

SOLUTION OVERVIEW:

ALERT LOGIC[®] CLOUD DEFENDER[®]

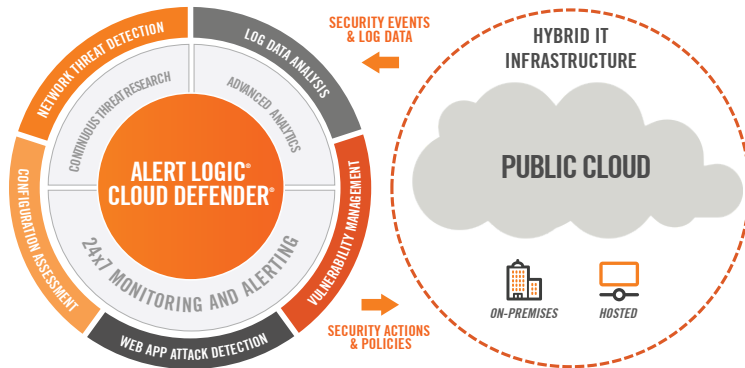
INTEGRATED SECURITY-AS-A-SERVICE FOR THE CLOUD

Few things are as important to your business as maintaining the security of your sensitive data. Protecting your brand, evolving your products and services, growing your customer base, and maintaining your competitive advantage depend on the protection of this data. In the past, when individual hackers used “smash-n-grab” methods to steal your data, protection strategies were straightforward. However, the threat landscape has become more complex. Hackers are more organized, using multi-vector targeted attacks to penetrate your environments, conceal their presence, and steal as much of your data as possible.

Building a comprehensive security platform to combat these attackers by integrating multiple point product, and recruiting and training your staff to manage them around the clock is complex and expensive. With your sensitive data in both on-premises datacenters and in the cloud, you may need different solutions for each environment, increasing both the initial investment and on-going costs required to maintain them effectively.

It is clear that meeting today’s security challenges using yesterday’s products is not possible. You need a security strategy that allows you to stay ahead of these attackers no matter where your sensitive data resides. The right strategy is one that moves you from a siloed, reactive, technology centric approach to an integrated, proactive, knowledge-centric approach to securing your data.

ALERT LOGIC® CLOUD DEFENDER® DELIVERS THIS NEW STRATEGY



Alert Logic® Cloud Defender® is a fully managed cloud-based suite of security and compliance solutions for cloud, on-premises, and hybrid infrastructures to make it easy for any organization to purchase, deploy, and reach their security goals, all without being a security expert. With no large capital investment, lengthy implementation, or heavy training requirement, and a simple subscription model, Alert Logic Cloud Defender is the easiest way for an organization to keep their proprietary data secure.

Powered by our threat data analytics platform and security intelligence team, Alert Logic Cloud Defender allows organizations to:

IDENTIFY AND MITIGATE NETWORK THREATS

With real-time network monitoring and proactive incident identification, our security experts are able to alert organizations quickly when an attack is detected. We provide 24x7 monitoring of network traffic looking for threats that could compromise data or impact system availability.

DETECT SECURITY ISSUES AND ANALYZE EVENTS FROM LOG DATA

Certified security experts analyze log data from various sources to identify suspicious activity that may indicate a security risk. With Alert Logic, organizations can reduce the costs associated with audit preparation, in addition to gaining deeper visibility into the activity occurring throughout their environment by automating the collection, aggregation, and normalization of log data.

PROTECT AGAINST WEB APPLICATION THREATS

The combination of our signature-based detection and an embedded learning engine provide protection by detecting both known attacks and deviations from your expected application behavior. Web Application Firewall security experts in our Security Operations Center (SOC) manage and monitor your environment 24x7, 365 days a year to ensure your web applications and business are protected.

IDENTIFY VULNERABILITIES AND ASSESS YOUR SECURITY POSTURE

Central to any security strategy is understanding the current state of your security posture, and Alert Logic makes that easy. By providing complete visibility of your environment and the impact vulnerabilities have on your environment, you can gain insight into your risk profile and obtain actionable intelligence to improve your security and compliance posture.

CORRELATE DISPARATE SECURITY EVENTS TO IDENTIFY HIGH PRIORITY SECURITY ISSUES

Alert Logic aggregates security events and incidents from various data sources, creates correlation rules, manages threat intelligence content, and cross-correlates security data to identify high priority issues and incidents that may affect your environment.

COMPLIANCE WITHOUT COMPLEXITY

Organizations can reduce the burden associated with meeting their key compliance requirements across their on-premises, cloud, and hybrid environments. Cloud Defender maps to specific mandates, such as PCI DSS, Sarbanes-Oxley and HIPAA, enabling customers to be confident that those requirements are fulfilled.

THE ALERT LOGIC DIFFERENCE

Alert Logic Cloud Defender solves many different security and compliance challenges for organizations, including:

CENTRALIZED SECURITY MANAGEMENT



Whether your datacenter infrastructure is on-premises, cloud or both, Cloud Defender protects them all and provides a single user experience, eliminating the need for a security solution for each type of environment. Additionally, Cloud Defender offers integrated security tools to comprehensively and consistently protect your data at several layers of the application stack - network, system, and web application.

SCALABLE THREAT DETECTION AND RESPONSE MANAGEMENT



Cloud Defender delivers a managed security solution, providing the benefits of traditional security solutions without the cost and complexity of internal deployment and management. It combines advanced technology and security expertise to deliver the features, security content, threat investigation, and a call from our security experts to walk you through the remediation process when a high priority incident is detected to protect your environment. Unlike traditional solutions requiring hardware purchase, implementation of complex software, correlation rule configuration and internally generated security content, Cloud Defender includes everything needed for an effective security solution in an easy-to-use solution that scales as your company grows.

NATIVE PUBLIC CLOUD SECURITY



Cloud Defender is delivered from the cloud, providing you a solution that is easy to get up and running, and also designed to protect your environments in your on-premises, cloud and hosted infrastructure.

EXPERT ONBOARDING AND OPERATIONALIZATION

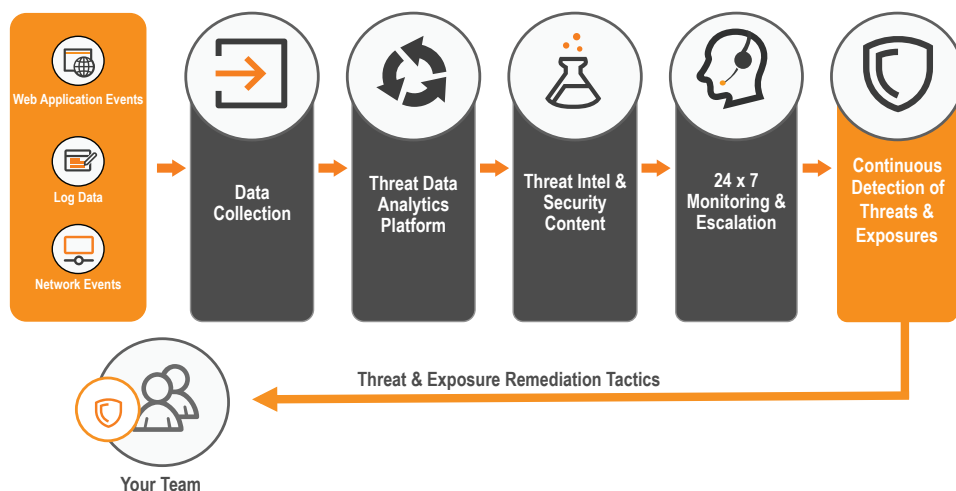


Security investments often go unused or are deployed with partial or default settings – placing businesses at risk while never fully realizing their investments. Our security professionals ensure proper deployment, configuration, tuning and optimization of Cloud Defender.

Every customer is assigned an Alert Logic onboarding project manager (OPM) to manage the entire process and onboarding team of 20+ specialist including: Project Managers, Onboarding Engineers, NOC Technicians, Network & System Administrators, Security Analysts and Product Trainers.

INTEGRATED SECURITY DELIVER RESULTS

When protecting your sensitive data is your number one priority you need a integrated solution designed specifically for that purpose. With Alert Logic Cloud Defender organizations can protect their web applications, networks and computing infrastructure with a fully integrated solution from a single vendor they can trust. Offering an easy to understand licensing model, Cloud Defender not only takes the complexity out of security and compliance, it also takes the frustration and confusion out of purchasing.



CLOUD DEFENDER: BUILT TO PROTECT YOUR SENSITIVE DATA

Alert Logic Cloud Defender combines advanced technology with a team of certified security and compliance experts working 24x7 to keep your data safe, secure, and your environment compliant.

- Protects sensitive data on-premises, in the cloud and hybrid infrastructures with a single solution
- Integration of network, application and system protection delivers deeper insight into threats
- Managed and monitored by security experts providing continuous protection
- Subscription model provides protection at a lower cost than traditional security solutions

ALERT LOGIC CLOUD DEFENDER TAILORED FOR YOUR AWS DEPLOYMENTS

- Elastic scalability to protect your AWS environment as it changes
- Automatic asset discovery through AWS APIs
- Collects and analyzes key AWS data including S3, CloudTrail, and ELB data
- Continuous vulnerability assessment of AWS infrastructure
- Multi-region and VPC support

To learn more about how Alert Logic Cloud Defender can help protect your sensitive data visit www.alertlogic.com