

Huntress

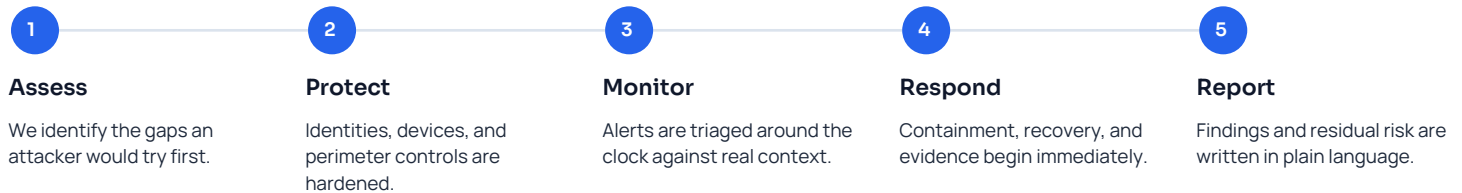
Managed endpoint detection and response.



Most organizations cannot staff a security operations center around the clock — but attackers do not keep business hours. Massive IT deploys and manages the Huntress platform so our customers get enterprise-grade threat detection and response, backed by the Huntress 24/7 AI-assisted SOC, without hiring a single security analyst.

Service illustration • Cybersecurity

A clear path to delivery



Product areas & practical applications

Product area	Practical application
Huntress Managed EDR	endpoint detection and response for workstations and servers, with 24/7 threat hunting, active remediation, and managed antivirus included
Huntress Managed ITDR	identity threat detection and response for Microsoft 365 and Google Workspace, catching account takeover, privilege escalation, and malicious inbox rules
Huntress Managed SIEM	log collection and correlation across endpoints, firewalls, cloud, and SaaS apps with simple per-source pricing
Huntress Managed SAT	security awareness training and phishing simulations built from real threat intelligence, managed for you

When to talk to us

- Ransomware and malware that slips past traditional antivirus
- Business email compromise and Microsoft 365 account takeover
- No after-hours coverage — alerts that sit unread until Monday morning

Deployment & ongoing support

Massive IT is a Huntress partner. We handle deployment, tuning, and day-to-day management of the platform, and we act on what the Huntress SOC finds — isolating endpoints, remediating threats, and closing identity gaps. When an incident escalates, our engineers work the problem alongside Huntress analysts so nothing falls between vendors.

Scope and licensing vary by environment. Product availability and support terms are confirmed during planning.