HUNTRESS

Datasheet

Managed Breach Detection
Hunting for Malicious Footholds

Huntress is a cloud-delivered managed breach detection service that hunts for threats by focusing on an indicator that is often overlooked—malicious footholds on the endpoint

What is a Malicious Foothold?

Traditional security products focus on keeping attackers out. But what happens when an attacker breaks through? In today's everchanging threat landscape, security experts are encouraging organizations to assume a compromise has already taken place.

Huntress was created with offensive security in mind. Attackers will continually pivot in order to find ways around preventive security, which takes effort and patience. As an attacker, what do you do once you finally gain access? You establish persistence, or a foothold, on a system in order to maintain your access long-term.

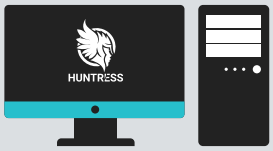
Footholds are created by leveraging common operating system features, such as services, scheduled tasks, and other persistence mechanisms. These mechanisms are used to routinely execute specific actions or applications when a computer boots up or a user logs in. A foothold is established when an attacker uses a persistence mechanism to run malware or perform some other malicious action, such as creating a backdoor account. Huntress monitors for footholds and when found, delivers actionable recommendations and instructions for removal.

Key Features

- **Simple to deploy and manage** with lightweight agent that uses less than 1% CPU and 20MB RAM at idle
- **Complements existing security stack** with focus on persistence
- **Integrates with leading business automation platforms** with more support continously being added
- **Expert analysis with actionable recommendations** that are easy to follow without extensive security training
- **Multi-tenant dashboard** for centralized management

How Huntress Works

1



The Huntress agent is installed on workstations and servers to collect and send metadata about persistent applications to the Huntress cloud for analysis.

2

Our automated engine performs initial analysis of the data. Then our ThreatOps team reviews the full context of that data to determine the classification which cannot be completely replicated through automation.

3

When a foothold is identified, a custom incident report is delivered that includes details and easy to follow instructions for eliminating the threat. Furthermore, these instructions can be automated with our Assisted Remediation feature.

> With Huntress, CloudJumper now has additional insight into possible footholds that could compromise the integrity of our solution. This coupled with the easy to follow actions for remediation provided by Huntress made this a clear cut win for improving our security posture to enhance the value we provide.
>
> **Richard Helms**
> Director of Managed Workspace
> CloudJumper

Simple Deployment

As a cloud-delivered solution, Huntress is extremely simple to deploy and manage. Installation involves pushing out a lightweight agent using automated deployment scripts. Furthermore, updates are automatically rolled out to enable new features and perform routine maintenance.

Huntress focuses on malicious footholds, a new indicator on the endpoint. This makes it slide into any security stack without any overlap of existing technology. There are no prerequisites; everything you need to start hunting is already included in the Huntress solution—including support.

ThreatOps

Threats change and new ones emerge all the time. Automated engines alone cannot keep up as attackers are always coming up with new methods to avoid detection. Our ThreatOps team sees new examples of this every day while reviewing thousands of new persistence mechanisms and hunting for malicious footholds. Our focus on persistent threats necessitates analysis by both automated engines and humans. This is where ThreatOps comes in—it is the backbone of what we deliver at Huntress.

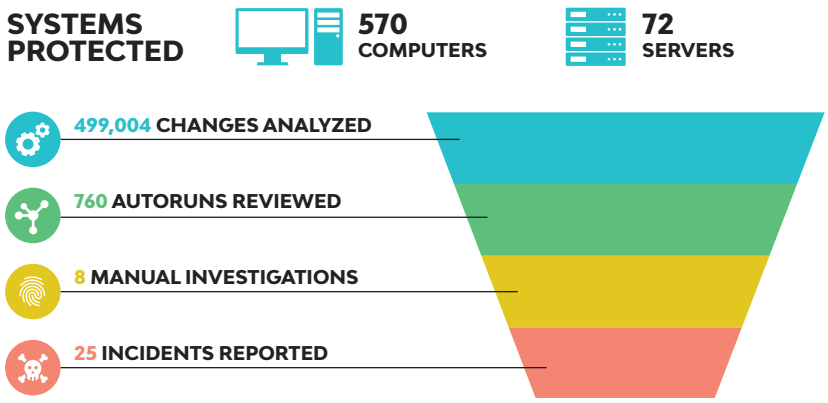
By using contextual clues in their investigations, our ThreatOps team has the experience and expertise to recognize and piece together various indicators that make up a malicious foothold. At the end of the day, their mission is to help you accelerate your incident response by confirming each incident even before it hits your inbox along with easy-to-follow instructions for remediation.

Assisted Remediation

Our remediation instructions are already simple to follow; we've taken it a step further with Assisted Remediation. When our ThreatOps team confirms a malicious foothold on one of your endpoints, they will generate an incident ticket that includes details about the threat as well as targeted actions for response. Assisted Remediation allows you to approve the automatic execution of these actions by the Huntress agent, simplifying your ability to respond and enabling faster recovery.

Monthly & Quarterly Reports

Our threat reports help measure and justify the value of security to your 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.



Huntress Labs
support@huntress.com
1 (833) 486-8669

Sign up for a free trial and learn more at huntress.com

HUNTRESS