Critical Detection Capabilities

Managed Detection and Response

ALERT LOGIC™

Contents

Executive Summary

Alert Logic is a Managed Detection & Response (MDR) vendor who delivers peace of mind from threats by combining 24/7 SaaS security with visibility and detection coverage wherever your systems reside. We achieve this through a platform that provide complete coverage of your attack surface and turns data into valuable information which can be actioned to improve the security posture of your organization.

This document provides additional detail into some of the detection capabilities of the Alert Logic MDR service.

Introduction

Detecting cyber threats to critical systems and infrastructure is more challenging than ever. Organizations are moving away from multiple, complex, point solutions to alternatives that simplify and reduce costs associated with threat detection. One approach growing in popularity is managed detection and response (MDR). Alert Logic is the industry's first SaaS-enabled MDR provider, delivering unrivalled security value. Our purpose-built technology and team of MDR security experts protect your organization and empower you to resolve whatever threats may come. Alert Logic's detection capabilities and services deliver meaningful detection outcomes uses five critical capabilities:

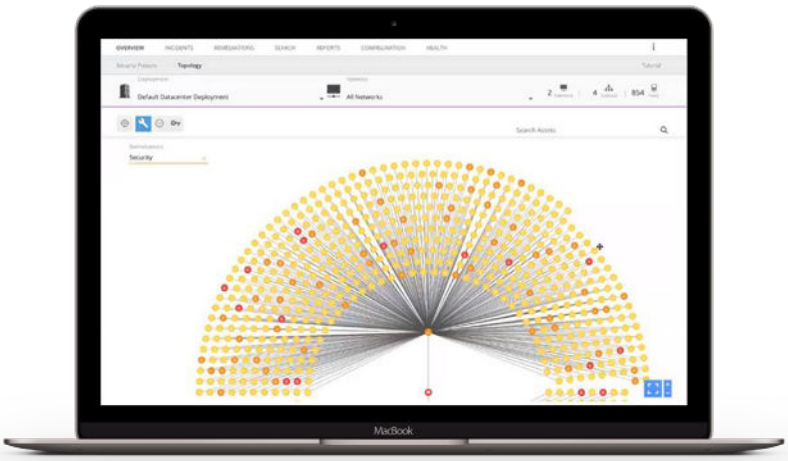
1. Comprehensive Visibility through Discovery and Assessment
2. Continuously Updated Threat Intelligence
3. Advanced Analytics
4. Community Defense
5. Broad Compliance

Visibility

Comprehensive visibility is vital for effective threat detection because as the saying goes, *you can't secure what you can't see*. Visibility includes discovery of assets across your environment, including those in the public cloud, your network infrastructure, endpoints, off-the-shelf and custom web applications, containers, and additional data sources for enrichment and context.

ASSET LOCATION	DATA SOURCE	DESCRIPTION
AWS	AWS API + CloudTrail	Cloud asset discovery and log file delivery for analysis
Azure	Resources API	Cloud asset discovery
Data Center & Google Cloud Platform	Alert Logic appliance	Discovery using IP address range belonging to network
Windows/Linux	Alert Logic agent	Provides host-level metadata updates

Once the data sources are identified the information must be refreshed on a regular basis. To do this, Alert Logic uses a tailored recurring polling process. Alert Logic presents this coverage through a topology map which allows you and our Security Operations Center (SOC) analysts to view assets, configuration details, and protection levels, then integrate the data in any event investigation.



Topology Map

Vulnerability Assessment

Identifying and classifying weaknesses that could be exploited by a bad actor is the next step. This is achieved through application and operating system assessment to identify exposures such as known vulnerabilities, mis-configurations, and password complexity which are the most common areas to exploit according to our SOC data.

Alert Logic maintains a constantly growing library of ~120,000 vulnerabilities which is a combination of open-source intelligence feeds and metadata from our 4000+ customers. Our team of experts provide guidance to ensure you achieve efficiency with configuration, scoping, and knowledge transfer with remediation guidance and response options. This information is also presented through easy to use dashboards and reports.

Alert Logic is also a PCI Approved Scanning Vendor (PCI-ASV) and provides dedicated scanning and reporting to satisfy PCI compliance requirements with remediation assistance. Multiple compliance mandates can be met including HIPAA, HITRUST, and SOC2.

Alert Logic continually assesses your AWS and Azure configuration by performing cloud configuration checks. The checks cover security best practices, drawing from multiple sources like Center for Internet Security (CIS) and the cloud providers themselves.

The CIS benchmarks are also available to you as separate, certified reports.

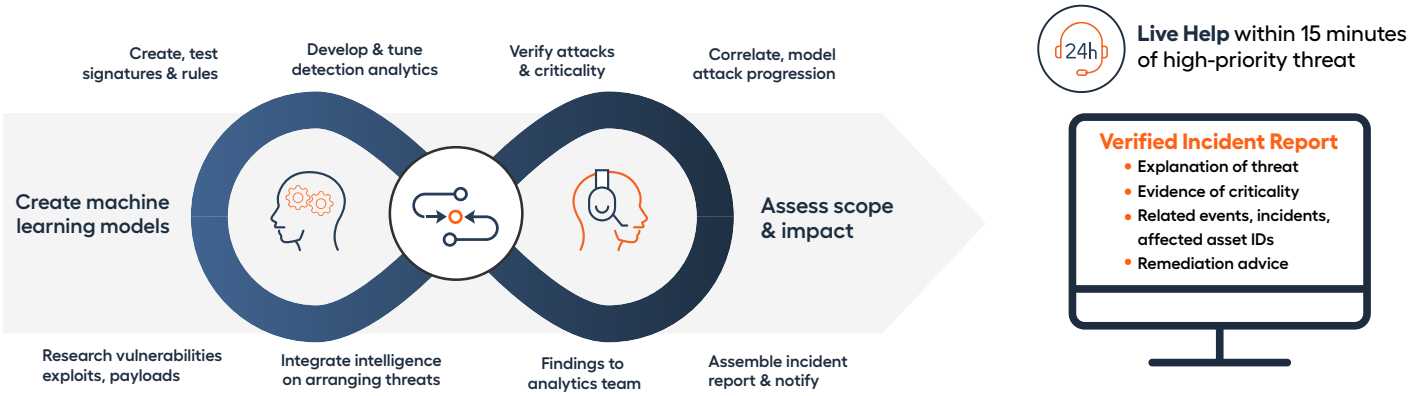
Threat Intelligence

Threat intelligence plays a critical role in providing effective managed detection and response. It requires a combination of knowledge and expertise to add context to make data actionable. Alert Logic has built a strong threat intelligence team which works as an organized and coordinated group of multi-disciplined research teams. Below is a sample of the different Alert Logic threat intelligence functions:

- **MALWARE ANALYSTS** — study what different types of malware samples do when they get executed to help prevent it from spreading
- **NETWORK SECURITY EXPERTS** — analyze attacks at the network layer to create effective detection techniques
- **VULNERABILITY RESEARCHERS** — study how vulnerabilities can be detected as quickly as possible
- **DATA SCIENTISTS** — study large structured and unstructured data sets to improve data models that create actionable outcomes

These teams work together to create an integrated security model which is continuously improved to help customers achieve outcomes that matter. Coupled with our SOC, this results in a one-stop-shop that provides you with vigilance 24/7, eliminates noise and false positives, and augments incidents with severity and remediation guidance.

Integrated Security Model



Advanced Analytics

A collection of sophisticated techniques is used to identify threats in the Alert Logic MDR platform. Below is a sample of some of those techniques and their purposes.

Log Data Monitoring

A core function in threat detection is mining and parsing log data to find hidden threats. This function requires several types of data feeds, advanced analytics, machine learning, human insights, and expertise to improve the data models and reduce false positives. Alert Logic provides:

- Insights from log analysis to recognize issues that need to be remediated to prevent future attacks
- 24/7 expertise to help resolve any incidents based on logs and other detection sources
- Understanding of network traffic, protocols, and alert volumes at a high level and drill down to uncover the necessary details using intuitive dashboards
- Actionable insights by leveraging machine learning and other analytics to filter out noise
- Guidance to ensure all relevant detection sources are optimally configured during the deployment process
- Compliance adherence by scanning regularly and storing logs for one year

There are several types of data sources and each of them provide distinct information for Alert Logic's team of experts for detecting threats.

Log Sources

SOURCE PLATFORM	DESCRIPTION
AWS	Logs ingested from AWS are used for two specific use cases; automation and threat detection
Azure	Logs ingested from Azure are used for two specific use cases; automation and threat detection
Operating System	Operating system logs give Alert Logic information about access and significant events
Server	Server applications are prone to attack and exploitation, logs from these sources provide valuable information
Anti-Virus	Provides key insights for alerting and Security Operations Center (SOC) support, such as detection of known hacking tools and writing to privileged locations
Database	Database access logs can provide valuable intelligence around access and change in the database system
Devices	Ingestion of device logs can provide valuable intelligence around perimeter access and exploitation of the devices themselves
Other	Alert Logic can accept logs from a huge variety of sources. Some security sources will generate incidents based on their output

We offer integration with applications, including API-based integration with SaaS applications and passive log collecting through syslog forwarding with most firewall platforms. Available applications include products for authentication, productivity, management, and more. Alert Logic serves as a remote collector to receive log data from SaaS and firewall applications related to different incident types, depending on the product type.

The Application Registry is a repository of platform integrations in your Configuration page in the Alert Logic console, and new integration points are continually being added. The Application Registry allows you to configure multiple third-party applications to collect and generate logs. Integration with third-party applications adds administrative and security value to your organization.

The next section we will go into more detail about what we do with different types of logs.

Enhanced Detection With Firewall Logs

Currently we process logs for Cisco, Fortinet, and Palo Alto Networks firewalls. Alert Logic leverages analytics to generate insights of relevant security information that is derived from one or multiple sources from the firewall application log data. These insights can identify security patterns and allow us to conduct threat hunting. Examples include:

- Brute force password guessing for a user for a certain amount of time
- An anomalous number of resource downloads for a user deviated from normal activity
- An unknown service or process in the environment that is being used by a public facing system
- Activity from a blacklisted IP address

Enhanced Detection For Authentication Application

To battle credential theft, organizations often use Identity & Access Management (IAM) solutions. Alert Logic has built collectors to capture data from Auth0, OKTA, and Cisco Duo to create security content that is used to generate incidents for key security use cases. Security incident examples from IAM log data include:

NAME	DESCRIPTION
Brute force activity	Trigged once attempts thresholds for single user or multiple users
Login attempt from risky IP	Failed login attempt from known malicious IP addresses
Multi country login	User login from multiple countries on the same day
Credential stuffing	Brute force attack using leaked credentials
Privilege escalation	User grants administrator privilege to other users

Enhanced Detection For AWS and Azure

Cloud security is a shared responsibility and each cloud service provider interprets that in their own way. We leverage our relationships to make security simple and transparent for you no matter where you are on your cloud journey.

Migration Phase: This phase is focused on removing barriers and gaining alignment to enable a cloud-first strategy. In this phase Alert Logic helps you by addressing the cloud security skills gap with our SOC and threat research team. Our platform provides heterogenous coverage for cloud and on-prem environments, and the ability to bring all the elements together to maintain compliance.

Modernization Phase: In this phase security needs to keep pace with IT so the organization may become more agile. Alert Logic helps you by identifying misconfigurations in the cloud and potential vulnerabilities in applications, automating vulnerability detection to quickly identify and fix application and operating system vulnerabilities, and address threats in containers and web applications to confidently deliver security applications quickly.

Optimization Phase: Organizations in this phase are cloud-only and focused on maximizing their efficiencies. Alert Logic helps you in this phase by providing a unique agent-based solution which enables Network IDS for North/South as well as East/West traffic. Our platform is optimized for multi-cloud environments so organizations can choose the right cloud for the right workload while maintaining security. Native API integration into AWS and Azure enables critical data aggregation for a full picture of the entire cloud surface.

Enhanced Detection For SaaS Applications

Alert Logic builds collectors for Office 365, G-Suite, and Salesforce. We also have an API to address the long tail of other applications. All of this is used to create security content for use cases. A sample includes:

- User Login Anomalies
- User Behavior Anomalies
- Suspicious Administrative Actions

Network Traffic Analysis (NTA)

Networks Traffic Analysis (NTA) identifies attacks as they traverse in and out of the network. It analyzes traffic to and from all devices looking for patterns, abnormal behavior, and writing telemetry signatures. This allows detection of lateral movement, brute force attacks, privilege escalation, ransom ware, and C&C exploits.

Enhanced Detection For Containers

Alert Logic provides the industry's only network intrusion detection solution and log management for containers and applications in hybrid and multi-cloud environments. By analyzing North/South as well as East/West traffic we can rapidly detect network intruders leading to shorter dwell time and reducing the impact of a successful attack. Our integrated, agent-based solution protects all workloads (container or not) and provides a graphical representation of a compromised container and its relationships.

Web Log Analytics

Alert Logic Web Log Analytics (WLA) enhances our web app threat detection capabilities by adding log-based threat detection and solves the visibility issue caused by modern transport encryption. This unique log-based threat detection analyzes the decrypted web server access logs (Apache, NGINIX, IIS) using a combination of pattern-matching, anomaly detection, signatures, and advanced correlations providing coverage for much of the OWASP Top 10.

Alert Logic WLA includes these capabilities:

- Signature-based Detection of General Web Attack Methods
  - SQL Injection
  - Cross-site Scripting (XSS)
  - Automated Threats
  - File Path Traversal
  - Command Injection (CMDi)
- Known Vulnerability and Exploit Detection and Attribution
  - Exploits Targeting Known Vulnerabilities (CWE)
  - Known Web Shell Compromises that Lead to Remote Exploitation
- Anomaly-based Detection
  - Brute-force Password Guessing Login Attempts
  - Unknown Web Shell Compromises

These detection capabilities allow Alert Logic to detect incidents across a wide spectrum which include:

INCIDENT	DESCRIPTION
Web Reconnaissance	Clear enumerating or attack activity detected
Server Error	Attack activity generating 500-type error responses from targeted web server
Access to Unauthorized Resource	Injection or Remote Command Execution followed by access to potentially uploaded (anomalous) resource indicating upload and access to web shell
Access to Anomalous Resource	Access to URL paths that are anomalous
Attack Targeting Specific Vulnerabilities	Exploits against specific known vulnerabilities
Unauthorized Vulnerability Scan	Web server attack observation from an unknown source
Authorized Vulnerability Scan	Attack from Alert Logic or other known provider as part of security assessment, auditing, or pen testing

Alert Logic WLA is a unique solution which identifies attacks across all custom web apps throughout the enterprise, providing visibility into the most vulnerable and attacked applications, and allowing security leaders to make data-driven decisions on security controls.

File Integrity Monitoring (FIM)

Alert Logic's FIM detects unauthorized change events to operating system, content, and application files for Windows and Linux servers. This includes integrity of system directories, registry keys, and values on the operating system. By monitoring for suspicious file change events, your organization can meet many compliance standards. Alert Logic sees the primary use case in compliance for PCI-DSS 10.5.5 and 11.5 which is change detection for log files and critical system files. It also satisfies additional compliance requirements including SOX Section 404, HIPAA - §164.312 (b), (c)(1) & (2), SOC 2, and HITRUST which all include change detection controls for integrity of files and folders.

This detection technology leverages the rich telemetry data from the Alert Logic agent installed on servers so there is no additional agent footprint necessary. Once configured it creates a repository of all SHA1 hashes of the monitored paths and records any deviations. Reporting will include information of any file change events including time stamp, host name, file path, event type, and deployment. This helps provide context to understand if the changes are from external bad actors, well-meaning insiders, or malicious insiders engaging in nefarious activities.

Endpoint Detection

Alert Logic's Endpoint Detection intelligently blocks attacks through a combination of machine-learning attribute analysis and real-time behavior analysis and provides deep visibility without impacting performance. Our next-generation endpoint coverage dynamically combines machine-learning and behavior indicators to identify file-less and binary file attacks while reducing false positives for Microsoft Windows and Windows Server. This includes hosted instances of these platforms on AWS, Azure, Google Cloud, Oracle Cloud, and on macOS at no additional cost.

Alert Logic gathers thousands of samples each day and uses machine learning to analyze these samples to improve coverage and accuracy. Customers then transparently receive new models to get the best detection, resulting in fewer false positives because the model has already been trained with the specific software that customers are running. Alert Logic Endpoint Detection can run alongside existing anti-virus and endpoint security tools to provide the last line of defense.

Community Defense

To achieve community defense a security vendor needs a large data set. Alert Logic has more than 4,000 customers providing billions of IDS events and trillions of logs which are analyzed by our security platform, pushing over 7,000 incidents to our SOC each week. Each incident is manually triaged against your specific rule set to decide if it is a real incident and needs escalation. On average there are two high/critical incidents each month.

When Alert Logic identifies an attack pattern and its respective target, we are able to parse through rich telemetry data to identify and proactively inform you if you fit the same profile and provide guidance to mitigate the potential of falling victim to this type of attack.

Compliance

Alert Logic helps you advance your compliance program quickly without hiring new staff, and comply with mandates and standards such as PCI, HIPAA, HITRUST, SOC 2, GDPR and NIST. Alert Logic also provides several audit-enabling reports and help your staff stay one step ahead of requirements, mandates, and auditors.

Conclusion

Security professionals agree there is no silver bullet in security as no investment will provide 100% guarantee. Threat detection is a critical component for achieving desired security outcomes. It must have wide visibility and be paired with strong security expertise to provide actionable intelligence and improve security posture. Alert Logic has the most robust ecosystem coverage with a large team of expertise across multiple security disciplines, making enterprise class security affordable for all organizations. This allows your organization to be better prepared for future attacks, compliance mandates, world events, or the next phase of your digital transformation journey.

To learn more about how we can help improve the security posture of your organization, please explore Alert Logic's online resources.