HUNTRESS

Huntress Security Platform

Accelerate Security Defense and Protect Your Clients

Huntress helps you accelerate your response to constantly evolving security challenges by tracking, isolating and remediating malicious activity that other tools miss.

The Power of Detection and Response

Attackers are constantly evolving, exploiting new vulnerabilities and successfully dwelling in network environments. There are countless examples of attackers evolving right around us, not waiting for us to evaluate options before making our next move.

The Huntress Security Platform enables faster response to this constant evolution by bringing an iterative approach to defenders. Leveraging powerful detection, response, and remediation capabilities, Huntress stops hackers in their tracks with technology built to catch activity that slips by preventive security measures. Our team of ThreatOps researchers investigate and analyze incidents in order to separate active threats from false positives and deliver actionable results.

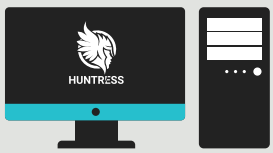
As threats evolve and needs change, the Huntress Platform will continuously add new detection and response capabilities to meet new security demands without requiring additional investment. By tearing down hurdles associated with procurement of new technology, Huntress makes it easier to adapt defenses to improve security posture and ultimately make it harder for attackers.

Key Features

- **Enhance your security stack** with advanced detection and response powered by ThreatOps
- **Remediate issues quickly** with easy to follow instructions (no advanced cybersecurity training needed)
- **Stay ahead of the curve** with continuous updates and new features at no additional cost
- **Deploy and manage easily** with lightweight agent and robust management integrations
- **Centralize management** with a multi-tenant dashboard

How Huntress Works

Install



Our agent automatically captures, collects, and sends data to our cloud for analysis of potential threats.

Analyze

Our automated engine performs initial analysis of the data collected by the agent. Then our ThreatOps team reviews the full context of that data to determine the classification and severity.

Remediate

When a threat is confirmed, a unique incident is delivered containing details and easy to follow instructions for eliminating or remediating the threat.

Focused Detection and Response

Malicious Footholds

At the core of the Huntress platform is our ability to identify malicious footholds. Footholds are persistence mechanisms attackers use to gain long-term access by exploiting commonly found Windows auto-start applications. By abusing these auto-start applications, attackers can slip by other security tools and remain undetected while planning their next move. Huntress monitors for footholds and delivers actionable instructions for removal. In addition, Assisted Remediation speeds recovery by simplifying your ability to respond and allowing you to approve automatic execution of recommended response actions.

Ransomware Canaries

Like the old canary in the coal mine, our Ransomware Canaries enable faster and earlier detection of potential ransomware incidents. When deployed, small lightweight files are placed on all protected endpoints—and if that file is modified or changed in any way, an investigation is immediately opened with our ThreatOps team to confirm whether those changes are the result of a ransomware attack or malicious encryption.

External Recon

Hackers are constantly looking for low-hanging fruit and commonly exploited “easy” entry points. External Recon gives you visibility into your external attack surface by monitoring exposed services. For example, remote desktop services (RDP) are common for system management, but purposefully having it exposed to the public Internet is much less common especially without hardened controls. Highlighting these external exposures informs decisions by telling you where to focus in improving your external security posture.

ThreatOps

ThreatOps is the backbone of what we deliver at Huntress. The reality is, threats change and new ones emerge all the time; automated engines alone cannot keep up. By using contextual clues in their investigation, our ThreatOps team has experience and expertise to recognize and piece together various indicators that make up a security incident. At the end of the day, their mission is to help you accelerate your incidence response by confirming each incident even before it hits your inbox along with easy-to-follow actions for remediation.

Managed Antivirus

By providing centralized management and visibility, Managed AV enables you to reclaim and amplify existing investment in Microsoft Defender Antivirus and open up more options to strengthen your security stack.

Your Huntress Partner is:

SIM2K
6330 E 75th St., Ste. 214
Indianapolis, IN 46250
317.251.7920 • www.sim2k.com
sales@sim2k.com

HUNTRESS