# A New Approach

TECHNOLOGY PARTNERS
manage • protect • monitor • care

HUNTRESS

# ACTIVE THREAT HUNTING

## Why Does it Work?

Modern antivirus programs primarily focus on signatures, definitions, and heuristics. From there, they look for patterns to identify known viruses. But in a threat landscape that is constantly evolving, does this strategy really work? It does…to a point. That's where managed detection and response comes in.

Our industry-leading threat hunting tool complements your existing security stack to identify new footholds, regardless of the infection vector.

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

## How Does it Work?

### COLLECTION

1

Our lightweight endpoint agent collects data from desktops, laptops, and servers. This data is then sent to the Huntress Analysis Engine for inspection. Worried about productivity? Don't be.

The agent's lightweight design ensures that your users won't even notice that Huntress is working.

### ANALYSIS

2

Once we receive the data, our analysis engine uses algorithms and machine learning to proactively hunt footholds and investigate suspicious persistence methods. Each process is evaluated using a combination of file reputation, frequency analysis, and other proprietary algorithms.

When a threat is detected, Huntress delivers prioritized remediation recommendations to you and all other affected users.

**Defying Offense. Inspiring Defense.** | Visit huntresslabs.com to learn more.