DATA SHEET:

esLOG

SIEM outcomes without the headaches of SIEM management.

UNRESTRICTED VISIBILITY

Gain critical and flexible visibility across your network assets, regardless if your data is in the cloud, on-premises or in between.

FOCUSED RESEARCH AND DEVELOPMENT

Benefit from a dedicated team of researchers who power esLOG with cutting edge detections of threat actor tactics, techniques and procedures (TTPs).

APPLIED ANALYSIS FROM HUMAN EXPERTS

Minimize threat actor dwell time and understand the context behind threats to your business as they emerge, 24x7x365.

REDUCED RISK IN MODERN HYBRID ENVIRONMENTS

Take action within traditional network components, as well as cloud infrastructure and apps. Respond to and manage risk across your entire environment.

esLOG is a fully managed solution that delivers on the outcomes you hope to have from a Security Information and Event Management (SIEM) tool, high-efficacy security utility to detect and respond to threats leveraging your existing security investments, without the day-to-day challenges of SIEM management like creating or revising rules and conducting investigations.

Powered by one of the industry's most powerful cloud-based data analytics platforms, esLOG aggregates and enriches logs from assets across your environment, providing the critical visibility required to detect advanced threats. A dedicated team manages the entire counterthreat content creation process, from the creation of detectors to the deployment of runbooks, ensuring your defenses evolve with the threat landscape. This empowers analysts from eSentire's 24x7x365 Security Operations Centers (SOCs) to swiftly investigate and respond to events on your behalf, shrinking the dwell time of threat actors targeting your hybrid environment.

Robust Hybrid Environment Coverage

Detect and respond to threats in the "big three" cloud providers.

Cloud infrastructure

Azure

Google Cloud

aws

Cloud applications

G Suite

Microsoft 365

Further counterthreat TTPs leveraging common security infrastructure and tools (including but not limited to):

- EDR/EPP Tools (Carbon Black, Crowdstrike, Trend Micro, etc.)
- Network security technology (Palo Alto, Cisco, etc.)
- Email security platforms (Outlook, Gmail, Proofpoint, etc.)
- VPN providers (Palto Alto, Cisco, etc.)
- Web gateway solutions (Citrix)

THREAT COVERAGE

Detect a multitude of attack types and techniques (including but not limited to):

- Phishing attacks
- Suspicious and/or unusual user behavior
- Data exfiltration
- Privilege escalations and alterations
- Insider threats
- Cloud service misconfigurations
- Modular malware
- Cryptojacking
- Defense evasion
- Suspicious VPN activity

FEATURES

24x7x365 Coverage

Expert analysts from eSentire's two global SOCs monitor for and investigate events around the clock.

Atlas XDR Platform

Signals from esLOG and other eSentire Managed Detection and Response (MDR) solutions are ingested and enriched by ATLAS, our purpose-built XDR platform that accelerates SOC investigations and response to threats on your behalf.

Anchored by the eSentire Global Threat Framework

The structure that informs the entire counterthreat research and development roadmap from detector creation, deployment and maintenance.

MITRE ATT&CK Mapped

From broad tactic categories down to individual technique IDs, all esLOG detectors and runbooks are mapped to the MITRE framework.

Innovative Machine Learning Applications

AI-powered security force multipliers that hunt and respond to elusive threats through vast amounts of data.

Time to Value

A flexible SaaS delivery that is up and running in the fraction of the time of a traditional SIEM deployment.

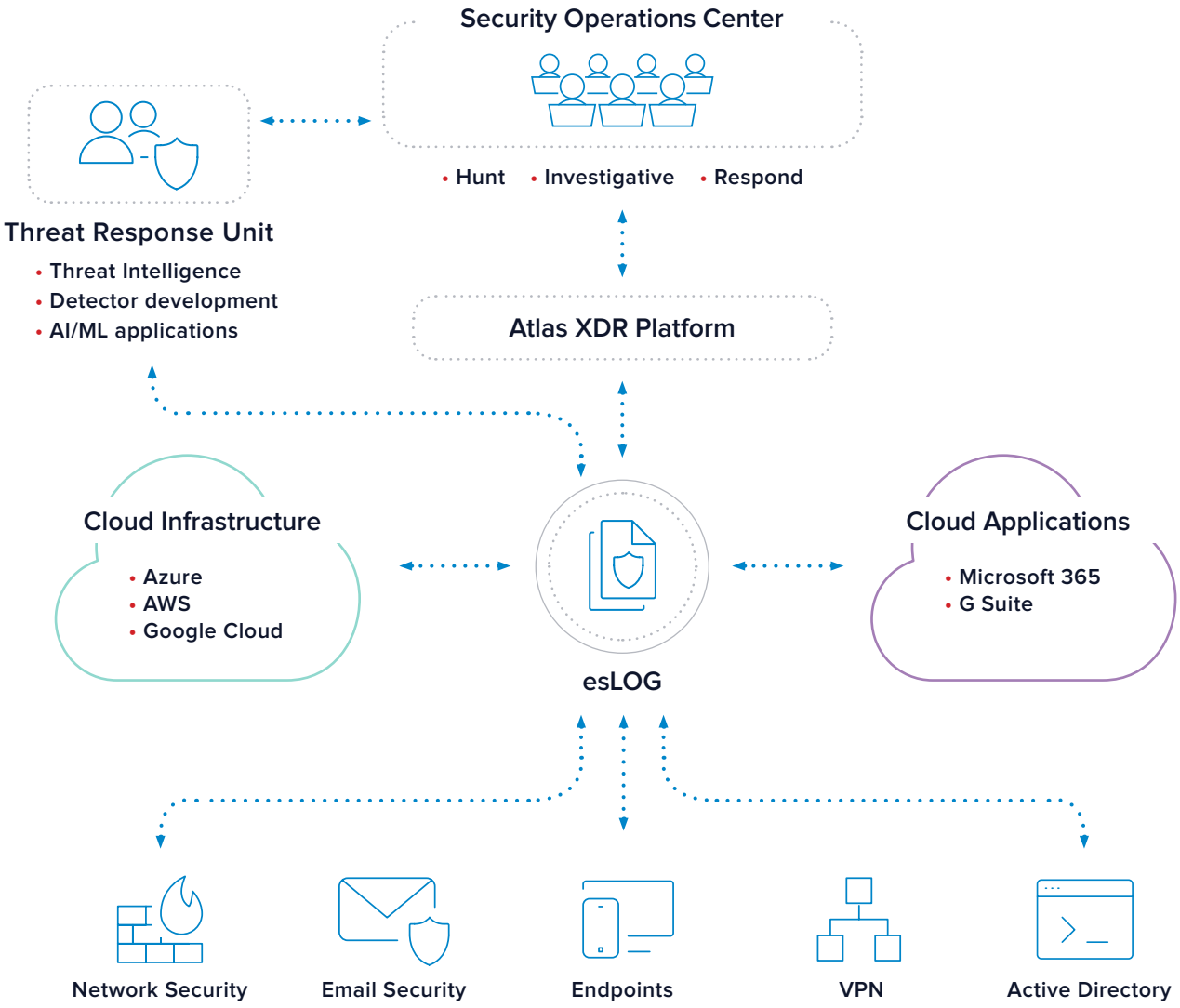
Flexible Log Consumption, Analysis and Storage Options

Focus on the data that matters the most to your business in order to maximize your investment.

Simplified Compliance Management

Satisfy and report on the logging regulatory requirements of frameworks such as HIPAA, PCI, GDPR, etc.

HOW IT WORKS



OUTCOMES

- Account for risk across your network assets
- Detect threats that traditional technologies miss
- Decrease threat actor dwell time
- Decrease false positives and increase true positives for your security team
- Human cybersecurity expertise as an extension of your team
- Efficiencies and cost savings versus DIY security
- Satisfy compliance mandates
- Decrease overall risk of business disruption

TRUSTED BY

- High-net-worth finance organizations
- Large state healthcare networks
- Major retail brand names
- AM100 law firms
- Sports and entertainment giants

> "Excellent customer service, comprehensive set of monitoring services. Innovation and improvements to existing services and continued innovation for increasing visibility."

— Christopher Meinders
Security Manager, Baker Botts LLC

Ready to get started? We're here to help.

Reach out and schedule a meeting to learn more.

eSentire, Inc., founded in 2001, is the category creator and world's largest **Managed Detection and Response (MDR)** company, safeguarding businesses of all sizes with the industry-defining, cloud-native Atlas platform that removes blind spots and enables 24x7 threat hunters to contain attacks and stop breaches within minutes. Its threat-driven, customer-focused culture makes the difference in eSentire's ability to attract the best talent across cybersecurity, artificial intelligence and cloud-native skill sets. Its highly skilled teams work together toward a common goal to deliver the best customer experience and security efficacy in the industry. For more information, **visit www.esentire.com** and follow **@eSentire**.