eSENTIRE.

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.

62% **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.

66% **of organizations** say traditional security solutions either don't work or have limited cloud functionality.

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

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.

56% **of organizations** handle at least **1,000** alerts per day.

68% **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.

84% **of organizations** do not have a thorough mapping to the MITRE ATT&CK framework.

70% **of organizations** are seeking out employees that have the skills to apply the MITRE ATT&CK framework.

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.

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:

- 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 (Palo Alto, Cisco, etc.)
- Web gateway solutions (Citrix)

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

Phishing attacks

Unusual user behavior

Data exfiltration

Cloud service misconfigurations

Privilege escalations

Defense evasion

Suspicious VPN activity

0101
1001
0110

Cryptojacking

You also increase MITRE ATT&CK coverage by **20%** on top of endpoint and network MDR services.

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

[1,2] Cloud Threat Protection Report, Cybersecurity Insiders 2020 , [3] Cloud Security Report, IS2, 2019, [4] Sumo Logic State of SecOps and Automation, 2020,
[5] The State of MITRE ATT&CK threat-informed defense, Cybersecurity Insiders 2021

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

Reach out and schedule a meeting to learn more.

eSENTIRE.

eSentire, Inc., is The Authority in **Managed Detection and Response** Services, protecting the critical data and applications of 1000+ organizations in 70+ countries from known and unknown cyber threats. Founded in 2001, the company's mission is to hunt, investigate and stop cyber threats before they become business disrupting events. Combining cutting-edge machine learning XDR technology, human expertise, and proven security operations leadership, eSentire mitigates business risk, and enables security at scale. The Team eSentire difference means enterprises are protected by the best in the business with a named Cyber Risk Advisor, 24/7 access to SOC Cyber Analysts and Elite Threat Hunters, and industry-leading threat intelligence research from eSentire's Threat Response Unit (TRU). eSentire provides Managed Risk, Managed Detection and Response and Digital Forensic and Incident Response services. For more information, visit **www.esentire.com** and follow **@eSentire**.