

eSentire Managed Log

Critical threat visibility and deeper investigation capabilities for hybrid environments.

Problem 1: Visibility into an expanding attack surface

Modern IT environments are expansive, including endpoints, networks and various cloud environments.

of organizations are using 11 or more cloud services and applications.

57% of organizations say the growth of cloud applications and services are driving an increase in security alerts.

of organizations say traditional security solutions either don't work or have limited cloud functionality.

of sources, greatly contributing to threat detection and investigation.

Adding log coverage increases the breadth of visibility, acquiring signals from a number

Problem 2: Reliable and relevant threat context

For threats that span technology boundaries, multi-signal correlation, enhanced threat investigation, and bolstered threat hunting capabilities take significant expertise which could mean the difference between prevention or business disruption.

of organizations handle at least 1,000 alerts per day.

of organizations said important issues are hidden in a flood of minor issues and noise.

Adding log coverage increases the breadth of visibility, acquiring signals from a number of sources, greatly contributing to threat detection and response.

of organizations do not have a thorough mapping

to the MITRE ATT&CK framework. of organizations are seeking out

employees that have the skills to apply the MITRE

The Solution: Adding log coverage for deeper threat detection with your eSentire MDR services The more we see, the better outcomes we can deliver. eSentire Managed Log enables

multi-signal Managed Detection and Response (MDR) by leveraging signals from your hybrid environment and helping make sense of thier associated risks.

cloud providers.

Detect and respond to threats in the "big three"

common security infrastructure and tools:

Further counterthreat TTPs leveraging

Cloud Infrastructure







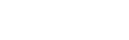
 Network security technology (Palo Alto, Cisco, etc.)

 EDR/EPP Tools (Carbon Black, Crowdstrike, Trend Micro, etc.)

- Email security platforms (Outlook, Gmail, Proofpoint, etc.)
- VPN providers (Palto Alto, Cisco, etc.)
- Web gateway solutions (Citrix)

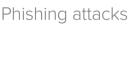
GSuite Microsoft 365

Cloud Applications





With eSentire Managed Log you get high-efficacy threat detections:



Cloud service

misconfigurations



Privilege

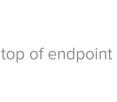
escalations





Defense evasion





0101 1001 0110

Cryptojacking

Trusted Bv:



High-net-worth



Large state



Major retail





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.