DATA SHEET:

Get Deeper Investigation and Correlation with esLOG

Enhance your existing Managed Detection and Response (MDR) investment by ingesting data from additional sources like Cloud IaaS and SaaS, VPN providers, email security tools and more.

FULL VISIBILITY, INVESTIGATION, AND CORRELATION

Gain visibility, deeper investigation, and correlation of cloud, application, network, server and endpoint data

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 AND RAPID RESPONSE IN HYBRID ENVIRONMENTS

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

esLOG is a fully managed solution that delivers critical visibility across modern hybrid environments, enhancing the ability to detect and respond to threats without the day-to-day challenges of curating security signals from various sources like cloud infrastructure, SaaS applications and security infrastructure.

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 and investigation required to detect advanced threats . A dedicated team manages the entire counter-threat content creation process, from the creation of detectors to the deployment of runbooks, ensuring your defenses evolve with the threat landscape. This enables human-led investigation and correlation from eSentire's 24x7x365 Security Operations Centers (SOCs) analysts who swiftly respond to events on your behalf, shrinking the dwell time of threat actors targeting your hybrid environment.

As integrated technologies, we can isolate and exert immediate control at the network and endpoint level in your environment to block malicious IPs and isolate infected endpoints with esNETWORK and esENDPOINT, enhancing your eSentire MDR services. This is the force multiplier coming into effect during containment with esNETWORK and esENDPOINT.

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 loss prevention
- Privilege escalations and alterations
- Insider threats
- Cloud service misconfigurations
- Modular malware
- Cryptojacking
- Email Security

FEATURES

24x7x365 Coverage & Rapid Response

Human-led investigation and correlation from expert analysts in our 2 global SOCS across log data for known and unkown threats

Atlas XDR Platform

Signals from esLOG and other eSentire MDR solutions are ingested and enriched by ATLAS, our purpose-built cloud XDR platform. Patented machine learning eliminates noise, enables real-time detection and response, and automatically blocks known and unknown threats.

Anchored by the eSentire Global Threat Framework

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

MITRE ATT&CK Mapped

From the broad tactic categories down to individual technique IDs, 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

esLOG has a flexible SaaS deployment model that is up and running almost immediately.

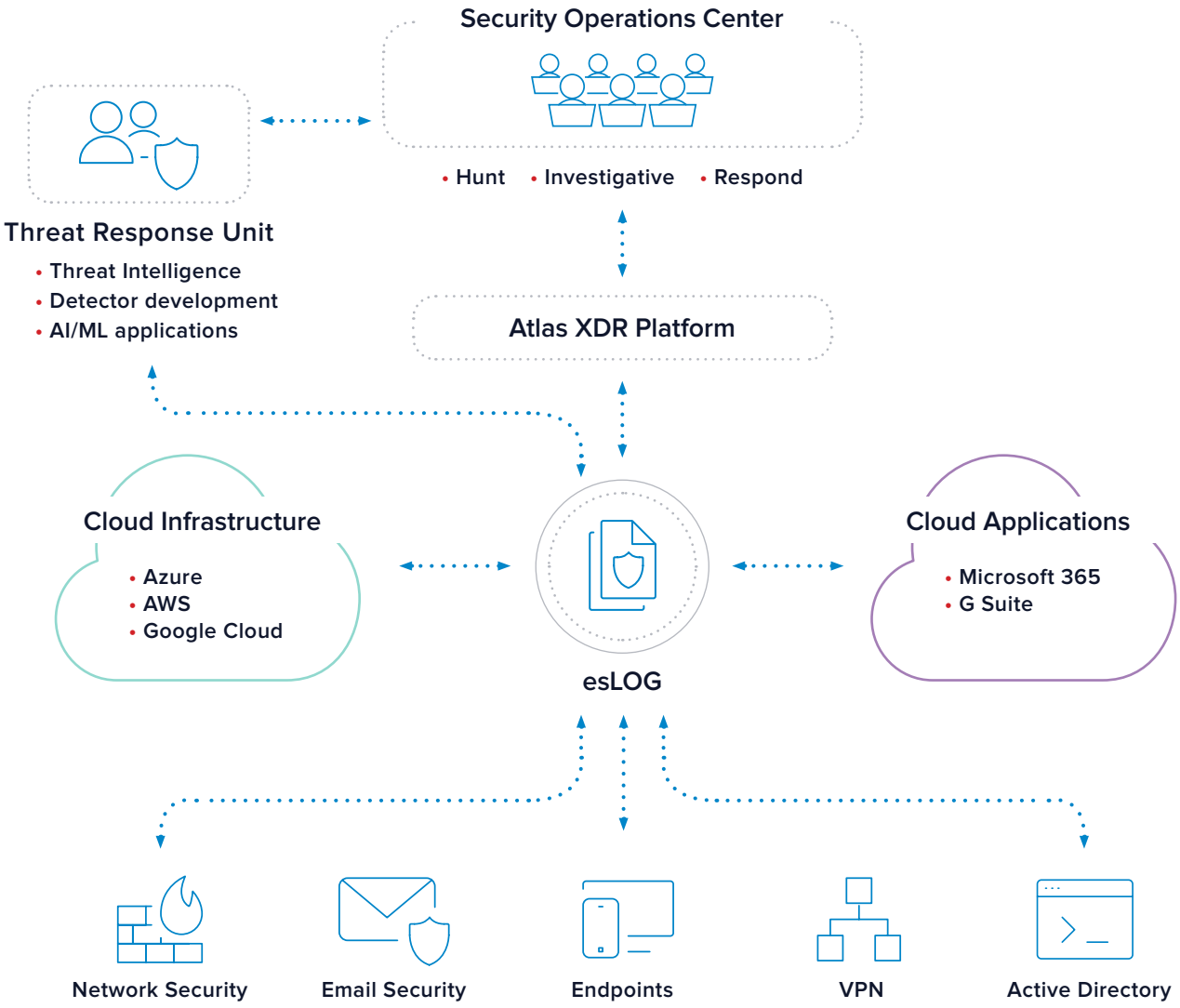
Flexible Log Consumption, Analysis and Storage Options

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



YOUR OUTCOMES

- Reduce risk across your cloud, application, network, server and endpoint assets
- Detect threats that traditional technologies miss
- Decrease threat actor dwell time
- Decrease false positives and increase true positives for your security team
- Human-led investigations and expert analysts act as an extension of your team
- Overall enhancement of your existing eSentire eMDR services
- 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**.