

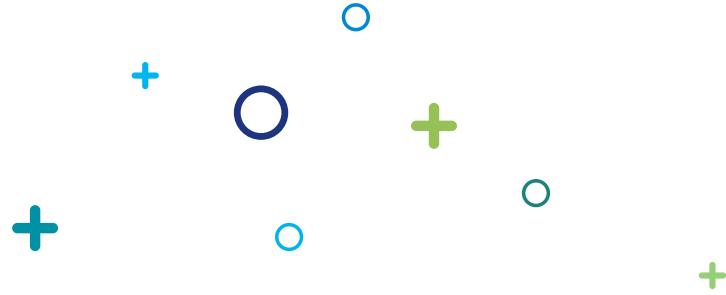


Workshop guide



Mastering Endpoint Security:

From Zero Trust to
Enterprise Access



Workshop guide

Duration: 1 hour

What you'll need:

- M365 tenant
- Global Admin
- MDE & Intune licenses
- PowerShell 7.0



Code of Conduct

- Be considerate, respectful and collaborative
- Be courteous to everyone
- Communicate openly and thoughtfully and encourage others to do the same
- Be considerate of the ideas and thoughts of other attendees, even if they differ from your own
- Be mindful of your surroundings and of your fellow attendees
- Respect the rules and policies of the venue



Workshop Agenda

1. Zero Trust with Microsoft
2. **DEMO - Zero Trust Readiness Assessment**
3. Enterprise Access Model
4. Intune Management Tool
5. **DEMO - Intune Manager**
6. Security Baselines
7. **DEMO - Importing security baselines**
8. Introduction to MDE
9. Onboarding with Intune
10. Post onboarding tasks & common mistakes
11. Validate MDE
12. Proactive hunting & incident response
13. **DEMO – Using the Unified SecOps portal**



Microsoft Solutions
Architect

 Threatscape

 SquaredUp



 TIKIT



[Linktr.ee](#)



Principal Consultant



PERFORMANTA



TIKIT



SquaredUp



Marcus
Burnap





What is Zero Trust with Microsoft?

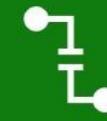
Zero Trust Principles



Verify explicitly



Use least
privileged access



Assume breach

"never trust, always verify"



Endpoints

Corporate

Personal



What is Zero Trust with Microsoft?

> 3 steps completed 12 seconds

Feb 12, 5:03 PM

Zero Trust with Microsoft is a security strategy that focuses on three core principles: verify explicitly, use least privilege access, and assume breach. This approach is designed to protect people, devices, applications, and data regardless of where they are located.

Core Principles of Zero Trust

1. **Verify explicitly:** Always authenticate and authorize based on all available data points, including user identity, location, device health, service or workload, data classification, and anomalies.
2. **Use least privilege access:** Limit user access with Just-In-Time (JIT) and Just-Enough-Access (JEA), risk-based adaptive policies, and data protection to minimize exposure.
3. **Assume breach:** Minimize blast radius and segment access. Verify end-to-end encryption and use analytics to get visibility, drive threat detection, and improve defenses.

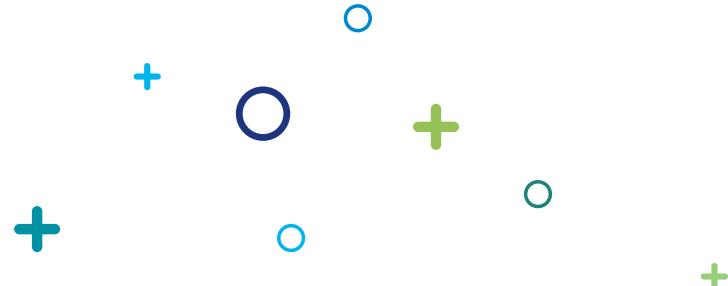
Microsoft Solutions for Zero Trust

Microsoft Intune





[Learn more](#)



Key Rules

Cloud-Enforced Security Policies

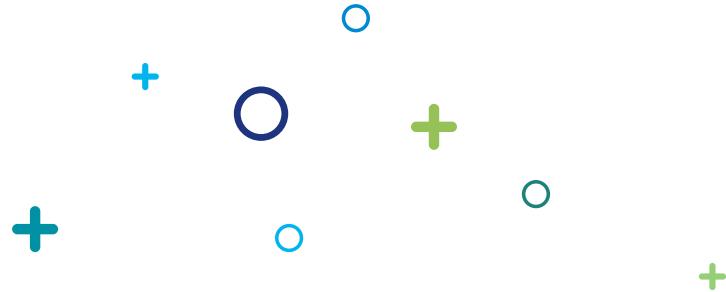
Automated Threat Response

Secure Platforms & Apps

Pre-Access Policy Enforcement



[Learn more](#)



Deployment Objectives

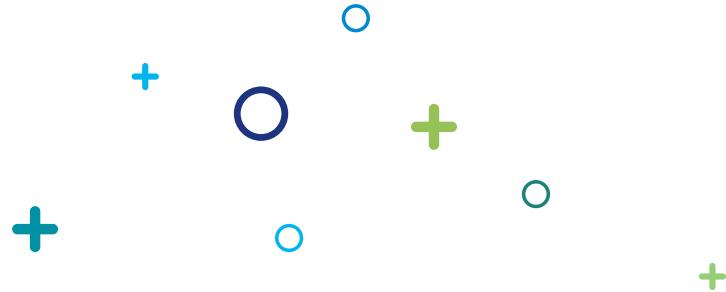
Register endpoints with cloud identity providers

Enforce access controls for cloud-managed & compliant devices

Implement Data Loss Prevention (DLP) policies



[Learn more](#)



Deployment Objectives

Register endpoints with cloud identity providers

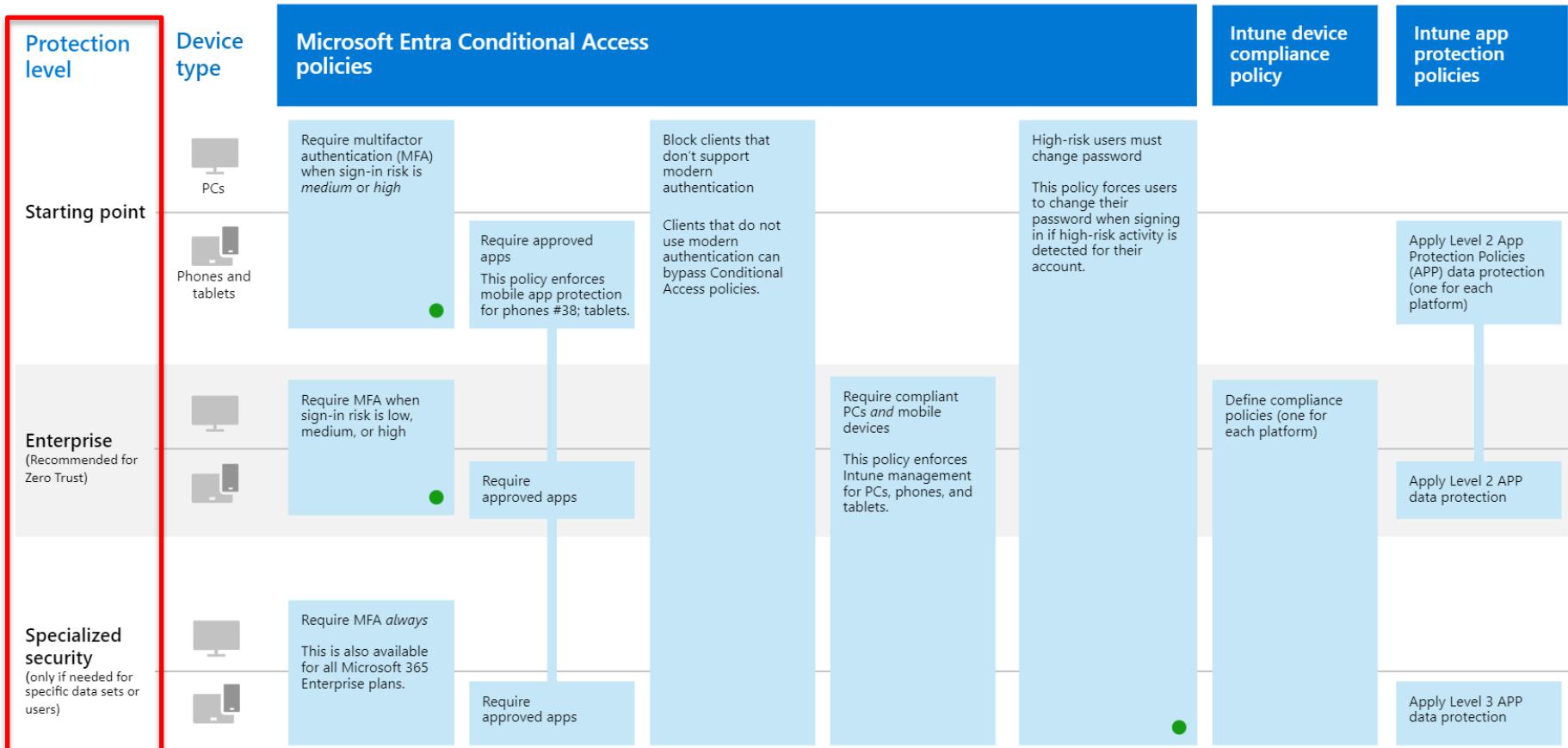
Enforce access controls for cloud-managed & compliant devices

Implement Data Loss Prevention (DLP) policies

Deploy endpoint threat detection & monitoring

Adaptive access based on endpoint risk

Zero Trust identity and device access policies



PCs include devices running the Windows or macOS platforms

Phones and tablets include devices running the iOS, iPadOS, or Android platforms

● Requires Microsoft 365 E5, Microsoft 365 E3 with the E5 Identity add-on, Microsoft 365 with EMS E5, or individual Microsoft Entra ID P2 licenses

Zero Trust identity and device access policies

Protection level

Device type

Microsoft Entra Conditional Access policies

Starting point



PCs



Phones and tablets

Require multifactor authentication (MFA) when sign-in risk is *medium or high*

Block clients that don't support modern authentication

Require approved apps
This policy enforces mobile app protection for phones #38; tablets.

Clients that do not use modern authentication can bypass Conditional Access policies.

Enterprise

(Recommended for)



Require MFA when sign-in risk is low, medium, or high

Require compliant PCs and mobile devices

This policy enforces



Starting point



Phones and tablets

Require multifactor authentication (MFA) when sign-in risk is *medium or high*

Require approved apps

This policy enforces mobile app protection for phones #38; tablets.

Block clients that don't support modern authentication

Clients that do not use modern authentication can bypass Conditional Access policies.



Enterprise

(Recommended for Zero Trust)



Require MFA when sign-in risk is low, medium, or high

Require approved apps

Require compliant PCs *and* mobile devices

This policy enforces Intune management for PCs, phones, and tablets.



Specialized security

(only if needed for specific data sets or

Require MFA *always*

This is also available for all Microsoft 365 Enterprise plans.

Enterprise

(Recommended for Zero Trust)



Require MFA when sign-in risk is low, medium, or high

Require approved apps

Require compliant PCs and mobile devices

This policy enforces Intune management for PCs, phones, and tablets.

Specialized security

(only if needed for specific data sets or users)



Require MFA *always*

This is also available for all Microsoft 365 Enterprise plans.

Require approved apps

PCs include devices running the Windows or macOS platforms

Phones and tablets include devices running the iOS, iPadOS, or Android platforms

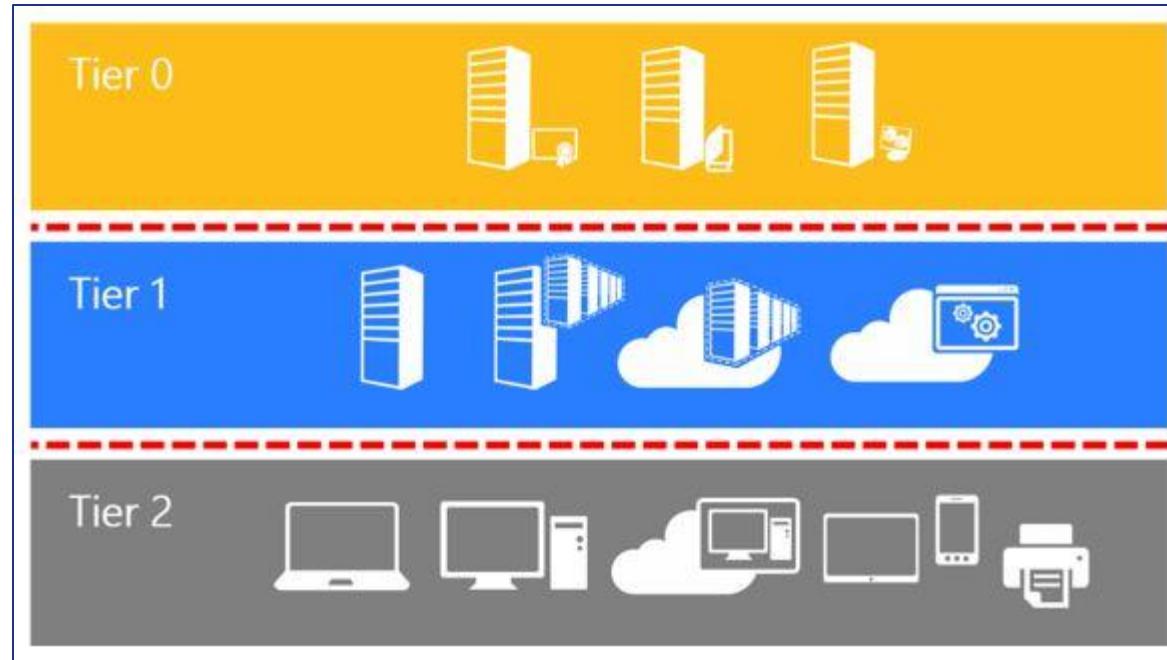
● Requires Microsoft 365 Identity add-on, Microsoft Entra ID P2 license



How can we assess
our readiness?

Demo 1: Microsoft Zero Trust Assessment Tool

AD tier model





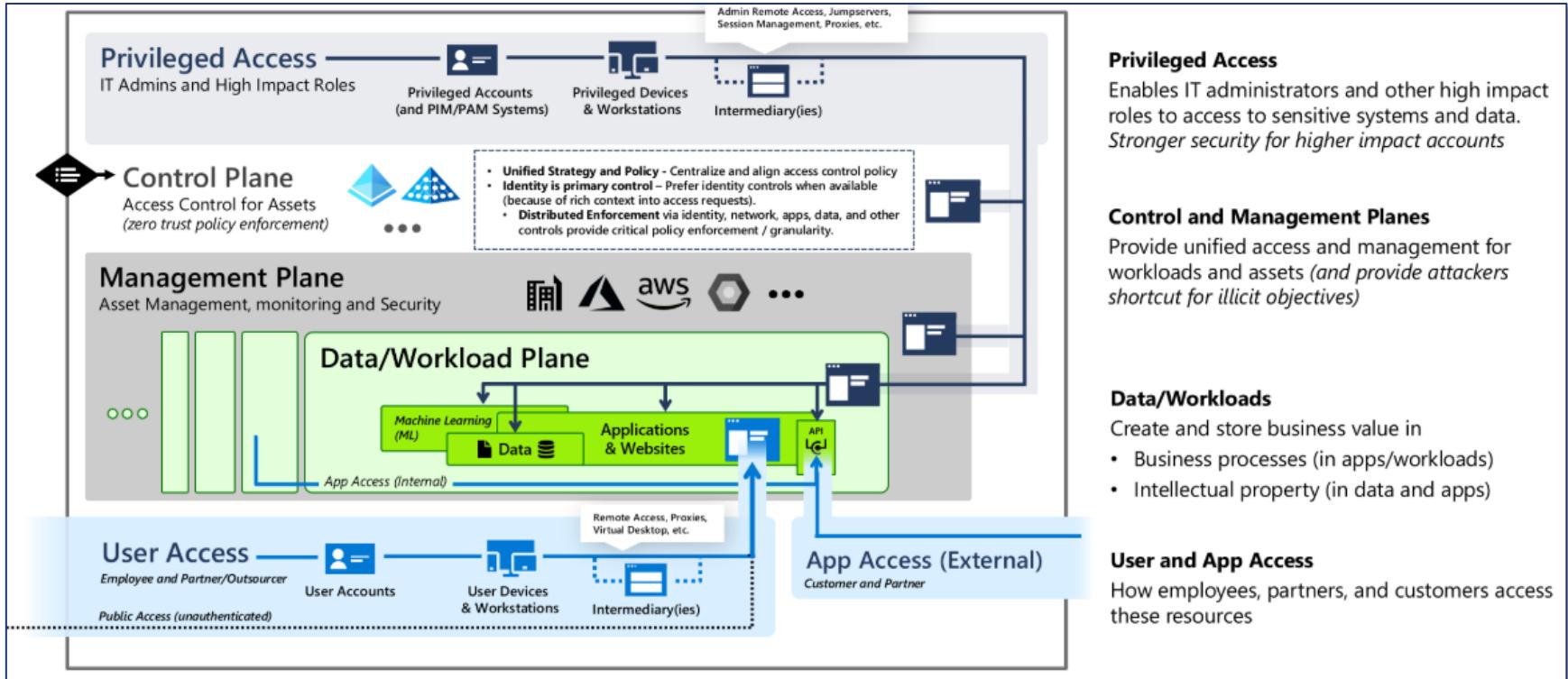
AD tier model



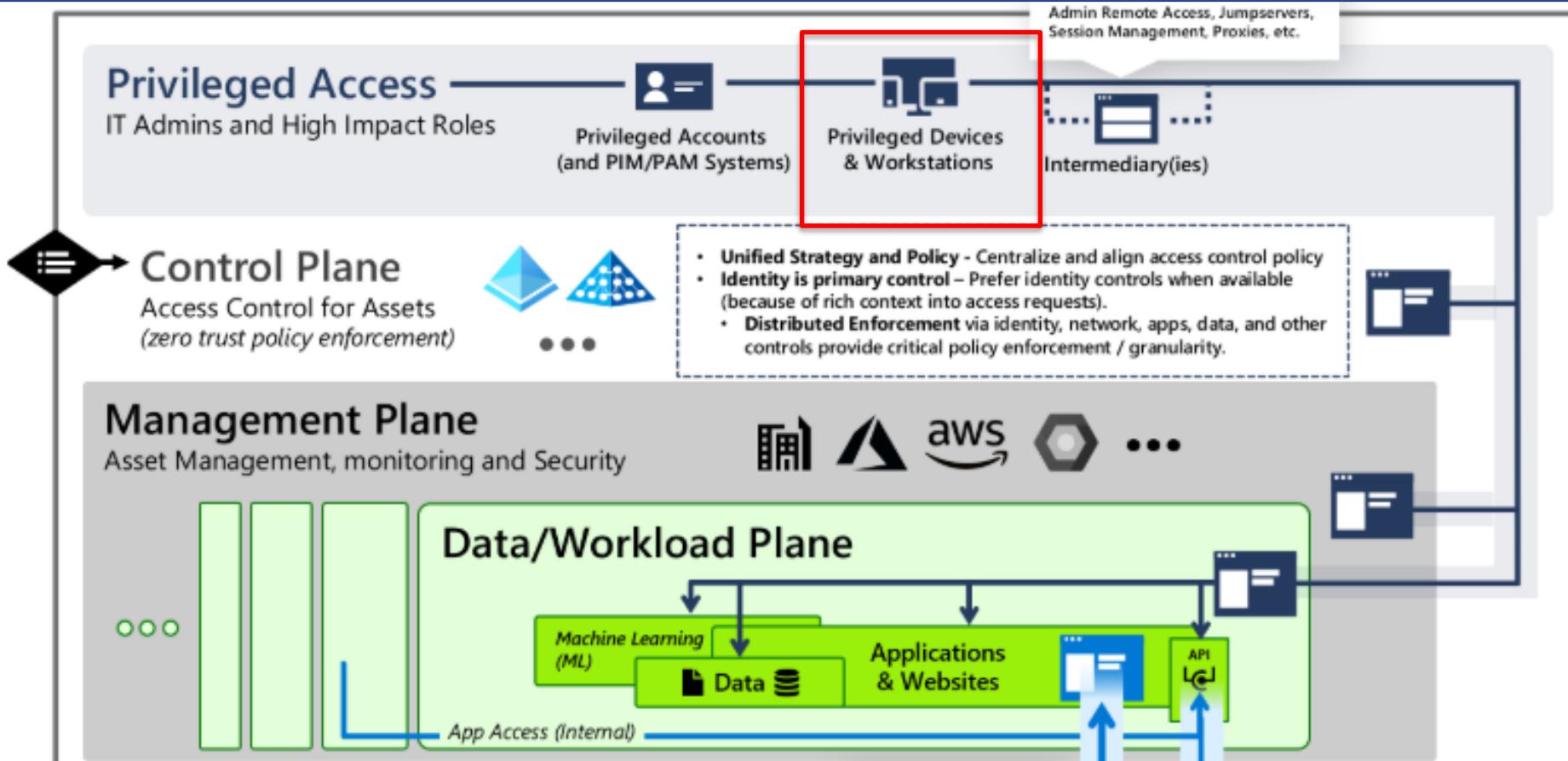
AD tier model



Enterprise Access Model

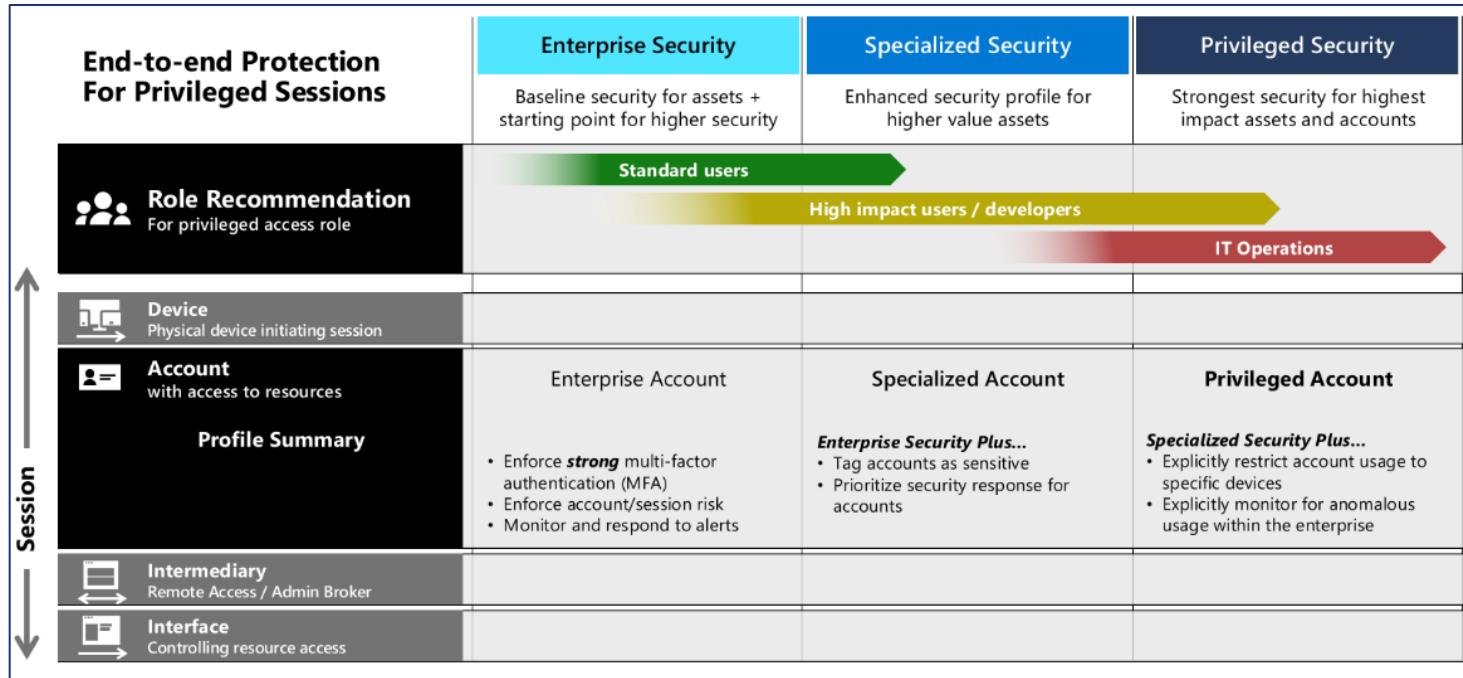


Enterprise Access Model





Securing Privileged Access



Enterprise Access Model



Securing Privileged Access

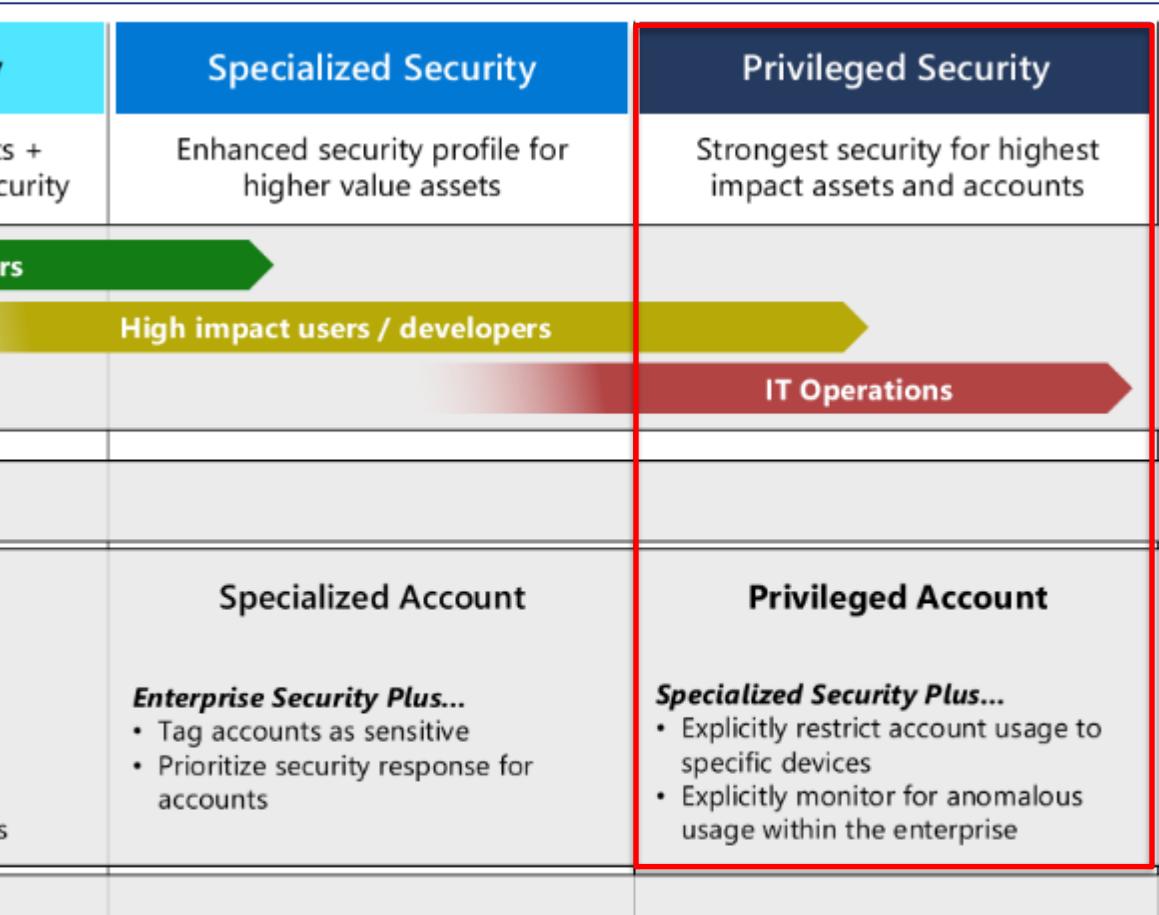
[Learn more](#)

Enterprise Security	Specialized Security	Privileged Security
Baseline security for assets + starting point for higher security	Enhanced security profile for higher value assets	Strongest security for highest impact assets and accounts
Standard users	High impact users / developers	IT Operations
Enterprise Account	Specialized Account	Privileged Account
<ul style="list-style-type: none">Enforce strong multi-factor authentication (MFA)Enforce account/session riskMonitor and respond to alerts	Enterprise Security Plus... <ul style="list-style-type: none">Tag accounts as sensitivePrioritize security response for accounts	Specialized Security Plus... <ul style="list-style-type: none">Explicitly restrict account usage to specific devicesExplicitly monitor for anomalous usage within the enterprise

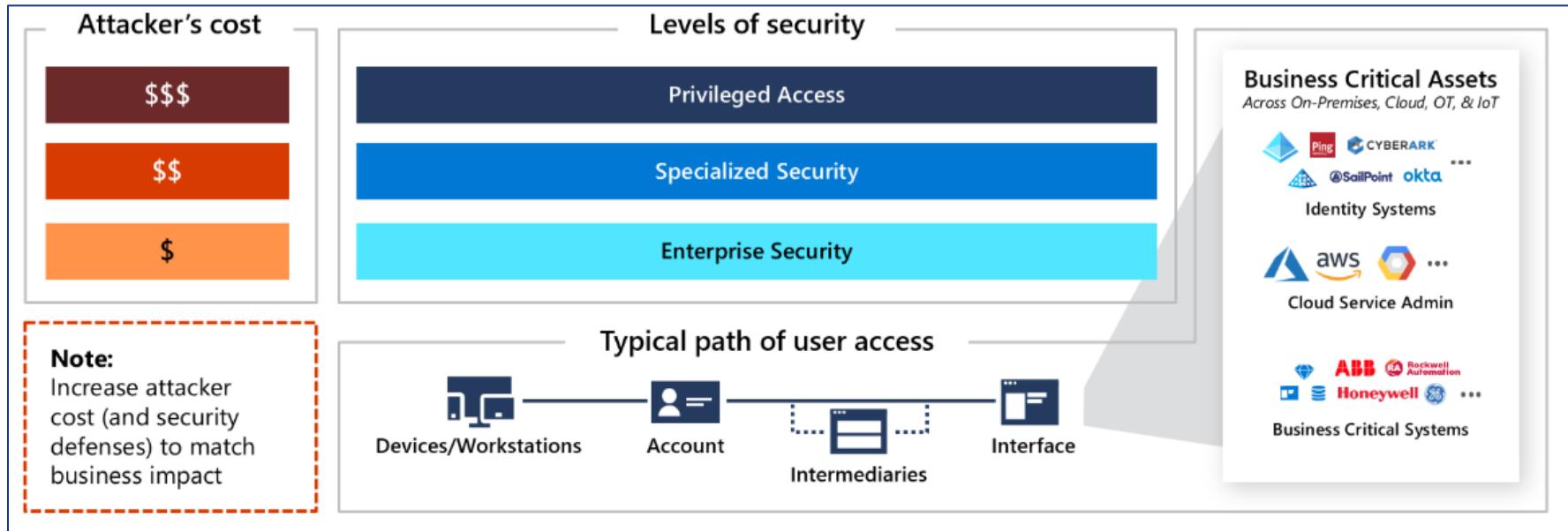


[Learn more](#)

Securing Privileged Access



Securing Privileged Access





Device compliance × Conditional Access × Tiering

Compliance	Conditional Access	Tier	Description
Custom compliance	Require compliant device Require PAW	0	Privileged
No Defender risk DHA Minimum OS version	Require compliant device	1	Specialised
Firewall Antivirus TPM BYOD support	Require compliant OR hybrid/Entra ID joined device	2	Enterprise

New

Conditional Access policy

[Learn more](#)

Name *

CA111-Admins-AllApps-AnyPlatform-Com...

Assignments

Users

[Specific users included](#)

Target resources

No target resources selected

Conditions

0 conditions selected

Access controls

Grant

[Block access](#)

Enable policy

[Report-only](#) On [Create](#)

Filter for devices

Configure a filter to apply policy to specific devices. [Learn more](#)

Configure

Yes

No

Devices matching the rule:

- Include filtered devices in policy
 Exclude filtered devices from policy

You can use the rule builder or rule syntax text box to create or edit the filter rule.

And/Or	Property	Operator	Value	
	ExtensionAttribute1	Equals	privilegedAccessWorkstation	

[Add expression](#)

Rule syntax

device.extensionAttribute1 -eq "privilegedAccessWorkstation"

Edit

[Done](#)



Key differences & when to use each approach

Feature		Zero Trust Identity & Device Policies	Privileged Access Strategy (EAM)
Scope		All users and devices	Privileged access accounts and admins
Focus		Identity security, device compliance, and app protection	Privileged admin workstations, least privilege, and just-in-time access
Primary Goal		Secure endpoint and identity access across all users	Prevent attackers from gaining control of high-value admin accounts
Three Tiers		Starting Point, Enterprise, Specialised Security	Enterprise, Specialised, Privileged
Applies to		Employees, contractors, all corporate devices	Admins, security teams, Tier 0 accounts
Key Controls		MFA, Conditional Access, device compliance, app protection	PAWs, Just-in-Time Access, least privilege enforcement



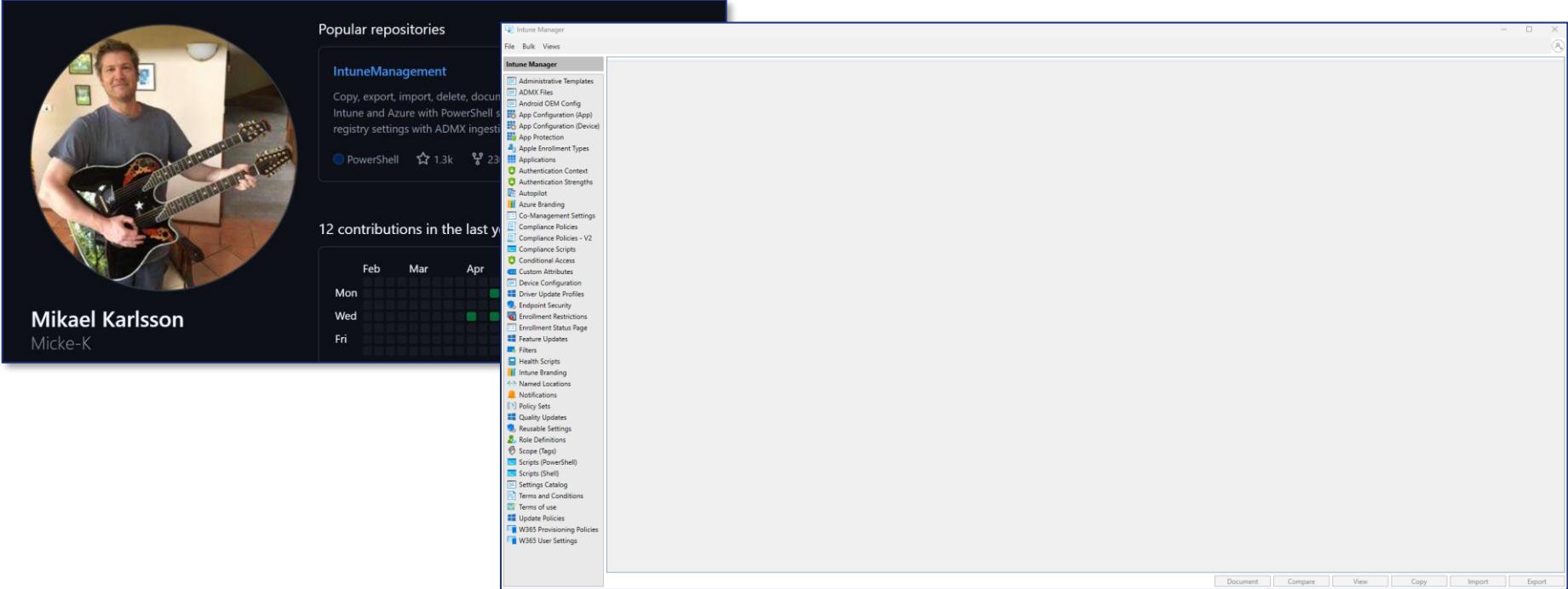
Key differences & when to use each approach

Feature		Zero Trust Identity & Device Policies	Privileged Access Strategy (EAM)
Scope		All users and devices	Privileged access accounts and admins
Focus		Identity security, device compliance, and app protection	Privileged admin workstations, least privilege, and just-in-time access
Primary Goal		Secure endpoint and identity access across all users	Prevent attackers from gaining control of high-value admin accounts
Three Tiers		Starting Point, Enterprise, Specialised Security	Enterprise, Specialised, Privileged
Applies to		Employees, contractors, all corporate devices	Admins, security teams, Tier 0 accounts
Key Controls		MFA, Conditional Access, device compliance, app protection	PAWs, Just-in-Time Access, least privilege enforcement





Intune Management Tool



Popular repositories

IntuneManagement

Copy, export, import, delete, document Intune and Azure with PowerShell scripts and registry settings with ADMX ingestions.

PowerShell 1.3k 23

12 contributions in the last year

Feb Mar Apr

Mon Wed Fri

Mikael Karlsson
Micke-K

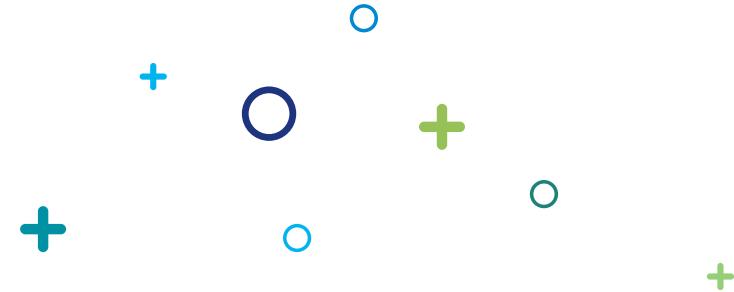
Intune Manager

- Administrative Templates
- ADMX Files
- Android OEM Config
- App Configuration (App)
- App Configuration (Device)
- App Protection
- Apple Enrollment Types
- Applications
- Authentication Context
- Authentication Strengths
- Autopilot
- Azure Branding
- Co-Management Settings
- Compliance Policies
- Compliance Policies - V2
- Compliance Scripts
- Conditional Access
- Custom Attributes
- Device Configuration
- Driver Update Profiles
- Enrollment Strategy
- Endpoint Protection
- Endpoint Restrictions
- Enrollment Status Page
- Feature Updates
- Filters
- Health Scripts
- Intune Branding
- Named Locations
- Notifications
- Policy Sets
- Quality Updates
- Reusable Settings
- Role Definitions
- Scope (Tag)
- Scripts (PowerShell)
- Scripts (Shell)
- Settings Catalog
- Terms and Conditions
- Terms of use
- Update Policies
- W355 Provisioning Policies
- W355 User Settings

Document Compare View Copy Import Export



[Learn more](#)



Intune Manager

Backup configurations

Simplify policy deployment &

Version control

replication

Document policies



Import / Export and Document policies.

Demo 2: Using Intune Manager



Security Baselines

The screenshot shows the 'Create profile' screen in the Microsoft Endpoint Manager Admin Center. The navigation bar on the left includes Home, Dashboard, All devices, Apps, Endpoint security, Reports, Users, Groups, Tenant administration, and Troubleshooting + support. The main area shows a breadcrumb path: Home > Endpoint security | Security baselines > Security Baseline for Windows 10 and later | Profiles > Create profile ... Security Baseline for Windows 10 and later. The 'Configuration settings' tab is selected. A sidebar on the left lists categories: Basics, Configuration settings, Scope tags, Assignments, and Review + create. Under Configuration settings, sections include: Administrative Templates, Auditing, Browser, Data Protection, Defender, Device Guard, Device Lock, Dma Guard, Experience, and Firewall. The Firewall section contains configuration options: Enable Domain Network Firewall (True), Enable Log Dropped Packets (Enable Logging Of Dropped Packets), Default Outbound Action (Allow), Disable Inbound Notifications (True), Log Max File Size (Configured, 16384), and Default Inbound Action for Domain (Block). The status bar at the bottom indicates the profile is 100% complete.

OpenIntuneBaseline

The screenshot shows the GitHub profile page for James Robinson [MVP]. The profile picture is a circular photo of a man smiling. The bio reads: "Community-driven baseline to accelerate Intune adoption and learning." It has 568 stars and 120 forks. The contributions chart shows activity across the last year, with most contributions occurring in September. The pinned repository is "OpenIntuneBaseline" (Public), which is described as a "Community-driven baseline to accelerate Intune adoption and learning." The GitHub URL is "https://github.com/SkipToTheEndpoint/OpenIntuneBaseline".



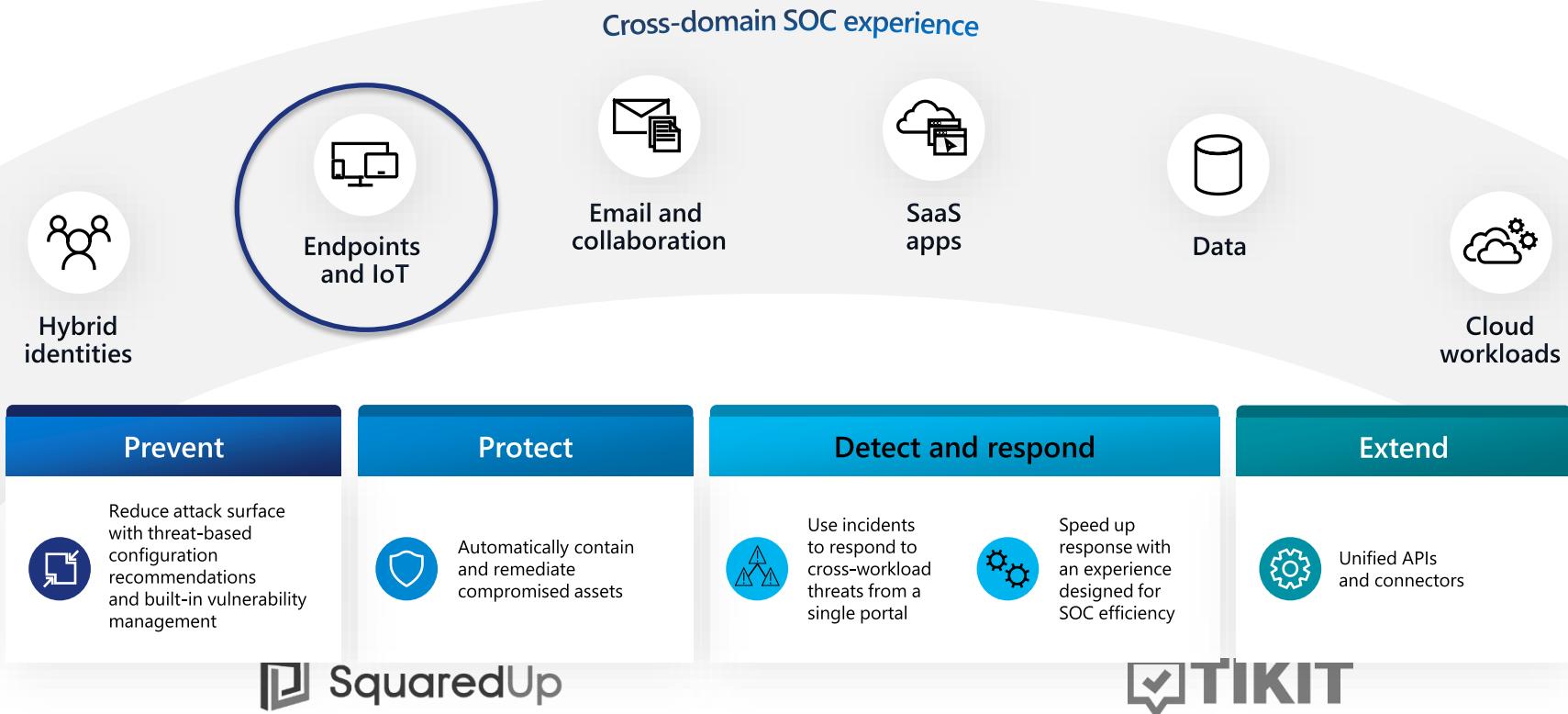
Harden those
endpoints.

Demo 3: Creating security baselines

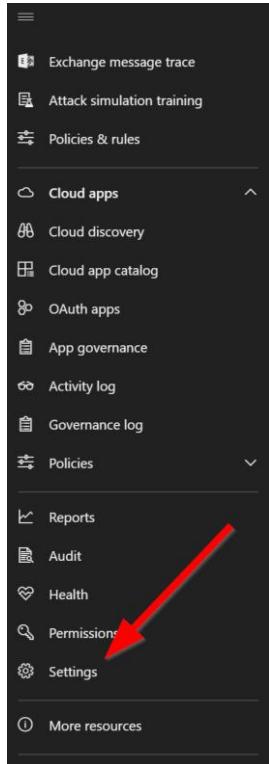


Microsoft Defender XDR

Build a unified defense with XDR



Onboarding using Intune



The screenshot shows the "General" settings page under "Advanced features".

General

Advanced features

Licenses

Email notifications

Auto remediation

Permissions

Roles

Device groups

Rules

Alert suppression

Deception rules

Indicators

Process Memory Indicators

Web content filtering

Microsoft Intune connection

FORWARDS endpoint security alerts and their triage status to MICROSOFT COMPLIANCE CENTER, ALLOWING YOU TO ENHANCE INSIDER RISK MANAGEMENT POLICIES WITH ALERTS AND REMEDIATE INTERNAL RISKS BEFORE THEY CAUSE HARM. FORWARDED DATA IS PROCESSED AND STORED IN THE SAME LOCATION AS YOUR OFFICE 365 DATA.

On

Authenticated telemetry

CONNECTS TO MICROSOFT INTUNE TO ENABLE SHARING OF DEVICE INFORMATION AND ENHANCED POLICY ENFORCEMENT.

On

Preview features

KEEP AUTHENTICATED TELEMETRY TURNED ON TO PREVENT SPOOFING TELEMETRY INTO YOUR DASHBOARD.

On

Endpoint Attack Notifications

ENABLES MICROSOFT TO ACTIVELY HUNT FOR CRITICAL THREATS TO BE PRIORITIZED BASED ON URGENCY AND IMPACT OVER YOUR ENDPOINT DATA. FOR PROACTIVE HUNTING ACROSS THE FULL SCOPE OF MICROSOFT DEFENDER XDR INCLUDING THREATS THAT SPAN EMAIL, COLLABORATION, IDENTITY, CLOUD APPLICATIONS, AS WELL AS ENDPOINTS; [LEARN MORE](#) ABOUT MICROSOFT DEFENDER EXPERTS.

Apply

Onboarding using Intune

Home > Tenant admin | Connectors and tokens > Connectors and tokens

Connectors and tokens | Microsoft Defender for Endpoint

Search Refresh Save Discard Delete

Windows

- Windows enterprise certificate
- Microsoft Endpoint Configuration Manager
- Windows 365 partner connectors
- Windows data

The Microsoft Defender for Endpoint connector is active for iOS and Android but a risk assessment is not included in a compliance policy for these platforms. To protect devices, a risk assessment must be included in a compliance policy.

Connection status: Enabled (Last synchronized: 05/02/2025, 08:53:09)

Endpoint Security Profile Settings

Allow Microsoft Defender for Endpoint to enforce Endpoint Security Configurations: On

Compliance policy evaluation

Connect Android devices version 6.0.0 and above to Microsoft Defender for Endpoint: On

Connect iOS/iPadOS devices version 13.0 and above to Microsoft Defender for Endpoint: On

Connect Windows devices version 10.0.15063 and above to Microsoft Defender for Endpoint: On

Enable App Sync (sending application inventory) for iOS/iPadOS devices: On

Send full application inventory data on personally owned iOS/iPadOS devices: On

Block unsupported OS versions: Off

Apple

- Apple VPP Tokens

Android and ChromeOS

- Managed Google Play
- Chrome Enterprise
- Firmware over-the-air update

Cross platform

- Microsoft Defender for Endpoint
- Mobile Threat Defense
- Partner device management
- Partner compliance management
- TeamViewer connector

Allow Microsoft Defender for Endpoint to enforce Endpoint Security Configurations: On

Connect Android devices version 6.0.0 and above to Microsoft Defender for Endpoint: On

Connect iOS/iPadOS devices version 13.0 and above to Microsoft Defender for Endpoint: On

Connect Windows devices version 10.0.15063 and above to Microsoft Defender for Endpoint: On

Enable App Sync (sending application inventory) for iOS/iPadOS devices: On

Send full application inventory data on personally owned iOS/iPadOS devices: On

Block unsupported OS versions: Off

Onboarding using Intune

Home > Endpoint security

Endpoint security | Endpoint detection and response

Search

Overview

- Overview
- All devices
- Security baselines
- Security tasks

Manage

- Antivirus
- Disk encryption
- Firewall
- Endpoint Privilege Management
- Endpoint detection and response**
- App Control for Business (Preview)
- Attack surface reduction

Summary EDR Onboarding Status

Defender for Endpoint Connector Status

Defender for Endpoint connector enabled

Microsoft Defender for Endpoint

Microsoft Defender for Endpoint client configuration package type

Onboarding blob from Connector

Sample Sharing

[Deprecated] Telemetry Reporting Frequency

Endpoint detection and response (EDR) policies

+ Create policy Refresh Export Columns

Policy name	Policy type	Assigned	Platform	Target
MDE Onboarding	Endpoint detection and response	Yes	Windows	MDM, MicrosoftSense

Onboarding using Intune

The screenshot shows the Microsoft Intune security dashboard for a device. At the top, it displays 'No known risks' and 'Critically: None Active'. Below this, the 'Overview' tab is selected, showing the following details:

Category	Type
Computers and Mobile	Unknown

Subtype: Workstation, Discovery sources: [Icon], Primary user: [Redacted], OS: Windows 11 64-bit (Release 22H2 Build 22621.4751), SAM name: -, Health state: Active, Data sensitivity: None, IP addresses: 10.200.150.228, MAC address: -, First seen: Jan 8, 2025 3:39:18 PM, Last seen: Feb 6, 2025 1:49:01 PM, Onboarding status: Onboarded.

On the right side, there are several sections:

- Active alerts (Last 180 days):** No active alerts or incidents.
- Security assessments:** Exposure level: High (69 active security recommendations, Discovered vulnerabilities: 265, Critical: 5, High: 127, 2 more).
- Logged on users (Last 30 days):** 2 logged on users. Most logons: [Icon], Least logons: [Icon], Newest logon: [Icon]. A note says: Get more details on users and better protect your identities and identity infrastructure by activating Microsoft Defender for identity sensors. Learn More.
- Device health status:** Full scan status is unknown. Scan history table:

Type	Date & time
Last full scan	No scan performed
Last quick scan	Completed, Feb 5, 2025 10:22:11 AM
Security intelligence	Version 1.421.1728.0, Feb 6, 2025 2:26:29 AM
Engine	Version 1.1.24090.11, Feb 6, 2025 2:26:32 AM
Platform	Version 4.18.24090.11, Jan 9, 2025 9:32:42 AM
Defender Antivirus mode	Active, Feb 6, 2025 5:34:32 PM

Post onboarding tasks / common mistakes

The screenshot shows the Microsoft Defender XDR interface. On the left, there's a sidebar with 'Device discovery' and a list of options: Discovery setup, Exclusions, Monitored networks, Enterprise IoT, and Authenticated scans. Below this is a 'Sensor health state' section with a red border, listing several devices as 'Active' except for one which is 'Inactive'. The main area is titled 'Discovery setup' and contains configuration for device discovery modes. It highlights 'Standard discovery (recommended)' with an option to 'Enable Log4j detection (CVE-2021-44228)'. A red box surrounds this section. Below it, under 'Select which devices to use for Standard discovery', the 'All devices (recommended)' option is selected. Another red box surrounds this section. To the right, five configuration items are listed:

Setting	Status
Cloud Block Level	High
Cloud Extended Timeout	50
Submit Samples Consent	Send all samples automatically.
Enable Network Protection	Enabled (block mode)
PUA Protection	PUA Protection on. Detected items are blocked. They will show in history along with other threats.

Post onboarding tasks / common mistakes

Advanced hunting

New query | Clear text passwords in the registry | Endpoint Status Report | +

Schema Functions Queries ... Run query Last 7 days Save Share link Create detection rule

Search

Favorites

Your favorites list is empty. To add an item, click the menu next to it and select "Add to Favorites"

Shared queries

Suggested

Microsoft 365 Defender

Clear text passwords in the registry

Downloads

Electron vulnerability exploitation

Endpoint Status Report

Files with double extensions

Hidden PowerShell window

MSI installation from the web

PowerShell downloads

Registry autostart

Regsvr32.exe remote scriptlets

Startup folder additions

Windows 7 RDP vulnerability (mitigated)

Windows 7 RDP vulnerability (unmitigated)

Zero-day attack reported by Korean CERT

Query

```
// Best practice endpoint configurations for Microsoft Defender for Endpoint deployment.
DeviceVmSecureConfigurationAssessment
| where ConfigurationId in ("scid-91", "scid-2000", "scid-2001", "scid-2002", "scid-2003", "scid-2010", "scid-2011", "scid-2012", "scid-2013", "scid-2014", "scid-2015", "scid-2016", "scid-2017", "scid-2018", "scid-2019", "scid-2020", "scid-2021", "scid-2022", "scid-2023", "scid-2024")
| summarize arg_max(Timestamp, IsCompliant, IsApplicable) by DeviceId, ConfigurationId
| extend Test = case(
    ConfigurationId == "scid-2000", "SensorEnabled",
    ConfigurationId == "scid-2001", "SensorDataCollection",
    ConfigurationId == "scid-2002", "ImpairedCommunications",
    ConfigurationId == "scid-2003", "TamperProtection",
    ConfigurationId == "scid-2010", "AntivirusEnabled",
    ConfigurationId == "scid-2018", "CloudProtection"
)
```

Getting started Results Query history

Export Show empty columns 1827 items Search 00:01.769 Chart type Full screen

Filters: Add filter

DeviceId	AntivirusEnabled	AntivirusReporting	AntivirusSignatureVersion	BehaviorMonitoring	CloudProtection	ImpairedCommunication
1 > 1	GOOD	N/A	GOOD	GOOD	BAD	GOOD
1 > 1	GOOD	GOOD	GOOD	GOOD	GOOD	GOOD
1 > 1	GOOD	N/A	GOOD	GOOD	BAD	GOOD
1 > 1	GOOD	N/A	GOOD	GOOD	BAD	GOOD
1 > 1	GOOD	GOOD	GOOD	GOOD	GOOD	GOOD
1 > 1	GOOD	GOOD	GOOD	GOOD	GOOD	GOOD
1 > 1	GOOD	GOOD	GOOD	GOOD	GOOD	GOOD
1 > 1	GOOD	GOOD	GOOD	GOOD	GOOD	GOOD
1 > 1	GOOD	GOOD	GOOD	GOOD	GOOD	GOOD
1 > 1	GOOD	N/A	GOOD	GOOD	BAD	GOOD
1 > 1	GOOD	GOOD	GOOD	GOOD	GOOD	GOOD

Three red arrows point to the 'CloudProtection' column in the last three rows of the table, highlighting potential issues.

Post onboarding tasks / common mistakes

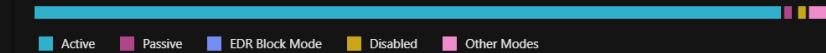
<input type="checkbox"/> Enable Microsoft Defender Antivirus email scanning	Windows	1	Security controls (Antivirus)
<input type="checkbox"/> Block Win32 API calls from Office macros	Windows	1	Security controls (Attack Surface Reduction)
<input type="checkbox"/> Block Office applications from creating executable content	Windows	1	Security controls (Attack Surface Reduction)
<input type="checkbox"/> Set controlled folder access to enabled or audit mode	Windows	1	Security controls (Exploit Guard)
<input type="checkbox"/> Secure Microsoft Defender Firewall domain profile	Windows	1	Security controls (Firewall)
<input type="checkbox"/> Turn on PUA protection in block mode	Windows	1	Security controls (Antivirus)
<input type="checkbox"/> Encrypt all BitLocker-supported drives	Windows	1	Security controls (Bitlocker)
<input type="checkbox"/> Disable merging of local Microsoft Defender Firewall connection rules with group policy firewall rules for the P...	Windows	1	Security controls (Firewall)
<input type="checkbox"/> Onboard devices to Microsoft Defender for Endpoint	Other	1	Security controls (Onboard Devices)

Device Health

Sensor health & OS Microsoft Defender Antivirus health

Antivirus mode

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



Post onboarding tasks / common mistakes

The screenshot shows the Microsoft Defender for Endpoint settings page. It includes sections for EDR features like 'Enable EDR in block mode' and 'Automatically resolve alerts', and a 'Tamper protection' section. A red box highlights the 'Enable EDR in block mode' toggle switch. Another red box highlights the 'Tamper protection' toggle switch. To the right, there's a 'Streamlined Connectivity Readiness' section with a note about EDR Sense and a table titled 'AV Component Details' showing various software versions.

System-wide WinHTTP proxy	Direct access (no proxy server).
AV Component Details	
Defender AV Platform Version	4.18.24050.7
Defender AV Security Intelligence Version	1.413.409.0
Defender AV engine Version	1.1.24050.5
Defender Is Tamper Protected	False
Defender Tamper Protection Source	Signatures
Defender Is Tamper Protection Exclusions Enabled	False



Post onboarding tasks / common mistakes

CP004.00 - GBL - PRD - Win - Device Security - Audit and Event Logging (Devices-All)
Device configuration profile

[Delete](#)

Configuration settings [Edit](#)

Administrative Templates

Auditing

Account Logon Audit Credential Validation Success+ Failure

Account Logon Logoff Audit Account Lockout Failure

Account Logon Logoff Audit Group Membership Success

Account Logon Logoff Audit Logoff Success+ Failure

Account Logon Logoff Audit Logon Success+ Failure

Account Management Audit Application Group Management Success+ Failure

Edit profile - CP008.00 - GBL - PRD - Win - MDAV - Additional Configuration (Devices-All)
Settings catalog

[Configuration settings](#) [Review + save](#)

+ Add settings

Defender [Remove category](#)

117 of 125 settings in this category are not configured

Quick Scan Include Exclusions If you set this setting to 0 or do not configure it, exclusions ar...

Enable File Hash Computation Enable

Hide Exclusions From Local Admins If you enable this setting, local admins will no longer be able to ...

Hide Exclusions From Local Users If you enable this setting, local users will no longer be able to ...

Intel TDT Enabled If you configure this setting to enabled, Intel TDT integration ...

Oobe Enable Rtp And Sig Update If you enable this setting, real-time protection and Security In...

Performance Mode Status Performance mode is disabled. A service restart is required af...

Support Log Location %ProgramData%\Microsoft\IntuneManagementExtension\Logs

Post onboarding tasks / common mistakes



On

Live Response

Allows users with appropriate RBAC permissions to investigate devices that they are authorized to access, using a remote shell connection.



On

Live Response for Servers

Allows users with Live Response privileges to connect remotely to servers (Windows Server or Linux devices) that they are authorized to access.



On

Live Response unsigned script execution

Enables using unsigned PowerShell scripts in Live Res

Disable Local Admin Merge ⓘ

Disable Local Admin Merge

AV011.00 - GBL - DEV - Win - Antivirus - MDAV Update - Ring 1 - Pilot (Devices-WinClients)

Defender Update controls

AV012.00 - GBL - DEV - Win - Antivirus - MDAV Update - Ring 2 - UAT (Devices-WinClients)

Defender Update controls

AV013.00 - GBL - DEV - Win - Antivirus - MDAV Update - Ring 3 - Production (Devices-WinClients)

Defender Update controls



Tell me about common mistakes when configuring MDE

> 3 steps completed 9 seconds

Feb 13, 11:31 AM

Common mistakes when configuring Microsoft Defender for Endpoint (MDE) include:

- 1. Insufficient Time for Data Collection:** Not allowing enough time for traffic information to be collected after enabling MDE integration. It can take up to two hours for data to show up in Microsoft Defender for Cloud Apps [4].
- 2. Endpoint Devices Behind a Forward Proxy:** Traffic from endpoint devices behind a forward proxy is not visible to MDE and isn't included in Cloud Discovery reports [4].
- 3. Incorrect Permissions and Requirements:** Not setting up the correct permissions and requirements, such as ensuring the administrative user account has the necessary security roles [3].
- 4. Not Following Deployment Guides:** Skipping steps in the deployment guides, which provide detailed instructions on attack surface reduction, next-generation protection, configuration score, and more [2].

These are some of the common pitfalls to avoid when configuring MDE to ensure optimal security and functionality.

Validate configurations

EDR test: Clean Windows Event logs

Run the following commands for checking the EDR reporting capabilities for malicious activities (cleaning Windows event logs)

```
wevtutil cl system  
wevtutil cl application  
wevtutil cl security
```

EDR test: create a scheduled task

For testing MITRE T1053 create a scheduled task. When correctly configured Defender for Endpoint alerts for a masqueraded task or service.

Run the following command:

```
schtasks /Create /F /SC MINUTE /MO 3 /ST 07:00 /TN CMDTestTask /TR "cmd /c date /T > C:\Windows\Temp\current_date.txt"
```

AV test: Dump LSASS.exe memory using comsvcs.dll

Run the following PowerShell command line for dumping LSASS.exe memory using comsvcs.dll. In all situations, the lsassdump hack tool must be prevented from running and dumping the secrets.

```
C:\Windows\System32\rundll32.exe C:\windows\System32\comsvcs.dll, MiniDump (Get-Process lsass).id $env:TEMP\lsass-comsvcs.dmp full
```

Microsoft Defender ATP Home Resources Feedback Sign In

Microsoft Defender ATP

The following demo scenarios will help you learn about the capabilities of Microsoft Defender Advanced Threat Protection (ATP). None of the sample files are actually malicious, they are all harmless demonstration files. We encourage you to read the [Microsoft Defender Antivirus documentation](#), and download the [Evaluation guide](#).

VDI testing guide

Download this guide to test new virtual desktop infrastructure security intelligence update features. This requires VMs and a host running Windows 10 Insider Preview build 18323 or later.

Cloud-delivered protection

You can confirm that cloud-delivered protection is working properly on your computer.

Block At First Sight (BAFS) [Sign in required](#)

With the BAFS feature in Microsoft Defender Antivirus, newly discovered files will be analyzed and blocked shortly thereafter on any computer.

Potentially Unwanted Applications (PUA)

You can confirm that Potentially Unwanted Applications (PUA) are being blocked on your network by downloading a fake PUA file.

Attack Surface Reduction

Reduce your attack surfaces by minimizing the places where your organization is vulnerable to cyberthreats and attacks. For more information please refer to the [attack surface reduction documentation](#), and download the [Evaluation guides](#).

Attack Surface Reduction (ASR) [Sign in required](#)

Controlled Folder Access (CFA) [Sign in required](#)

Network Protection (NP)

Home - Microsoft Defender Testground

Validate configurations

The screenshot shows a GitHub repository named 'MDEtester' with 40 commits over the last year. The repository contains files like 'Tools', 'LICENSE', 'README.md', and 'README'. Below the repository view, there is a detailed description of the 'MDE Tester' feature, its purpose, and a table comparing two PowerShell scripts: 'MDEtesterTP.ps1' and 'MDEtesterWP.ps1' based on the testing features they provide.

PS script	Testing features
MDEtesterTP.ps1	1. Microsoft Defender for Endpoint, Tamper Protection
MDEtesterWP.ps1	1. Microsoft Defender SmartScreen 2. Microsoft Defender Exploit Guard, Network Protection 3. Microsoft Defender for Endpoint, URL Indicators 4. Microsoft Defender for Endpoint, Web Content Filtering

MDEtesterTP.ps1

Prerequisites

- `MDEtesterTP.ps1` helps confirm the status of Microsoft Defender for Endpoint, Tamper Protection. However, to test AV tampering in `MDEtesterTP.ps1`, enabling Tamper Protection is required.
- Run `MDEtesterTP.ps1` script as Administrator.

LearningKijo/MDEtester: MDE Tester is designed to help testing various features in Microsoft Defender for Endpoint.

Validate configurations

ThomasVrhydn/MDE-troubleshooter: This tool is designed to assist you in analyzing issues related to Defender for Endpoint on your local endpoint. It offers a centralized view of the security configuration, log files, updates, and provides access to the Performance Analyzer.

MDE-troubleshooter

INFO

This tool is designed to assist you in analyzing issues related to Defender for Endpoint on your local endpoint. It offers a centralized view of the security configuration, log files, updates, and provides access to the Performance Analyzer.

Please note that this is the initial version of the tool. If you encounter any bugs or have suggestions for enhancements, I encourage you to submit them on my GitHub page. Your feedback and reports are greatly appreciated.

Defender AV:

- AMEngineVersion: 1.1.24090.11
- AMEngineLastVersion: 4.18.24090.11
- AMMinimized: Normal
- AMServiceVersion: 4.18.24090.11
- SignatureVersion: 1.421.1374.0
- TamperSource: Intune
- TamperStatus: True
- Signature Last Update: 1/15/2025 8:52 AM
- SignatureFallBackOrder: 2

CloudBlockLevel: High
BlockAtFirst: False
CloudTimeout: 50
CloudTimeout: 90

EnableFileHashCom: Disabled

Show ASR rules

Performance

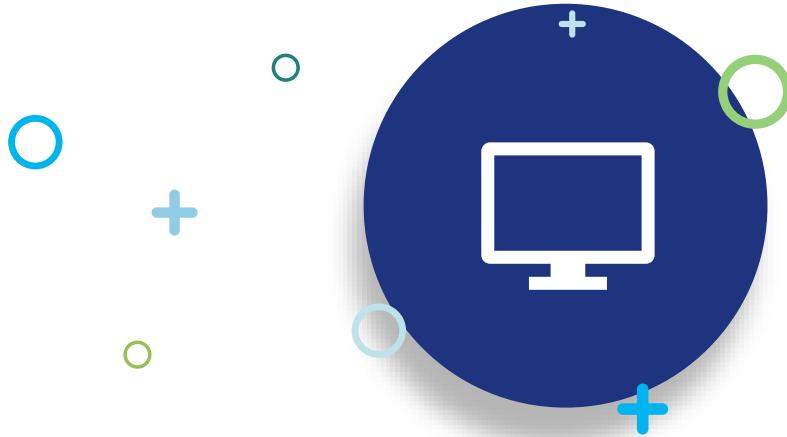
- Run Performance Analyze
- ShowPerformanceReport
- Top 10 Files
- Top 10 Extensions
- Top 10 Processes
- Top 10 Scans

Show Microsoft Protection Log
Download ClientAnalyzer

MS Instant Engine: 4.18.24090.11
MS Instant Platform: 1.1.24090.11
MS Instant Signature: 1.421.1375.0

Check for latest updates
Update intel updates

Show Sense logs
Show Defender AV logs
Show Exclusions



Time to hunt.

Demo 4: Using the Unified SecOps portal



Customizable, cloud-native SIEM
monitoring a breadth of data

Microsoft Sentinel

Analyst experience

- › Investigation
- › Prioritized incident queue
- › Hunting
- › SOAR
- › Detections
- › MITRE dashboards
- › Search
- › Solution packages

Enterprise readiness

- › Scale, multi-tenancy, resiliency, RBAC

Security analytics

- › Correlation and normalization
- › Customizable automation
- › UEBA
- › Threat intelligence platform
- › SOC optimization



300+ third-party solutions



Data

- › Connectors
- › Data storage
- › Industry standards
- › .CEF, Syslog

XDR with out of the box protection
across workloads

Microsoft Defender XDR

Analyst experience

- › Investigation
- › Prioritized incident queue
- › Hunting across workloads
- › Automated detection and response
- › Attack disruption
- › Posture management
- › Correlated incidents

Enterprise readiness

- › Scale, multi-tenancy, resiliency, RBAC

Security analytics

- › Correlation and normalization
- › Entity profiles
- › Microsoft Threat Intelligence and analytics



Data

Modern workplace

- › Hybrid identities, endpoints, IoT, email, collaboration tools, SaaS apps, and documents

Cloud workloads

- › Multicloud alerts, signals, and asset information for Microsoft Azure, Amazon Web Services, and Google Cloud Platform

Proactive hunting and incident response

Learning KQL

SecurityEvent

```
| where EventID == 4625  
| project TimeGenerated, AccountName  
| order by TimeGenerated desc
```

<https://mcloudteck.substack.com/p/learning-basic-kql-for-the-sc-200>

Marcus Burnap - Microsoft Security - Sentinel - Defender XDR

Learning basic KQL for the SC-200

Learning KQL for SC-200: Deep Dive into Core Principles

MARCUS BURNAP JAN 08, 2025

4 2 1 Share

Recently, someone preparing for the SC-200 exam came to me and said, “KQL is my weakest skill—how can I improve it?” As someone that has already been there (And myself no master of KQL) I understood their challenge. KQL can seem overwhelming at first, (From a non coding or click-ops background) but the truth is, you don’t need to master every operator or function to get thru the exam—or in real-world scenarios.

The secret to mastering KQL lies in focusing on the foundational 20% of concepts that enable you to solve 80% of practical problems. These core principles, when applied effectively, can help you analyse failed logins, identify suspicious activities, and correlate alerts with sign-ins—all essential tasks for both the SC-200 and using MS security tooling in the future!

This guide is my response to that question. It’s designed to help those preparing for the SC-200 focus on the initial most impactful parts of KQL, providing the skills and confidence to not only pass the exam but also apply KQL effectively in real-world scenarios.



Proactive hunting and incident response

The screenshot shows the KQL Search interface with a dark theme. At the top, it displays "KQL Search" and "Search engine for KQL Queries". Below this are three buttons: "Assistant" (blue), "Generator" (green), and "Lab" (red). A section titled "Our Sponsors" features logos for "glueckkanja", "Manajing", and "Master KQL at blu raven Academy". A search bar contains the placeholder "Search... (e.g. User Risk, Password Change, MITRE, Device Compliance)". Below the search bar are buttons for "Show Advanced Filters", "Newsletter", "Popular Queries", "Statistics", "Submit query", and "Device Query". Two cards are displayed below the filters:

- LLM Hunting In A MDE Environment**
Author: Steven Lim
Released: February 11st, 2025
- Using Graph Pre Consent Explorer Data For Microsoft Graph Threat Hunting**
MicrosoftGraphActivityLogs GraphPreConsent
Author: Steven Lim
Released: February 10th, 2025

At the bottom, there are links for "Documentation", "Download Client", "Data Sources", "Material Examples", "Privacy", "Imprint", "Made by SquaredUp with ❤️ and ❤️", "Stats", "KQL Community", "FAQ", and a "Logout" button.

Proactive hunting and incident response

Multi-stage incident involving Execution & Discovery on one endpoint

High | Active | Unassigned |

Attack story Alerts (14) Assets (2) Investigations (0) Evidence and Response (15) Summary

Play attack story Unpin all Show all

Incident graph Layout Group similar nodes

Jan 5, 2025 12:02 AM New Suspicious mshta process launched

Jan 5, 2025 12:02 AM New Suspicious PowerShell download or encoded command execution

Jan 5, 2025 12:02 AM New Suspicious process executed PowerShell command

Jan 5, 2025 12:02 AM New Suspicious PowerShell command line

Jan 5, 2025 12:02 AM New Suspicious process executed PowerShell command

Jan 5, 2025 12:04 AM New Possible theft of passwords and other sensitive web browser information

Jan 5, 2025 12:04 AM New Suspicious discovery indicative of Virtualization/Sandbox Evasion

Jan 5, 2025 12:04 AM New

2 UrIs

Login Data

5 Processes

RELATED THREATS

Technique Profile: Malicious use of PowerShell
11 impacted assets

View threat analytics report

Tool Profile: Information stealers
8 impacted assets

View threat analytics report

Incident details

Assigned to Unassigned Incident ID 2342

Classification Not set Categories Execution, Defense evasion, Credential access, Discovery

First activity Jan 5, 2025 12:02:13 AM Last activity Jan 5, 2025 12:12:01 AM

Impacted assets

Devices (1) Risk Level Exposure Level

Manage incident Activity log ...

Open device page View in map Device value ...

Resource ID

Resource group

Device management

Managed by Intune MDE Enrollment N/A

Set criticality Manage tags Report device inaccuracy Run Antivirus Scan Collect Investigation Package Restrict App Execution Initiate Automated Investigation Initiate Live Response Session Isolate Device Ask Defender Experts Action center Download force release from isolation script Go hunt Turn on troubleshooting mode

Alert name Severity Status Last activity

Possible theft of... High New Jan 5, 2025 12:12:01 AM

Possible theft of... Medium New Jan 5, 2025 12:05:01 AM

Possible theft of... Medium New Jan 5, 2025 12:05:01 AM

A process was in... Medium New Jan 5, 2025 12:12:01 AM



- Home
- Exposure management
- Investigation & response
- Incidents & alerts
- Hunting
 - Advanced hunting 1
 - Custom detection rules
- Actions & submissions
- Partner catalog
- Threat intelligence
- Assets
- Microsoft Sentinel
- Identities
- Endpoints
- Email & collaboration
- Cloud apps
- Cases
- SOC optimization

Advanced hunting

[Copilot](#) [Help resources](#) [Query resources report](#) [Schema reference](#)[Demo*](#) [+](#)[Schema](#)[Functions](#)[Queries](#) 2

...

[Search](#)

Favorites

Your favorites list is empty. To add an item, click the menu next to it and select "Add to Favorites"

Shared queries

[Microsoft Sentinel](#)[Hunt Queries](#)[Demo](#)[Hunting Queries](#)[Performance](#)[Suggested](#)[Remote Code Execution alert](#)

My queries

Save a query in this folder so you can quickly access it later.

Community queries 3

[ASR rules](#)[Campaigns](#)[Run query](#)[Last 24 hours](#)[Save](#)[Share link](#)[Manage rules](#)

Query

[DeviceEvents](#) 4[Getting started](#)[Results](#)[Query history](#)[Export](#)[Show empty columns](#)

63 items

[Search](#)00:02.665 Low[Chart type](#) [Full screen](#)[Filters:](#) [Add filter](#)

	TimeGenerated	Timestamp	DeviceId	DeviceName	ActionType	SHA256	InitiatingPr
<input type="checkbox"/>	> 13 Feb 2025 10:39:... 13 Feb 2025 10:39:02	140b2e6761ac9b575...	dev-opencti.ge3bo4o...	ScriptContent	44bf9ddda4a4102596...	14923	
<input type="checkbox"/>	> 13 Feb 2025 10:39:... 13 Feb 2025 10:39:02	140b2e6761ac9b575...	dev-opencti.ge3bo4o...	ScriptContent	2b86e05f7eb7bb3b6b...	14923	
<input type="checkbox"/>	> 13 Feb 2025 10:39:... 13 Feb 2025 10:39:02	140b2e6761ac9b575...	dev-opencti.ge3bo4o...	ScriptContent	c851f20baca9f6d4580...	14923	
<input type="checkbox"/>	> 13 Feb 2025 10:39:... 13 Feb 2025 10:39:02	140b2e6761ac9b575...	dev-opencti.ge3bo4o...	ScriptContent	87e3508917c33cc116...	14923	
<input type="checkbox"/>	> 13 Feb 2025 10:40:... 13 Feb 2025 10:40:41	140b2e6761ac9b575...	dev-opencti.ge3bo4o...	ScriptContent	67a34f1ba05278d50...	25695	
<input type="checkbox"/>	> 13 Feb 2025 10:40:... 13 Feb 2025 10:40:58	140b2e6761ac9b575...	dev-opencti.ge3bo4o...	ScriptContent	484b6a9de8b41aa93...	27188	
<input type="checkbox"/>	> 13 Feb 2025 10:41:... 13 Feb 2025 10:41:45	140b2e6761ac9b575...	dev-opencti.ge3bo4o...	ScriptContent	4949c220a844071ee...	34032	
<input type="checkbox"/>	> 13 Feb 2025 10:42:... 13 Feb 2025 10:42:13	140b2e6761ac9b575...	dev-opencti.ge3bo4o...	ScriptContent	d27b77e4169d05540...	36377	
<input type="checkbox"/>	> 13 Feb 2025 10:42:... 13 Feb 2025 10:42:13	140b2e6761ac9b575...	dev-opencti.ge3bo4o...	ScriptContent	e3ff960a5627d01eb1...	36376	
<input type="checkbox"/>	> 13 Feb 2025 10:42:... 13 Feb 2025 10:42:13	140b2e6761ac9b575...	dev-opencti.ge3bo4o...	ScriptContent	1983c659b042b1ec2...	36375	
<input type="checkbox"/>	> 13 Feb 2025 10:50:... 13 Feb 2025 10:50:24	140b2e6761ac9b575...	dev-opencti.ge3bo4o...	ScriptContent	df4742a00d9f68ad9e...	93538	
<input type="checkbox"/>	> 13 Feb 2025 10:52:... 13 Feb 2025 10:52:03	140b2e6761ac9b575...	dev-opencti.ge3bo4o...	ScriptContent	249f431f59c5eeee20...	105763	
<input type="checkbox"/>	> 13 Feb 2025 10:52:... 13 Feb 2025 10:52:02	140b2e6761ac9b575...	dev-opencti.ge3bo4o...	ScriptContent	f02fd7f25613a571d8f...	105383	

Microsoft Defender

Search

Copilot Email notification settings Help resources

Threat analytics

Ransomware: 113 | Extortion: 0 | Phishing: 69 | Hands on keyboard: 0 | Activity group: 210 | Vulnerability: 134 | Attack campaign: 0 | Tool or technique: 0

Latest threats

Activity Profile: Sapphire Sleet uses fraudulent Zoom domains in recent spear-phish... 0 / 0

Activity Profile: BadPilot campaign - Seashell Blizzard subgroup conducts multiyear... 0 / 0

Activity Profile: Forest Blizzard targeting Western civilian transportation 0 / 0

Tool Profile: GoldBackdoor 0 / 0

Active Alerts | Resolved Alerts | No Alerts

High-impact threats

Threat Overview Profile: On-premises credential theft 84 / 103

Activity Profile: Storm-0300 ransomware activity 68 / 87

Tool Profile: Mimikatz 68 / 87

Threat Overview Profile: Human-operated ransomware 41 / 48

Active Alerts | Resolved Alerts | No Alerts

Highest exposure threats

Tool Profile: LaZagne 22

Tool Profile: GoldBackdoor 15

Activity Profile: Onyx Sleet using Epsilon Red ransomware 15

Activity Profile: Recent OSINT trends in botnet threats 15

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

Search

520 items | Customize columns | Filter

Threat	Alerts	Impacted assets	Threat exposure level	Misconfigured devices	Vulnerable devices	Report type	Published
Threat Overview Profile: On-premises credential theft	84 active / 103	84 / 8	0 - Low	2	0	Tools & techniques	1 Feb 2024 17:21
Tool Profile: Mimikatz	68 active / 87	68 / 6	15 - Low	2	Not available	Tools & techniques	6 Jul 2023 15:17
Activity Profile: Storm-0300 ransomware activity	68 active / 87	68 / 6	15 - Low	2	Not available	Attack campaigns	9 Jan 2023 17:21
Threat Overview Profile: Human-operated ransomware	41 active / 48	41 / 3	15 - Low	2	Not available	Tools & techniques	13 Jul 2021 18:05
Technique Profile: Brute-force attacks	1 active / 1	1 / 1	15 - Low	2	Not available	Tools & techniques	26 Sep 2023 21:05
Activity Profile: Sapphire Sleet uses fraudulent Zoom domains in r...	0 active / 0	0 / 0	0 - Low	Not available	Not available	Attack campaigns	12 Feb 2025 19:45

SquaredUp

TIKIT

- Check some setting we have spoken about tonight.
- Understand the unified portal is Active!
- Threat Hunts based on your environment can run constantly.
- Incidents and Alerts - Overview page
- Understand Reactive actions you can take on a device.
- Understand the Security Copilot embedded Guided Response.
- Show how Threat Intelligence is included when using Security Copilot.
- Use Built in Hunting rules.
- Use Security Copilot to generate a hunting query relating to Mimikatz



Resources

[Zero Trust deployment plan with Microsoft 365](#)

[Common identity and device access policies](#)

[Privileged access deployment](#)

[Intune Management Tool](#)

[OpenIntuneBaselines](#)

[MDE enhanced auditing](#)

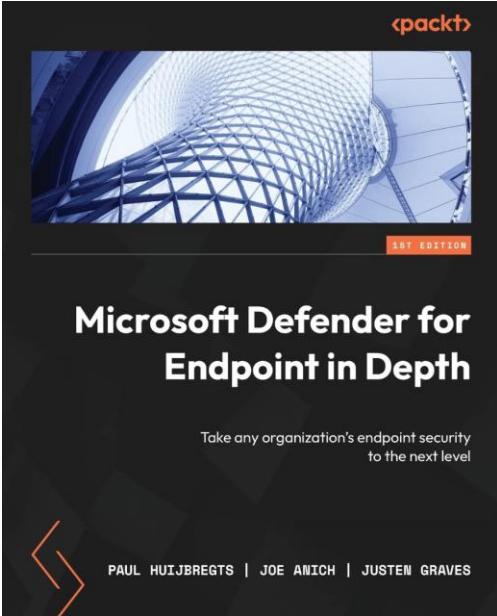
[Validate MDE protection capabilities](#)

[Defender Testground](#)

[MDE Tester](#)

[KQL Search](#)

Win a copy of...
Microsoft Defender for
Endpoint in Depth



Want to present?
<https://sessionize.com/ExpertsLiveUK>

