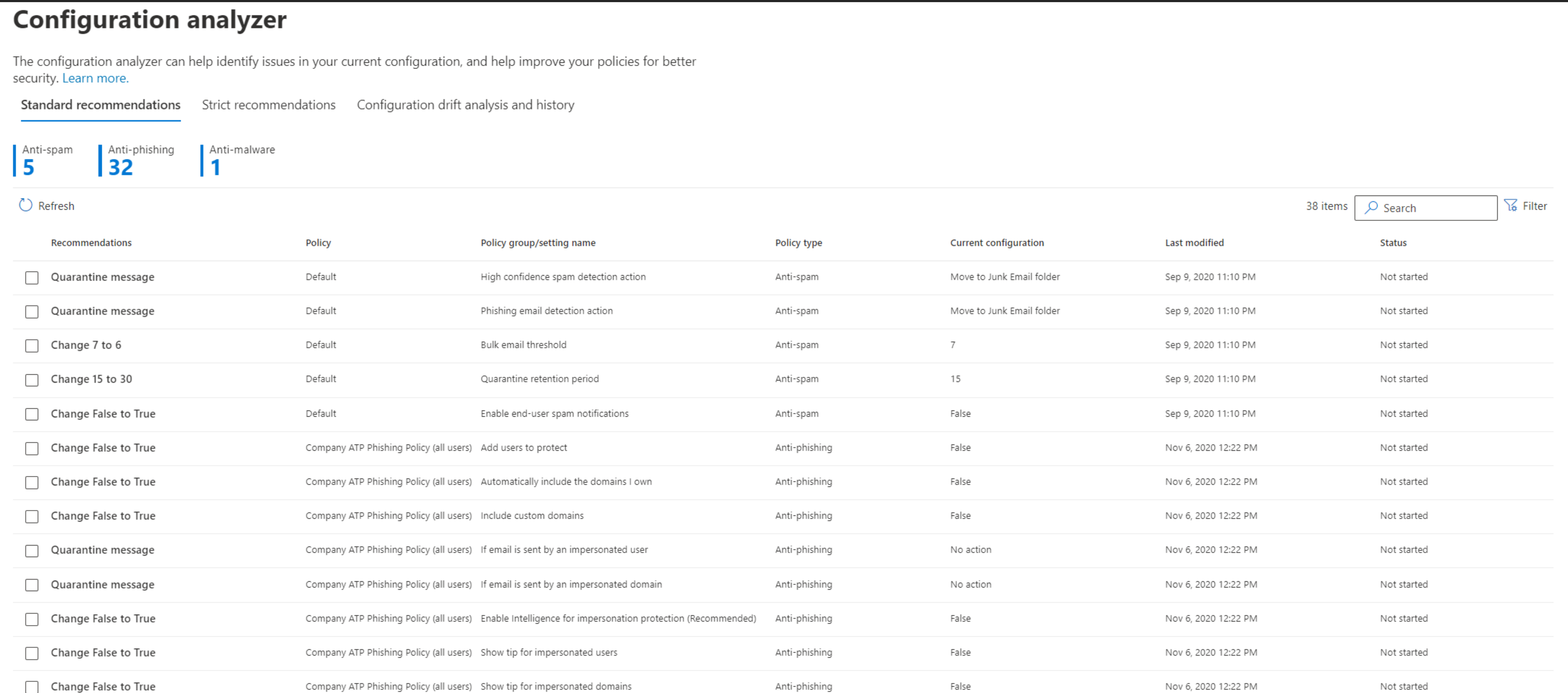
Summary

Areas

Anti-Spam Policies	0	6	11
Advanced Threat Protection Policies	0	13	16
DKIM	0	1	1

https://www.powershellgallery.com/packages/ORCA

New School - Configuration Analyzer



Configuration analyzer

The configuration analyzer can help identify issues in your current configuration, and help improve your policies for better security. Learn more.

Anti-spam	Anti-phishing	Anti-malware
5	32	1

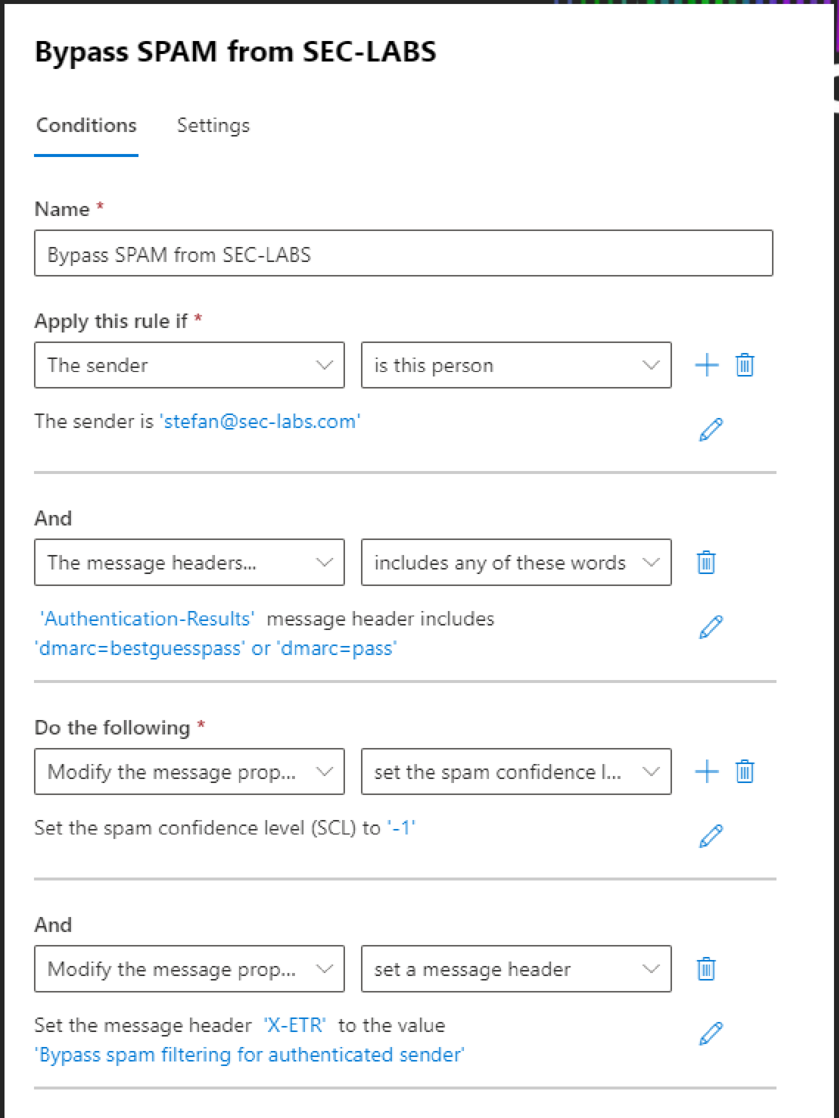
	Recommendations	Policy	Policy group/setting name	Policy type	Current configuration	Last modified	Status
□	Quarantine message	Default	High confidence spam detection action	Anti-spam	Move to Junk Email folder	Sep 9, 2020 11:10 PM	Not started
□	Quarantine message	Default	Phishing email detection action	Anti-spam	Move to Junk Email folder	Sep 9, 2020 11:10 PM	Not started
□	Change 7 to 6	Default	Bulk email threshold	Anti-spam	7	Sep 9, 2020 11:10 PM	Not started
□	Change 15 to 30	Default	Quarantine retention period	Anti-spam	15	Sep 9, 2020 11:10 PM	Not started
□	Change False to True	Default	Enable end-user spam notifications	Anti-spam	False	Sep 9, 2020 11:10 PM	Not started
□	Change False to True	Company ATP Phishing Policy (all users)	Add users to protect	Anti-phishing	False	Nov 6, 2020 12:22 PM	Not started
□	Change False to True	Company ATP Phishing Policy (all users)	Automatically include the domains I own	Anti-phishing	False	Nov 6, 2020 12:22 PM	Not started
□	Change False to True	Company ATP Phishing Policy (all users)	Include custom domains	Anti-phishing	False	Nov 6, 2020 12:22 PM	Not started
□	Quarantine message	Company ATP Phishing Policy (all users)	If email is sent by an impersonated user	Anti-phishing	No action	Nov 6, 2020 12:22 PM	Not started
□	Quarantine message	Company ATP Phishing Policy (all users)	If email is sent by an impersonated domain	Anti-phishing	No action	Nov 6, 2020 12:22 PM	Not started
□	Change False to True	Company ATP Phishing Policy (all users)	Enable Intelligence for impersonation protection (Recommended)	Anti-phishing	False	Nov 6, 2020 12:22 PM	Not started
□	Change False to True	Company ATP Phishing Policy (all users)	Show tip for impersonated users	Anti-phishing	False	Nov 6, 2020 12:22 PM	Not started
□	Change False to True	Company ATP Phishing Policy (all users)	Show tip for impersonated domains	Anti-phishing	False	Nov 6, 2020 12:22 PM	Not started

MDO go do

- Configuration Analyzer
- EOP Hardening
    - Allowed filetypes
- Move e-mail actions to Quarantine
- Reduce Allow lists in favor for stricter Exchange Transport Rules
    - Sender + DMARC set SCL -1
- Look for policies overriding threat

Advanced Hunting – Emails with threat detection and overriding policy

```
EmailEvents
| where isnotempty(ThreatTypes ) and
        OrgLevelAction == "Allow"
| summarize count() by OrgLevelPolicy
```



Bypass SPAM from SEC-LABS

Name *

Bypass SPAM from SEC-LABS

Apply this rule if *

The sender | is this person

The sender is 'stefan@sec-labs.com'

And

The message headers... | includes any of these words

'Authentication-Results' message header includes 'dmarc=bestguesspass' or 'dmarc=pass'

Do the following *

Modify the message prop... | set the spam confidence l...

Set the spam confidence level (SCL) to '-1'

And

Modify the message prop... | set a message header

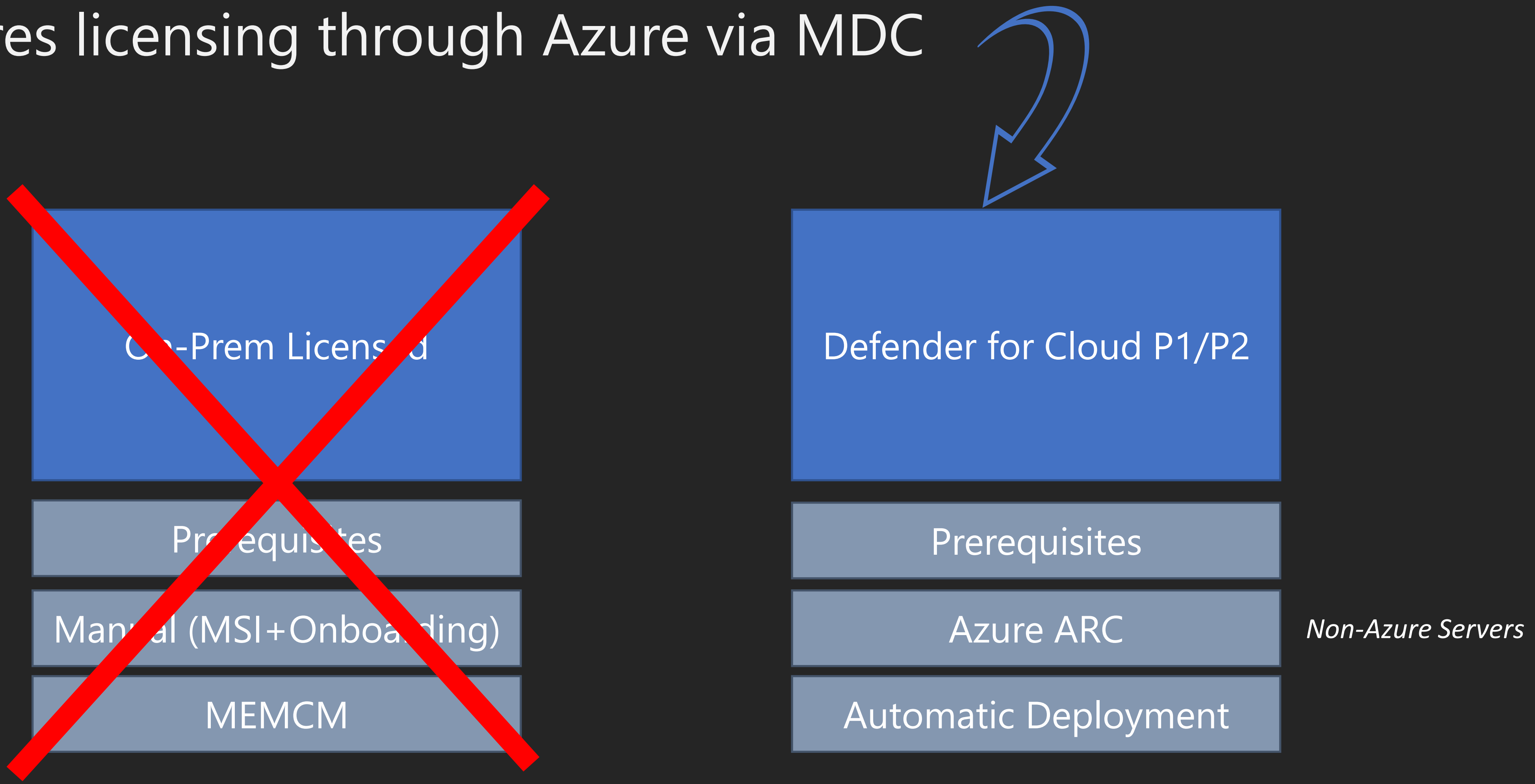
Set the message header 'X-ETR' to the value 'Bypass spam filtering for authenticated sender'

MDE for Servers

Microsoft Defender for Endpoints for Servers

Red or Blue Pill – Not any more

Requires licensing through Azure via MDC



~~On-Prem Licensed~~

~~Prerequisites~~

~~Manual (MSI+Onboarding)~~

~~MEMCM~~

Defender for Cloud P1/P2

Prerequisites

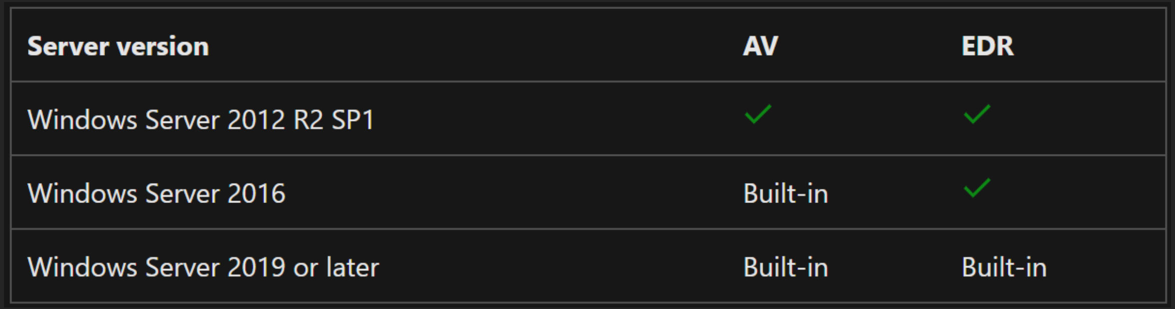
Azure ARC

Automatic Deployment

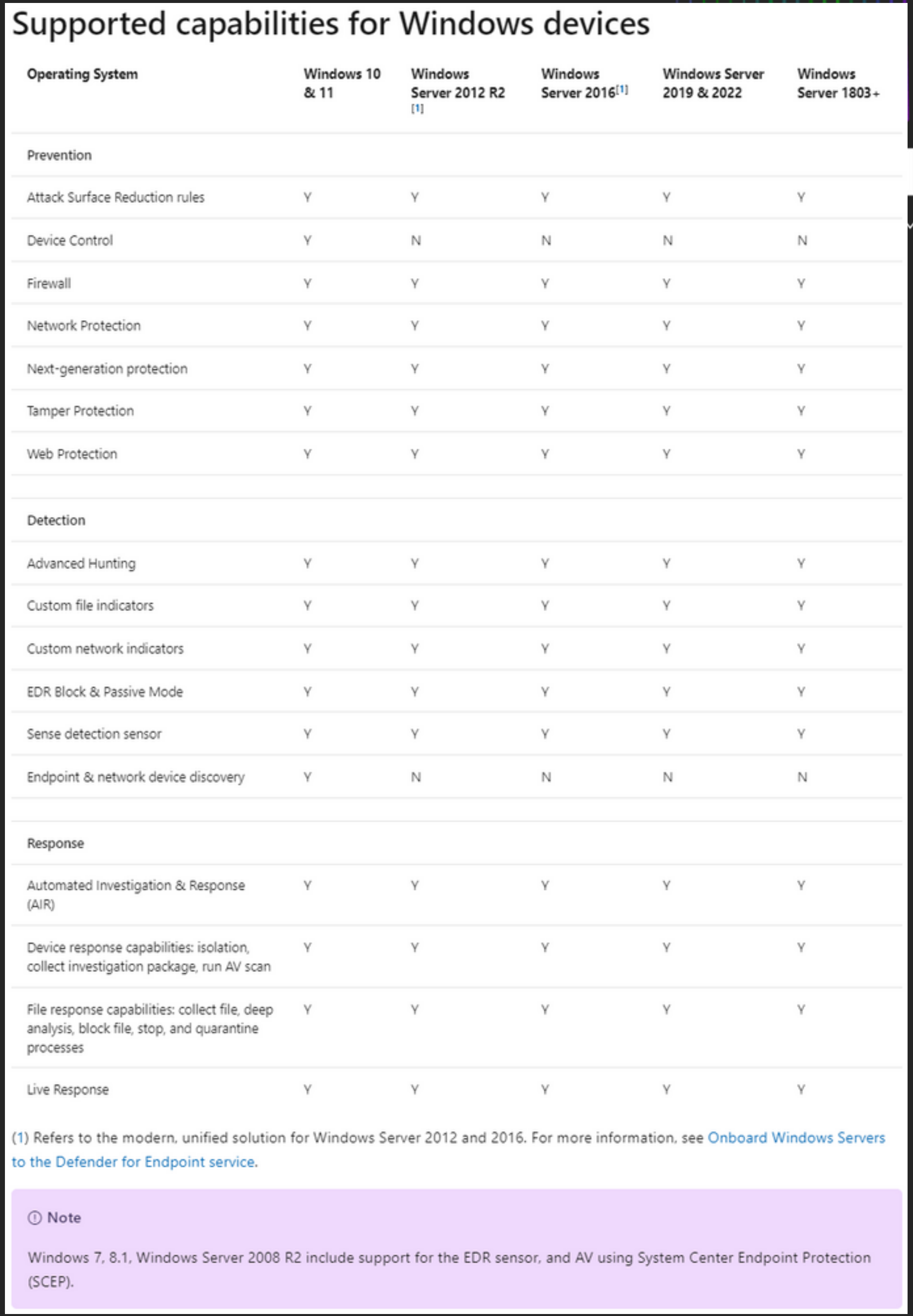
Non-Azure Servers

MDE unified agent

- April 2021 New Server Agent GA (2012 R2 / 2016)
- MMA Agent EOL August 2024
- Feature parity with clients



Server version	AV	EDR
Windows Server 2012 R2 SP1	✓	✓
Windows Server 2016	Built-in	✓
Windows Server 2019 or later	Built-in	Built-in



Supported capabilities for Windows devices

Operating System	Windows 10 & 11	Windows Server 2012 R2 [1]	Windows Server 2016[1]	Windows Server 2019 & 2022	Windows Server 1803+
Prevention					
Attack Surface Reduction rules	Y	Y	Y	Y	Y
Device Control	Y	N	N	N	N
Firewall	Y	Y	Y	Y	Y
Network Protection	Y	Y	Y	Y	Y
Next-generation protection	Y	Y	Y	Y	Y
Tamper Protection	Y	Y	Y	Y	Y
Web Protection	Y	Y	Y	Y	Y
Detection					
Advanced Hunting	Y	Y	Y	Y	Y
Custom file indicators	Y	Y	Y	Y	Y
Custom network indicators	Y	Y	Y	Y	Y
EDR Block & Passive Mode	Y	Y	Y	Y	Y
Sense detection sensor	Y	Y	Y	Y	Y
Endpoint & network device discovery	Y	N	N	N	N
Response					
Automated Investigation & Response (AIR)	Y	Y	Y	Y	Y
Device response capabilities: isolation, collect investigation package, run AV scan	Y	Y	Y	Y	Y
File response capabilities: collect file, deep analysis, block file, stop, and quarantine processes	Y	Y	Y	Y	Y
Live Response	Y	Y	Y	Y	Y

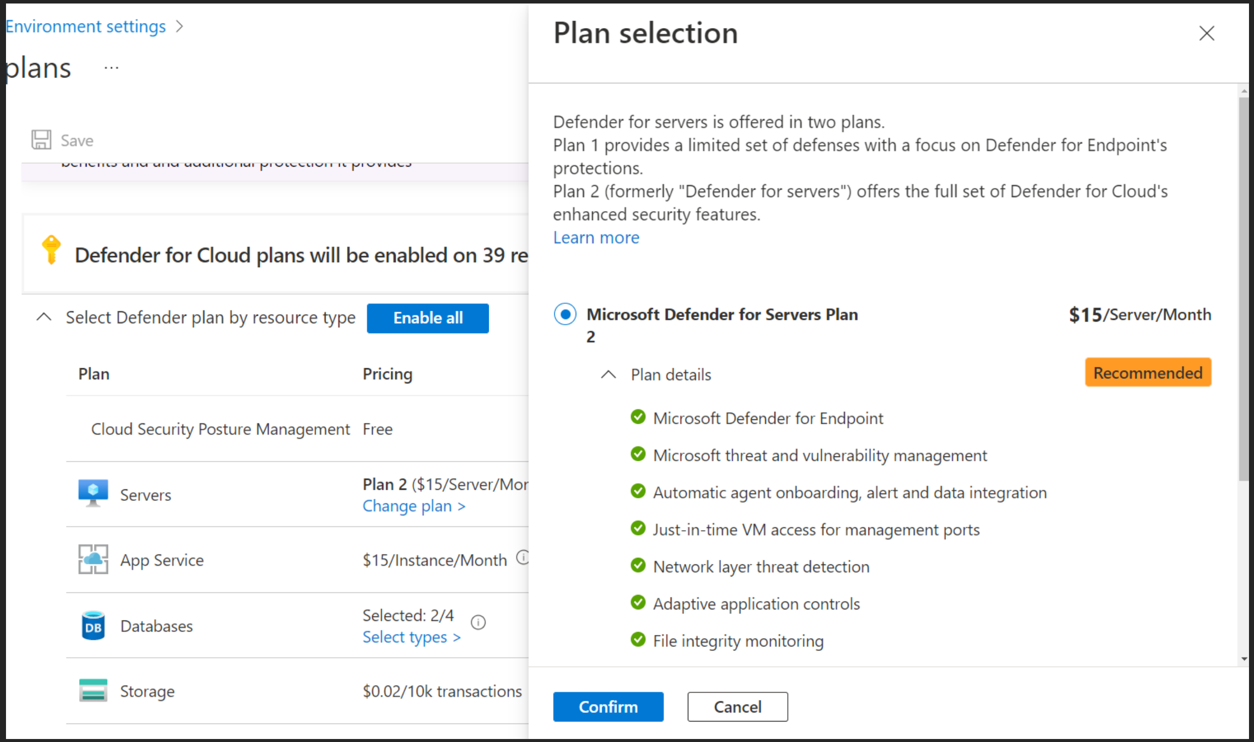
(1) Refers to the modern, unified solution for Windows Server 2012 and 2016. For more information, see Onboard Windows Servers to the Defender for Endpoint service.

ⓘ Note

Windows 7, 8.1, Windows Server 2008 R2 include support for the EDR sensor, and AV using System Center Endpoint Protection (SCEP).

Deploy with Defender for Cloud

- Enable unified solution



Environment settings >

plans ···

Save

Defender for Cloud plans will be enabled on 39 re

Select Defender plan by resource type

Plan	Pricing
Cloud Security Posture Management	Free
Servers	**Plan 2** ($15/Server/Mor Change plan >
App Service	$15/Instance/Month
Databases	Selected: 2/4 Select types >
Storage	$0.02/10k transactions

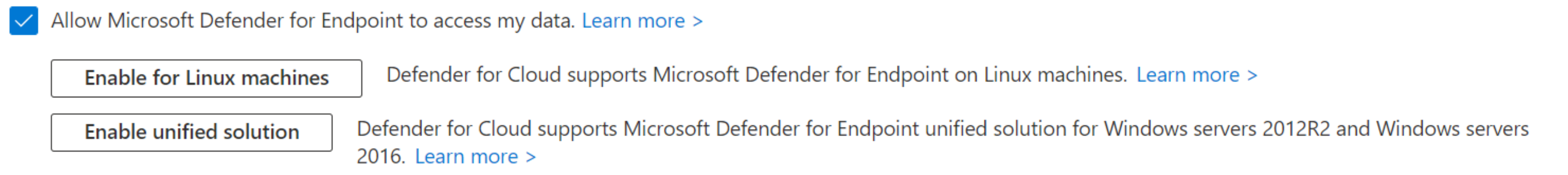
Plan selection

Defender for servers is offered in two plans.
Plan 1 provides a limited set of defenses with a focus on Defender for Endpoint's protections.
Plan 2 (formerly "Defender for servers") offers the full set of Defender for Cloud's enhanced security features.
Learn more

● **Microsoft Defender for Servers Plan 2** **$15**/Server/Month

Plan details

- ✓ Microsoft Defender for Endpoint
- ✓ Microsoft threat and vulnerability management
- ✓ Automatic agent onboarding, alert and data integration
- ✓ Just-in-time VM access for management ports
- ✓ Network layer threat detection
- ✓ Adaptive application controls
- ✓ File integrity monitoring



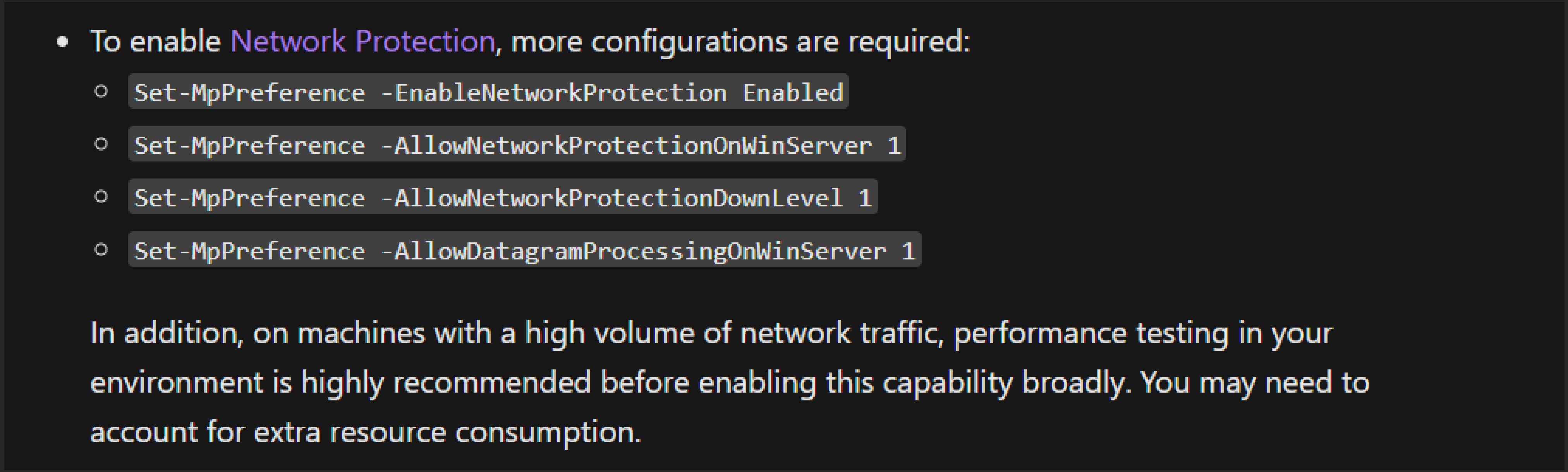
☑ Allow Microsoft Defender for Endpoint to access my data. Learn more >

Defender for Cloud supports Microsoft Defender for Endpoint on Linux machines. Learn more >

Defender for Cloud supports Microsoft Defender for Endpoint unified solution for Windows servers 2012R2 and Windows servers 2016. Learn more >

https://learn.microsoft.com/en-us/azure/defender-for-cloud/plan-defender-for-servers-select-plan

NOTE ! Network Protection



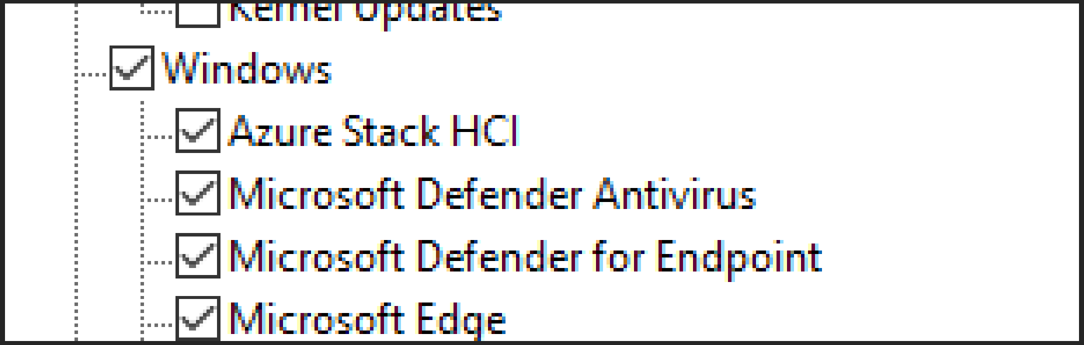
- To enable Network Protection, more configurations are required:
  - `Set-MpPreference -EnableNetworkProtection Enabled`
  - `Set-MpPreference -AllowNetworkProtectionOnWinServer 1`
  - `Set-MpPreference -AllowNetworkProtectionDownLevel 1`
  - `Set-MpPreference -AllowDatagramProcessingOnWinServer 1`

  In addition, on machines with a high volume of network traffic, performance testing in your environment is highly recommended before enabling this capability broadly. You may need to account for extra resource consumption.

https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-server-endpoints?view=o365-worldwide

New sensor update

- Important, Maintain the new sensor through update KB5005292
  - WSUS/MEMCM
    - Classification: Definition Updates
    - Product : Defender for Endpoint
  - Manual
    - https://www.catalog.update.microsoft.com/Search.aspx?q=KB5005292



□ Kernel Updates
☑ Windows
  ☑ Azure Stack HCI
  ☑ Microsoft Defender Antivirus
  ☑ Microsoft Defender for Endpoint
  ☑ Microsoft Edge

Common Pitfalls and Lessons learned

- FW audit log turned off
- Don’t forget to configure and harden AV, not just focus on deploying EDR
- New path, and custom detection exclusions
- No AV GUI on 2012 R2, only basic operations in 2016 GUI
- A few ASR Rules not supported on Server OS:
  - Attack surface reduction rules reference | Microsoft Docs
- Network events not populate if not patched
  - October 12, 2021 monthly rollup (KB5006714)
- No Automatic exclusions 2012 R2
- Review Dynamic AAD Group Rules before enrolling
- Operating system upgrades aren't supported. Offboard then uninstall before upgrading.

MDE

Microsoft Defender for Endpoint

Harden Defender Configuration

- Cloud Protection
  - MAPSReporting = 2
  - CloudBlockLevel = 2
  - CloudExtendedTimeout = 50
- Network Protection
  - EnableNetworkProtection = 1
- SubmitSamplesConsent = 3 (Always) | 1 (Safe Samples)

Requirement for Cloud Protection

- Tamper Protection
- Firewall Auditing
  - auditpol /set /subcategory:"Filtering Platform Packet Drop" /failure:enable
  - auditpol /set /subcategory:"Filtering Platform Connection" /failure:enable

Requirement for Firewall Report and Hunting events

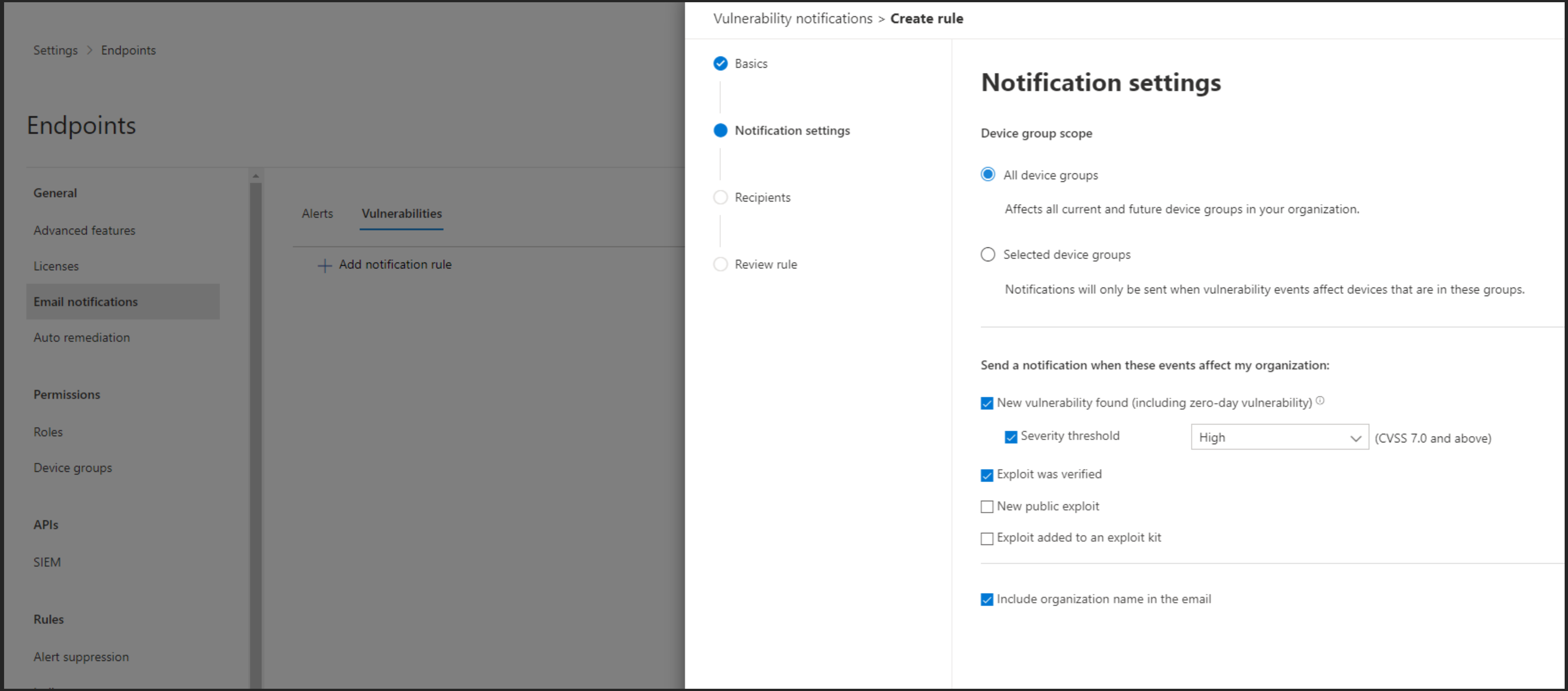
- AttackSurfaceReduction
- DefaultActions
  - Quarantine
- EDR BlockMode
- Exclusions
- DisableLocalAdminMerge
- General Auditing
  - https://learn.microsoft.com/en-us/microsoft-365/security/defender/advanced-hunting-extend-data?view=o365-worldwide

TVM

Threat and Vulnerability Management

Configure email notifications for vulnerabilities

- Keep up to date - Don’t miss a severe vulnerability



Notification settings

Device group scope

● All device groups

Affects all current and future device groups in your organization.

○ Selected device groups

Notifications will only be sent when vulnerability events affect devices that are in these groups.

Send a notification when these events affect my organization:

☑ New vulnerability found (including zero-day vulnerability)

☑ Severity threshold High (CVSS 7.0 and above)

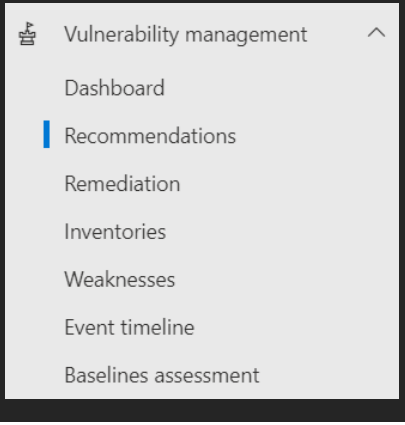
☑ Exploit was verified

□ New public exploit

□ Exploit added to an exploit kit

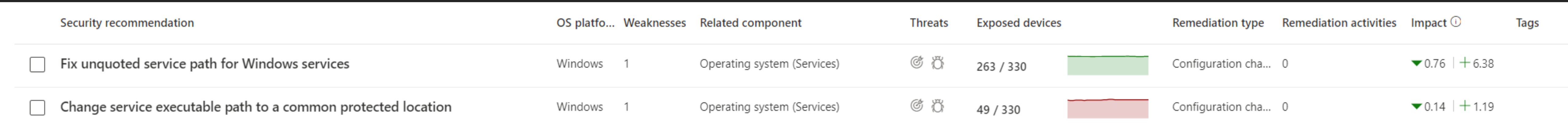
☑ Include organization name in the email

Service Executables – Instant Admin privilege



Vulnerability management

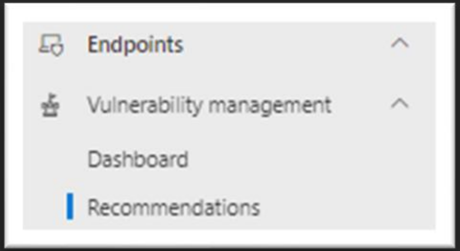
- Dashboard
- Recommendations
- Remediation
- Inventories
- Weaknesses
- Event timeline
- Baselines assessment



	Security recommendation	OS platfo...	Weaknesses	Related component	Threats	Exposed devices		Remediation type	Remediation activities	Impact ⓘ	Tags
□	Fix unquoted service path for Windows services	Windows	1	Operating system (Services)		263 / 330	🟩	Configuration cha...	0	▼0.76 | +6.38	
□	Change service executable path to a common protected location	Windows	1	Operating system (Services)		49 / 330	🟥	Configuration cha...	0	▼0.14 | +1.19	

scid-3001
scid-3002

SMB and Shares

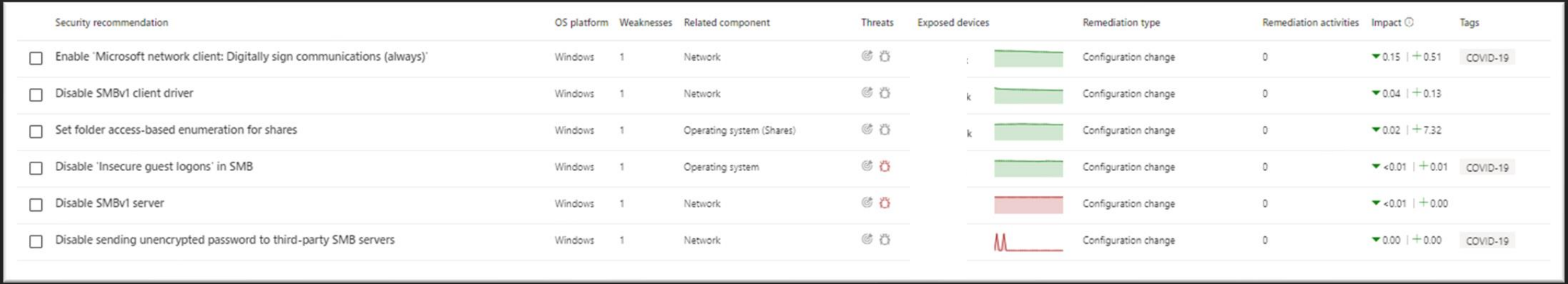


Endpoints

Vulnerability management

Dashboard

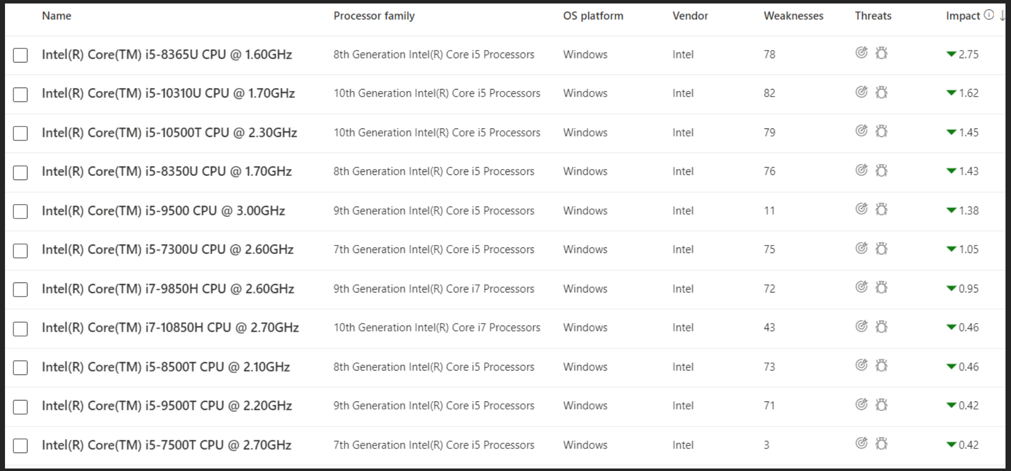
Recommendations



	Security recommendation	OS platform	Weaknesses	Related component	Threats	Exposed devices	Remediation type	Remediation activities	Impact ⓘ	Tags
□	Enable 'Microsoft network client: Digitally sign communications (always)'	Windows	1	Network	◎ ✱	:	Configuration change	0	▼0.15 | +0.51	COVID-19
□	Disable SMBv1 client driver	Windows	1	Network	◎ ✱	k	Configuration change	0	▼0.04 | +0.13	
□	Set folder access-based enumeration for shares	Windows	1	Operating system (Shares)	◎ ✱	k	Configuration change	0	▼0.02 | +7.32	
□	Disable 'Insecure guest logons' in SMB	Windows	1	Operating system	◎ ✱		Configuration change	0	▼<0.01 | +0.01	COVID-19
□	Disable SMBv1 server	Windows	1	Network	◎ ✱		Configuration change	0	▼<0.01 | +0.00	
□	Disable sending unencrypted password to third-party SMB servers	Windows	1	Network	◎ ✱		Configuration change	0	▼0.00 | +0.00	COVID-19

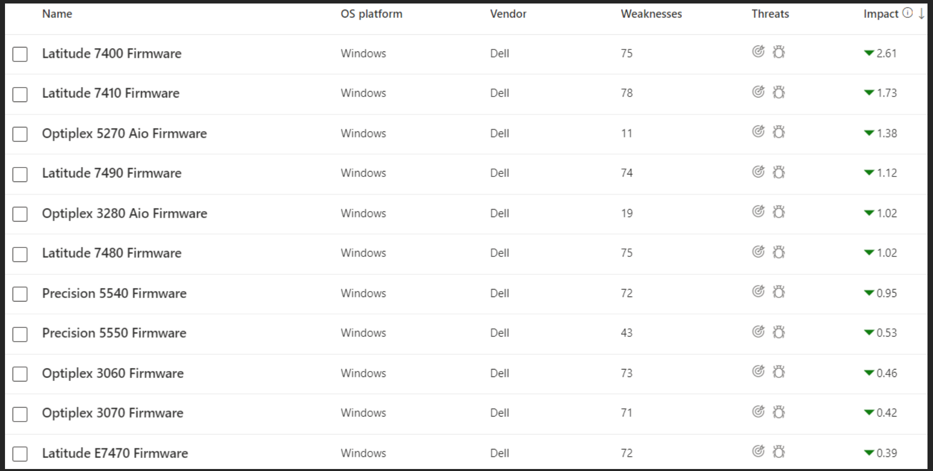
Hardware and Firmware

CPU



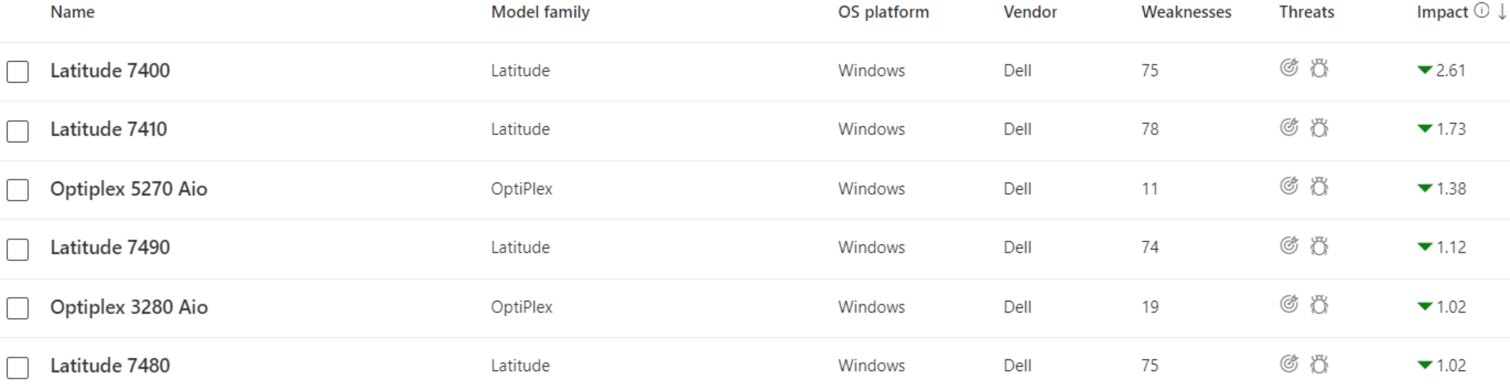
	Name	Processor family	OS platform	Vendor	Weaknesses	Threats	Impact ⓘ ↓
□	Intel(R) Core(TM) i5-8365U CPU @ 1.60GHz	8th Generation Intel(R) Core i5 Processors	Windows	Intel	78	◎ 🐞	▼2.75
□	Intel(R) Core(TM) i5-10310U CPU @ 1.70GHz	10th Generation Intel(R) Core i5 Processors	Windows	Intel	82	◎ 🐞	▼1.62
□	Intel(R) Core(TM) i5-10500T CPU @ 2.30GHz	10th Generation Intel(R) Core i5 Processors	Windows	Intel	79	◎ 🐞	▼1.45
□	Intel(R) Core(TM) i5-8350U CPU @ 1.70GHz	8th Generation Intel(R) Core i5 Processors	Windows	Intel	76	◎ 🐞	▼1.43
□	Intel(R) Core(TM) i5-9500 CPU @ 3.00GHz	9th Generation Intel(R) Core i5 Processors	Windows	Intel	11	◎ 🐞	▼1.38
□	Intel(R) Core(TM) i5-7300U CPU @ 2.60GHz	7th Generation Intel(R) Core i5 Processors	Windows	Intel	75	◎ 🐞	▼1.05
□	Intel(R) Core(TM) i7-9850H CPU @ 2.60GHz	9th Generation Intel(R) Core i7 Processors	Windows	Intel	72	◎ 🐞	▼0.95
□	Intel(R) Core(TM) i7-10850H CPU @ 2.70GHz	10th Generation Intel(R) Core i7 Processors	Windows	Intel	43	◎ 🐞	▼0.46
□	Intel(R) Core(TM) i5-8500T CPU @ 2.10GHz	8th Generation Intel(R) Core i5 Processors	Windows	Intel	73	◎ 🐞	▼0.46
□	Intel(R) Core(TM) i5-9500T CPU @ 2.20GHz	9th Generation Intel(R) Core i5 Processors	Windows	Intel	71	◎ 🐞	▼0.42
□	Intel(R) Core(TM) i5-7500T CPU @ 2.70GHz	7th Generation Intel(R) Core i5 Processors	Windows	Intel	3	◎ 🐞	▼0.42

BIOS



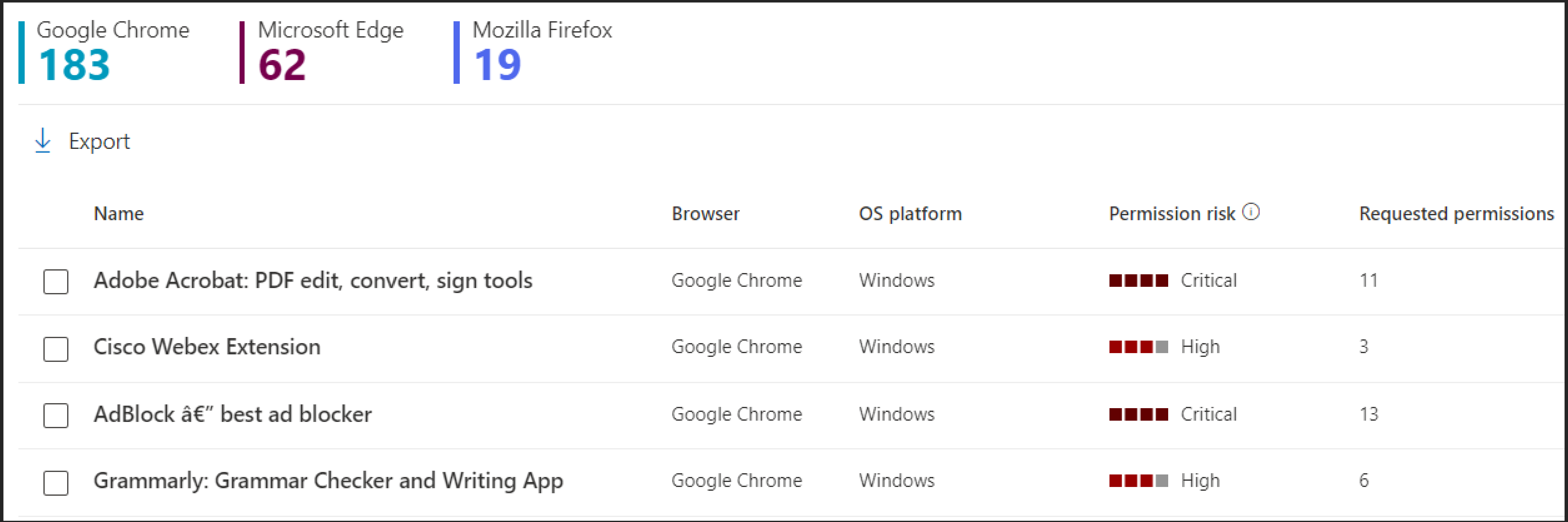
	Name	OS platform	Vendor	Weaknesses	Threats	Impact ⓘ ↓
□	Latitude 7400 Firmware	Windows	Dell	75	◎ 🐞	▼2.61
□	Latitude 7410 Firmware	Windows	Dell	78	◎ 🐞	▼1.73
□	Optiplex 5270 Aio Firmware	Windows	Dell	11	◎ 🐞	▼1.38
□	Latitude 7490 Firmware	Windows	Dell	74	◎ 🐞	▼1.12
□	Optiplex 3280 Aio Firmware	Windows	Dell	19	◎ 🐞	▼1.02
□	Latitude 7480 Firmware	Windows	Dell	75	◎ 🐞	▼1.02
□	Precision 5540 Firmware	Windows	Dell	72	◎ 🐞	▼0.95
□	Precision 5550 Firmware	Windows	Dell	43	◎ 🐞	▼0.53
□	Optiplex 3060 Firmware	Windows	Dell	73	◎ 🐞	▼0.46
□	Optiplex 3070 Firmware	Windows	Dell	71	◎ 🐞	▼0.42
□	Latitude E7470 Firmware	Windows	Dell	72	◎ 🐞	▼0.39

MODELS



	Name	Model family	OS platform	Vendor	Weaknesses	Threats	Impact ⓘ ↓
□	Latitude 7400	Latitude	Windows	Dell	75	◎ 🐞	▼2.61
□	Latitude 7410	Latitude	Windows	Dell	78	◎ 🐞	▼1.73
□	Optiplex 5270 Aio	OptiPlex	Windows	Dell	11	◎ 🐞	▼1.38
□	Latitude 7490	Latitude	Windows	Dell	74	◎ 🐞	▼1.12
□	Optiplex 3280 Aio	OptiPlex	Windows	Dell	19	◎ 🐞	▼1.02
□	Latitude 7480	Latitude	Windows	Dell	75	◎ 🐞	▼1.02

Browser Extensions



Google Chrome 183

Microsoft Edge 62

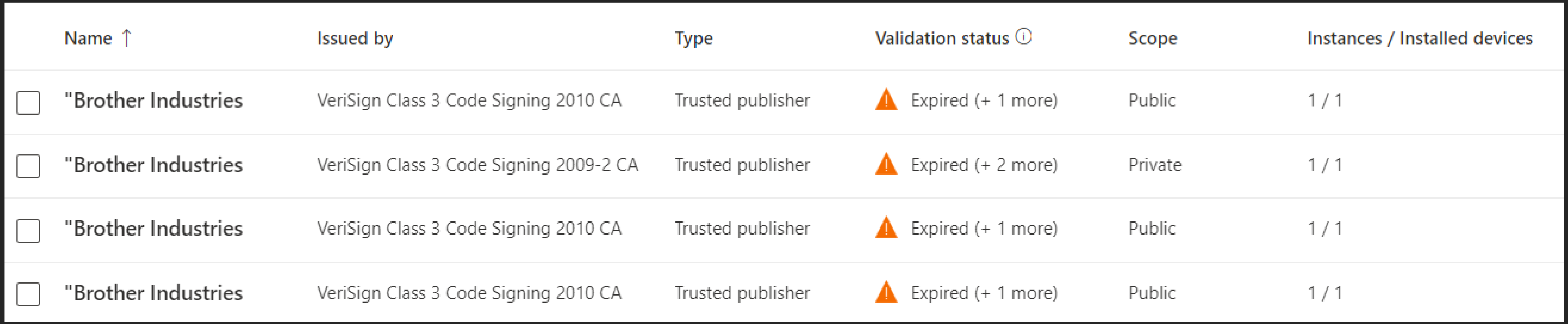
Mozilla Firefox 19

Export

	Name	Browser	OS platform	Permission risk ⓘ	Requested permissions
□	Adobe Acrobat: PDF edit, convert, sign tools	Google Chrome	Windows	■■■■ Critical	11
□	Cisco Webex Extension	Google Chrome	Windows	■■■□ High	3
□	AdBlock â€" best ad blocker	Google Chrome	Windows	■■■■ Critical	13
□	Grammarly: Grammar Checker and Writing App	Google Chrome	Windows	■■■□ High	6

Certificates

NORDIC
— VIRTUAL SUMMIT —

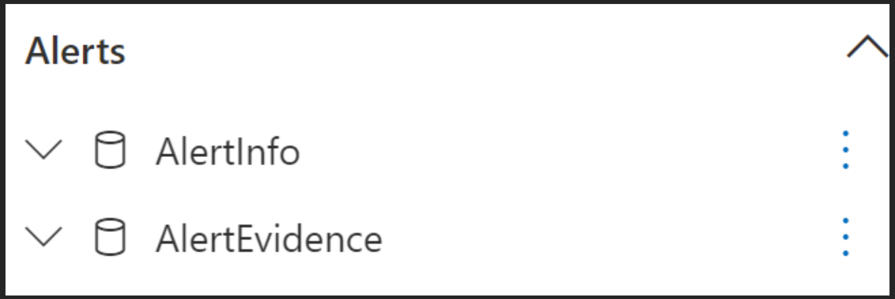


	Name ↑	Issued by	Type	Validation status ⓘ	Scope	Instances / Installed devices
□	"Brother Industries	VeriSign Class 3 Code Signing 2010 CA	Trusted publisher	⚠ Expired (+ 1 more)	Public	1 / 1
□	"Brother Industries	VeriSign Class 3 Code Signing 2009-2 CA	Trusted publisher	⚠ Expired (+ 2 more)	Private	1 / 1
□	"Brother Industries	VeriSign Class 3 Code Signing 2010 CA	Trusted publisher	⚠ Expired (+ 1 more)	Public	1 / 1
□	"Brother Industries	VeriSign Class 3 Code Signing 2010 CA	Trusted publisher	⚠ Expired (+ 1 more)	Public	1 / 1

Threat Hunting

Defender data-model

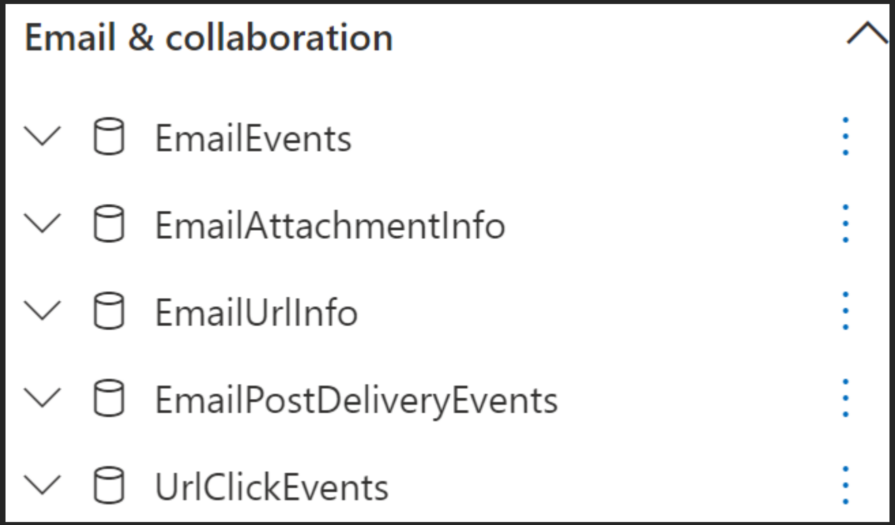
Alerts



Alerts

- AlertInfo
- AlertEvidence

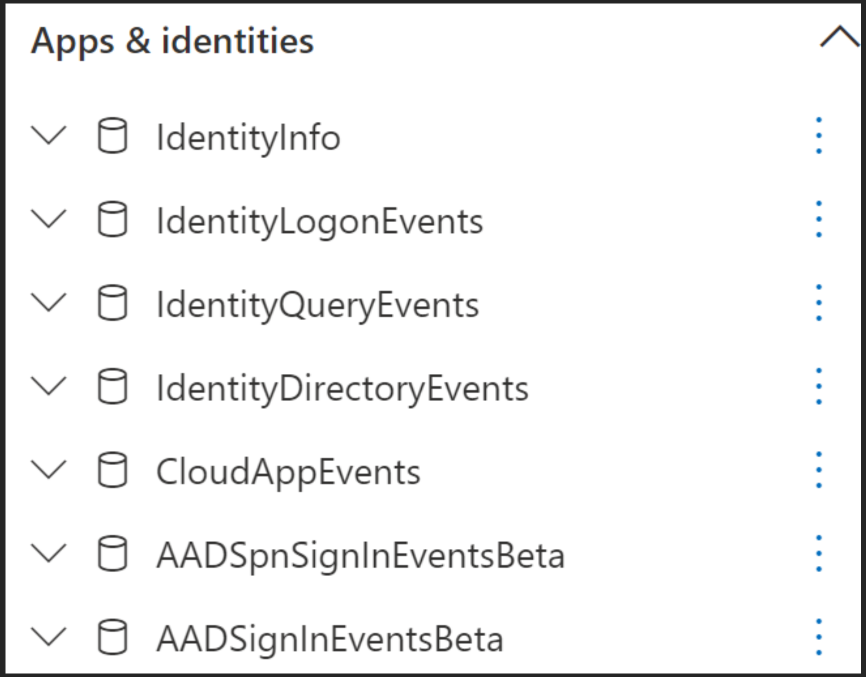
E-mail



Email & collaboration

- EmailEvents
- EmailAttachmentInfo
- EmailUrlInfo
- EmailPostDeliveryEvents
- UrlClickEvents

MDCA / AAD / AD

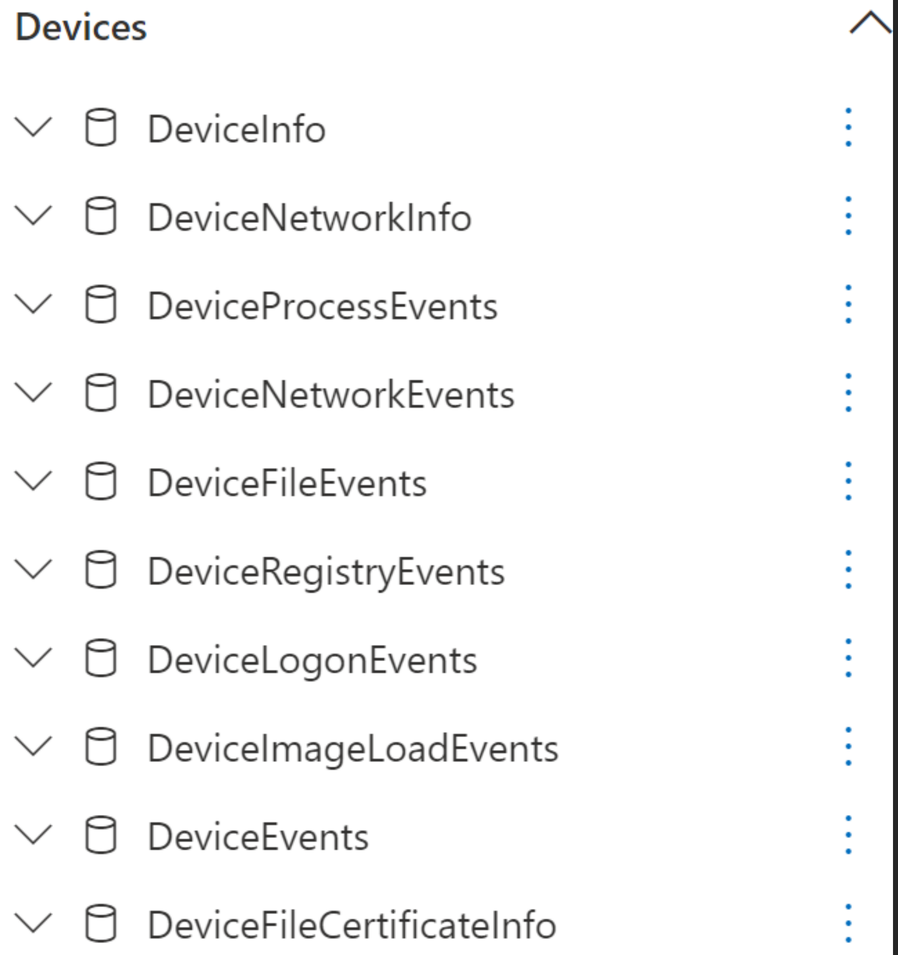


Apps & identities

- IdentityInfo
- IdentityLogonEvents
- IdentityQueryEvents
- IdentityDirectoryEvents
- CloudAppEvents
- AADSpnSignInEventsBeta
- AADSignInEventsBeta

Defender data-model

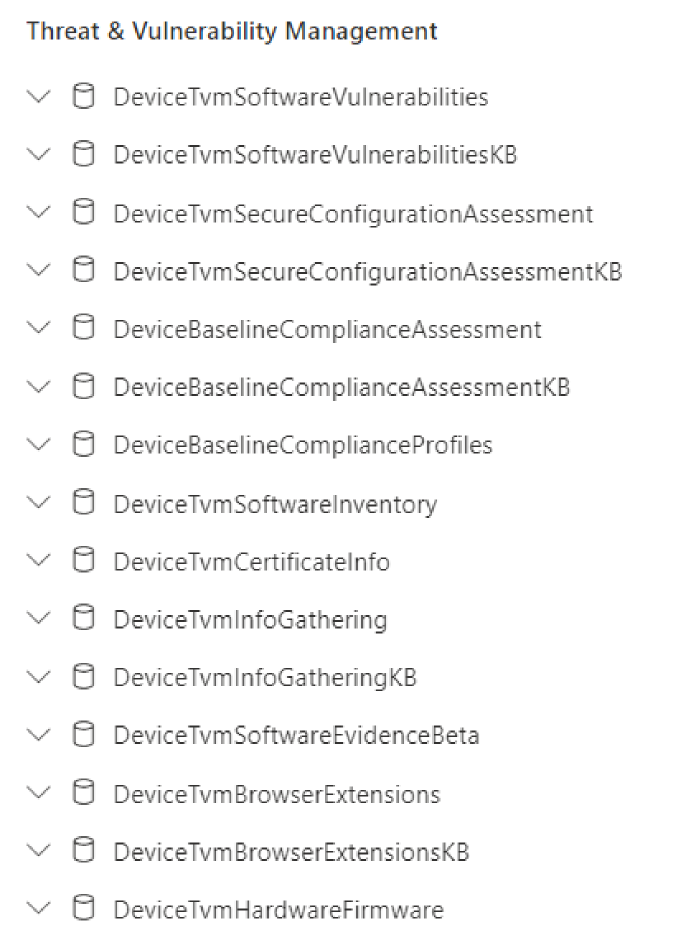
Device



Devices

- DeviceInfo
- DeviceNetworkInfo
- DeviceProcessEvents
- DeviceNetworkEvents
- DeviceFileEvents
- DeviceRegistryEvents
- DeviceLogonEvents
- DeviceImageLoadEvents
- DeviceEvents
- DeviceFileCertificateInfo

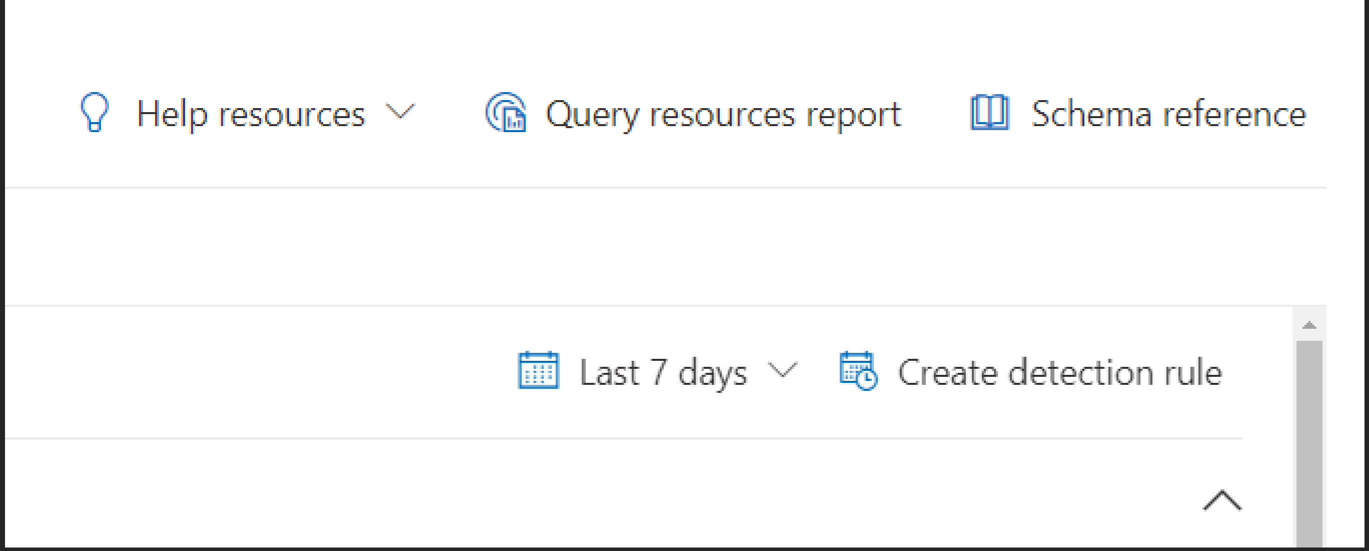
Vulnerabilities and Configuration

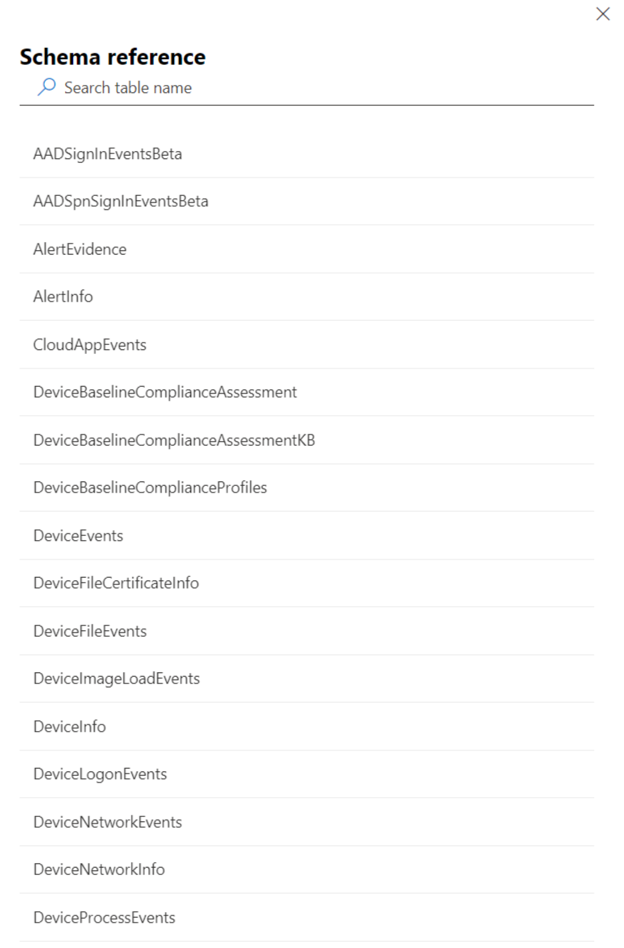


Threat & Vulnerability Management

- DeviceTvmSoftwareVulnerabilities
- DeviceTvmSoftwareVulnerabilitiesKB
- DeviceTvmSecureConfigurationAssessment
- DeviceTvmSecureConfigurationAssessmentKB
- DeviceBaselineComplianceAssessment
- DeviceBaselineComplianceAssessmentKB
- DeviceBaselineComplianceProfiles
- DeviceTvmSoftwareInventory
- DeviceTvmCertificateInfo
- DeviceTvmInfoGathering
- DeviceTvmInfoGatheringKB
- DeviceTvmSoftwareEvidenceBeta
- DeviceTvmBrowserExtensions
- DeviceTvmBrowserExtensionsKB
- DeviceTvmHardwareFirmware

Defender data-model schema ref





Schema reference

Search table name

- AADSignInEventsBeta
- AADSpnSignInEventsBeta
- AlertEvidence
- AlertInfo
- CloudAppEvents
- DeviceBaselineComplianceAssessment
- DeviceBaselineComplianceAssessmentKB
- DeviceBaselineComplianceProfiles
- DeviceEvents
- DeviceFileCertificateInfo
- DeviceFileEvents
- DeviceImageLoadEvents
- DeviceInfo
- DeviceLogonEvents
- DeviceNetworkEvents
- DeviceNetworkInfo
- DeviceProcessEvents

Identifying Logins were user is Local Admin

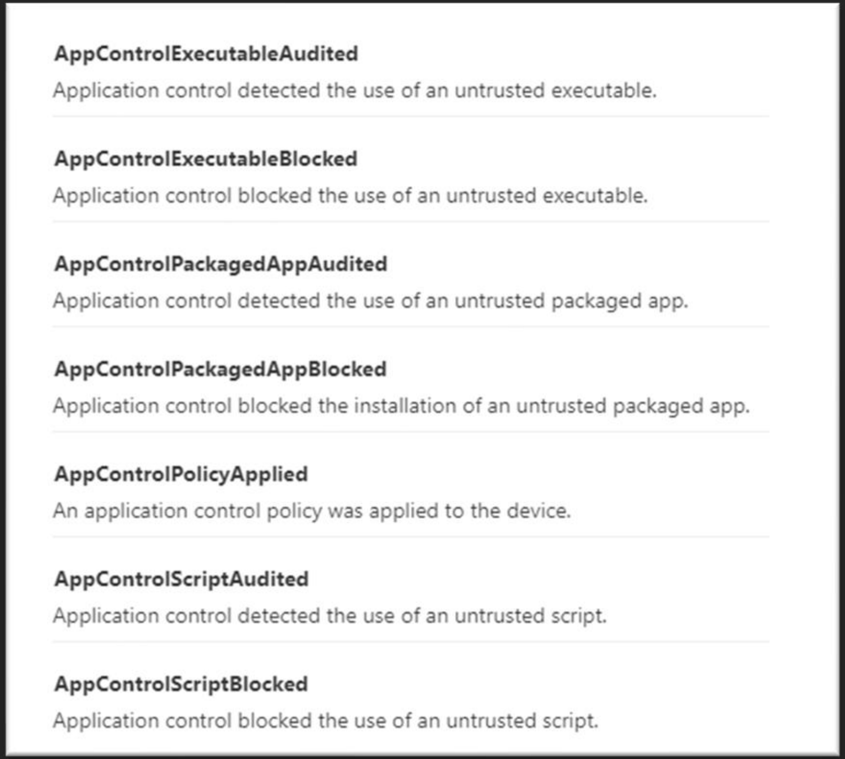
```
DeviceLogonEvents
| where Timestamp >= ago(30d)
| where IsLocalAdmin == 1
//| where LogonType == "Interactive"
| summarize count() by DeviceName, AccountName,LogonType
| sort by AccountName
```

Identifying Logins were user is Tier Admin

```
DeviceLogonEvents
| where Timestamp >= ago(30d)
| where AccountName startswith "a1-" or AccountName
startswith "a2-"
| where LogonType == "Interactive"
| summarize count() by DeviceName, AccountName,LogonType
| sort by AccountName
```

AppLocker Events

```
DeviceEvents
| where ActionType == 'AppControlExecutableAudited'
```



AppControlExecutableAudited
Application control detected the use of an untrusted executable.

AppControlExecutableBlocked
Application control blocked the use of an untrusted executable.

AppControlPackagedAppAudited
Application control detected the use of an untrusted packaged app.

AppControlPackagedAppBlocked
Application control blocked the installation of an untrusted packaged app.

AppControlPolicyApplied
An application control policy was applied to the device.

AppControlScriptAudited
Application control detected the use of an untrusted script.

AppControlScriptBlocked
Application control blocked the use of an untrusted script.

Firewall Exposure

```
DeviceNetworkEvents
| where ActionType == "InboundConnectionAccepted"
| extend IPaddress =
extract(@"\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}",0,LocalIP)
| where IPaddress !startswith "127.0.0"
| extend IsPrivate = ipv4_is_private(IPaddress)
| where IsPrivate == 0
```

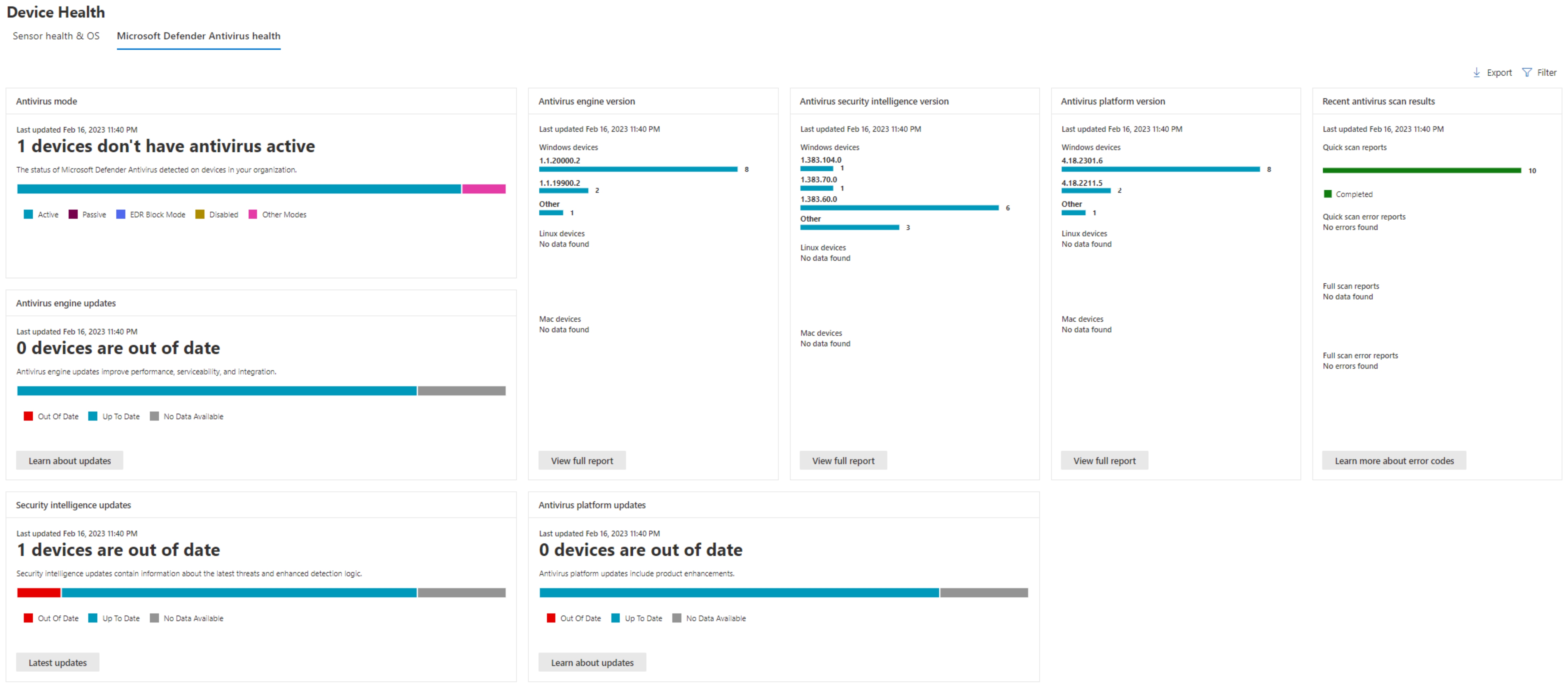
PowerShell Version 2

```
DeviceImageLoadEvents
| where InitiatingProcessFileName =~
         "powershell.exe" and
         FileName in~(
              "system.management.automation.ni.dll",
              "System.Management.Automation.dll")
         and FolderPath matches regex
                        @"[12]\.(\d)+\.(\d)+\.(\d)+"
```

Firewall Events

```
DeviceEvents
| where ActionType startswith "Firewall"
```

Device Health Report



Device Health

Sensor health & OS | **Microsoft Defender Antivirus health**

Export | Filter

Antivirus mode

Last updated Feb 16, 2023 11:40 PM

1 devices don't have antivirus active

The status of Microsoft Defender Antivirus detected on devices in your organization.

■ Active ■ Passive ■ EDR Block Mode ■ Disabled ■ Other Modes

Antivirus engine version

Last updated Feb 16, 2023 11:40 PM

Windows devices

1.1.20000.2 8

1.1.19900.2 2

Other 1

Linux devices
No data found

Mac devices
No data found

View full report

Antivirus security intelligence version

Last updated Feb 16, 2023 11:40 PM

Windows devices

1.383.104.0 1

1.383.70.0 1

1.383.60.0 6

Other 3

Linux devices
No data found

Mac devices
No data found

View full report

Antivirus platform version

Last updated Feb 16, 2023 11:40 PM

Windows devices

4.18.2301.6 8

4.18.2211.5 2

Other 1

Linux devices
No data found

Mac devices
No data found

View full report

Recent antivirus scan results

Last updated Feb 16, 2023 11:40 PM

Quick scan reports

10

■ Completed

Quick scan error reports
No errors found

Full scan reports
No data found

Full scan error reports
No errors found

Learn more about error codes

Antivirus engine updates

Last updated Feb 16, 2023 11:40 PM

0 devices are out of date

Antivirus engine updates improve performance, serviceability, and integration.

■ Out Of Date ■ Up To Date ■ No Data Available

Learn about updates

Security intelligence updates

Last updated Feb 16, 2023 11:40 PM

1 devices are out of date

Security intelligence updates contain information about the latest threats and enhanced detection logic.

■ Out Of Date ■ Up To Date ■ No Data Available

Latest updates

Antivirus platform updates

Last updated Feb 16, 2023 11:40 PM

0 devices are out of date

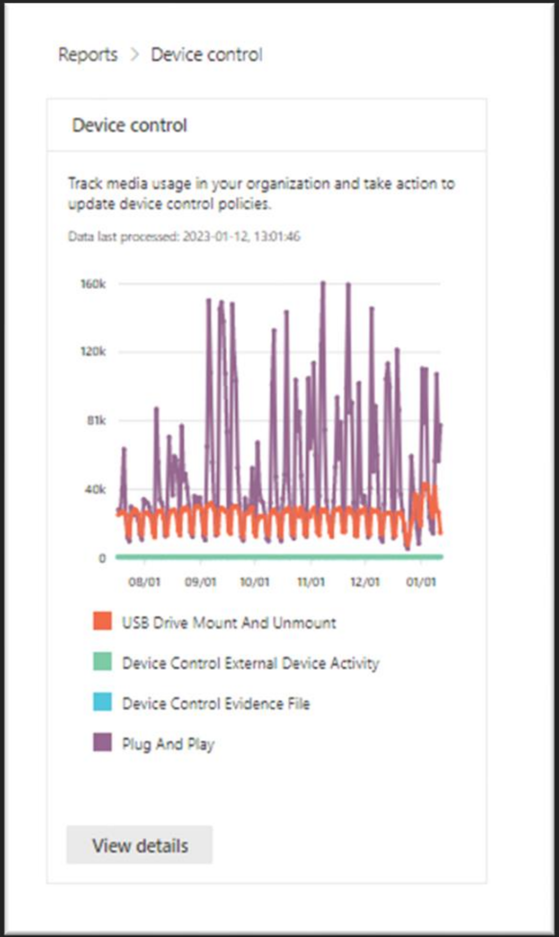
Antivirus platform updates include product enhancements.

■ Out Of Date ■ Up To Date ■ No Data Available

Learn about updates

https://security.microsoft.com/devicehealth?viewid=devicehealthreport

USB Report



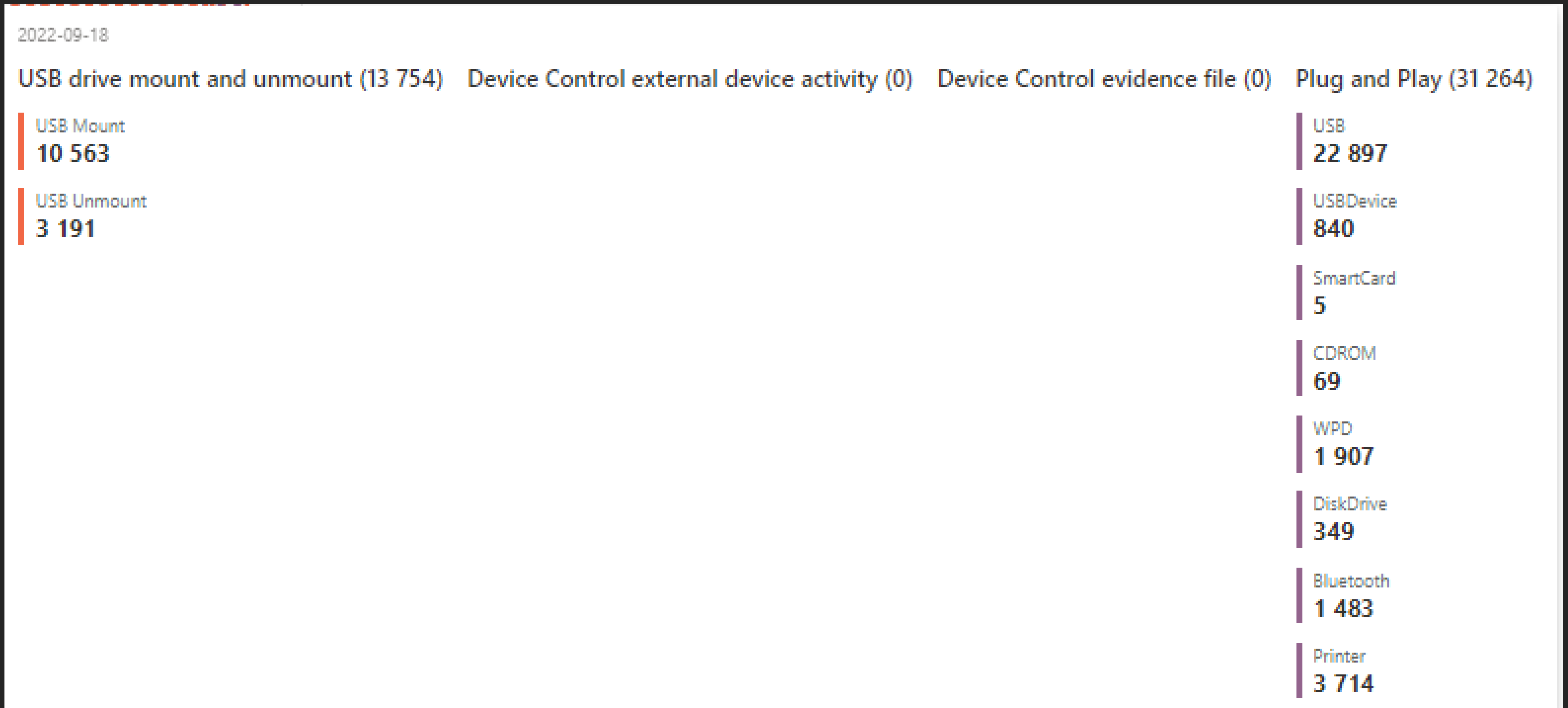
Reports > Device control

Device control

Track media usage in your organization and take action to update device control policies.

Data last processed: 2023-01-12, 13:01:46

160k
120k
81k
40k
0
08/01
09/01
10/01
11/01
12/01
01/01
🟥 USB Drive Mount And Unmount
🟩 Device Control External Device Activity
🟦 Device Control Evidence File
🟪 Plug And Play
View details



2022-09-18

USB drive mount and unmount (13 754)

USB Mount
10 563

USB Unmount
3 191

Device Control external device activity (0)

Device Control evidence file (0)

Plug and Play (31 264)

USB
22 897

USBDevice
840

SmartCard
5

CDROM
69

WPD
1 907

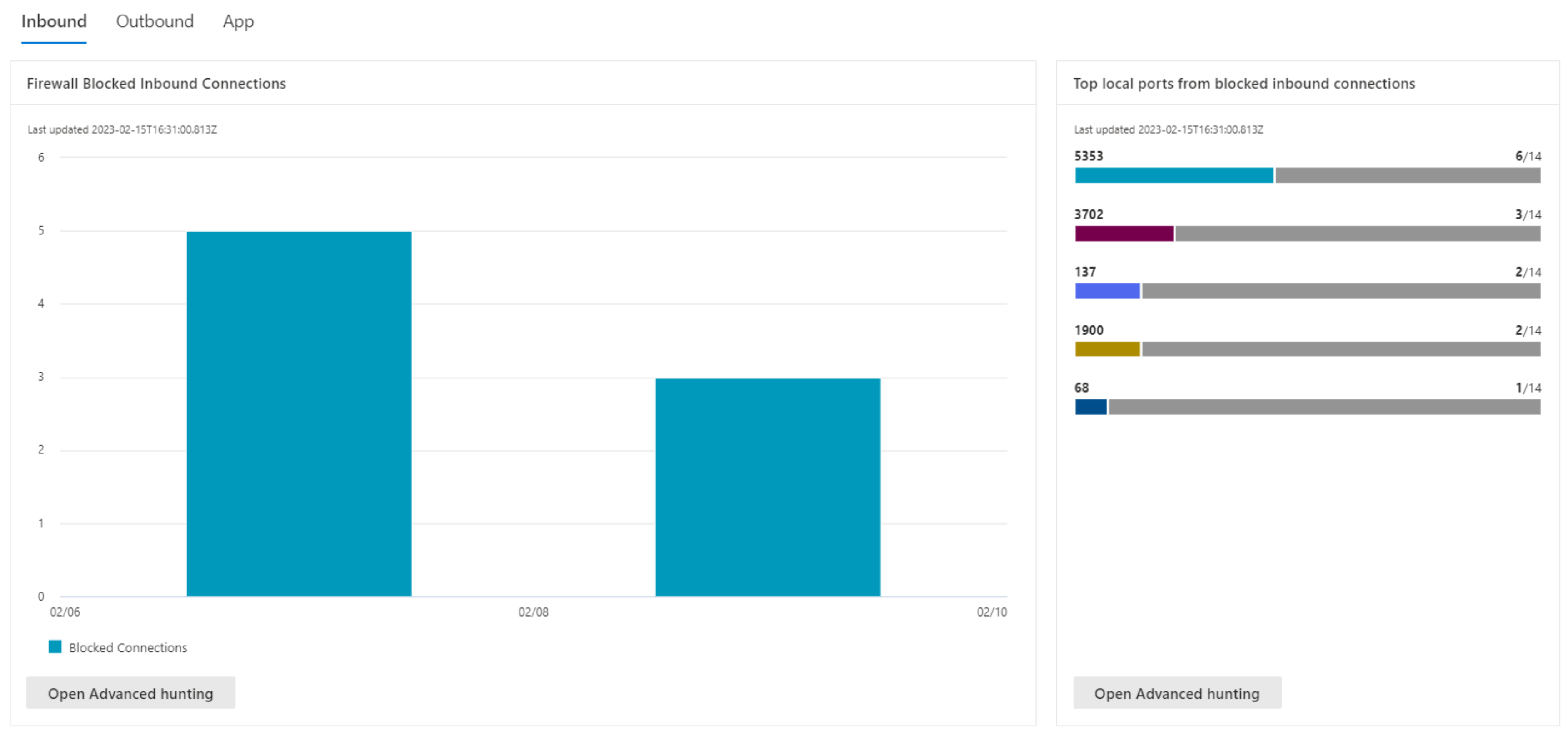
DiskDrive
349

Bluetooth
1 483

Printer
3 714

Firewall Report

NORDIC
— VIRTUAL SUMMIT —

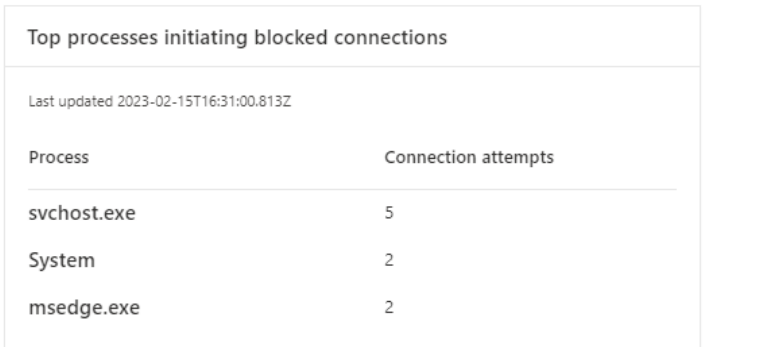


Firewall Blocked Inbound Connections

Last updated 2023-02-15T16:31:00.813Z

Top local ports from blocked inbound connections

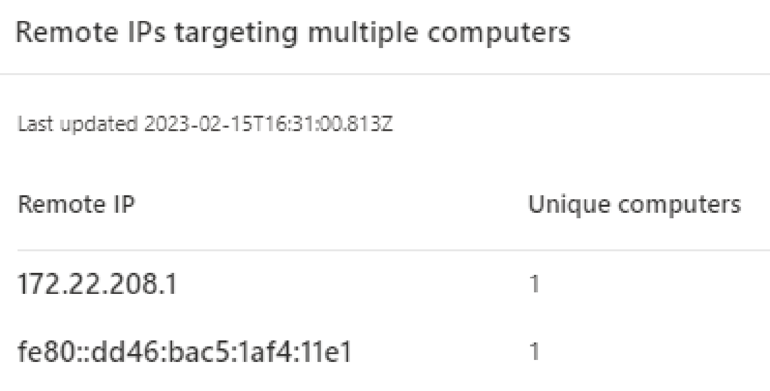
Last updated 2023-02-15T16:31:00.813Z



Top processes initiating blocked connections

Last updated 2023-02-15T16:31:00.813Z

Process	Connection attempts
svchost.exe	5
System	2
msedge.exe	2



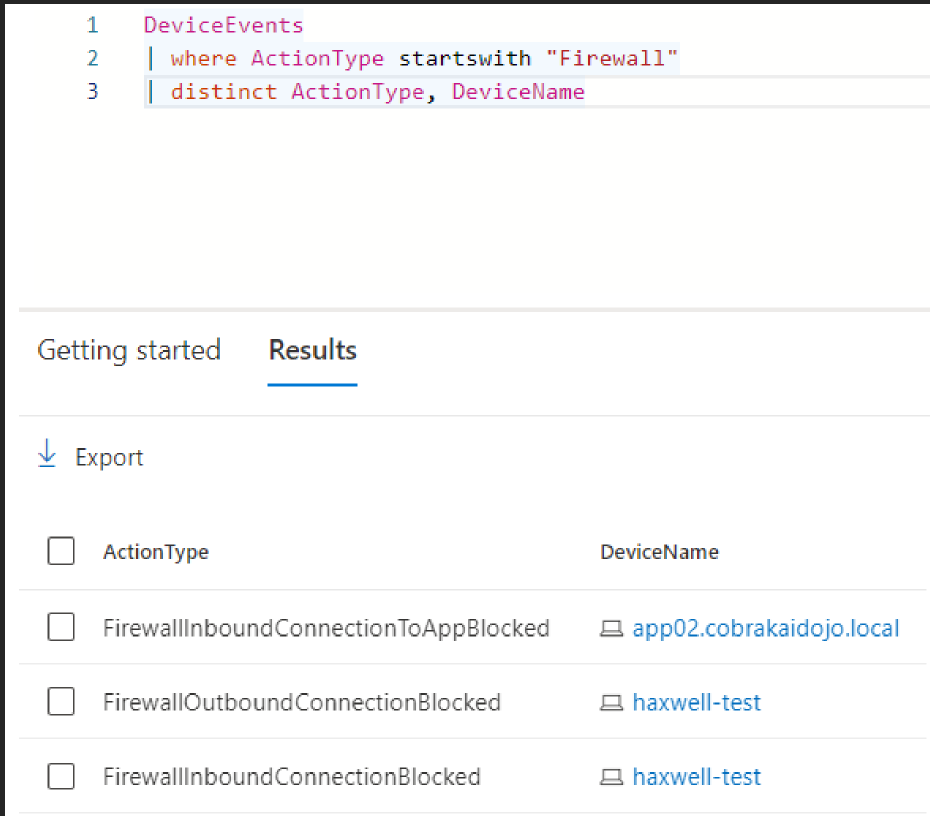
Remote IPs targeting multiple computers

Last updated 2023-02-15T16:31:00.813Z

Remote IP	Unique computers
172.22.208.1	1
fe80::dd46:bac5:1af4:11e1	1

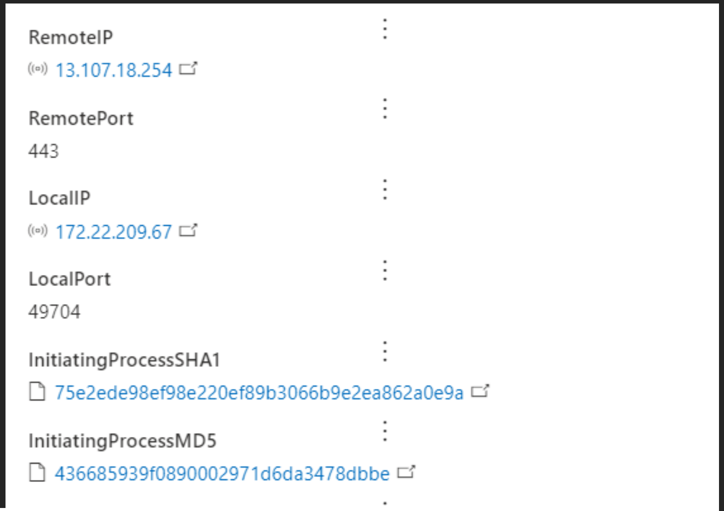
https://security.microsoft.com/firewall

Firewall in Advanced Hunting



```
DeviceEvents
| where ActionType startswith "Firewall"
| distinct ActionType, DeviceName
```

□	ActionType	DeviceName
□	FirewallInboundConnectionToAppBlocked	app02.cobrakaidojo.local
□	FirewallOutboundConnectionBlocked	haxwell-test
□	FirewallInboundConnectionBlocked	haxwell-test



RemoteIP
13.107.18.254

RemotePort
443

LocalIP
172.22.209.67

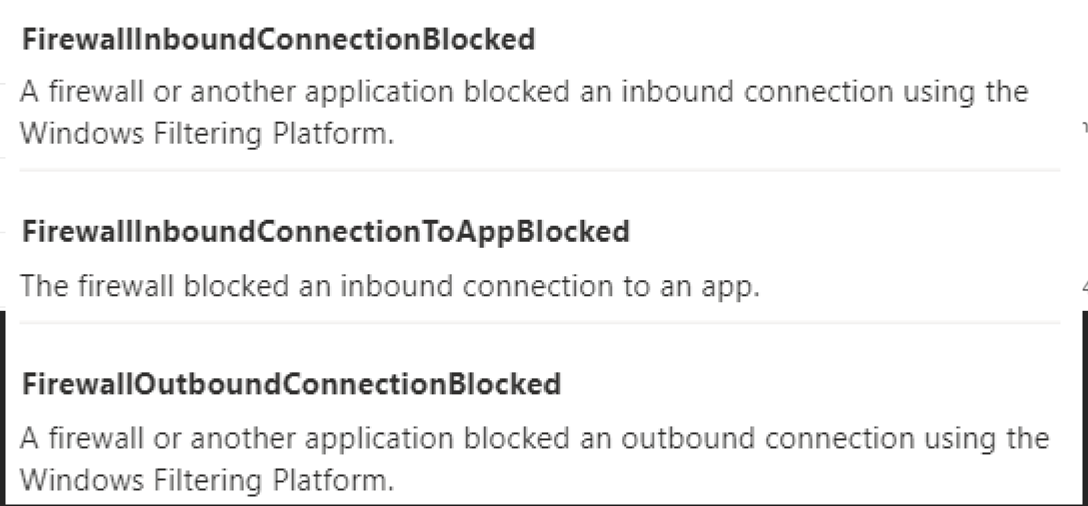
LocalPort
49704

InitiatingProcessSHA1
75e2ede98ef98e220ef89b3066b9e2ea862a0e9a

InitiatingProcessMD5
436685939f0890002971d6da3478dbbe

ı2txyewy

4bsbneegw0kyx...



FirewallInboundConnectionBlocked

A firewall or another application blocked an inbound connection using the Windows Filtering Platform.

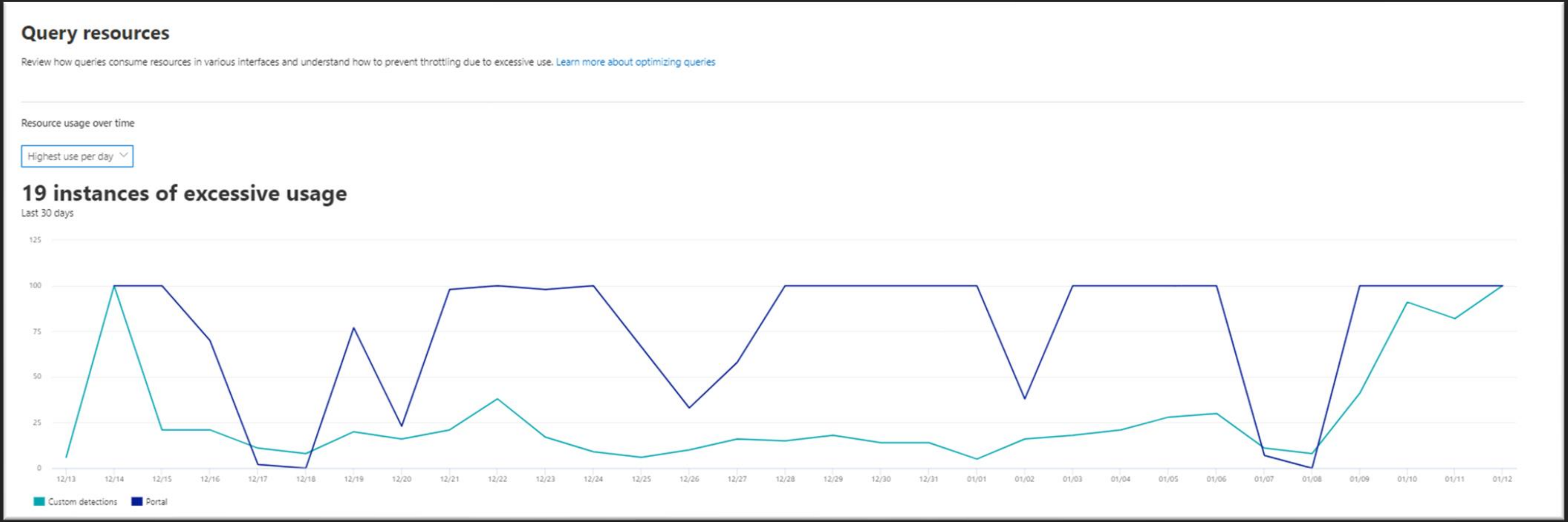
FirewallInboundConnectionToAppBlocked

The firewall blocked an inbound connection to an app.

FirewallOutboundConnectionBlocked

A firewall or another application blocked an outbound connection using the Windows Filtering Platform.

M365D Query Consumption



Query resources

Review how queries consume resources in various interfaces and understand how to prevent throttling due to excessive use. Learn more about optimizing queries

Resource usage over time

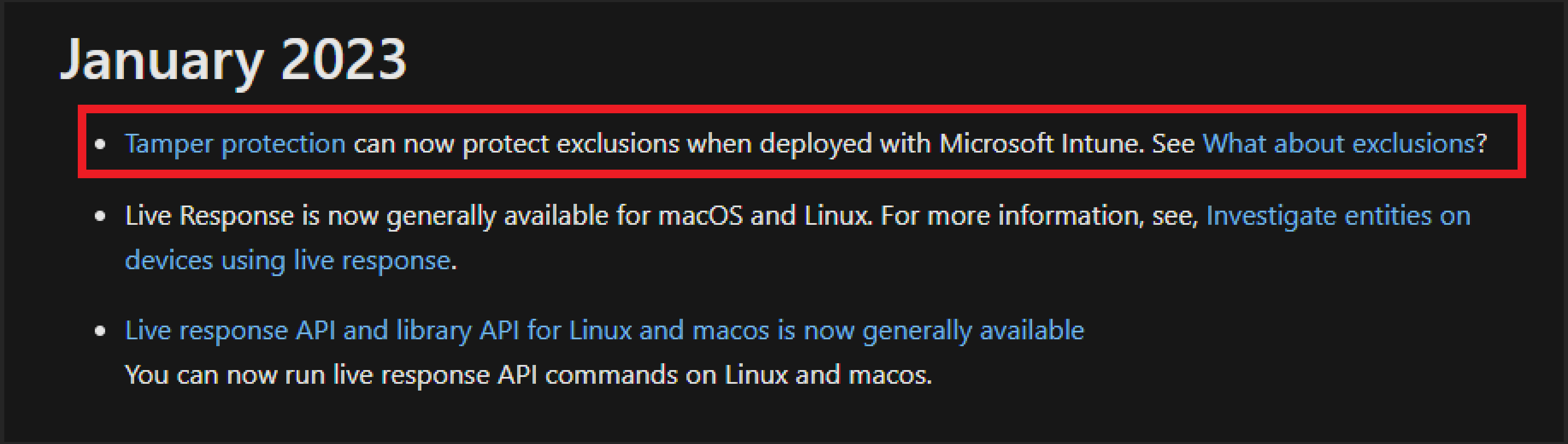
Highest use per day

19 instances of excessive usage

Last 30 days

https://security.microsoft.com/advanced-hunting/quotareport

Tamper Protection - Excluions



January 2023

- Tamper protection can now protect exclusions when deployed with Microsoft Intune. See What about exclusions?
- Live Response is now generally available for macOS and Linux. For more information, see, Investigate entities on devices using live response.
- Live response API and library API for Linux and macos is now generally available
  You can now run live response API commands on Linux and macos.

THANK YOU

Mattias Borg
blog.sec-labs.com
@mattiasborg82

Stefan Schörling
blog.sec-labs.com
@stefanschorling

Nordic Virtual Summit 2023 - 4th edition

We want your feedback!

Thank you!

MSEndPointMgr.com
#MSEndPointMgr

System Center User Group
Finland
#SCUGFI

System Center User Group
Denmark

#SCUGDK

System Center User Group
Sweden
#SCUGSE

Modern Management User Group
Norway
#MMUGNO