HUNTRESS

Managed EDR

Discover the Power of Process Insights: Endpoint Detection and Response Backed by the Huntress 24/7 SOC

Gain deeper endpoint visibility and stop hackers in their tracks

- Built to filter out the noise and only deliver an incident report when a threat is verified, or action is needed.
- Easy for non-security professionals because the Huntress Security Operations Center team provides added context and instructions to remediate or take appropriate next steps.
- Designed around the core set of EDR capabilities insurance carriers are looking for.
- Harder for threats that have gotten past preventive measures to hide with continuous monitoring of process executions and associated metadata.
- Huntress' EDR technology collects targeted process data from endpoints without blocking or impeding any of your existing security tools.

> **“I always tell other companies that Huntress is what lets me sleep at night, this just proves it. Process Insights identified an attacker preparing to deploy malware and stopped what would have been a bad attack.”**
>
> **Dustin Bolander** | Owner at Clear Guidance Partners

Key Features

The Power of “Managed”

Say goodbye to false positives and massive alert queues. Our security experts investigate suspicious behavior, triage alerts and hunt hackers down—without putting any of that burden on your team.

Enhanced Threat Intelligence

Capture threat actor activity between initial access and eventual impact to get a complete picture of how hackers are targeting your protected endpoints.

Greater Endpoint Visibility

Identify actively exploited systems—including tracing back to cause—with granularity that makes it extremely hard for hackers to hide.

Near Real-Time Forensics

In the event of an incident, Huntress' SOC analysts will use Managed EDR to conduct near real-time forensics and hunt for threats in your protected network.

Cybersecurity Framework Alignment

Better understand threat actor behaviors and motives by mapping malicious or suspicious processes to popular cybersecurity frameworks.

Managed EDR In Action

1

Collect

The Huntress agent continuously captures process execution data directly from the endpoint, including but not limited to its privilege level, command line arguments and lineage.

2

Detect

Huntress applies custom-tuned detection logic to the data collected by our agent, making SOC Analysts aware of the suspicious activity that requires investigation.

3

Analyze

SOC Analysts dig deep into the continuous stream of data to confirm the activity is indeed malicious, greatly eliminating false positives.

4

Report

Our SOC will provide you with a custom incident report sharing our findings and outlining next steps. This can be delivered via email or ticketing system.

5

Remediate

You can execute the recommended automated remediation steps or get detailed instructions for additional work that should be completed.

6

Adapt

Threat intelligence gets fed back into our platform to become smarter over time and more effective at stopping previously unknown threats.

The Huntress Difference

Using our powerful Managed EDR functionality and its included features, Huntress will work alongside your IT and security team to detect, isolate, and remediate malicious threats across your endpoints, including persistent threats, antivirus evasion, ransomware, and more.

Persistent Footholds

Eliminate persistent threats hiding in plain sight on Windows and Mac. We monitor for malicious footholds, and when found, we deliver actionable recommendations and instructions for removal.

Managed Antivirus

Make the most of your frontline virus protection with Microsoft Defender, managed by Huntress. With centralized management and visibility, you can amplify your existing investments in Microsoft Defender and open up more options to strengthen your security stack.

Ransomware Canaries

Catching ransomware early is key. Like the old canary in the coal mine, Huntress enables faster and earlier detection of potential ransomware incidents to help you respond quicker and reduce the spread.

External Recon

Highlight external vulnerabilities to tighten perimeter defenses. Huntress gives you visibility into external attack surfaces by monitoring for potential exposures caused by open ports connected to remote desktop services, shadow IT, and more.

24/7 SOC Coverage

Unmatched human expertise in your back pocket. Our SOC team looks into potential threats, analyzes hacker tradecraft, creates incident reports, helps remediate cyber threats, and provides a degree of expertise and support that software-only solutions simply can't match.

**Start your
free trial today.**

HUNTRESS.COM