Huntress EDR & ITDR — 24×7 SOC Managed Security

Huntress Endpoint Detection & Response (EDR) and Identity Threat Detection & Response (ITDR) deliver enterprise grade protection designed to stop advanced threats before they cause damage. Backed by a 24×7 Human Centric with AI assisted Security Operations Center (SOC), your endpoints and identities are continuously monitored by expert analysts who validate alerts and coordinate rapid remediation. Twin Technology deploys, manages, and optimizes Huntress across your environment—keeping your business secure, compliant, and resilient.

Key Benefits

SOC

Human Centric Monitored 24×7 includes AI Assisted SOC
Continuous threat hunting, alert validation, and rapid response by Huntress' global SOC.

EDR

Definitive Endpoint Protection
Detect and isolate malicious activity, persistent footholds, and ransomware behaviors across Windows, macOS, and Linux.

ID

Identity Threat Defense
Shut down account takeover, credential theft, session hijacking, rogue OAuth apps, and BEC attempts.

MGT

Managed by Twin Technology
End-to-end deployment, tuning, reporting, and remediation guidance tailored to your environment.

FP

Low Noise
High-confidence, SOC validated alerts reduce false positives and alert fatigue.

SLA

Fast Response
Industry leading time to respond with clear, actionable steps and one click approvals.

What We Protect

Endpoints	Stops malware, targeted attacks, and persistence. Real time detection, isolation, and remediation with SOC validated alerts only.
Identities	Detects suspicious logins, MFA bypass, stolen session tokens, rogue apps, and shadow inbox rules to prevent account takeover and BEC.
Cloud & Email	Monitors Microsoft 365 tenants for risky app consents, abnormal access, and inbox manipulation. Integrates with Microsoft Defender.
Visibility & Reporting	Clear incident reports, prioritized remediation, monthly health summaries, and executive ready metrics.

Service Deliverables (Twin Technology)

• Onboarding & deployment of Huntress EDR and ITDR agents/tenants
• 24×7 monitoring with SOC validated alerts and incident handling
• Threat containment, guided remediation, and change coordination
• Microsoft 365 & Defender integration and policy optimization
• Monthly security reporting and executive summaries
• Proactive hardening recommendations and roadmap reviews

Proof Points

• <1% false positive rate (EDR)

• 8 minute MTTR (EDR)

• Near realtime EDR with SOC

• Identity protections: session hijacking, rogue OAuth, credential theft

References