DATA SHEET

eSENTIRE

esLOG+

Critical visibility accelerating detection across modern hybrid IT environments

CLOUD, HYBRID, OR ON-PREMISES.

Gain critical threat visibility that evolves regardless of your environment. Remove potentially dangerous blind spots.

DETECT. HUNT. PRIORITIZE.

Identify the most elusive of threats. Focus on those that matter most.

VALIDATE. ACCELERATE. REMEDIATE.

Minimize threat actor dwell time with rapid response to prevent business disruption.

COMPLIANCE. REPORTING. SIMPLIFICATION.

Realize the traditional benefits of a SIEM without the complexity and cost.

Whether your data is on-premises, in the cloud or somewhere in between, esLOG+ evolves with the requirements of your modern hybrid IT environment. This cloud-native, SIEM alternative, embedded in eSentire's Managed Detection and Response services, aggregates meaningful and actionable intelligence from your network assets, endpoints, applications and cloud services. And, you can have it up and running in a fraction of the time of a traditional SIEM.

esLOG+ is designed to be more than a compliance and reporting tool. esLOG+ provides critical visibility across your threat landscape to eSentire Security Operations Center (SOC) analysts who leverage big data analytics, machine learning, customized rule-sets and behavioral analysis to make sense of expected and unexpected events and behaviors across your environment. Proprietary threat-hunting methodology and full forensic investigation are performed to confirm a threat's presence and determine the extent to which the threat actor has spread. Minimizing threat actor dwell time, false positives are eliminated and our analysts alert you to confirmed threats, giving you step-by-step guidance to contain and eliminate attacks. Data visualizations, customizable reporting and KPIs are available, giving your team visibility to what our analysts are investigating and ensuring you meet the strictest of regulatory requirements.

VISIBILITY

esLOG+ handles the on-premises sources you expect a traditional SIEM to cover, with the added ability to support a collection of custom applications via script. It also delivers an extensive library of available integrations including, but not limited to:

AWS Services

Microsoft

- Active Directory
- Azure
- O365

Compliance and Security

- Box
- Duo
- Cylance
- Crowdstrike
- Cisco ASA
- Okta
- Palo Alto
- Trend Micro
- Zscalar

Database

- Microsoft SQL
- MongoDB
- MySQL
- Oracle

DevOps

- Docker
- Github
- Jenkins
- Kubernetes

Google Compute Platform

IT Infrastructure

Operating System

- Host Metrics
- Linux
- Windows

Storage

Web Server

- Apache
- Apache Tomcat
- IIS
- Nginx

WHAT IS esLOG+ DESIGNED TO SOLVE FOR?

- Improving visibility and scalability across hybrid IT environments
- Reducing costly deployment, staffing and ongoing maintenance requirements
- Accelerating time-to-value
- Applying advanced analytic and hunting capabilities to detect known and unknown threats
- Correlating multiple events into a single incident
- Mapping threats to affected resources
- Performing ad hoc queries on stored data for forensics
- Accelerating investigation and response times
- Eliminating false positives
- Prioritizing alerts
- Simplifying reporting
- Addressing policy and compliance requirements

FEATURES

24x7 MONITORING WITH CRITICAL THREAT VISIBILITY

Cross-Platform Monitoring and Visibility

esLOG+ collects, aggregates and monitors data across on-premises, cloud, multi-cloud and hybrid platforms like AWS, Microsoft Azure, Apache, and the Google Cloud Platform providing our 24x7x365 SOC analysts with critical visibility to threats across your entire threat landscape.

- *Azure Cloud Security*

  esLOG+ utilizes machine learning and monitoring capabilities across your Azure environment for real-time visibility, analysis and data visualizations.

- Google Cloud Platform Security

  esLOG+ integrates directly into your GCP environment, providing instant insights into potential security issues and user activity for Google VPC, IAM, Cloud Audit and Google App Engine.

- *AWS Security*

  esLOG+ integrates with your AWS cloud environment providing SOC analysts with a comprehensive view to see who is accessing AWS and when they make changes (CloudTrail), what they change (Config), where this impacts network traffic and latency (VPC Flow), and how this affects your security and compliance posture (Inspector).

- *Apps for Extended Log Analytics*

  esLOG+ extends functionality of log analytics with an extensive library of apps that help optimize data collection for better security monitoring.

ADVANCED DETECTION CAPABILITIES AND HUMAN-BASED THREAT HUNTING EMPOWER RAPID INVESTIGATION AND RESPONSE

Embedded Threat Hunting and Forensic Investigation

esLOG+ includes embedded threat hunting and forensic investigation of aggregated log data to accelerate precision that facilitates rapid response and threat containment.

Big Data Analytics

esLOG+ leverages the power of big data and advanced analytics to end-user behavior, to detect anomalies (deviations from the established baseline) and to flag exceptions to identify real and potential threats.

Machine Learning Integration

esLOG+ utilizes machine learning and predictive analytics to make sense of expected and unexpected behavior across your environment with pattern, anomaly and outlier detection.

Real-time Search and Visualizations

esLOG+ has preconfigured and customizable searches and dashboards with KPIs, giving our SOC analysts and your security team visibility into abnormal behaviors illuminating what matters most.

Log Retention

esLOG+ retains all raw log data giving SOC analysts the ability to correlate information with data from esENDPOINT and esNETWORK to conduct thorough forensic investigations, drill down into details and assist with root cause analysis on any security incident.

False Positive Elimination

esLOG+ increases the velocity and accuracy of threat detection so our SOC analysts can determine what is noise vs. true security events to ensure your team is only alerted to verified threats.

SIMPLIFIED MANAGEMENT WITH DATA VISUALIZATIONS AND REPORTING

Co-Management

esLOG+ provides a co-managed model with access to run your own advanced search queries, generate alerts, manage profiles, run reports, and investigate events alongside our SOC analysts.

Time to Value

esLOG+ is a pure SaaS offering that features simple-to-deploy collectors with rich filtering capabilities that can be up and running within minutes. It offers access to all the latest capabilities without the need for time-consuming, expensive deployment and upgrades.

Simplified Compliance Management Reporting

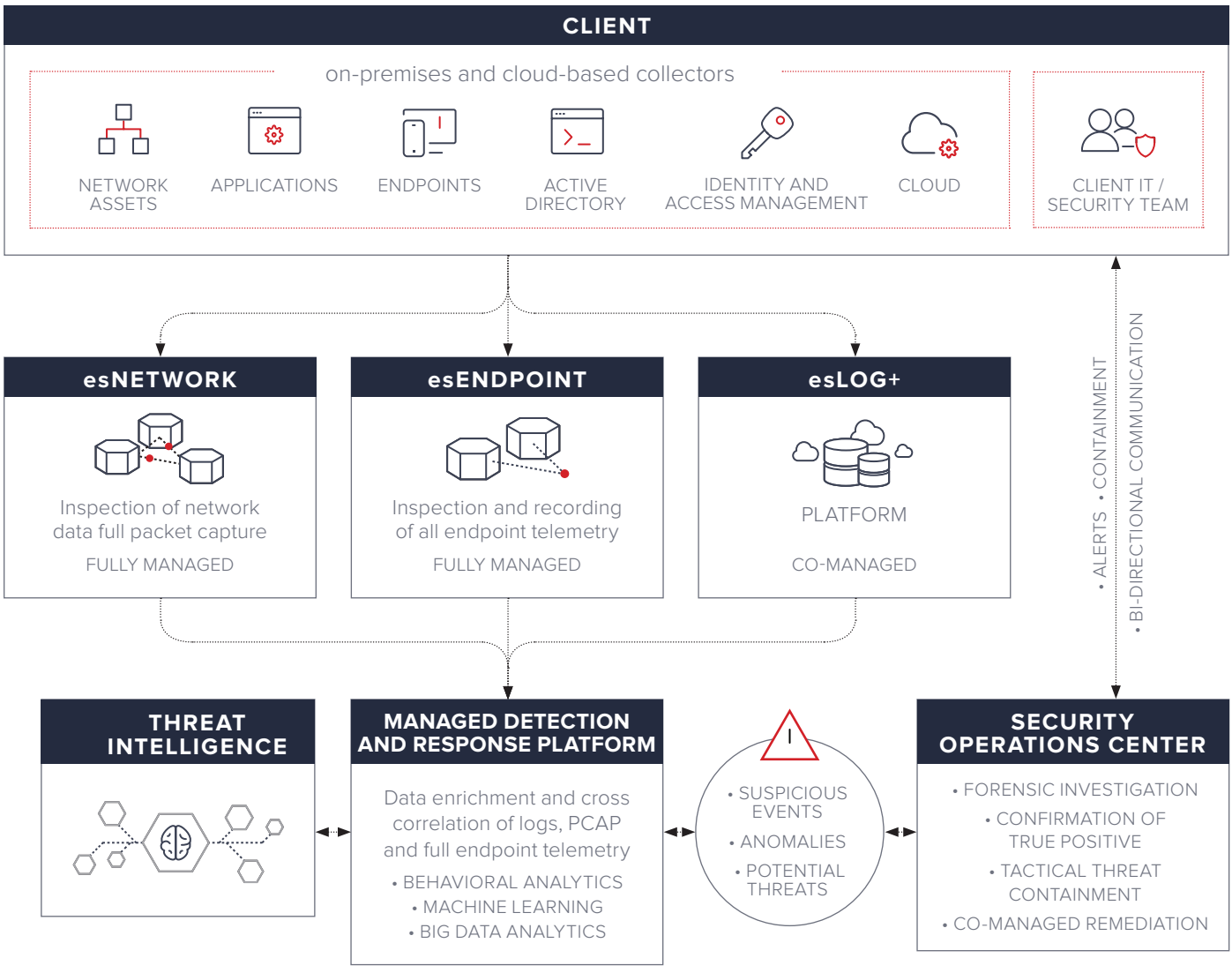
esLOG+ ensures compliance mandates are met with centralized logging, continuous monitoring, and automated retention policies with various out of the box, and custom security reports that meet regulatory requirements such as HIPAA, PCI, SEC, GDPR, and more.

BENEFITS

- Comprehensive 24x7x365 threat monitoring
- Complete threat visibility across your threat landscape
- Flexibility to run your own queries, alerts, profiles, reports, and investigate events alongside eSentire analysts
- Removes traditional complexity and cost of a SIEM with rapid time-to-value
- Comprehensive, correlated and accurate analytics of security events provided by eSentire's SOC
- Detection of known and unknown threats
- Improved post-attacks forensics
- Reduction of false positives
- Minimizes threat actor dwell time with integrated response
- Threat containment* and co-managed remediation
- Unparalleled insight with visualizations and customizable searches
- Simplified compliance management and reporting

**Requires esNetwork and/or esEndpoint*

HOW DOES IT WORK?



BETTER TOGETHER: esLOG+, esNETWORK AND esENDPOINT

Logs provide critical visibility that enable better observation, orientation and decision making in disrupting the attacker kill chain. But, logs alone are limited in the depth of data that permits deeper investigation and remediation of security incidents. In addition, log-based security can delay detection of events and response due to lag time of inbound signals as opposed to the near-instantaneous feedback of a live network stream or endpoint technology. The greater the signals and forensic data available to analysts, the greater their ability to cross-correlate information that accelerates hunting, detection and response.

eSentire's esNETWORK provides the gold standard for forensic data, with timestamps, full-packet capture and analysis with the ability to contain threats through TCP resets. esENDPOINT provides deep insight into processes, file changes, and more at the host level, with the ability to isolate damaged systems or stop processes in near real-time. esLOG+, when deployed in combination with esENDPOINT and esNETWORK, provides our SOC analysts with a comprehensive set of enriched signals that eliminates blind spots in which threats can lurk. Most Managed Detection and Response providers rely solely upon log data and are limited to simple alerts generated by myopic prevention technologies. esLOG+, when deployed with esENDPOINT and esNETWORK, enables our analysts to go beyond alerts empowering their ability to take action on your behalf. Implementing host isolation or network communication disruption, threats are contained in near real-time, mitigating risk to your organization.

WHY eSENTIRE?

	Other Managed Security Services Providers	eSentire
Initial Deployment and Setup		
Account/Role Setup	✓	✓
Setup/Deployment/Configuration of Collectors	✓	✓
Configuration of Sources	✓	✓
Training and Onboarding	✓	✓
Dashboard Setup	✓	✓
Ongoing Dashboard Maintenance	✓	✓
On-going Operations		
Deployment/Setup of New Collectors and Apps	✓	✓
Parsing Operations	✓	✓
Log Collection, Management and Correlation	✓	✓
Writing of Search Queries	Limited	✓
Modification of Search Queries	Limited	✓
Creation of Reports	✓	✓
Modification of Reports	✓	✓
Patches, Hot fixes, and Functional Updates	✓	✓
Creation of Correlation Rules	Limited	✓
Modification of Correlation Rules	Limited	✓
Threat Intelligence Integration/Updates		✓

	Other Managed Security Services Providers	eSentire
Monitoring		
24x7 Monitoring	✓	✓
Incident Investigation and Management		
Threat Hunting		✓
Forensics & Investigation		✓
Correlation With Full Endpoint Telemetry*		✓
Correlation With PCAP Data From The Network*		✓
False Positive Elimination		✓
Alerts	✓	✓
Tactical Threat Containment: Host*		✓
Tactical Threat Containment: Network*		✓
Response Plan	✓	✓
Remediation Guidance	✓	✓
Reporting		
Daily Log Review For PCI		✓
Monthly Reporting (system generated)	✓	✓
Creation/Maintenance of standard reports	✓	✓
Creation/Maintenance of customized reports	✓	✓
Compliance Report Creation/Updates	✓	✓
Report Validation and Review	✓	✓

**Requires esNetwork and/or esEndpoint*

NEXT STEPS

Put eSentire MDR to the test

Learn more about eSentire MDR

Learn more about eSentire Advisory Services

Access free cybersecurity tools and resources

in partnership with

About eSentire:

eSentire is the largest pure-play Managed Detection and Response (MDR) service provider, keeping organizations safe from constantly evolving cyber-attacks that technology alone cannot prevent. Its 24x7 Security Operations Center (SOC), staffed by elite security analysts, hunts, investigates, and responds in real-time to known and unknown threats before they become business-disrupting events. Protecting more than $6 trillion in corporate assets, eSentire absorbs the complexity of cybersecurity, delivering enterprise-grade protection and the ability to comply with growing regulatory requirements. For more information, visit **www.eSentire.com** and follow **@eSentire.**

About Sumo Logic:

Sumo Logic is the leading cloud-native, machine data analytics platform that delivers continuous intelligence across the entire application life-cycle and stack. More than 1,600 customers around the globe rely on Sumo Logic for the analytics and insights to build, run and secure their modern applications and cloud infrastructures. With Sumo Logic, customers gain a service-model advantage to accelerate their shift to continuous innovation, increasing competitive advantage, business value and growth.

Founded in 2010, Sumo Logic is a privately held company based in Redwood City, CA and is backed by Accel Partners, DFJ, Greylock Partners, IVP, Sapphire Ventures, Sequoia Capital and Sutter Hill Ventures. For more information, visit **www.sumologic.com.**