Huntress + Microsoft Defender

Get premium endpoint threat detection and response with Huntress and Microsoft

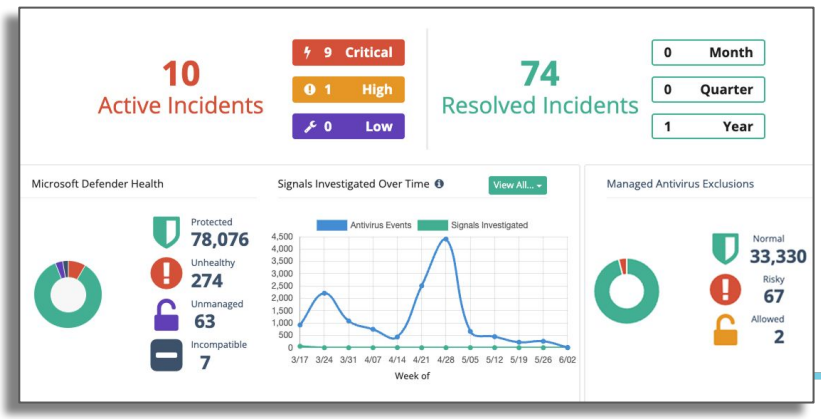
More Protection, Less Cost

Benefit From Your Investment in Huntress and Microsoft

Managed Defender Antivirus comes free with Huntress Managed EDR, enabling you to extract maximum value from Defender Antivirus, a built-in and often untapped Windows OS security tool. This enables you to save and re-invest more money back into your business.

Make Microsoft Defender for Endpoint More Actionable for Stronger Protection

Using Defender for Endpoint? The Huntress SOC investigates Defender for Endpoint alerts at scale across 12,000+ Huntress customers. We separate signal from noise, so you stop wasting time on false positives and only get actionable reports on confirmed threats. It's the power of Defender for Endpoint, minus the alert fatigue.



Key Benefits

Centralized Visibility
One location to see the health and status for all hosts.

Centralized Policy Management
For Defender AV, Huntress offers flexible configuration and policy compliance enforcement across all endpoints. Easily apply Huntress-recommended settings or your own.

Enjoy 24/7 Peace of Mind
Our 24/7 global SOC team has your back around the clock monitoring and responding to threats detected by Defender with an industry-leading 8 minute MTTR. Risky exclusions are also surfaced by the SOC to help reduce an endpoint's attack surface.

Assisted Remediation
Powered by the Huntress Platform, Assisted Remediation automates the execution of actions needed to contain and remediate threats.

Monitored Defender for Endpoint
When using Microsoft's premium endpoint protection solutions for Windows, macOS, and Linux, Huntress will monitor and respond to alerts as another source of threat detection at no additional charge.

HUNTRESS

Microsoft Defender Integration Comparison

	Delivery Method	Administration & Configuration	Visibility, Health, & Status	SOC Incident Triage
Microsoft Defender Antivirus	Uses the Huntress agent for data collection	Huntress has recommended configurations that can be easily implemented If other configurations are used, Huntress will evaluate configurations and flag risky exclusions we recommend changing	Huntress portal provides visibility into: – Defender AV signature status –policy compliance –Microsoft Defender Tamper Protection Status – task log – risky exclusions – Defender alerts – signals investigated by the Huntress SOC	Microsoft Defender Antivirus Critical and High Severity alerts are investigated and remediated by our 24/7 AI-assisted SOC for continuous protection
Microsoft Defender for Endpoint	Data collection is supported via an API integration with Microsoft	Huntress does not oversee the configuration of Microsoft Defender for Endpoint	Huntress portal provides visibility into: – status of MDE installation and whether permissions have been granted – alerts from Microsoft Defender – signals investigated by the Huntress SOC	Microsoft Defender for Endpoint Critical and High Severity alerts are investigated and remediated by our 24/7 AI-assisted SOC for continuous protection

Hear from peers who have saved time and money

> We've used Huntress for a couple of years now. Initially as a sort-of backup 'insurance policy' in case anything got past our existing Webroot AV, but now we've ditched Webroot altogether and use Defender + Huntress EDR as a more cost-effective and better performing package.
>
> Steve B | Verified G2 Review for Huntress Managed EDR

> Easy to deploy, leverages Windows Defender so we get simplicity, extra feature set and management for the same overall cost as comparable antivirus.
>
> Verified User, IT Professional | G2 Review for Huntress Managed EDR

HUNTRESS

Fully-managed, enterprise-grade endpoint threat detection and response.

Huntress Managed EDR

Persistent Footholds

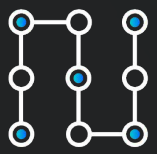
Eliminate persistent threats hiding in plain sight on Windows and macOS.

Malicious Process Behavior

Focus on behavioral analysis to identify and stop shady hacker activity.

Ransomware Canaries

Catch potential ransomware incidents early.



Lateral Movement

Detect attackers expanding through a network.

External Recon

Highlights external entry points to reduce your attack surface.

Threat Response

From immediate threat containment to active remediation to guided recovery, Huntress is there for you at every step.

Huntress By the Numbers

46%
EDR Customers Using Defender Antivirus

8 minute
Mean-time-to-respond

4.9/5
G2 Customer Rating

98.8%
Client Satisfaction

You deserve a next-level experience. Explore the ways Huntress protects *all* businesses. Start your free trial today at huntress.com/start-trial

HUNTRESS