FORTRA

GUIDE

# Critical Detection Capabilities

## Introduction

Detecting cyberthreats 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. Fortra's Alert Logic MDR®, the industry's first SaaS-enabled managed detection and response provider, delivers unrivaled security value. Our purpose-built technology and team of security experts protect your organization and empower you to resolve whatever threats may come. Alert Logic's detection capabilities and delivery of meaningful detection outcomes uses five critical capabilities:

1. Comprehensive Asset Visibility
2. Continuously Updated Threat Intelligence
3. Advanced Analytics
4. Community Defense
5. Broad Compliance

## Comprehensive Asset Visibility

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

We integrate these data sources within several types of deployments:

| 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 data sources are established, the information must be refreshed on a regular basis. We accomplish this through a tailored recurring polling process.

IT estates are dynamic and always evolving, requiring constant updates to ensure asset coverage remains consistently high. We recommend and help you set up rediscovery of new assets through polling at least once per day, and more frequent polling as needed to identify more granular changes in areas like asset configuration. 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.

### Vulnerability Assessment

Once visibility is achieved, the next step is to identify and classify weaknesses that could be exploited by a bad actor. This is achieved through internal and external vulnerability scanning to identify exposures including known vulnerabilities, misconfigurations, password complexity, and many more.

Our vulnerability library contains approximately 120,000 vulnerabilities which combines open source intelligence feeds and metadata from our 4000+ customers. Our team also provides guidance to ensure you achieve efficiency with configuration, scoping, and knowledge transfer. Outputs are available in multiple report options allowing your security staff to choose which report or set of reports works best for vulnerability management. We also offer remediation guidance and tuning assistance.

Alert Logic is a PCI Approved Scanning Vendor (PCI ASV) and provides dedicated scanning and reporting to satisfy PCI compliance requirements with remediation assistance. Other compliance mandates available include HIPAA, HITRUST, and SOC2.

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

CIS results are available to you as separate, certified reports as well as a unified list including scanning vulnerabilities.

## Continuously Updated Threat Intelligence

Cyberthreat 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. Our threat intelligence team works as an organized and coordinated group of experts across different areas. Following is a sample of the different Alert Logic roles:

**Malware Analysts** — study what different types of malware samples do when they get executed to help prevent them from spreading

**Network Security Experts** — analyze attacks at the network layer to create effective detection techniques

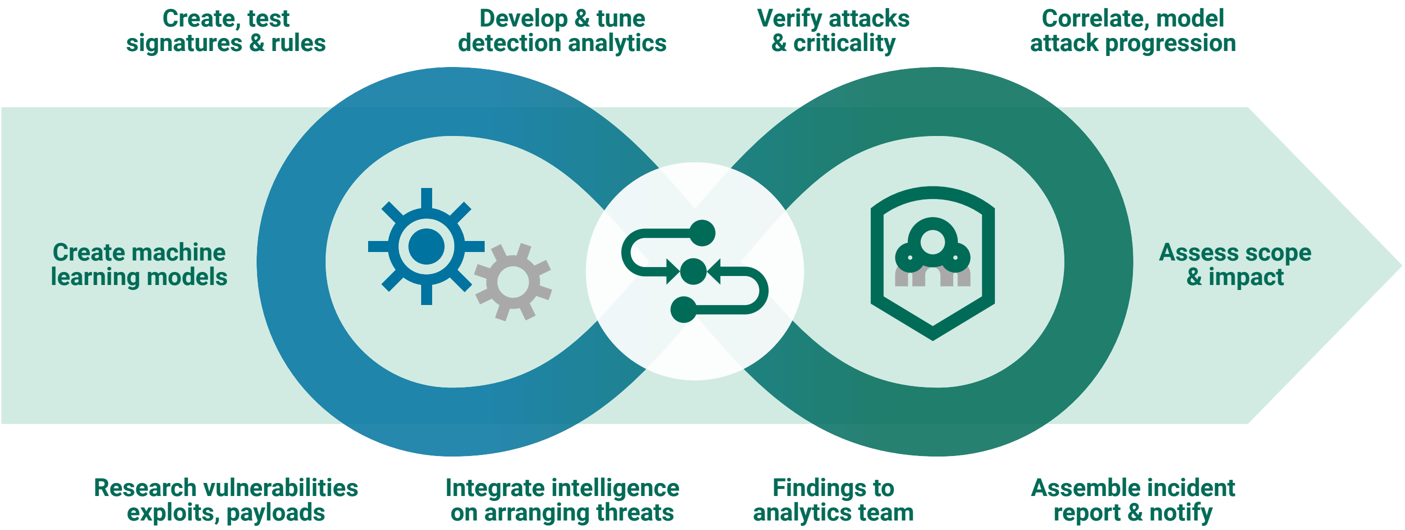
**Reverse Engineers** — take apart software programs and focus on how a vulnerability works

**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

**Security Architects** — bring all the elements together so customers can achieve their security outcomes

This result is a one-stop-shop that provides you with vigilance 24/7, eliminates noise and false positives, and validates incidents with severity and remediation guidance.


Create, test signatures & rules
Develop & tune detection analytics
Verify attacks & criticality
Correlate, model attack progression
Create machine learning models
Assess scope & impact
Research vulnerabilities exploits, payloads
Integrate intelligence on arranging threats
Findings to analytics team
Assemble incident report & notify

# Advanced Analytics

A collection of multiple 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

OA 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, and expertise to improve data models and reduce false positives. Alert Logic provides:

- Insights from logs to recognize issues that need to be remediated to prevent future attacks
- Log monitoring for real-time malicious activity detection
- 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
- Dramatically reduce wasted activity because the noise is already filtered out
- Oversight to ensure all relevant detection sources are optimally configured during the deployment process
- Compliance requirements by scanning regularly and storing logs for one year

There are several types of data sources and each provides distinct information for detecting threats.

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 Alert Logic Console Configuration page; new integration points are continuously 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.

## Enhanced Detection with Firewall Logs

Alert Logic performs observations of relevant security information derived from one or multiple sources from the firewall application log data. Observations do not always meet our criteria to generate an incident but can demonstrate security value. Observations can identify security patterns and allow you to conduct threat hunting.

Examples of observations Alert Logic can perform if detected from firewall application log data include:

- An IP address in logs matches with listed blacklisted IP addresses
- 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
- A new created service in the environment that is being used by a customer or external systems (generates incident)
- Blacklisted IP addresses creating successful connections to most popularly exploited services in the network of a customer (generates incident)
- A blacklisted IP address successfully probed a new internal resource (generates incident)
- Alert Logic processes logs from the following firewalls:
  - Cisco
  - Fortinet
  - Palo Alto

## Enhanced Detection with Authentication Application (Auth0, Cisco Duo, Okta)

To battle credential theft, organizations often use multi-factor authentication (MFA). Alert Logic has built collectors to capture data from Auth0, Okta, and Cisco Duo MFA applications to create security content that is used to generate incidents for key security use cases.

While MFA products provide different levels of logging detail, incidents generated fall into the following categories:

- Administrative Actions
- User Login AD
- User Behavior AD

### The Alert Logic Okta collector can collect data relevant to:

- Event Log Information
- User Information
- Group and Group Membership Information
- Application and Application Assignment Information

### The Alert Logic Auth0 Log Collector gathers data relevant to:

- Successful User Logins
- Failed User Logins, Including Reason for Failure
- Token Exchanges (Success & Failure)
- Login Warnings
- User Deletions
- Connection Errors
- User Signup Events
- Email Verification Events
- Password Changes
- Rate Limiting Events
- Operational Events
- Operational Errors

### The Alert Logic Cisco Duo collector polls the following APIs for various types of data:

- Authentication
- Administrator
- Telephony
- Offline Enrollment

## Enhanced Detection with IaaS (AWS, Azure)

Each cloud provider has unique offerings, so Alert Logic works closely with the cloud providers to understand their security challenges and provide services tailored to them. Leveraging this relationship and expertise means removing a significant factor in an already steep learning curve, reducing risk significantly along the three primary phases of the 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 integration into cloud with API-driven integration into AWS and Azure enables critical data aggregation for a full picture of the entire cloud surface.

### Enhanced Detection with CRM/SaaS (O365, SFDC)

Alert Logic builds collectors to capture data from Office 365, Salesforce, and other applications to create security content to generate incidents for key security use cases. Examples include:

- Microsoft Office 365 Exchange Audit Logs
- SharePoint Audit Logs
- General Audit Logs
- Administrative Actions
- User Login AD
- User Behavior AD

### Enhanced Detection with Third-Party EDR/Anti-Virus (Carbon Black, Cisco AMP, CrowdStrike, Cylance, SentinelOne)

EDR solutions are highly effective at protecting endpoints. However, bad actors constantly innovate their attack techniques to evade detection. Analyzing EDR logs help surface these stealthy attacks that slip through, including:

- Administrative Actions
- User Login AD
- User Behavior AD

## Network Traffic Analysis

Networks Traffic Analysis (NTA) identifies attacks as they traverse in and out of the network. NTA 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, ransomware, 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 and East/West traffic, we 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.

Amazon ECS
Amazon EKS
AWS Fargate
Elastic Beanstalk
kubernetes
CoreOS
docker

## Web Log Analytics

Fortra's 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, IIS, NGINIX) using a combination of pattern-matching, anomaly detection, signatures, and advanced correlations providing coverage for much of the OWASP Top 10.

Alert Logic WLA capabilities include:

- 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 includes:

| 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 that identifies attacks across all custom web apps throughout an enterprise, providing visibility into the most vulnerable and attacked applications. It also allows security leaders to make data-driven decisions on security controls.

## File Integrity Monitoring

Forta's Alert Logic File Integrity Monitoring (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. We see 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, all of which include change detection controls for integrity of files and folders.

This detection technology leverages the rich telemetry data from our agent installed on servers so no additional agent footprint is necessary. Once configured, it creates a repository of all SHA1 hashes of the monitored paths and records any deviations. Alert Logic recommends a recurring reporting and review schedule to investigate the detected changes. 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

Fortra's Alert Logic 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, Oracle Cloud, and macOS at no additional cost. Unlike solutions that generate models every four to six months to identify malicious files, Alert Logic automatically gathers thousands of samples daily 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 already was trained with the specific software that customers are running. Our Endpoint Detection can run alongside existing antivirus and endpoint security tools as 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 weekly. Each incident is triaged manually against your specific rule set to determine if it is a real incident needing escalation. On average, there are two high/critical incidents each month.

When Alert Logic identifies an attack pattern and its respective target, we 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.

## Broad Compliance

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

## Conclusion

Security professionals agree there is no silver bullet in security as no investment provides a 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 highly skilled SOC and threat research team, making enterprise-class security affordable for all organizations. We help your organization be better prepared for future attacks, compliance mandates, world events, or the next phase of your digital transformation journey.

**For more information, please visit alertlogic.com.**

FORTRA

Fortra.com

**About Fortra**

Fortra is a cybersecurity company like no other. We've created a simpler, stronger, and more straightforward future for our customers. Our trusted experts and best-in-class portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally for cybersecurity that prevails. Learn more at fortra.com.