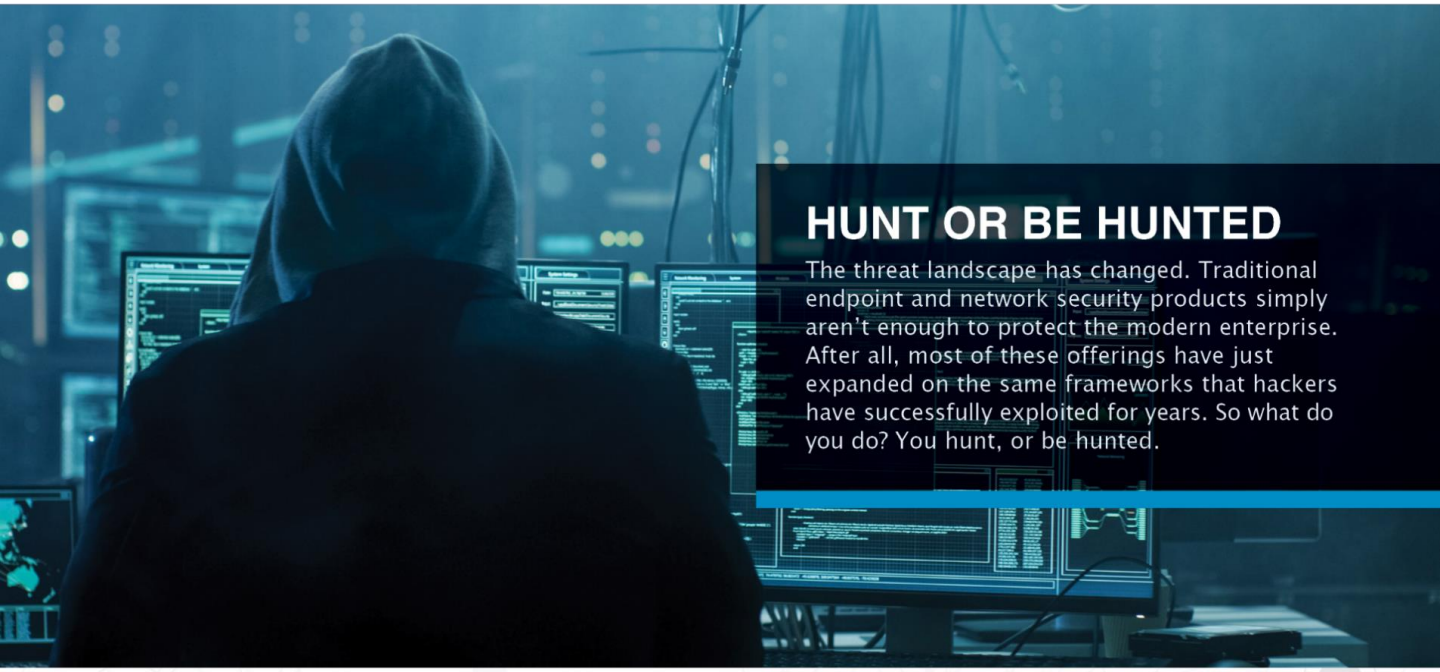
FLAGSHIP
MANAGED BREACH DETECTION

powered by HUNTRESS



HUNT OR BE HUNTED

The threat landscape has changed. Traditional endpoint and network security products simply aren't enough to protect the modern enterprise. After all, most of these offerings have just expanded on the same frameworks that hackers have successfully exploited for years. So what do you do? You hunt, or be hunted.

A Different Way

In a security environment that is ever changing, the best way to stay on top of potential threats is to start throwing punches. Huntress Labs' "collect-and-analyze" approach to active threat detection makes hackers earn every inch of their access. Working in tandem, our proprietary endpoint agent and U.S. based threat operations team significantly reduces the time to detection, allowing you to destroy malicious footholds as soon as they are created. It's an unbeatable combination: machine learning and tenured forensic security experts.

You Can't Afford Business as Usual

$11.7 MILLION
– the average estimated cost of cyber attacks to global firms per year[1]

$5 BILLION
– the estimated total damages of ransomware globally in 2017[2]

60%
– the portion of SMBs that took 30+ days to recover from a hack[3]

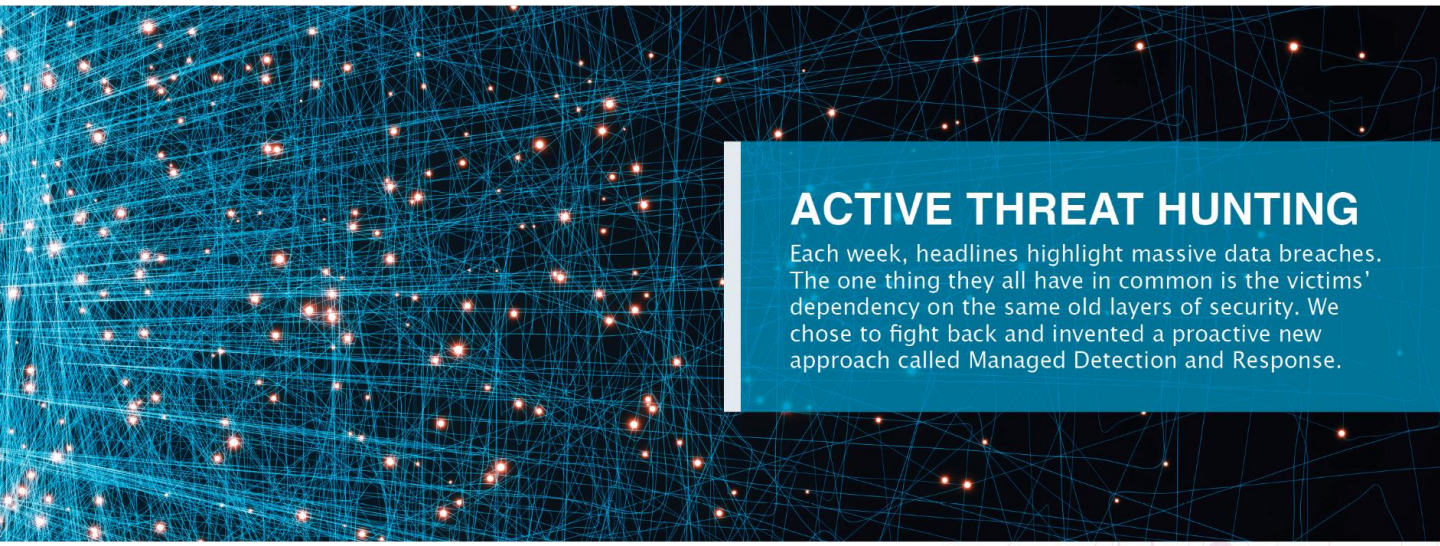
3X
– the rate at which the cyber crime epidemic will necessitate new IT security positions[4]

1 https://www.securitymagazine.com/articles/88338-cyber-crime-costs-117-million-per-business-annually
2 https://www.csoonline.com/article/3153707/security/top-5-cybersecurity-facts-figures-and-statistics-for-2017.html
3 https://www.darkreading.com/endpoint/most-small-businesses-lack-response-plan-for-hacks/d/d-id/1327181
4 https://www.csoonline.com/article/3200024/security/cybersecurity-labor-crunch-to-hit-35-million-unfilled-jobs-by-2021.html

FLAGSHIP

MANAGED BREACH DETECTION

powered by HUNTRESS



ACTIVE THREAT HUNTING

Each week, headlines highlight massive data breaches. The one thing they all have in common is the victims' dependency on the same old layers of security. We chose to fight back and invented a proactive new approach called Managed Detection and Response.

Why Does it Work?

Modern antivirus programs primarily detect malicious applications and behaviors using patterns, called heuristics and signatures, to identify known viruses. But in a threat landscape that is constantly evolving, does this strategy really work? It does…to a point. This is where Managed Detection and Response comes in.

Our industry-leading threat hunting solution complements your existing security stack to identify new and old footholds missed by antivirus, regardless of how your computers were compromised.

ADVANTAGE:
Huntress makes hackers earn every inch of their access within the networks we protect.

How Does it Work?

COLLECTION

1

Our endpoint agent collects a new type of indicator called "persistence mechanisms" from desktops, laptops, and servers. This data is then sent to our cloud-based analysis engine for deep inspection. Worried about productivity or data privacy? Don't be.

The agent's lightweight design ensures your users won't even notice that Huntress is constantly monitoring. As for your data, it's all encrypted—in transit and at rest.

ANALYSIS

2

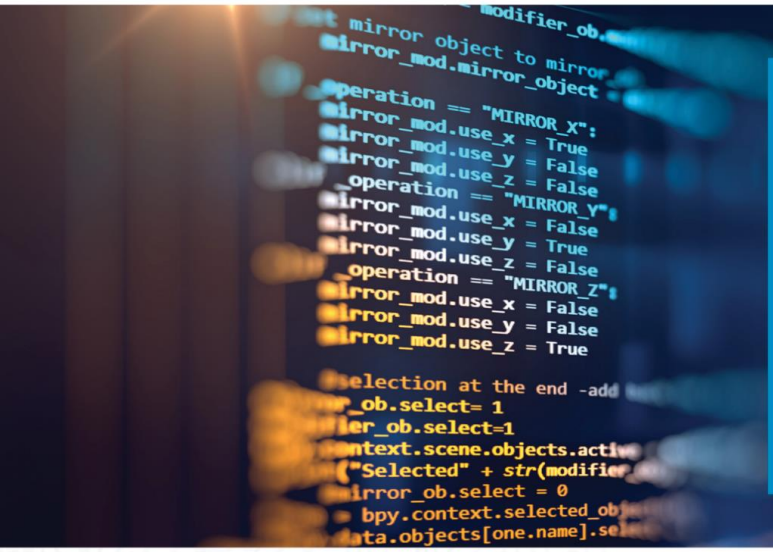
Once we receive the data, our analysis engine and threat operations team uses file reputation, frequency analysis, and machine learning to quickly hunt and investigate suspicious footholds.

When a threat is detected, Huntress delivers more than an alert. Your IT Staff receives step-by-step recommendations to prioritize the threat, remediate the incident, and address the root cause.

FLAGSHIP

MANAGED BREACH DETECTION

powered by HUNTRESS



DEFENSE REIMAGINED

There's no getting around it: cyber attackers are growing increasingly sophisticated in their tactics. From web apps and operating systems to hardware and human error, today's hackers leave no potential vulnerability unchecked. But that's why you have antivirus, right? Not so fast.

If recent headlines have taught us anything, it's this: A determined hacker can bypass even the most robust security program. So what should an organization do? The answer is simple: layer your defenses to address the gaps in your strategy.

Defense in Depth

Developed by former NSA cyberwarfare operators, our managed detection and response service represents a new layer in the security stack. Combining automated collection tools with expert analysis, our team actively hunts down threats that may have slipped past other layers of protection. On a daily basis, this new approach uncovers hackers abusing trusted applications and built-in Windows features to evade defenses for months.

Designed to complement your existing security strategy, Huntress analyzes the overlooked methods attackers use to persist within your network. Our managed detection and response service allows you to address these gaps, stopping advanced threats and cutting-edge malware in their tracks. This defense-in-depth model reduces time to detection and provides more comprehensive protection for your organization's IT assets.

Are You Covered?

	Antivirus	Huntress
Monitors Application Behavior	▬	
Protects Users Without Interruptions	▬	▬
Prevents Known Malicious Threats	▬	
Minimizes Risk of Downtime & Data Loss	▬	▬
Proactively Hunts Anomalous Threats		▬
Triages Events with Human Analysts		▬
Prioritizes Alerts with Business Context		▬
Delivers Resilience & Remediation Guidance		▬

FLAGSHIP

MANAGED BREACH DETECTION

powered by HUNTRESS

FIGHT BACK

It seems like every week another major corporation announces a large-scale security breach. For IT Managers, it's a concern that is requiring an increasing amount of time—and it's not a problem that is limited to Fortune 500 companies.

In the past, cyber attackers typically targeted a single large organization with the hopes of landing one significant payout. Today, hackers are more strategic. They distribute their efforts, targeting a number of smaller firms in order to yield multiple smaller payouts—and it's a system that is working. So what do you do about it? Easy. You take the fight to them.

Hit First

Traditional enterprise security products focus on keeping hackers out. But what happens when someone breaks through? In today's ever-changing threat landscape, security experts are encouraging organizations to assume that a compromise has already taken place. That's where Huntress comes in. Developed by ex-NSA hackers, our Managed Detection and Response service augments your existing security stack by proactively seeking out potential footholds and persistence methods.

The process is simple. First, our lightweight endpoint agent will gather data and submit it to our cloud for analysis. From there, our highly skilled team and algorithms will review the data to identify any potential threats. If a breach is detected, we'll provide your IT Staff with an actionable report, along with step-by-step instructions to remediate the threat.

The best part? Your team won't need any specialized (and costly) training.

Why Huntress Labs?

Operated by Operators

Our threat operations team is comprised of former penetration testers and reverse engineers with over a decade of advanced forensic security experience.

Plays Well With Others

Our active threat hunting system works seamlessly with your current security stack.

We Do The Heavy Lifting

Our algorithms and experts actively hunt for hackers, identifying and reporting their footholds and persistence methods.

Turnkey Remediation

When a threat is detected, you'll receive step-by-step instructions that tell you how to eliminate it once and for all.

Deploy in Minutes

Our partners have deployed Huntress to THOUSANDS of clients in less than 10 minutes using their existing RMM software.