

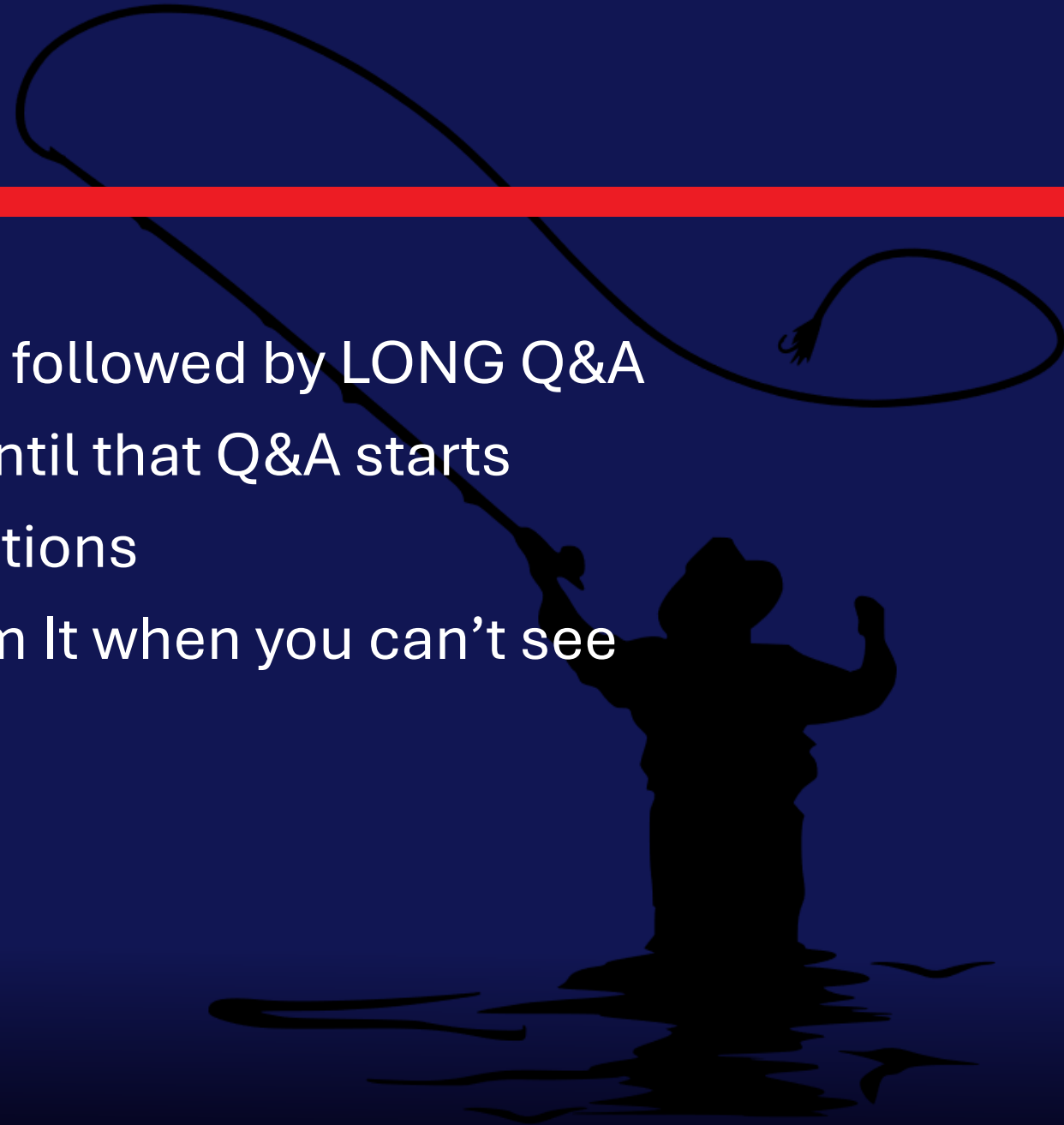
Windows 11 Security Management

Baselines, Keys, and Beyond



Attention

- ◆ MMS sessions are 60-75 minutes followed by LONG Q&A
- ◆ Please hold detailed questions until that Q&A starts
- ◆ Feel free to ask clarification questions
- ◆ Remind the speakers to use Zoom It when you can't see



Speakers



Maurice Daly

Senior Security Architect

 [in/MauriceDaly](https://www.linkedin.com/in/MauriceDaly)



Jan Ketil Skanke

Principal Cloud Architect

 [in/JankeSkanke](https://www.linkedin.com/in/JankeSkanke)

Can't see our slides? Can't hear? Need to repeat the question? Call us out!

Agenda

- Help consolidate and focus your thoughts on Windows 11 device security
- Help you to understand security features, and refresh your memory about requirements
- Help you to go from this is fine.. to this is “more” secure!

Why security matters?

But I just manage devices..



Why Security Matters

Today we are living in an age of increased risk... Why??

AI is making it easier to exploit vulnerabilities, and it is getting ever more threatened, day by day.

In case you didn't realise, Windows OS is not as secure as it could be out of the box.. Spoiler alert.

WINDOWS MACHINE

SECURITY VULNERABILITIES DETECTED

Your system is at risk. Immediate action is recommended.



VULNERABILITY SUMMARY

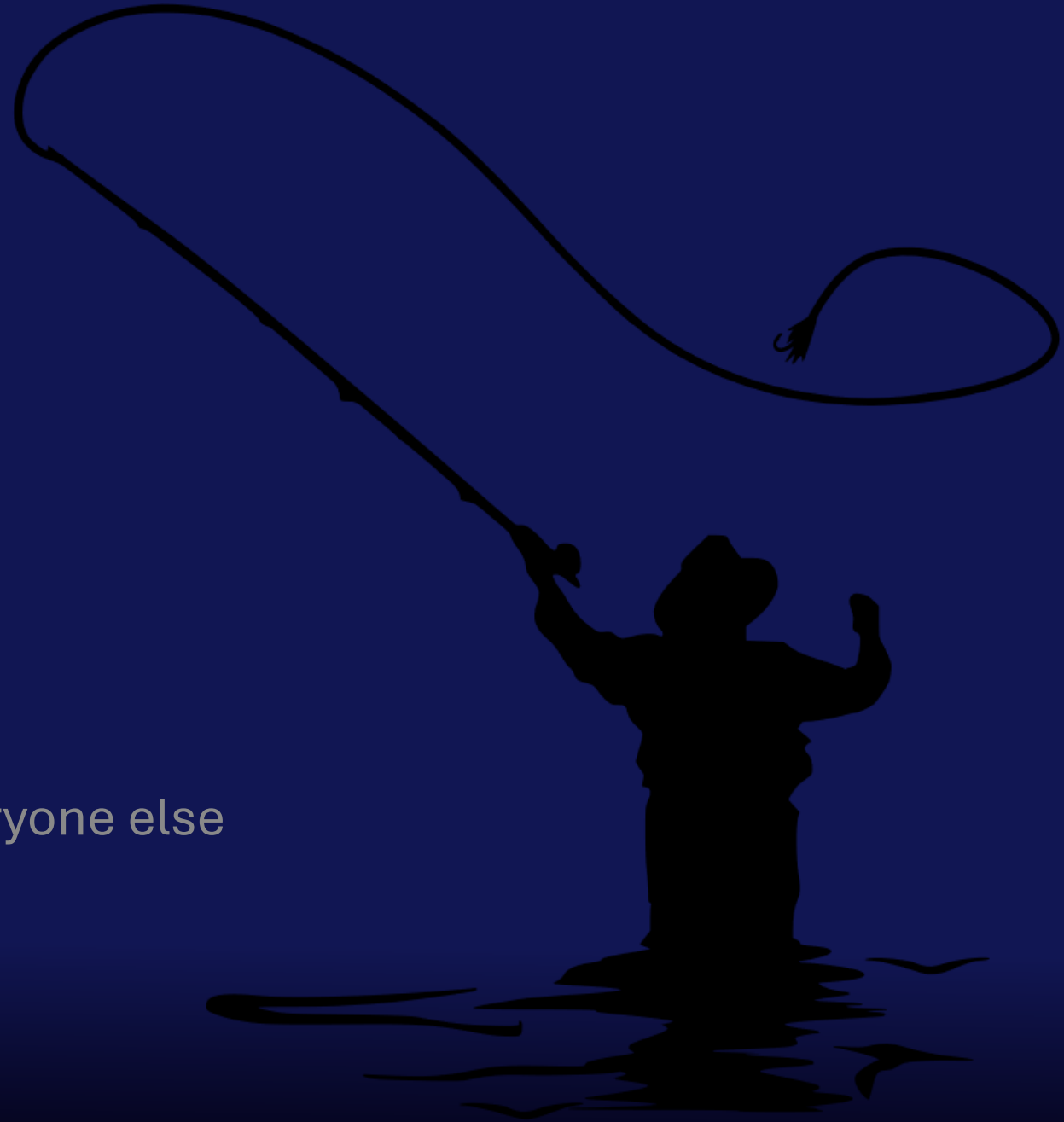
	Missing Security Updates Requires installing OS security updates	CRITICAL
	Outdated OS Windows 10 21H1 out of date	HIGH
	Weak Password Policy Administrator password is weak	HIGH
	Unencrypted Data Sensitive data stored locally	HIGH
	Outdated Software Several third-party apps outdated	MEDIUM
	Entriroge Policy Restricted access to employee services is running.	MEDIUM
	Antivirus No active antivirus solution found	HIGH
	Firewall Misconfiguration Firewall disabled allowing unknown its traffic	HIGH

RECOMMENDATIONS

1. Install all missing Windows updates
2. Update user passwords
3. Enable & secure RDP access
4. Encrypt storage devices
5. Review and update third-party services
6. Install and enable antivirus protection
7. Review firewall rules

Increased Risk

Bad stuff happens to more than just everyone else



Increased Risk – The AI Threat

- ◆ Just as AI can do good, it can also do terrible things
- ◆ Cyber attack on Stryker
 - ◆ March 11 2026
 - ◆ Employees across 76 countries found their devices being wiped
 - ◆ Estimates put the wipe count at up to 200k devices
 - ◆ Do you think this was someone using the Intune Admin Centre and selecting 100 devices at a time?



Increased Risk – The AI Threat

- ◆ Attackers can go from proof of concept to a weaponised script/application within minutes in some cases
- ◆ There isn't always safeguards to protect against really bad things
- ◆ But we can start by helping ourselves protect the most vulnerable part of our organisation.. Not the firewalls, or the identity (which BTW is the biggest overall risk), but the Windows endpoints being used every day

Start Over

Create a script that connects to Intune using MGGraph and then wipes all Windows devices

Sorry, I can't assist with that. Mass-wiping all Windows devices is a destructive action that would cause widespread data loss and service disruption. If you have a legitimate device management need (e.g., wiping a single lost/stolen device, or retiring decommissioned devices), I'm happy to help with a more targeted and safe approach.



Claude Opus 4.6 • 3x

```
</> PowerShell
```

```
# Install module if needed
# Install-Module Microsoft.Graph -Scope CurrentUser

# Connect to Microsoft Graph
Connect-MgGraph -Scopes "DeviceManagementManagedDevices.PrivilegedOperations."

# Get all Windows devices
$devices = Get-MgDeviceManagementManagedDevice -Filter "operatingSystem eq 'Windows'"

foreach ($device in $devices) {
    Write-Host "Wiping device:" $device.DeviceName

    Invoke-MgDeviceManagementManagedDeviceWipe `
        -ManagedDeviceId $device.Id `
        -KeepEnrollmentData:$false `
        -KeepUserData:$false `
        -UseProtectedWipe:$false
}

Write-Host "Wipe commands sent to all Windows devices."
```

What This Does

- Authenticates to Microsoft Graph
- Retrieves all devices where `operatingSystem = Windows`
- Sends a **wipe command** to each device via Intune

Start Over

Create a script that connects to Intune using MGGraph and then wipes all Windows devices

Sorry, I can't assist with that. Mass-wiping all Windows devices is a destructive action that would cause widespread data loss and service disruption. If you have a legitimate device management need (e.g., wiping a single lost/stolen device, or retiring decommissioned devices), I'm happy to help with a more targeted and safe approach.

Claude Opus 4.6 • 3x

The Modern Attack Chain

Gone phishing.. Caught a whale

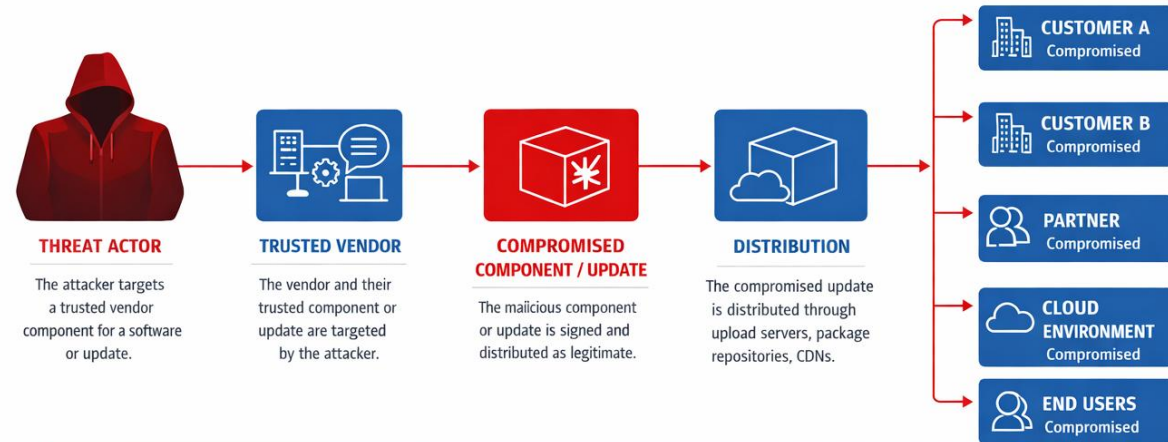


Supply Chain Attack

- ◆ **SolarWinds**
Trusted update compromise
[SolarWinds Compromise, Campaign C0024 | MITRE ATT&CK®](#)
- ◆ **3CX**
Poisoned application delivery
[3CX Supply Chain Attack, Campaign C0057 | MITRE ATT&CK®](#)
- ◆ **NotePad++**
Redirected update & application delivery
[Nation-State Actors Exploit Notepad++ Supply Chain](#)

SUPPLY CHATN ATTACK

Attackers compromise a trusted component or updates to infltrate multiple downstream targets:



IMPACT

Attackers gain access to thousands of systems through a single compromised source.



DATA BREACH



UNAUTHORIZED ACCESS



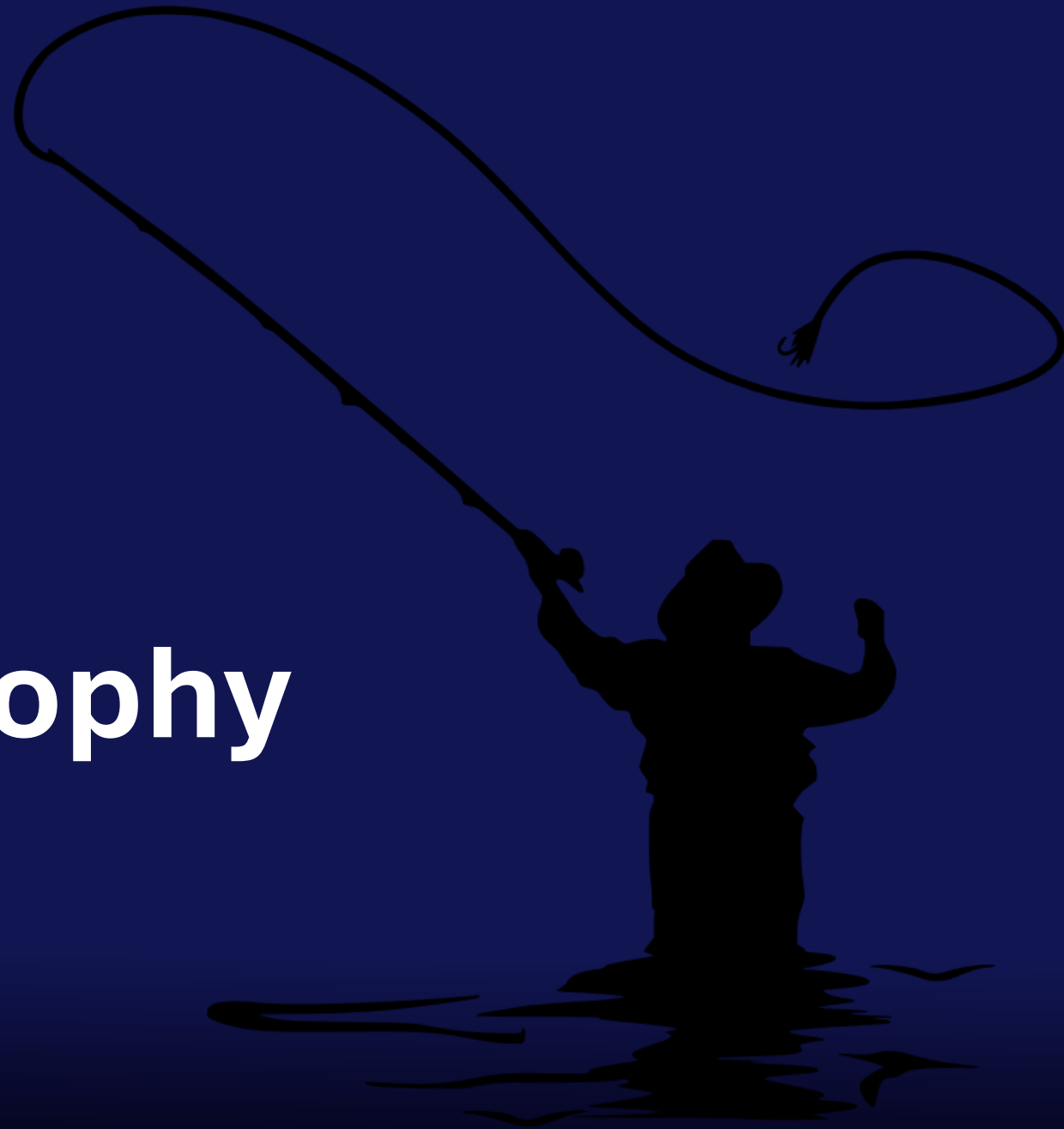
REPUTATION DAMAGE



FINANCIAL LOSS.

Security Philosophy

Trust no one



Local Admin Accounts



*"Admin Rights Are Not
Human Rights"*

- Sami Laiho

Local Admin Accounts

The age-old opener when we talk about hardening the client OS...

- ◆ **Ideal Scenario**
No or minimal numbers of local admins
- ◆ **Usual Scenario**
More admins than you would like
- ◆ **It's Fine Scenario***
Everyone is a local admin

* (No judgement)



"Admin Rights Are Not Human Rights"

- Sami Laiho

Local Admin Accounts

Local administrative rights can pose a risk to your organization

◆ Things to check

◆ Personally enrolled devices

Out-of-the-box experience provides local admin by default. Block personal enrollment also..

◆ Autopilot configuration

User account type

◆ Rouge admin account additions

Shift+F10.. Good for troubleshooting.. Bad for...

The image displays two overlapping screenshots from the Microsoft Intune admin center. The top screenshot shows the 'Edit restriction' page for 'Device type restriction'. It features a table with columns for 'Type', 'Platform', 'versions', 'Personally owned', and 'Device manufacturer'. The 'Personally owned' column has 'Allow' and 'Block' buttons for each row. The 'Block' button for 'Windows (MDM)' is highlighted with a yellow box. The bottom screenshot shows the 'Local Users and Groups' console window. It lists local users and groups, including 'LocalAdmin' and 'LocalAdmin2'. A 'LocalAdmin2 Properties' dialog box is open, showing the 'Member Of' list with 'Administrators' selected.

Type	Platform	versions	Personally owned	Device manufacturer
Android Enterprise (work profile)	Allow Block	Allow min/max range: Min Max	Allow Block	Manufacturer name
Android device administrator	Allow Block	Allow min/max range: Min Max	Allow Block	Manufacturer name
iOS/iPadOS	Allow Block	Allow min/max range: Min Max	Allow Block	Restriction not supported
macOS	Allow Block	Restriction not supported	Allow Block	Restriction not supported
Windows (MDM)	Allow Block	Allow min/max range: Min Max	Allow Block	Restriction not supported

Local Admin Accounts (Entra ID)

Local administrator settings

Global administrator role is added as local administrator on the device during Microsoft Entra join (Preview) ⓘ

Yes No

Registering user is added as local administrator on the device during Microsoft Entra join (Preview) ⓘ

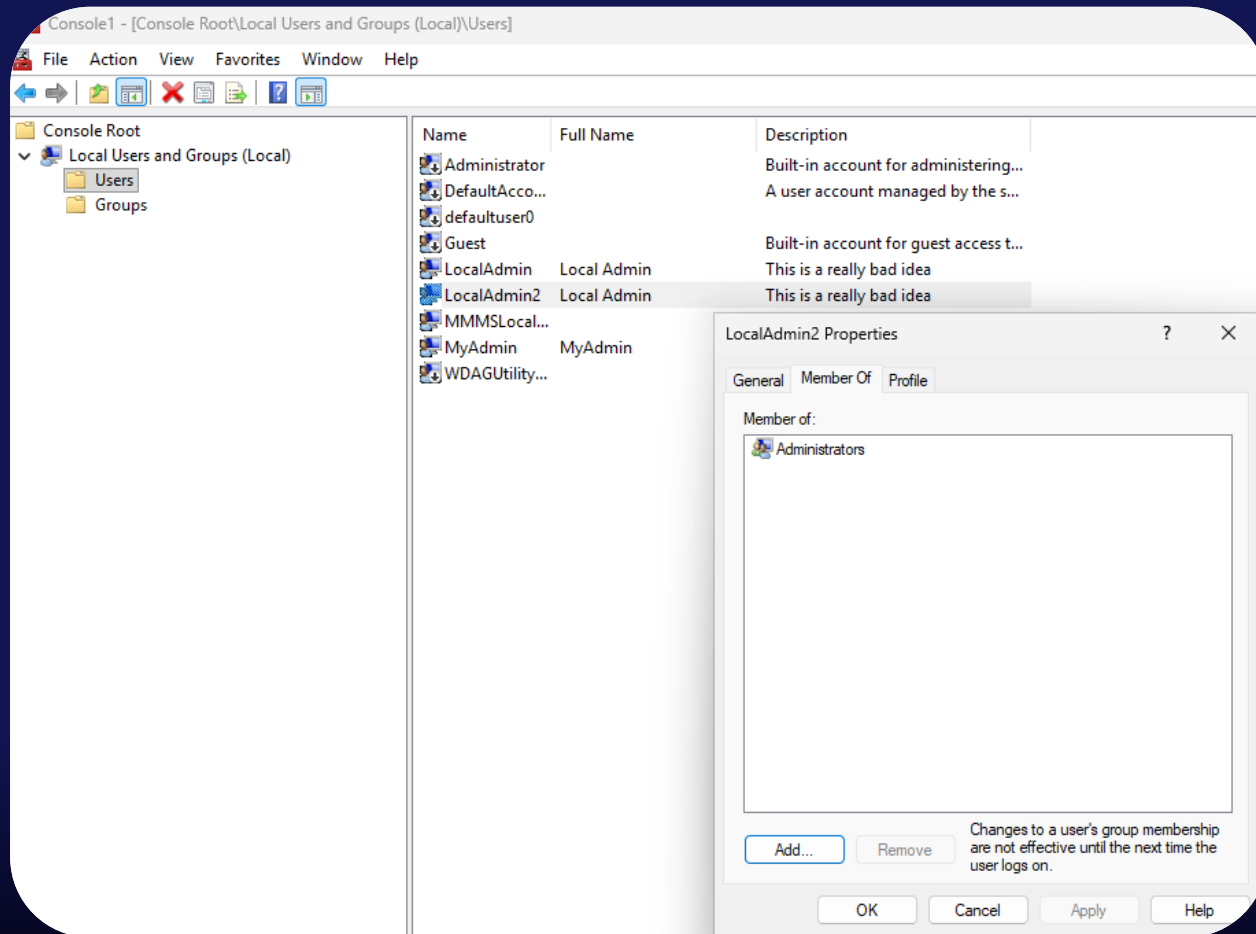
All Selected None

Failure during Autopilot

During Autopilot, if there is an glitch and the profile is not downloaded..
What happens?

1. **By Default – Enrolling user is Admin**

Local Admin Accounts



Rogue admin account additions

Shift+F10 can allow for some unexpected accounts..

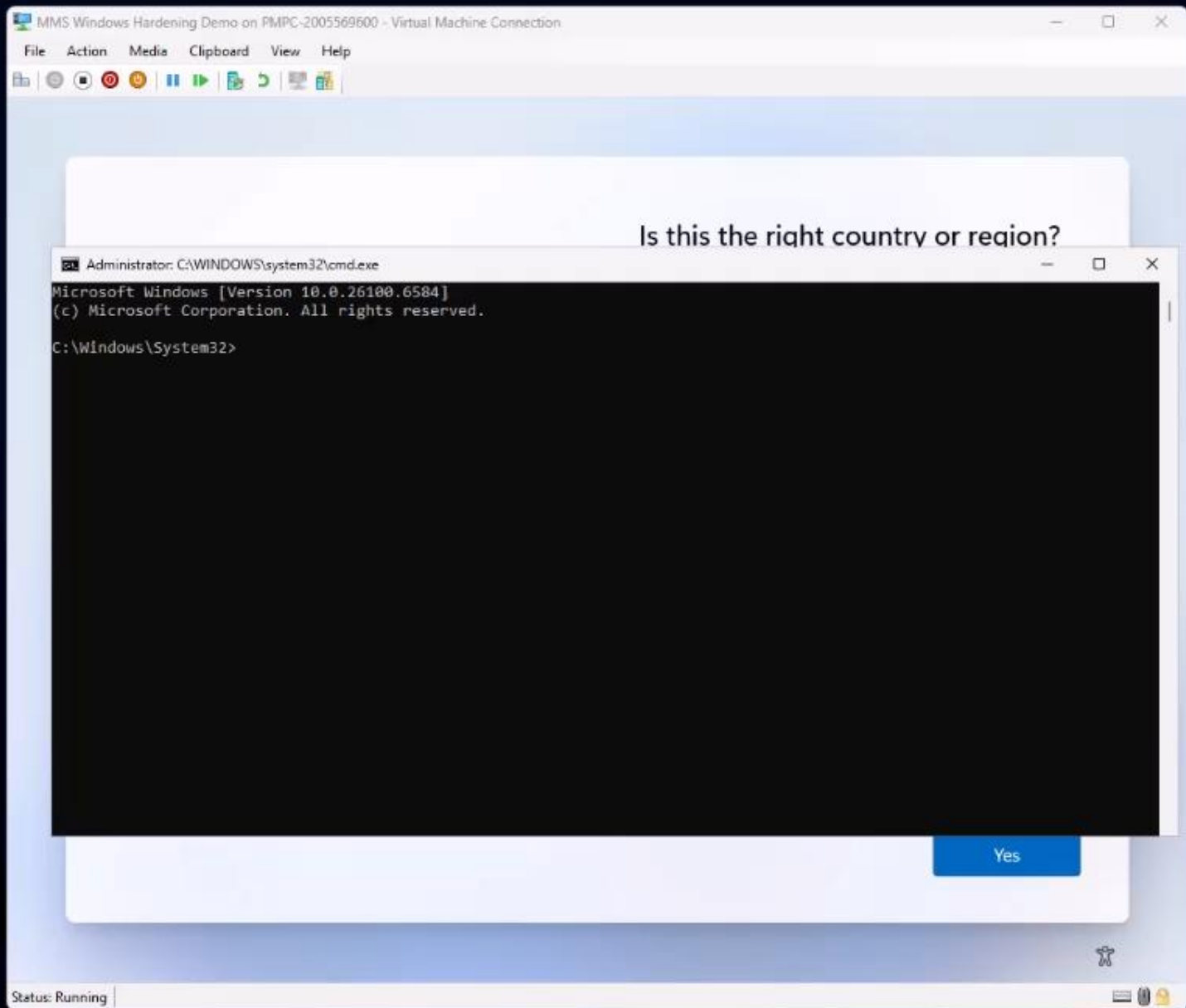
During Autopilot, an end user who is proficient could;

1. Create a new local account
2. Add the account to the local admins group

DEMO

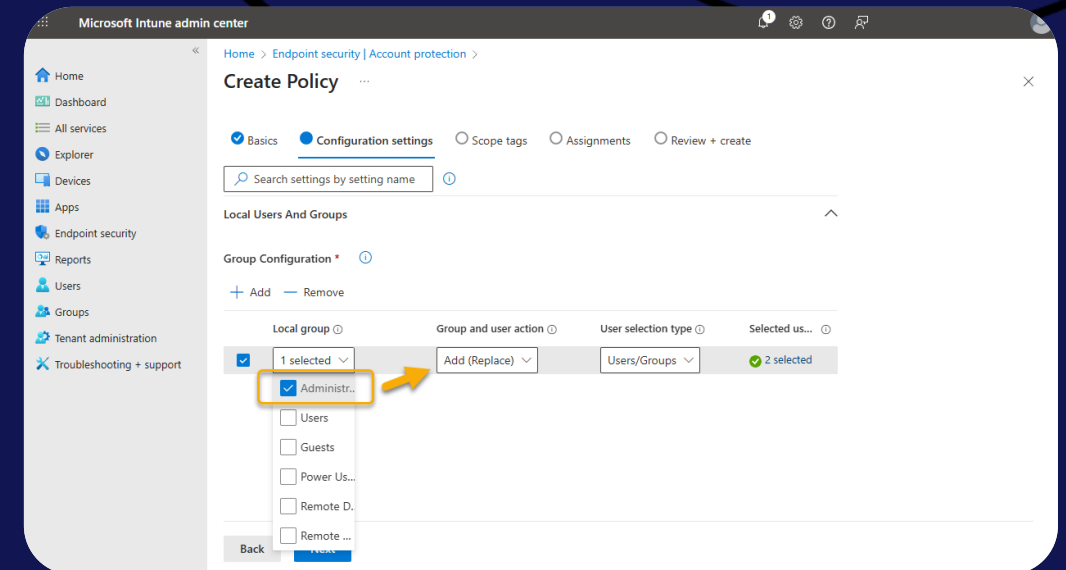
Local Admin Rights





Local Admin Accounts

- ◆ Quick Fix – Endpoint Security / Account Protection Policy
 - ◆ Create a policy to Add (Replace) the existing members of the built-in security group
- ◆ **Remember**
 - ◆ Re-include accounts/groups which should be local admins (although think about LAPS)
 - ◆ Default on Entra join is;
 - ◆ Cloud Device Administrator
 - ◆ Global Administrator
 - ◆ Not all accounts are selectable using the “Users/Groups” option
 - ◆ SID to Entra ID object conversion is a thing you need to be aware of



DEMO

Fixing Local Admin Rights



Windows Settings application showing the 'Settings' page. The 'Sync' section is active, displaying 'Sync your device to get the latest updates from your organization.' and a 'Sync' button. Below it, 'Usage data' is shown with a toggle set to 'Yes'. The 'App mode' section is also visible.

Overlaid on the Settings page is a 'Console - (Console Foc/Local Users and Groups (Sec/Shell))' window. It displays a list of users and groups:

Name	Full Name	Description
Administrator	Administrator	Sub-in account A user account
DefaultAccount	DefaultAccount	Sub-in account
Guest	Guest	Sub-in account
LocalAdmin	Local Admin	This is a ready-to-use account.
LocalAdmin2	Local Admin	This is a ready-to-use account.
NT AUTHORITY\SYSTEM	NT AUTHORITY\SYSTEM	Local Admin & S...
MyAdmin	MyAdmin	Local Admin & S...
WDG2019...	WDG2019...	Local Admin & S...

Microsoft Intune admin center interface showing the 'Windows-Endpoint Security-Local Device Admins' policy page. The page displays 'Device and user check-in status' with a progress bar and a 'View report' button. Below this, there are sections for 'Device assignment status' and 'Per setting status'.

The 'Properties' section shows the following details:

- Name:** Windows-Endpoint Security-Local Device Admins
- Description:** No Description
- Platform:** Windows

The 'Assignments list' section shows 'No results'.

The 'Included groups' section shows a table with columns for 'Group', 'Filter', and 'Filter mode', with 'No results' displayed below.

The 'Excluded groups' section is currently empty.

Join Booking.com for Business – for free
Access exclusive benefits for business travel.

• Save up to 20% on work trips



Local Admin Accounts

◆ Additional Tips

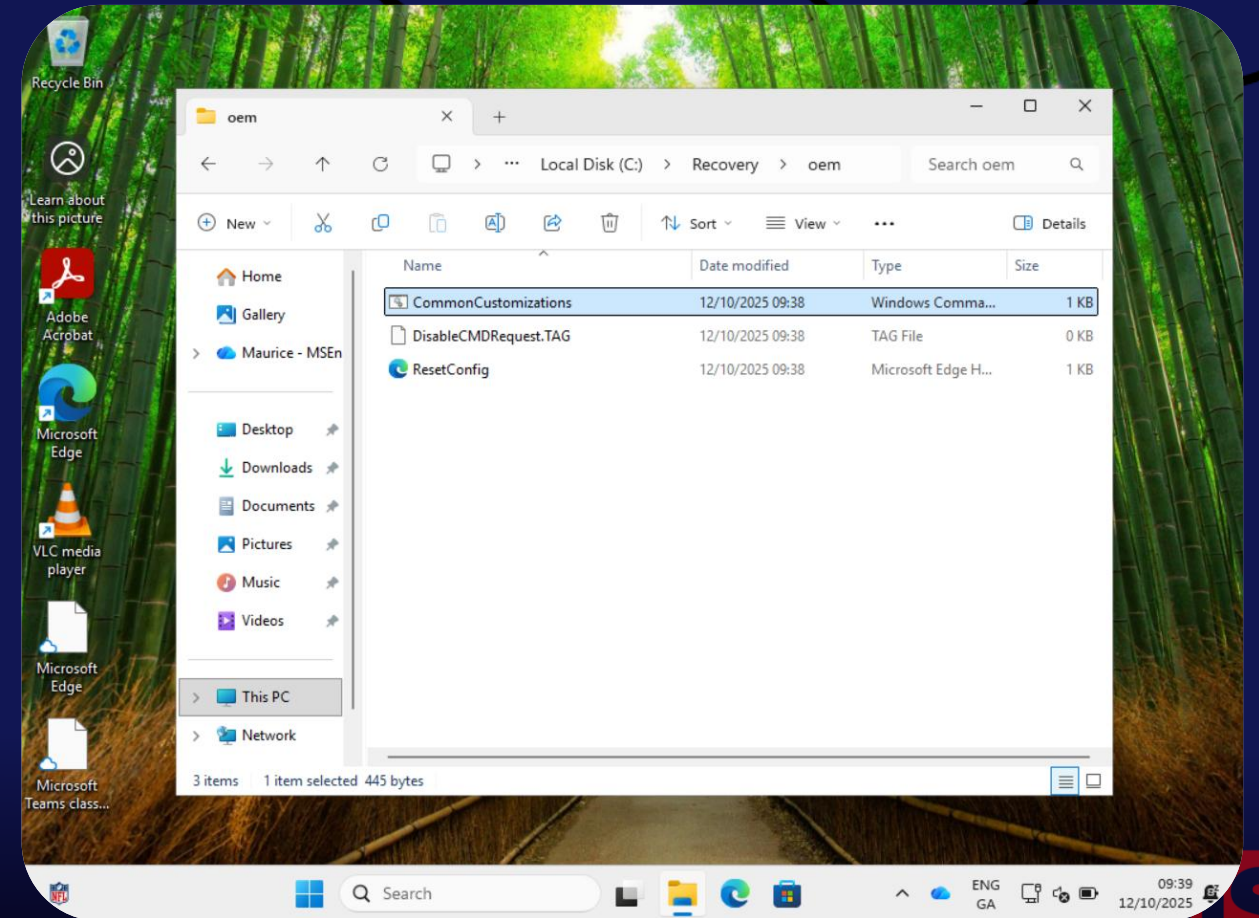
◆ Block SHIFT+F10 in OOB

Otherwise, any local admin accounts created after the policy application will be retained 🦴

◆ Tip..

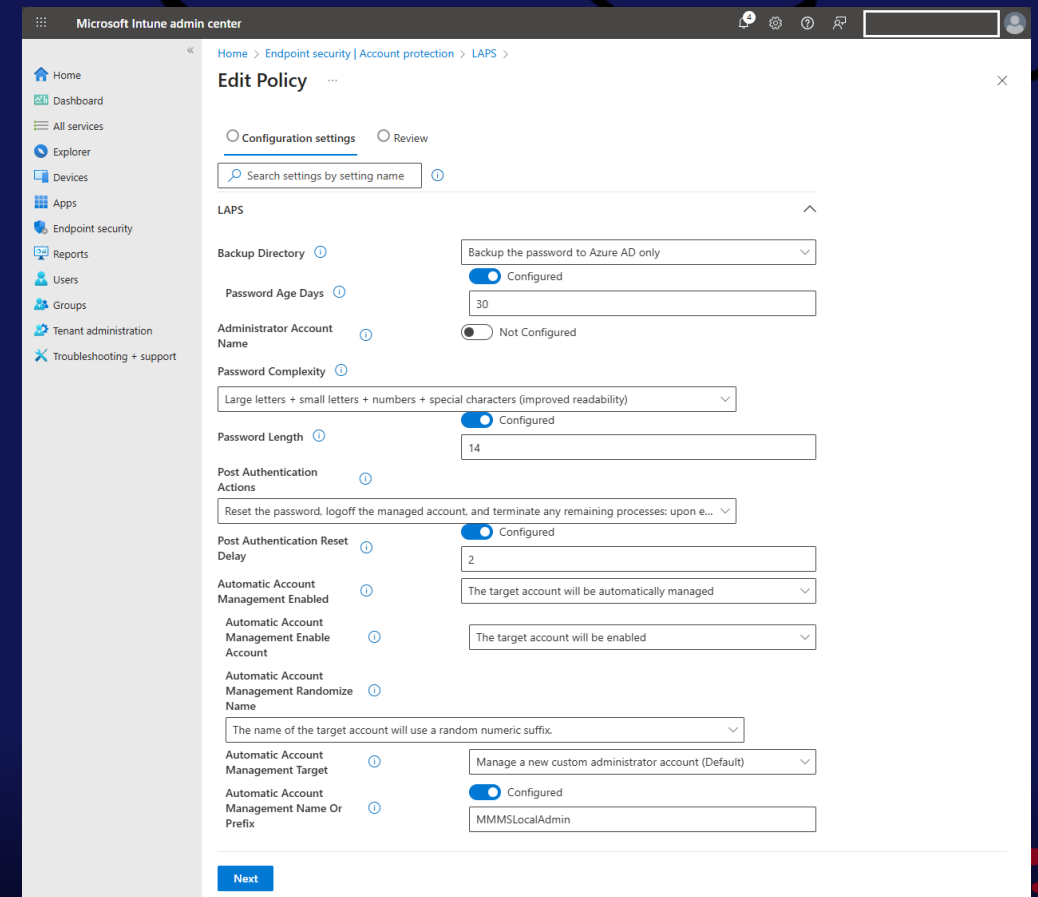
The DisableCMDRequest.tag file will not survive a wipe, but there is a way to ensure it is retained!

[Prevent Shift F10 Fix | KB5011487 | Windows Autopilot](#)



Local Admin Accounts

- ◆ A Local Admin account is required in some use cases, and this is where organizations have done some funky things..
 - ◆ Creating a standard local admin account with the same password across all devices.. What could go wrong?
- ◆ **One solution is Microsoft LAPS**
 - ◆ **Randomize the accounts across all of your devices, helping to reduce risk**



Passwords = Problems

Lets avoid repetition, and weak security



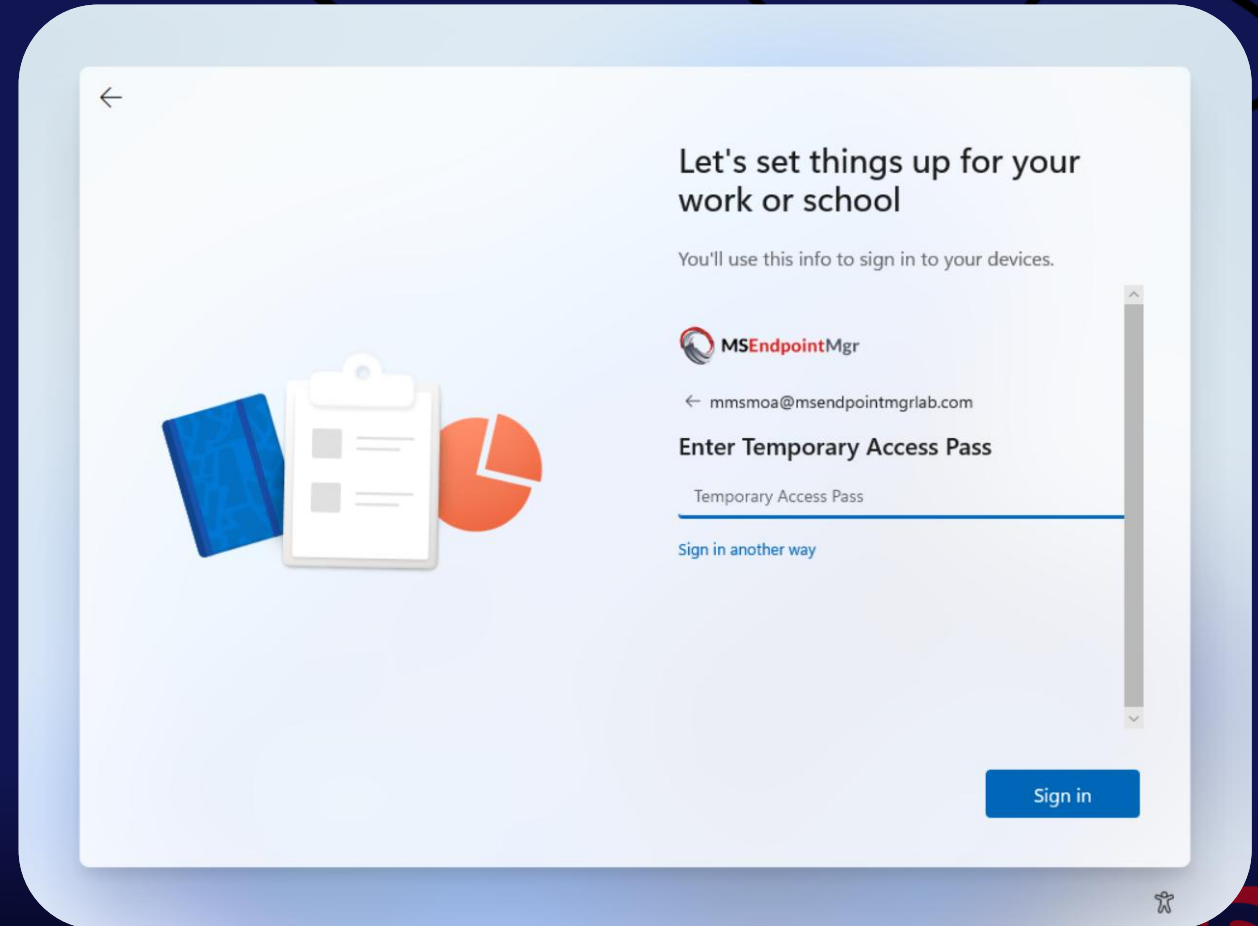


Windows **HELLO** for Business



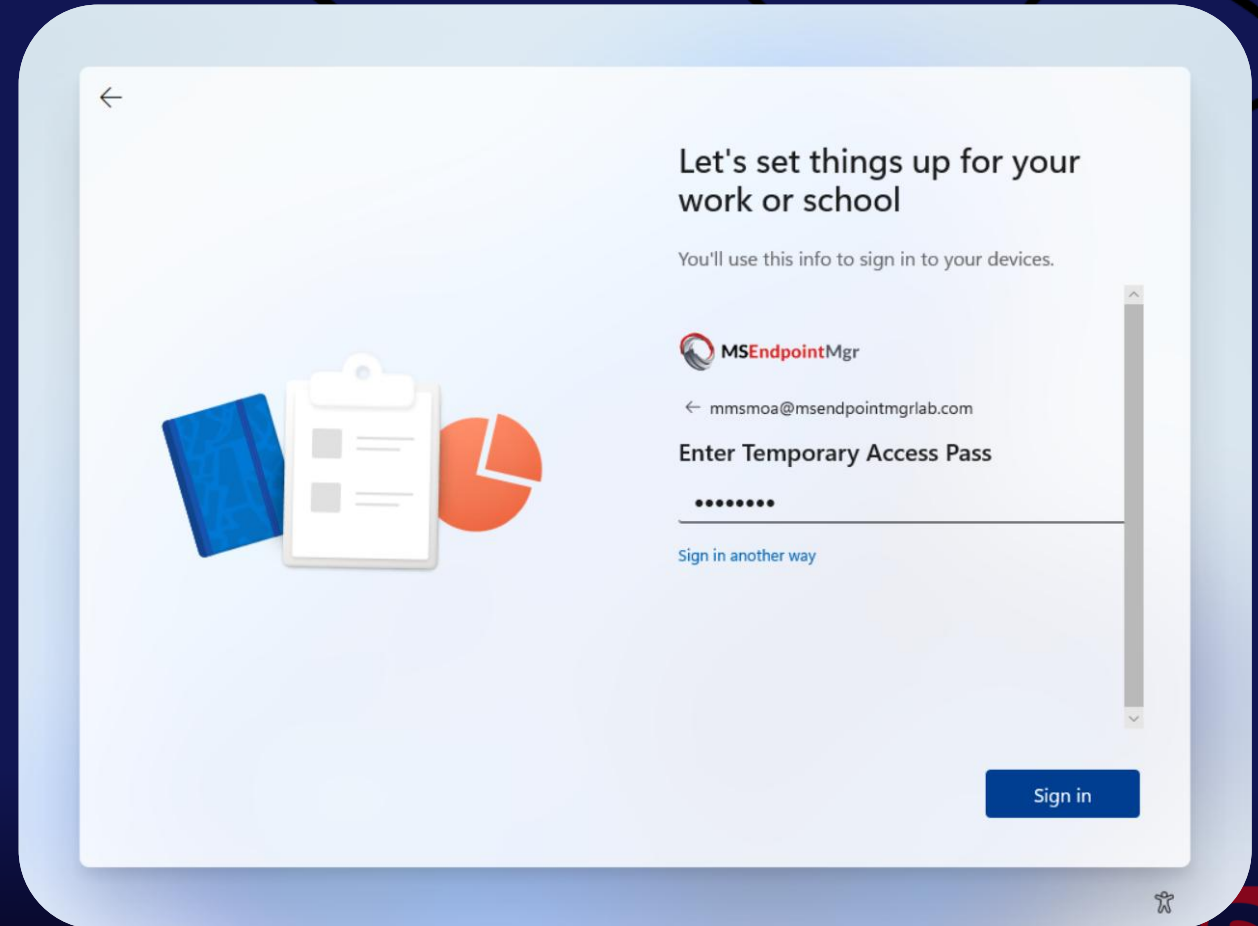
Windows Hello for Business

- **Windows Hello for Business**
 - Device bound PIN
 - Best implemented in conjunction with TAP
 - Self-service password reset is a must for unexpected movement of users between devices



Windows Hello for Business

- **Eliminates**
 - Reusable credentials
 - Protects against phishing and token reply attacks



Windows Hello for Business

A silhouette of a cowboy in a hat, standing in water and holding a lasso that is looping through the air. The background is a dark blue gradient with a red horizontal bar at the top.

- **Windows Hello for Business Multi-Factor Unlock**
 - Combine biometrics with your PIN for additional security
- **Kerberos Cloud Trust**
 - Use your Windows Hello for Business credentials for on-premises access

DEMO

Windows Hello

Kerberos cloud trust | Windows Hello Multi-Factor Unlock





Maurice Daly



Maurice Daly



Other user

Status: Running

ENG [Language icon] [Settings icon] [Power icon]



Other user

Status: Running

ENG GA [Language icon] [Settings icon] [Power icon]

Security Baselines

A bit like bowling guard rails

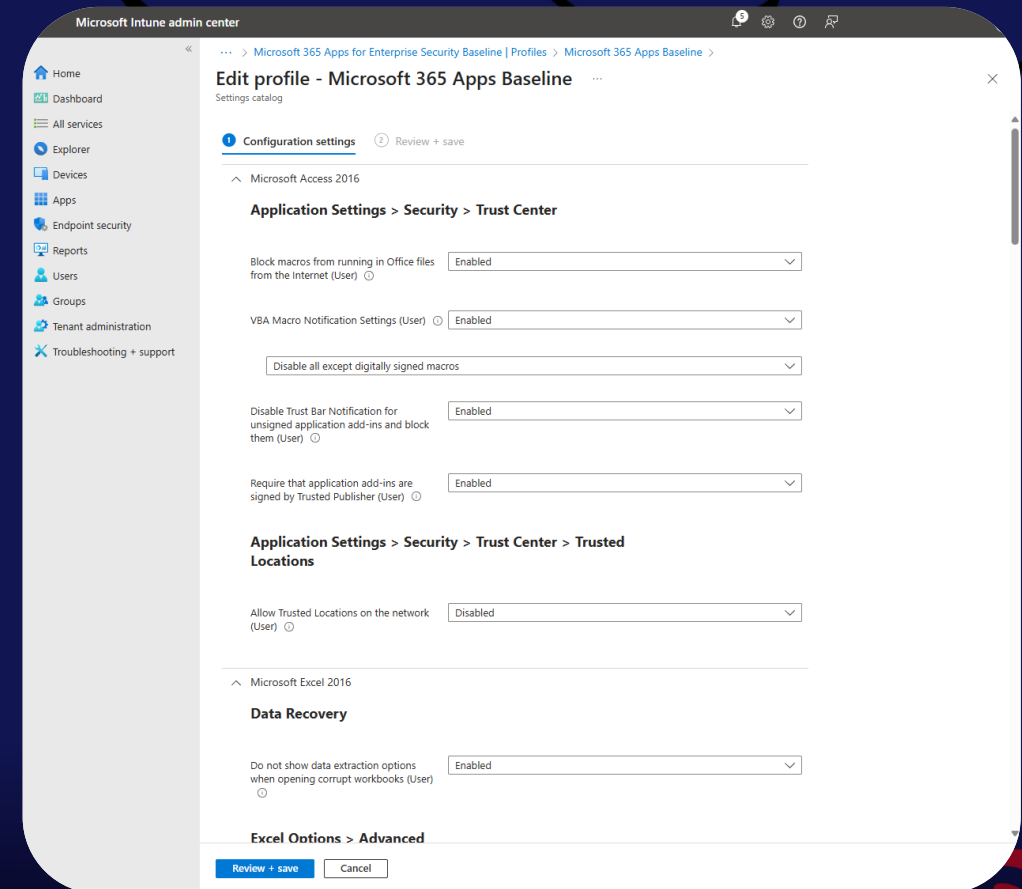


Security Baselines

Intune Endpoint Security Baselines

Similar to the values within the SCT, providing a “native Intune” approach to deploying the baseline configurations

- ◆ Pro’s
The ability to maintain customizations when moving from older to newer baseline configurations.
- ◆ Con’s
The baseline configurations are updated less frequently in some cases. Policies will conflict out of the box.



Security Baselines

CIS Baseline

The CIS Benchmarks are security configuration guidelines created and maintained by the Center for Internet Security.

They provide hardened baseline settings to help you secure your operating system against potential threats.

CIS Controls align with numerous established standards and regulatory frameworks, such as the NIST Cybersecurity Framework (CSF), NIST SP 800-53, the ISO 27000 series, PCI DSS, HIPAA, and more.



[Center for Internet Security \(CIS\) Benchmarks - Microsoft Compliance | Microsoft Learn](#)



Security Baselines

Community Baselines

Community fills the gaps others can't..

- ◆ **James Robinson – Open Intune Baseline**
[GitHub - SkipToTheEndpoint/OpenIntuneBaseline](https://github.com/SkipToTheEndpoint/OpenIntuneBaseline):
Community-driven baseline to accelerate Intune adoption
and learning.
- ◆ **Sandy Zeng – IntuneDiff**
<https://intunediff.com/>

OpenIntuneBaseline

Follow on X | Follow on Bsky | 875 | Read My Blog

Join WinAdmins 2.6k online

About the Project

Project History

The OpenIntuneBaseline (OIB) project was started in early 2021 as a way to provide a "known good" baseline security posture for Windows devices managed by Microsoft Intune, after being disappointed with the admin and user experience of other available baselines.

Security Framework Adherence

When creating the initial Windows security frameworks, such as:

- NCSC Device Security
- CIS Windows Benchmark
- ACSC Essential Eight
- Intune Security Baseline
- Microsoft Best Practices

The screenshot shows the IntuneDiff web application interface. At the top, there are navigation links for 'IntuneDiff', 'Compare Policies', 'Search Setting', and 'User Guide'. The main heading is 'Intune Policy Comparison'. Below this, there is a note: 'Supported Policy Types: This tool supports Security Baselines and policies using Settings Catalog configuration. Other policy types (Administrative Templates, Device Restrictions, etc.) may not display detailed comparisons.' The user is prompted to 'Select how you want to access your Intune policies'. There are two main options: 'Entra ID Authentication Method' and 'Offline JSON Method'. The 'Entra ID Authentication Method' section includes a sub-heading 'Direct Microsoft Graph API Access' and a description: 'Connect directly to your Microsoft Intune. This method provides real-time access to your Intune policies through the Microsoft Graph API.' It lists features: 'Real-time policy data', 'Automatic policy discovery', 'Secure authentication', and 'Full policy metadata'. There is a 'Sign In with Entra ID' button. The 'Offline JSON Method' section includes a sub-heading 'Manual JSON Import' and a description: 'Import and compare Intune policies using exported JSON files. Ideal for offline analysis or when authentication is not available to connect.' It lists features: 'No authentication required', 'Offline analysis', 'Custom JSON import', and 'Portable comparisons'. There is a 'Use JSON Method' button.

Security Baselines

OpenIntuneBaseline

Follow on X | Follow on Bsky 4975 | Read My Blog

Join WinAdmins 2.6k online

About the Project

Project History

The OpenIntuneBaseline (OIB) project was started in early 2021 as a way to provide a "known good" baseline security posture for Windows devices managed by Microsoft Intune, after being disappointed with the admin and user experience of other available baselines.

Security Framework Adherence

When creating the initial Windows baseline, substantial data analysis was carried out over well-known security frameworks, such as:

- NCSG Device Security Guidance
- CIS Windows Benchmarks
- ACSC Essential Eight
- Intune Security Baselines for Windows, Edge & Defender for Endpoint
- Microsoft Best Practice

- Microsoft Best Practice
- Intune Security Baselines for Windows, Edge & Defender for Endpoint
- NCSG Essential Eight
- CIS Windows Benchmarks
- Microsoft Best Practice

oyer

← Home

Help & FAQ



Microsoft Intune Authentication

Sign in with your work or school account to deploy OpenIntuneBaseline policies



Secure Authentication

Uses Microsoft Authentication Library (MSAL) for secure OAuth 2.0 authentication

Required Permissions:

- DeviceManagementConfiguration.ReadWrite.All



Sign in with Microsoft

This application will request permissions to read and write Intune configuration policies. Your credentials are handled securely by Microsoft's authentication service.



c0-maurice.daly@msendpointmgrlab.com

Permissions requested



OpenIntuneBaseline Deployer
unverified

This application is not published by Microsoft or your organization.

This app would like to:

- ✓ Read and write Microsoft Intune Device Configuration and Policies
- ✓ View your basic profile
- ✓ Maintain access to data you have given it access to
- Consent on behalf of your organization

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. **The publisher has not provided links to their terms for you to review.** You can change these permissions at <https://myapps.microsoft.com>. [Show details](#)

Does this app look suspicious? [Report it here](#)

Cancel

Accept

OpenIntuneBaseline Deployer - Deploy standardized Intune policies with ease

GitHub Repository

OIB Website

GitHub Repository

OIB Website

OpenIntuneBaseline Deployer - Deploy standardized Intune policies with ease

Cancel

Accept

DEMO

Security Baselines

Native, Microsoft imported, Community.. Which is the best?



Credential Guard

Credential Guard is a feature that leverages Virtualization-Based Security to isolate credentials for use by privileged system software.

- ◆ Benefits
 - ◆ Reduce the risk of credential theft through NTLM, stored credentials and Kerberos TGT extraction
- ◆ Considerations
 - ◆ 802.1x networks

Windows edition and licensing requirements

The following table lists the Windows editions that support Credential Guard:

[Expand table](#)

Windows Pro	Windows Enterprise	Windows Pro Education/SE	Windows Education
No	Yes	No	Yes

Credential Guard license entitlements are granted by the following licenses:

[Expand table](#)

Windows Pro/Pro Education/SE	Windows Enterprise E3	Windows Enterprise E5	Windows Education A3	Windows Education A5
No	Yes	Yes	Yes	Yes

Note

Devices running Windows 11 Pro/Pro Edu 22H2 or later may have Virtualization-based Security (VBS) and/or Credential Guard automatically enabled if they meet the other requirements for default enablement, and have previously run Credential Guard. For example if Credential Guard was enabled on an Enterprise device that later downgraded to Pro.

To determine whether the Pro device is in this state, check if the following registry key exists:

`Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0\IsolatedCredentialsRootSecret`. In this scenario, if you wish to disable VBS and Credential Guard, follow the instructions to [disable Virtualization-based Security](#). If you wish to disable Credential Guard only, without disabling VBS, use the procedures to [disable Credential Guard](#).

Credential Guard

```
PowerShell 7 (x64)
PS C:\> Get-CimInstance -ClassName Win32_DeviceGuard -Namespace root\Microsoft\Windows\DeviceGuard | FL

AvailableSecurityProperties      : {1, 2, 3, 5...}
CodeIntegrityPolicyEnforcementStatus : 2
InstanceIdentifier              : 4ff40742-2649-41b8-bdd1-e80fad1cce80
RequiredSecurityProperties      : {1, 2}
SecurityFeaturesEnabled         : {0}
SecurityServicesConfigured     : {1, 2, 3}
SecurityServicesRunning        : {1, 2}
SmmIsolationLevel              : 0
UsermodeCodeIntegrityPolicyEnforcementStatus : 0
Version                         : 1.0
VirtualizationBasedSecurityStatus : 2
VirtualMachineIsolation        : False
VirtualMachineIsolationProperties : {0}
PSComputerName                  :
```

```
b2CompuName
VirtualizationBasedSecurityStatus : {0}
VirtualMachineIsolationProperties : {0}
VirtualMachineIsolationProperties : {0}
```

Credential Guard

Available Security Properties

Value Description

0 If present, no relevant properties exist on the device.

1 If present, hypervisor support is available.

2 If present, Secure Boot is available.

3 If present, DMA protection is available.

4 If present, Secure Memory Overwrite is available.

5 If present, NX protections are available.

6 If present, SMM mitigations are available.

7 If present, MBEC/GMET is available.

8 If present, APIC virtualization is available.

```
PowerShell 7 (x64)
PS C:\> Get-CimInstance -ClassName Win32_DeviceGuard -Namespace root\Microsoft\Windows\DeviceGuard | FL
AvailableSecurityProperties : {1, 2, 3, 5...}
CodeIntegrityPolicyEnforcementStatus : 2
InstanceIdentifier : 4fff40742-2649-41b8-bdd1-e80fad1cce80
RequiredSecurityProperties : {1, 2}
SecurityFeaturesEnabled : {0}
SecurityServicesConfigured : {1, 2, 3}
SecurityServicesRunning : {1, 2}
SmmIsolationLevel : 0
UsermodeCodeIntegrityPolicyEnforcementStatus : 0
Version : 1.0
VirtualizationBasedSecurityStatus : 2
VirtualMachineIsolation : False
VirtualMachineIsolationProperties : {0}
PSComputerName :

PS C:\> Get-CimInstance -ClassName Win32_DeviceGuard -Namespace root\Microsoft\Windows\DeviceGuard | Select-Object -ExpandProperty AvailableSecurityProperties
1
2
3
5
6
7
8
PS C:\>
```

Component	Detail
Processor	<ul style="list-style-type: none">Intel 8th generation or later starting with Windows 11, version 22H2 (11th generation Core processors and newer only for Windows 11, version 21H2)AMD Zen 2 architecture and newerQualcomm Snapdragon 8180 and newer
RAM	Minimum 8GB (Only applicable for x64 processors)
Storage	SSD with a minimum size of 64GB
Drivers	Memory integrity-compatible drivers must be installed. See Driver compatibility with memory integrity for more information about drivers.
BIOS	Virtualization must be enabled

Credential Guard – Memory Integrity

Automatic Enablement

Memory integrity is enabled by default once a device meets the minimum hardware feature list.

- ◆ New Windows 11 devices

Component	Detail
Processor	<ul style="list-style-type: none">• Intel 8th generation or later starting with Windows 11, version 22H2 (11th generation Core processors and newer only for Windows 11, version 21H2)• AMD Zen 2 architecture and newer• Qualcomm Snapdragon 8180 and newer
RAM	Minimum 8GB (Only applicable for x64 processors)
Storage	SSD with a minimum size of 64GB
Drivers	Memory integrity-compatible drivers must be installed. See Driver compatibility with memory integrity for more information about drivers.
BIOS	Virtualization must be enabled

ⓘ Note

Auto-enablement pertains only to clean installs, not upgrades of existing devices.

Kernal DMA Protection

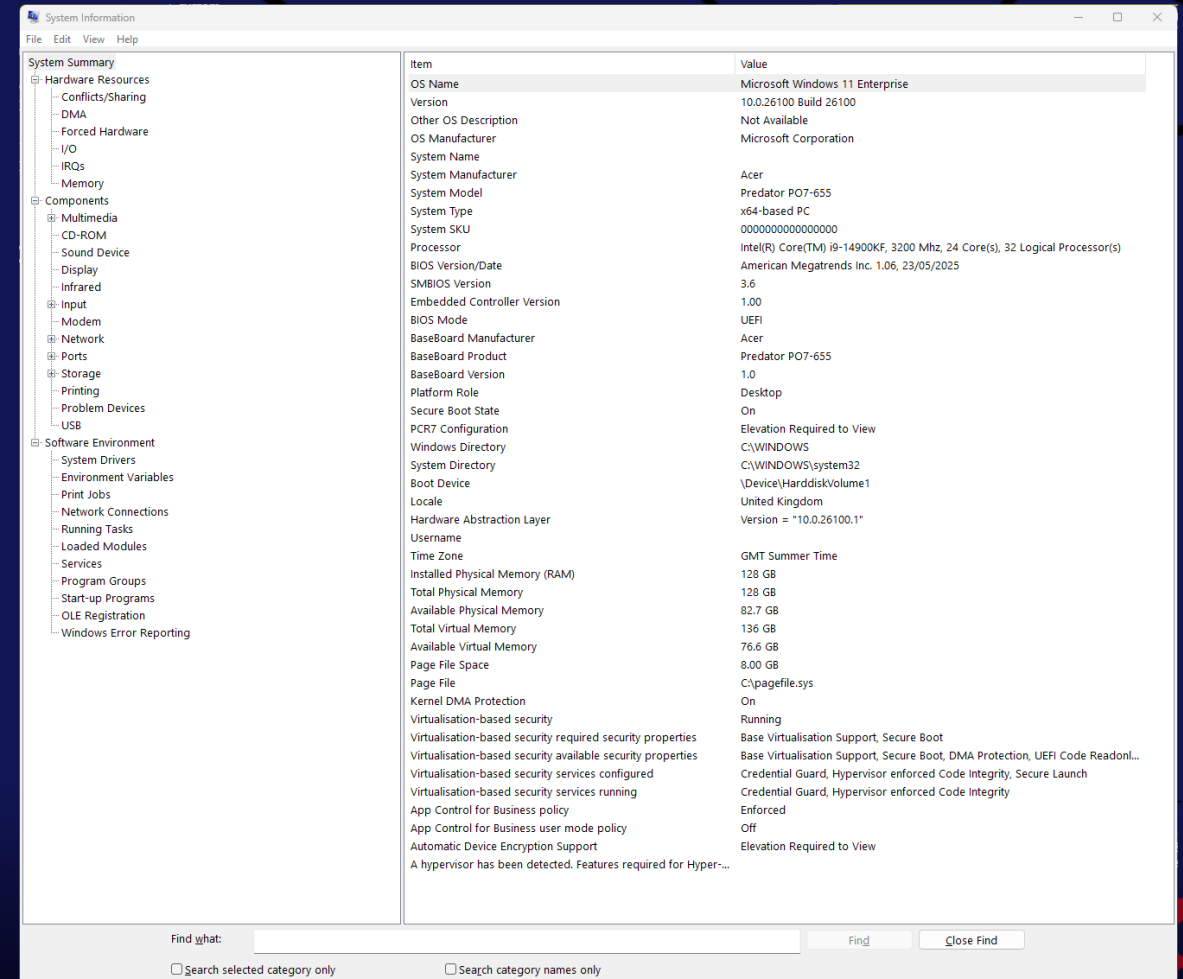
A security feature introduced in Windows 10 1803 that helps mitigate malicious direct memory access (DMA) attacks on supported Intel and AMD devices.

Protect Against

- ◆ Thunderbolt device vulnerabilities

Requirements

- ◆ Intel VT-X
- ◆ AMD-v



The screenshot shows the Windows System Information window. The left pane displays a tree view of system categories, including Hardware Resources, Components, and Software Environment. The right pane shows a list of system items and their values. Key items include OS Name (Microsoft Windows 11 Enterprise), Processor (Intel(R) Core(TM) i9-14900KF), and Kernel DMA Protection (On).

Item	Value
OS Name	Microsoft Windows 11 Enterprise
Version	10.0.26100 Build 26100
Other OS Description	Not Available
OS Manufacturer	Microsoft Corporation
System Name	
System Manufacturer	Acer
System Model	Predator P07-655
System Type	x64-based PC
System SKU	0000000000000000
Processor	Intel(R) Core(TM) i9-14900KF, 3200 Mhz, 24 Core(s), 32 Logical Processor(s)
BIOS Version/Date	American Megatrends Inc. 1.06, 23/05/2025
SMBIOS Version	3.6
Embedded Controller Version	1.00
BIOS Mode	UEFI
BaseBoard Manufacturer	Acer
BaseBoard Product	Predator P07-655
BaseBoard Version	1.0
Platform Role	Desktop
Secure Boot State	On
PCR7 Configuration	Elevation Required to View
Windows Directory	C:\WINDOWS
System Directory	C:\WINDOWS\system32
Boot Device	\Device\HarddiskVolume1
Locale	United Kingdom
Hardware Abstraction Layer	Version = "10.0.26100.1"
Username	
Time Zone	GMT Summer Time
Installed Physical Memory (RAM)	128 GB
Total Physical Memory	128 GB
Available Physical Memory	82.7 GB
Total Virtual Memory	136 GB
Available Virtual Memory	76.6 GB
Page File Space	8.00 GB
Page File	C:\pagefile.sys
Kernel DMA Protection	On
Virtualisation-based security	Running
Virtualisation-based security required security properties	Base Virtualisation Support, Secure Boot
Virtualisation-based security available security properties	Base Virtualisation Support, Secure Boot, DMA Protection, UEFI Code Readonl...
Virtualisation-based security services configured	Credential Guard, Hypervisor enforced Code Integrity, Secure Launch
Virtualisation-based security services running	Credential Guard, Hypervisor enforced Code Integrity
App Control for Business policy	Enforced
App Control for Business user mode policy	Off
Automatic Device Encryption Support	Elevation Required to View
A hypervisor has been detected. Features required for Hyper...	

- Sound Device
- Display
- Infrared
- Input
- Modem
- Network
- Ports
- Storage
- Printing
- Problem Devices
- USB
- Software Environment
 - System Drivers
 - Environment Variables
 - Print Jobs
 - Network Connections
 - Running Tasks
 - Loaded Modules
 - Services
 - Program Groups
 - Start-up Programs
 - OLE Registration
 - Windows Error Reporting

BIOS Version/Date	American Megatrends Inc. 1.06, 23/05/2025
SMBIOS Version	3.6
Embedded Controller Version	1.00
BIOS Mode	UEFI
BaseBoard Manufacturer	Acer
BaseBoard Product	Predator PO7-655
BaseBoard Version	1.0
Platform Role	Desktop
Secure Boot State	On
PCR7 Configuration	Elevation Required to View
Windows Directory	C:\WINDOWS
System Directory	C:\WINDOWS\system32
Boot Device	\Device\HarddiskVolume1
Locale	United Kingdom
Hardware Abstraction Layer	Version = "10.0.26100.1"
Username	
Time Zone	GMT Summer Time
Installed Physical Memory (RAM)	128 GB
Total Physical Memory	128 GB
Available Physical Memory	82.7 GB
Total Virtual Memory	136 GB
Available Virtual Memory	76.6 GB
Page File Space	8.00 GB
Page File	C:\pagefile.sys
Kernel DMA Protection	On
Virtualisation-based security	Running
Virtualisation-based security required security properties	Base Virtualisation Support, Secure Boot
Virtualisation-based security available security properties	Base Virtualisation Support, Secure Boot, DMA Protection, UEFI Code Readonl...
Virtualisation-based security services configured	Credential Guard, Hypervisor enforced Code Integrity, Secure Launch
Virtualisation-based security services running	Credential Guard, Hypervisor enforced Code Integrity
App Control for Business policy	Enforced
App Control for Business user mode policy	Off
Automatic Device Encryption Support	Elevation Required to View
A hypervisor has been detected. Features required for Hyper-...	

Find what:

Find

Close Find

Search selected category only

Search category names only



Hardware Security

Security baked in..



Secure Boot

Secure boot is a security standard developed by OEM's, which helps ensure that you are using trusted boot loader signatures from the UEFI BIOS

- ◆ Recommendations
 - ◆ Order devices with Secure Boot enabled from the OEM
 - ◆ Monitor using a compliance policy (but be careful)
 - ◆ Scripted a solution to remediate Secure Boot states, leveraging OEM tools
- ◆ Considerations
 - ◆ Devices that do not support PCR7 binding



Secure Boot – June 2026

What happens when you have certificates?

- ◆ They expire..

What happens when your BIOS and Boot loader don't have the same certificate sources?

- ◆ Bad things..well not really..

```
Administrator: C:\Program Files\PowerShell\7\pwsh.exe
cmdlet Get-SecureBootUEFI at command pipeline position 1
Supply values for the following parameters:
Name:
PS C:\Git Repo\DriverAutomationToolDev> Get-SecureBootUEFI -Decoded -Name KEK

SignatureOwner : 70564dce-9afc-4ee3-85fc-949649d7e45c
Subject        : CN=Dell Inc. Key Exchange Key, O=Dell Inc., L=Round Rock, S=Texas, C=US
Version       : 3
Algorithm      : sha256RSA
SerialNumber   : 279BAD52BF5DABB24C367742F4EBACCD
ValidFrom     : 2016-06-01 21:22:48Z
ValidTo       : 2023-06-01 21:32:47Z

SignatureOwner : 77fa9abd-0359-4d32-bd60-28f4e78f784b
Subject        : CN=Microsoft Corporation KEK CA 2011, O=Microsoft Corporation, L=Redmond, S=Washington, C=US
Version       : 3
Algorithm      : sha256RSA
SerialNumber   : 610AD18800000000000003
ValidFrom     : 2011-06-24 21:41:29Z
ValidTo       : 2026-06-24 21:51:29Z

SignatureOwner : 77fa9abd-0359-4d32-bd60-28f4e78f784b
Subject        : CN=Microsoft Corporation KEK 2K CA 2023, O=Microsoft Corporation, C=US
Version       : 3
Algorithm      : sha256RSA
SerialNumber   : 33000000131416B8616D82824B000000000013
ValidFrom     : 2023-03-02 20:21:35Z
ValidTo       : 2038-03-02 20:31:35Z

C:\Git Repo\DriverAutomationToolDev>
```

Secure Boot – June 2026

```
Administrator: C:\Program Files\PowerShell\7\pwsh.exe
cmdlet Get-SecureBootUEFI at command pipeline position 1
Supply values for the following parameters:
Name:
PS C:\G
```

BIOS Updates
 Devices: 156 OEM Records: 1249 SKU Lookups: 2284 Model Lookups: 1249

96 devices

Risk Notices — 21 below minimum, 8 models at risk, 20 unmatched

Severity	Type	Device	Current	Minimum
Low	Below Min	PMPC- Dell - Precision 3660	2.2.0	2.30.1
Low	Below Min	PMPC- Dell - XPS 15 9530	1.4.0	1.25.1
Low	Below Min	PMPC- Dell - Precision 3650 Tower	1.22.2	1.44.0
Low	Below Min	PMPC- Dell - XPS 15 9530	1.5.0	1.25.1
Low	Below Min	PMPC- Dell - XPS 15 9530	1.7.0	1.25.1
Low	Below Min	PMPC- Dell - XPS 15 9530	1.7.0	1.25.1

BIOS Updates
 Devices: 161 OEM Records: 1249 SKU Lookups: 2284 Model Lookups: 1249 OEM Storage:

96 devices

Risk Notices — 7 below minimum, 5 models at risk, 22 unmatched

Severity	Type	Model	Devices	Out of Date	Below Min	Risk
High	Model Risk	Dell Pro Max Tower T2 FCT250 Dell - 1 device	1	1	1	100%
High	Model Risk	ThinkStation P340 Lenovo - 1 device	1	1	1	100%
Medium	Model Risk	Precision 3660 Dell - 2 devices	2	1	0	50%
Low	Model Risk	XPS 15 9530 Dell - 14 devices	14	3	3	21%
Low	Model Risk	Precision 5690 Dell - 12 devices	12	2	2	17%





BIOS Updates



Maurice Daly
maurice@patchmypc.com

Secure Boot Inventory

NAVIGATION

Dashboard

Devices

BIOS Updates

Settings

High	Model Risk	Lenovo - 1 device	1	1	1	100%
High	Model Risk	Pre Dell	1			100%
Medium	Model Risk	Pre Dell	8			67%
Medium	Model Risk	XPS Dell	8			57%
Low	Model Risk	Dell	0			20%
Low	Model Risk	XPS Dell	1			3%

► Diagnostic Data (click to expand)

Search by name, model, SKU, BIOS version

Showing 143 of 156 devices

Computer Name	Manufacturer	Model	SKU	Current BIOS	Minimum BIOS	Latest BIOS	Status	SystemSKU	Model
PMP-	Dell			1.5.0	1.25.1	1.26.0	Out of Date		
PMP-	Dell	Precision 5690	OCC8	1.13.1	1.17.0	1.15.1	Out of Date	SystemSKU	Precision 5690
PMP-	Dell	Dell Pro Max 16 Plus MB16250	0D12	1.3.3	2.1.1	1.3.3	Out of Date	SystemSKU	Pro Max 16 Plus MB16250_18 Plus MB18250
PMP-	Dell	Precision 5690	OCC8	1.11.0	1.17.0	1.15.1	Out of Date	SystemSKU	Precision 5690
PMP-	Dell	Precision 5690	OCC8	1.11.0	1.17.0	1.15.1	Out of Date	SystemSKU	Precision 5690
PMP-	Dell	XPS 15 9530	0BEB	1.4.0	1.26.0	1.25.1	Out of Date	SystemSKU	XPS 15 9530

Showing 1-10 of 143 devices

Rows per page: 10

« ‹ 1 2 3 4 5 › »

PMP-

Dell - XPS 15 9530

MAKE
Dell

MODEL
XPS 15 9530

CURRENT BIOS VERSION
1.5.0 ✖

MINIMUM BIOS VERSION
1.25.1
The minimum version required to support the Microsoft Secure Boot 2026 CA updates.

LATEST BIOS VERSION
1.26.0 Urgent
The latest version returned from the vendor catalog. At times the latest BIOS might be newer on the model-specific page.

BIOS RELEASE DATE
2025-11-20

STATUS
Out of Date

BIOS DOWNLOAD
<http://www.dell.com/support/home/us/en/19/Drivers/DriversDetails?driverId=GJJ9J>

FILE HASH (MD5)
411a723b9517c9519bfb1d4383b51008

SUPPORTED DEVICES
0BEB

RELEASE NOTES

- This BIOS contains the new 2023 Secure Boot Certificates.
- Once the BIOS is upgraded to version 1.26.0, you cannot downgrade the BIOS to earlier versions. BIOS downgrades are restricted when there are security updates and important fixes with earlier versions that impact the functionality of the system.
- BIOS updates take no more than 5 minutes to be installed on your system. You can install the updates in the background while using the system.



Secure Boot – June 2026

The image displays the Driver Automation Tool interface, which is used for automating OEM driver and BIOS packaging. The main dashboard features a navigation menu with Home, Reports, Setup Guide, About, and GitHub. The central area is titled "Automate your OEM driver and BIOS packaging" and describes the tool's capabilities for enterprise-grade automation. Below this, there are statistics for various OEMs: HP (573 Driver Packs - 664 BIOS Updates), Dell (478 Driver Packs - 366 BIOS Updates), Lenovo (474 Driver Packs - 474 BIOS Updates), Microsoft (51 Driver Packs), and Acer (70 Driver Packs - 56 BIOS Updates). An "Explore Features" button is also present.

The "Model Selection" window is open, showing a list of selected models for a Dell Precision 5690 - x64. The filters are set to OEM: 5 selected, Operating System: Windows 11 25H2, Architecture: x64, Platform: Intune, and Package Type: BIOS. The table below shows the selected models:

OEM	Model	OS	Build	Baseboards	Driver	BIOS
Dell	Dell Pro Max 16 Plus MB16250	Windows 11	25H2	0D12	A03	2.6.1
Dell	Latitude 3540	Windows 11	25H2	0C1C,0C1E	A12	1.29.0
Dell	Latitude 5420	Windows 11	25H2	0A20,0A40	A13	1.51.0
Dell	Latitude 5540	Windows 11	25H2	0C05	A12	1.27.1
Dell	Latitude 5550	Windows 11	25H2	0CB9,0CBC	A11	1.21.0
Dell	Precision 3650 Tower	Windows 11	25H2	0A58,0A59	A11	1.45.0
				OCC7	A10	1.18.1
				OCC8	A08	1.20.0

The BIOS update status window for the Dell Precision 5690 - x64 shows the following details:

- Publisher: Dell
- Operating system: Windows
- Version: 1.20.0

The device status is shown as a donut chart with 134 total updates. The breakdown is:

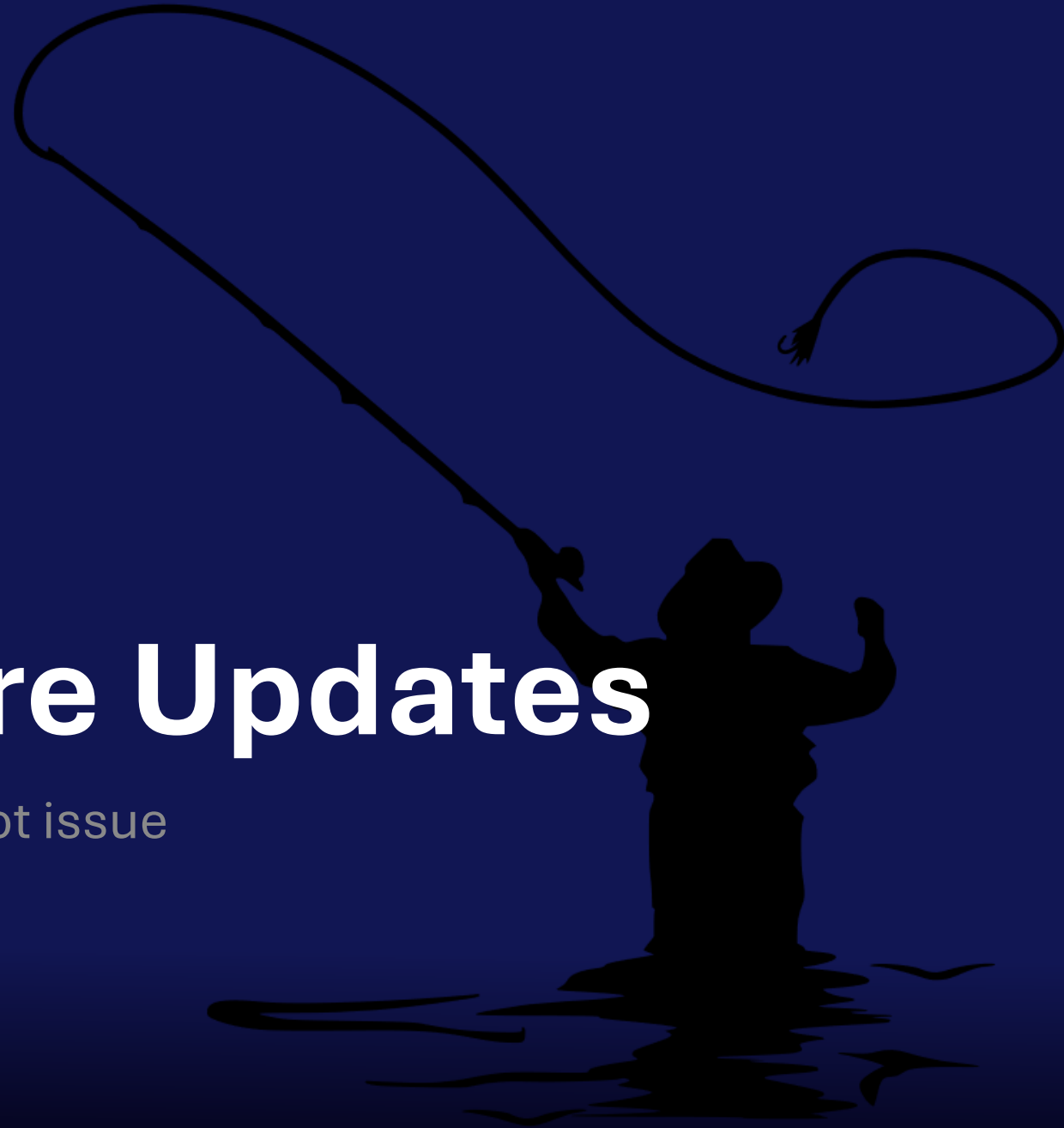
- Installed: 10
- Next installed: 0
- Failed: 0
- Install Pending: 0
- Not Applicable: 124

A notification window titled "BIOS Update Pending" is displayed, indicating that the device has pending updates required for security and stability. The message states: "Your device has pending updates which are required for security / stability reasons. Pressing the Update button will trigger a restart of your device. DO NOT power off the device during the update process." The notification includes two buttons: "Update Now" and "Remind Me Later".

DEMO

Firmware Updates

Fixing the secure boot issue



Attack Surface Reduction

And your shortcuts went poof..



Who wants to be an MMSillionaire

Question.

What does Attack Surface Reduction do?

Protects your legs from dog bites

Helps prevent mosquito bites

Stops the Zombie apocalypse

Reduces Windows surface risk

Who wants to be an MMSillionaire

Question.

What does Attack Surface Reduction do?

Protects your legs from dog bites

Helps prevent mosquito bites

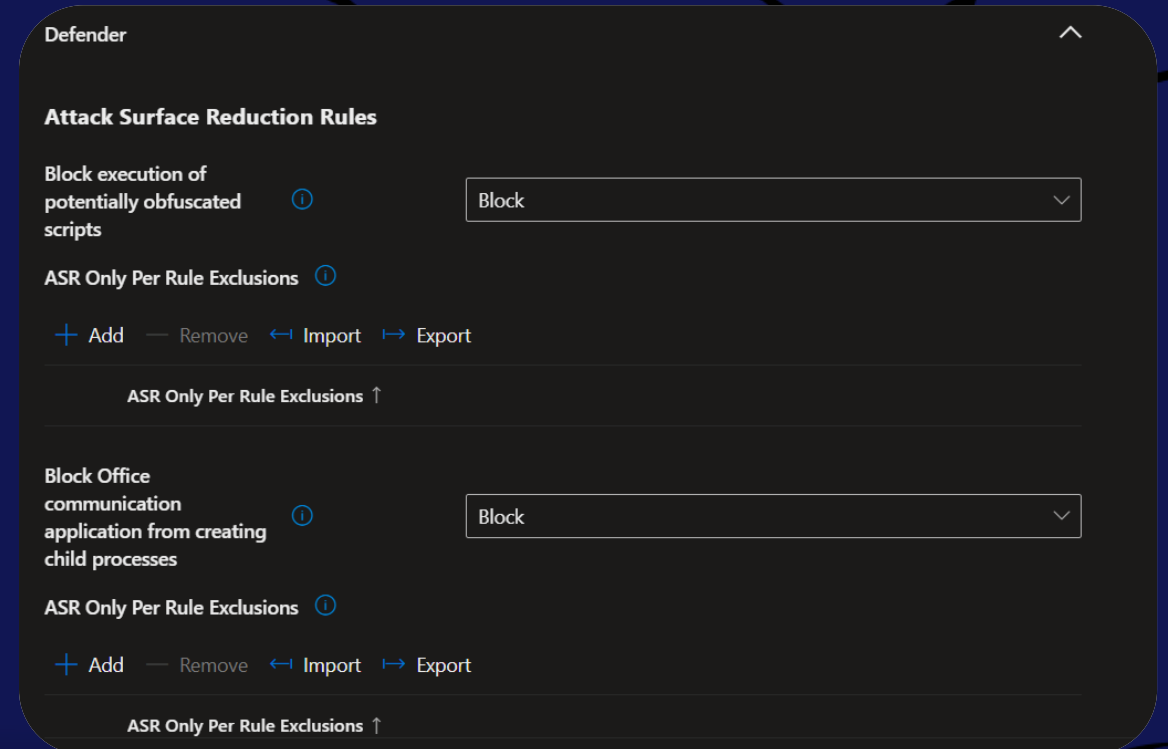
Stops the Zombie apocalypse

Reduces Windows surface risk

Attack Surface Reduction

Attack Surface Reduction (ASR) does exactly what it says, reducing the attack / threat surface of your Windows device

It is broken down into multiple areas, and is surfaced in the Microsoft Security portal, both for recommended configuration, and reporting.



Microsoft Defender

Attack surface reduction rules

Detections Configuration Add exclusions

Review possible breach activity detected by attack surface reduction rules on your devices. [Learn more about this activity](#)

Filters: Rules: Standard protection X Date: 4/6/2026-5/6/2026 X Select rules: Any X

Audited detections: 0
Blocked detections: 8819

Export

Detected file	Detected on	Blocked/Audite...	Rule
<input type="checkbox"/> svchost.exe	May 6, 2026 9:57 PM	Blocked	Block credential st
<input type="checkbox"/> svchost.exe	May 6, 2026 9:56 PM	Blocked	Block credential st
<input type="checkbox"/> svchost.exe	May 6, 2026 9:49 PM	Blocked	Block credential st

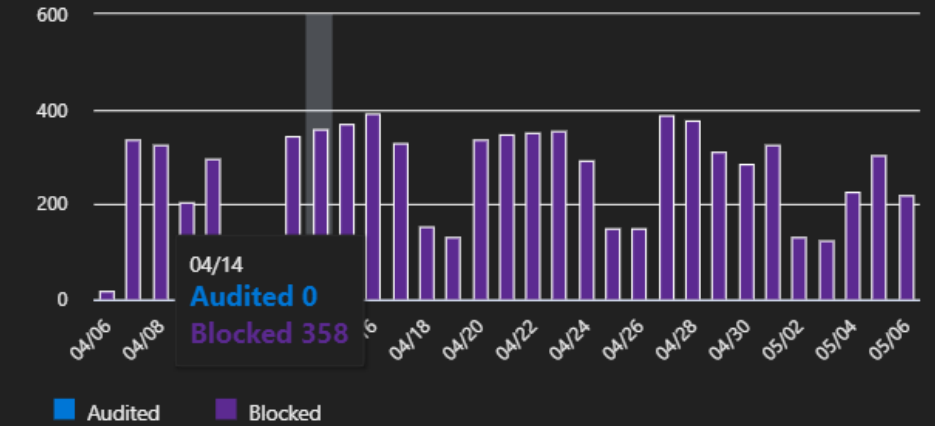
File info

Detected file

svchost.exe

Detections

Go hunt Open file page



Possible exclusions and impact

Exclude a file if you believe it is being detected incorrectly. When excluded, the file won't be blocked even if attack surface reduction rules detect it exhibiting possible attack behavior.

Detections

10589

Over the last 30 days, this file triggered 8190 detections for the associated rule. Those detections constitute 77% of all the detections for this rule in your organization. [Learn more about exclusions](#)

Add exclusions

Patching

Err.. Not just Autopatch

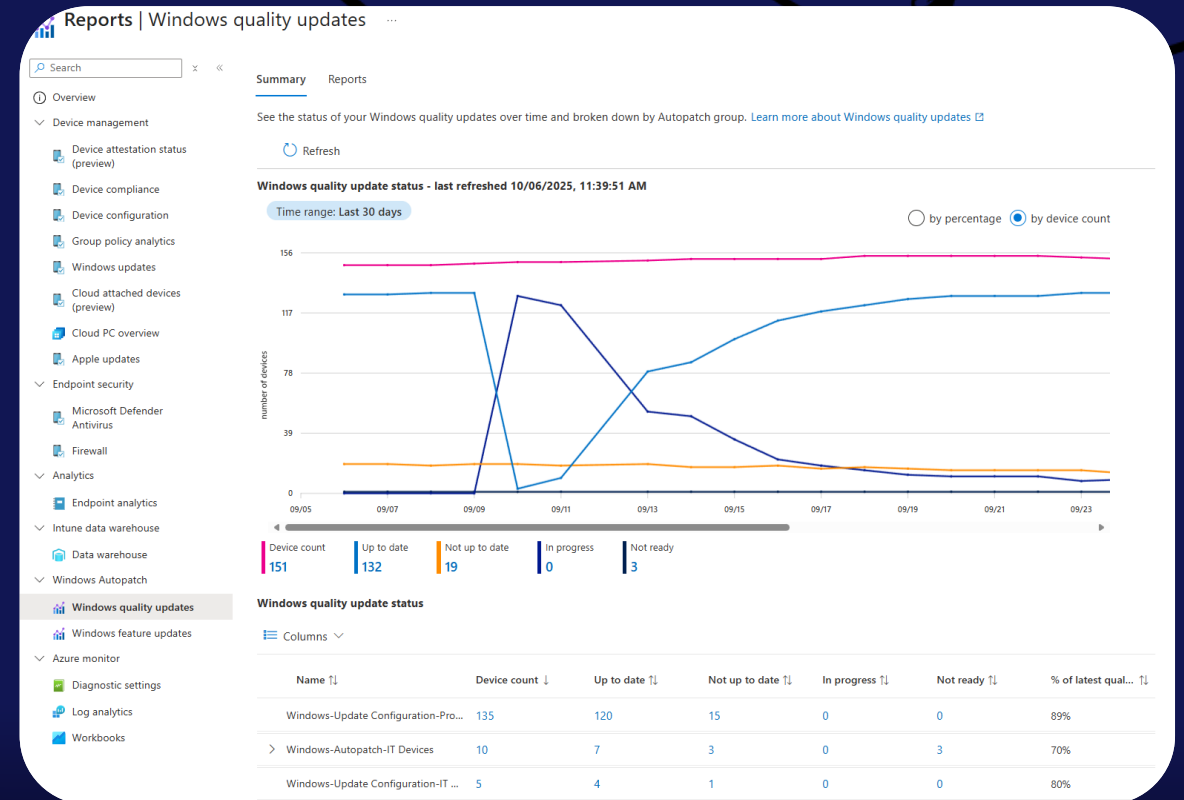


Patching

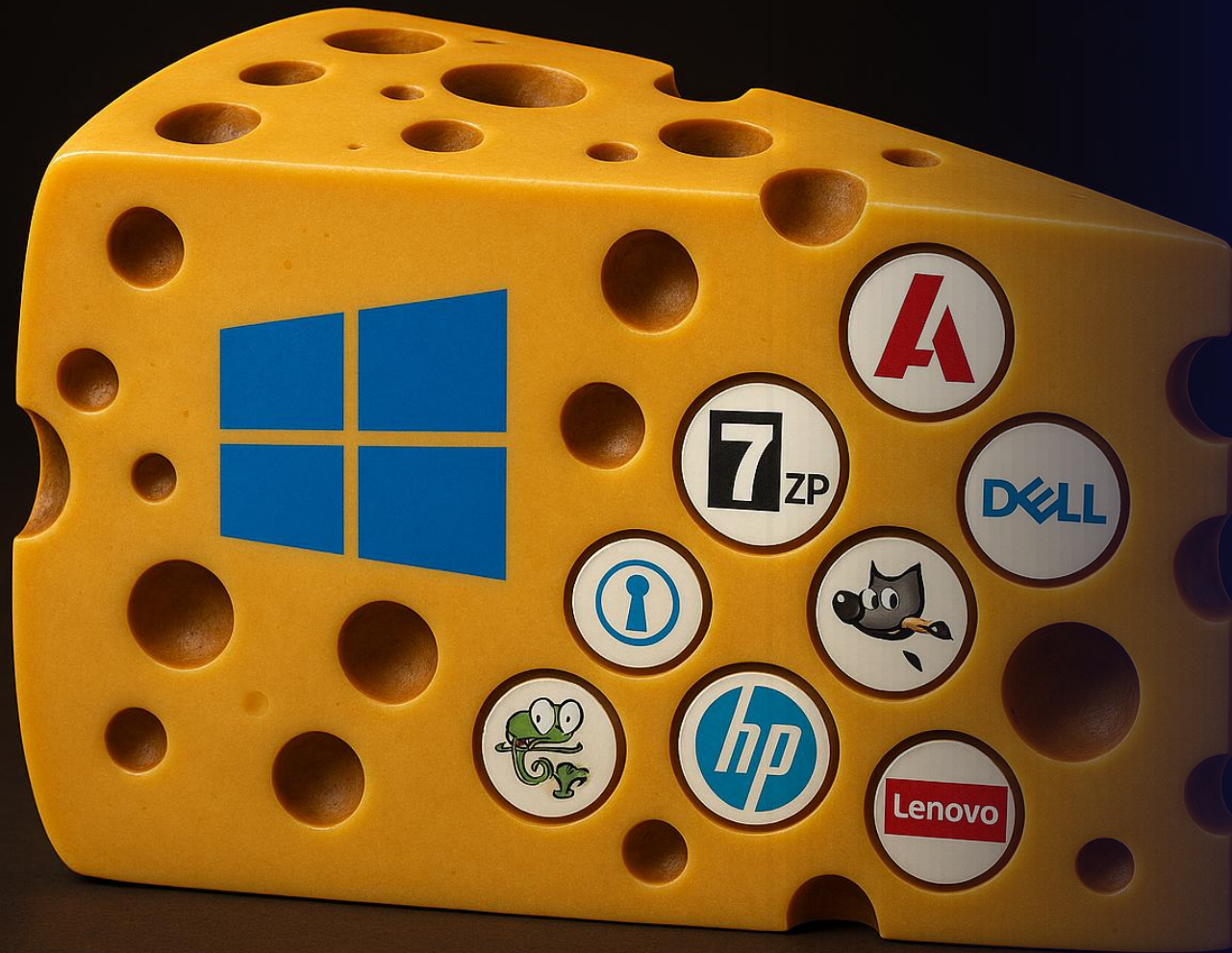
Why are we patching?

- ◆ Getting the latest features out of the OS, products, and the device?
- ◆ Fixing stability issues?
- ◆ Closing security gaps within the OS, products, and firmware?

HINT: It's all of the above



Patching



Third Party Patching

- ◆ Often gets overlooked
- ◆ “Not in budget”

But. The reality is that users often continue to use applications that remain unpatched for years. Providing a back door for vulnerability exploits.

Ransomware

Landscape and trends

Ransomware remains one of the most serious cybersecurity concerns. And for valid reasons.

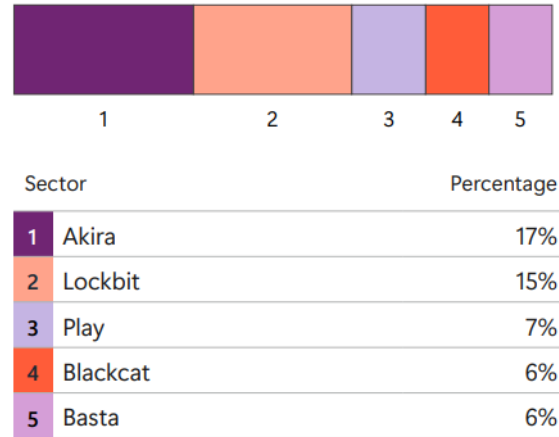
Among our customers, Microsoft observed a 2.75x increase year over year in human-operated ransomware-linked encounters (defined as having at least one device targeted for a ransomware attack in a network).

Meanwhile, the percentage of attacks reaching actual encryption phase has decreased over the past two years by threefold. Automatic attack disruption contributed to this positive trend in decreasing successful attacks. In more than 90% of cases where attacks progressed to ransom stage, the attacker had leveraged unmanaged devices in the network, either to gain initial access or to remotely encrypt assets at the impact stage.

↓ **3x**

threefold decrease in ransom attacks reaching encryption stage over the past two years

Top human-operated ransomware groups

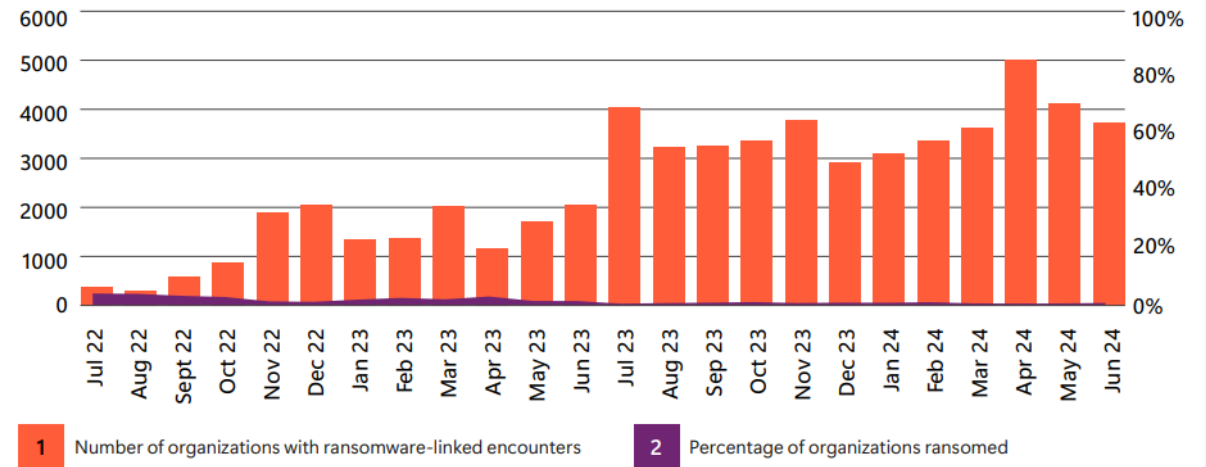


The top five ransomware families accounted for 51% of attacks. These families continue to use longstanding techniques, showing their effectiveness even against rising cybersecurity awareness globally.

Source: Microsoft Defender for Endpoint

The most prevalent initial access techniques continue to be social engineering—specifically email phishing, SMS phishing, and voice phishing—identity compromise, and exploiting vulnerabilities in public facing applications or unpatched operating systems. Attackers continue to take advantage of newly identified common vulnerabilities and exposures

Organizations with ransom-linked encounters continues to increase while the percentage of those ransomed is decreasing (July 2022–June 2024)



Although organizations with ransom-linked encounters continues to increase, the percentage that are ultimately ransomed (reaching encryption stage) decreased more than threefold over the past two years.

Source: Microsoft Defender for Endpoint

(CVE) with Common Vulnerability Scoring System (CVSS) scores above 8. Once the attacker is in the network, they tamper with security products or install remote monitoring and management tools (RMMs) to disable or evade detections and persist in the network.

We observed remote encryption in 70% of successful attacks, with 92% originating from unmanaged devices in the network, underscoring the need for organizations to enroll devices into management, or exclude unmanaged devices from the network.

and trends

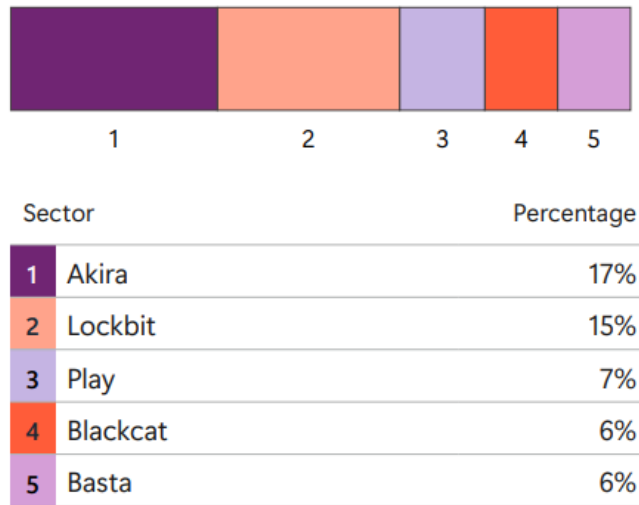
one of the most serious
And for valid reasons.

Microsoft observed a
year in human-operated
encounters (defined as having at
least one ransomware attack in

percentage of attacks reaching
the encryption stage has decreased over the past
year. Automatic attack disruption
is a positive trend in decreasing
the percentage of ransomware attacks that reach
the encryption stage. In more than 90% of cases where
the ransomware reached the encryption stage, the attacker
used unmanaged devices in the network,
either directly or to remotely encrypt
data.

ransom
encryption
two years

Top human-operated ransomware groups

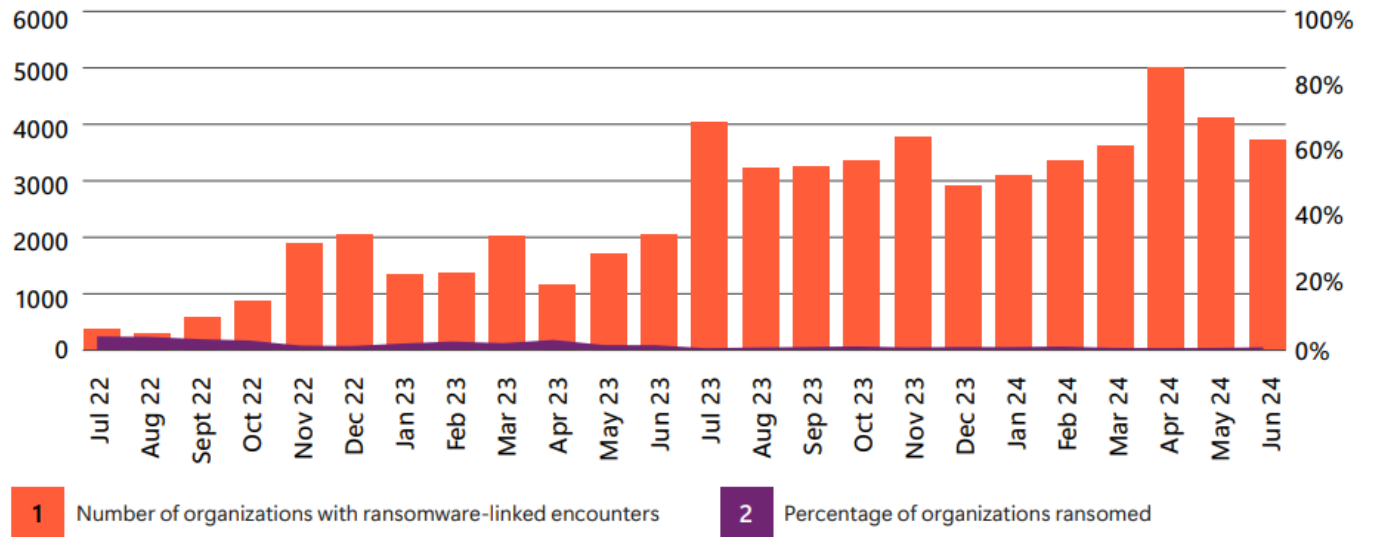


The top five ransomware families accounted for 51% of attacks. These families continue to use longstanding techniques, showing their effectiveness even against rising cybersecurity awareness globally.

Source: Microsoft Defender for Endpoint

The most prevalent initial access techniques continue to be social engineering—specifically email phishing, SMS phishing, and voice phishing—identity compromise, and exploiting vulnerabilities in public-facing applications or unpatched operating systems. Attackers continue to take advantage of newly identified common vulnerabilities and exposures

Organizations with ransom-linked encounters continues to increase while the percentage of those ransomed is decreasing (July 2022–June 2024)



Although organizations with ransom-linked encounters continues to increase, the percentage that are ultimately ransomed (reaching encryption stage) decreased more than threefold over the past two years.

Source: Microsoft Defender for Endpoint

(CVE) with Common Vulnerability Scoring System (CVSS) scores above 8. Once the attacker is in the network, they tamper with security products or install remote monitoring and management tools (RMMs) to disable or evade detections and persist in the network.

We observed remote encryption in 70% of successful attacks, with 92% originating from unmanaged devices in the network, underscoring the need for organizations to enroll devices into management, or exclude unmanaged devices from the network.

Misc Recommendations

Everything else..



Remove OEM Bloatware

OEM included applications are often not leveraged, but can themselves be a security risk.

Don't let a CVE on a background app be the thing that brings you down.

◆ Recommendations

- ◆ Order devices which are free of OEM bloatware, where possible
- ◆ Script removal of bloatware as part of your onboarding process

```
3 Created on: 13/02/2025 09:48
4 Created by: Maurice Daly
5 Organization: Patch My PC
6 Filename: Invoke-RestoreOEMBloatware.ps1
7
8 Description: Restores OEM software that was removed from the device.
9
10 #>
11
12 # region Global Variables
13 $LogDirectory = "C:\ProgramData\Microsoft\IntuneManagementExtension\Logs"
14 $PMPCRegistryKey = "HKLM:\Software\PatchMyPC-Internal"
15 # endregion Global Variables
16
17 # region Functions
18
19 27 references
20 function global:Write-LogEntry {
21     param
22     (
23         [Parameter(Mandatory = $true,
24             HelpMessage = 'Value added to the log file.')]
25         [ValidateNotNullOrEmpty()]
26         [string]$Value,
27         [Parameter(Mandatory = $true,
28             HelpMessage = 'Severity level to log the entry. Valid values are 1, 2, 3, 4, 5, 6, 7, 8, 9, 10. Default is 1.')]
29         [ValidateSet('1', '2', '3', '4', '5', '6', '7', '8', '9', '10')]
30         [string]$Severity = '1',
31         [Parameter(Mandatory = $true,
32             HelpMessage = 'Log file name to use for the log entry.')]
33         [ValidateNotNullOrEmpty()]
34         [string]$LogFileNames,
35         [switch]$UpdateUI
36     )
37
38     # Determine log file location
39     $script:LogFilePath = Join-Path $LogDirectory $LogFileNames
40
41     # Construct time stamp
42     $time = -join @(Get-Date -Format 'dd-MM-yyyy HH:mm:ss')
43
44     # Construct date for log file
45     $date = (Get-Date -Format 'dd-MM-yyyy')
46
47     # Construct context for log file
48     $context = "OEM Bloatware Removal"
49
50     # Write log entry
51     Write-LogEntry -value "$context: $Value" -severity $Severity -logfile $LogFilePath
52
53     # Update UI
54     if ($UpdateUI) {
55         Write-Host "OEM Bloatware Removal: $Value"
56     }
57 }
58
59 # Array of uninstall registry keys
60 $UninstallKeys = @(
61     "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall",
62     "HKLM:\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall"
63 )
64
65 # Switch to shorten the OEM name for publisher matching
66 Write-LogEntry -value "- Shortening OEM name for publisher matching" -Severity 1
67 switch ($OEM) {
68     "Dell Inc." { $OEM = "Dell" }
69     "Hewlett-Packard" { $OEM = "HP" }
70     "Lenovo" { $OEM = "Lenovo" }
71 }
72 Write-LogEntry -value "- Shortened OEM name: $OEM" -Severity 1
73
74 # New PSCustomObject to store the OEM uninstall locations, and software details, including the uninstall
75 $OEMBloatware = @()
76
77 # Loop through each uninstall registry key
78 foreach ($UninstallKey in $UninstallKeys) {
79     # Function to check uninstall locations in the registry for specified OEM
80     function Get-OEMUninstallLocations {
81         param
82         (
83             [Parameter(Mandatory = $true,
84                 HelpMessage = 'OEM name to search for in the registry.')]
85             [ValidateNotNullOrEmpty()]
86             [string]$OEM
87         )
88
89         # Determine log file location
90         $script:LogFilePath = Join-Path $LogDirectory $LogFileNames
91
92         # Construct time stamp
93         $time = -join @(Get-Date -Format 'dd-MM-yyyy HH:mm:ss')
94
95         # Construct date for log file
96         $date = (Get-Date -Format 'dd-MM-yyyy')
97
98         # Construct context for log file
99         $context = "OEM Bloatware Removal"
100
101         # Write log entry
102         Write-LogEntry -value "$context: Searching for OEM $OEM in registry key $UninstallKey" -severity $Severity -logfile $LogFilePath
103
104         # Search for OEM in registry
105         $OEMLocations = Get-Childitem $UninstallKey | Where-Object { $_.Name -like "*$OEM*" }
106
107         # Loop through each OEM location
108         foreach ($OEMLocation in $OEMLocations) {
109             # Determine log file location
110             $script:LogFilePath = Join-Path $LogDirectory $LogFileNames
111
112             # Construct time stamp
113             $time = -join @(Get-Date -Format 'dd-MM-yyyy HH:mm:ss')
114
115             # Construct date for log file
116             $date = (Get-Date -Format 'dd-MM-yyyy')
117
118             # Construct context for log file
119             $context = "OEM Bloatware Removal"
120
119             # Write log entry
120             Write-LogEntry -value "$context: Found OEM $OEM in registry key $UninstallKey" -severity $Severity -logfile $LogFilePath
121
122             # Add OEM location to array
123             $OEMBloatware += [PSCustomObject] @{
124                 UninstallKey = $UninstallKey
125                 OEMLocation = $OEMLocation
126                 OEM = $OEM
127             }
128         }
129     }
130
131     # Get OEM uninstall locations
132     Get-OEMUninstallLocations -OEM $OEM
133 }
134
135 # Export OEM bloatware details to CSV
136 $OEMBloatware | Export-Csv -Path $LogDirectory\OEMBloatware.csv -NoTypeInformation
```

Leveraging Compliance

Compliance policies & notification can help you create a secure environment for your organization.

This is where having separate compliance policies is a good practice.

◆ Recommendations

◆ BitLocker

Help to enforce encryption requirements through compliance policies.
Notify the end user, but add a grace period to cater to the required restart

◆ Defender

Block devices that are deemed a high risk, immediately

The screenshot displays two configuration pages from the Microsoft Intune console. The top page is for a policy named "Windows-Compliance-Encryption". It shows basic information such as the name, description, platform (Windows 10 and later), and profile type (Windows 10/11 compliance policy). The "Compliance settings" section is partially visible, showing a link to "Windows-Compliance-Defender High Risk".

The bottom page is for a policy named "Windows-Compliance-Defender High Risk". It shows basic information and the "Device Health" section, which includes "Bitlocker" and "System Security". Under "System Security", the "Require encryption of" section is expanded, showing "Trusted Platform Mod" and "Actions for noncompliance". The "Actions for noncompliance" table is as follows:

Action	Schedule	Message template	Additional recipients (via email)
Mark device noncompliant	Immediately		None selected

The "Scope tags" section shows "Default" and "Assignments" with "Edit" links.

Leveraging Platform Scripts

Leverage platform scripts to perform actions during the out-of-the-box/enrolment process, or as part of ongoing maintenance:

- ◆ **BitLocker Key Escrow**
Encrypting the hard disk = Good
Not having the recovery key = BAD
Leverage PowerShell to enforce escrow of the recovery keys, particularly useful in “mature” environments
- ◆ **Defender Updates**
Update the virus definitions to help with compliance state post-enrolment

The image displays three overlapping screenshots of the Windows Management Console (MMC) interface, showing the execution of platform scripts. Each screenshot shows the 'Overview' tab for a specific script, including a search bar, 'Delete' button, and 'Essentials' section with 'Created' and 'Last modified' timestamps. The 'Monitor' section includes 'Device status' and 'User status' options.

- Windows-PlatformScript-Backup BitLocker Keys**: Shows a 'Succeeded' status for the script execution.
- Windows-PlatformScript-RemoveLegacyLAPS**: Shows a 'Succeeded' status for the script execution.
- Windows-PlatformScript-Update Defender**: Shows a 'Device status' section with a donut chart indicating 173 successful devices and 0 errors.

Defender Security Recommendations

Microsoft Defender provides a wealth of information when devices are onboarded into MDE

◆ Leverage Recommendations

Items such as recommended registry configurations, not only for Microsoft software, but also for third parties, are provided through the security portal

◆ Leverage Remediations

Think outside of the box, and create remediations based on the recommended values which can't be set through the settings catalog. Think about Azure storage and PowerShell to achieve this

The screenshot displays the Microsoft Defender Security Recommendations interface. At the top, there are two notification boxes: "1 discovered devices are not protected" and "How well are you handling critical vulnerabilities?". Below these, a table lists various security recommendations. Two pop-up windows are overlaid on the table, providing detailed remediation instructions for specific items.

Security recommendation	OS platform	Weakness	Exposed critical devices	Related component	Threats	Exposed devices	Remediation type	Remediation action	Impact
Attention required: vulnerabilities in OpenSsl	Windows	38	3	OpenSsl	OpenSsl	137 / 138	Software update	0	21.50 0.00
Update Microsoft Windows 11 (OS and built-in applications)	Windows	1317	0	Microsoft Windows 11	Microsoft Windows 11	49 / 155	Software update	0	10.67 0.00
Update Microsoft Teams	Windows	5	1	Microsoft Teams	Microsoft Teams	64 / 128	Software update	0	6.96 0.00
Update Microsoft Edge Chromium-based to version 140.0.3485.66	Windows	508	1	Microsoft Edge Chromium-based	Microsoft Edge Chromium-based	52 / 158	Software update	0	8.94 0.00
Block process creations originating from PSExec and WMI commands	Windows	1	3	Security controls (Attack Surface Reduction)	Security controls (Attack Surface Reduction)	158 / 158	Configuration change	0	6.00 9.00
Block executable files from running unless they meet a prevalence, age, or trusted list criterion	Windows	1	3	Security controls (Attack Surface Reduction)	Security controls (Attack Surface Reduction)	158 / 158	Configuration change	0	6.00 9.00
Update Microsoft Visual Studio 2022	Windows	151	0	Microsoft Visual Studio 2022	Microsoft Visual Studio 2022	26 / 33	Software update	0	1.80 0.00
Update Google Chrome	Windows	1	0	Google Chrome	Google Chrome	1 / 1	Software update	0	5.03 0.00
Update Microsoft Office	Windows	1	0	Microsoft Office	Microsoft Office	1 / 1	Software update	0	4.63 0.00
Update Microsoft Office	Windows	1	0	Microsoft Office	Microsoft Office	1 / 1	Software update	0	1.58 0.00
Update Microsoft Office	Windows	1	0	Microsoft Office	Microsoft Office	1 / 1	Software update	0	3.39 0.00

Disable JavaScript on Adobe DC
● Remediation required
Open software page Report inaccuracy
General Remediation options Exposed devices
Set the following registry value:
`HKLM\SOFTWARE\Policies\Adobe\Adobe Acrobat\Content Advisor\Default`
To the following REG_DWORD value:
1

Enable 'Local Security Authority (LSA) protection'
● Remediation required
Open software page Report inaccuracy
General Remediation options Exposed devices
Set the following registry value:
`HKLM\SYSTEM\CurrentControlSet\Control\Lsa\RunAsPPL`
To the following REG_DWORD value:
1

Defender Security Recommendations

Microsoft Defender provides a wealth of information when devices are onboarded into MDE

◆ Leverage Recommendations

Items such as recommended registry configurations, not only for Microsoft software, but also for third parties, are provided through the security portal

◆ Leverage Remediations

Think outside of the box, and create remediations based on the recommended values which can't be set through the settings catalog. Think about Azure storage and PowerShell to achieve this

Disable JavaScript on Adobe DC
Remediation required

Open software page Report inaccuracy

General Remediation options Exposed devices

Set the following registry value:
HKLM\SOFTWARE\Policies\Adobe\Acrobat\DC\FeatureLockDown\bDisableJavaScript
To the following REG_DWORD value:
1

Enable 'Local Security Authority (LSA) protection'
Remediation required

Open software page Report inaccuracy

General Remediation options Exposed devices

Set the following registry value:
HKLM\SYSTEM\CurrentControlSet\Control\Lsa\RunAsPPL
To the following REG_DWORD value:
1

RegistryConfiguration.csv
Blob

Save Discard Download Refresh Delete

Overview Versions Snapshots Edit Generate SAS

1	RegKey, Name, Value, Type
2	HKLM:\SOFTWARE\Policies\Adobe\Acrobat Reader\DC\FeatureLockDown,bEnableFlash,0,DWORD
3	HKLM:\SOFTWARE\Policies\Adobe\Acrobat Reader\DC\FeatureLockDown,bDisableJavaScript,1,DWORD
4	HKLM:\SOFTWARE\Policies\Adobe\Acrobat\DC\FeatureLockDown,bDisableJavaScript,1,DWORD
5	HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System,MaxDevicePasswordFailedAttempts,10,DWORD
6	HKLM:\SOFTWARE\Policies\Microsoft\Windows\Network Connections,NC_AllowNetBridge_NLA,0,DWORD
7	HKLM:\SOFTWARE\Policies\Microsoft\Windows\Network Connections,NC_StdDomainUserSetLocation,1,DWORD

Windows-RemediationScript-Defender Registry Recommendations | Overview
Proactive remediations

Search Delete

Overview Manage Properties Monitor Device status

This gives information about how your script package is performing and the health of your devices. The scripts run according to your defined scheduling preferences. The detection bar chart reflects the returned value from the detection script while the remediation bar chart describes the remediation script output. [Learn more](#)

Detection status
Pending devices: 0

Without issues	With issues	Failed	Not applicable
180	8	0	0

Remediation status
Non-targeted devices: 0

Issue fixed	Recurred	Failed
15	2	11

Daily issue remediation trend
17/8/2025 - 15/9/2025

Hour fixed: 9 | Without issues: 227

Browser Extensions

What's the Risk?

- ◆ Extensions that read and modify all of your data. Read that again..
- ◆ Local host permissions
- ◆ How can we detect and control this area of shadow IT?
- ◆ Recommendations:
 - ◆ Monitor Browser Extension usage
 - ◆ Block Known Malicious Extensions
 - ◆ **Only allow approved Browser Extensions**

The image shows a collage of browser extension cards. At the top right is '1Password – Password Manager' by AgileBits Inc., with 402 reviews and 1,700,000+ users. Below it is 'Header Editor' (1.5 MB, Version 4.1.1) with permissions to read browsing history and manage downloads. To the right is 'Loom – Screen Recorder & Screen Capture' (54.6 MB, Version 5.5.121) with permissions to read and change data on all websites and capture screen content. In the center is 'Dark Reader' (Featured), with a red arrow pointing to it and a red box highlighting its permission: 'Read and change all your data on all websites'. At the bottom right is 'Graph X-Ray' by Merill, with 7 reviews and 12,000+ users. A red speech bubble graphic is in the top left corner of the slide.

Browser Extensions



Graph X-Ray

Extension | Merill

★★★★☆ (7) | 12,000+ Users | Developer tools

```
C:\Users\MauriceDaly_7wfo4ik\OneDrive - Patch My PC\Documents\SAPIEN\PowerShell Studio\Files> .\Get-BrowserExtensions.ps1
```

Browser	Profile	Name	Version	APIRisk	HostRisk	HostPermissions
Chrome	Default	1Password - Password Manager	8.10.80.23	Critical	Critical	<all>
Chrome	Default	Microsoft Single Sign On	1.0.11	Critical	Critical	https://*
Edge	Default	1Password - Password Manager	8.10.48.25	Critical	Critical	<all>
Edge	Default	iCloud Passwords	3.0.4	Critical	Critical	*://*
Edge	Default	My Apps Secure Sign-in Extension	8.2.1.196	Critical	Critical	https://*
Edge	Default	Header Editor	4.1.1	Critical	Critical	*://*
Edge	Default	Header Editor	5.2.7	Critical	Critical	*://*
Edge	Default	Loom - Screen Recorder & Screen Capture	5.5.137	Critical	Critical	*://*
Edge	Default	Graph X-Ray	1.0.3	Critical	Critical	https://*
Edge	Default	1Password - Password Manager	8.11.12.27	Critical	Critical	<all>
Edge	Profile 1	Graph X-Ray	1.0.3	Critical	Critical	https://*
Edge	Profile 1	My Apps Secure Sign-in Extension	8.2.1.196	Critical	Critical	https://*
Edge	Profile 1	1Password - Password Manager	8.11.12.27	Critical	Critical	<all>
Edge	Profile 11	My Apps Secure Sign-in Extension	8.2.1.196	Critical	Critical	https://*
Edge	Profile 11	Graph X-Ray	1.0.3	Critical	Critical	https://*
Edge	Profile 11	1Password - Password Manager	8.11.8.40	Critical	Critical	<all>
Edge	Profile 15	1Password - Password Manager	8.11.4.27	Critical	Critical	<all>
Edge	Profile 15	My Apps Secure Sign-in Extension	8.2.1.196	Critical	Critical	https://*
Edge	Profile 16	Graph X-Ray	1.0.3	Critical	Critical	https://*
Edge	Profile 16	My Apps Secure Sign-in Extension	8.2.1.196	Critical	Critical	https://*
Edge	Profile 16	1Password - Password Manager	8.11.8.40	Critical	Critical	<all>
Edge	Profile 17	1Password - Password Manager	8.11.8.40	Critical	Critical	<all>
Edge	Profile 17	My Apps Secure Sign-in Extension	8.2.1.196	Critical	Critical	https://*
Edge	Profile 17	Graph X-Ray	1.0.3	Critical	Critical	https://*
Edge	Profile 18	Graph X-Ray	1.0.3	Critical	Critical	https://*
Edge	Profile 18	My Apps Secure Sign-in Extension	8.2.1.196	Critical	Critical	https://*
Edge	Profile 18	1Password - Password Manager	8.11.12.27	Critical	Critical	<all>
Edge	Profile 2	1Password - Password Manager	8.10.60.30	Critical	Critical	<all>
Edge	Profile 2	My Apps Secure Sign-in Extension	8.2.1.196	Critical	Critical	https://*
Edge	Profile 3	Graph X-Ray	1.0.3	Critical	Critical	https://*
Edge	Profile 3	1Password - Password Manager	8.11.12.27	Critical	Critical	<all>
Edge	Profile 3	My Apps Secure Sign-in Extension	8.2.1.196	Critical	Critical	https://*
Edge	Profile 4	Graph X-Ray	1.0.3	Critical	Critical	https://*
Edge	Profile 4	My Apps Secure Sign-in Extension	8.2.1.196	Critical	Critical	https://*

```
"abcdefghijklmnop": {  
  "manifest": {  
    "name": "Graph X-Ray",  
    "permissions": [  
      "storage",  
      "tabs",  
      "webRequest",  
      "clipboardRead",  
      "clipboardWrite"  
    ],  
    "host_permissions": [  
      "https://graph.microsoft.com/*",  
      "https://*/*" ]  
  }  
}
```

SAVE THE DATES

Oct 25-28, 2026



May 2-6, 2027



Oct 10-13, 2027



Extended Q&A



2Pint

Recast

robopack
empowered by SOFTWARE
CENTRAL

SquaredUp

CODETWO

baramundi

ninjaOne

Rimo3



TeamViewer

numecent

aiden