



Defender for Defenders

About

Stefan Schörling

Head of MDR @ Onevinn



Twitter: @stefanschorling

Blog: blog.sec-labs.com



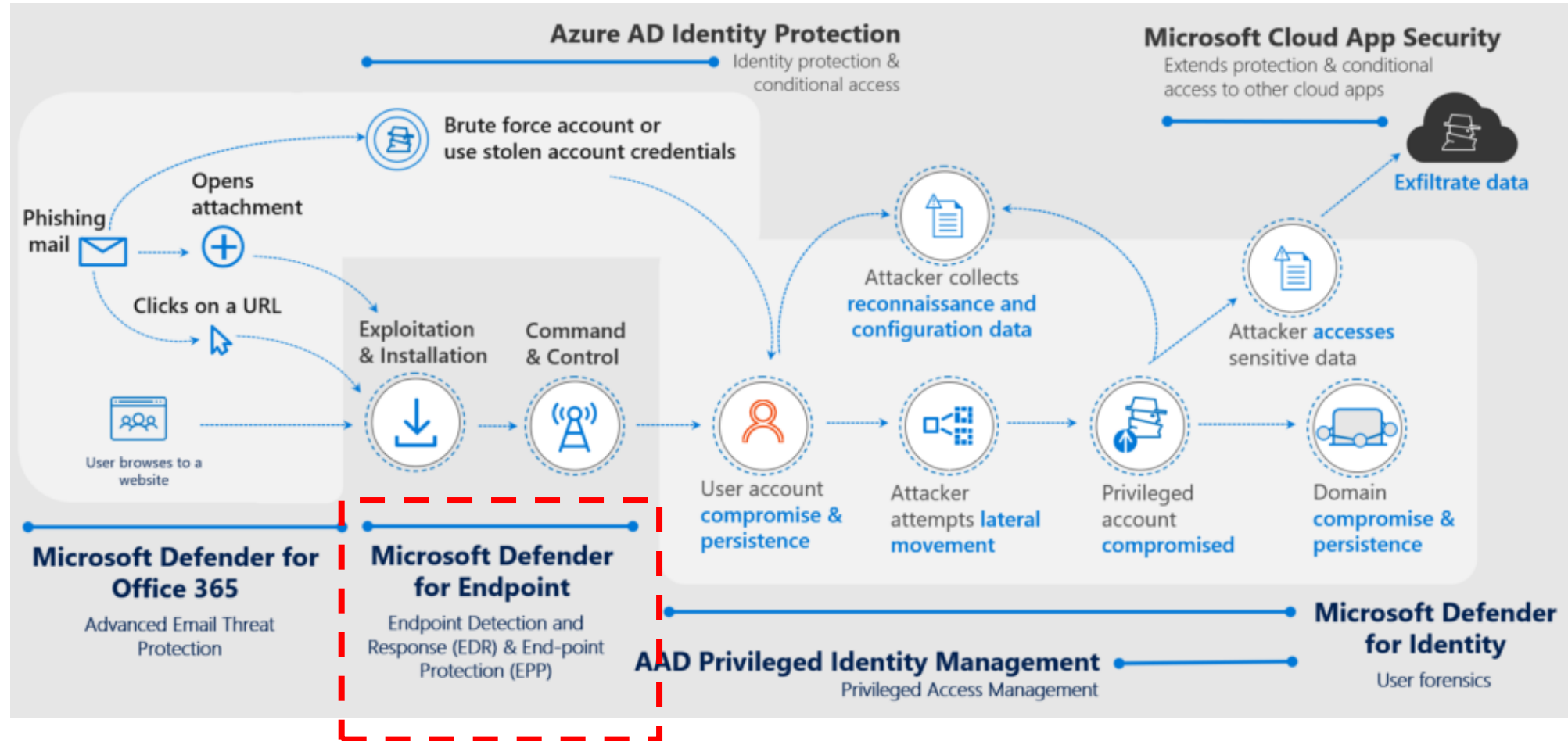
Agenda

- M365 Defender Intro
- SIEM vs XDR
- M365 Defender data-model
- MDE
 - Common misconfigurations
 - Using MDE data as a client admin
- Important M365D Changes

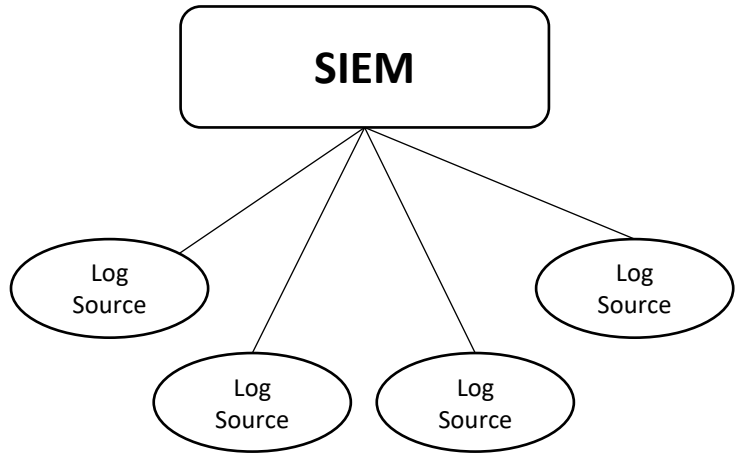
Defender Overview

- **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**

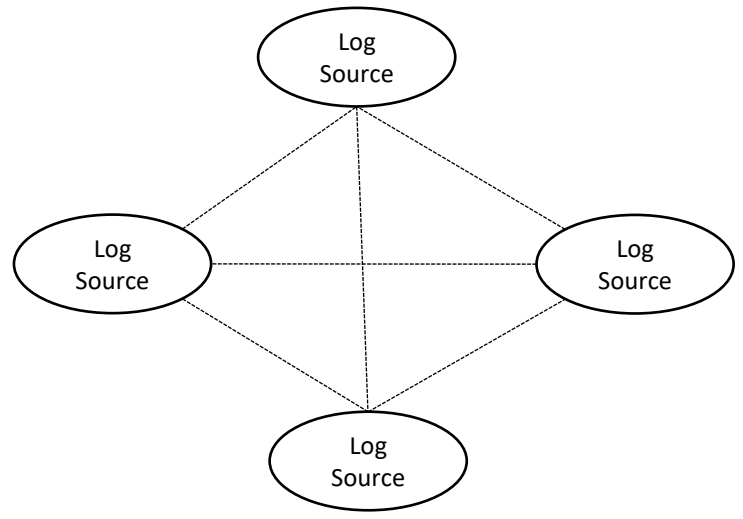
- *MDC - Defender for Cloud*
- *MD4IoT - Microsoft Defender for IoT*



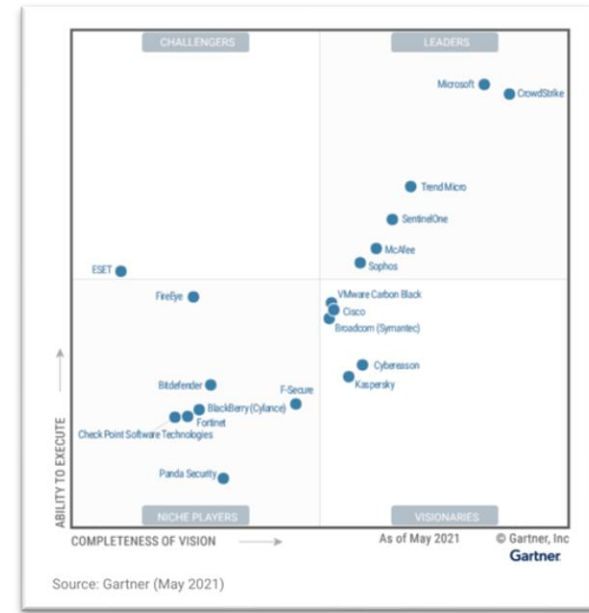
SIEM vs XDR



XDR



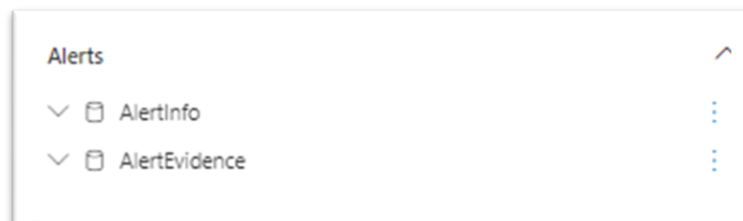
Extended Detection and Response



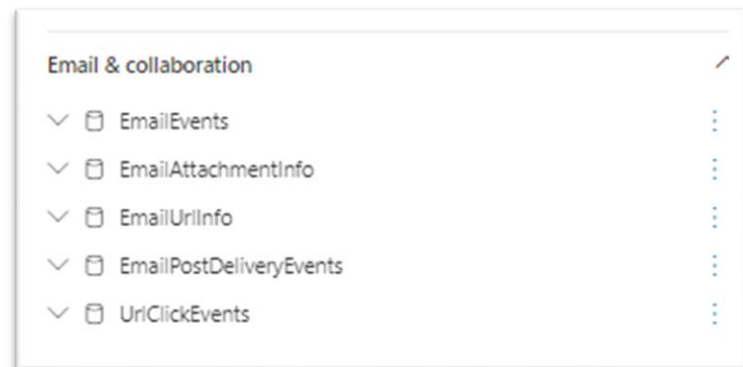
Defender data-model



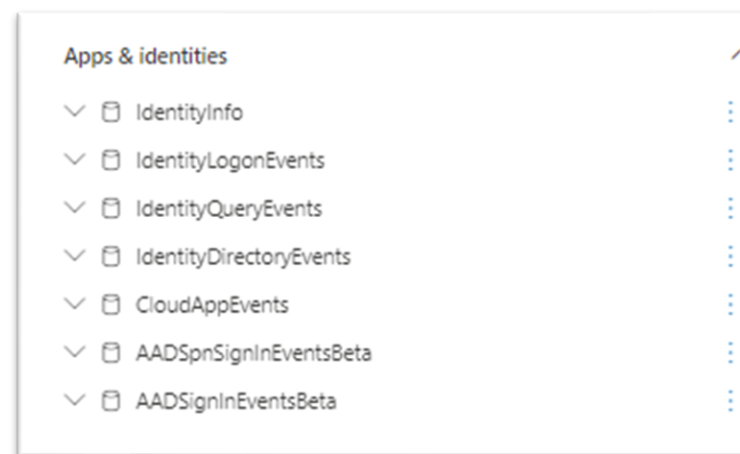
Alerts



E-mail

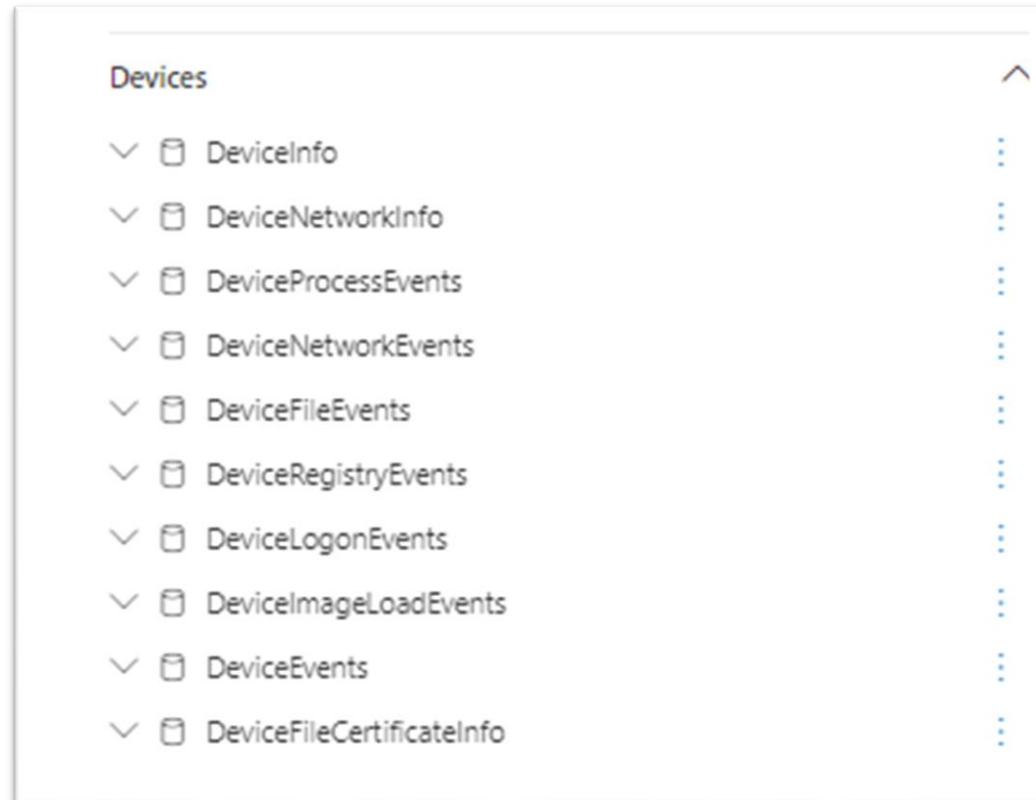


MDCA / AAD

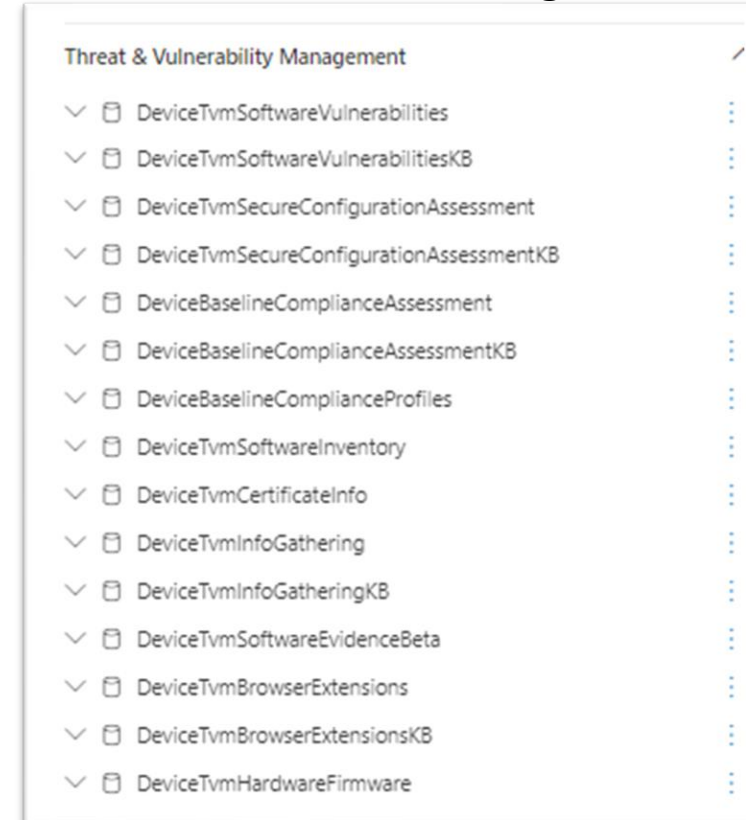


Defender data-model

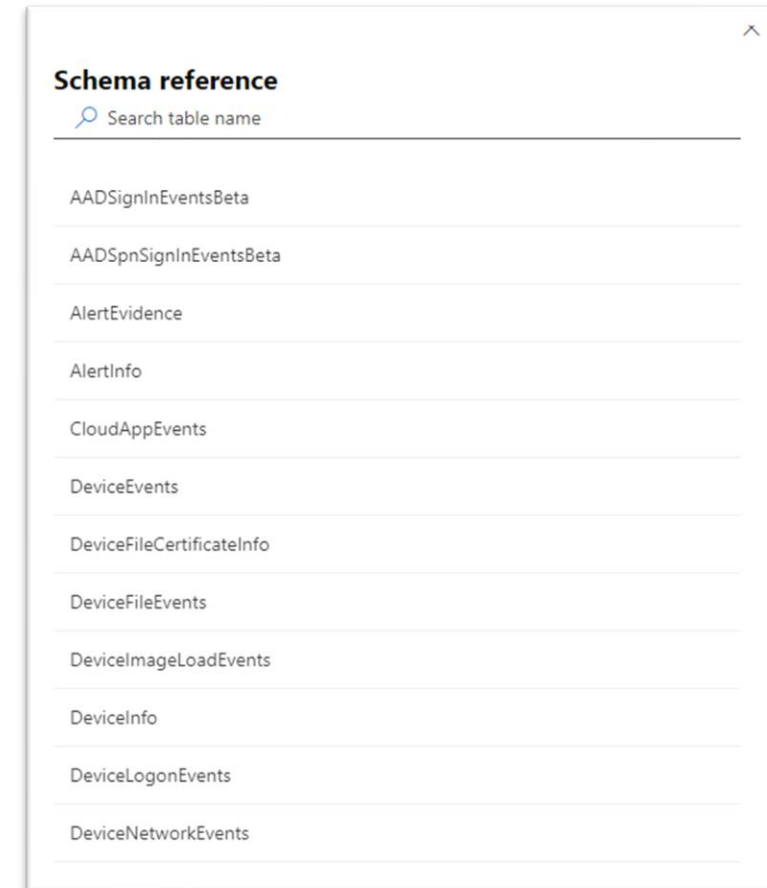
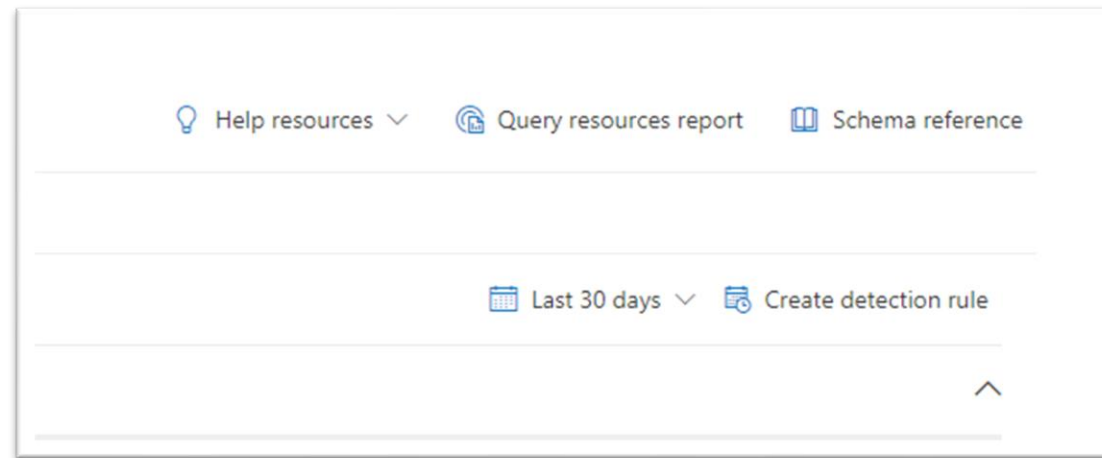
Device



Vulnerabilities and Configuration



Defender data-model schemaref





Common MDE misconfigurations

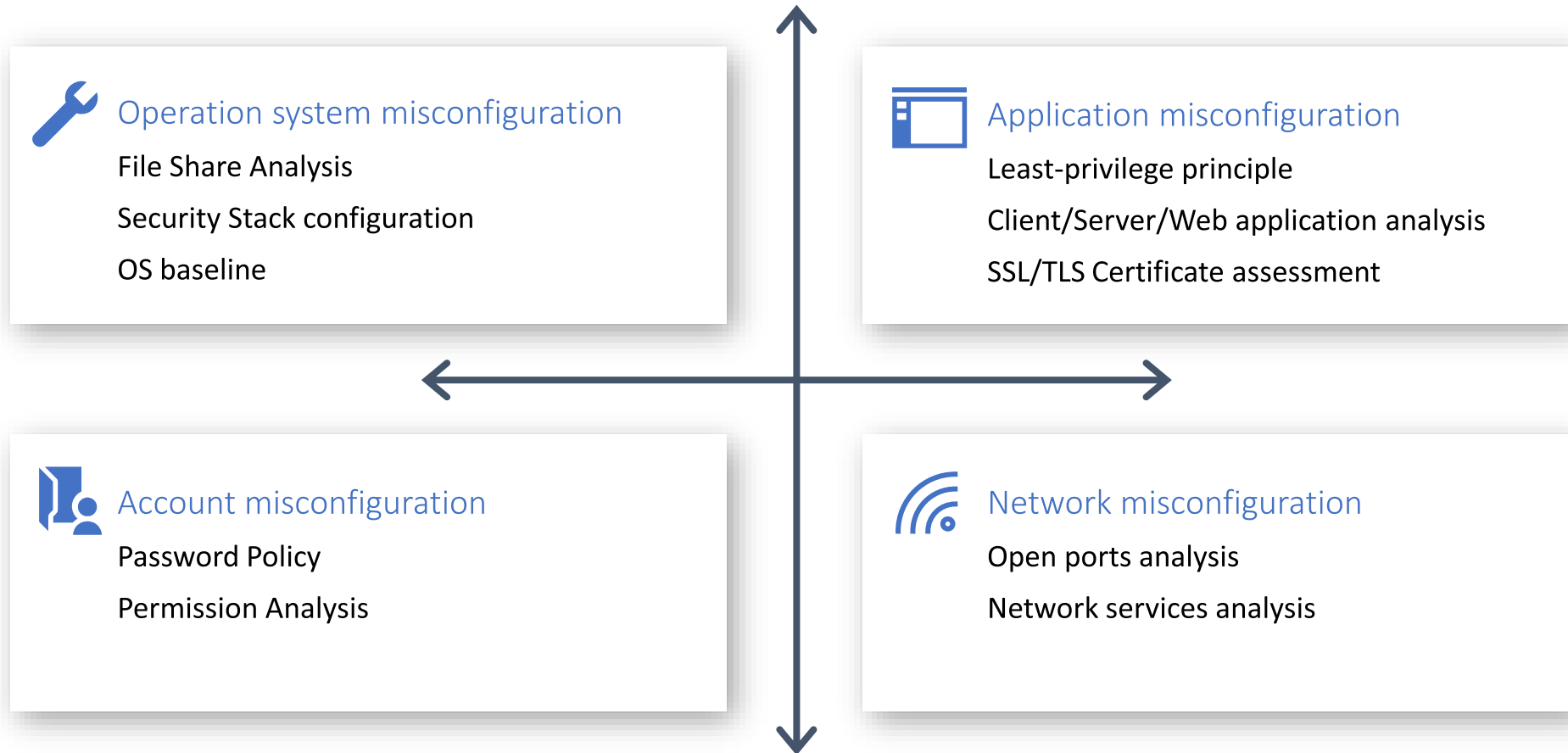
- Cloud Protection
 - MAPSReporting = 2
 - CloudBlockLevel = 2
 - CloudExtendedTimeout = 50
- Network Protection
 - EnableNetworkProtection = 1
- SubmitSamplesConsent = 3 (Always) | 1 (Safe Samples)
- Tamper Protection
- Firewall Auditing
 - auditpol /set /subcategory:"Filtering Platform Packet Drop" /failure:enable
 - auditpol /set /subcategory:"Filtering Platform Connection" /failure:enable
- 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>



Defender use cases for client admins

- TVM
 - Software Vulnerabilities and Inventory
 - Security Recommendations
 - Security Baselines
- Additional Hunting
 - Administrative Accounts
 - USB
 - Application Launch from USB
 - USB Device Usage
 - AppLocker
 - Firewall
 - PowerShell version usage
 - ASR Exclusions
- Reports
 - Device Health
 - Firewall Report
 - Device Usage

Threat and Vulnerability Management







Service Executables

Endpoints

Vulnerability management

Dashboard

Recommendations

Security recommendation	OS platform	Weaknesses	Related component	Threats	Exposed devices	Remediation type	Remediation activities	Impact
<input type="checkbox"/> Change service executable path to a common protected location	Windows	1	Operating system (Services)	 	41	<div></div>	Configuration cha... 0	▼ 0.75 + 6
<input type="checkbox"/> Fix unquoted service path for Windows services	Windows	1	Operating system (Services)	 	17	<div></div>	Configuration cha... 0	▼ 0.28 + 2

scid-3001
scid-3002























Firmware Updates

Endpoints

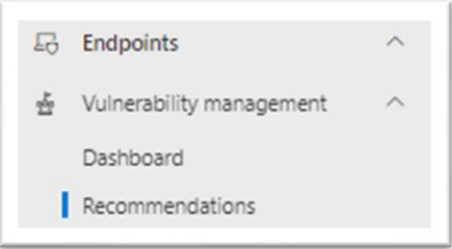
Vulnerability management



















Dashboard

Recommendations

<input type="checkbox"/>	Update Hp Integrated Lights-out 5 Firmware to version 2.72.0.0	Other	4	Hp Integrated Lights-out 5 Firmware	 	10 / 21		Firmware update	0	▼ <0.01
<input type="checkbox"/>	Update Hp Elitebook 820 G2 Firmware to version 1.31.0.0	Windows	5	Hp Elitebook 820 G2 Firmware	 	6 / 6		Firmware update	0	▼ <0.01
<input type="checkbox"/>	Update Dell Poweredge C6420 Firmware to version 2.15.1.0	Windows	1	Dell Poweredge C6420 Firmware	 	5 / 41		Firmware update	0	▼ <0.01
<input type="checkbox"/>	Update Dell Latitude 7290 Firmware to version 1.28.0.0	Windows	73	Dell Latitude 7290 Firmware	 	4 / 5		Firmware update	0	▼ <0.01
<input type="checkbox"/>	Update Dell Optiplex 7440 Aio Firmware to version 1.19.0.0	Windows	23	Dell Optiplex 7440 Aio Firmware	 	4 / 5		Firmware update	0	▼ <0.01
<input type="checkbox"/>	Update Dell Latitude 7275 Firmware to version 1.17.0.0	Windows	67	Dell Latitude 7275 Firmware	 	3 / 3		Firmware update	0	▼ <0.01
<input type="checkbox"/>	Update Dell Precision 3930 Rack Firmware to version 2.22.0.0	Windows	47	Dell Precision 3930 Rack Firmware	 	3 / 3		Firmware update	0	▼ <0.01
<input type="checkbox"/>	Update Hp Elitebook X360 1030 G3 Firmware	Windows	101	Hp Elitebook X360 1030 G3 Firmware	 	2 / 2		Firmware update	0	▼ <0.01
<input type="checkbox"/>	Update Dell Latitude 5300 2-in-1 Firmware to version 1.24.0.0	Windows	72	Dell Latitude 5300 2-in-1 Firmware	 	2 / 2		Firmware update	0	▼ <0.01

SMB and Shares



Security recommendation	OS platform	Weaknesses	Related component	Threats	Exposed devices	Remediation type	Remediation activities	Impact ⓘ	Tags
<input type="checkbox"/> Enable 'Microsoft network client: Digitally sign communications (always)'	Windows	1	Network	 	15	 Configuration change	0	▼ 0.15 + 0.51	COVID-19
<input type="checkbox"/> Disable SMBv1 client driver	Windows	1	Network	 	2	 Configuration change	0	▼ 0.04 + 0.13	
<input type="checkbox"/> Set folder access-based enumeration for shares	Windows	1	Operating system (Shares)	 	14	 Configuration change	0	▼ 0.02 + 7.32	
<input type="checkbox"/> Disable 'Insecure guest logons' in SMB	Windows	1	Operating system	 	13	 Configuration change	0	▼ <0.01 + 0.01	COVID-19
<input type="checkbox"/> Disable SMBv1 server	Windows	1	Network	 	3	 Configuration change	0	▼ <0.01 + 0.00	
<input type="checkbox"/> Disable sending unencrypted password to third-party SMB servers	Windows	1	Network	 	0	 Configuration change	0	▼ 0.00 + 0.00	COVID-19

Vulnerability Timeline

Event timeline

New vulnerabilities
340







New zero-day vulnerabilities
0

Exploitable vulnerabilities
3

New configuration assessments
0

[Export](#)

Filters: Date events occurred: 12/12/2022-1/12/2023

Date (UTC) ↓	Event	Related component	Originally impacted de
<input type="checkbox"/> Jan 12, 2023 12:00 ...	 Oracle Jre has 7 new vulnerabilities, impacting 74k devices	Oracle Jre	74k (45%)
<input type="checkbox"/> Jan 12, 2023 12:00 ...	 Oracle Jdk has 10 new vulnerabilities, impacting 1.33k devices	Oracle Jdk	1.33k (1%)
<input type="checkbox"/> Jan 12, 2023 12:00 ...	 Oracle Mysql has 32 new vulnerabilities, impacting 100 devices	Oracle Mysql	100 (<1%)
<input type="checkbox"/> Jan 12, 2023 12:00 ...	 Oracle Mysql Workbench has 5 new vulnerabilities, impacting 171 devices	Oracle Mysql Workbench	171 (<1%)
<input type="checkbox"/> Jan 12, 2023 12:00 ...	 Oracle Mysql Workbench for Mac has 5 new vulnerabilities, impacting 16 devices	Oracle Mysql Workbench for Mac	16 (<1%)
<input type="checkbox"/> Jan 12, 2023 12:00 ...	 Apple Iphone Os has a new vulnerability, impacting 5 devices	Apple Iphone Os	5 (<1%)

Filter

[Clear filters](#)

Type

- ☐ New vulnerability
- ☐ New public exploit
- ☐ Exploit added to an exploit kit
- ☐ Exploit was verified
- ☐ New zero-day vulnerability
- ☐ New security update for zero-day vulnerability
- ☐ New configuration assessment

Originally impacted devices (%)above 0%

Date events occurred

Between

Dec 12, 2022

And

Jan 12, 2023

Vulnerability Notifications

Vulnerability notifications > **Create rule**

☒ Basics

☐ Notification settings

☐ Recipients

☐ Review rule

Name email notification

Create a notification rule to send an email when there is a new policy

Name *

New policy

Description

Enter a description for your notification rule

☒ Activate notification rule

Vulnerability notifications > **Create rule**

☒ Basics

☒ Notification settings

☐ Recipients

☐ Review rule

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.

Clients

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



Identifying Logins where 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

USB

DeviceEvents

```
| where ActionType == 'PnpDeviceConnected'  
| extend PNP = parsejson(AdditionalFields)  
| extend ClassName = PNP.ClassName  
| extend PnPDeviceId = PNP.DeviceId  
| extend DeviceDescription = PNP.DeviceDescription  
| extend VendorIds = PNP.VendorIds  
| where PnPDeviceId startswith '@'USBSTOR\  
| project Timestamp, DeviceName, DeviceId, ClassName,  
DeviceDescription, PnPDeviceId, VendorIds, ReportId
```

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
```

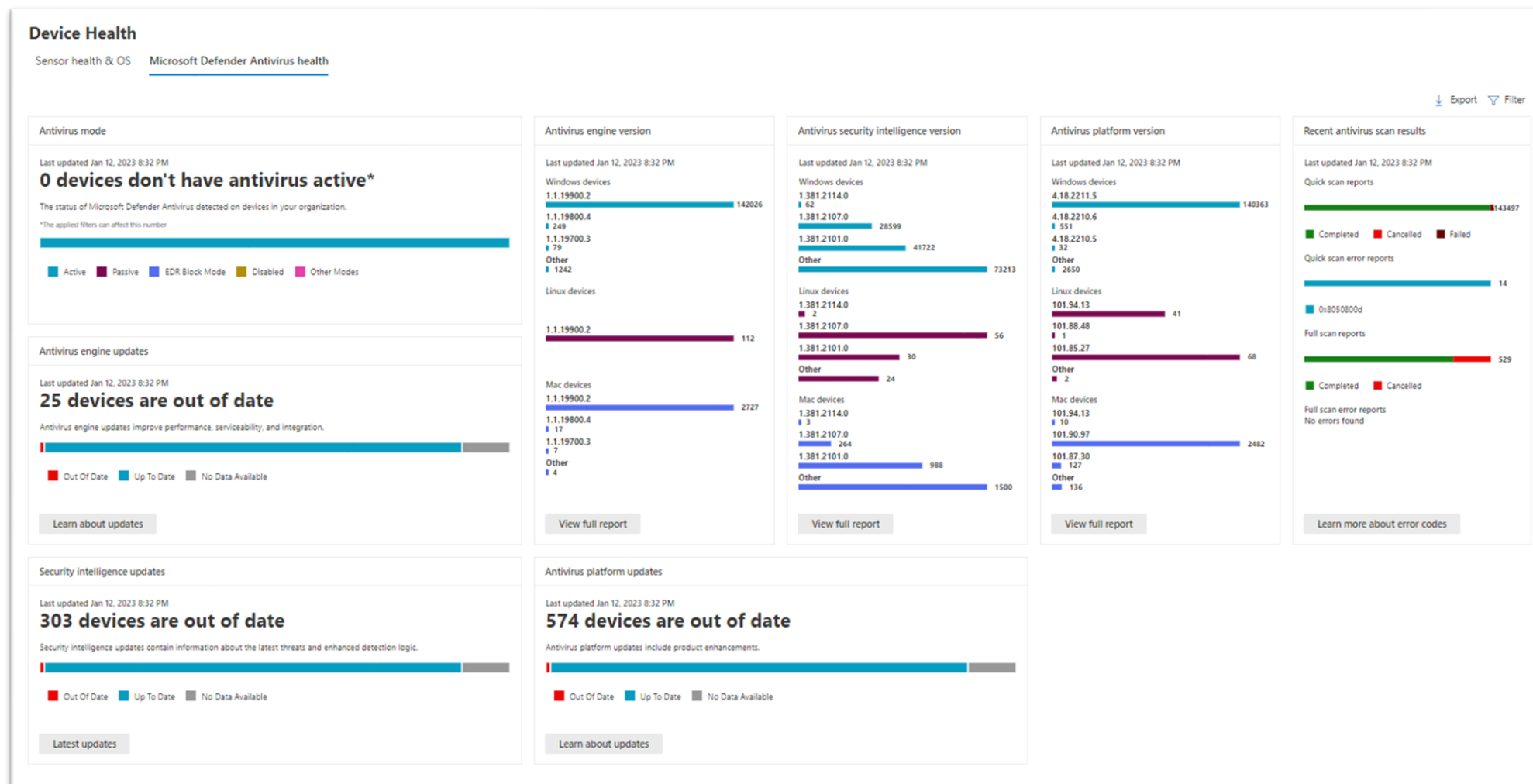


PowerShell Version

DeviceImageLoadEvents

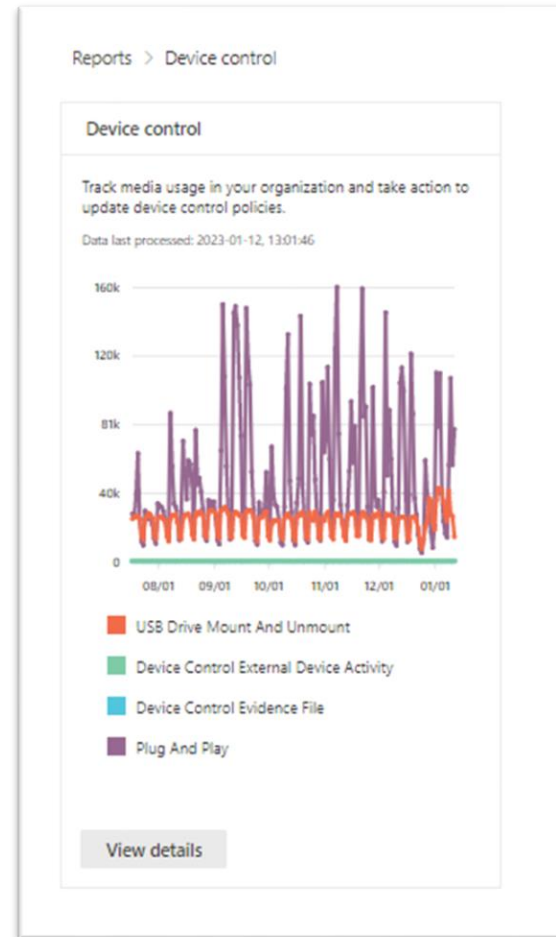
| where InitiatingProcessFileName =~ 'powershell.exe' and FileName
in~('system.management.automation.ni.dll','System.Management.Auto
mation.dll') and FolderPath matches regex @"[12]\.(\d)+\.(\d)+\.(\d)+"

Device Health Report



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

USB Report



2022-09-18

USB drive mount and unmount (13 754) Device Control external device activity (0) Device Control evidence file (0) Plug and Play (31 264)

USB Mount
10 563

USB Unmount
3 191

USB
22 897

USBDevice
840

SmartCard
5

CDROM
69

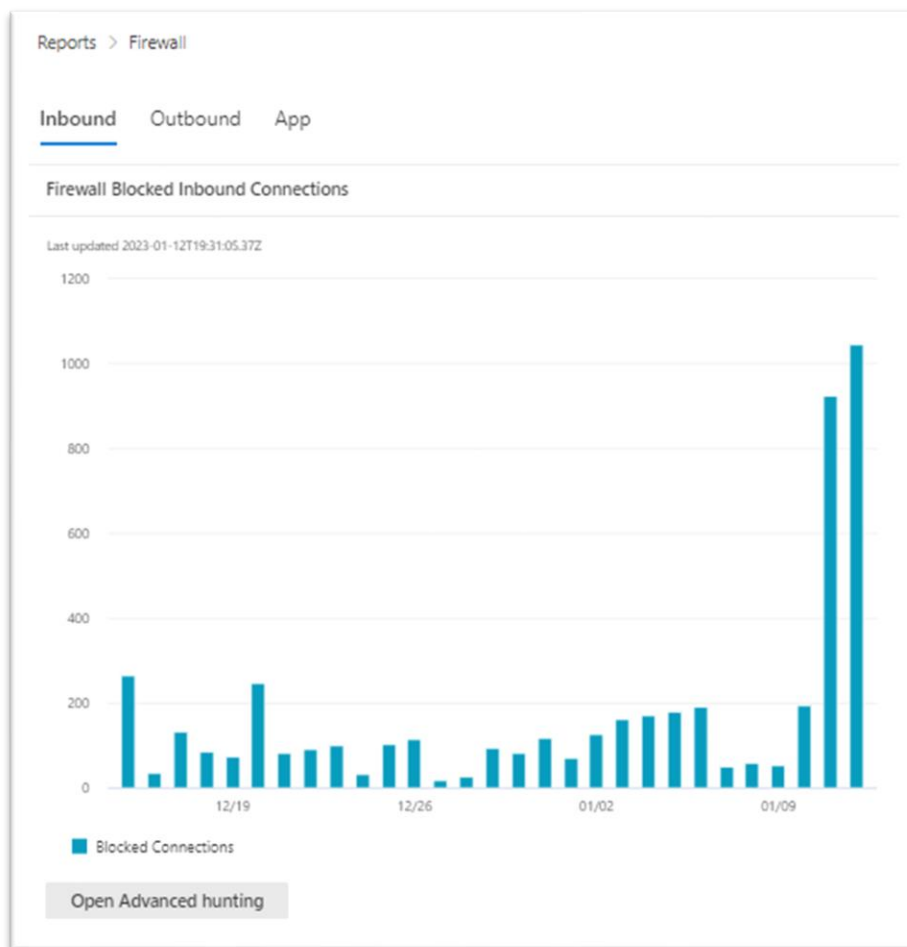
WPD
1 907

DiskDrive
349

Bluetooth
1 483

Printer
3 714

Firewall Report





Important M365D changes

- MDE Server Agent
- MDI Action Account
- Preview: M365D Unified RBAC
- Preview: Query Consumption
- Tamper Protection

MDE Server Agent

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

Go Upgrade!

<https://techcommunity.microsoft.com/t5/microsoft-defender-for-endpoint/defending-windows-server-2012-r2-and-2016/ba-p/2783292>



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).

MDI Action Account

Defender for Identity release 2.193

Released October 30, 2022

- **New security alert: Abnormal Active Directory Federation Services (AD FS) authentication using a suspicious certificate**

This new technique is linked with the infamous NOBELIUM actor and was dubbed "MagicWeb" – it allows an adversary to implant a backdoor on compromised AD FS servers, which will enable impersonation as any domain user and thus access to external resources. To learn more about this attack, read [this blog post](#).

- Defender for Identity can now use the LocalSystem account on the domain controller to perform remediation actions (enable/disable user, force user reset password), in addition to the gMSA option that was available before. This enables out of the box support for remediation actions. For more information, see [Microsoft Defender for Identity action accounts](#).
- Version includes improvements and bug fixes for internal sensor infrastructure.

MDI Action Account

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

General

Sensors

Directory services accounts

Manage action accounts

VPN

Health issues

Portal redirection

About

Entity tags

This list contains credentials that sensors can use to perform actions on on-premises Active Directory users, such as disable user, reset user password and more. 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

Filter

 Filters

Domain: **Any** ▾

Group managed service account: **Any** ▾

⬇ Export + Add credentials

1 item  Customize columns

Account	Domain	Group managed service account ⓘ
<input type="checkbox"/> mdi_svc02	CONTOSO.COM	True

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

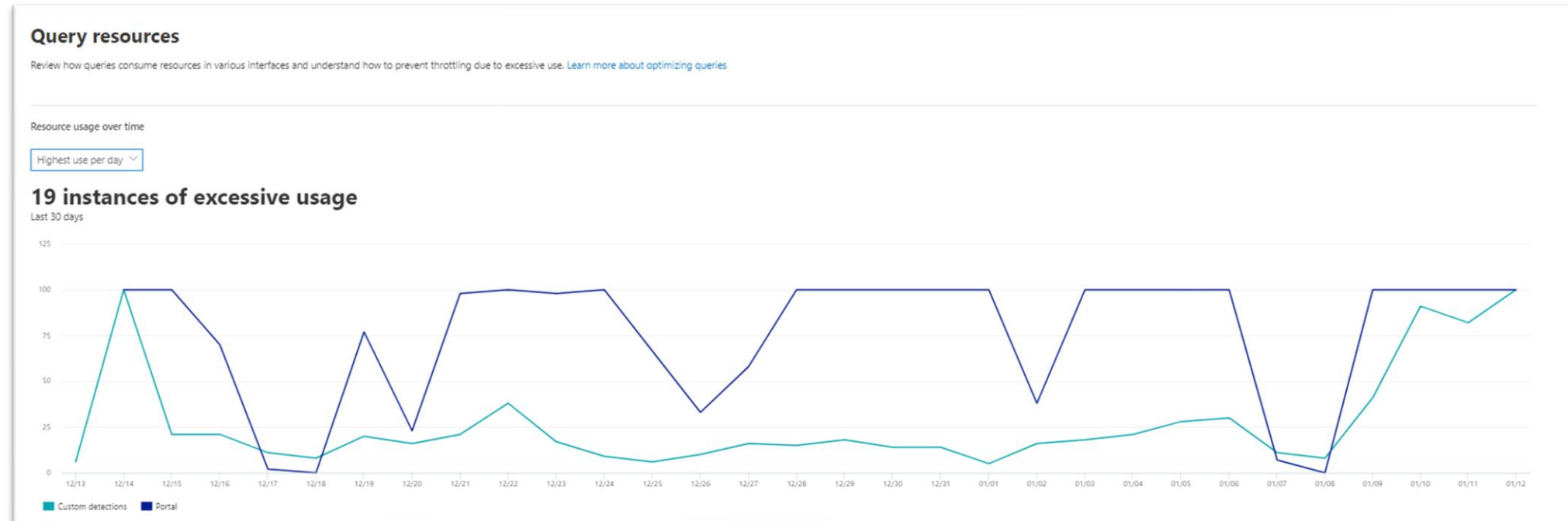
Roles give users permission to view data and complete tasks in Microsoft 365 Defender. Help keep your organization secure

[i](#) Import your existing roles from other data sources.

[+](#) Create custom role [≡](#) Import roles [✎](#) Edit [🗑](#) Delete roles

<input type="checkbox"/> Role name	Description	Data source
<input type="checkbox"/> M365 Defender Administrators	⋮	All Scopes
<input type="checkbox"/> Onevinn MDR Security Analysts	⋮	All Scopes
<input type="checkbox"/> Onevinn MDR Security Administrators	⋮	All Scopes

M365D Query Consumption



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

Tamper Protection - Exclusions

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

