

# Web Application Firewall

Fully Managed Critical Web Application Protection

## Hassle-Free Enterprise-Level WAF

Web applications are an important part of your business and a vital part of how customers interact with you. Unfortunately, web applications also give attackers another gateway into your critical assets and data. Businesses need to distinguish the good traffic from the bad in real-time, accurately.

Alert Logic delivers a highly versatile, enterprise-level, cloud-ready WAF that comes with a team of experts to eliminate the complexity for you.

### With Alert Logic's Fully Managed WAF You Receive

#### COMPLETE SETUP AND MANAGEMENT

From installation, deployment through to configuration, our experts ensure your Web Application Firewall is ready to block threats against your critical web applications. Our analysts fine-tune your WAF by monitoring your web application traffic, whitelisting valid requests and data, and building a policy that blocks malicious web traffic and other undesired activity.

As new threats emerge and your apps and portfolio change, our analysts will update your policy as needed or required. Our services eliminate the steep learning curve and associated staffing costs that come with managing a WAF.

#### TRADITIONAL AND BEHAVIOR BASED THREAT DETECTION

Alert Logic's WAF provides comprehensive features to protect your web applications. Whitelisting, blacklisting, and signature-based blocking are augmented by a learning engine that builds a model of your application to recognize activity that deviates from a known-good baseline of traffic. Using both a positive and negative security model in this way means the Alert Logic WAF knows how to recognize malicious activity as well as unexpected activity.

#### ALERT LOGIC WEB APPLICATION FIREWALL INCLUDES THE FOLLOWING

- 24/7 Support from our SOC
- Managed Deployment
- Ongoing Management & Tuning
- WAF Policy Building and Management
- Zero-Day Emerging Threat Detection
- Rule and Behavior-Based Detection
- Usage-based Application Learning
- Auto-Scaling and High Availability Setup
- Web-Application Aware Policies

## TUNED AND OPTIMIZED

Combining deep expertise in web applications and security with an intimate knowledge of the web application threat landscape, our dedicated team partners with you to optimize the Alert Logic technologies based on your unique profile.

Our out-of-the-box policies cover 10,000+ vulnerabilities, including unique flaws in off-the-shelf and custom web applications (e.g., OWASP Top 10, URL tampering, web scraping, buffer overflow attacks, Zero-Day web application threats, and DoS attacks.)

## LEVERAGING ALERT LOGIC'S INTELLIGENCE

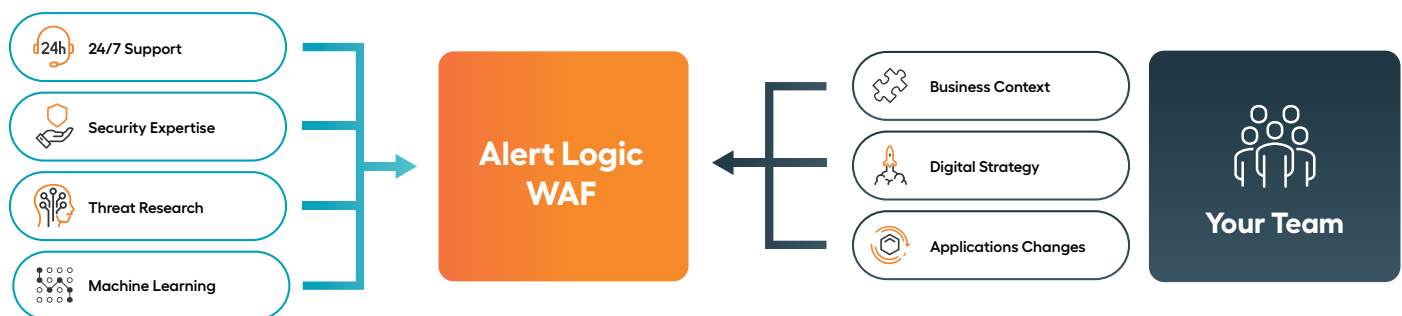
People are a critical component of Alert Logic's solutions and we have invested in security talent since 2002. This investment in deep security expertise allows Alert Logic to build detection technologies that provide broader and deeper protection than other providers or tools alone ever can. Behavioral-based content is leveraged to detect, monitor for, and block, more unusual attacks that WAFs with more specific signatures will miss.

izations, Alert Logic provides 24/7 peace of mind to our customers. Alert Logic provides the expertise our customers need to identify threats and respond more quickly.

- Cutting-edge threat intelligence and research maintain pace with the threat landscape.
- Expert security specialists place threats into context and verify incidents so that you can focus on what matters to your business
- Access to an industry-leading and always up-to-date security platform
- Security guidance and recommendations 24/7

We provide the security & WAF expertise to make sure your Alert Logic WAF is appropriately configured and a close partnership with your development and engineering teams, who understand application changes and functionality, allows us to provide a complete service.

Let us worry about the intricacies of WAF management and configuration so your delivery teams can focus on providing the best business value of your applications.



## ENTERPRISE-GRADE WEB APPLICATION SECURITY WITHOUT THE HASSLE

Effective web application protection requires a unique set of skills – cloud security experts who understand security, business applications, and cloud workloads. Alert Logic's team becomes an extension of your security team and eliminates the complexity of policy building and the challenges of ongoing threat management.

## WORKLOAD PROTECTION WHEREVER YOUR APPS ARE

The Alert Logic Web Application Firewall supports deployment in AWS, Azure, Google Cloud, physical and virtual environments including SSL offloading, auto-scaling load-balancing, and traditional high availability models.

## BLOCK MALICIOUS TRAFFIC, BUSINESS CONTINUES

From the attacker's perspective, web applications are attractive targets. A compromised web application allows attackers to steal information from the connected databases and infect other users of the site with web-based malware. Protecting web applications through the safe filtering of requests means no disruption to revenue and business operations.

## RAPID ADHERENCE TO COMPLIANCE

Immediately meet the web application firewall requirement of PCI DSS 6.6 & other compliance mandates. PCI DSS penetration tests are often performed from inside the network as well as outside, to try to attack web applications through all possible vectors. Cloud-based WAFs may be bypassed and can fail this requirement.

## Alert Logic's WAF is setup and managed by our team of experts and provides enterprise-grade WAF capabilities to protect your website, including:

Request and response web application learning, including
- Global and path specific parameters
- Static content and extension whitelisting/blacklisting
- Cookies
Request Header rewrites
DoS mitigation, request rate limiting
Full control over attack class criticality that extends to blocking based on a 3x-5x strike policy
Source IP tracking and access control
- Geo-IP blocking and Country whitelisting/blacklisting
External log notification
Sensitive Data Masking
Evasion and Multi-Encoding Detection
Configurable Header and Attack Signature validation
Validation of server requests and access, including filtering down to
- Request
- HTTP method
- Protocol
- Web service validation
- File upload
- URL path
- Cookies
- Dynamic application and parameter/path support
Broad signature set allows capture of zero-days and emerging web application threats
HTTP request and connection throttling for DoS mitigation
Session and CSRF protection
End to end request encryption
Trusted clients and domains
Backend server cloaking
Output headers validation and rewriting
Application Delivery Control
- Virtual Host configurations
- Redirects
- Load Balancing with session or cookie-based persistence
- Static & Dynamic Caching
- Acceleration and optimization

The Alert Logic WAF provides a front-line defense for your web applications, complimenting Alert Logic's MDR Services, which provide 24/7 Managed Detection & Response services for all assets.

## Essentials

Combat your risk of exposure to threats and protect your endpoints.

HYBRID ASSET DISCOVERY

VULNERABILITY SCANNING

CLOUD CONFIGURATION CHECKS

ENDPOINT DETECTION & RESPONSE

PCI DSS AND ASV PROGRAM SUPPORT

## Professional

Comprehensive 24/7 security visibility, protection, and reporting.

24/7 THREAT MANAGEMENT

15-MINUTE ESCALATION SLA

NETWORK MONITORING

LOG MANAGEMENT & MONITORING

CLOUD CHANGE MONITORING

USER BEHAVIOR MONITORING

## Enterprise

Threat Hunting, individualized protection and customized response.

ASSIGNED SECURITY EXPERT

THREAT HUNTING

PROACTIVE TUNING & OPTIMIZATION

WEEKLY REVIEW

EXTENDED SECURITY INVESTIGATIONS

SECURITY POSTURE REVIEW

Visit [www.AlertLogic.com/MDR](https://www.AlertLogic.com/MDR) to learn more