



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.