



Power the Next Generation of Managed Security Services with Splunk

The security landscape is shifting. As complexity grows and data volumes increase, managed service providers (MSPs) like you support customers dealing with a surge in alert fatigue, data silos, and AI-driven threats.

Splunk Enterprise Security (ES) isn't just another tool to manage: It is the high-performance engine that can power your existing managed security services portfolio. By integrating Splunk ES as an option in your current portfolio, you gain a unified, AI-powered security operations (SecOps) platform. It allows you to deliver superior security outcomes, differentiate your brand, and capture the high-end enterprise market that requires more than just standard log management.

Your MSP expertise and customer reach already set you apart. Add Splunk capabilities in security information and event management (SIEM), security

orchestration, automation, and response (SOAR), user and entity behavior analytics (UEBA), and threat intelligence, and you can offer a range of security services — from basic to premium. Each service can be tailored to your customers' specific needs.

Unified visibility and data access enable more use cases to help MSPs create flexible managed security solutions customized to a wide array of industries and customers. By leveraging the combined power of Splunk and Cisco, you gain access to a full-stack security architecture — from network to endpoint to data — that is easier to sell, deploy, and manage as a comprehensive, unified offering.

Ready to capture more market share and deliver higher-value managed services? Splunk is the launch pad to get you there.

Challenge

Reduce risk and untangle complexity for your customers

With rising customer expectations, and an ever-evolving threat landscape driven by AI, 78% of security leaders surveyed in the [Splunk State of Security 2025](#) report said they are struggling with dispersed and disconnected tools.

Bloated and disjointed tech stacks — either on the customer end or the MSP side — limit scalability and hinder models needed to extend security coverage across hybrid environments.

Swiveling between too many tools slows threat detection, investigation, and response (TDIR) and increases risk for both service providers and their customers.

Security innovation suffers, and customers can't evolve past basic detection to advanced services like observability. Compliance efforts to meet regulatory requirements and certification cycles may further strain resources.

Solution

Scale your managed security delivery

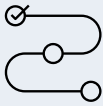
Splunk ES addresses critical SecOps challenges and helps MSPs deliver the next era of managed security services.

- **AI-powered efficiency:** Security operations center (SOC) teams are often understaffed. Embedded AI and automation in Splunk ES help analysts handle more complex investigations with less manual effort. This drives operational efficiency, enabling you to scale your business and drive value for your customers without the need for linear headcount growth.
- **Flexible service options:** The flexible Splunk platform supports tiered managed security services, helping you move customers from basic monitoring to high-value, strategic partnerships. Your customers can explore the following tiers:
 - **Basic:** Co-managed monitoring (with standardized reporting and correlation)
 - **Advanced:** Managed detection and response (MDR) with automated alerting
 - **Strategic:** Co-managed SOC with pre-approved remedial action capabilities: vulnerability management, digital forensics, and compliance
- **Architectural flexibility:** Your customers operate across cloud, on-premises, and hybrid environments. Splunk enables you to ingest and secure data anywhere, without costly replatforming or duplicate data ingestion.
- **The “a-la-carte” upsell:** Once the platform is established, you can offer specialized services like digital forensics, penetration testing, or National Institute of Standards and Technology (NIST)-aligned compliance reporting to customers as they mature, creating continuous upsell opportunities without needing a full-service redesign.

Splunk has been named a **Leader in the Gartner® Magic Quadrant™** for security information and event management 11 consecutive times.

Core use cases for scalable, high-value service delivery

To support these tiers, Splunk ES offers the following use cases that streamline your delivery and enhance your value proposition:



Managed detection and response:

Standardize SOC delivery. With pre-built correlations and streamlined workflows in Splunk you can reduce triage time and deliver consistent, high-fidelity alerting at scale.



Splunk SIEM as a managed service:

Deliver continuous monitoring and actionable security insights. Equip your analysts to make proactive decisions and speed TDIR instead of fighting a deluge of alerts.



Integrated threat intelligence:

Monetize security context. Correlating Cisco Talos and Splunk threat intelligence with your customers' unique data lets you offer a premium intelligence tier that provides faster, more accurate incident prioritization.



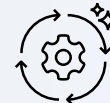
Comprehensive anomaly detection:

UEBA in Splunk uses machine learning (ML) to baseline normal behavior, automatically surfacing anomalies without the need for constant, manual rule tuning.



Proactive threat hunting with agentic AI:

Move from reactive to proactive. Use agentic AI to automate the creation of playbooks to test hypotheses, allowing you to provide proactive security outcomes that differentiate your practice.



Automation for operational excellence:

Turn expertise into an asset. Build your standard operating procedures into Splunk SOAR playbooks once and continuously deploy them across your portfolio to slash response times and focus your analysts on critical work.

Build a better managed security business with Splunk

Splunk can support MSPs in differentiating services, upleveling managed security offerings, and untangling complexity for clients.

Join our worldwide partner community for insight on cultivating resilience and strengthening SecOps teams.

Visit [our partner page](#) for more details.



www.splunk.com