Managed Detection & Response

Solution Documentation

ALERT LOGIC™

APRIL 2022

Contents

Documentation

This document provides specifications on Alert Logic's MDR Solution and the roles and responsibilities of Alert Logic and Customer with respect to Alert Logic's MDR Solution.

Offerings

Alert Logic provides managed detection and response, risk assessment, and visibility solutions. Different combinations of these solutions can be deployed under a node-based single license as ordered by Customer.

Alert Logic MDR Essentials

MDR Essentials delivers security assessment and posture management and endpoint detection capabilities to Customers with internal and external vulnerability scanning, PCI DSS Approved Scanning Vendor (ASV) scans, including dispute management, as well as cloud configuration checks, risk scoring, and audit-ready compliance reports.

Alert Logic MDR Professional

Subject to the SLA, MDR Professional provides 24/7 threat detection for traditional, hybrid, and cloud infrastructures and applications with escalation notifications accompanied by guidance. MDR Professional includes the features available in MDR Essentials.

Alert Logic MDR Enterprise

The MDR Professional service can be augmented with MDR Enterprise, in which a security analyst within one of Alert Logic's Security Operations Centers (SOC) is personally assigned to the Customer.

Entitlement

Alert Logic's MDR Solution is licensed based on the total number of nodes to be included in the subscription.

Subscriptions are based on banded tiers of node entitlements. For example, if a customer has 40 nodes for licensing, they will be placed in the 26 to 50 node tier.

A node is classified as a system which has one or more of the following properties

- Has the Alert Logic Endpoint Detection agent installed
- Is included in discovery & vulnerability scans
- Sends network or log data to Alert Logic for analysis

For licensing purposes, Customers can assign nodes based on the following capabilities. For each licensed node Customers can choose to deploy the endpoint detection to one asset and the other functionality to a different asset:

	TOTAL CUMULATIVE ASSIGNABLE NODES			
	Licensed Nodes	**Endpoint Protection**	**Discovery & Vulnerability**	**IDS & Log Agent**
ESSENTIALS	100	100	100	0
PROFESSIONAL	100	100	100	100
ENTERPRISE	Monthly charge on top of MDR Professional license			

Each node which sends log data to Alert Logic has an allowance of 100MB of log data per day. SaaS sources, individual containers and serverless compute (e.g., AWS Fargate, AWS Lambda, Azure Functions) do not count as a node. However, they do count against the overall log volume entitlement.

Node discovery and calculation

Nodes are discovered and calculated based on a count of provisioned Alert Logic agents and using network discovery scans from the Alert Logic network appliance. A daily snapshot of node count is based on a de-duplicated count of agents & the discovery scan results.

Discovery scans will capture any device in a protected network with an open port or that responds to an ICMP echo response.

Daily node counts are averaged over a calendar month to minimize the cost implications of volatility introduced by changes and auto-scaling systems.

ENVIRONMENTS	DISCOVERY METHOD
AWS	Discovery of instances occurs in protected networks based on Cloud APIs
Azure	Discovery of instances occurs in protected networks based on Cloud APIs
Other Clouds	Hosts with provisioned agents
Physical & Virtual	Daily discovery scans
Container Systems	Based on a count of underlying host(s) that containers are deployed on, not individual containers

Calculation of usage for a calendar month is based on an average of hourly node counts for that month.

Implementation Options

Customers can implement Alert Logic's MDR Solution in a variety of infrastructure types; all implementations can be managed in a single online console. Customers have the option to segregate permissions, reporting, and other aspects of the MDR Solution through Alert Logic's account model and through separate implementations within each account, as described later in this document.

Implementations are supported by Alert Logic in cooperation with the Customer through onboarding and customer technical team enablement.

Automatic Mode

By allowing Alert Logic permissions on the indicated public cloud platforms activities such as network configuration, cloud log collection and appliance deployments can be performed automatically. Server and endpoint agent deployments must be performed by the Customer.

Manual Mode

In manual mode, configuration and appliance deployments must be carried out by the Customer or automated in its chosen framework.

Solution Overview

Alert Logic's MDR Solution is comprised of software as a service (SaaS) delivered technologies and tools combined with SOC Services.

The MDR Solution is deployed within a project framework delivered by Alert Logic based on Customer cooperation and Customer provided information.

Description

This section describes the customer-facing services for implementation, security operations, and support of the MDR Solution.

Implementation Support

Included in: MDR Solution | MDR Professional | MDR Enterprise

Alert Logic's MDR Solution depend on the technology deployed into the Customer's environments to collect, analyze, and forward data back to Alert Logic's systems for further analysis.

Customers are responsible for the installation of the appliances and system agents required to collect data. Appliance content, software updates, and agent version updates are managed by Alert Logic. Customers must choose either Europe or US as a location for storage of their data.

WHO DOES WHAT	
Alert Logic provides	Implementation and deployment expertise with remote support and guidance, SaaS-delivered deployed technology updates and a security analysis platform
Customers must	Configure their infrastructure, ensure appliances and agents can communicate with each other and Alert Logic systems. Ensure the deployment of the Alert Logic agent onto their systems is healthy and that new customers' systems are included in the deployment for protected networks by installing new agents or modifying network configuration
Partners can	Provide hands-on assistance for deployment and on-going management of the deployment of Alert Logic technologies into protected networks

Depending on the MDR offering subscribed to (MDR Essentials, MDR Professional or MDR Enterprise) deployment can include working on deploying scanning and detection technologies, setting up the service aspects, etc. Virtual meetings may be held that include Alert Logic project managers, technical implementation staff, and their Customer or partner counterparts.

Alert Logic will provide Customer access to a training portal, technical enablement (e.g., example deployment scripts and instructions), orientation and tuning & optimization preparation with Customer's cooperation.

24/7 Platform Support

Included in: MDR Solution | MDR Professional | MDR Enterprise

Subject to the SLA, support teams provide assistance with troubleshooting deployments, user interface, and general product queries, such as console support, agent installation, the configuration of alerts, appliance management vulnerability scanning configuration and output.

Alert Logic's support team will work with the Customer and use commercially reasonable efforts to resolve requests by providing advice, guidance, and the appropriate knowledge base articles, if any.

Vulnerability Insight Support

Included in: **MDR Solution** **MDR Professional** **MDR Enterprise**

Alert Logic will assist Customers with configuring scans within the console for PCI, external, or internal scans, verifying scanning scope and determining whether a complete scan of systems is possible.

Customers may contact support teams for guidance on how to identify and potentially remediate vulnerabilities that have been identified by an internal or external scan, or to tune out false positives.

PCI Dispute & PCI DSS & ASV Program Support

Included in: **MDR Solution** **MDR Professional** **MDR Enterprise**

Alert Logic provides dedicated scanning and reporting features and services for PCI Scanning. Alert Logic is a PCI-approved scan vendor (ASV).

Following a PCI Scan, the Customer will review its compliance report and may notice failures against elements of its environment. If there are false-positive results or the Customer has compensating controls in place, the Customer is able to dispute these scan results via the Alert Logic Console but may also choose to contact Alert Logic Support directly. Disputes will be reviewed and responded to by PCI ASV accredited team members.

MDR Concierge

Included in: **MDR Professional** **MDR Enterprise**

Customers are assigned a single point of contact for business planning and service management activities.

The concierge performs strategic account planning and account health, business, roadmap, and security posture reviews in cooperation with the Customer and based on Customer provided information. The MDR Concierge will hold regularly scheduled calls and, where appropriate, attend Customer's meetings virtually for more in-depth reviews.

24/7 Threat Management

Included in: **MDR Professional** **MDR Enterprise**

Alert Logic monitors Customer environments for exploitation of services. Data from the deployed security technologies are sent back to Alert Logic's systems for further analysis. Subject to the SLA, 24/7 Security Operations perform further analysis, triage and escalate verified incidents to Customer contacts with guidance and suggested actions to help mitigate potential damage.

WHO DOES WHAT	
Alert Logic provides	Subject to the SLA, 24/7 Security Operations and required technology to monitor for threats and escalate them to customers
Customers should	Ensure availability of appropriate employees to receive escalations and should have a documented process for staff to follow if Alert Logic escalates an incident to them
Partners can	Act as an intermediary taking escalation calls from Alert Logic and performing remediation on behalf of the Customer with their consent

Escalation

Included in: MDR Professional MDR Enterprise

Designated Security Experts will triage and analyze detected incidents of a high enough severity to determine whether the observed threat is legitimate (true-positive) or benign activity (false-positive). When detected threats are determined true-positive, experts will seek to identify indicators that prove or suggest (where insufficient data is available to be comprehensively accurate) whether the attack was successful or unsuccessful, and will pin the indicating IDS events or logs to the incident within the Alert Logic Console, along with notes to back up their analysis. The expert will provide recommendations to the Customer designed to help prevent similar attacks.

Depending on the nature and success of the incident, the expert can set the threat rating to either Low, Medium, High, or Critical.

Incident Criticality

<table>
<tr><th>SEVERITY</th><th>DESCRIPTION</th><th>ESCALATION POLICY</th><th>CUSTOMER ACTIONS</th></tr>
<tr><td>Critical</td><td rowspan="2">Problems requiring immediate remediation to reduce exposure</td><td>Escalate to the designated contacts in priority order until successful</td><td rowspan="2">Review email/phone escalation when received & take appropriate action</td></tr>
<tr><td>High</td><td>Provide direct customer support throughout the duration of the incident</td></tr>
<tr><td>Medium</td><td>Incidents requiring closer observation and monitoring, but do not require real-time response</td><td rowspan="2">System automatically escalates via email to all designated security contacts</td><td rowspan="2">Access the Alert Logic Console to view incident details</td></tr>
<tr><td>Low</td><td>Common events, often referred to as "Internet Noise," which are automatically logged for reporting</td></tr>
</table>

All incidents are available to view in detail in the Alert Logic Console

On-Demand Tuning & Sensor Optimization

Included in: MDR Professional MDR Enterprise

Customer may request that detection technologies be tuned to reduce false-positive incident generation or incidents that are of no interest/value to the Customer.

A security analyst will review recent incidents, IDS events, and logs in any known context of the Customer's environment and look to identify any trends or high-volume activity that could be considered noisy to the Customer.

The analyst will schedule a mutually convenient time with the Customer to seek additional context of the Customer's environment and a better understanding from the Customer as to what notifications and escalations it perceives to be valuable and those that are not. The analyst may suggest some changes based on its prior review, but ultimately will gather the Customer's expectations and provide options for tuning Alert Logic's detection technologies.

Once options have been agreed upon by the Customer, the analyst will tune detection technologies following standard processes and provide confirmation of implementation to the Customer via the open Support ticket.

Log Review

Included in: MDR Professional MDR Enterprise

The Log Review service generates reports on notable observations using a combination of rule-based analytics and machine learning generated baseline anomalies against sourced data, within the past 24 hours.

Observations are anomalies and other indicators of suspicious activity that are not immediate calls to action, but may generate security insights upon review.

Results are customized by Customer's organization's trends and patterns at the account, host, and user levels. As part of the Log Review Service Customers receive guidance, custom tuning, and manual checks. Customers are encouraged to schedule the various use case reports daily so that the activity can be reviewed and validated that the detected anomalies represent approved system and user behavior, particularly those seeking to satisfy PCI DSS 10.6.

Logs analyzed in the Log Review service include:

- Microsoft Active Directory
- Oracle and SQL Databases
- Network Devices
- Windows Server
- UNIX/Linux
- Amazon Web Service

Designated Security Expert

Included in: MDR Enterprise

Customers are assigned a single point of contact for security operations to support the MDR Solution.

The Designated Security Expert carries out several on-request and pro-active activities such as threat hunting, weekly reviews, virtual customer meetings, and providing on-request, comprehensive, security posture reports.

Designated security experts work with the assigned MDR Concierge.

Continuous Threat Hunting

Included in: MDR Enterprise

The Designated Security Expert will receive regular reports on sensors within Customer networks that are generating high volumes of events and will proceed to investigate the activity upon which the sensor is firing for potential threats. If a threat is identified, the analyst will create an incident and escalate the activity to the Customer as per standard Incident Analysis processes.

Pro-Active Tuning & Sensor Optimization

Included in: MDR Enterprise

The Designated Security Expert will review recent incidents, IDS events, and logs in any known context of the Customer's environment and look to identify any trends or high-volume activity.

The Designated Security Expert will schedule a mutually convenient time, or leverage the weekly security review, to discuss what notifications and escalations the analyst perceives to be valuable and those that are not. The analyst will gather the Customer's expectations and provide options for tuning Alert Logic's detection technologies designed to meet the Customer's requirements.

Once options have been agreed upon by the Customer, the Designated Security Expert will tune detection technologies following standard processes and provide confirmation of implementation to the Customer.

Tuning

Events and incident thresholds are tuned by the SOC in response to internal processes and Customer requests. Tuning adjusts the severity and likelihood of incidents or turns them off completely.

WHO DOES WHAT	
Alert Logic provides	Technology for monitoring network packets including appropriate content and systems for detection of threats, against customer systems and applications, including tuning
Customers must	Ensure port mirroring, and agents are configured or deployed, request tuning where required in response to incidents
Partners can	Manage escalations and provide hands-on remediation for incident

Extended Security Investigations

Included in: **MDR Enterprise**

Upon identification or suspicion of a threat or attack against a Customer's infrastructure, Customer may request assistance from Alert Logic to analyze data from the affected environment to ascertain and report upon the legitimacy of the suspected threat and or its impact.

Alert Logic will review and analyze available data and metadata ingested from the Customer environment to identify the suspected threat reported and communicate any perceived successful or failed attacks against the infrastructure.

Alert Logic will facilitate the investigation analysis through analyzing data from the following sources (where available/applicable):

- IDS Events
- Raw IDS traffic packet captures
- Event logs
- Web Application Firewall Deny Logs
- User behavior analysis
- Recent vulnerability scan results
- Network diagrams and asset discovery data

Should Alert Logic require access to additional data that has not been in scope for monitoring by Alert Logic, Alert Logic may request this data from Customer to support its investigation.

When Alert Logic has reached a conclusion, this information will be presented back to the Customer in the form of a summary, along with any key evidence or observations.

Weekly Security Review

Included in: MDR Enterprise

An optional weekly call with a Customer to discuss the findings of the data acquired that relate to its current security posture.

This report is generated on a per-customer basis. It provides a summary of Customer activity and security findings, including observations for addressing the security architecture, policies, process, and configuration gaps to help improve the Customer's security posture.

Annual Virtual On-site

Included in: MDR Enterprise

Once per calendar year, the Designated Security Expert will meet with Customers virtually to hold in-depth meetings, meet key stakeholders and build relationships to foster a collaborative approach to protecting the Customer's systems.

The virtual meetings can cover a variety of topics, including:

- Customer Architecture Overview
- Solution Training
- Security & Solution Health
- Analyst Processes & Practice

Hybrid Asset Discovery

Included in: MDR Solution | MDR Professional | MDR Enterprise

Alert Logic will help discover assets in configured networks and build an asset model. The asset model contains data on servers, networks, and other assets, depending on the environment.

The asset model can be interacted with through the topology map in the Alert Logic user interface.

Customers can access the asset model programmatically via the Alert Logic Assets API.

WHO DOES WHAT	
Alert Logic provides	Technology for discovery of assets, visualization and enrichment of incidents and reports
Customers must	Configure their systems to allow access of discovery scans, send appropriate cloud logs and/or deploy the Alert Logic agent
Partners can	Integrate the Alert Logic Asset API with Customer or partner ITSM or other IT systems to enrich systems and provide the foundations of a CMDB

Discovery Process

Included in: MDR Solution | MDR Professional | MDR Enterprise

Where available, cloud services are integrated with the MDR Solution in order to ingest asset details for inclusion in the asset model.

In other environments, a combination of network scanning from the Alert Logic appliance and data from installed system agents is used.

Discovery by environment

ENVIRONMENT	METHOD / SOURCE	MINIMUM FREQUENCY	REQUIREMENTS
AWS	AWS API augmented by recommended Cloud Trail Integration	Once per day	AWS IAM Role
Azure	Resources API	Once per day	Azure RBAC Role
Other	Network appliance discovery scan and/or Agent	Once per day	Open ports and ICMP echo*

**ICMP Echo is the minimum requirement for asset discovery, Customers should configure scanning credentials to get more asset detail.*

Once assets are discovered, Customers can configure the scope of protection for each environment.

Internal & External Vulnerability Scanning

Included in: MDR Essentials | MDR Professional | MDR Enterprise

Alert Logic uses vulnerability scanning information for pro-active notification of increased risk.

CATEGORY	DESCRIPTION
Security	Known CVE Vulnerabilities, dangerous access setup and standards contraventions (e.g., CIS Benchmark)
Configuration	Configurations that affect Alert Logic's visibility for detecting threats*
External	Security Exposures found during external scans

**Service affecting configurations will be displayed for features appropriate for the scope of protection in that deployment.*

Scanning of internal and external assets is managed in the user interface and vulnerabilities are collated into remediation recommendations based on a common action (e.g., where upgrading to a certain software version can fix multiple vulnerabilities).

Internal Scanning

Alert Logic runs both authenticated scanning of installed software and unauthenticated network port scans within Customer environments. These scans are switched on by default and require configuration of Customer-owned infrastructure to allow access to hosts and systems by scanning infrastructure. Whenever possible, the Alert Logic network appliance should have unrestricted access to protected networks.

When configuring each deployment, the schedule that scans will run on can be configured varying between "on a specific day within an 8-hour window" and "whenever necessary." In AWS, scans are initiated by changes detected when Cloud Trail notifies that an asset has changed, e.g., a new EC2 instance is started.

External Scanning

Alert Logic provides unlimited external vulnerability scans against Customer's public services. External assets for scanning are configured in the deployment configuration, where a DNS name or IP address can be added.

External scans are configured to assess open ports and web applications for vulnerabilities, including, but not limited to, OWASP Top 10 vulnerabilities.

WHO DOES WHAT	
Alert Logic provides	End-to-end external scanning services from Alert Logic's data centers, scheduling, reporting and vulnerability management systems with 24/7 support
Customers must	Configure external assets for scanning and decide on scanning schedules
Partners can	Provide extended services for mitigation of discovered vulnerabilities

Cloud Configuration Checks

Included in: MDR Solution | MDR Professional | MDR Enterprise

Alert Logic creates security remediations when issues related to the configuration of cloud services have been identified during a scan.

Alert Logic's system will monitor and present security problems found in both AWS and Azure. Setup of access is required.

PLATFORM	PRE-REQUISITES
AWS	Create a CloudTrail and SNS topic Setup AWS IAM policy Setup AWS Cross-account role
Azure	Create an app registration in Azure Create a custom RBAC role Grant permissions to access Microsoft Graph Grant permissions to access Azure Key Vault

Alert Logic may also create configuration remediations when issues related to Customer's deployment can hinder Alert Logic from delivering, such as no agents or appliance installations, or a misconfiguration where an appliance cannot connect to the backend. The following are some examples in which Alert Logic will create a configuration remediation:

- Hosts have not been recently scanned
- Insufficient policy and role privileges
- AWS Config is not enabled in all regions

As the security remediations and the configuration remediations are dependent on the Customer's environment and the Customer's assistance, the security remediations and the configuration remediations are provided on an "AS IS" basis.

Cloud CIS Benchmarks

Included in: MDR Solution | MDR Professional | MDR Enterprise

Alert Logic provides real-time reporting based on industry-standard CIS (Center for Internet Security) Benchmarks for Amazon Web Services and Microsoft Azure. These reports are based on logs ingested and vulnerability scans, which provide details on configurations and activity that diverges from the CIS standards.

PLATFORM	PRE-REQUISITES
AWS	Create a CloudTrail and SNS topic Setup AWS IAM policy Setup AWS Cross-account role
Azure	Create an app registration in Azure Create a custom RBAC role Grant permissions to access Microsoft Graph Grant permissions to access Azure Key Vault

Endpoint Detection

Included in: **MDR Solution** **MDR Professional** **MDR Enterprise**

If deployed by Customer, Alert Logic monitors Customer's Windows and Mac endpoints using a dedicated agent.

PLATFORM TYPE	DETAILS	NOTES
Desktop	Windows 7, 8.1 and 10 macOS 10.12 and higher	Virtual Desktops Supported Proxy Aware (Windows only)
Server	Windows Server 2008 R2, 2012, 2016	Virtual Servers Supported

Continuous Learning Engine

Recommended learning time: Two weeks (in detect only mode)

Minimum learning time: 8 Hours

Alert Logic recommends that endpoints are deployed in detect mode at first, to allow the system time to learn the environment. After the learning period, turn on protect mode or continue in detect mode.

PCI Scanning

Included in: **MDR Solution** **MDR Professional** **MDR Enterprise**

Alert Logic provides scanning that covers:

> *6.1 Identify newly discovered security vulnerabilities*
>
> *11.2 Perform network vulnerability scans by an ASV at least quarterly or after any significant network change (Includes 11.2.1, 11.2.2 and 11.2.3)*

The scans provide vulnerability details with detailed descriptions, impacted hosts, risk level, and remediation tips for each vulnerability.

In the user interface, the Customer can find an attestation of scan compliance which includes an overall summary of network posture, compliance status, assertion that the scan complies with PCI requirements, an executive summary overview of scan results and a statement of compliance or non-compliance.

WHO DOES WHAT	
Alert Logic provides	Audit ready reporting and with local business hours accredited PCI Approved Scan Vendor (ASV) support
Customers must	Configure assets for scanning and decide on scanning schedules, review reports, and mitigate or attest to issues
Partners can	Provide extended services for mitigation of discovered vulnerabilities, review customer systems and processes for a deeper PCI assessment

File Integrity Monitoring

Included in: **MDR Professional** **MDR Enterprise**

Alert Logic File Integrity Monitoring is designed to help detect unauthorized change events to operating system, content, and application files for Windows and Linux servers. These include system directories, registry keys, and values on the operating system order to meet the following compliance mandate:

- *PCI-DSS 10.5.5 Change detection mechanism for log files*
- *PCI-DSS 11.5 Change detection mechanism for critical system files, configuration files, or content files*

In the user interface, Customers can schedule recurring reports to receive to receive the details of file change events across multiple date ranges. Change events include time stamp, affected host name, and file attributes.

WHO DOES WHAT	
Alert Logic provides	Scheduled and on-demand audit reporting
Customers must	Configure assets for monitoring and ensure exclusions do not apply to the aforementioned files and directories Must also maintain file backup and retention policy in the event a tampered file requires recovery to pre-tampered state
Partners can	Provide extended services for configuration of monitored directories and file paths, review reports, present findings, and recover files

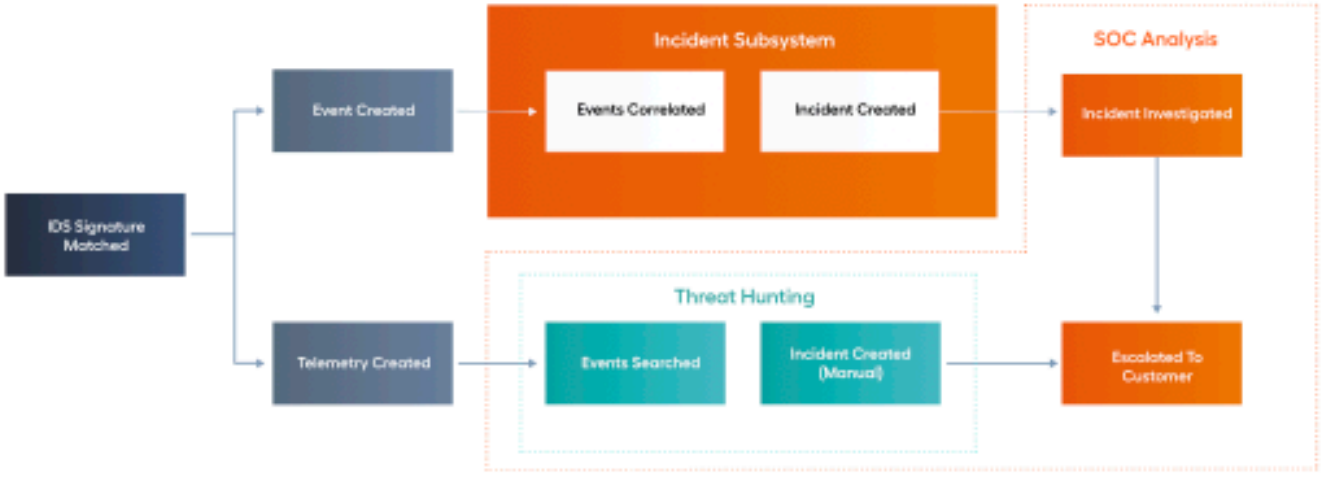
Network Monitoring

Included in: **MDR Professional** **MDR Enterprise**

Threat data is collected during the monitoring of the network traffic between systems; this data is collected using a direct connection to switches (via a port mirror or span port) or via the Alert Logic agent and processed by the Network Appliance.

The appliance uses signatures to monitor for specific attacks as well as for broader data collection and analysis.

Events raised by signatures are fed back to Alert Logic's systems for further analysis based on incident content or threat hunting by security operations and to create telemetry data.



Network Event Incident Process

Incidents are generated based on configured thresholds in the incident subsystem or created manually based on threat hunting searching and analysis.

Log Data Monitoring

Included in: **MDR Professional** **MDR Enterprise**

Alert Logic provides services and systems to ingest, parse, and store logs from Customer's systems to support.

Alert Logic provides numerous log message parsers for many sources. Logs can be ingested from a wide variety of sources. Any flat file or Syslog source can be sent to Alert Logic and searched in the user interface, allowing the Customer to perform historical and near real-time searching. Historical searchces are limited to contracted log retention periods.

Log Analysis

After ingestion, log messages that have parsers are extracted and analyzed using rules maintained by Alert Logic. Log messages which trigger these rules are analyzed by the Security Operations Center.

Log Analysis Alert Logic & Customer Workflow

Log Collection & Search with 12 Month Retention

Included in: MDR Professional MDR Enterprise

Log data can be collected from different sources, including flat file, syslog, Windows, and various cloud providers.

Twelve-month log retention is provided for Customers within the cost of the Solution, and extended retention periods are available at extra cost.

Customers can use the Alert Logic user interface to search logs in an unstructured and structured way using SQL like language, saving those searches to re-run later or send emails at a defined interval based on the results.

WHO DOES WHAT	
Alert Logic provides	Collection, secure storage, log parsers, and incident detection content
Customers must	Ensure new systems are sending their logs to Alert Logic, request new log parsers and content where required

Web Log Analytics

Included in: MDR Professional MDR Enterprise

Alert Logic Web Log Analytics is designed to help detect anomalous behavior, attempted attacks, and unauthorized vulnerability scans.

WHO DOES WHAT	ATTACK EXAMPLES
Signature-based detection of general web attack methods	SQL Injection Cross-site Scripting (XSS) OS Commanding
Known vulnerability and exploit detection and attribution	Exploits targeting known vulnerabilities (CWE) Web shells
Anomaly-based detection	Web shells - unknown Directory traversal Local and remote file inclusion

Cloud Security Service Integration

Included in: MDR Professional MDR Enterprise

AWS

Alert Logic integrates with AWS using log and API methods, listed here:

GuardDuty: Alert Logic integrates with AWS GuardDuty to ingest incidents generated with the service into the Alert Logic user interface, allowing customers to view incidents and affected asset and related remediation details.

Alert Logic provides a cloud formation template to use for the setup of the CloudWatch Events collector and Lambda function to a single AWS region for GuardDuty integration.

Security Hub: Alert Logic is available to add as a provider for AWS Security Hub, enabling this feeds closed and verified Alert Logic incidents into the Security Hub for reporting.

Azure

Logs can be collected from the Azure platform to monitor access and change. These include Azure Activity and Security logs.

Event Hub: Integration with Azure Event Hub allows Alert Logic to collect logs from Azure services and perform machine-learning analytics for behavior and anomaly detection against security logs.

Office 365: Logs from Office 365 can be ingested through the Event Hub connector to store and enable searching in the Alert Logic interface.

API

Alert Logic provides API for the Customers or partners to use for integration purposes.

Cloud Change Monitoring

Included in: MDR Professional MDR Enterprise

By analyzing changes to cloud environments, through the ingestion of logs, configuration changes can generate incidents that are escalated to Customers.

For example:

- Create Security Group
- Attach User Policy
- Change Password
- Create User
- Console Login Failure

PLATFORM	PRE-REQUISITES
AWS	Create a CloudTrail and SNS topic Setup AWS IAM policy Setup AWS Cross-account role
Azure	Create an app registration in Azure Create a custom RBAC role Grant permissions to access Microsoft Graph Grant permissions to access Azure Key Vault

User Behavior Monitoring

Included in: MDR Professional MDR Enterprise

Alert Logic provides user behavior anomaly detection (UBAD) in enterprise environments. Machine-learning determines baselines in AWS, Azure, and Office 365.

Intelligent Response™

Included in: MDR Professional | MDR Enterprise

Alert Logic Intelligent Response™ is designed to help Customers minimize impact of a breach with the right balance of automation and human interaction. The embedded SOAR capabilities provide users a workflow to enable response actions across network, endpoints, and cloud environments. These include:

- Isolate Host – Block incoming and outgoing network activity of an endpoint
- Disable Credentials – Block usernames and passwords from accessing the network
- Shun Attacker – Block an external IP attack by updating a rule at the network edge

In the user interface, Customers are provided a list of its active response actions and a history of the response actions executed with time stamps, trigger, and asset.

Real-time Reporting & Dashboards

Included in: MDR Essentials | MDR Professional | MDR Enterprise

Real-time reporting is available in the Alert Logic user interface.

Customers can schedule reports to be emailed to configured contacts.

TOPIC	REPORT EXAMPLES
Risk	Monthly Security Posture Threat Risk Index Summary & Trends Enterprise Risk
Threats	Incident Analysis Periodic Summaries AWS Incident Analysis Azure Incident Analysis Account Summary Log Review Analysis Web Application Analysis Event Analysis
Vulnerabilities	Vulnerability Analysis Top 10 Vulnerability Lists Current Vulnerability Finder Vulnerable Hosts Explorer Vulnerability Change Trends Vulnerability Distribution Explorer
Remediations	Configuration Remediations Security Remediations

Compliance	CIS AWS Benchmarks CIS Microsoft Azure Benchmarks PCI DSS Audit HIPAA-HITECH Security Audit HITRUST Security Audit
Service	Entitlement Usage Capability Usage Solution Health

Deployment

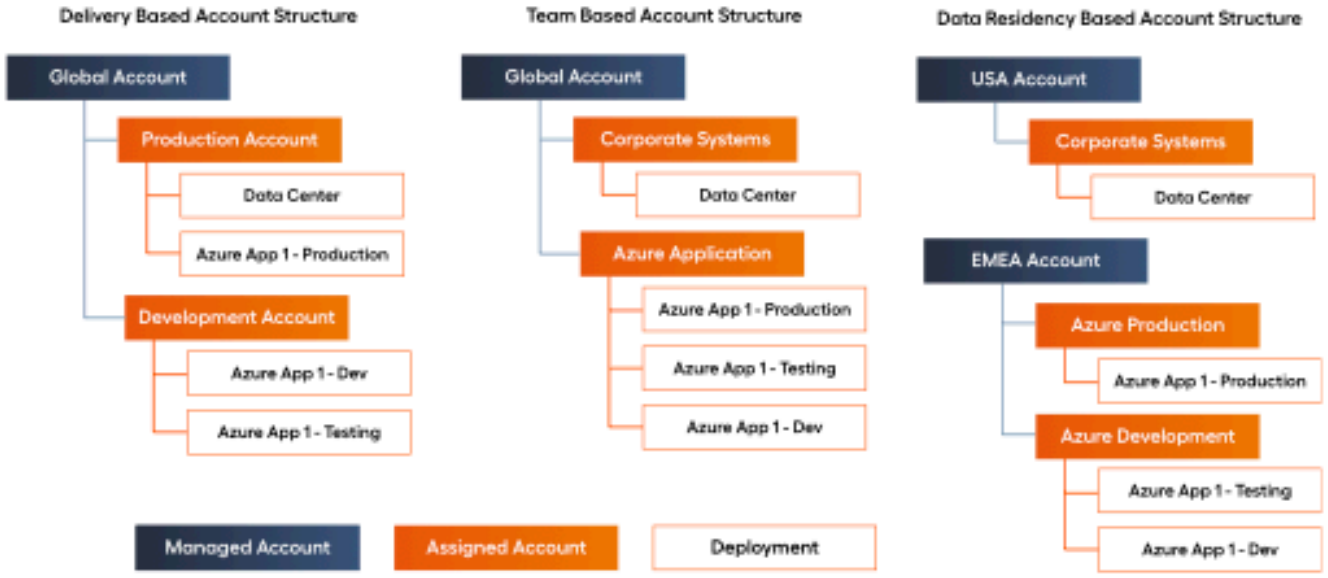
Account and Deployment Hierarchy

Customer can choose to have multiple accounts with Alert Logic in a parent and child hierarchy, referred to as Managed and Assigned accounts, respectively. As part of onboarding, Alert Logic project managers, with Customer's cooperation and provided information, may help define the hierarchy.

Data residency with Alert Logic can be chosen at the Managed Account level.

Within each account, Customer can configure multiple deployments to separate some configuration and enable further filtering based on different architectures or environments—e.g., AWS Account or data center.

Example Account Hierarchies



Scope of Protection

Each deployment can be configured with different levels of protection for configured networks, choosing either Essentials, Professional, or Enterprise to define which Alert Logic protection level is applied.

The table below indicates the security technologies deployed into the environment at each protection level:.

PROTECTION LEVEL	TECHNOLOGY FEATURES	DEPENDENCIES
Essentials	Asset Discovery Internal Vulnerability Scanning External Vulnerability Scanning Cloud Configuration Checks Extended Endpoint Protection	Network or Scan Appliance* Endpoint Agent
Professional Enterprise	Asset Discovery Internal Vulnerability Scanning External Vulnerability Scanning Cloud Configuration Checks Endpoint Detection Network Packet Monitoring Log Data Monitoring	Network Appliance Scan Appliance* Endpoint Agent Log Appliance* Agent

**Depending on the environment these components may not be required, refer to individual target environment sections later in this document.*

Appliances

APPLIANCE TYPE	PURPOSE	DATA COLLECTION METHODS
Network	Monitor network packets, perform internal scanning and asset discovery where required	Port Mirror Agent PCAP WMI SSH
Log	Collect, compress and forward logs to Alert Logic for storage and analysis	Syslog File Share Windows Event
Cloud Scanning	Deployed to scan cloud environments	TCP WMI SSH

**An additional charge is incurred for physical appliances.*

Agents

AGENT TYPE	PURPOSE	DATA COLLECTION	RESOURCE PROFILE
Server	Deployed to servers to collect network packet data and log data	Packet Capture Syslog Event Log	< 10% CPU Single Core Mirror Server Internal Network (depending on configured exclusions) Log Data compressed before sending externally*
Endpoint	Deployed to desktop computers to monitor behavior for anomalies	Kernel & Process monitoring	< 5% CPU Single Core Minimal network usage

Remote Collector	Deployed on servers to collect and forward single Syslog feeds	Syslog	< 5% CPU Single Core Log Data compressed before sending externally*

** Logs are sent at a compression rate of 15:1-18:1. The agent uses a compression algorithm based on the gzip model to reduce the sent packets.*

The Alert Logic server agent is installed onto Windows and Linux servers to collect network packets, forwarding them to the nearest appliance for analysis, and collect logs. Those logs can be sent to an appliance for on-premises deployments or directly to the Alert Logic cloud for all deployment types.

The Alert Logic endpoint agent is installed onto Windows and Apple desktop and laptop computers.

Cross-Network Protection

Customers must first configure agents and appliances within environment to connect with other networks before Customers can set up cross-network protection.

Network Packet Inspection

Network data can be collected using a port mirror (or Switched Port Analyzer, "SPAN") configuration or through the deployment of the Alert Logic agent.

A port mirror or SPAN is a configuration option for network switches where the switch will copy any traffic going through one or more ports on the switch to a destination port for traffic inspection.

The switch port configured to forward traffic should be connected to the Alert Logic appliance network port identified by the Alert Logic deployment team. After which the networks to be monitored need to be configured in the Alert Logic Configuration UI.

Encrypted traffic must be decrypted before being analysed; the certificate is loaded onto the Network Appliance through the Alert Logic User Interface. Network Intrusion detection systems (NIDS) do not support Diffie-Hellman or any other similar key protocol, now existing or hereinafter invented.

Overall for the deployment, various exclusions can be applied, networks, hosts, and specific ports can be excluded from monitoring and internal or external scanning.

Log Data Collection

Alert Logic is continually adding new supported sources.

SOURCE TYPE	NOTABLE SOURCES	COLLECTION METHODS
Flat File	Apache Logs	Appliance Agent S3
Syslog	Unix/Linux Authentication Logs	Appliance Agent

Windows Event	Security Log	Appliance Agent
AWS Services	Cloud Trail S3 Storage	S3
Azure Services	Azure Security Logs Office 365	Azure Event Hub

Log Sources

SOURCE PLATFORM	NOTABLE SOURCES*
AWS	AWS CloudTrail, EC2, IAM
Azure	Azure AD, Office 365, Azure Event Hub
Operating System	Windows, Linux
Server	Active Directory, Apache, Microsoft IIS
Anti-Virus	McAfee, Sophos, Symantec, Kaspersky
Database	MySQL
Devices	Fortigate, FireEye MPS, Cisco ASA
Other	Logs from other resources, i.e., OSSEC

**This is not a complete list, refer to Alert Logic Support to verify parsers for Customer's systems and devices.*

Discovery & Vulnerability Scans

Customers can configure how often it wants scans run to discover new assets based on frequency or specific schedule.

Defaults

SCAN TYPE	NAME	FREQUENCY
Discovery	Scan as often as necessary	Light scan twice per day
Internal	Scan as often as necessary	Once per day
External	Scan as often as necessary	Once per day

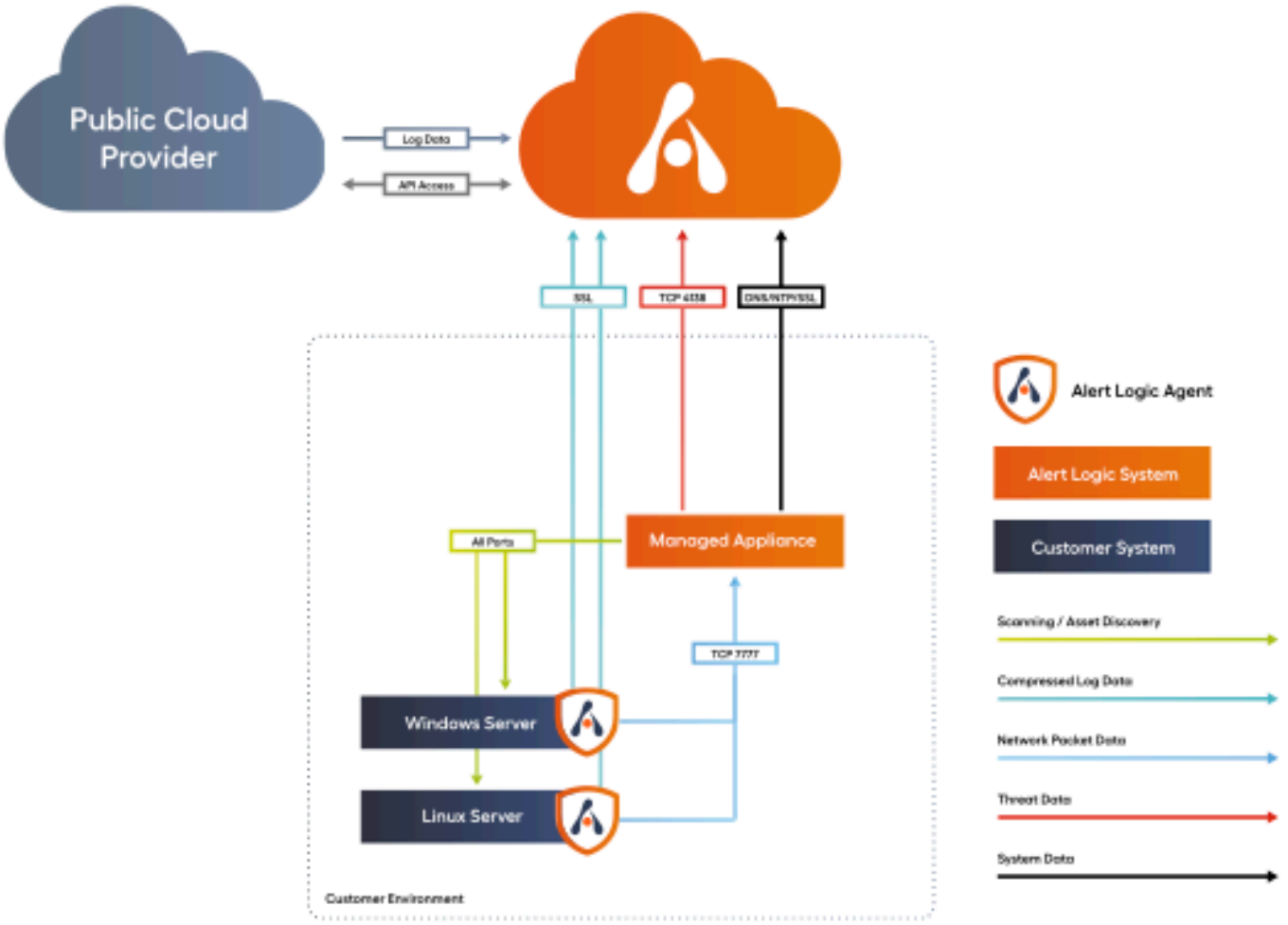
Deployment Types

Alert Logic supports physical, cloud, and hybrid deployment options depending on Customer's environment.

Agent Deployments

Used for any environment type, Alert Logic's monitoring can be deployed using a purely agent-based approach.

Depending on which features are licensed within an environment, not all ports indicated in the diagram below will be used.



Logical deployment architecture for agent-based deployments

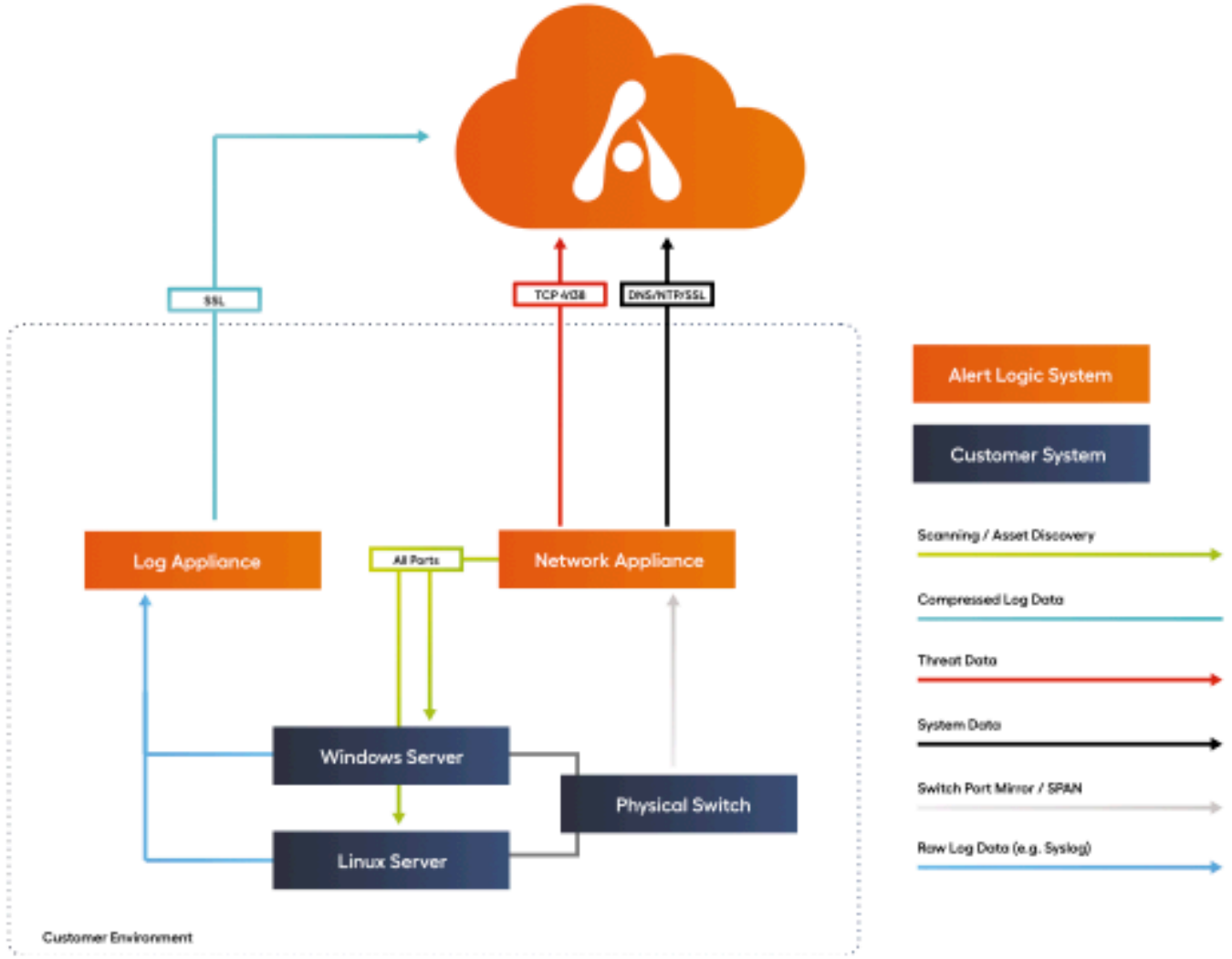
Physical Deployments

Used for on-premises deployments an appliance can be deployed to collect and forward log data and another to take network data from physical switches.

Alert Logic can be deployed into physical environments using server appliances supplied by Alert Logic to be installed by the Customer into its data center.

Alert Logic appliances should be deployed for each network that requires protection.

A network switch can be configured to forward all network packets to the appliance via a port mirror, and a log management appliance deployed to collect logs from the servers, firewalls and other devices via standard ports. Customer is responsible for installing and deploying physical appliances at Customer's site.



Logical deployment architecture for physical infrastructure deployments

This diagram shows the most important ports that need to be configured. Refer to http://docs.alertlogic.com for detailed network requirements for your chosen Alert Logic region.

Port Mirrors and Agents Configuration

Deployment can be done by using the Alert Logic agent or a port mirror configuration.

VMware

Alert Logic provides VMWare appliances for deployment into Customer's virtual estates. Customer is responsible for resource usage in virtual estates.

Cloud AWS

In Amazon Web Services, deployment can be largely automated when the required permissions are configured. Appliances are supplied as an 'Amazon Machine Image' shared with the Customer's accounts during deployment, accompanied with example cloud formation scripts.

Deployments can be done in fully automatic mode or optionally in manual mode depending on Customer requirements. In manual mode setup must be done in the AWS account by the Customer or partner. Fully automated mode provides for improved agent lifecycle management, optimized appliance deployments and auto-detection of new assets and changed configurations.

DEPLOYMENT MODE	CUSTOMER SETUP	METHOD
Automatic	Cross-Account Role AWS IAM Policy Role ARN	Cloudformation
Manual	AWS IAM Policy Role ARN CloudTrail log source S3 bucket SNS topic SQS queue	Customer Choice

The full permission policy document does **not** allow Alert Logic to:

- Retrieve secret keys or credentials from IAM
- Retrieve data from data stores other than S3
- Perform these actions from any other AWS account
- Grant access to the protected account to any other AWS account or user
- Modify IAM credentials or policies

Where required a network appliance will be deployed in a public subnet along with auto-scaling configured scanning appliances. The scanning appliances will auto-scale as needed and can be made to scale to zero appliances when not needed.

Appliances are recommended to be deployed in each VPC that needs to be protected.

Marketplace

AWS customers can sign-up and deploy Alert Logic services via the AWS Marketplace (search for "Alert Logic" in the marketplace to find the listings). Customers can choose between a European and USA deployment, which determines where their data is held.

Azure

For Azure deployments, Customer must configure Microsoft Azure resources to allow Alert Logic to monitor their assets. All procedures require administrative permission in the Azure portal.

Customer must create an app registration, and then use Azure role-based access control (RBAC) to create and assign a role to that app registration. This enables fine-grained access management for Azure accounts.

To further Customer's security configuration measures, Customer must grant certain permissions to access Microsoft Graph and Azure Key Vault. This practice is required for compliance with Center for Internet Security (CIS) benchmarks for Microsoft Azure and allows Alert Logic to perform CIS benchmark checks on Customer deployments.

Marketplace

For the MDR Professional deployment a Bring Your Own License (BYOL) appliance can be obtained in the Azure Marketplace by searching for Alert Logic, Customers will see an Alert Logic Professional BYOL which they can deploy.

Access

Customer can access the Alert Logic Console here: http://console.overview.alertlogic.com.

During onboarding, users will be set up for the primary contacts, Cusotmer can add new users with various levels of permissions.

	ROLE TYPE					
Permission Type	**Administrator**	**Owner**	**Power User**	**Support / Care**	**Read Only**	**Notification Only**
Full Access & User Management						
Modify Managed Accounts						
Modify Assigned Accounts						
Read Managed Accounts						
Read Assigned Accounts						

Alert Logic recommends the use of a multi-factor authentication when logging into accounts.

API Access

Access to the API requires an account configured as well as a key requested via the user interface. API Authentication is via username/password and Google Authenticator.

Vulnerability & Exposure Management

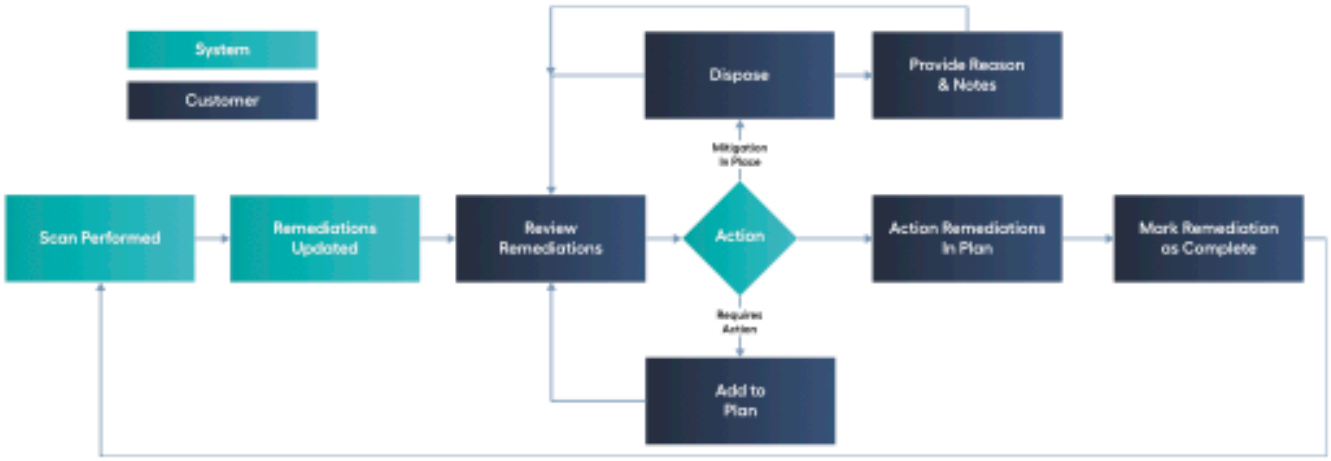
Prioritization & Filtering

Prioritization by deployment or network can be made based on the Threat Risk Index.

Prioritization by severity can be performed on the Remediation summary.

Filtering remediations in the list can be made based on several facets, including Category, cloud region, network/vpc/vnet, Application, Tags, Alert Logic deployment, AMI and more.

Filtering remediations can be done using the topology map.



WHO DOES WHAT	
Alert Logic provides	Content for known vulnerabilities and configuration checks, up-to-date reporting, and support for scanning
Customers must	Allow network access by the Alert Logic appliance and provide credentials for servers. Manage vulnerabilities; e.g., Patch servers and update configurations or mark them as mitigated in the user interface
Partners can	Provide managed services to mitigate/patch vulnerabilities

Notifications

Notifications can be triggered based on incidents, observations, saved searches, reports and other platform output the Customer can configure.

Incidents are high fidelity findings that indicate detection of attack or compromise activity. Observations are anomalies and other indicators of suspicious activity that are not immediate calls to action but may generate security insights upon review.

Connectors are available to push notifications directly to Customer's chosen collaboration or ticketing system or configure custom webhooks based on JSON.

Native support for popular 3rd party ticketing & messaging platforms including Jira, Jira Service Desk (JSD), ServiceNow, PagerDuty, Slack and Microsoft Teams.

TYPE	TRIGGERS	FILTERS
Telephone	High or critical incidents	Customers can request tuning of incidents to affect severity
Email	All Incidents	Incident Severity
	Observations	N/A
	Reports	N/A
	Saved Log Searches	N/A
Connector (Webhook)	All Incidents	Incident Severity
	Observations	N/A
	Reports	N/A

WHO DOES WHAT	
Alert Logic provides	A platform to provide notifications of important activities based on Customer preferences
Customers must	Configure notification preferences or contact Alert Logic to ensure that notification preferences are setup appropriately based on Customer's requirements

Incident Management

Customers are responsible for having an incident response plan that is set up to receive and evaluate the output of Alert Logic's service.

In the event recommendations are made by Alert Logic that are not covered by existing processes, an internal escalation process should exist that aligns with the Customer's organizational structure.

Finally, incidents should be closed by the Customers, including details of changes.

Example Process

Software & Service Updates

Software updates to Alert Logic will be provided on an as-needed basis and can include new features, improvements to existing features, and technical fixes.

For changes to the Alert Logic Console, Alert Logic will automatically apply the software updates on the following schedules based on location.

CHANGE TYPE	DESCRIPTION	US CHANGE WINDOW	EU CHANGE WINDOW
Standard	Not service impacting	20:00 – 03:00 CT Monday - Friday	21:00 – 04:00 UTC Monday - Friday
Emergency	Required to mitigate service disruption	As needed	
Major*	Service Impacting	20:00 – 03:00 CT Saturday - Sunday	21:00 – 04:00 UTC Saturday – Sunday
Content – Signatures	Non-emergency IDS signature updates	21:00 & 04:00 GMT Monday, Wednesday & Friday	
Content - Vulnerability	Non-emergency vulnerability detection updates	05:00 GMT Daily	
Content - Log Parsers	Non-emergency log parser and content updates	08:00 GMT Tuesdays & Thursdays	

**Alert Logic will communicate to Customers regarding major changes with at least six business days advance notice.*

Alert Logic will communicate change/maintenance windows via the URLs below:

- US: https://console.clouddefender.alertlogic.com/core/maintenance/window
- UK: https://console.alertlogic.co.uk/core/maintenance/window

Current service status can be viewed via the URL below:

- https://status.alertlogic.com/#

For questions regarding the above US schedules, contact Alert Logic Support at

- US: +1 877-484-8383 (Option 2) or +1 713-484-8383 (Option 2).
- UK: +44 (0) 203 011 5533 (Option 2).

Support

Alert Logic provides resources for Customers to get 24/7 product support, access documentation, receive training and access example automation scripts. These resources are provded on an as-need basis.

	URL	USAGE
Support	http://support.alertlogic.com	Manage, view, and raise non-urgent product support requests at this URL, contact numbers are available here for urgent requests
Docs	http://docs.alertlogic.com	Reference material for deploying and configuring Alert Logic solutions
Learn	http://learn.alertlogic.com	Online training for customers
Source	https://github.com/alertlogic	Example source code and scripts for deployment, data collection, API queries and more

Customer Responsibilities and Interaction with Alert Logic

Customer enablement will require Customer participation to ensure that Alert Logic receives the right level of Customer feedback and activity to ensure a successful deployment.

Service continuity will require Customer participation to ensure that Alert Logic receives relevant data for analysis and has the appropriate escalation contacts.

RESPONSIBILITY	DESCRIPTION
Agent Installation	Customer is responsible for installing agents, configuring appropriate firewall access to enable agent communication, and notifying Alert Logic when installation of agents is complete. Customer is responsible for configuring appropriate access to enable appliance communication.
Appliance Installation	On premises, Customer is responsible for racking and installing the physical appliance(s) (if aplicable), and/or loading and installing the virtual appliance image. Customer is respon- sible for providing network access to the appliance(s) for Alert Logic personnel, configuring appropriate firewall access to enable appliance communication, and notifying Alert Logic when installation of the appliance(s) is complete. In the cloud, the Customer is responsible for configuring appropriate Security Group access to enable appliance communication.
Technical Deployment	Customer is responsible for the provision of appropriate technical resources and information during the Customer enablement project. Technical resources are required to attend the project Kick Off and orientation sessions and to carry out project activity required to establish the service during the Customer enablement project, including following the training curriculum. Technical resources are also required to provide information and context about the Customer environment to enrich the service.

Operational Integration	Customer is responsible for the provision of appropriate operational resources and information during the customer enablement project. Operational resources are required to carry out integration activity to ensure the Customer transition is ready to consume the Alert Logic services. During the Customer enablement project these resources will be required to attend service orientation and complete the training curriculum.
Access to assets	Customer is responsible for identifying target AWS, Azure and/or Data Center environments and assets to include within the service and ensuring that technologies are installed appropriately for the desired scope of service and properly configured to access all monitored networks, including any necessary changes to on-premise equipment such as firewalls and switches.
Scanning	Customer is responsible for confirming the actual IP addresses, domains, or address ranges are specifically allocated to Customers prior to initiating any scans. Alert Logic depends upon a reliable connection between the Alert Logic hosted scan technologies and Customer target networks / systems. If a reliable connection is unavailable for any reason, Alert Logic will not be responsible for the service level commitments for that period. Customer is responsible to ensure that there is no "Scan Interference" as defined in PCI SSC's "ASV Program Guide" during the PCI Scans.
Log Collection	Customer must ensure that collection for target source log data and networks are properly installed in Professional and validate log and event data is being sent back to Alert Logic for storage and analysis. Customer is responsible for configuration of the desired level of log collection in audit log settings. Customer who has configured and implemented log collection black-out periods (for example, cache log data on local machine during business hours for single upload after business hours) should recognize that this collection configuration will delay log ingestion, aggregation, and normalization by the threat management capabilities in the Professional level of coverage.
Connectivity to Alert Logic	Capabilities depend upon a reliable connection between the Alert Logic assets, the protected network, and the Security Operations Center. If the source network is unavailable for any reason, then event collection and correlation will be impeded. Alert Logic will not be responsible for the service level commitments for that period. In the event the Extended Endpoint Protection agent loses network connectivity, the agent will continue to function but will be unable to receive updates and send event data to the Alert Logic console. Once connectivity is restored, all queued events will be sent to the Alert Logic portal.
Monitored System Availability	Customer is responsible for ensuring that Customer-owned networks, systems, and applications within the scope of the Cloud Insight service are maintained and functioning properly. Customer is also responsible for the deployment, management and event triage of the Alert Logic Extended Endpoint Protection. Alert Logic depends upon reliable log, event, and scan data from Customer networks. Systems that are off-line, in error, or otherwise in a state that degrades the collection of log and event data inhibit service delivery. Customer is responsible for ensuring that Customer-owned networks, systems, and applications within the scope of the Professional service are maintained and functioning properly.
Managed WAF	The service depends upon reliable security-relevant data from monitored networks, systems, websites, and applications. Systems that are off- line, in error, or otherwise in a state that degrades the generation of security event information inhibit service delivery. Customer is responsible for ensuring that Customer-owned websites, networks, systems, and applications within the scope of the Enterprise Managed WAF service are maintained and functioning properly. This includes monitoring for backend application availability, even if the application is inline/protected by Enterprise Managed WAF.
Service Optimization	Customer is responsible for participating in ongoing service optimization activities such as performing agreed upon network or application changes and changes to Customer information. If Customer subscribed to the MDR Enterprise service add-on, it is responsible for attending meetings scheduled at a mutually convenient time and at an agreed frequency, so that the designated analyst can share findings and recommendations in a timely manner.
Operational and Environmental Changes	Customer is responsible for communicating all relevant changes to Customer environments that may impact vulnerability scanning, log and event collection/correlation. Customers of the managed WAF add-on are responsible for communicating all relevant changes to Customer environments as they may impact the scope of monitoring including but not limited to changes in utilized IP space by the web server, major changes to web applications, and cloud environments, among others.
Alerting and Notifications	Customer is responsible for configuring escalation E-mail and phone alerting and notification with accurate and updated information – through self-service in the Alert Logic Console or by contacting the SOC. Customers should include both security and technical contacts when they configure notifications so that the appropriate parties may be quickly reached and notified of a given condition.