ATLAS PLATFORM

eSentire Atlas SIEM

eSentire MDR for Log (Atlas SIEM) delivers critical visibility across your multi-cloud and hybrid environments without the day-to-day challenges of log management No SIEM sprawl. No rip-and-replace. Every tool you already run, working harder.

Every autonomous action is explainable, reversible, and policy-bound

6.5 mins Avg. AI Investigation, from Signal to Finding

95% Verdict Agreement with Tier-3 Analysts

MDR for Log That Enriches, Not Just Ingests

Traditional MDR providers ingest logs but rarely act on them. eSentire Atlas SIEM surfaces collected logs across all AI and SOC investigations and applies hundreds of real-time analytics to surface new signals for investigation — continuously sharpened by Atlas AI — catching detections generic MDR misses. Every signal feed the CASO flywheel: investigate, expose, validate, repeat.

Multi-Signal Visibility

Log signals cross-correlated with each other, endpoint, network, cloud, and identity in one workflow.

- No SIEM replacement required
- Cloud, hybrid, on-premises coverage

Controlled Autonomy Investigations

Atlas AI investigates every detection. Every conclusion is explainable and every action is reversible with a human-on-the-loop always.

- Avg 6.5 min from signal to finding
- 95% Tier-3 analyst agreement
- 24/7 expert SOC oversight always

Continuous Security Flywheel

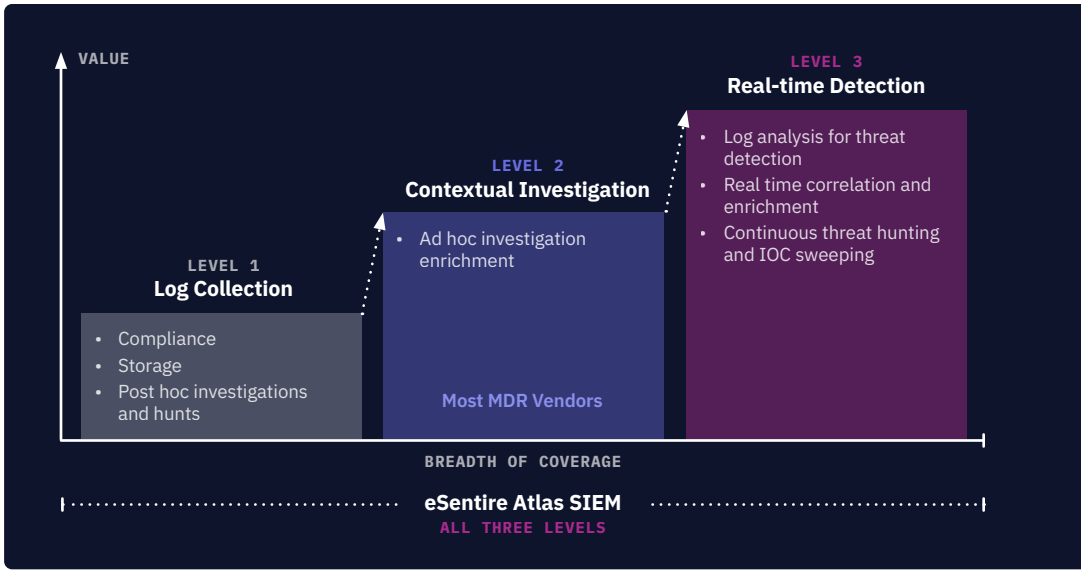
Every incident tightens your defenses. Logs may generate a signal to be investigated or can be used by investigations to enrich and support.

- TRU builds hundreds of detectors/ runbooks per quarter
- MITRE ATT&CK mapped, updated continuously
- Exposure intelligence flows across full stack

THE ESENTIRE DIFFERENCE

There's a hierarchy of value in security operations — and most MDR providers barely clear the first rung. Collecting logs for retroactive hunting and compliance reporting is table stakes while using those logs to add context and depth to active investigations is slightly better. But real-time analysis of critical logs to surface net-new signals and drive live detections? That's where the gap is — and that's where eSentire operates.

Three levels. Most vendors deliver one. eSentire delivers all three.



ATTACK COVERAGE

Hunting, Investigation and Detection: Across the Full Attack Lifecycle

- Phishing and business email compromise
- Data exfiltration
- Modular malware
- Insider threats and anomalous user behavior
- Cloud service misconfigurations
- Privilege escalations and alterations
- Cryptojacking
- Suspicious VPN activity
- Defense evasion techniques
- Lateral movement and attack progression

PLATFORM CAPABILITIES

What Atlas SIEM Delivers

Six core capabilities from day one, all accessible from a single console without touching your existing log infrastructure.

1 Unified Log Visibility

Single pane of glass for all log sources and Atlas-native detections. Anything that outputs a log is centralized and correlated in Atlas.

2 Threat Detection Across Hybrid Environments

100+ attack types detected using business rules, MITRE ATT&CK techniques, and user behavior, such as phishing, exfiltration, insider threats, cloud misconfigurations, privilege escalation, and more.

3 Investment Protection, Not Replacement

Enrich signals from every tool you already own, surfacing detections that never reach the SOC today. No rip-and-replace. Every investment works harder.

4 AI Investigations

Every detection is investigated by the Atlas AI Operative. Findings are explainable, reversible, and policy-bound. Analysts get confirmed findings, not raw alerts.

5 Unlimited Log Ingest

Included with eSentire MDR packages. Flat pricing when purchased in MDR packages—no volume-based fees. Unlimited log ingestion for threat hunting and detection.

6 Continuous Detection Improvement

All content is tracked for accuracy post-deployment. TRU tunes and decommissions detection content continuously.

WHY ESENTIRE

The Authority in Managed Detection and Response

25 years of 24/7 SOC expertise embedded in Atlas for enterprise-grade MDR without the enterprise-sized team.

- 2,000+ organizations protected across 80+ countries
- 153,000+ autonomous investigations completed since May 2025
- Founded in 2001 with 25 years of SOC expertise embedded in Atlas
- Named MDR Leader in Forrester Wave™
- Closed AI-investigated alerts, not just surfaced
- 511,000+ human-equivalent hours delivered by Atlas AI
- CASO Flywheel — every incident automatically hardens the environment
- Vendor-independent, so we work with your full stack today and tomorrow

Ready to stop treating your logs as signal noise?

Talk to an eSentire expert. Learn how eSentire Atlas SIEM delivers multi-signal visibility, AI-powered investigations, and Controlled Autonomy SecOps — explainable, reversible, and fully accountable.

REQUEST A DEMO →