Solution Brief

eSENTIRE

Atlas Integration: Splunk

Add expert MDR coverage on top of your existing Splunk investment without any migration.

Overview

For most enterprises, Splunk is where years of log data lives and that data doesn't move easily. Organizations shouldn't have to choose between protecting their existing SIEM investment and getting MDR coverage for their business demands.

Every Splunk deployment is different. Years of custom configurations, unique schemas, and varying detection rule quality mean no two environments look the same, and that's exactly what has made Splunk integrations hard to scale.

46% Market share
Splunk is the most widely deployed SIEM in the enterprise.

Full enterprise SIEM migrations can take up to **One year** including a full rewrite, data remapping and query language translations.

The eSentire Atlas Platform now integrates directly with Splunk, enabling eSentire to ingest alerts, investigate them within the Atlas Platform, and remotely query Splunk data on demand without touching the Splunk environment. eSentire normalizes data across any Splunk deployment, so the SOC gets a clean actionable signal regardless of how your Splunk is built.

Three Splunk modules that eSentire integrates with:

1 Splunk Cloud

Splunk's fully managed SaaS platform. Splunk handles maintenance, upgrades, and scaling. The fastest path to getting Splunk up and running.

2 Splunk Enterprise

The self-hosted version of Splunk, deployed on your customer's own infrastructure. Common in enterprises with strict data residency, compliance, or sovereignty requirements.

3 Splunk Enterprise Security

A premium security layer built on top of Splunk Cloud or Enterprise that turns it into a full SIEM. This is the version most enterprise security teams are running and comes with built-in detections, threat intelligence, and case management.

Why This Matters

- **Alert ingestion & investigation:** Splunk alerts flow into the Atlas Platform, enriched and investigated by AI with expert led investigation.
- **Remote query via Atlas Actions:** SOC Analysts query Splunk on demand, no Splunk UI access or local accounts required.
- **Data forking:** Selected Splunk log data is forked to Atlas for local multi-signal processing.
- **All deployments supported:** Splunk Cloud, Splunk Enterprise and Splunk Enterprise Security.
- **No extra cost for coverage:** Coverage for Splunk deployments are included with eSentire packages.

How It Works

1

Install

The client installs eSentire add-on (available directly in Atlas Platform) plus the required Splunk Technology add-on for Splunk Enterprise Security (if applicable). For on-prem deployments, the Atlas Gateway is also required.

2

Connect

The client creates an API token in Splunk and links it to eSentire via the Integrations page in Atlas Settings, entering the instance URL, token, and index.

3

Monitor

eSentire's SOC monitors Splunk-generated alerts 24/7. Alerts flow into Atlas, enriched and correlated across all signals.

4

Investigate & Respond

Critical events are escalated with recommended actions. SOC Analysts can remotely query the client's Splunk via Atlas Actions for on-demand enrichment.

Why eSentire

- 2,000+ organizations protected across 80+ countries
- Founded in 2001 with 25 years of SOC expertise embedded in Atlas
- Named MDR Leader in Forrester Wave™
- 300+ technology integrations Atlas connects to any signal across your existing stack
- Continuous Offensive and Defensive Flywheel, every incident
- Vendor-independent, so we work with your full stack today and tomorrow

> *"We look at eSentire to be the experts. We trust them implicitly. They're with us through the thick and thin till the end."*

CISO, Financial Services
GARTNER PEER INSIGHTS

> *"eSentire has been an indispensable partner. Their proactive monitoring and strategic advice have contributed to a significant improvement in our cyber resilience."*

Security Leader, Six-year customer
GARTNER PEER INSIGHTS

2,000+ organizations in **80+** countries | **25** years of SOC expertise | **2M+** endpoints protected | MDR Leader, Forrester Wave™

Ready to Get Started?

Connect with an eSentire Security Specialist to see Managed Detection & Response working across your environment.

LET'S TALK SECURITY →

eSentire is a leader in Controlled Autonomy SecOps, protecting 2,000+ organizations across 35+ industries around the world. Founded in 2001, the company's Controlled Autonomy SecOps operating model pairs agentic AI operatives with engineered human-judgment controls, delivering expert-depth security outcomes at machine speed without ceding accountability to opaque automation. Powered by the unified agentic AI Atlas Platform, eSentire's Atlas AI + 24/7 expert human SOC coverage delivers offensive capabilities that preempt exposures before attackers do, detect, and respond to stop threats in real time. For more information, visit **www.esentire.com** and follow **@eSentire**.