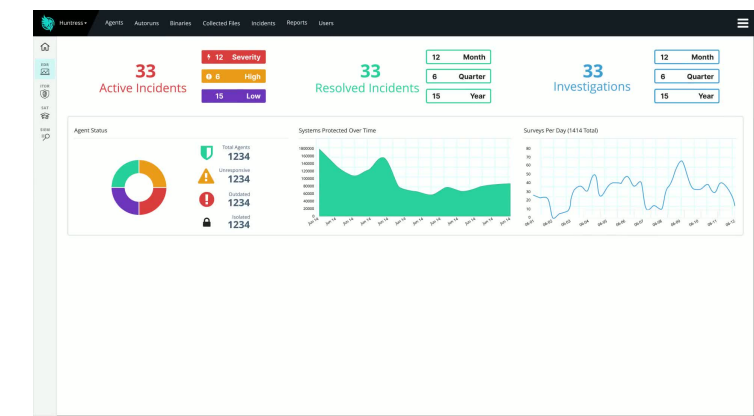


Managed Detection & Response

Keep devices well managed and add human-led threat detection with Huntress Managed EDR. Endpoint maintenance and threat response work together, rather than leaving your team to interpret alerts alone.



Huntress dashboard sample - Not live customer data

Technology + human expertise

24/7 Huntress SOC

Human-led investigation backed by threat hunters and AI-assisted operations.

Investigate, then act

Endpoint signals become incident context, containment, and remediation guidance.

Coexists with antivirus

Works alongside existing antivirus, including Microsoft Defender; validate your configuration.

A clear response workflow

1
Deploy

Review device inventory, supported systems, existing antivirus, and rollout requirements.

2
Detect

The Huntress agent collects security signals and looks for suspicious activity.

3
Investigate

Huntress's 24/7 SOC investigates threats and adds context to incidents.

4
Respond

Contain threats and coordinate documented remediation and follow-up.

Two complementary layers of protection

Responsibility	Endpoint management	Huntress Managed EDR
Device inventory & maintenance	Know which devices exist and manage configuration, updates, and lifecycle.	Adds security telemetry to help investigate endpoint activity.
Prevention & detection	Antivirus and device policies provide preventive controls.	Looks for attacker behavior that warrants deeper investigation.
Alert ownership	Management alerts identify device and operational issues.	Huntress's 24/7 SOC investigates potential security incidents.
Response & follow-up	Support restores normal device operation and addresses configuration needs.	Containment, remediation guidance, and incident context inform recovery.

Before rollout

Confirm device inventory, OS eligibility, licensing, existing antivirus, response permissions, and who owns escalation and follow-up. Windows, macOS, and Linux support is subject to current product eligibility.

Huntress product capabilities are described from its Managed EDR page. Your Massive IT scope, platform eligibility, licensing, response permissions, and escalation responsibilities are confirmed in your agreement. No prevention or resolution guarantee.

CYBERSECURITY

Managed Detection and Response: a closer look

Around-the-clock detection, investigation, and response to threats across your environment.

From challenge to coverage

SIGNS IT IS TIME TO ACT

- 1 Increasingly targeted phishing and ransomware attacks
- 2 Limited visibility into endpoint and identity threats
- 3 Pressure from insurers, clients, and regulators
- 4 Uncertainty about where the biggest risks are

WHAT THE SERVICE COVERS

- Continuous threat detection and response
- Email and identity protection
- Vulnerability identification and remediation tracking
- User awareness training
- Incident response planning

Detection and response need more than an agent

Area	What we review	Why it matters
Coverage	Huntress deployment and supported endpoint visibility	Identify devices outside the agreed detection scope.
Investigation	Alert context, affected users and response authority	Separate suspicious signals from incidents requiring action.
Response	Containment approvals, escalation and recovery handoffs	Clarify what the managed service handles and what is separately scoped.

A self-reported coverage score does not validate threat detection or guarantee protection.

How an engagement runs

01

Discover

Review the current environment, priorities and constraints with your team.

02

Plan

Agree scope, owners, timing and how success will be reviewed.

03

Deliver

Carry out the agreed work with documented changes and checkpoints.

04

Review

Revisit results, open items and next priorities on an agreed cadence.

What good looks like

The results this service is designed to support. Actual results depend on your environment and the agreed scope.

Reduced likelihood and impact of incidents

Clear visibility into security posture

Better-prepared employees

Evidence to support insurance and audit requests

Questions clients ask

Do you guarantee we will never be breached?

No responsible provider can. Our focus is reducing risk, detecting threats early, and responding quickly.

Can you assess our current security?

Yes. A security assessment is often the best first step to prioritize investments.

Your next step

[Free self-assessment](#)

Endpoint & Identity Coverage

See gaps across devices and sign-ins.

massiveit.com/endpoint-assessment

[Talk to an engineer](#)

Book a consultation

Walk through your environment and get a scoped recommendation.

massiveit.com/consultation • (813) 518-5454

RELATED CYBERSECURITY SERVICES

Endpoint Detection and Response • Email Security • Security Awareness Training • Vulnerability Management • Security Assessments • Penetration Testing

Scope, licensing and service levels vary by environment and are confirmed in your agreement. This overview describes typical engagements, not guaranteed results.