Mastering Endpoint Security:

From Zero Trust to Enterprise Access

Workshop guide

SquaredUp

TIKIT

Duration: 1 hour

What you'll need:

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

Workshop guide

SquaredUp

TIKIT

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

SquaredUp

TIKIT

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**

SquaredUp

TIKIT

Nathan Hutchinson

Microsoft Solutions Architect

Threatscape

Linktr.ee

SquaredUp

TIKIT

Marcus Burnap

Principal Consultant

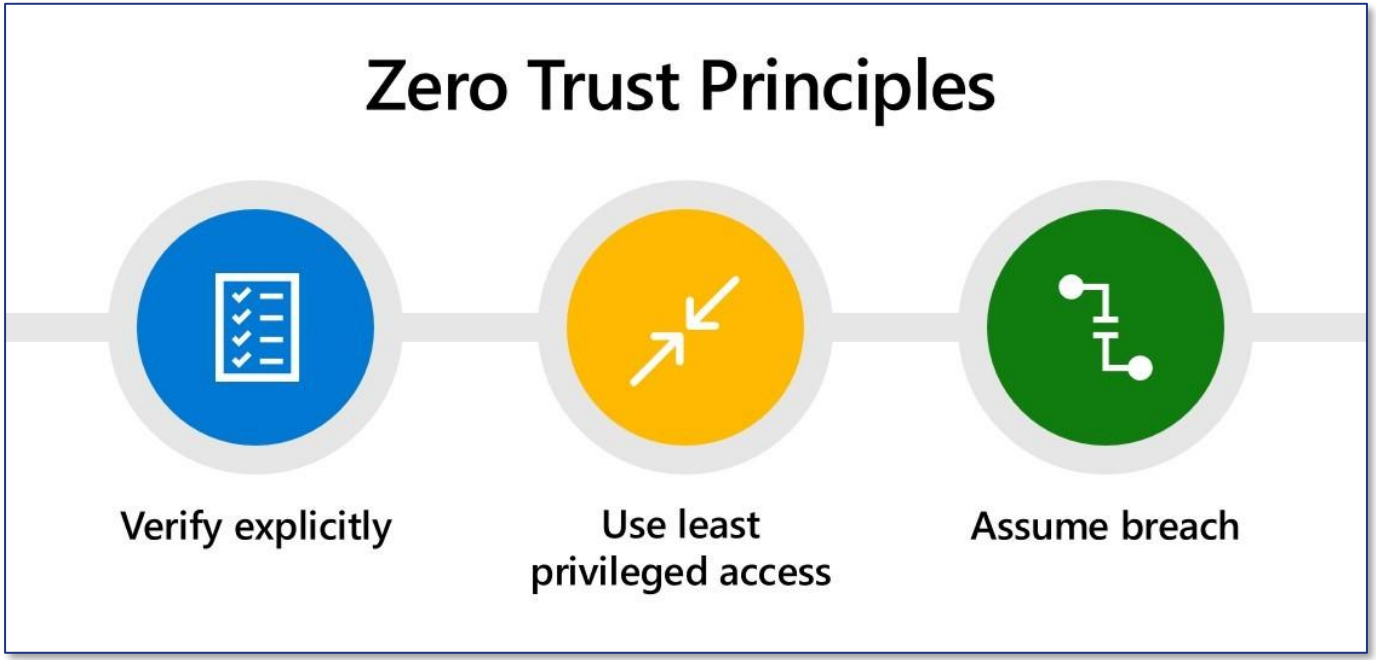
PERFORMANTA

Microsoft Most Valuable Professional

SquaredUp

TIKIT

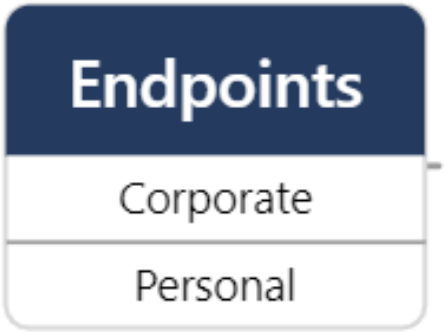
What is Zero Trust with Microsoft?



"never trust, always verify"

SquaredUp

TIKIT


Endpoints
Corporate
Personal

What is Zero Trust with Microsoft?

3 steps completed 12 seconds

Feb 12, 5:03 PM

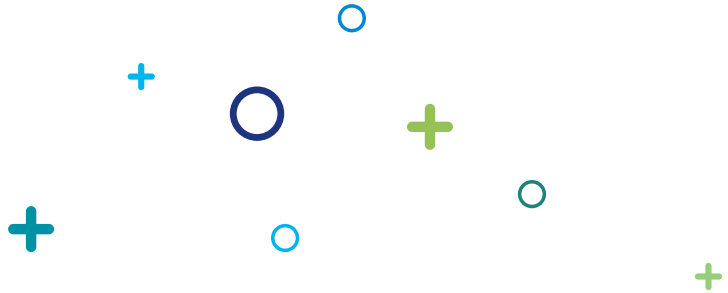
Zero Trust with Microsoft is a security strategy that focuses on three core principles: verify explicitly, use least privilege access, and assume breach. This approach is designed to protect people, devices, applications, and data regardless of where they are located.

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

SquaredUp

TIKIT

Learn more

Deployment Objectives

Register endpoints with cloud identity providers

Enforce access controls for cloud-managed & compliant devices

Implement Data Loss Prevention (DLP) policies

SquaredUp

TIKIT

Learn more

Deployment Objectives

Register endpoints with cloud identity providers

Enforce access controls for cloud-managed & compliant devices

Implement Data Loss Prevention (DLP) policies

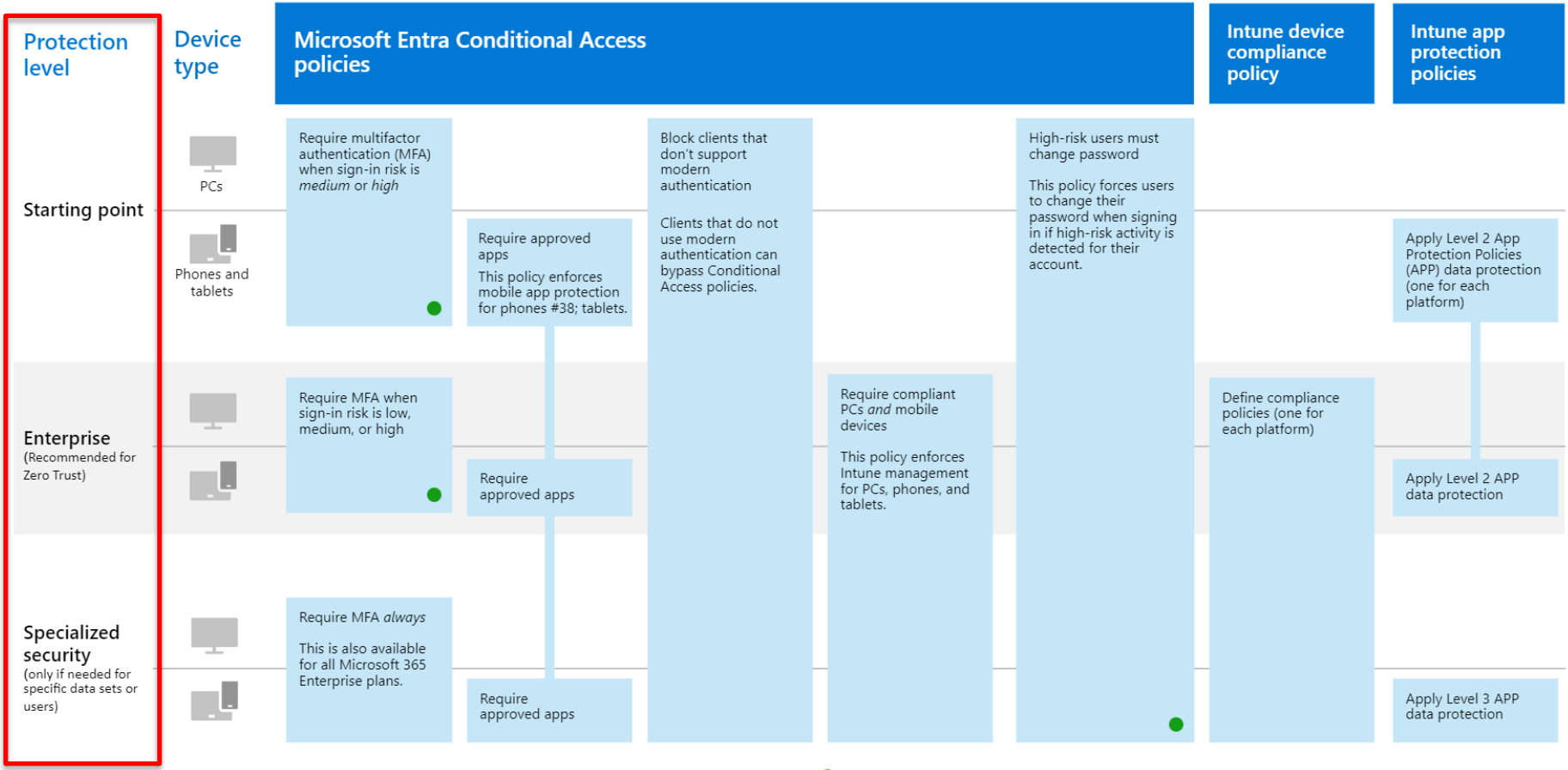
Deploy endpoint threat detection & monitoring

Adaptive access based on endpoint risk

SquaredUp

TIKIT

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

March 2024

Zero Trust identity and device access policies

Protection level	Device type	Microsoft Entra Conditional Access policies			
Starting point	PCs	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.	
	Phones and tablets				
Enterprise (Recommended for		Require MFA when sign-in risk is low, medium, or high			Require compliant PCs *and* mobile devices This policy enforces

PCs

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

Block clients that don't support modern authentication

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

Starting point

Phones and tablets

Require approved apps

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

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

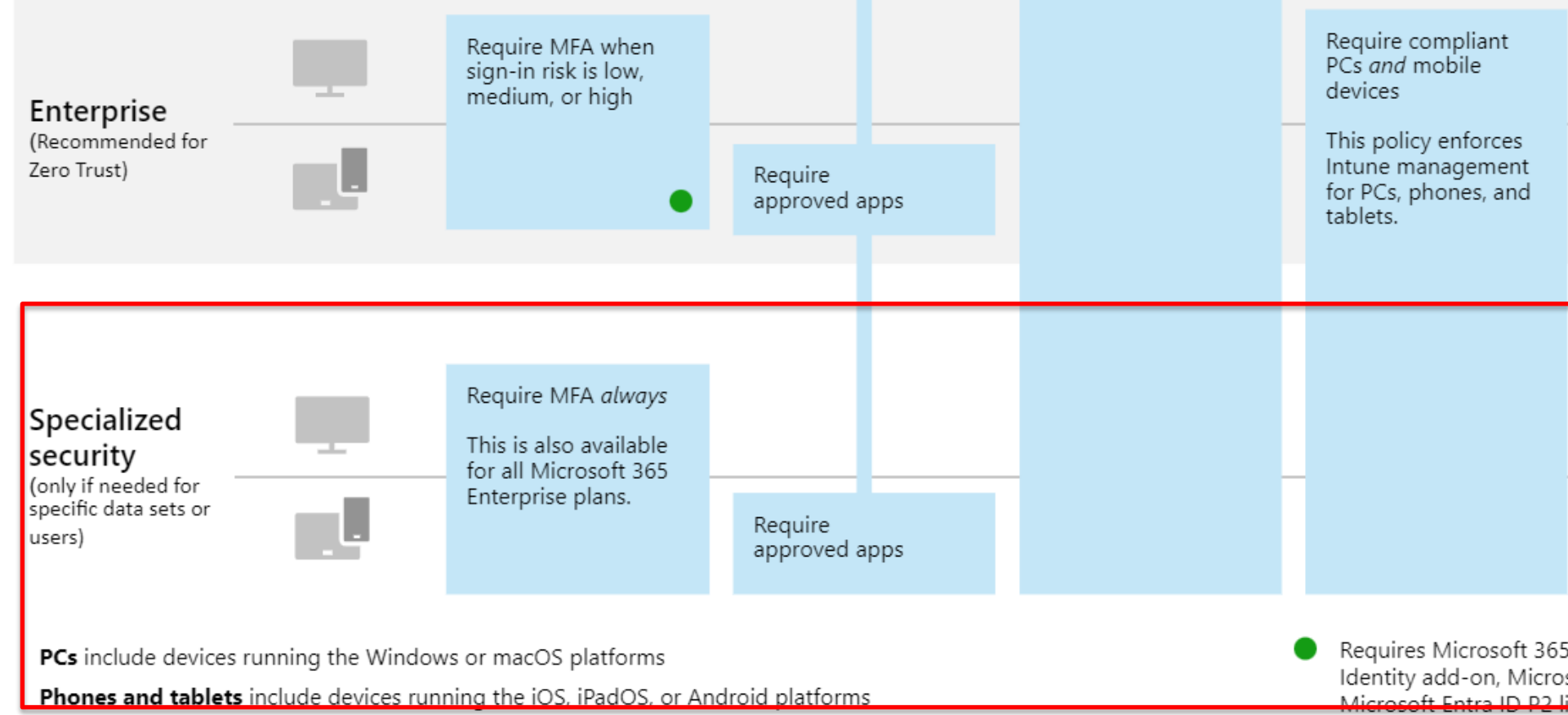
This policy enforces Intune management for PCs, phones, and tablets.

Specialized security

(only if needed for specific data sets or

Require MFA *always*

This is also available for all Microsoft 365 Enterprise plans.



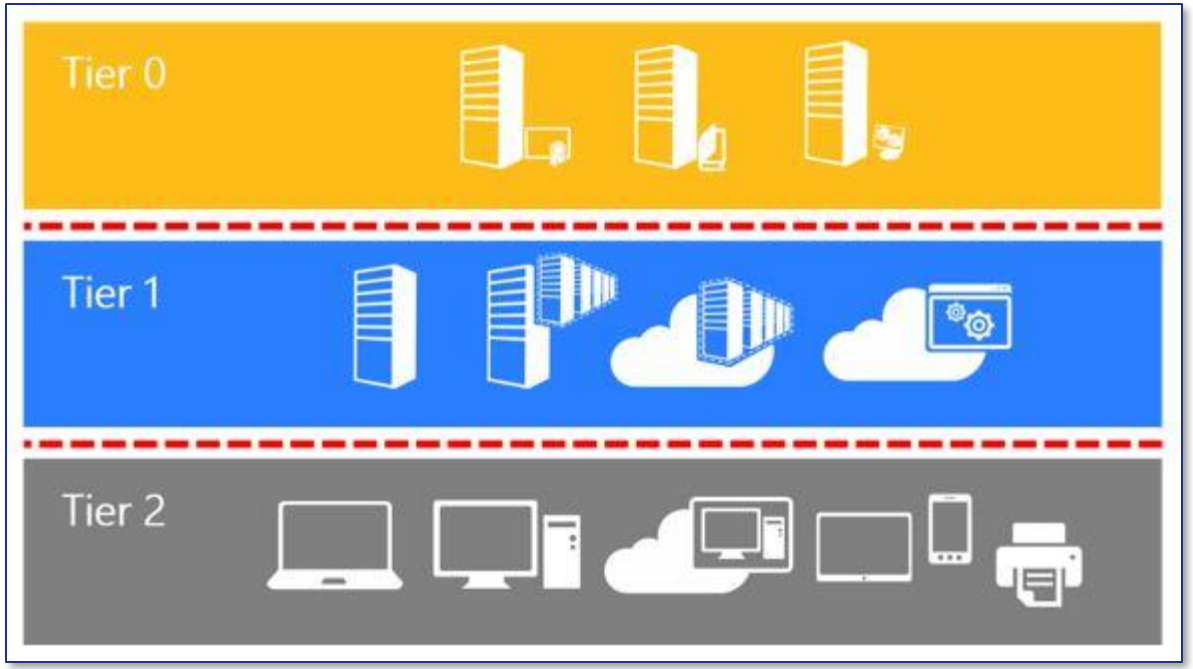
How can we assess our readiness?

Demo 1: Microsoft Zero Trust Assessment Tool

SquaredUp

TIKIT

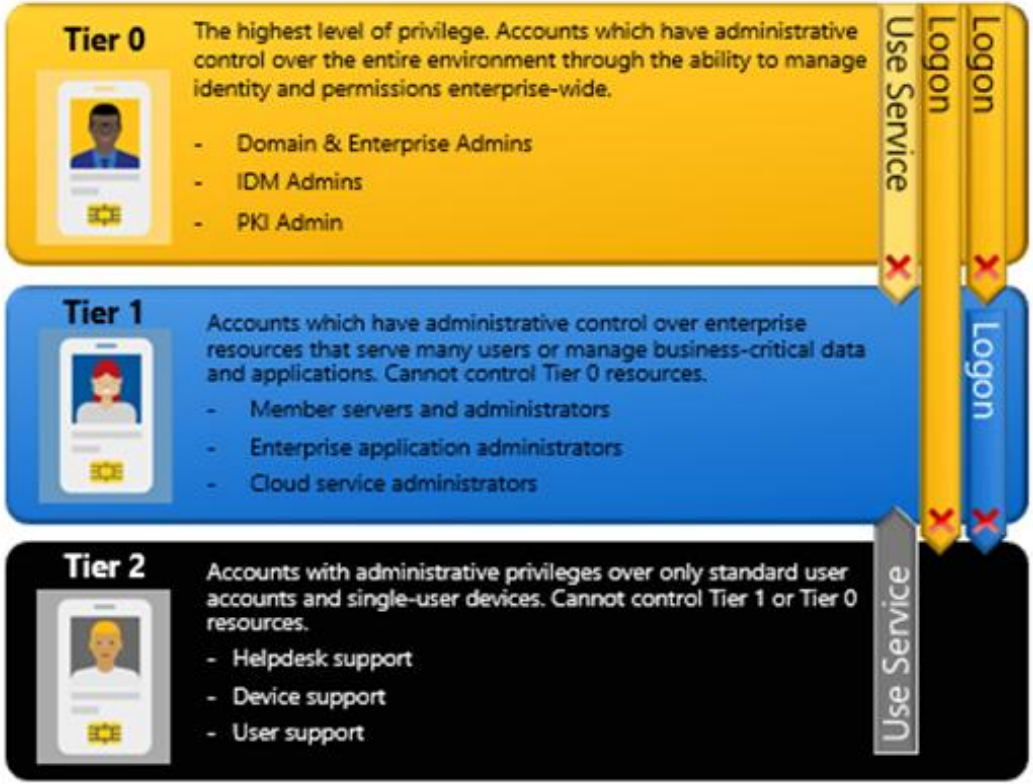
AD tier model



SquaredUp

TIKIT

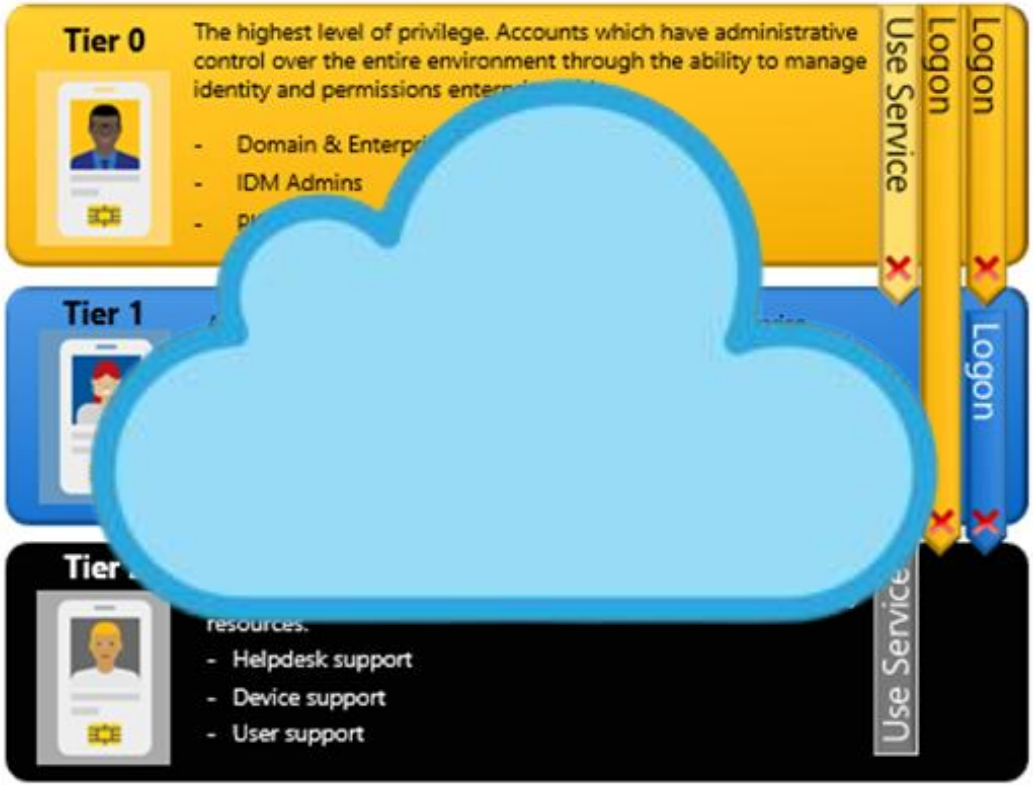
AD tier model



SquaredUp

TIKIT

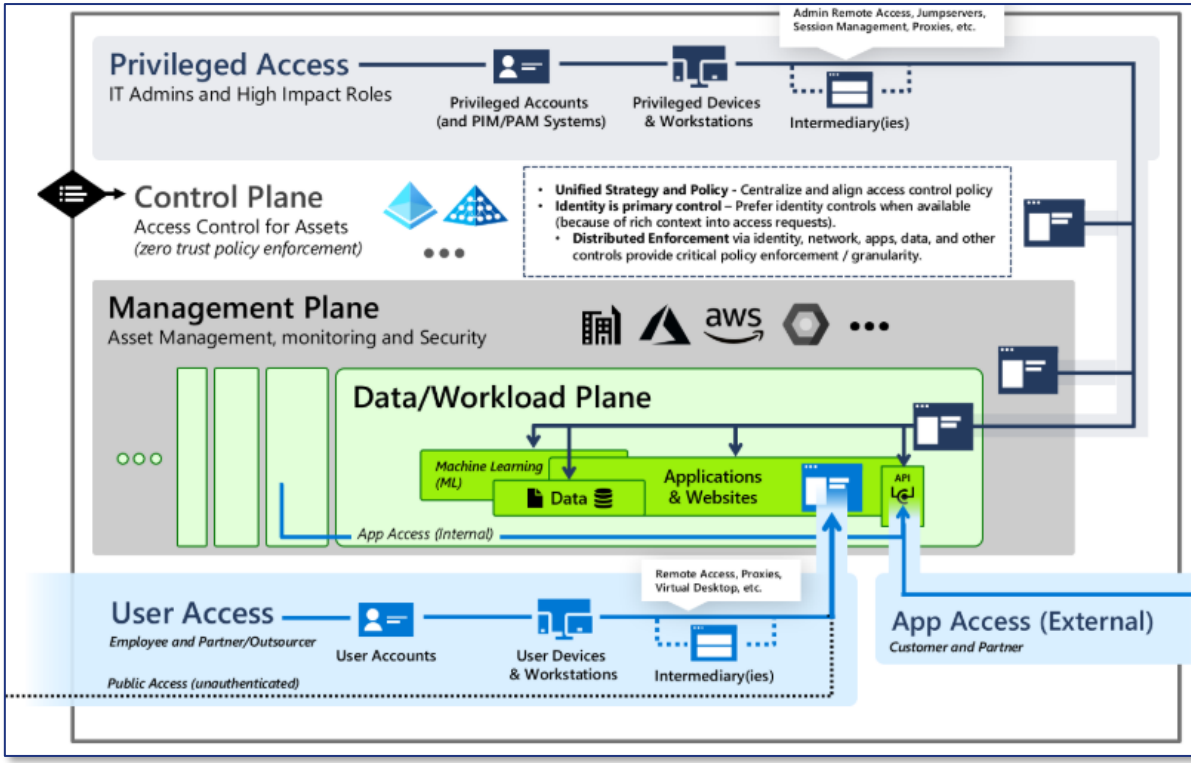
AD tier model



SquaredUp

TIKIT

Enterprise Access Model



Privileged Access

Enables IT administrators and other high impact roles to access to sensitive systems and data. *Stronger security for higher impact accounts*

Control and Management Planes

Provide unified access and management for workloads and assets *(and provide attackers shortcut for illicit objectives)*

Data/Workloads

Create and store business value in

- Business processes (in apps/workloads)
- Intellectual property (in data and apps)

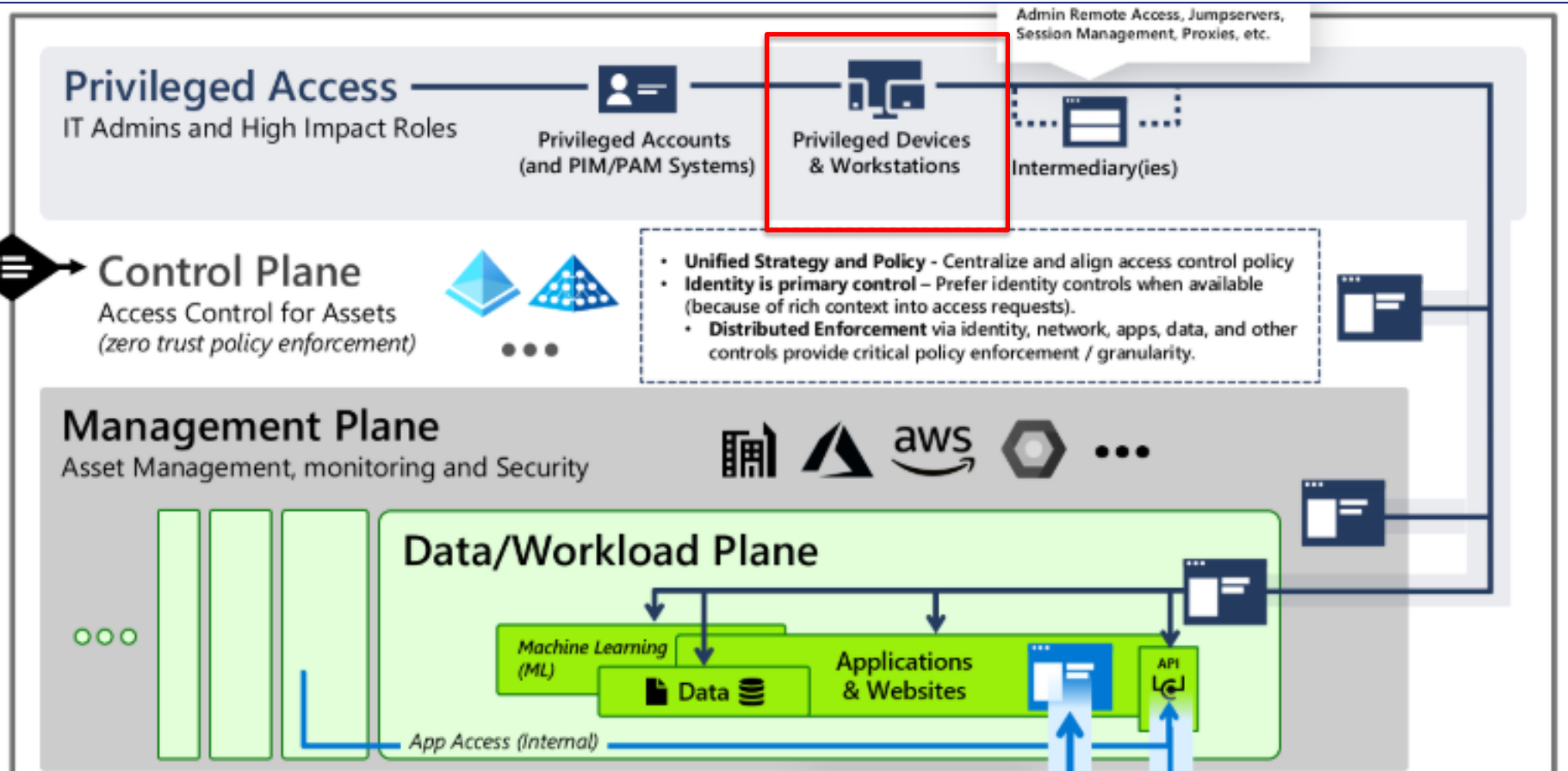
User and App Access

How employees, partners, and customers access these resources

SquaredUp

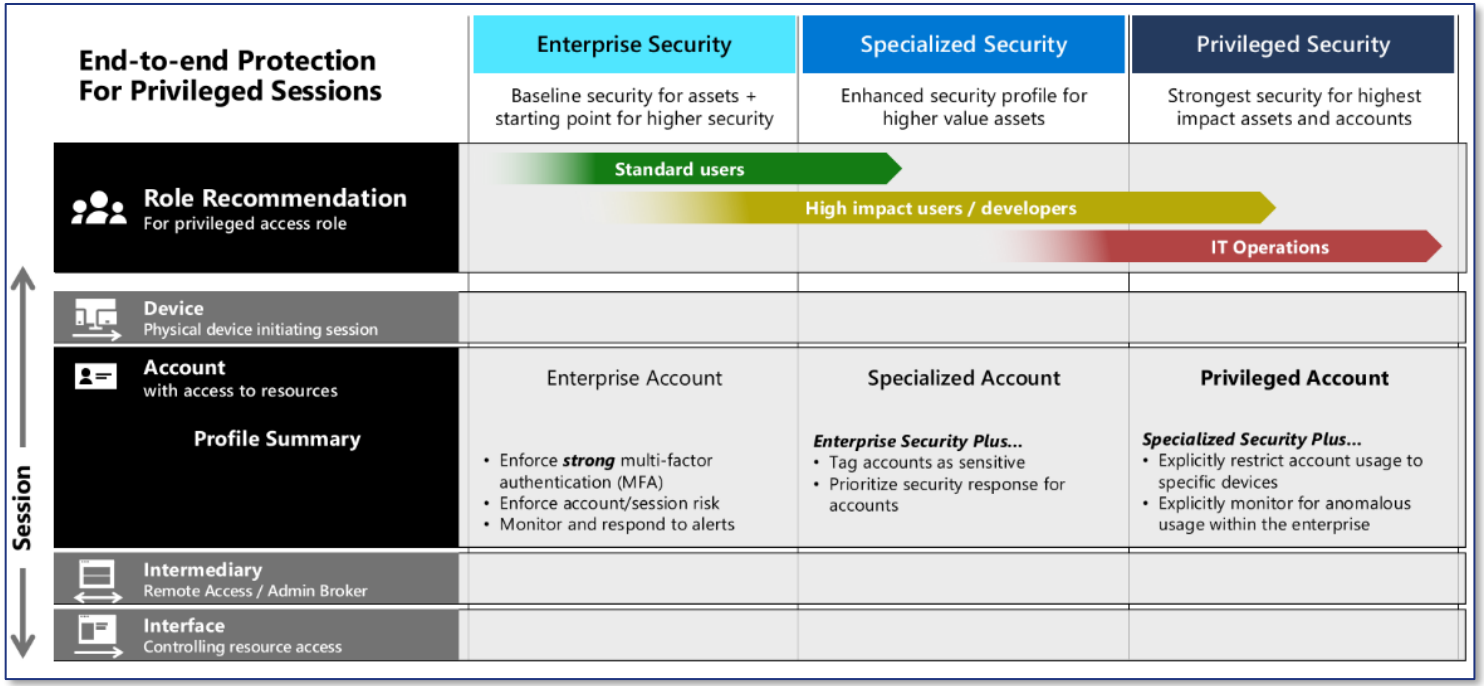
TIKIT

Enterprise Access Model



Securing Privileged Access

Learn more



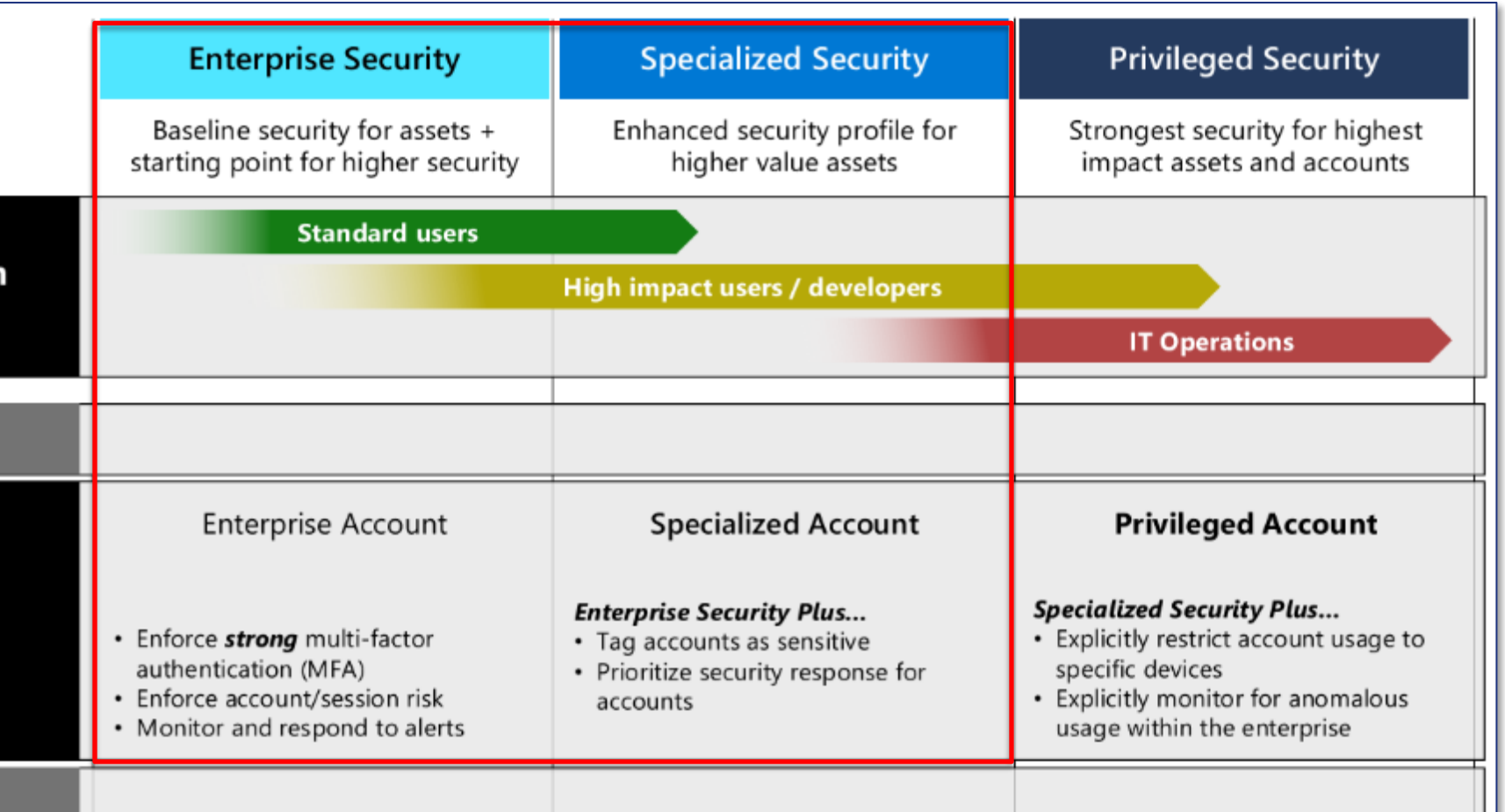
Enterprise Access Model

SquaredUp

TIKIT

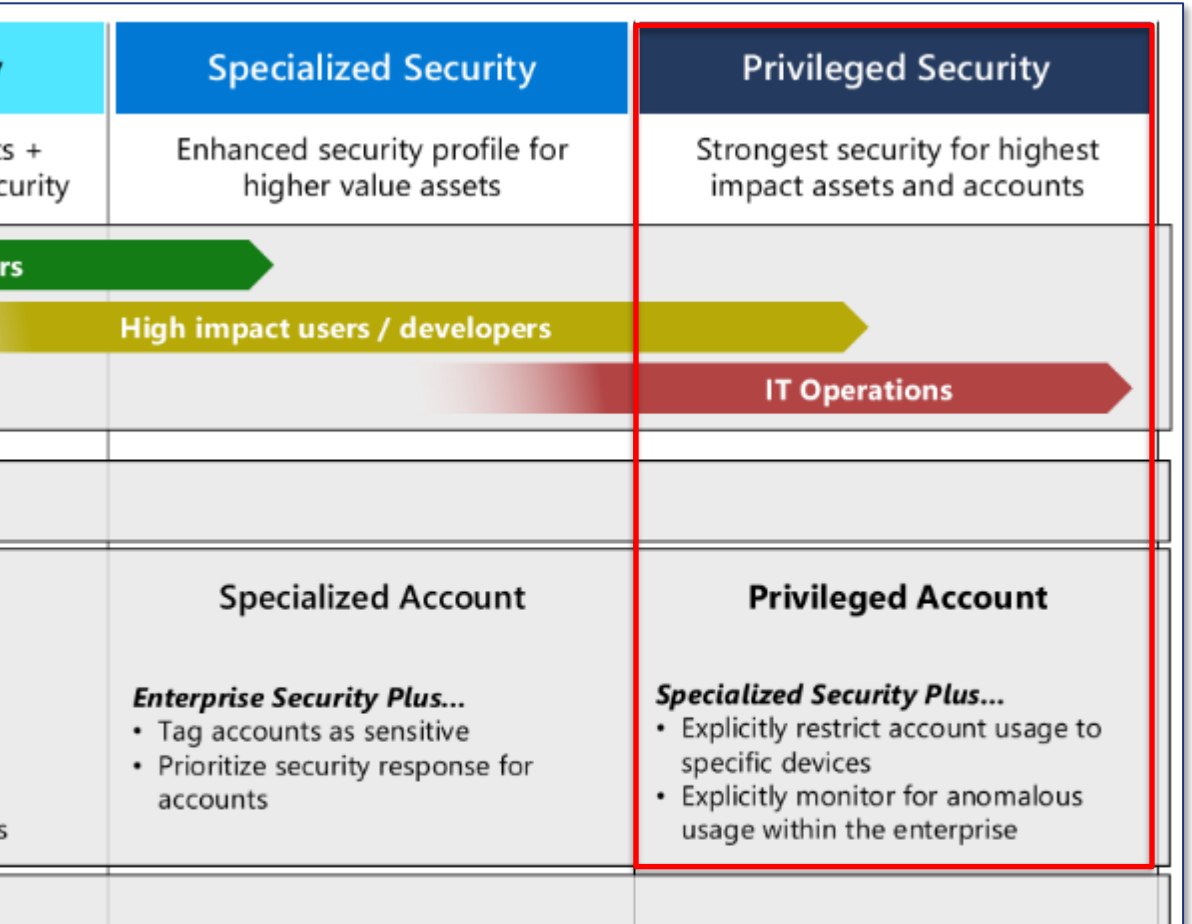
Securing Privileged Access

Learn more



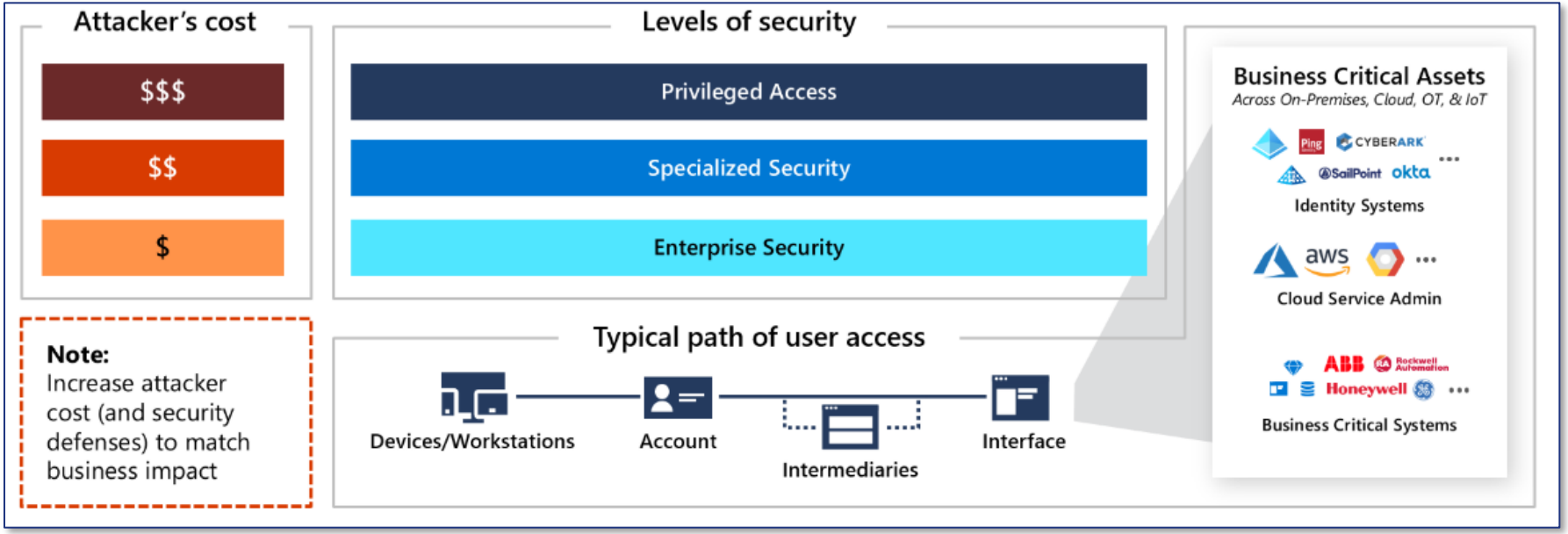
Securing Privileged Access

Learn more



TIKIT

Securing Privileged Access



SquaredUp

TIKIT

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 | Off

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

Edit

```
device.extensionAttribute1 -eq "privilegedAccessWorkstation"
```

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

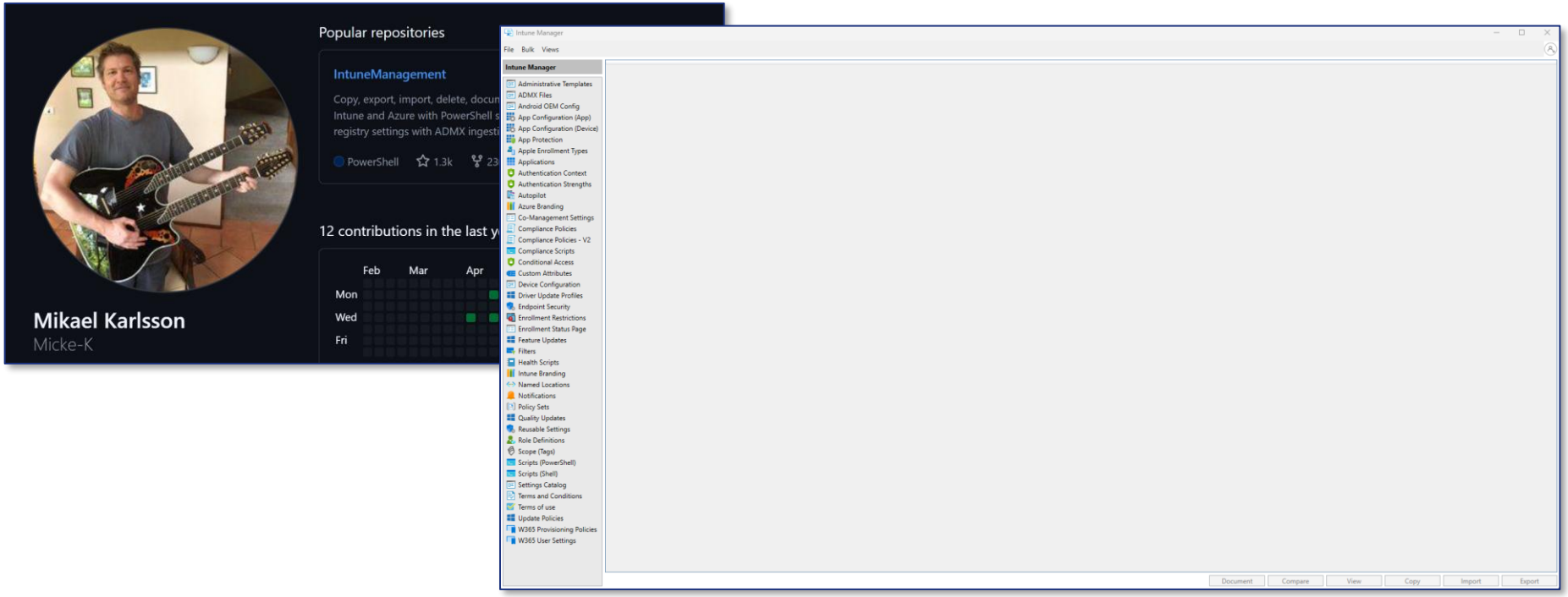
Key differences & when to use each approach

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

SquaredUp

TIKIT

Intune Management Tool



SquaredUp

TIKIT

Learn more

Intune Manager

Backup configurations

Version control

Simplify policy deployment & replication

Document policies

SquaredUp

TIKIT

Import / Export and Document policies.

Demo 2: Using Intune Manager

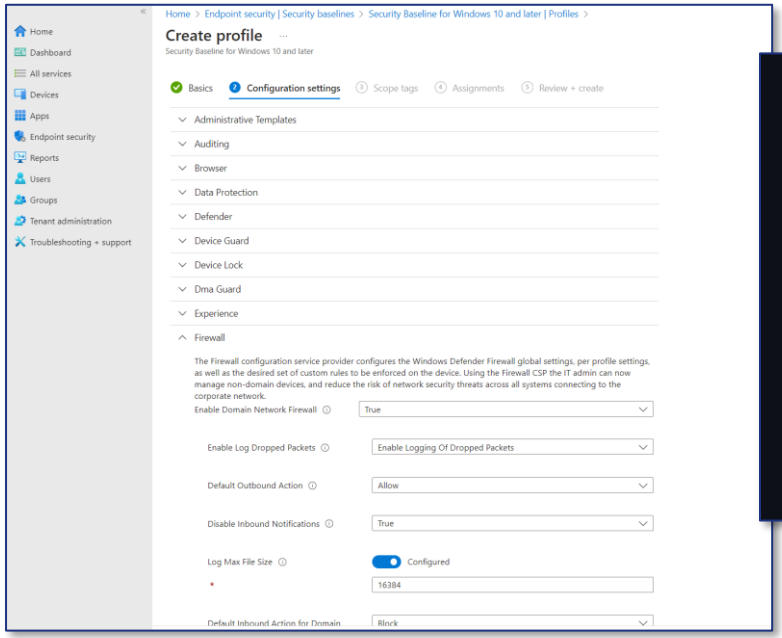
SquaredUp

TIKIT

SquaredUp

TIKIT

Security Baselines



OpenIntuneBaseline

SquaredUp

TIKIT

Harden those endpoints.

Demo 3: Creating security baselines

SquaredUp

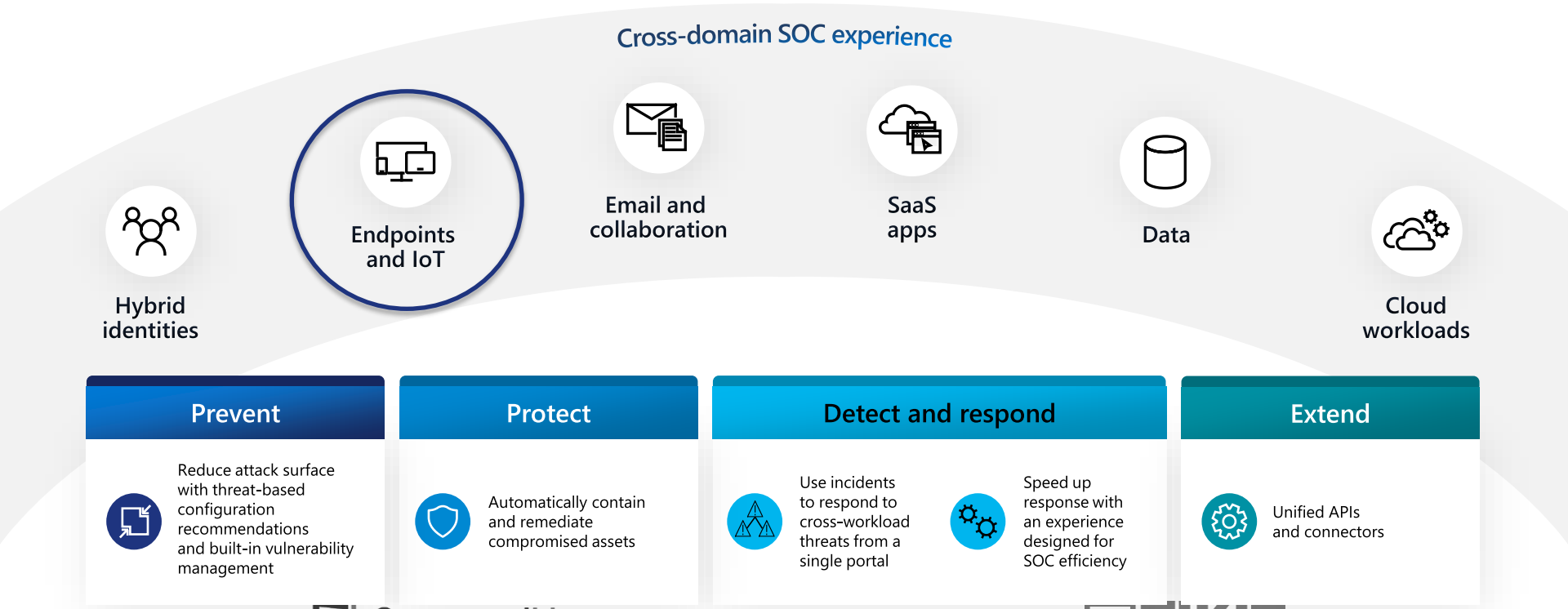
TIKIT

SquaredUp

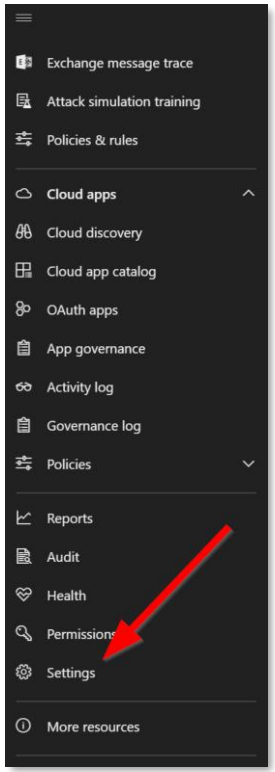
TIKIT

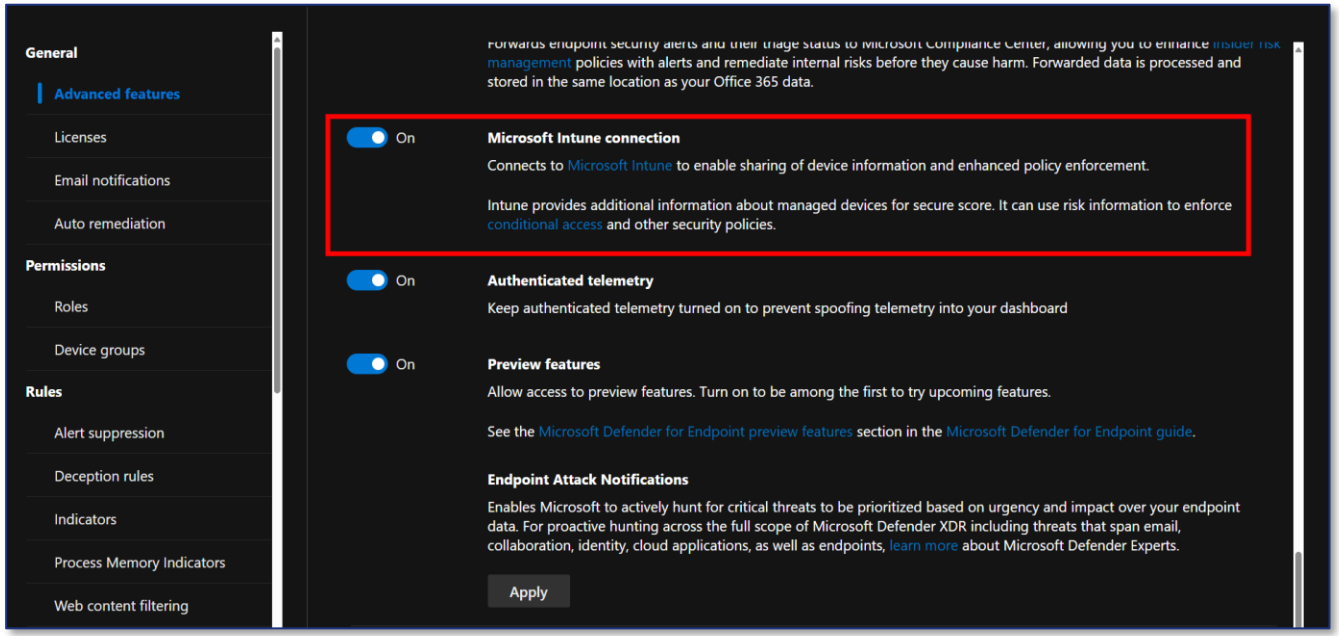
Microsoft Defender XDR

Build a unified defense with XDR



Onboarding using Intune

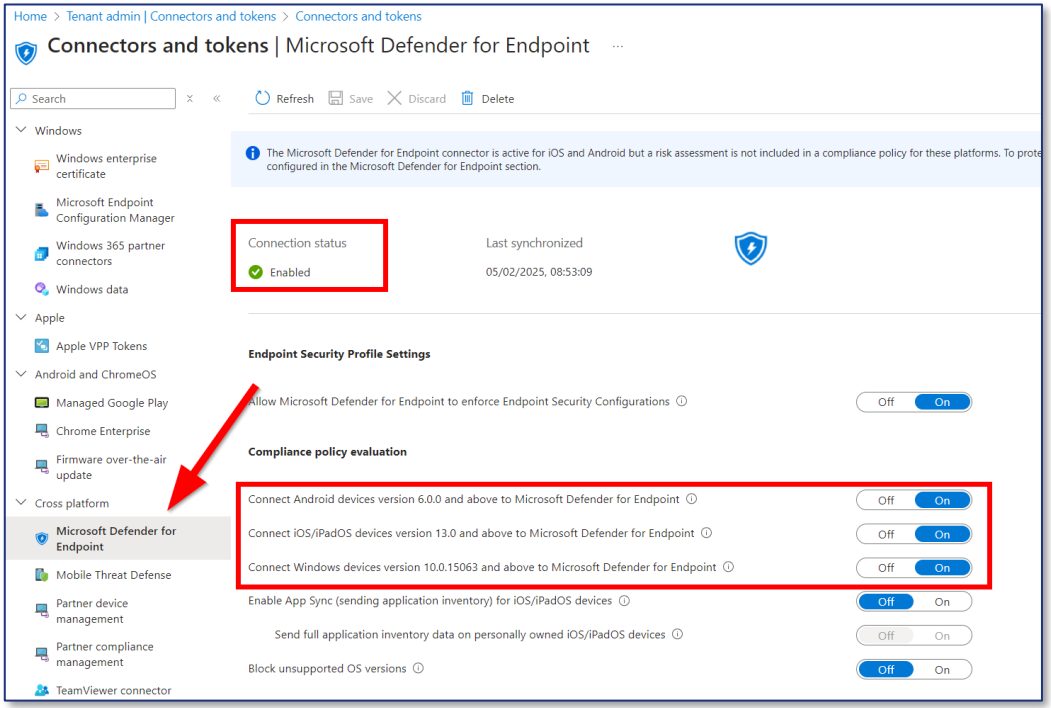




SquaredUp

TIKIT

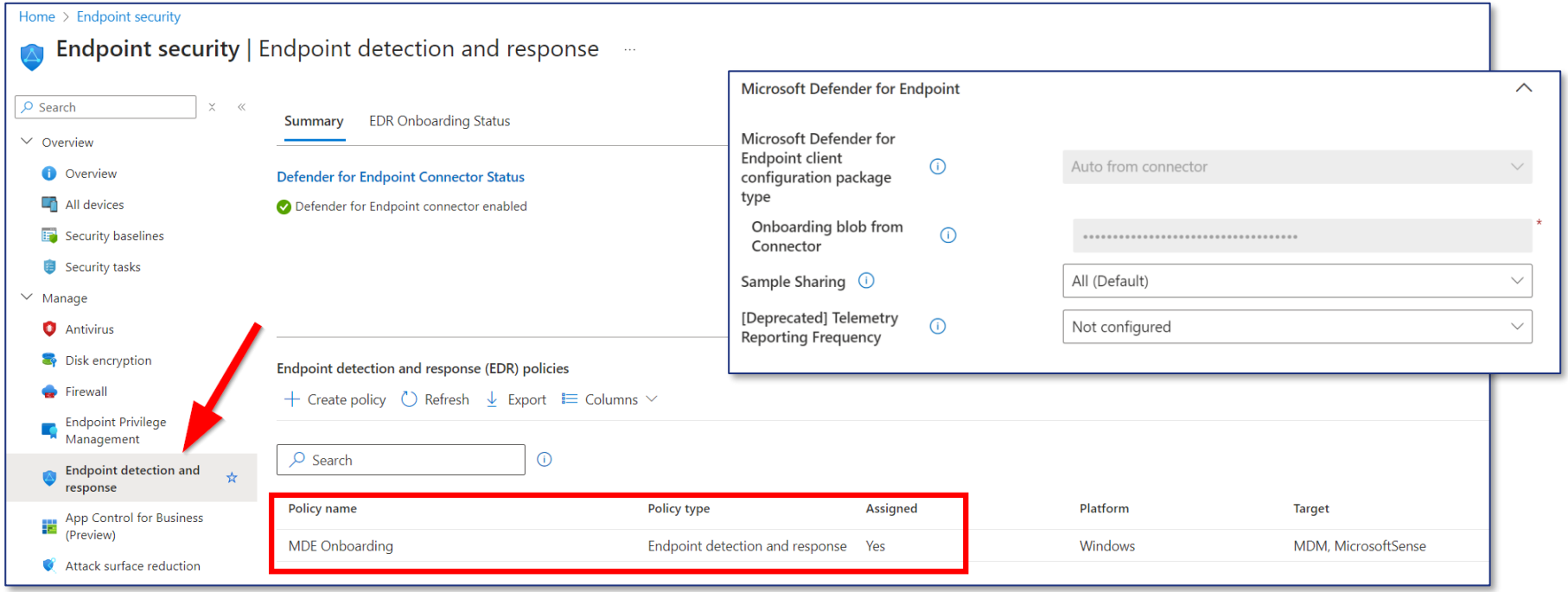
Onboarding using Intune



SquaredUp

TIKIT

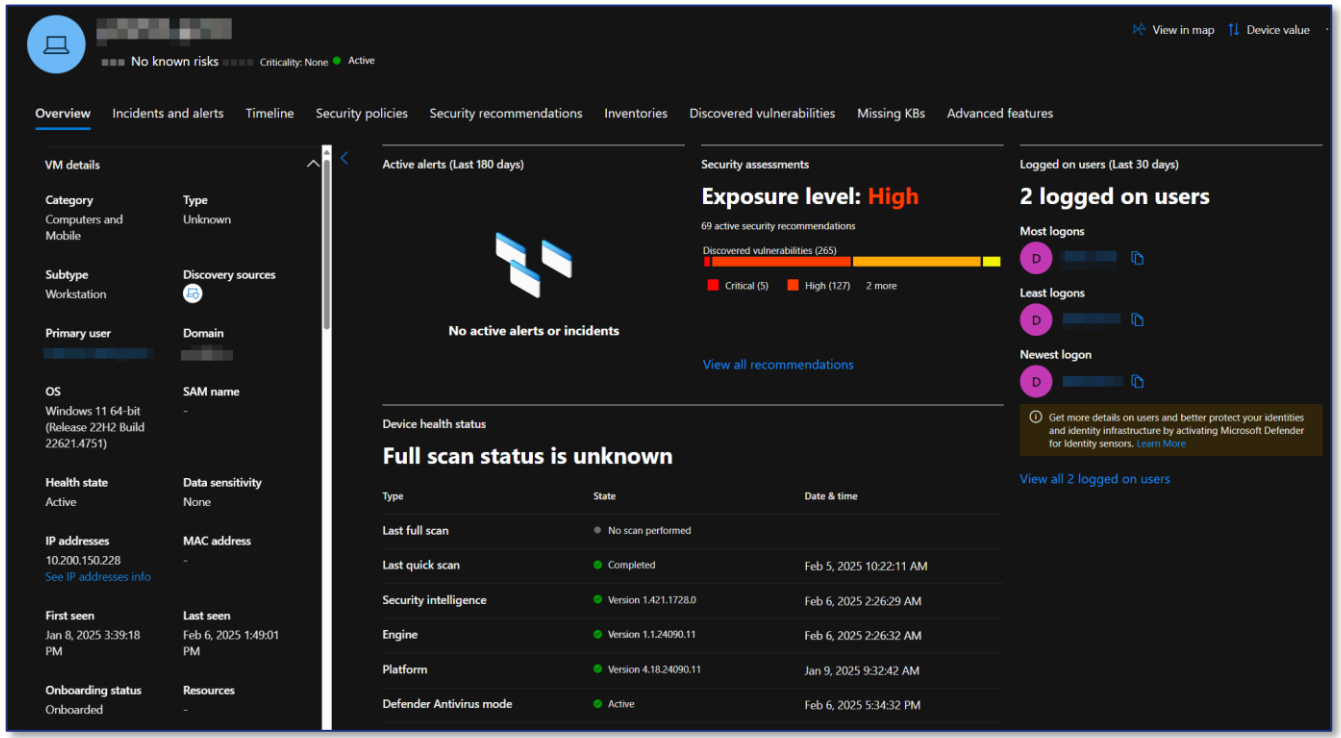
Onboarding using Intune



SquaredUp

TIKIT

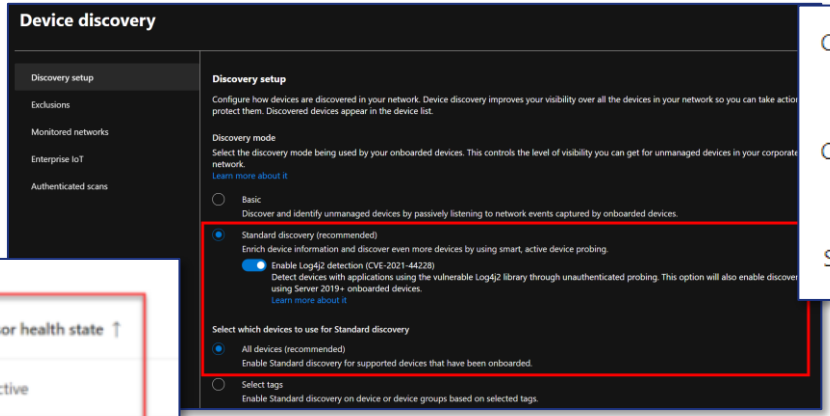
Onboarding using Intune

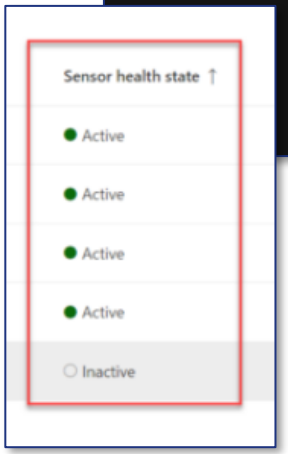


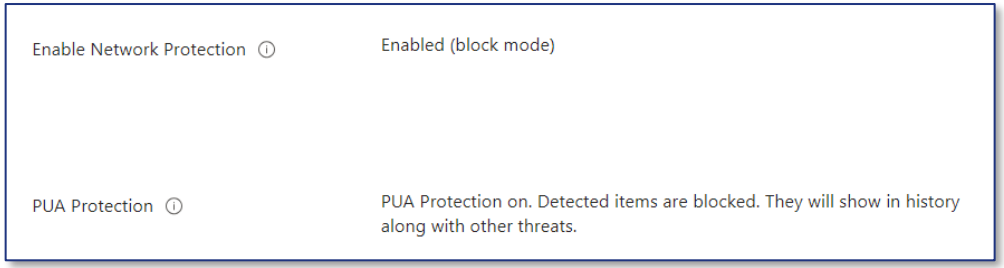
SquaredUp

TIKIT

Post onboarding tasks / common mistakes



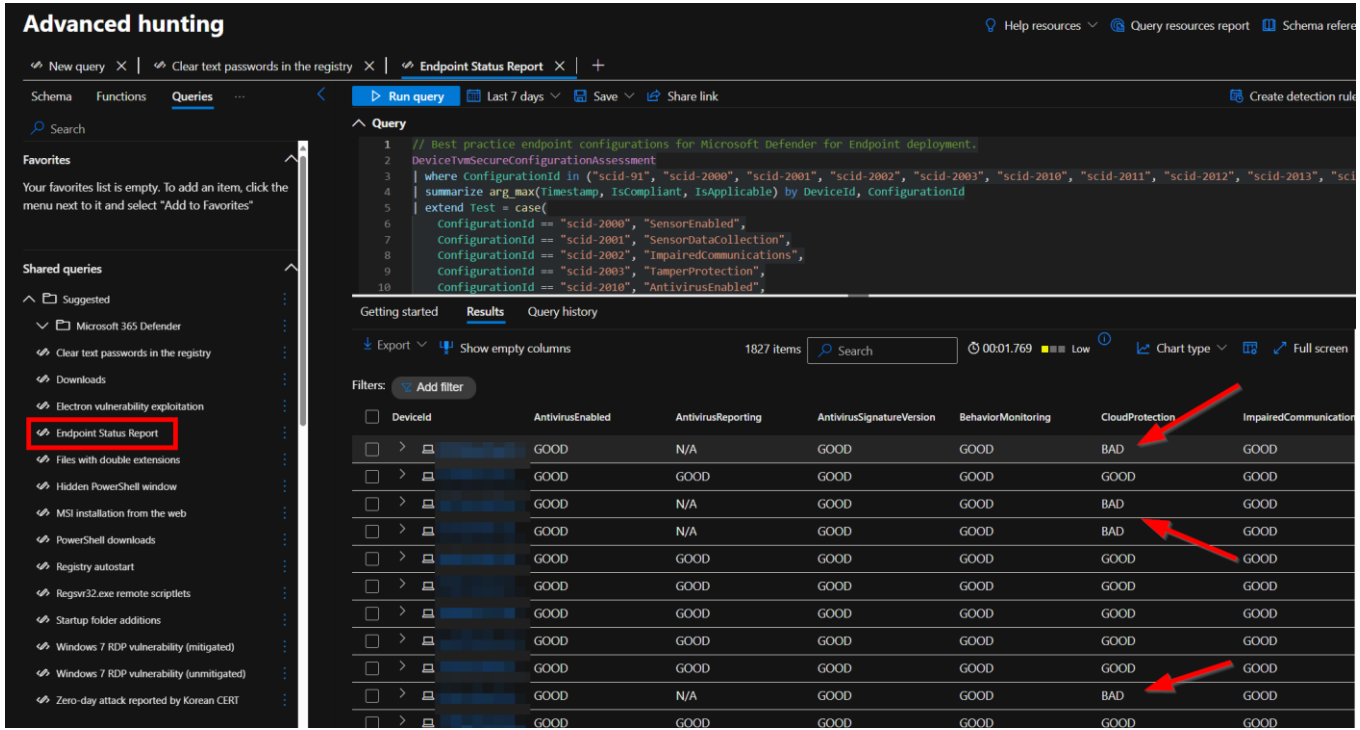




SquaredUp

TIKIT

Post onboarding tasks / common mistakes

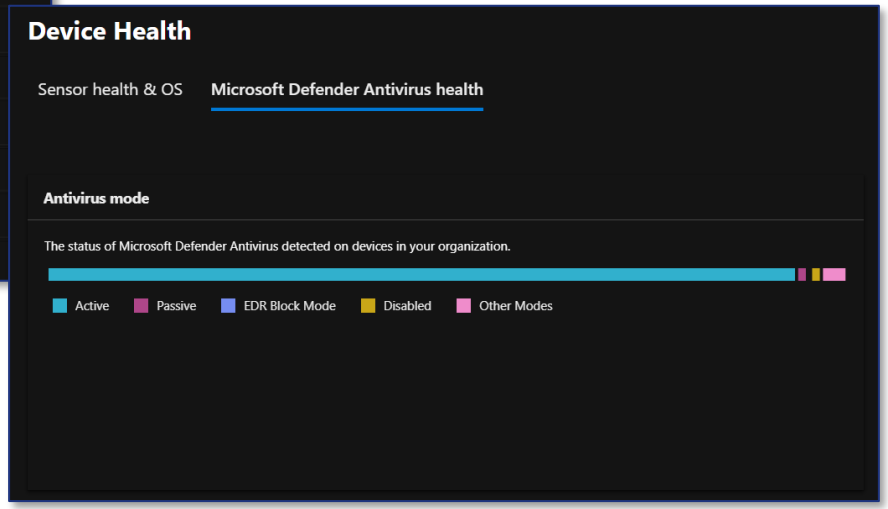


SquaredUp

TIKIT

Post onboarding tasks / common mistakes

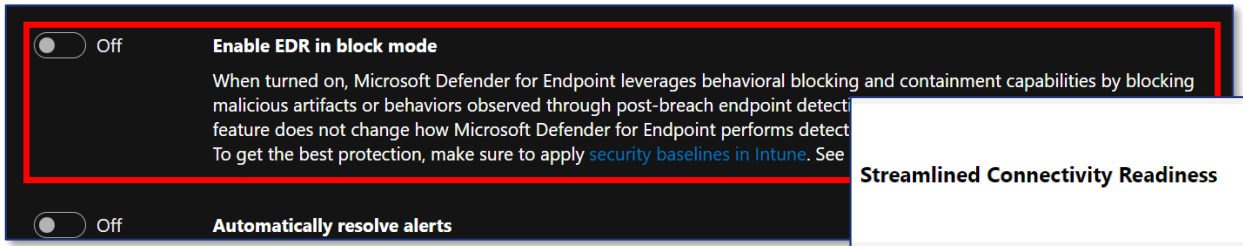
Enable Microsoft Defender Antivirus email scanning	Windows	1	Security controls (Antivirus)
Block Win32 API calls from Office macros	Windows	1	Security controls (Attack Surface Reduction)
Block Office applications from creating executable content	Windows	1	Security controls (Attack Surface Reduction)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

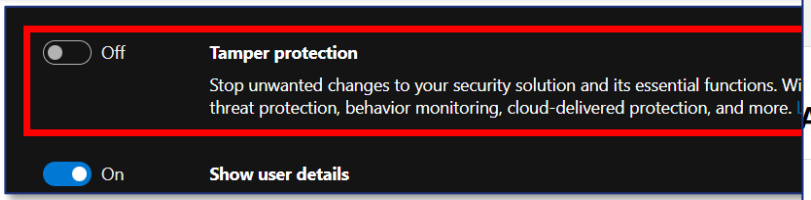


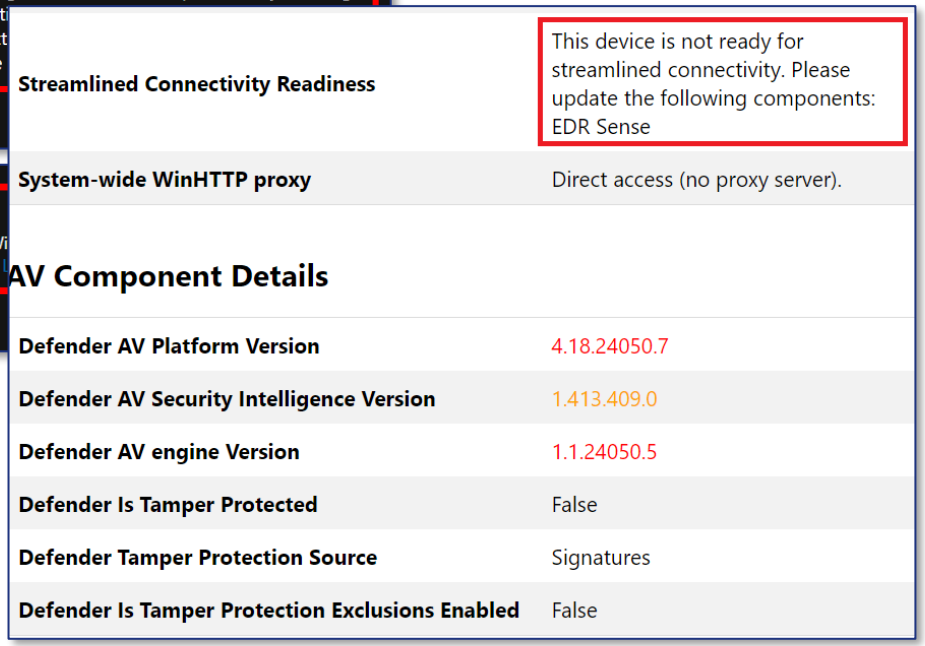
SquaredUp

TIKIT

Post onboarding tasks / common mistakes



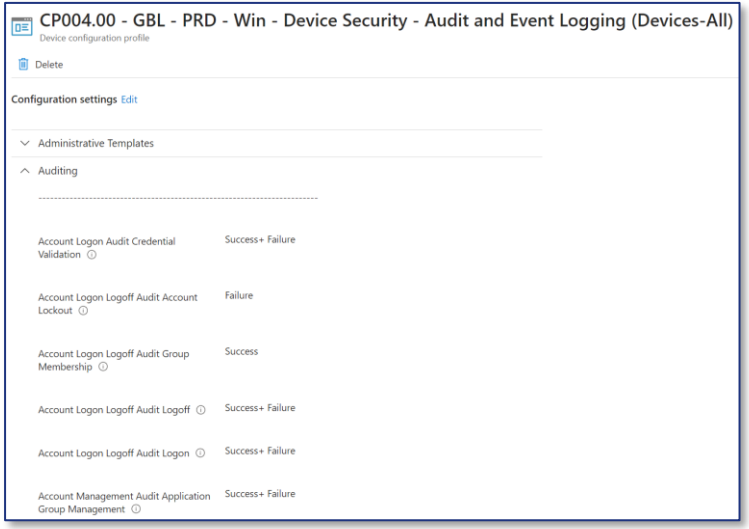


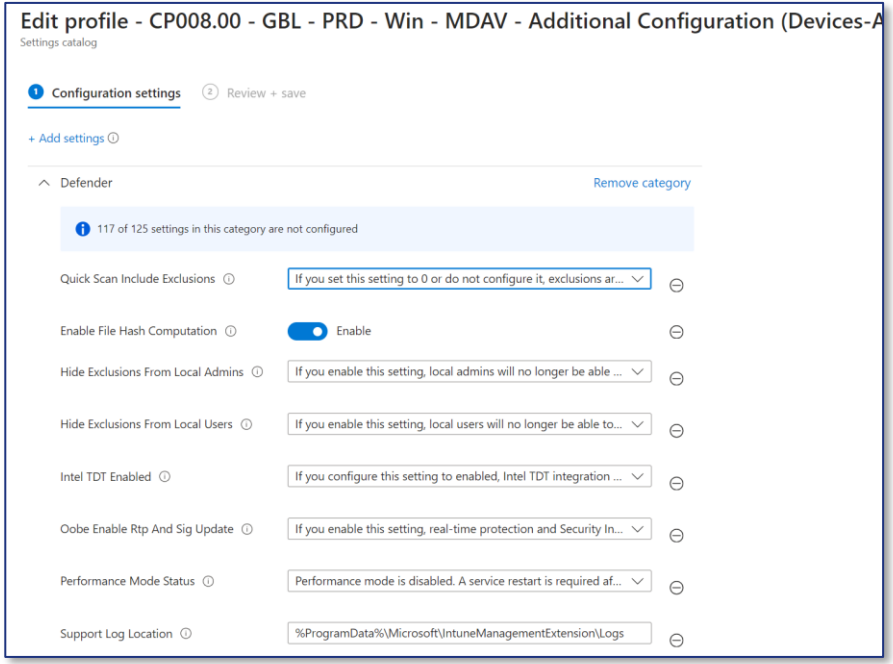


SquaredUp

TIKIT

Post onboarding tasks / common mistakes

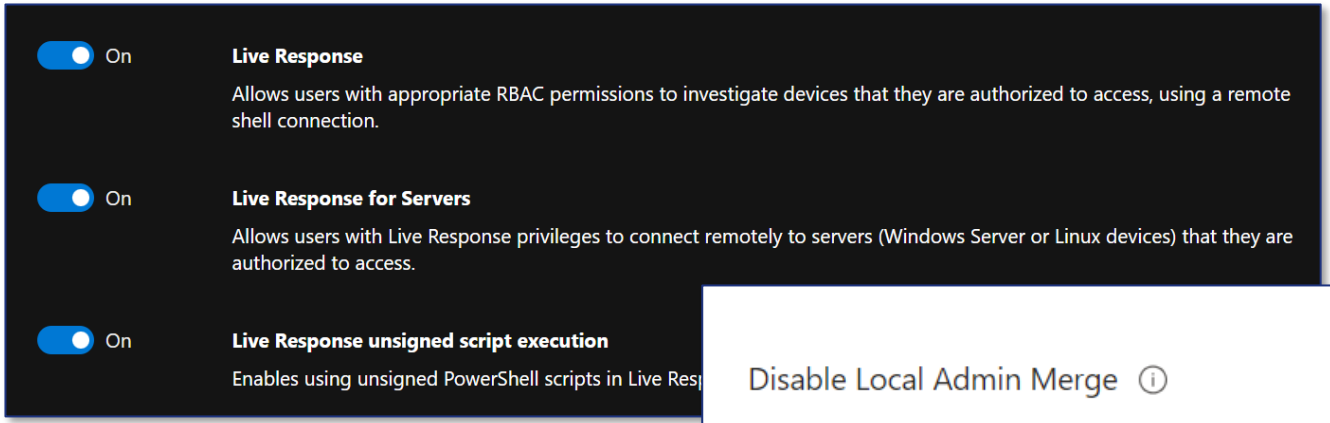


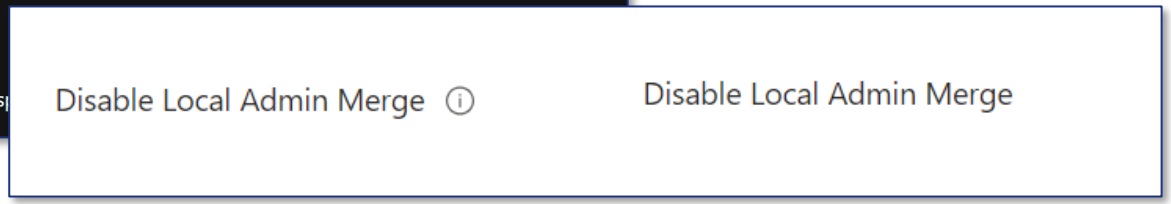


SquaredUp

TIKIT

Post onboarding tasks / common mistakes

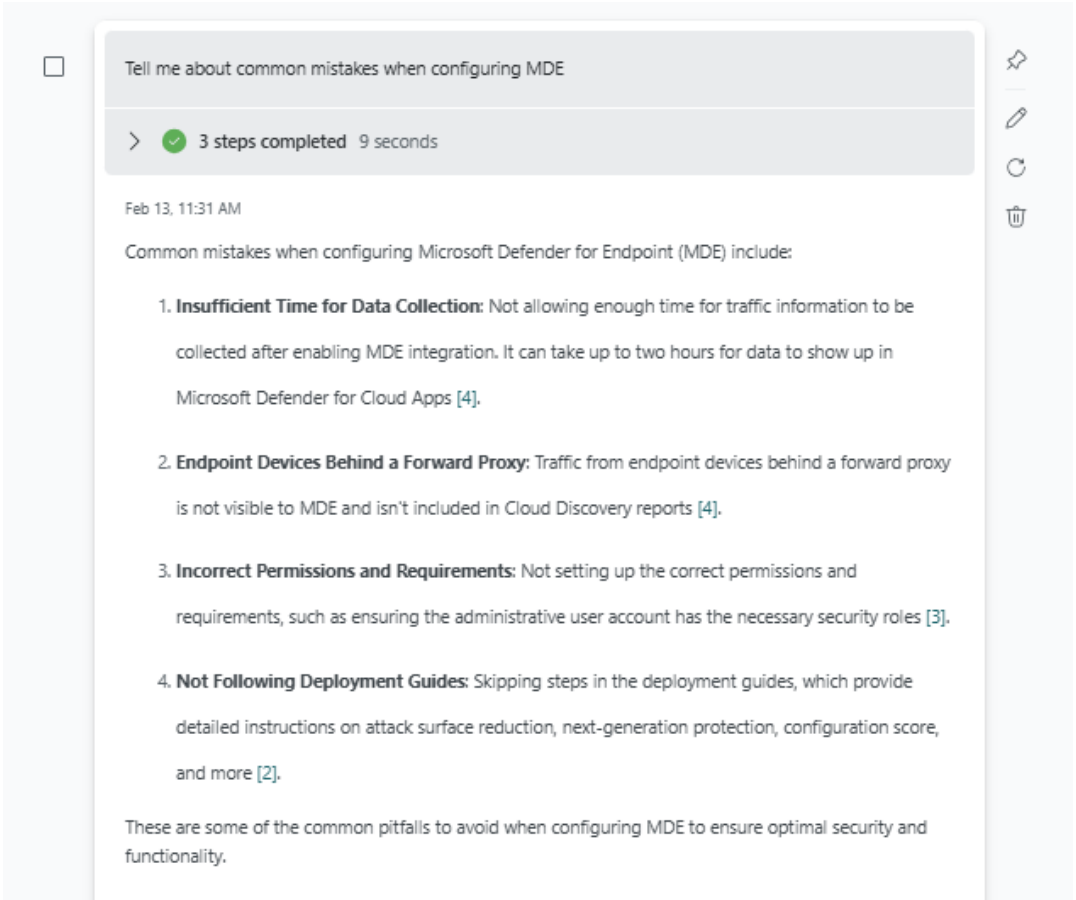




AV011.00 - GBL - DEV - Win - Antivirus - MDAV Update - Ring 1 - Pilot (Devices-WinClients)	Defender Update controls
AV012.00 - GBL - DEV - Win - Antivirus - MDAV Update - Ring 2 - UAT (Devices-WinClients)	Defender Update controls
AV013.00 - GBL - DEV - Win - Antivirus - MDAV Update - Ring 3 - Production (Devices-WinClients)	Defender Update controls

SquaredUp

TIKIT



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.

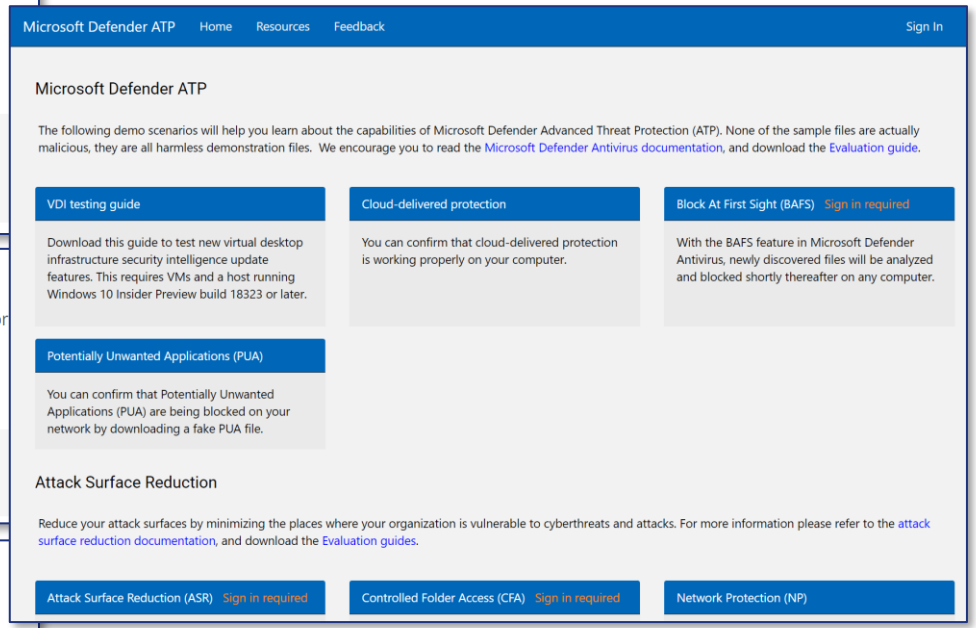
Run the following command:

```
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 $e
nv:TEMP\lsass-comsvcs.dmp full
```

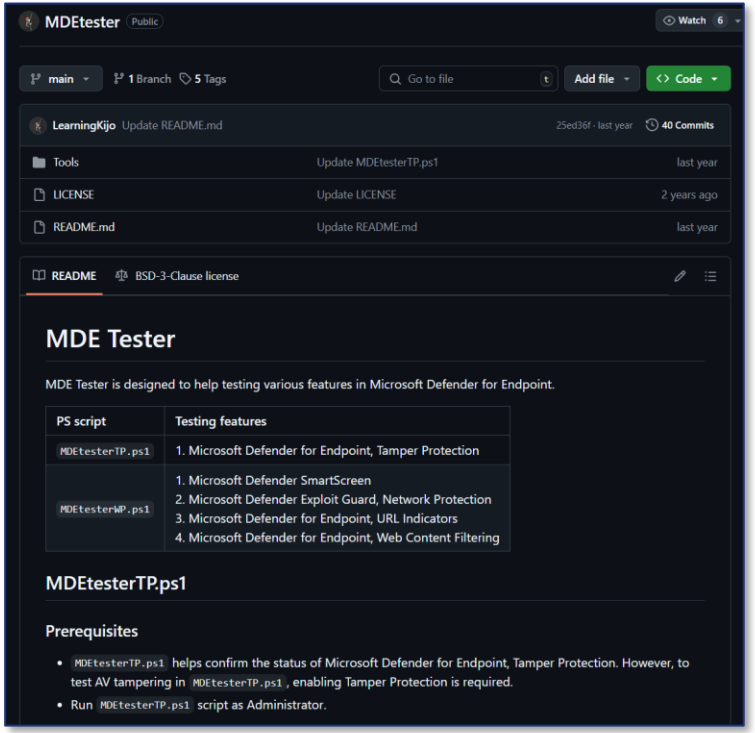


Home - Microsoft Defender Testground

SquaredUp

TIKIT

Validate configurations



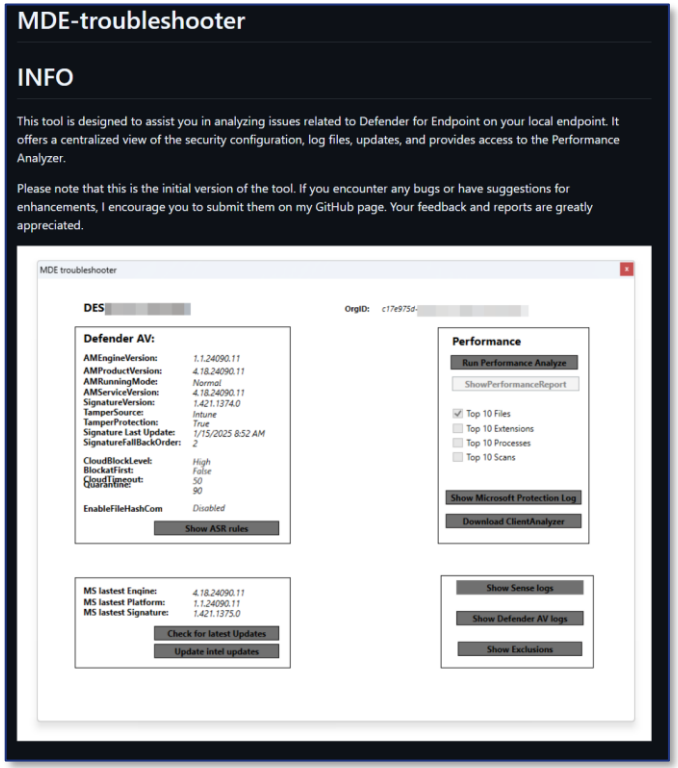
LearningKijo/MDEtester: MDE Tester is designed to help testing various features in Microsoft Defender for Endpoint.

SquaredUp

TIKIT

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.



SquaredUp

TIKIT

Time to hunt.

Demo 4: Using the Unified SecOps portal

SquaredUp

TIKIT

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

Data

300+ third-party solutions

CHECK POINT · SAP · ORACLE · CROWDSTRIKE · paloalto

- 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

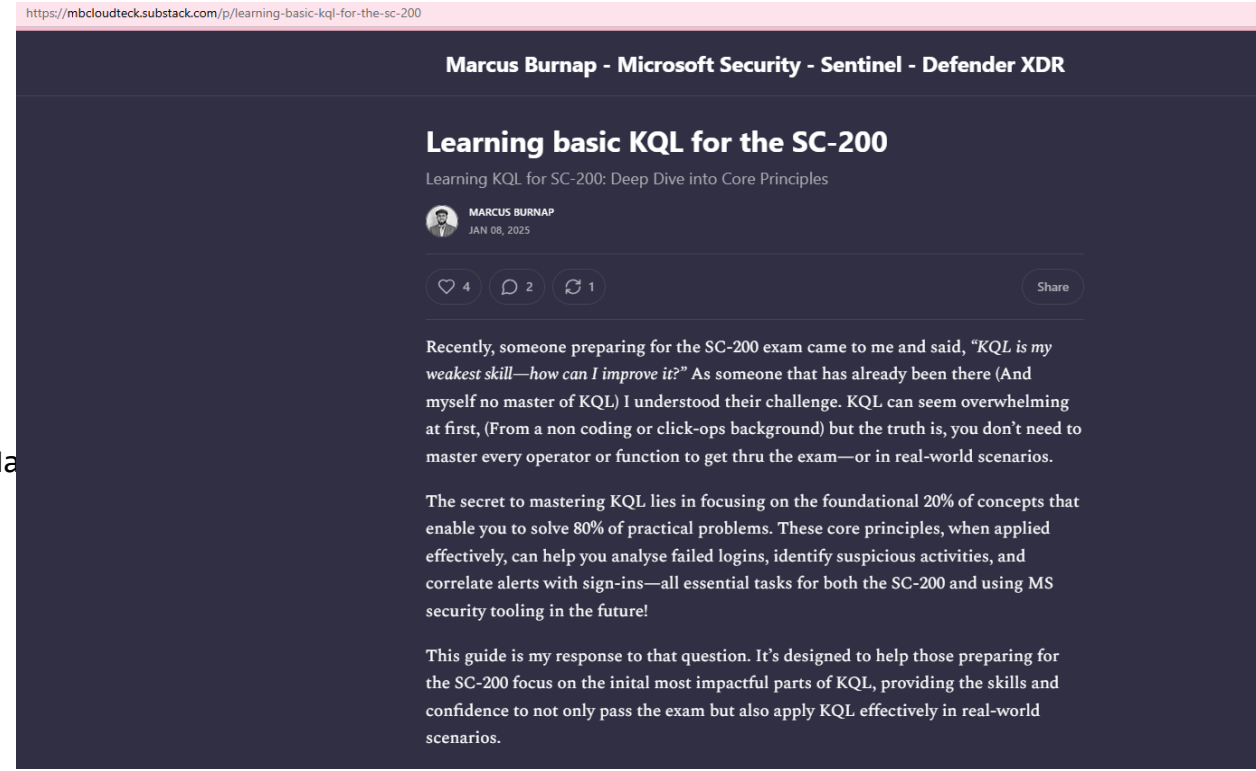
SquaredUp

TIKIT

Proactive hunting and incident response

Learning KQL

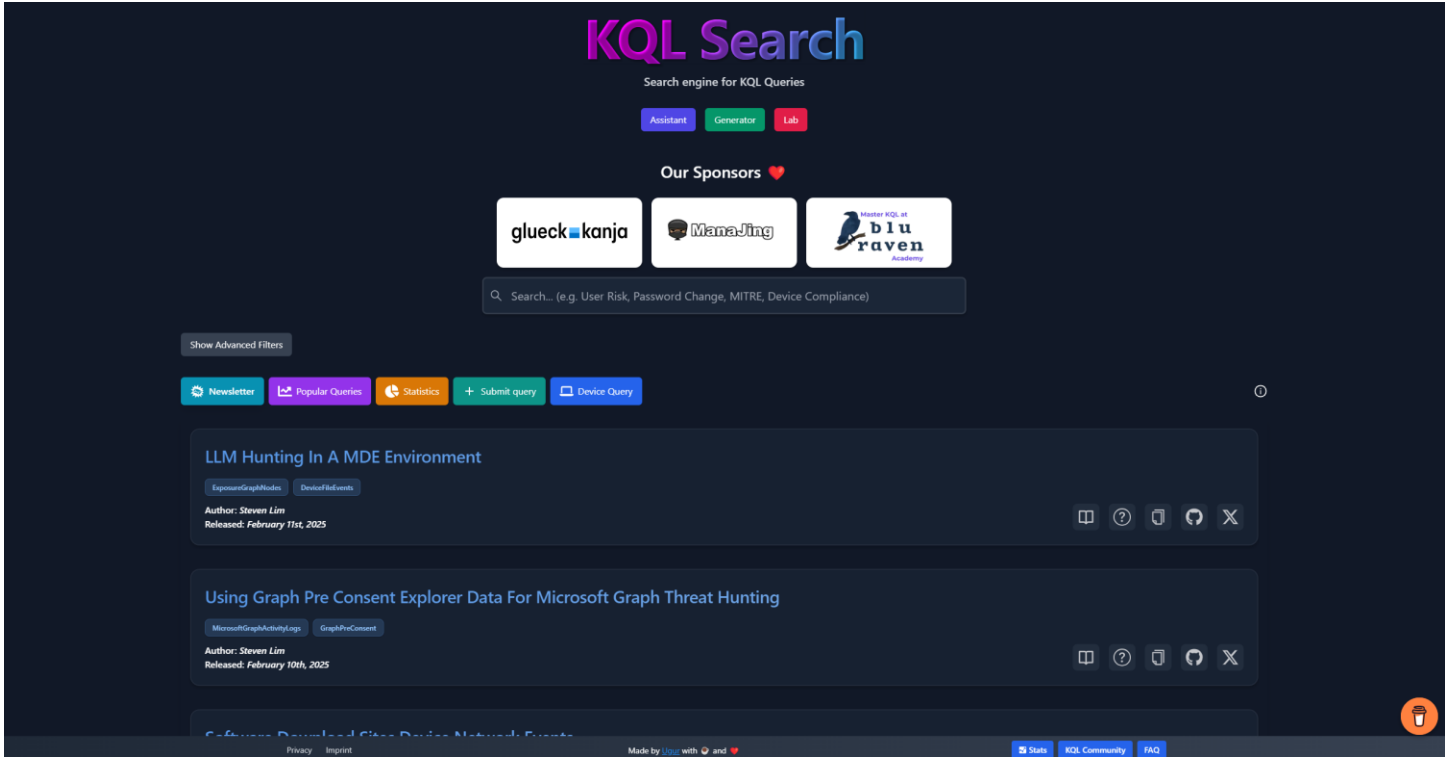
```
SecurityEvent
| where EventID == 4625
| project TimeGenerated, AccountNa
| order by TimeGenerated desc
```



SquaredUp

TIKIT

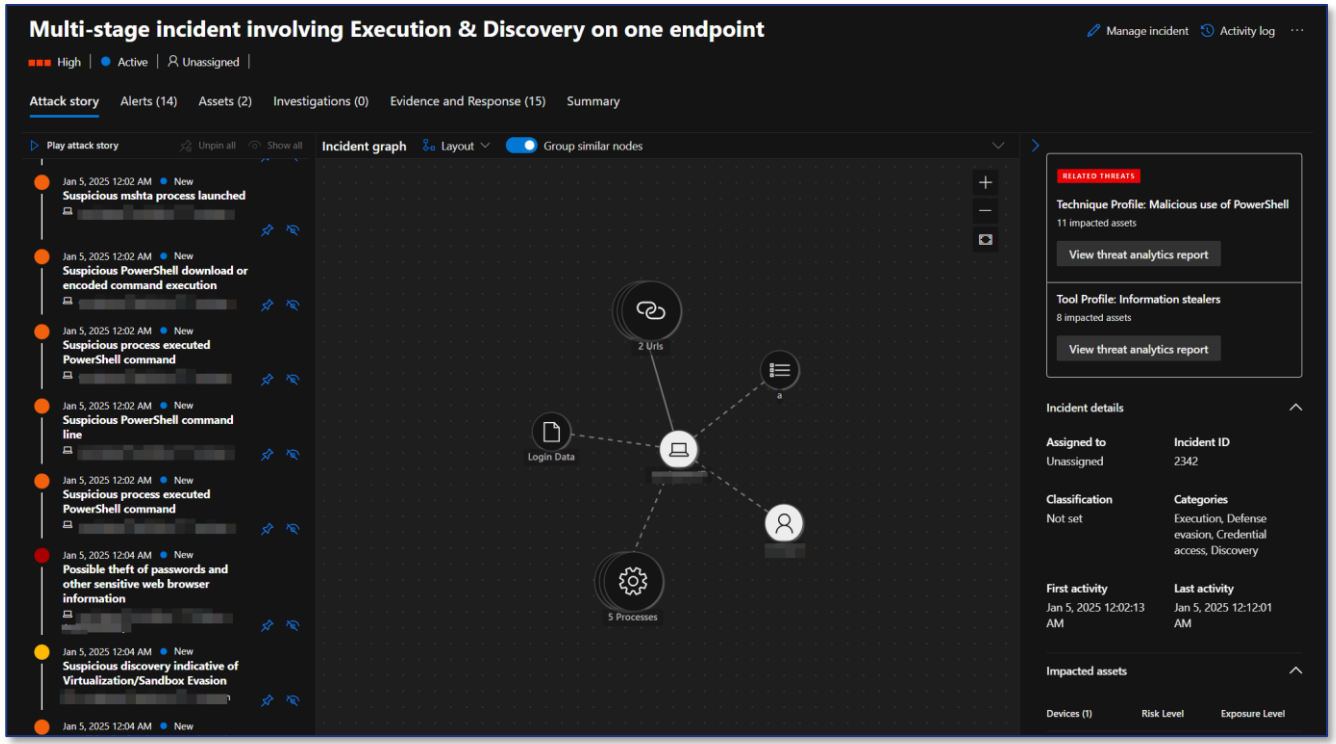
Proactive hunting and incident response

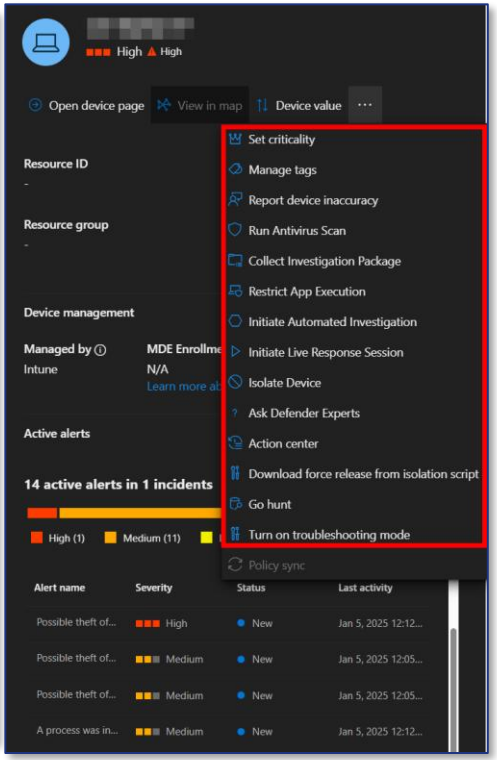


SquaredUp

TIKIT

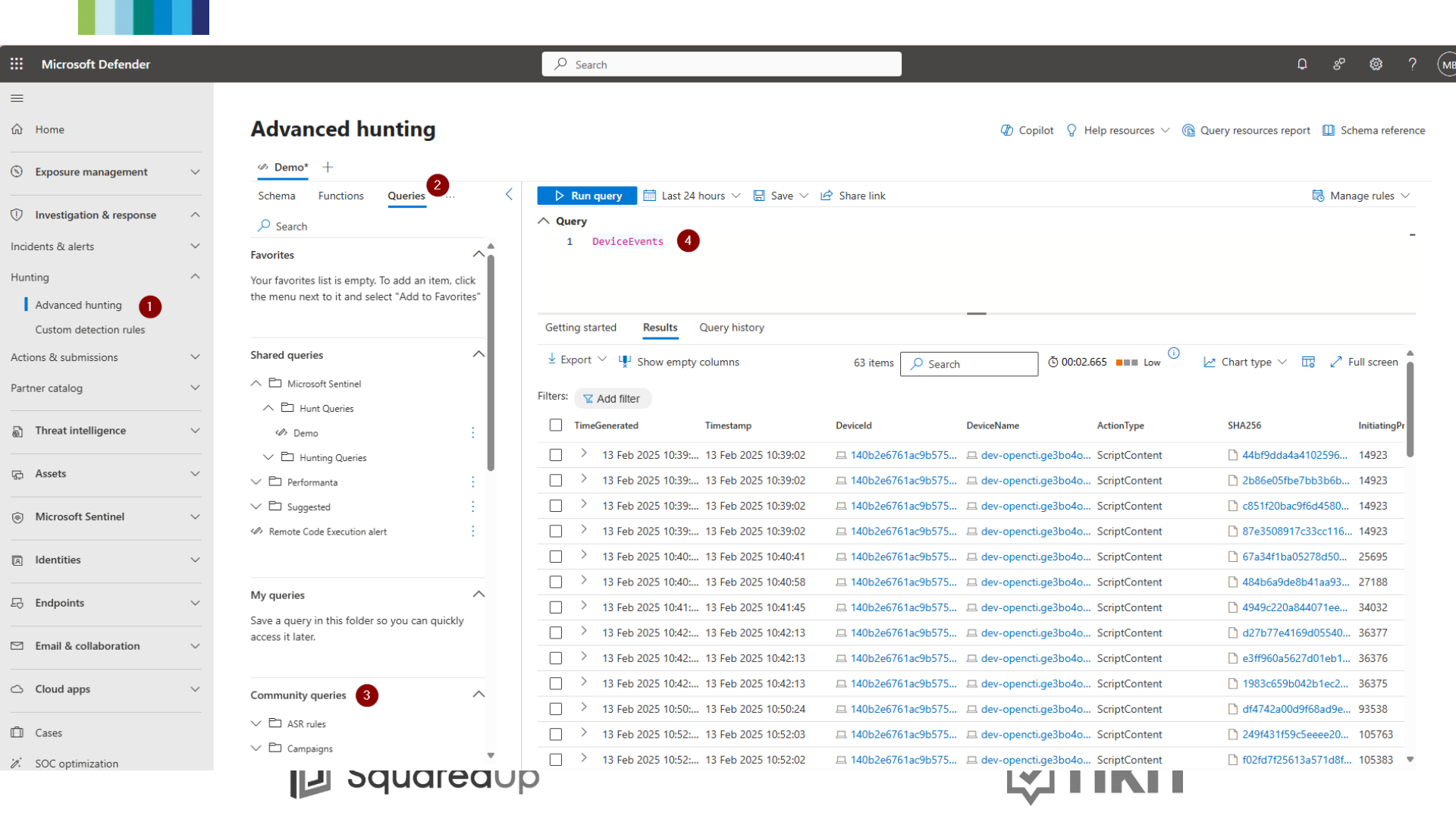
Proactive hunting and incident response





SquaredUp

TIKIT


Microsoft Defender
Search
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
Performanta
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
1 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
13 Feb 2025 10:39:... 13 Feb 2025 10:39:02 140b2e6761ac9b575... dev-opencti.ge3bo4o... ScriptContent 44bf9dda4a4102596... 14923
13 Feb 2025 10:39:... 13 Feb 2025 10:39:02 140b2e6761ac9b575... dev-opencti.ge3bo4o... ScriptContent 2b86e05fbe7bb3b6b... 14923
13 Feb 2025 10:39:... 13 Feb 2025 10:39:02 140b2e6761ac9b575... dev-opencti.ge3bo4o... ScriptContent c851f20bac9f6d4580... 14923
13 Feb 2025 10:39:... 13 Feb 2025 10:39:02 140b2e6761ac9b575... dev-opencti.ge3bo4o... ScriptContent 87e3508917c33cc116... 14923
13 Feb 2025 10:40:... 13 Feb 2025 10:40:41 140b2e6761ac9b575... dev-opencti.ge3bo4o... ScriptContent 67a34f1ba05278d50... 25695
13 Feb 2025 10:40:... 13 Feb 2025 10:40:58 140b2e6761ac9b575... dev-opencti.ge3bo4o... ScriptContent 484b6a9de8b41aa93... 27188
13 Feb 2025 10:41:... 13 Feb 2025 10:41:45 140b2e6761ac9b575... dev-opencti.ge3bo4o... ScriptContent 4949c220a844071ee... 34032
13 Feb 2025 10:42:... 13 Feb 2025 10:42:13 140b2e6761ac9b575... dev-opencti.ge3bo4o... ScriptContent d27b77e4169d05540... 36377
13 Feb 2025 10:42:... 13 Feb 2025 10:42:13 140b2e6761ac9b575... dev-opencti.ge3bo4o... ScriptContent e3ff960a5627d01eb1... 36376
13 Feb 2025 10:42:... 13 Feb 2025 10:42:13 140b2e6761ac9b575... dev-opencti.ge3bo4o... ScriptContent 1983c659b042b1ec2... 36375
13 Feb 2025 10:50:... 13 Feb 2025 10:50:24 140b2e6761ac9b575... dev-opencti.ge3bo4o... ScriptContent df4742a00d9f68ad9e... 93538
13 Feb 2025 10:52:... 13 Feb 2025 10:52:03 140b2e6761ac9b575... dev-opencti.ge3bo4o... ScriptContent 249f431f59c5eeee20... 105763
13 Feb 2025 10:52:... 13 Feb 2025 10:52:02 140b2e6761ac9b575... dev-opencti.ge3bo4o... ScriptContent f02fd7f25613a571d8f... 105383

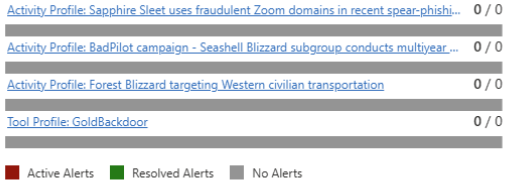
Home
Exposure management
Investigation & response
Incidents & alerts
Incidents
Alerts
Hunting
Advanced hunting
Custom detection rules
Actions & submissions
Partner catalog
Threat intelligence
Threat analytics
Intel management
Intel profiles
Intel explorer
Intel projects
Assets
Microsoft Sentinel
Identities

Threat analytics

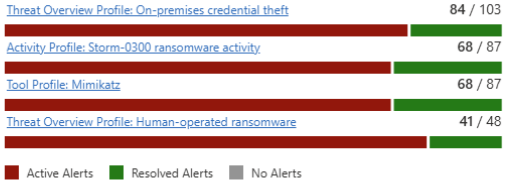
Copilot | Email notification settings | Help resources

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

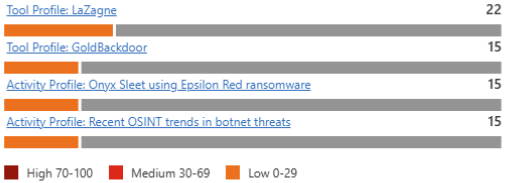
Latest threats



High-impact threats



Highest exposure threats



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	52 8	0 - Low	2	0	Tools & techniques	1 Feb 2024 17:21
Tool Profile: Mimikatz	68 active / 87	10 6	15 - Low	2	Not available	Tools & techniques	6 Jul 2023 15:17
Activity Profile: Storm-0300 ransomware activity	68 active / 87	10 6	15 - Low	2	Not available	Attack campaigns	9 Jan 2023 17:21
Threat Overview Profile: Human-operated ransomware	41 active / 48	6 3	15 - Low	2	Not available	Tools & techniques	13 Jul 2021 18:05
Technique Profile: Brute-force attacks	1 active / 1	41 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 - Low	Not available	Not available	Attack campaigns	12 Feb 2025 19:45

- 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

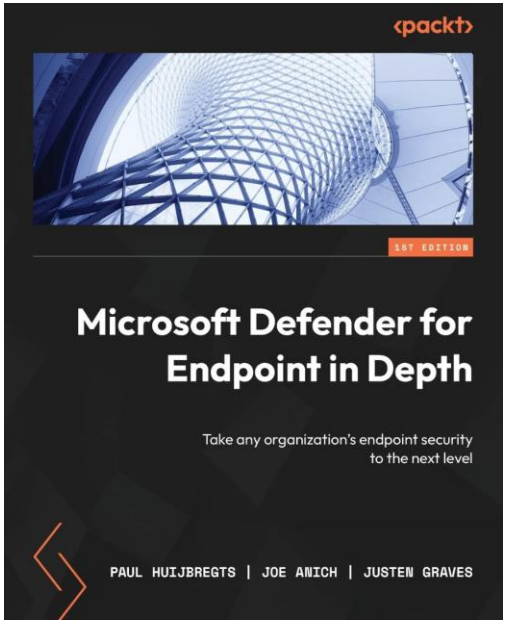
Resources

- 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

Experts Live UK

Win a copy of…

Microsoft Defender for Endpoint in Depth



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

SquaredUp

TIKIT