

Defender for Endpoint Internals

Questions by text?



7540



Speakers



Lewis Barry

Principal Security Architect
inforcer

 [in/lewis-barry](#)



Nathan McNulty

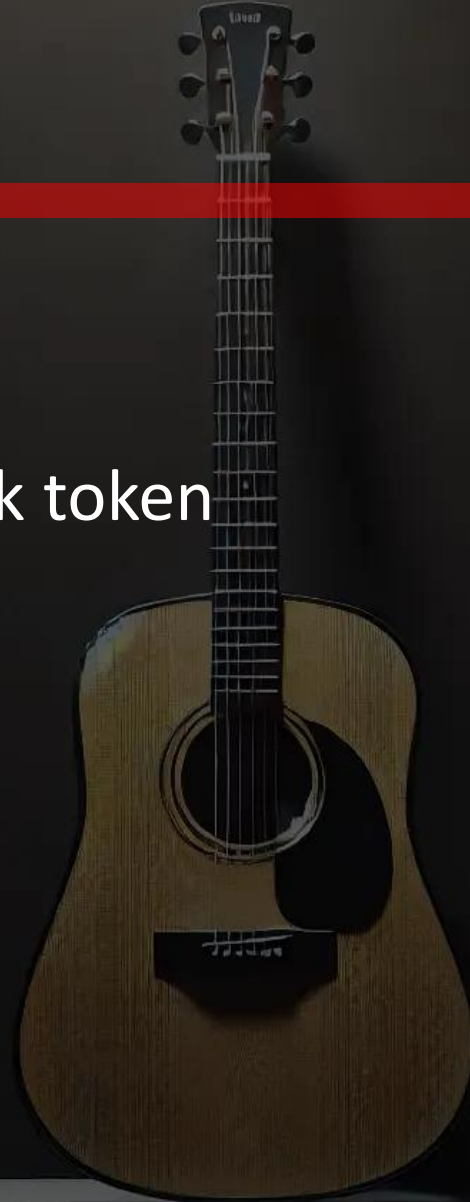
Sr. Security Solutions Architect
Patriot Consulting

 [@nathanmcnulty](#)

 [in/nathanmcnulty](#)

Rules of Engagement

- ◆ Put your bags under the seat
- ◆ Ask questions as we go
- ◆ If you make the room laugh, you get a drink token
- ◆ Tokens limited to 1 per person!!!!



Agenda

- ◆ Defender Antivirus
 - ◆ Protection engines
 - ◆ Attack surface reduction
 - ◆ Policy and Exclusion guidance
 - ◆ Passive mode
- ◆ Defender for Endpoint (EDR sensor)
 - ◆ XDR architecture
 - ◆ Telemetry sources
 - ◆ IR capabilities
 - ◆ Threat and vulnerability management
- ◆ Cloud Protection / Attack Disruption
- ◆ Security settings management
- ◆ Troubleshooting

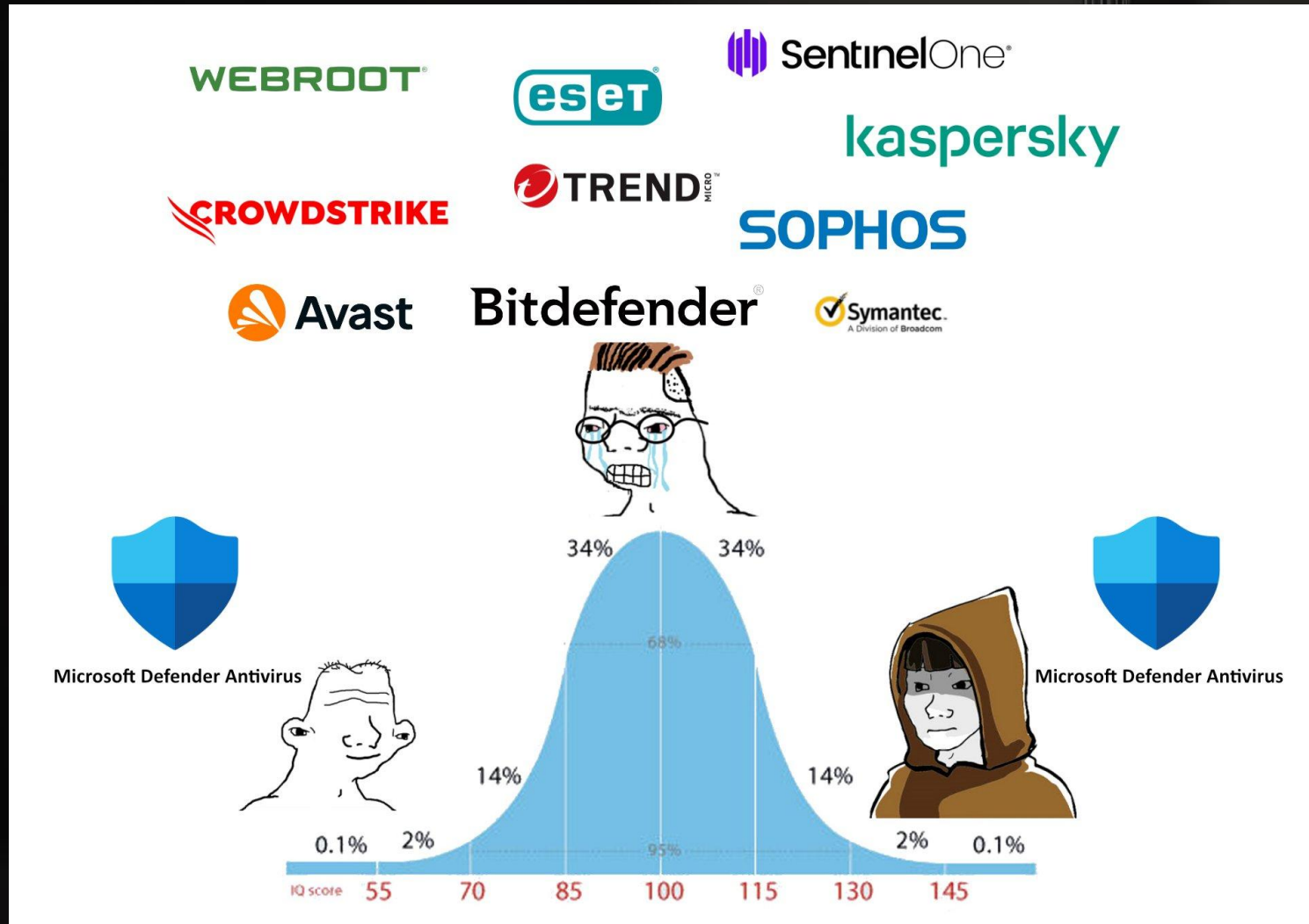


Before we go deeper...

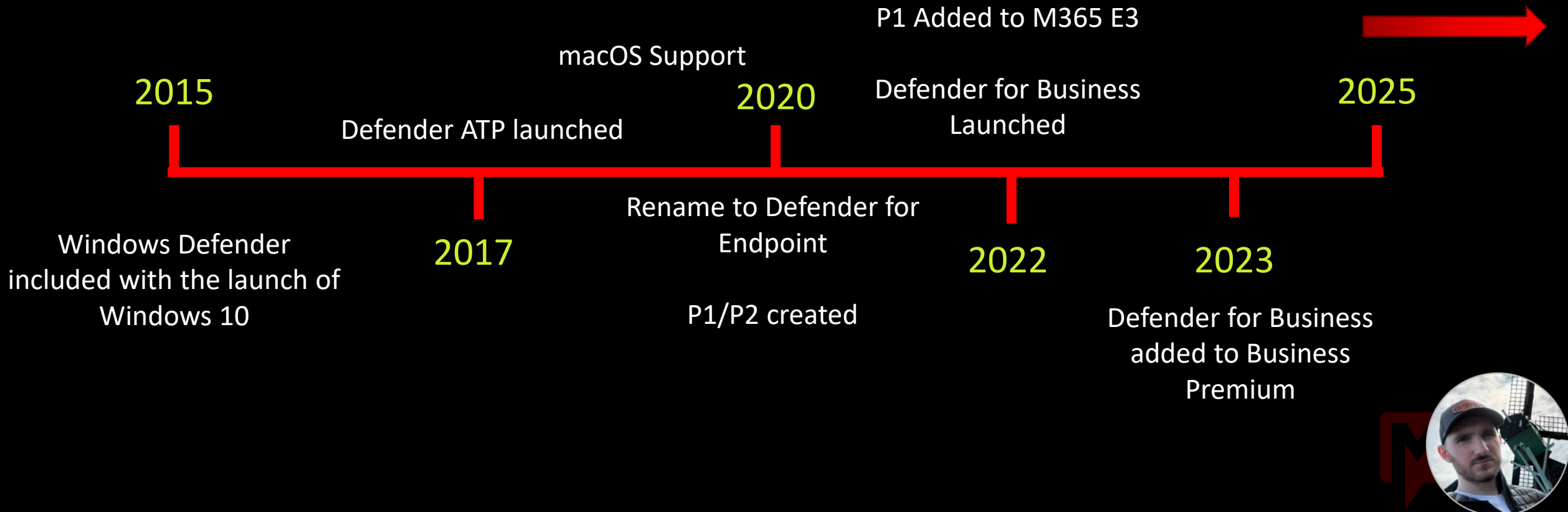
- ◆ Reminder of the role AV/EDR plays
- ◆ Maturity mapping & adding layers
- ◆ Making the right purchase **before** you implement



So, you picked Defender for Endpoint...



10 Years of Defender for Endpoint



Where should Defender sit?



'Left of Bang'

The Defenders



'Right of Bang'

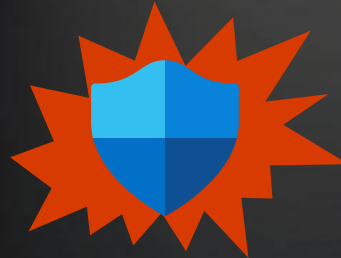
The Responders



Attack Timeline

'Left of Bang'

Prevent or lessen impact of attacks



'Right of Bang'

Rapidly and effectively manage attacks

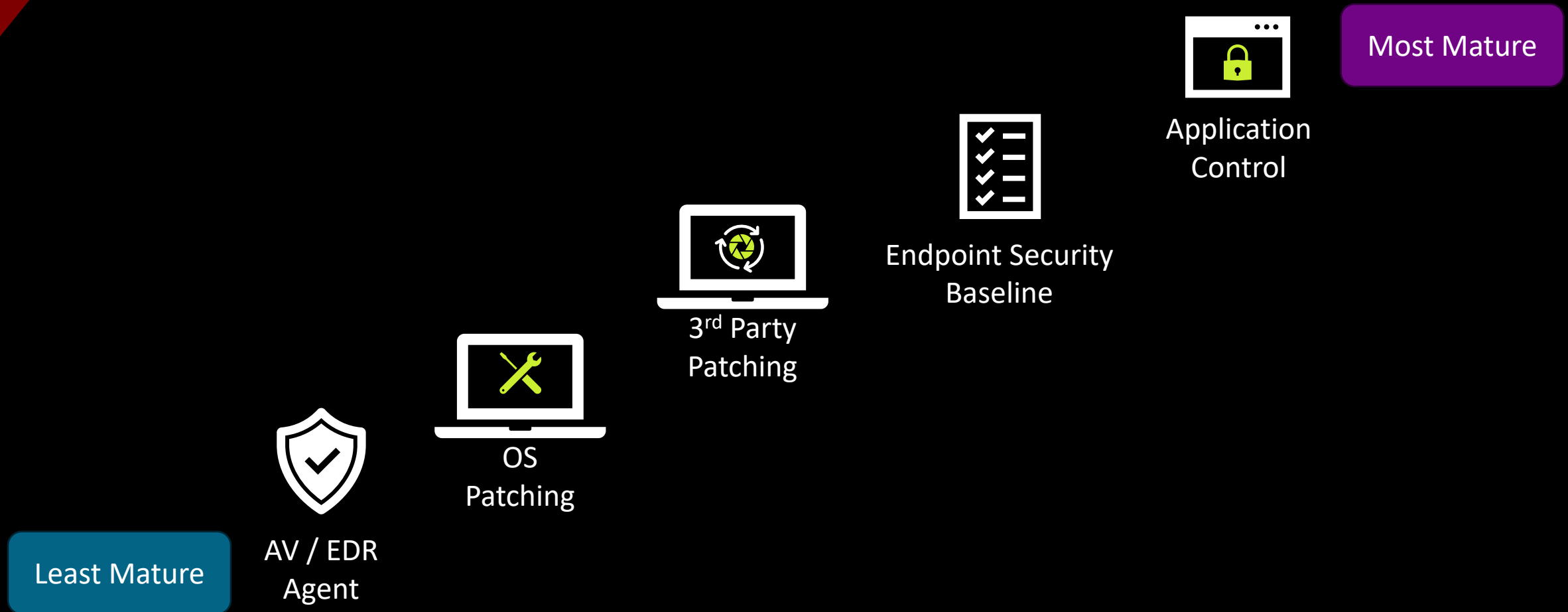


The job will never be 'done' or 'perfect', but it's important to keep doing (like cleaning a house)

NIST Cybersecurity Framework v2



Endpoint Security Maturity Scale



Most Adopted

Least Adopted

MMS

Endpoint Security Maturity Scale



AV / EDR
Agent



OS
Patching



3rd Party
Patching



Endpoint Security
Baseline



Application
Control



Licensing & Protection Debunked

*Yes, we're
going there!*

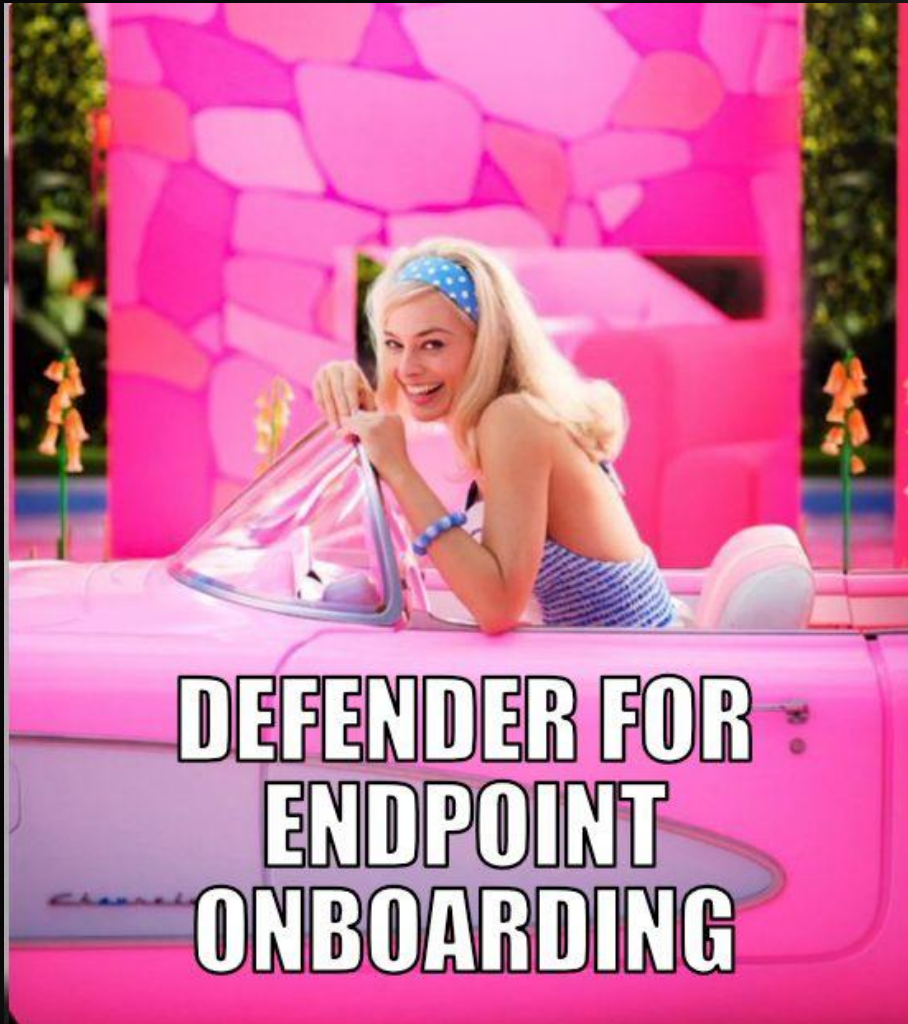
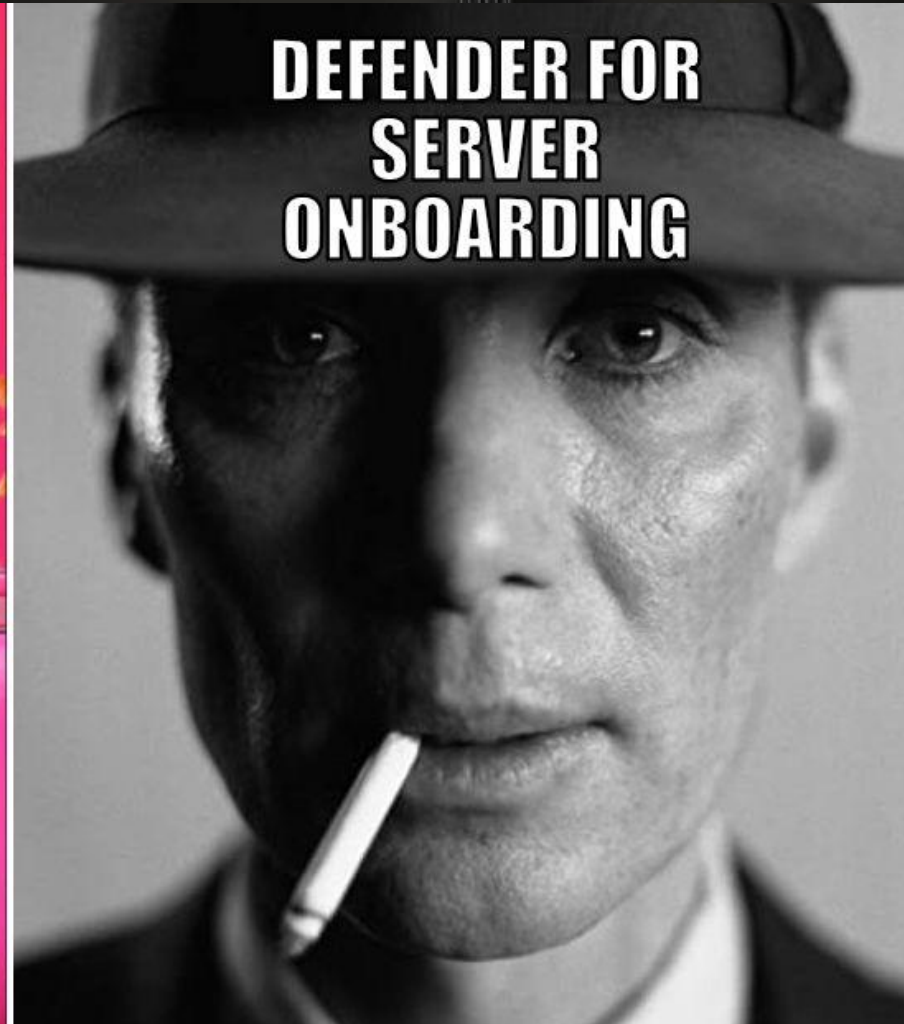
- ◆ Defender for Endpoint P1 – Included with M365 E3
- ◆ Defender for Endpoint P2 – Included with M365 E5
- ◆ Defender for Business – Included with M365 Business Premium

The AV protection is **the same** across all editions of Defender... Even consumer!

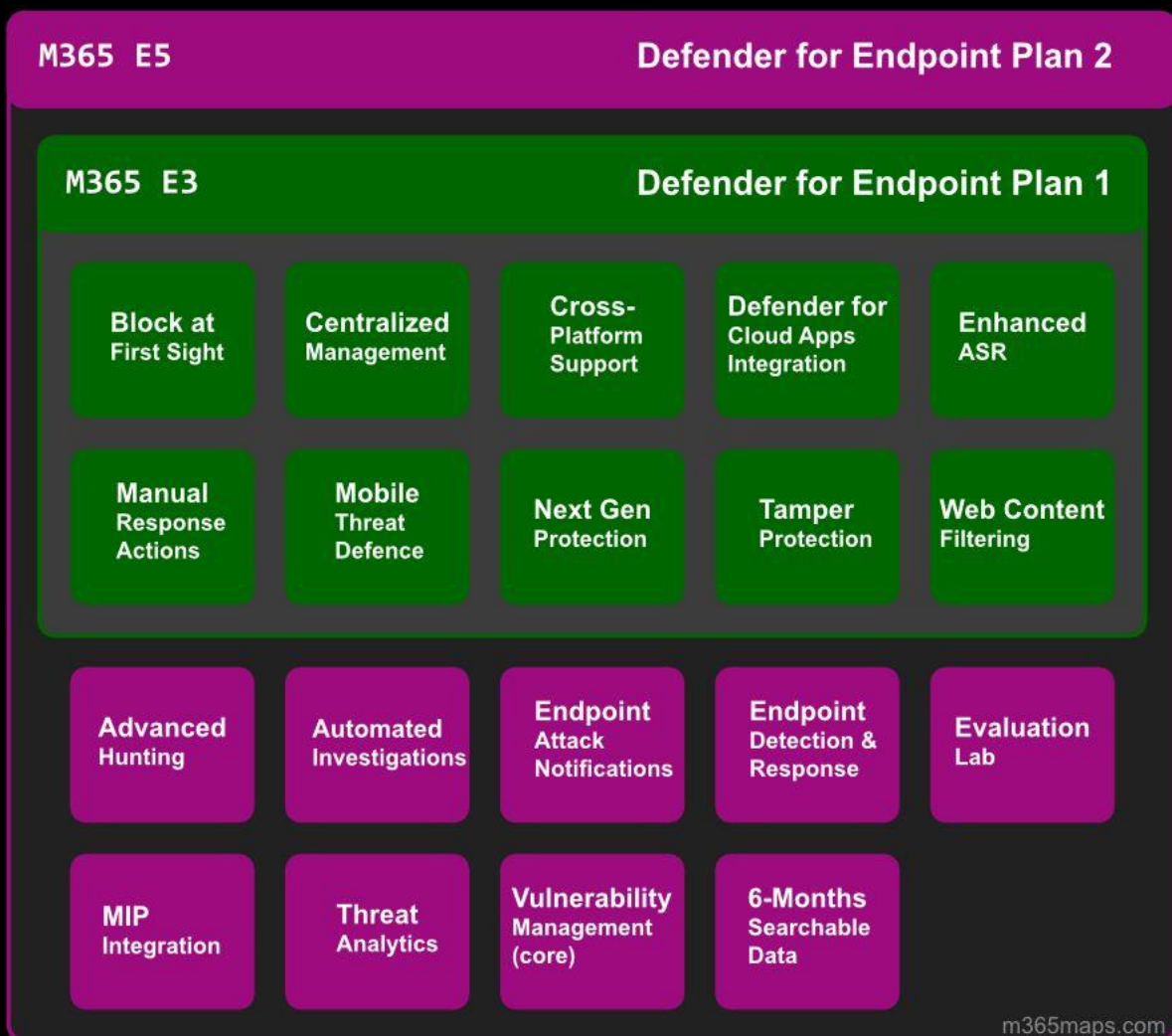
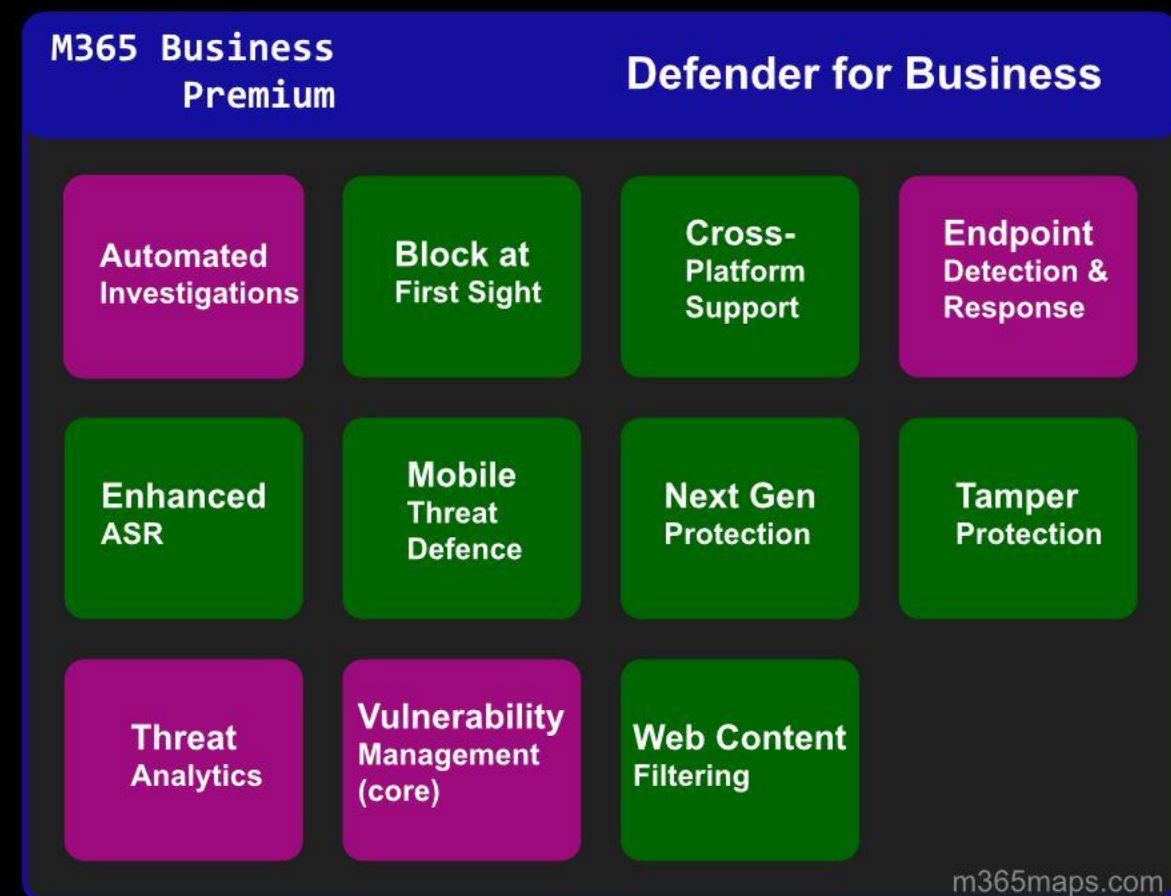


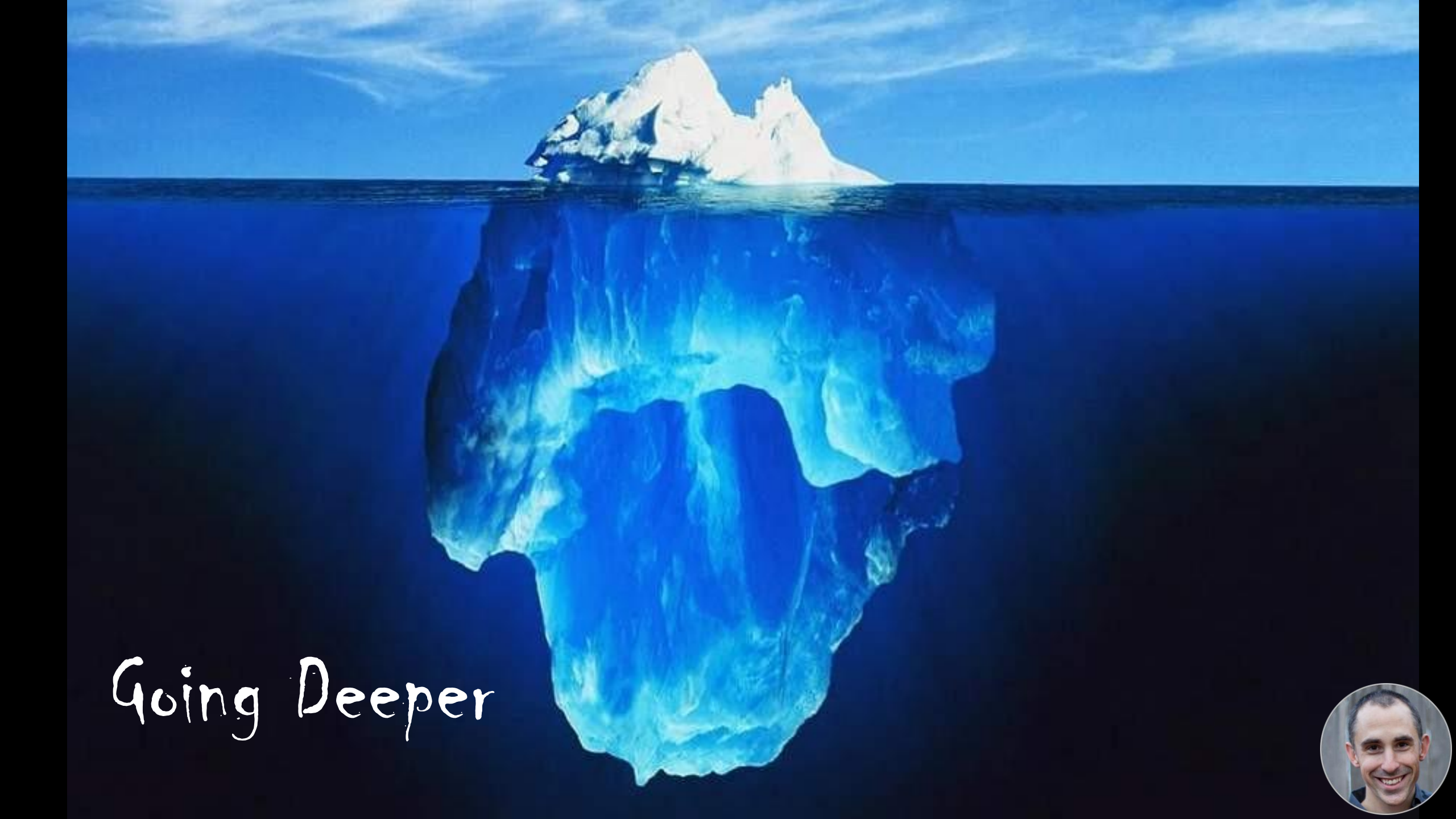
Defender for Server

*No, we're not
going there!*



Licensing and Protection Levels



A large iceberg floats in a deep blue ocean under a clear sky. The visible tip is small and jagged, while the submerged portion is much larger and more complex in shape, illustrating the concept of 'going deeper' into a subject.

Going Deeper



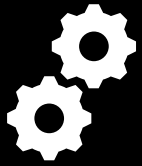
Protection engines

- ◆ ELAM and WdBoot
- ◆ WdFilter driver registers callbacks to analyze:
 - ◆ Process Creation, Image Load, Thread Creation, Image Verification, Object Operations, and Registry Operations
- ◆ Less static analysis, more heuristics and ML models
- ◆ File system filters
- ◆ Network inspection
- ◆ Cloud and caching



ELAM and WdBoot

Early Launch Antimalware



1. BIOS/UEFI



2. Windows
Boot Manager
starts OS loader



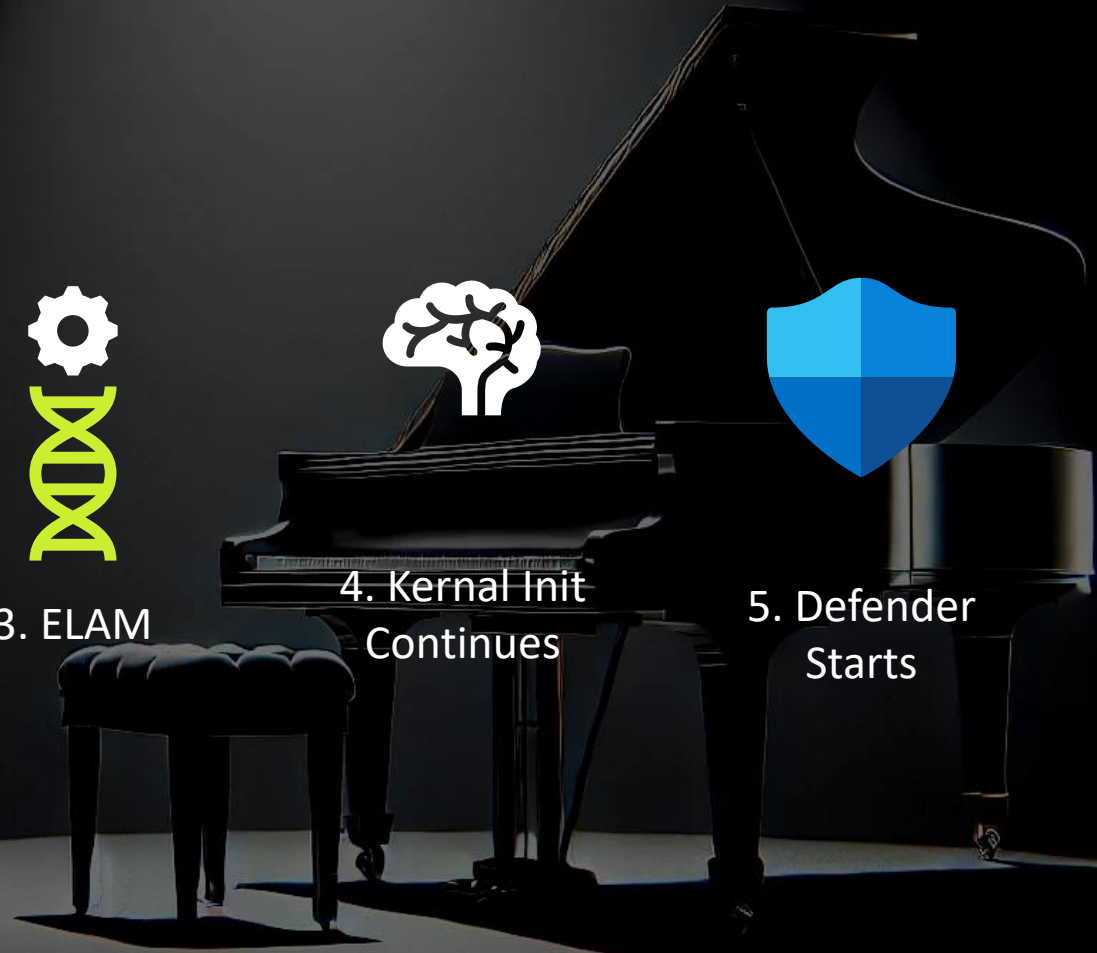
3. ELAM



4. Kernel Init
Continues



5. Defender
Starts



WdFilter.sys | Windows Defender Filter Driver



- ◆ Core part of Windows Defender
- ◆ Provides real-time file and registry protection



Found at:

`C:\Windows\System32\drivers\WdFilter.sys`



320000 - 329998: FSFilter Anti-Virus

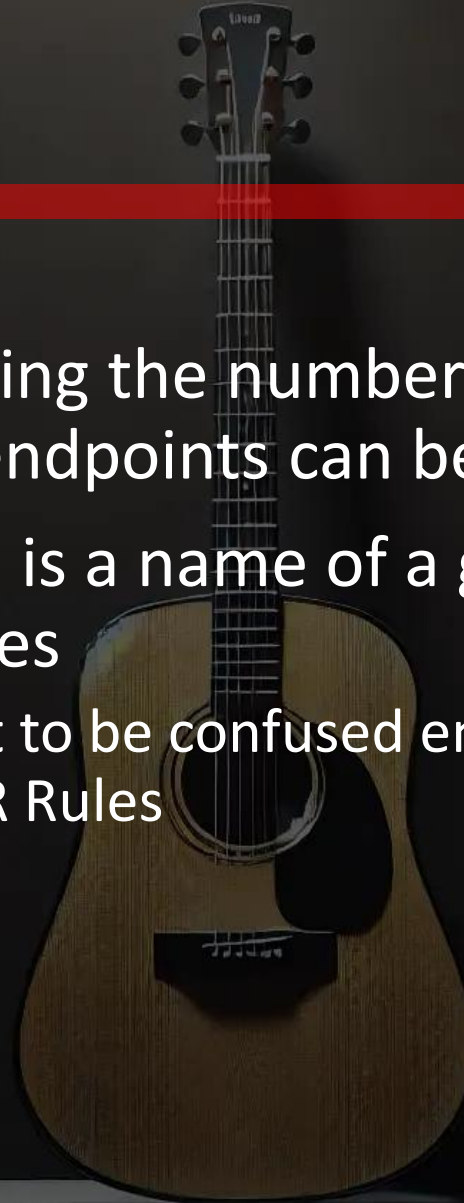
 Expand table

Minifilter	Altitude	Company
brynhldr.sys	329400	Activision Blizzard, Inc.
IstroDrv.sys	329380.5	IstroSec s.r.o.
XRFilter.sys	329375	XRITDX
tbmninifilter.sys	329370	Confluera Inc
CovAgent.sys	329365	Field Effect Software
trfsfilter.sys	329360	NetSecurity Corp
SentinelMonitor.sys	329355.5	SentinelOne, Inc.
ReveFltMgr.sys	329350	REVE Antivirus
MagicArmorDrv.sys	329345.5	Beijing VEDA Information Technology Co. Ltd

Attack Surface Reduction



- ◆ Reducing the number of ways your endpoints can be exploited
- ◆ “ASR” is a name of a group of features
 - ◆ Not to be confused entirely with ASR Rules



Attack Surface Reduction

- ◆ Attack Surface Reduction Rules
 - ◆ LUA and hidden exclusions!
- ◆ App Control for Windows/Business
- ◆ Controlled Folder Access
- ◆ Device Control
- ◆ Network Protection
- ◆ Exploit Protection
- ◆ Windows Firewall



ASR rule name:

Block abuse of exploited vulnerable signed drivers

Block Adobe Reader from creating child processes

Block all Office applications from creating child processes

Block credential stealing from the Windows local security authority subsystem (lsass.exe)

Block executable content from email client and webmail

Block executable files from running unless they meet a prevalence, age, or trusted list criterion

Block execution of potentially obfuscated scripts

Block JavaScript or VBScript from launching downloaded executable content

Block Office applications from creating executable content

Block Office applications from injecting code into other processes

Block Office communication application from creating child processes

Block persistence through WMI event subscription

Block process creations originating from PSEXEC and WMI commands

Block rebooting machine in Safe Mode

Block untrusted and unsigned processes that run from USB

Block use of copied or impersonated system tools

Block Webshell creation for Servers

Block Win32 API calls from Office macros

Use advanced protection against ransomware





```
GetRuleInfo = function()
  -- function num : 0_0
  local l_1_0 = {}
  l_1_0.Name = "Block credential stealing from the Windows local security authority subsystem (lsass.exe)"
  l_1_0.Description = "Windows Defender Exploit Guard detected an attempt to extract credentials from LSASS."
  return l_1_0
end
```

```
GetMonitoredLocations = function()
  -- function num : 0_1
  local l_2_0 = {}
  l_2_0["%windir%\system32\lsass.exe"] = 2
  return 7, l_2_0
end
```

```
GetPathExclusions = function()
  -- function num : 0_2
  local l_3_0 = {}
  l_3_0["%windir%\system32\WerFault.exe"] = 2
  l_3_0["%windir%\system32\WerFaultSecure.exe"] = 2
  l_3_0["%windir%\system32\mrt.exe"] = 2
  l_3_0["%windir%\system32\svchost.exe"] = 2
  l_3_0["%windir%\system32\wbem\WmiPrvSE.exe"] = 2
  l_3_0["%programfiles(x86)%\Microsoft Intune Management Extension\Microsoft.Management.Services.IntuneWindowsA"]
  return l_3_0
end
```



Block process creations originating from PsExec and WMI commands

This rule blocks processes created through [PsExec](#) and [WMI](#) from running. Both PsExec and WMI can remotely execute code. There's a risk of malware abusing functionality of PsExec and WMI for command and control purposes, or to spread an infection throughout an organization's network.

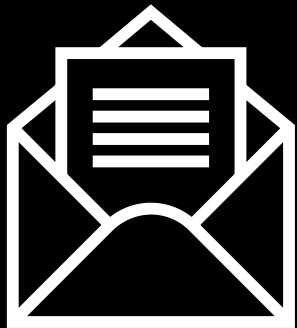
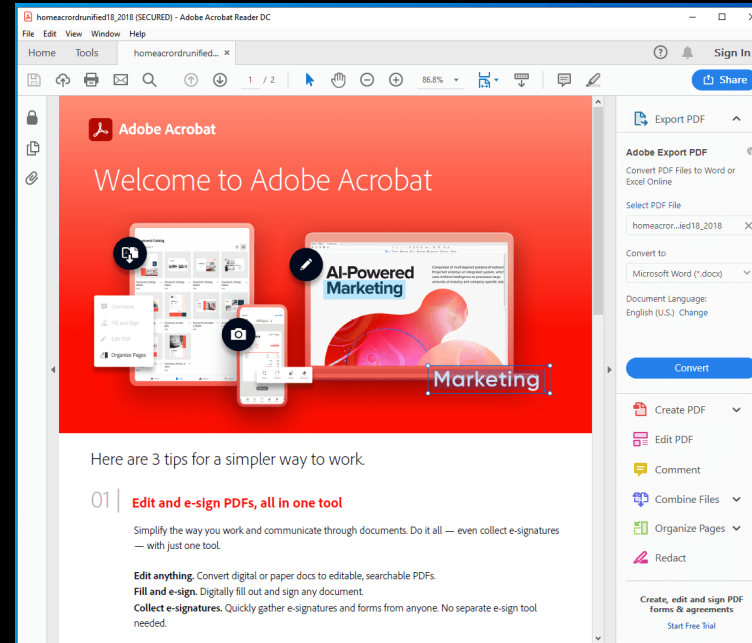
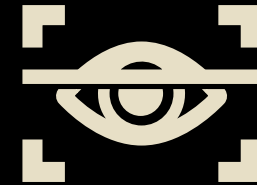
⚠ Warning

Only use this rule if you're managing your devices with [Intune](#) or another MDM solution. This rule is incompatible with management through [Microsoft Endpoint Configuration Manager](#) because this rule blocks WMI commands the Configuration Manager client uses to function correctly.

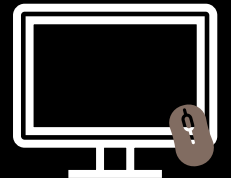


Attack Surface Reduction Rules

Block Adobe Reader from creating child processes



ASR Rule



REMOTE_ACCESS.exe



Attack Surface Reduction Rules

START IN AUDIT MODE



OWNED

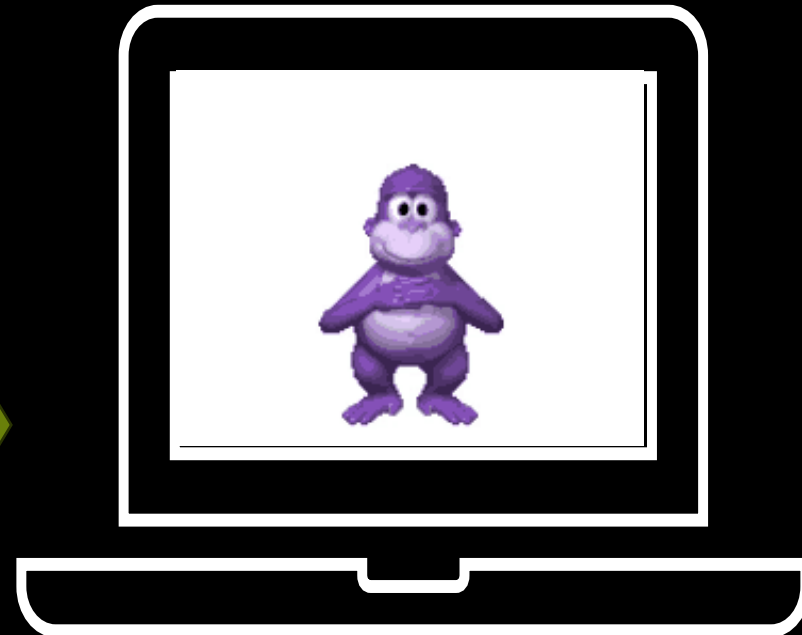
ASR Rules



Controlled Folder Access

Default folders

c:\Users\<username>\Documents
c:\Users\Public\Documents
c:\Users\<username>\Pictures
c:\Users\Public\Pictures
c:\Users\Public\Videos
c:\Users\<username>\Videos
c:\Users\<username>\Music
c:\Users\Public\Music
c:\Users\<username>\Favorites



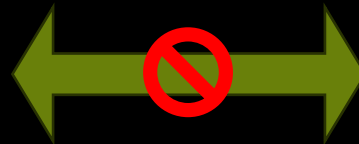
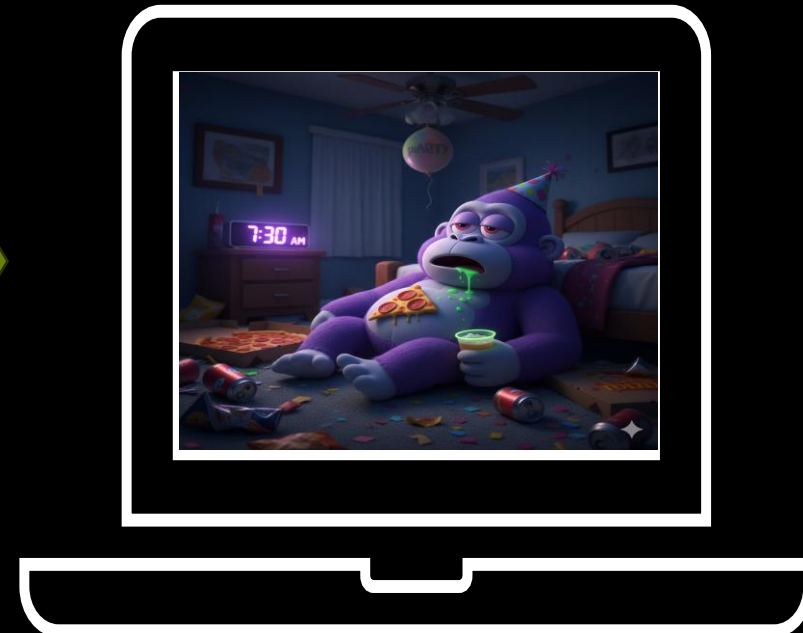
BonziBuddy.exe



Controlled Folder Access

Default folders

c:\Users\<username>\Documents
c:\Users\Public\Documents
c:\Users\<username>\Pictures
c:\Users\Public\Pictures
c:\Users\Public\Videos
c:\Users\<username>\Videos
c:\Users\<username>\Music
c:\Users\Public\Music
c:\Users\<username>\Favorites



BonziBuddy.exe



←

Windows Defender Security Center

—

□

×

☰

🏠

🛡️

💖

🔊

📁

👤

⚙️

Allow an app through Controlled folder access

If Controlled folder access has blocked an app you trust, you can add it as an allowed app. This allows the app to make changes to protected folders.

+

Add an allowed app

Most of your apps will be allowed by Controlled folder access without adding them here. Apps determined by Microsoft as friendly are always allowed.

test.exe

c:\apps

▼

Administrator: Windows PowerShell

Windows PowerShell

Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> Add-MpPreference -ControlledFolderAccessAllowedApplications "c:\apps\test.exe"

PS C:\Windows\system32>



Device Control

- Block by external device type
 - Removable devices
 - Printers
 - Windows Portal Devices (phones, etc.)
- Removable Storage Access Control
 - Control by PNP device attributes
 - Granular control of read vs write depending on device details and other conditions
- Printers
- Bluetooth devices



Network Protection – Part of AV policy

- ◆ Built on Zeek!
- ◆ SmartScreen
- ◆ Web content filtering (MDE)
- ◆ Network indicators (MDE)
- ◆ Requires Defender AV running in Active mode

Home > Endpoint security | Antivirus > Win - OIB - ES - Defender Antivirus - D - AV Configuration - v3.3 >

Edit Policy

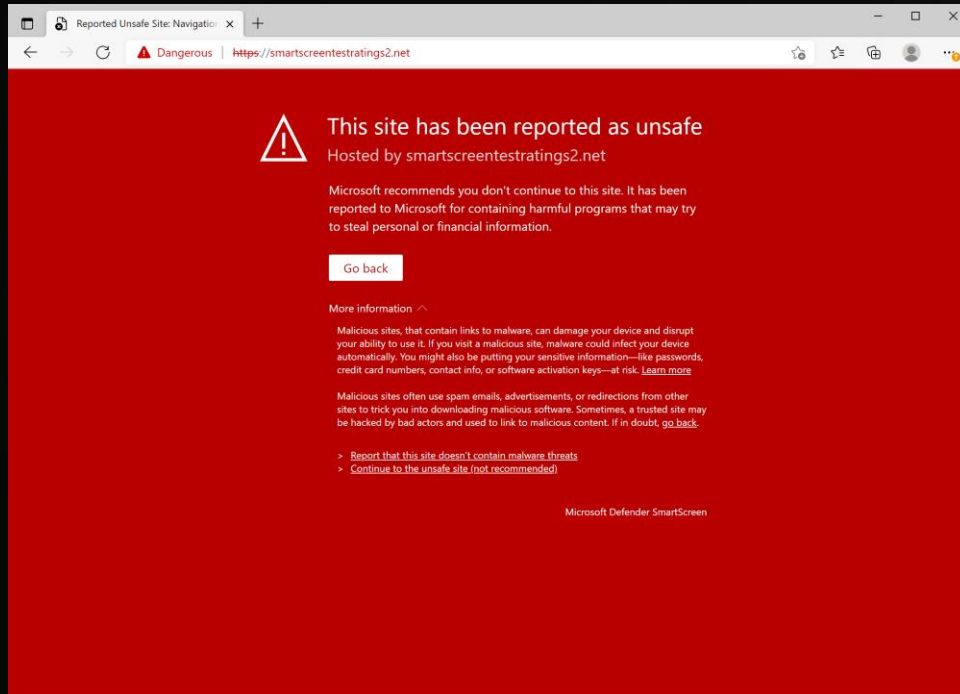
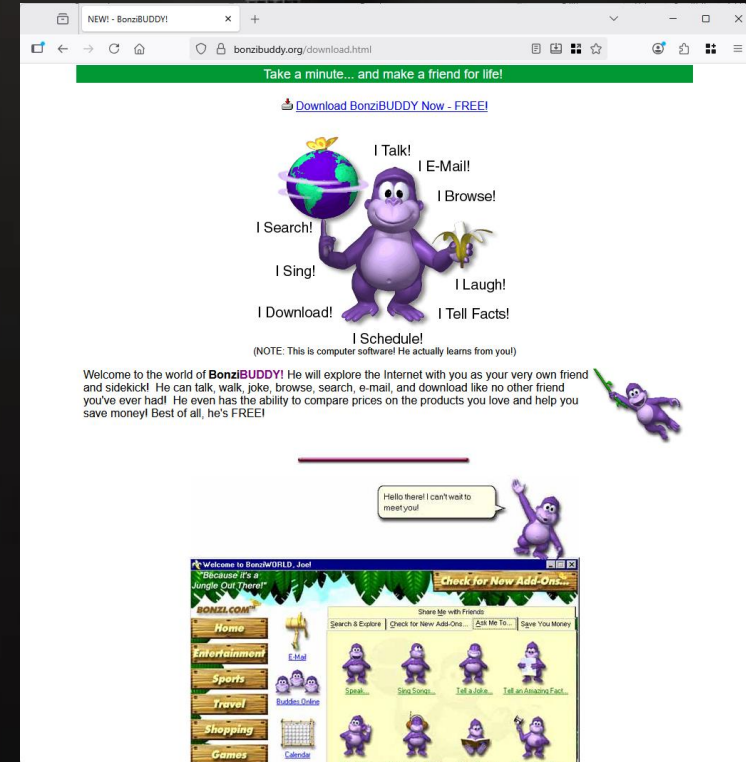
Microsoft Defender Antivirus

Avg CPU Load Factor	50
Archive Max Depth	☐ Not Configured
Archive Max Size	☐ Not Configured
Check For Signatures Before Running Scan	Enabled
Cloud Block Level	High
Cloud Extended Timeout	☒ Configured
Days To Retain Cleaned Malware	☐ Not Configured
Disable Catchup Full Scan	Disabled
Disable Catchup Quick Scan	Disabled
Enable Low CPU Priority	Enabled
Enable Network Protection	Enabled (block mode)
Excluded Extensions	

+ Add — Remove ← Import → Export



“SmartScreen Doesn’t work”

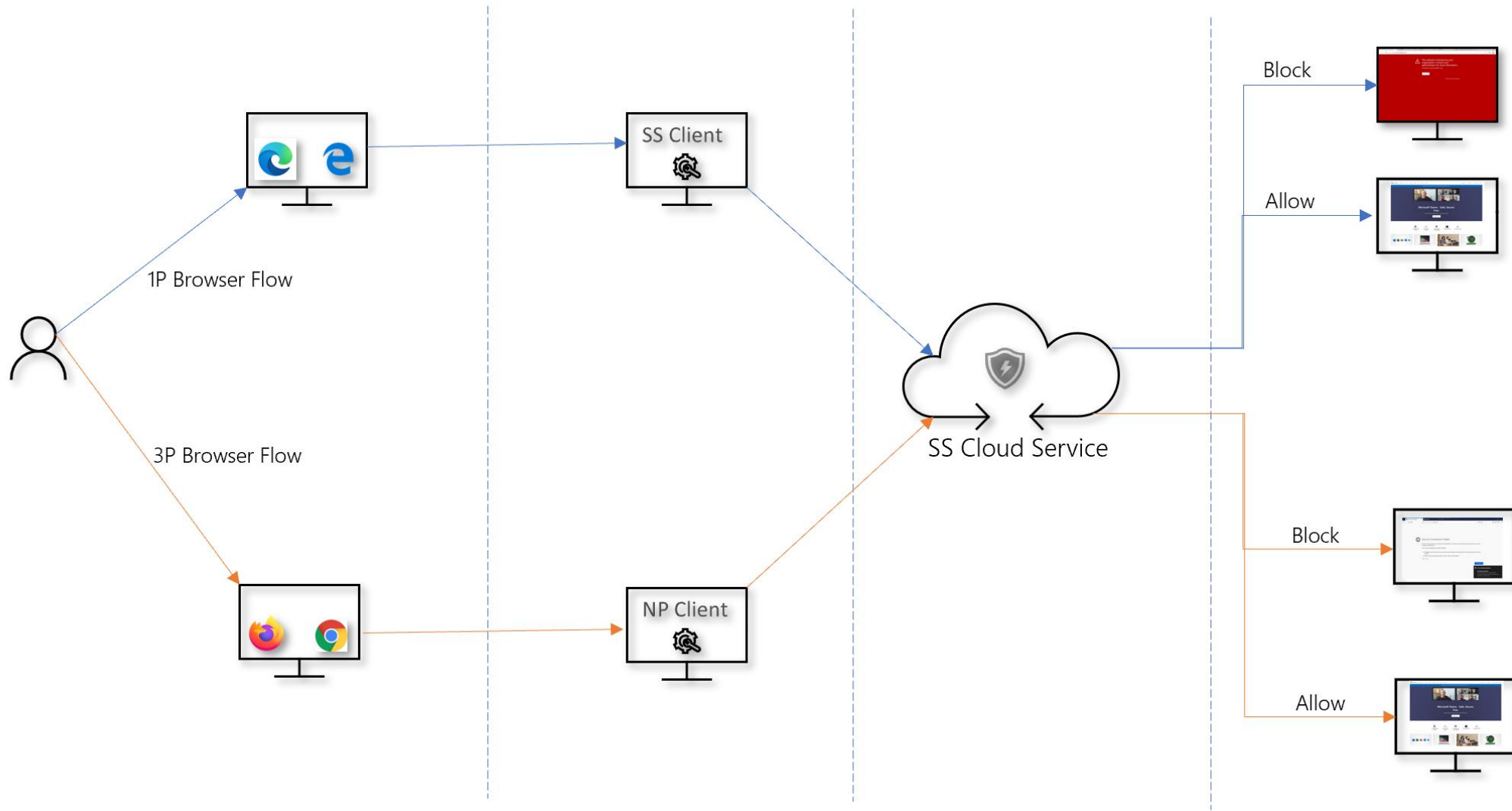


What the SmartScreen?

Feature	Defender SmartScreen 	Edge SmartScreen 
Scope	System-wide	Edge browser only
Protects against	Malicious apps/files	Phishing & bad sites
Works outside Edge	Yes	No
Uses same backend	Yes	Yes



Network Protection Does Work



Web Content Filtering

Add Policy

- ☒ General
- ☒ **Blocked Categories**
- ☐ Scope
- ☐ Summary

Blocked Categories

Select the web content categories to block. You can also view about access attempts to websites in all categories.

Adult Content

- ☐ Select all
- ☐ Cults
- ☐ Gambling
- ☐ Nudity
- ☐ Pornography/Sexually Explicit
- ☐ Sex Education
- ☐ Tasteless
- ☐ Violence

High Bandwidth

- ☐ Select all
- ☐ Download Sites
- ☐ Image Sharing
- ☐ Peer-to-Peer
- ☐ Streaming Media & Downloads

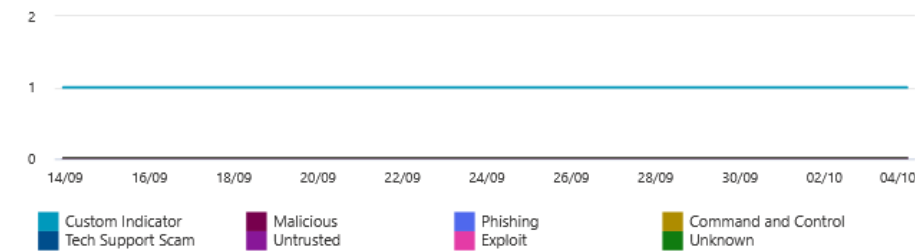
Legal Liability

- ☐ Select all

Reports > Web Protection

Web threat detections over time

Attempts to access malicious URLs



Web activity by category

Web categories with the most activity change

Sharp traffic spikes can indicate malicious internal activity

last update: Mon Oct 06 2025

Parent web category	Change in access requests
Legal Liability	No Change
Adult Content	No Change
High Bandwidth	No Change
Leisure	No Change
Uncategorized	No Change

Web threat summary

5 Attempts to access malicious URLs

Attempts to access malicious URLs

last update: Mon Oct 06 2025

Threat Category



Details

Indicators

Web activity summary

Total number of requests for web content in all URLs

last update: Mon Oct 06 2025

Requests



Details

Policies

Web content filtering summary

Attempts to access URLs in blocked categories

last update: Mon Oct 06 2025

Blocks



MDE vs Global Secure Access



MDE

Adult Content

- Cults
- Gambling
- Nudity
- Pornography/Sexually Explicit
- Sex Education
- Tasteless
- Violence

High Bandwidth

- Download Sites
- Image Sharing
- Peer-to-Peer
- Streaming Media & Downloads

Legal Liability

- Child Abuse Images
- Criminal Activity
- Hacking

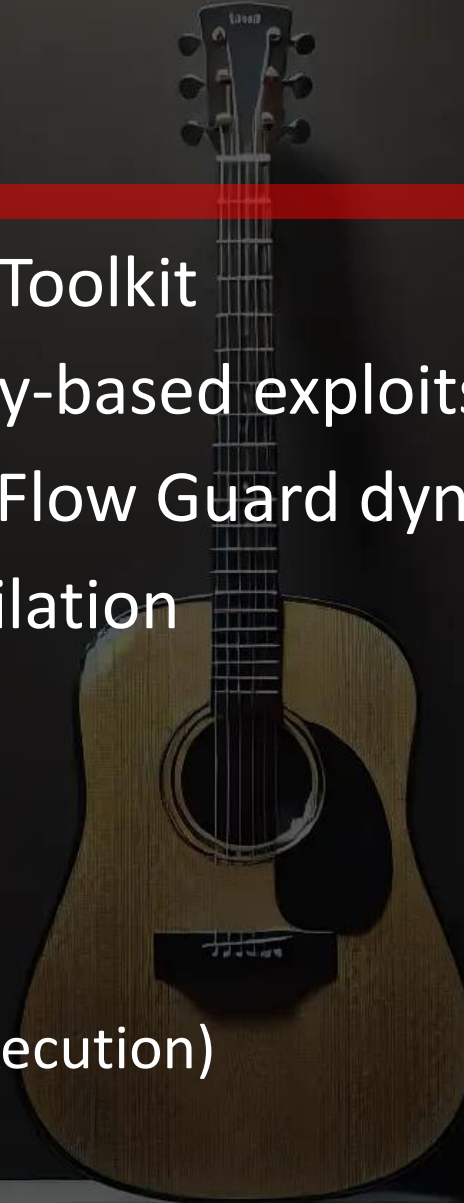
GSA

Liability (Adult content and Legal Liability)

- Alcohol And Tobacco
- Artificial Intelligence
- Child Abuse Images
- Criminal Activity
- Cheating
- Cryptocurrency Mining
- Dating And Personals
- Gambling
- Hacking
- Hate And Intolerance
- Illegal Drug
- Illegal Software
- Lingerie And Swimsuits
- Marijuana
- Nudity
- Pornography And Sexually Explicit
- Remote Access
- Self Harm

Exploit Protection

- ◆ Based on Enhanced Mitigation Experience Toolkit
- ◆ Hardens running processes against memory-based exploits
- ◆ Applies mitigations like DEP, ASLR, Control Flow Guard dynamically
- ◆ Protects even legacy apps without recompilation
- ◆ Techniques used
 - ◆ DEP (Data Execution Prevention)
 - ◆ ASLR (Address Space Layout Randomization)
 - ◆ ROP mitigations (stack pivot, caller check)
 - ◆ Arbitrary Code Guard (blocks dynamic code execution)
- ◆ Can stop DLL sideload/hijacking



Exploit Protection

- ◆ Defaults are safest
- ◆ Microsoft Security Benchmarks include safe improvements
- ◆ Other examples on GitHub:
 - ◆ Harvester57/Exploit-Protection-policy
 - ◆ jdgregson/Exploit-Protection-Settings
 - ◆ microsoft/ExploitProtectionConfiguration

Home > Endpoint security | Attack surface reduction >

Create Policy ...

Basics Configuration settings Scope tags Assignments Review + create

i Need to configure at least one setting to proceed. ×

i Search settings by setting name i

Exploit Guard ^

Exploit Protection Settings i ☐ Not Configured

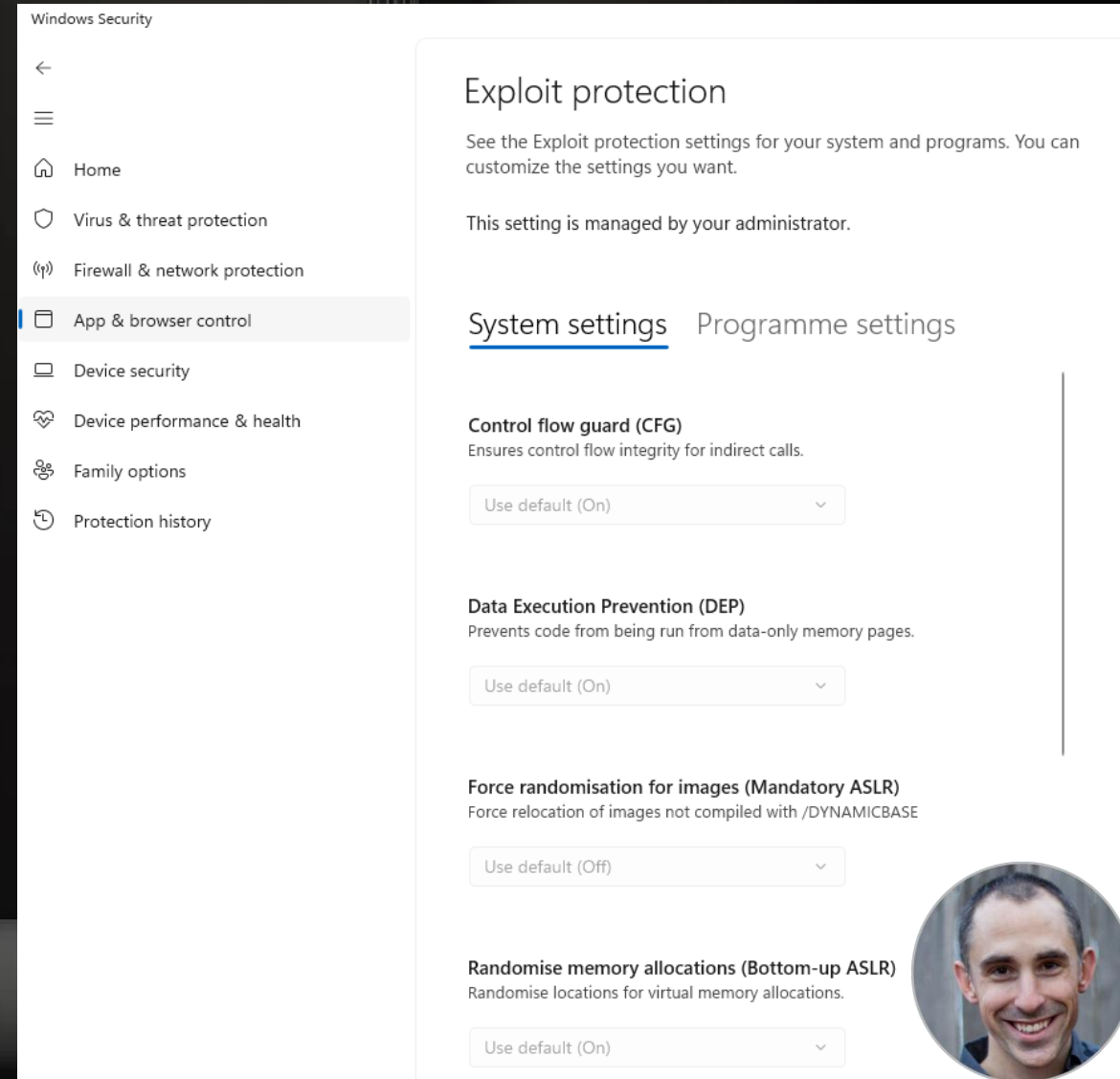
Windows Defender Security Center ^

Disallow Exploit Protection Override i ▼



The Challenge with Exploit Protection

- ◆ Developers need to be aware of what it is doing, in the *Microsoft Way*
- ◆ Relies on careful monitoring and creation of XML-based rules
- ◆ This should be one of the last ASR components you work on
 - ◆ Use for specific attack mitigations



Exploit Protection or Application Control?

- ◆ WDAC/AppLocker: Stops unauthorized code from running at all
- ◆ Exploit Protection: If code is allowed to run, prevents exploit techniques inside that process
- ◆ Check out Tom and Kim's session – Getting Started with WDAC and Managed Installer



Windows Firewall vs Indicators

◆ Custom network indicators

- ◆ Temporary restrictions
- ◆ Requires:
 - ◆ Defender AV in Active Mode
 - ◆ Network Protection Enabled

◆ Windows Firewall

- ◆ Long term restrictions
- ◆ Block lateral movement
- ◆ FQDN based filtering!
 - ◆ Block TLDs like .zip 🕶️
 - ◆ Defender AV in Active Mode
 - ◆ Network Protection Enabled

Dynamic keywords and Fully Qualified Domain Names (FQDN)

Dynamic keywords can be configured by defining a set of IP address ranges or FQDNs. Here are important things to consider when using FQDNs:

- FQDN support is for reducing the overhead of managing IP rules where IP addresses are dynamic and change frequently
- FQDNs aren't a replacement for IP addresses in all scenarios. IP addresses should be used when possible, for security and performance reasons
 - FQDN rules can affect performance on the endpoint, caused by DNS latency and other factors
 - FQDN isn't a secure DNS service. The FQDN resolution uses the default DNS configuration of the endpoint
- An FQDN rule requires a DNS query to happen for that FQDN to be resolved to an IP address. Traffic to IP addresses must generate a DNS query for FQDN rules
 - Limitations include: websites accessed via proxy, secure DNS services, certain VPN tunnel configurations, cached IPs on the endpoint
- While Partially Qualified Domain Names (PQDNs) are allowed, FQDNs are preferred. Wildcards * are supported for hosts, for example *.contoso.com

Two examples of FQDN rules are:

- Block all outbound and inbound by default and allow specific outbound traffic
- Block all inbound by default and block some specific outbound traffic



OWE D

Windows Firewall

Looking at auto-resolve



Policy Guidance

- ◆ Defaults are less than ideal
- ◆ Not all settings are available in Endpoint security
- ◆ Workload considerations
- ◆ Scheduled scans
- ◆ Client vs servers
- ◆ Updates



Exclusion Guidance

Path to exclude	Pros	Cons
%userprofile%	Doesn't do what you think	Doesn't do what you think
C:*	Defender CPU usage very low	You'll get hacked
%ExchangeInstallPath%	Microsoft told me to	Microsoft told me to

- ◆ Generally speaking... process > file > folder > extension
- ◆ Contextual exclusions are awesome
 - ◆ E:\Documents\TheBigOne.docx\:{Process:"C:\Program Files*\Microsoft Office\root\Office??\winword.exe"}



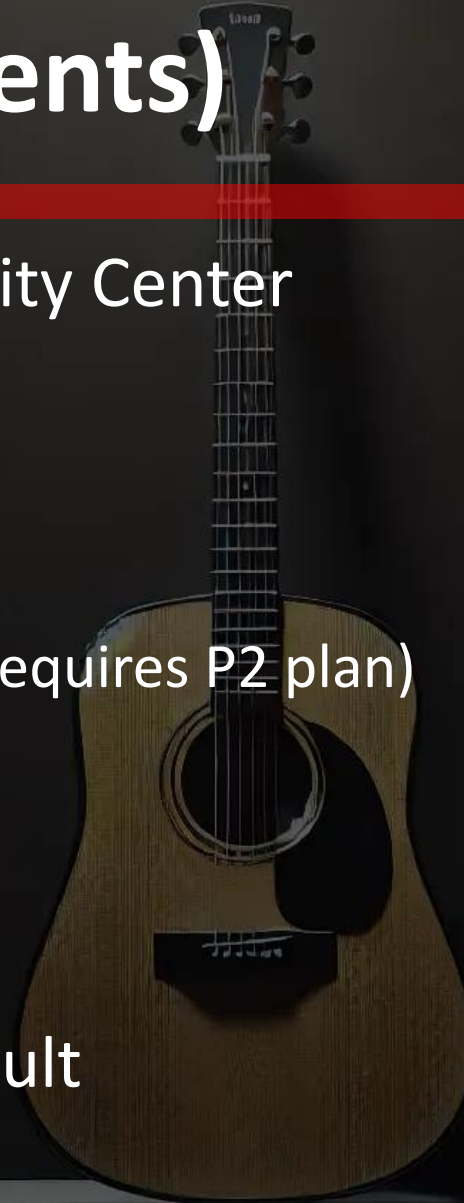
Update Guidance

- ◆ Update Intelligence definitions hourly
- ◆ Do not use WSUS/ConfigMgr for Intelligence Updates
- ◆ Microsoft Update is ideal
 - ◆ File shares are great for VDI and fallback
- ◆ Consider using update rings
- ◆ Unified Sensor (Server 2012/16)
 - ◆ Special - KB5005292



Passive Mode (Windows clients)

- ◆ 3rd party AV registers with Windows Security Center
- ◆ Defender goes into Disabled state
- ◆ Onboard to Defender for Endpoint puts Defender into Passive state
 - ◆ Switches to EDR in Block mode if configured (requires P2 plan)
- ◆ If migrating, assess health with Reports and pre-stage AV policies
- ◆ Servers and macOS are not passive by default



Longer answer - for bedtime reading Zzz...

When a device runs a non-Microsoft AV as the primary product, Microsoft Defender Antivirus (MDAV) is put into **passive** mode. If **EDR in block mode** is enabled and the EDR sensor raises a behavioral/post-breach detection, Defender for Endpoint will **invoke the MDAV remediation engine** to kill processes, quarantine/delete artifacts, and roll back related changes—even though MDAV isn't the primary AV. In the portal you'll see these actions as **Blocked/Prevented** in the Action center.

A quick flow:

1. **Primary AV = third-party, MDAV = passive**
2. **EDR** flags a malicious behavior/artifact
3. **EDR in block mode** authorizes **MDAV** to take remediation
4. Action appears as **Blocked/Prevented** in the portal's Action center

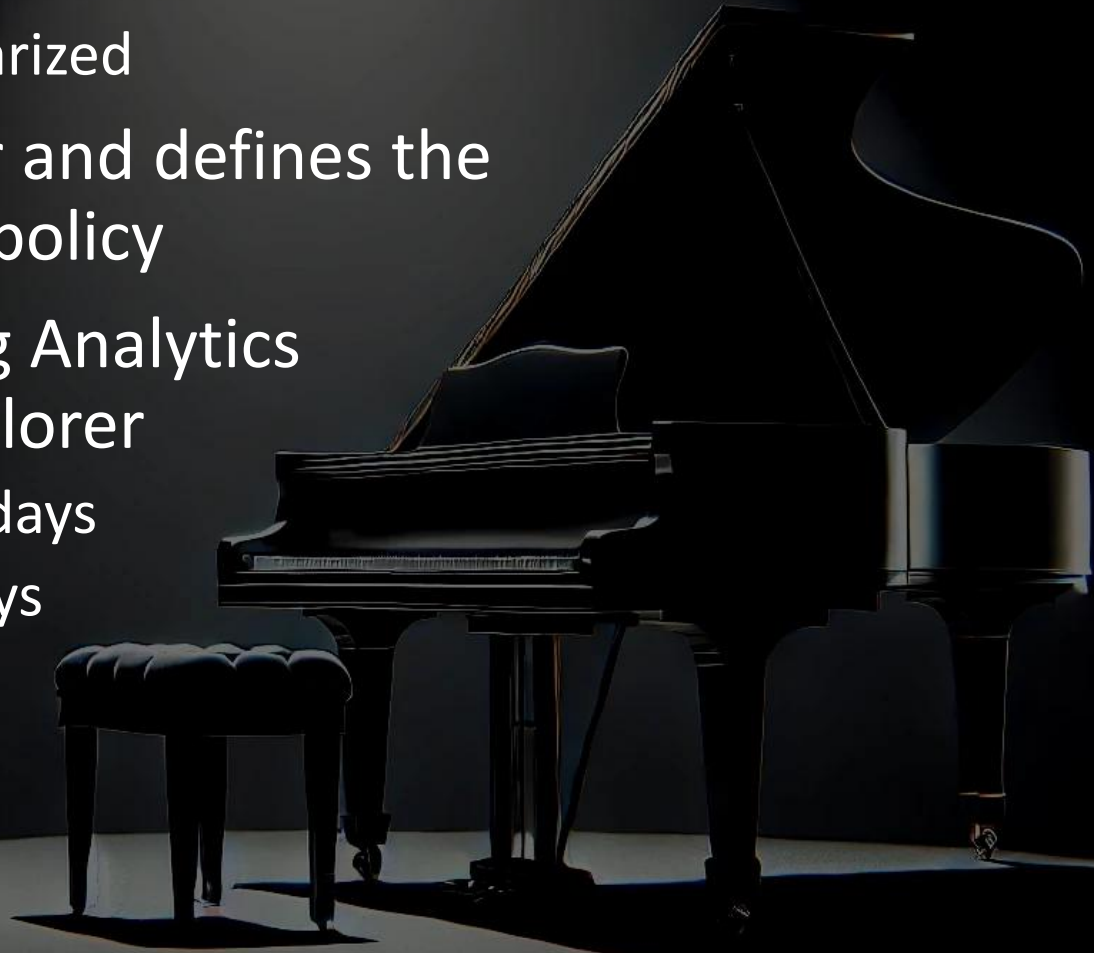
A couple of important nuances:

- ♦ This doesn't re-enable **real-time/on-access scanning** or other protections that require MDAV to be **active** (e.g., Network Protection; many ASR capabilities). Those remain off; your third-party AV is expected to cover them. EDR in block mode only uses MDAV to act **on EDR's detections**.
- ♦ **Microsoft's** guidance: if **MDAV is already your primary AV (active mode)**, there's **little benefit** to EDR in block mode and they say to leave it disabled.
- ♦ Keep **cloud protection (MAPS)** on and MDAV **intelligence up to date**, because EDR block actions rely on MDAV's engine and cloud-delivered detections.



XDR Architecture

- ◆ XDR sensor is natively built into Windows
 - ◆ EDR is one component, modularized
- ◆ Onboarding configures sensor and defines the workspace for telemetry and policy
- ◆ Very similar to Sentinel on Log Analytics with export to Azure Data Explorer
 - ◆ Advanced Hunting (LAW) – 30 days
 - ◆ Timeline / TVM (ADX) – 180 days



Telemetry sources

- ◆ Mssecflt.sys – kernel callbacks and file system filters
- ◆ ETW provider subscriptions
 - ◆ Threat Intelligence ETW
 - ◆ Impacted by advanced auditing policies
- ◆ Network
 - ◆ Zeek!
 - ◆ Device discovery
 - ◆ DNS but no TLS inspection
 - ◆ SenseNDR.exe
- ◆ Timeline vs Advanced Hunting



Tricks for adding telemetry ☺

- ◆ Advanced Auditing
 - ◆ Thanks Olaf Hartong!
- ◆ App Control for Windows/Business
 - ◆ CLM call out
- ◆ Scheduled Tasks
 - ◆ Capture with PowerShell logging
- ◆ Event.Write API permissions



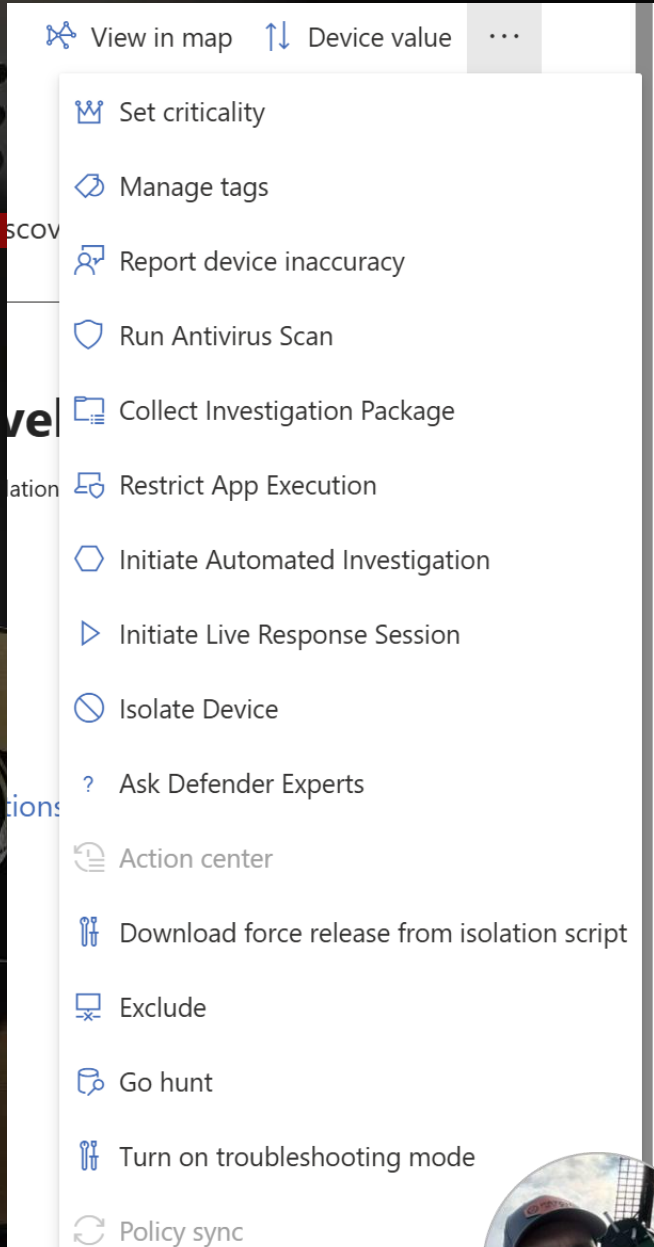
OWNED

Telemetry



Incident Response capabilities

- ◆ Automated Investigation and Remediation
 - ◆ Triage and data collection PowerShell scripts
- ◆ Machine Actions
 - ◆ AV scan, Automated investigation, Collect investigation package, Isolate device, Restrict app execution, and Live response
- ◆ Live Response
- ◆ Custom detections
- ◆ SenselR.exe



Live Response

Device Inventory > 5cd4[redacted] > Live response on 5cd[redacted]



Live response on 5cd[redacted]

Pending

Entity summary

Device details

View device details

Session Information

Session ID

CLRfcc1ae3b-513d-481f-b55c-8f03ec66df4f

Session created by

ladmin@conditionalaccess.uk

Session started

10 Oct 2025 16:19

Session ended

N/A

Duration

8s

Device Information

Command console

Command log

```
C:\> connect
\
```

Windows Defender AV detected 'Occamy' malware

Investigation #11 is running - Pending approval

Started
Feb 10, 2019, 8:41:20 PM

Total pending time: 2:19m

00:42:54
Pending approval

Cancel Investigation

Comment

Investigation details

Status

Pending approval

Remediation actions require review and approval.

Alert severity

Informational

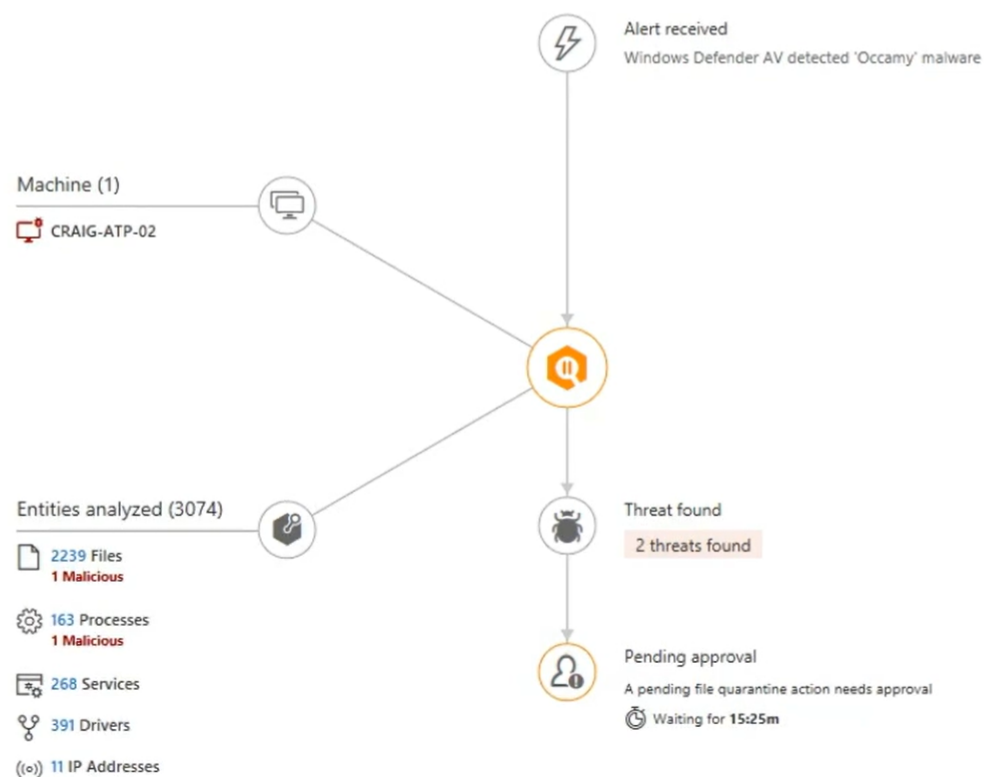
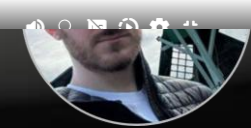
Category

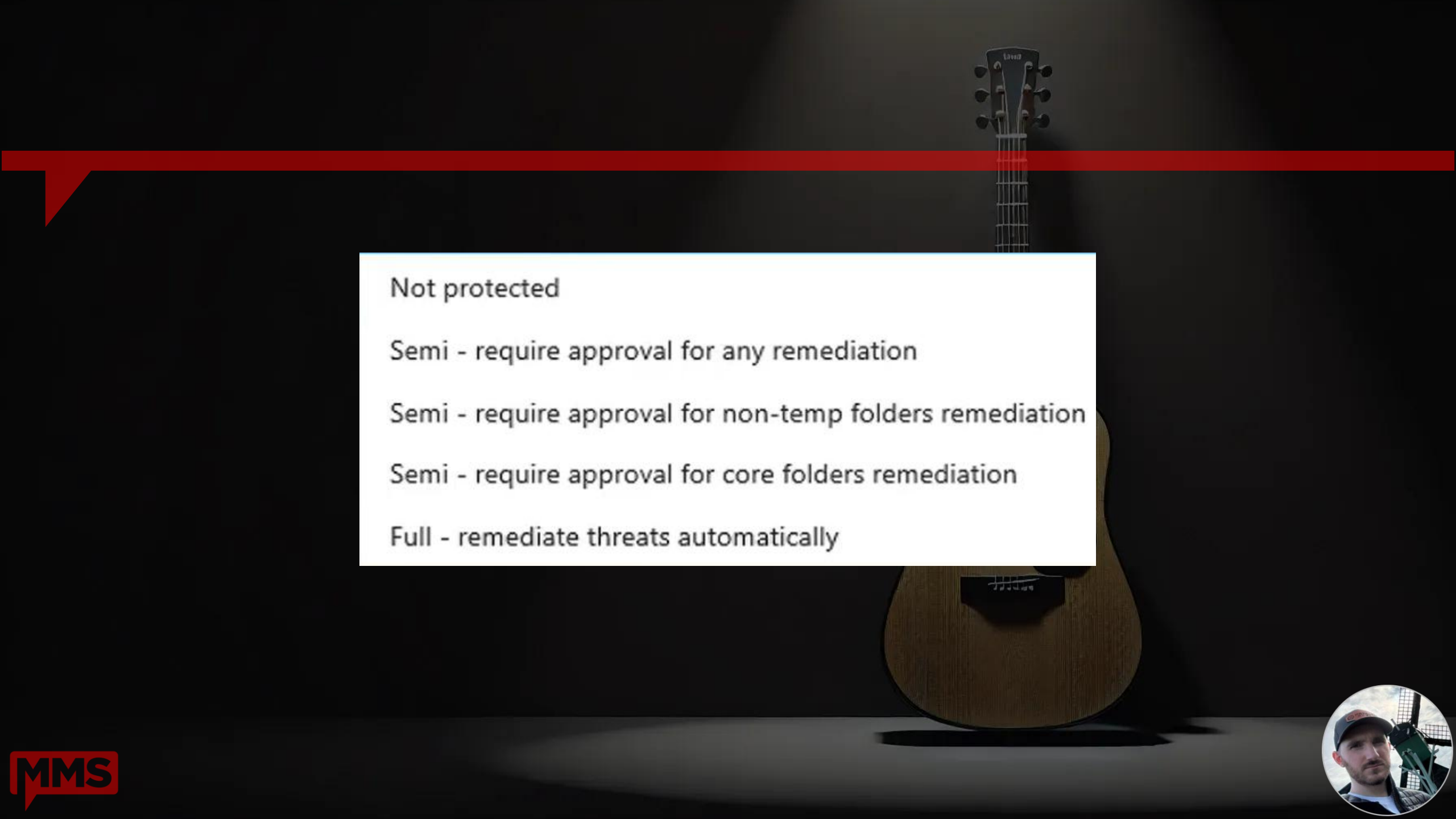
General

Detection source

Antivirus

Investigation graph Alerts (1) Machines (1) Key findings (2) Entities (3.07k) Log (28) Pending actions 1



An acoustic guitar is positioned vertically in the background, centered behind the text box. A thick red horizontal bar is located at the top of the slide, with a red triangular shape pointing downwards from its left end.

Not protected

Semi - require approval for any remediation

Semi - require approval for non-temp folders remediation

Semi - require approval for core folders remediation

Full - remediate threats automatically



AUTOMATION LEVELS

 Temp

 Other

 Windows

not protected



Semi - require approval for
any remediation



Semi - require approval for
non-temp folders



Semi - require approval for
core folders



Full - remediate threats
automatically



Status

An Automated investigation can be in one of the following status:

Status	Description
No threats found	No malicious entities found during the investigation.
Failed	A problem has interrupted the investigation, preventing it from completing.
Partially remediated	A problem prevented the remediation of some malicious entities.
Pending action	Remediation actions require review and approval.
Waiting for machine	Investigation paused. The investigation will resume as soon as the machine is available.
Queued	Investigation has been queued and will resume as soon as other remediation activities are completed.
Running	Investigation ongoing. Malicious entities found will be remediated.
Remediated	Malicious entities found were successfully remediated.
Terminated by system	Investigation was stopped by the system.
Terminated by user	A user stopped the investigation before it could complete.
Partially investigated	Entities directly related to the alert have been investigated. However, a problem stopped the investigation of collateral entities.

Custom Detections – USB Info

Custom detection

General

Alert settings

Automated actions

Scope

Review and create

General

Proactively monitor and react to threats by creating custom detections that search through your logs.

Detection name *

USB Flash Drive

Rule Description

Enter a description for your detection

Frequency * ⓘ

Continuous (NRT)

RECOMMENDATION

This query looks well-optimized to run in near real-time, we recommend running this rule in [Continuous \(NRT\) frequency](#).

Lookback ⓘ

Near real-time rules run continuously as events are collected and processed, so there is no lookback period.

Alert title *

USB Flash Drive

Severity *

Info

Category *

Discovery

MITRE techniques

Select MITRE techniques



Alert settings

Define the alert enrichment details.

 Explore query and results

Alert details * 

Alert title *

USB Flash Drive

Description *

USB flash drive has been used

Custom details

Entity mapping *

Identified entities determine how alerts are grouped into incidents. Make sure to carefully review the entities to ensure a high quality of incident correlation. [Read more](#)

Impacted Assets * 

Entity

 Device

Identifier 

HostName

Column 

DeviceName

 Add assets

Advanced hunting

 Run query  Share link

 Query results are presented in your local time zone as per settings. Kusto filters, however, work in UTC.

```
1 DeviceEvents
2 | where ActionType in ("UsbDriveMounted", "UsbDriveUnMounted")
3 | extend AdditionalFieldsParsed = parse_json(AdditionalFields)
4 | project Timestamp,
5 |     ReportId,
6 |     DeviceName,
7 |     DeviceId,
8 |     ActionType,
9 |     InitiatingProcessAccountName,
10 |     ProductName = tostring(AdditionalFieldsParsed["ProductName"]),
11 |     Manufacturer = tostring(AdditionalFieldsParsed["Manufacturer"]),
12 |     DriveLetter = tostring(AdditionalFieldsParsed["DriveLetter"])
13 | order by Timestamp desc
14
```



Part of incident: Multi-stage incident involving Discovery & Command and control on one endpoint [View incident page](#)

 **5cd4403...**

Risk level Informational

...

Windows11

All Devices

 **conditionalaccess.uk\lewis**

What happened

USB flash drive has been used

Custom detection

Actions taken

No actions taken in response to this custom detection.

Related events

Timeline Query results

Expand all

13/7/2025
10:24:46



Removable volume mounted to the system (D:)

Volume file



Path

\\?\Volume{10f88a3e-5fcb-11f0-ade6-dc4ba1481906}

 **USB Flash Drive**

Informational Detected New

...

Timestamp		ReportId	DeviceName	DeviceId	ActionType	InitiatingProcessAccountNa...	ProductName	Manufacturer	DriveLetter
☐	13 Jul 2025 10:24:46	1392	5cd4403h6h	c2db9c55b402b7a7dfc9...	UsbDriveMounted	lewis	Ultra	SanDisk	D:
Timestamp		13 Jul 2025 10:24:46							
ReportId		1392							
DeviceName		5cd4403h6h							
DeviceId		c2db9c55b402b7a7dfc915cc3264b0ce77d5d3fa							
ActionType		UsbDriveMounted							
InitiatingProcessAccount...		lewis							
ProductName		Ultra							
Manufacturer		SanDisk							
DriveLetter		D:							

Threat and Vulnerability Management

- ◆ Leverages EDR telemetry
 - ◆ Reduces performance impact, limited scanning
 - ◆ Might miss context, most VM tools do
- ◆ Additional data collection via PowerShell
 - ◆ App Control can break this
- ◆ One Full scan is recommended
 - ◆ Use TVM to determine this!
- ◆ SenseTVM.exe



A city skyline at dusk, likely Pittsburgh, with the PPG Place building prominently featured. The city lights are reflected in the water of the river. A large, multi-decked ferry boat is visible on the river in the foreground. The sky is a mix of purple, pink, and blue.

Threat and Vulnerability Management

OWE D



Cloud Protection

- ◆ Local analysis
- ◆ Metadata submission to Security Graph API
- ◆ Sample submission request
- ◆ Cloud detonation and analysis
- ◆ Emergency updates
- ◆ Post-inform (EDR)
 - ◆ EDR in Block Mode



Ensure 'Join Microsoft MAPS' is set to 'Disabled' (CIS LEVEL 2)

Created:2025/08/07 | Revised:2025/08/07

Overview

18.10.43.5.2 'Join Microsoft MAPS' recommended state is 'Disabled'.

Description

This policy setting allows you to join Microsoft Active Protection Service (MAPS), which Microsoft has now renamed to *Windows Defender Antivirus Cloud Protection Service* and then *Microsoft Defender Antivirus Cloud Protection Service*. Microsoft MAPS / Microsoft Defender Antivirus Cloud Protection Service is the online community that helps you choose how to respond to potential threats. The community also helps stop the spread of new malicious software infections. You can choose to send basic or additional information about detected software. Additional information helps Microsoft create new definitions and help it to protect your computer.

SYXSCORE

Severity: INFO

CVSS: N/A

Countermeasure: N/A

Public Aware: N/A

Weaponized: N/A

Security Settings Management

- ◆ Unified policy management
- ◆ Origin of MMP-C!
- ◆ Enrollment
 - ◆ Use existing device object
 - ◆ Synthetic device registration
- ◆ Management channels
 - ◆ Defender for Cloud
 - ◆ Configuration Manager
 - ◆ Intune





Security Settings Management

OWE D



Troubleshooting

- ◆ Onboarding
 - ◆ It's always ~~DNS~~ TLS inspection
- ◆ Migration
 - ◆ DisableAntispyware and other great things
- ◆ Configuration
 - ◆ Effective settings
- ◆ Performance
 - ◆ New-MpPerformanceRecording
- ◆ MDE Client Analyzer
 - ◆ MPLog!



Jam Sessions

A dimly lit music studio with various equipment. In the center, there's a desk with a computer monitor displaying 'MMS', a keyboard, and a mixing console. Several large speakers are positioned around the room. On the left, a guitar is leaning against a desk. On the right, two more guitars are visible. The room has soundproofing panels on the walls and a wooden floor.

**Be sure to find Wally and sign up for 1:1 time with a speaker
If you'd like to meet us privately, we are scheduled as follows:**

ALSO, Please be sure to leave feedback for your sessions on Sched!

Save the Dates

May 3-7, 2026



Oct 25-28, 2026



May 2-6, 2027



Extended Q&A



PATCH MY PC

 TeamViewer

 nerdio

eido

 baramundi

omnissa™

flexera™

 PDQ

 RECAST SOFTWARE

ninjaOne®

 2Pint

robopack 

 VIAMONSTRA
ONLINE ACADEMY

 systemcenterdudes

