Where Huntress Fits into your Stack

1% of companies employ qualified threat hunters. 99% settle for security automation like antivirus. The ThreatOps team hunts for attacker persistence in Windows systems. Huntress is the missing piece that fits seamlessly into any cybersecurity stack.

Understanding Persistence

We all want that one tool that can act as a silver bullet to fix all of our problems; unfortunately, there's no such thing in the cybersecurity world. Effective security requires a layered approach to keep the cost of an attack high enough to avoid becoming the easiest target available.

There's one layer that has been widely ignored by defenders due to a lack of awareness, expertise, and understanding: **Persistence**.

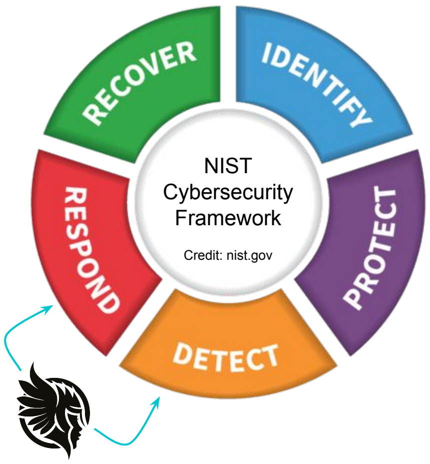
Attackers create persistence by adding, replacing, or hijacking legitimate auto-starting code in Windows systems. This is their top priority after initial access. Pretending to be a valid part of the OS renders security software useless allowing attacker to *Hide in Plain Sight*. Persistence enables attackers to dwell undetected for weeks and months and is the precursor to the payload in almost every targeted attack.

Detect and Respond to Persistent Threats

Since the inception of anti-virus in 1987, the cybersecurity industry has recycled the concept over and over to keep capturing customer budget. One look at the news illustrates the truth software vendors don't want you to understand:

If a bad actor is targeting you, automated safeguards alone won't stop them.
The 1% of companies who can afford it employ offensive security experts to constantly threat-hunt in their environments to detect and respond to attackers in real time.

Adding Huntress to any security stack provides managed threat hunting by security experts whose mission is to secure the 99%



> “ **Cyber threat hunters that are stealthier than the Russians must be unleashed on these networks to look for the hidden, persistent access controls. These information security professionals actively search for, isolate and remove advanced, malicious code that evades automated safeguards.**

Thomas Bossert
I Was the Homeland Security Adviser to Trump. We're Being Hacked.
- New York Times

Founded by Former NSA Cyber Operators. Backed By Cybersecurity Experts.
The Huntress founders are those cyber threat hunters that must be unleashed on these networks. Creating persistence on enemy targets was their mission during their 10+ year tenure on the most elite offensive cyber warfare team at the NSA. It was their task to remain undetectable by automation and dwell for years on the systems of their assigned targets. They've instilled that knowledge into the Huntress ThreatOps team to help companies like yours expel attacker's persistence mechanisms in minutes, instead of month after initial access.

> “ We are partnering with Huntress to fill a void that antivirus and our other security endpoint solutions have left open. The value and peace of mind that comes with their product cannot be overstated.

Jesse Roberts
Technical Services Manager
Dominant Systems Corporation

Where Huntress Fits

- **Adds threat hunting to find and expel** attackers' persistence in minutes instead of months after the fact
- **Doesn't interfere with the existing security stack** focusing on persistence in the OS layer
- **Compliments AV/NGAV** without conflict, interruption, high CPU utilization, or overlap
- **Simple to deploy, unnoticeable to users** with a lightweight agent (12Mb, under 2% CPU)
- **Augments Outsourced SOC, Managed SIEM/EDR** by focusing on persistent threats that can't be solved by the management of security software alone
- **Say “goodbye” to noisy alerts from false positives,** instead, expert incident analysis with actionable recommendations
- **Set it and forget it.** Unlike your traditional security tools, no fine-tuning required and reports are delivered to your inbox or ticketing tool
- **Continuous addition and iteration of new services at no additional cost** to keep up with constantly evolving threats
- **Affordable for any budget -** Add expert threat hunters to your team for less than the cost of most security software

What Does Huntress do?

HUNTRESS

ThreatOps

ThreatOps is the backbone of what we deliver at Huntress. You could call them our “SOC” but since they’re laser focused on hunting threats, ThreatOps is more appropriate…. (and it sounds cooler). Trained to hunt, investigate, reverse engineer, research, and discover persistence mechanisms by our founders, our ThreatOps team has the experience and expertise to recognize and piece together various indicators that make up a security incident. Threats change and new ones emerge all the time; automated engines alone cannot keep up. The ThreatOps mission is to hunt for and help you expel persistent attacks that otherwise would have gone unnoticed by your security software until after the payload was dropped.

Malicious Footholds

Huntress has its roots in hunting for malicious footholds. This is our core competency. This is what we do better than anyone. Footholds are persistence mechanisms that attackers use to gain long-term access by exploiting commonly found Windows auto-starting (persistent) applications. The Huntress agent is installed on Windows systems to create metadata from all persistent OS components (e.g. scheduled tasks, run keys, services, etc.), and sends them to the Huntress cloud for analysis. Automation analyzes and sorts the data collected by the Huntress agent. Then our ThreatOps team researches to determine whether any compromised or out of place auto-starting components are present. When a threat is identified and confirmed, a custom incident report is written and delivered that includes details and easy to follow instructions for eliminating or auto-remediating the threat via Assisted Remediation.

Assisted Remediation

An important feature of the Huntress for Malicious Footholds service is, Assisted Remediation. This is the easy-button. This feature allows you to review the ThreatOps teams’ remediation plan and approve with a single click the automatic removal of the malicious footholds by the Huntress agent, simplifying your ability to respond and enabling faster recovery.

External Recon

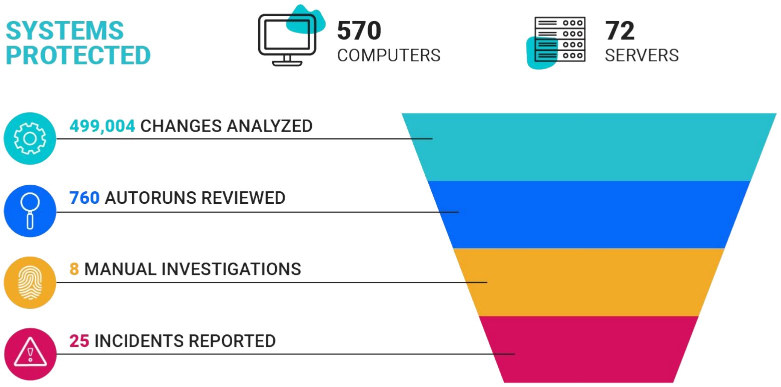
Over 50% of the time that organizations with under 1,000 employees are hit with ransomware, the initial access is an open RDP port. External recon scans for open ports (like RDP) based on the external IP of every agent, helping you become aware of common misconfigurations as they arise to minimize your threat landscape.

Ransomware Canaries

Some attacks occur without first creating persistence. Ransomware Canaries deliver faster detection of a ransomware incident to alert our customers to active outbreaks to speed the quarantine of the infected systems to mitigate the damage before it spreads.

Reports and Analytics

Threat reports help measure and justify the value of security to leaders and stakeholders. They showcase how our automated engines and our ThreatOps team work together to power our service and offer exactly what you need to address threats without the noise. In addition, these reports can be easily customized to match the brand of your organization.



SYSTEMS PROTECTED

570 COMPUTERS

72 SERVERS

499,004 CHANGES ANALYZED

760 AUTORUNS REVIEWED

8 MANUAL INVESTIGATIONS

25 INCIDENTS REPORTED

HUNTRESS

Discover the Huntress difference. Start your free 21-day trial today.

HUNTRESS.COM SALES@HUNTRESS.COM 1-833-HUNT-NOW