ALERT LOGIC®

HOW IT WORKS:

ALERT LOGIC® CLOUD DEFENDER™

MANAGED SERVICE EXPERTISE. SAAS SIMPLICITY.

Today's demand for cybersecurity, coupled with an evolving threat landscape, requires a security strategy that protects your data in an integrated, proactive, and knowledge-centric way. The legacy approach of buying multiple siloed products, attempting to integrate and manage them and staffing for 24 x 7 coverage does not offer the protection and visibility required and only puts additional stress on limited budgets and resources.

In many cases, organizations are forced to select solutions with fewer capabilities, hire junior level security experts or indefinitely delay purchase decisions for critical protection and compliance products. As cybercrime, hacktivism and insider threats continue to rise; organizations can no longer afford to forego fully protecting their environments. Fortunately, there is a better option for securing diverse environments: Alert Logic® Cloud Defender™. Unlike legacy products, Cloud Defender does not require dedicated hardware or security expertise from an organization. Delivered from the cloud, Alert Logic Cloud Defender is a fully managed offering that protects any network, application, or computing infrastructure, no matter where it resides.

SECURITY-AS-A-SERVICE: FULLY MANAGED SECURITY SOFTWARE DELIVERED FROM THE CLOUD

The adoption of Software-as-a-Service (SaaS) solutions has transformed how many organizations deliver business critical applications to their employees, partners and customers. SaaS allows companies to avoid costly implementation and maintenance activities while still meeting the demands of the business. Alert Logic embraced this delivery model from the beginning, developing cloud-based solutions from the start, and introduced Security-as-a-Service. Security-as-a-Service combines SaaS with managed services, extending the proven benefits of SaaS.

ALERT LOGIC SECURITY-AS-A-SERVICE:

Protects on-premises, cloud, and hybrid datacenters with a single solution

- Assists organizations with meeting compliance mandates without disrupting their normal business activities
- Identifies vulnerabilities across an organization's IT infrastructure in real-time
- Defends web applications from attacks to ensure availability and prevent data loss
- Analyzes logs across the application stack to identify malicious or anomalistic behavior
- Provides around-the-clock, 24x7 monitoring by a team of security and compliance experts

HOW ALERT LOGIC CLOUD DEFENDER TURNS DATA INTO ACTIONABLE INTELLIGENCE

Alert Logic Cloud Defender is a fully integrated security and compliance solution providing continuous protection in any IT environment. Following a scalable, highly automated process, Alert Logic Cloud Defender turns the vast amount of data generated by applications, network devices, servers, network traffic, websites, and more into intelligence that helps an organization protect their sensitive data.

STEP 1: DATA CAPTURE

Data from across an organization's environment is collected, aggregated, and stored in Alert Logic® ActiveAnalytics™ platform. Log data from any number of sources is collected with Alert Logic® Log Manager™ and stored for as long as you need it. Alert Logic® Threat Manager™ monitors customer network traffic to identify and collect threat information and Alert Logic Web Security Manager monitors web application traffic, collecting information about threats targeting web applications and websites. All of Alert Logic's products are designed with installation and configuration options to enable deployment in a variety of IT environments such as public and private clouds, hosting provider facilities, and on-premises networks.

- Products are deployed through any combination of physical/virtual appliances and agents
- Minimal performance impact to customer infrastructure
- Designed for any cloud and certified for deployment on all major Cloud platforms

STEP 2: BIG DATA GRID

Once data is collected, the ActiveAnalytics Platform's big data processing grid takes over. Powered by a service provider-grade infrastructure, customer data is processed and normalized to enable security rule correlation, ad hoc searching, and reporting by both Alert Logic Security Analysts and customer personnel. Built for unlimited scale, the ActiveAnalytics Platform processing grid gives every customer the ability to gain deep insight into their security and compliance posture. from the Alert Logic Security Operations Center (SOC) allowing internal IT staff to focus on other business critical projects.

- Natively multi-tenant, built for cloud scale
- 5 petabytes of data under management
- Over 400 million security events and 50,000 security incidents identified monthly

STEP 3: CORRELATION & ANALYTICS

The ActiveAnalytics platform includes a robust library of correlation rules to comprehend and identify behavior via log data analysis for security incident identification. This library is developed and maintained by the Alert Logic® ActiveIntelligence™ team, with frequent updates as the global security environment evolves. With automated access to these scenario-based correlation rules, organizations can avoid investing in expensive, complex standalone SIEM solutions and a security research team.

- Continuously updated intelligence feed for latest threats and vulnerabilities
- Security incident correlation, stream processing, data mining, and anomaly detection
- Incident identification from disparate security events

STEP 4: 24X7 SECURITY OPERATIONS CENTER ANALYST INVESTIGATION

Identified incidents are then enriched with correlation from additional security intelligence such as IP Reputation, GEO Location, and Watch Lists. This additional information assists the Alert Logic® ActiveWatch™ security analysts with determining incident validity and setting criticality to direct further action. Incident enrichment also includes an analyst's advice on containment and remediation.

- Proactive identification and response to suspicious activity
- Incident escalation with recommendations for resolution
- Simple view into security and compliance posture

STEP 5: ESCALATION & RESPONSE

Alert Logic ActiveAnalytics platform then identifies valid security events and suppresses false positives. When ActiveAnalytics determines a series of events to be a valid security threat, an incident is created. Depending on incident severity, escalation with remediation recommendations will be delivered via email or through an Alert Logic security analyst. The Alert Logic approach dramatically reduces false positives and keeps analysts and customers focused on real, actionable incidents.

- Low Priority: Sometimes referred to as "Internet noise," these events are automatically logged into the data store, visible within the UI, and available via reports showing the status and trending.
- Medium Priority: incidents consist of activities requiring closer observation and continued monitoring, but don't rise to the level of a realtime response. These types of incidents are typically auto-escalated by default to all pertinent security contacts via email notification.
- High Priority: Incidents require Alert Logic security analysts to proactively notify customers using all provided means of contact information available.
- Critical Priority: Incident escalations follow the same guidelines as High Priority Incidents, except that they will typically incorporate active defense blocking (if appropriate product functionality is present to enable) by the security analysts. For the duration of the incident, the customer will receive ongoing direct support from the Alert Logic Security Operations Center (SOC)

STEP 6: SECURITY ACTIONS & POLICIES

Alert Logic Cloud Defender enables Alert Logic security analysts to work with customers to take corrective action in the customer's environment. From firewall rule implementation to blocking the spread of malware and exfiltration of sensitive data, to suggesting policy changes and configurations, Alert Logic security analysts act as a natural extension of an organizations' IT security team.

THE ALERT LOGIC DIFFERENCE

Other security and compliance solutions may claim to provide a Security-as-a-Service product, but are they are only providing complex on-premises solutions from the cloud. Alert Logic Cloud Defender brings advanced technology and dedicated people together to provide true Security-as-a-Service all day, every day. With 24x7 data collection, processing, correlation, analytics, escalation, and security monitoring, organizations can be confident that their environments are secure.

ABOUT ALERT LOGIC

Alert Logic, the leader in security and compliance solutions for the cloud, provides Security-as-a-Service for on-premises, cloud, and hybrid infrastructures, delivering deep security insight and continuous protection for customers at a lower cost than traditional security solutions. Fully managed by a team of experts, the Alert Logic Security-as-a-Service solution provides network, system and web application protection immediately, wherever your IT infrastructure resides. Alert Logic partners with the leading cloud platforms and hosting providers to protect over 3,000 organizations worldwide. Built for cloud scale, our patented platform stores petabytes of data, analyses over 400 million events and identifies over 50,000 security incidents each month, which are managed by our 24×7 Security Operations Center. Alert Logic, founded in 2002, is headquartered in Houston, Texas, with offices in Seattle, Dallas, Cardiff, Belfast and London. For more information, please visit www.alertlogic.com.

ALERT LOGIC®

0615US