eSENTIRE

esLOG

The evolution of threat visibility

See everything. **Lose nothing.**

THE CHALLENGE

As threats evolve and hybrid IT environments increase the attack surface, traditional prevention will continue to leave organizations with dangerous blind spots.

54% of hackers that can complete an attack and exfiltrate data in under 15 hours

62% of attackers that say they can break into any environment

Chris Pogue, Nuix. *The Black Report 2018 (report_nuix_black_report_2018_web_us (1).pdf).* 2018.

THE NEED

The need for full threat visibility is evolving. Effective threat hunting now requires full visibility into:

1. Web Traffic
2. Email Traffic
3. Could Access
4. Endpoints
5. Network Traffic

Ponemon Institute. *Challenges to Achieving SIEM Optimization (File: Cyphort-Ponemon-SIEM-Report.pdf).* Sponsored by Cyphort. March 2017.

THE TRADITIONAL APPROACH

Traditional SIEM platforms used to be the answer. SIEMs aggregate and correlate data to identify patterns and trends that could indicate threats. But in today's hybrid IT environment, taking those measures alone can leave you vulnerable to attack. These platforms also present costly challenges and gaps in required features.

TOP 5 CHALLENGES OF CURRENT SIEM USERS	TOP 3 FEATURES CURRENT SIEM USERS ARE MISSING	WHY TRADITIONAL SIEMS DO NOT WORK FOR THE CLOUD
1 Tasks need to be automated to focus on priorities	1 Detect threats through advanced analytics	Securing microservices/containers
2 Greater visibility of network traffic	2 Prioritize threats, vulnerabilities and attacks	Rules are outdated as soon as they are created
3 More accurate, prioritized and meaningful alerts	3 Correlate multiple related events into single incident	Cloud dynamics make upfront planning and provisioning difficult
4 Additional staff to optimize, analyze and respond to alerts		Distinguishing noise from alerts from cloud data
5 Reduce complexity with additional staff		Hardware obsolescence

Ponemon Institute. *Challenges to Achieving SIEM Optimization (File: Cyphort-Ponemon-SIEM-Report.pdf).* Sponsored by Cyphort. March 2017.

A traditional siem will never be your silver bullet.

Introducing eSentire esLOG: Critical visibility accelerating detection and response across modern hybrid IT environments.

THE ANSWER TO EVOLVING THREATS

Introducing **eSentire esLOG**. eSentire esLOG combines critical visibility with threat hunting to enable rapid response. esLOG evolves with your threat landscape and the modern hybrid IT environment, while minimizing operational complexity. Advanced analytics are leveraged to detect threats, while our SOC analysts prioritize threats and correlate data. No blind spots. Rapid containment and response.

eSENTIRE

in partnership with

sumo logic

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 SIEM without the complexity and cost.

eSentire esLOG is the evolution of threat protection.

LEARN MORE ABOUT esLOG

eSENTIRE