FORTRA

SOLUTION BRIEF (Alert Logic)

Alert Logic Web Application Firewall

Hassle-Free, Enterprise-Level WAF

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

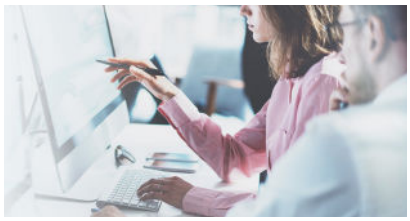
Fortra's Alert Logic Web Application Firewall (WAF) provides you a highly versatile, fully-managed, enterprise-level, cloud-ready solution supported by our team of experts.

What You Receive with Alert Logic's Managed WAF

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 activities.

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 our WAF knows how to recognize malicious and unexpected activity.

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 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, credential stuffing attacks, API attacks and DoS attacks).

SERVICES SUMMARY

KEY FEATURES

- 24/7 SOC Support
- Managed Deployment
- Ongoing Management and 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
- Proactive Virtual Patching
- Credential Attack Protection

Leveraging Alert Logic's Intelligence

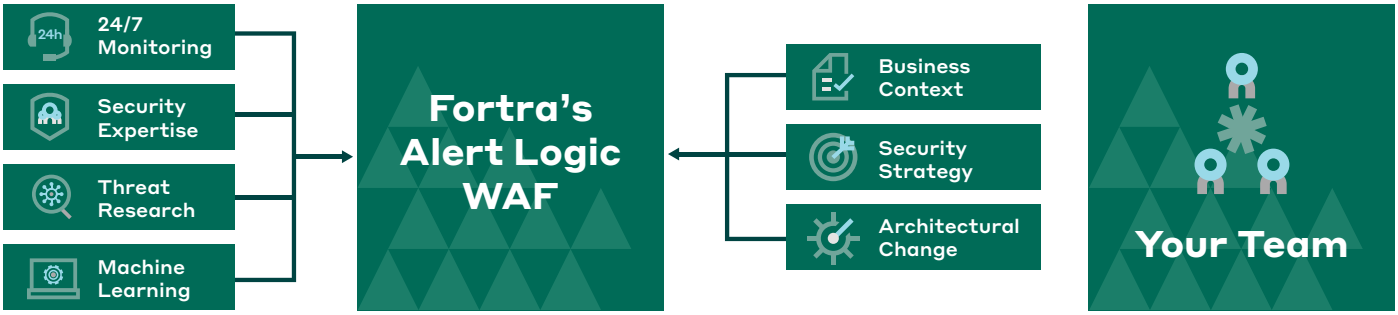
Since 2002, we have invested in the security talent that are a critical component of our solutions. This investment in deep security expertise allows us to build detection technologies that provide broader and deeper protection than other providers or tools ever can alone. Behavioral-based content is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

Alert Logic provides the expertise to identify threats and respond quickly. Service our customers receive includes:

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

We provide the security and expertise to ensure your Alert Logic WAF is appropriately configured. Our 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. Our experts become an extension of your security team, eliminating the complexity of policy building and challenges of ongoing threat management.

Workload Protection Wherever Your Apps Are

Our Web Application Firewall supports deployment in AWS, Azure, Google Cloud, and 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 safely filtering requests means no disruption to revenue and business operations.

Rapid Adherence to Compliance

Immediately meet the web application firewall requirement of PCI DSS 6.4 (formerly 6.6) and other compliance mandates. PCI DSS penetration tests often are 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 - Acceleration and optimization - Static & dynamic caching - Load balancing with session or cookie-based persistence

The Alert Logic WAF delivers a frontline defense for your web applications, complementing Fortra's Alert Logic MDR®, which provides 24/7 managed detection and 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 & 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

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.