Huntress Managed SIEM

Managed threat investigation, response, and robust compliance support, all at a predictable price.

SIEM providers talk a big game.

The promise: a single pane of glass, actionable visibility, and improved compliance and security posture.

The reality: complexity, noise, and unpredictable cost.

Simply put, SIEM is out of reach for most organizations Or, it used to be.

Huntress Managed SIEM changes the game by combining 24/7 threat response, fully owned technology, and predictable pricing to give you everything you need from SIEM—and nothing you don't.

Our expert SOC analysts help you find and neutralize threats earlier in the attack chain while our proprietary Smart Filtering Engine captures only the security data that matters, cutting out noise and unnecessary costs. Fully managed for you, it gives you long-term log retention, intuitive search, and clear reporting needed to speed investigations and be audit-ready without the stress.

Huntress Managed SIEM makes powerful threat response and robust compliance support accessible to everyone—without the big budget, big team, or big headaches that come with traditional SIEMs.

Key Outcomes

Reap the Rewards Without the Hassle
Save your precious resources for your top priorities. Let our experts handle the daily ins and outs of SIEM management.

Capture the Data That *Actually* Matters
Not all data is created equal. Collect what you need for security and compliance, and pay for nothing you don't.

Expose Hidden Attackers
Hackers rely on blending in. Uncover even the most concealed threats and hunt them down with Huntress SOC experts.

Stay Compliant
Show proof to regulators, third parties, and insurers that your security obligations are met.
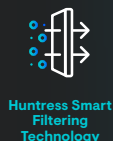
Control Costs and Eliminate Surprises
You get transparent, predictable pricing and the best return on your security investment.

Huntress 24/7 Human-Led SOC

Signal Ingest

Huntress Smart Filtering Technology
Security Relevant Data Capture
Normalization
Enrichment

Investigation & Threat Hunting
Intuitive Search of Indexed Storage
Data Rehydration from Cold Storage
SOC-Led Threat Hunting
Enhanced SOC Investigations for EDR & ITDR

Response
24/7/365 Monitoring
Malicious Threat Detection
Validation & False Positive Reduction
SOC-Generated Incident Reports

Compliance
Secure Data Storage
1 & 7 Year Retention
On-Demand Reporting

All the Benefits. None of the BS.
Fast Deployment
Fully Managed by Experts – Tuning, Optimization, Support
Predictable Billing & Cost Control

Huntress Managed Security Platform
Health Dashboard   Management Console   Data Reporting

HUNTRESS®

A Smarter Approach to SIEM

Don't get caught up in the old SIEM model that drowns you in complexity while sending your budget up in smoke. Huntress Managed SIEM removes complexity, cuts costs, and gives you real outcomes from your security and event data.

	Compliance	Investigation	Response	Cost Control	Ease of Use
Huntress	✅ Supports the requirements set by regulators, insurers, and third parties without breaking the bank.	✅ The Huntress SOC investigates to uncover risks that need attention like RDP brute force attempts and lateral movement.	✅ The Huntress SOC detects and remediates for you 24/7, delivering incident reports and fast resolution to confirmed threats.	✅ Ingests only relevant security data to slash data storage costs without compromising security visibility.	✅ Puts a team of experts in your corner day and night so you get all the benefits of SIEM without the burden.
Old School Solutions	❌ Checks the compliance box but struggles to deliver any other value, all while you're stuck with a big bill.	❌ Forces you to sift through noise to investigate and hunt yourself, so it's easy to miss threats.	❌ Makes you work nights and weekends to remediate threats and sort through false positives to find them.	❌ Hits you with confusing and inflexible pricing models that run up fees and become unsustainable for your business.	❌ Drowns overstretched teams in an endless tide of alerts and tasks, leading to burnout before you see any payoff.

> "With breaches in the past, we had to bring in an external team, install their tools, and wait for results. This time around, Managed SIEM handled it all. We told the SOC what we needed, ran a quick query, and immediately got clear answers."
>
> Dan Paquette, Managing Partner at Key Methods

Start your free trial today.

𝕏 in ▶ f

HUNTRESS