FORTRA™

SOLUTION BRIEF

Managed 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 Managed 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 Fortra 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

Our Managed 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 our 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 Fortra's Threat Intelligence

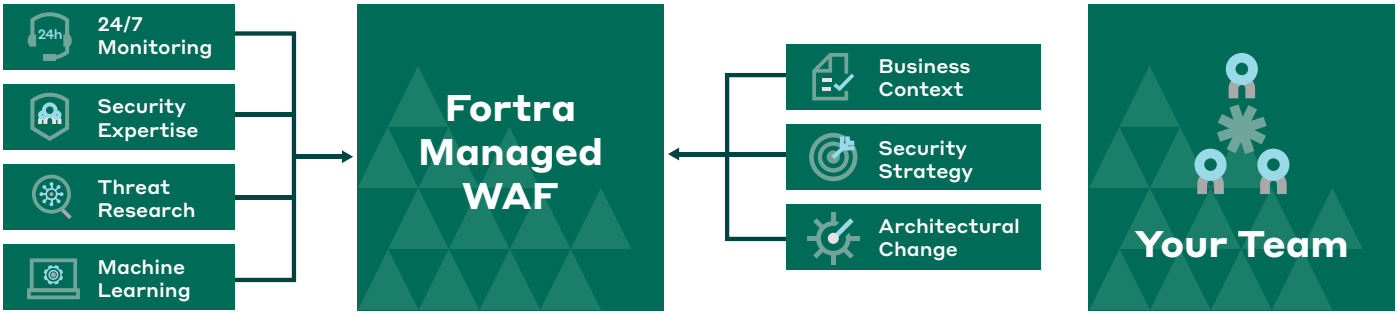
Since 2002, we have invested in the security talent that are a critical component of our solutions. This investment in deep security expertise allows us to build detection technologies that provide broader and deeper protection than other providers or tools ever can alone. Behavioral-based content is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

We provide 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 web 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 Fortra Managed 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 and API 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.

Fortra Managed WAF is setup and managed by our team of experts and provides enterprise-grade WAF capabilities to protect your website, including:

Feature/Capability	What It Means to You	How it Works
Advanced Application Protections	Utilize our WAF to protect applications that are inherently the most vulnerable to attack, including coverage for OWASP top 10 for both web applications and APIs.	Fortra web security experts optimize security policies informed by our Threat Intelligence network and machine learning. We then tune your application's specifications and business requirements to maintain security posture.
API Discovery and Protections	Protect your exposed API from application attacks with targeted policies informed by automated API discovery and mapping.	Our WAF automatically discovers APIs and builds API endpoint rules based on the API specification file. If the API is not previously documented, the learning engine will map it out and build in policy rules to protect it. This API protection is comprehensive and includes positive endpoint policies enforcing the API specification and anomaly detection along with anti-automation controls to counter volumetric and sequential attack patterns.
Emerging Threat Protection	Our WAF features forward-thinking policies with proven success in blocking zero-day attacks, providing mitigations against the most difficult threats to detect and block.	A combination of our advanced threat protections, machine learning, anomaly detections, and expert security policy optimization has had great success in defending against previously unknown attacks.
Managed Virtual Patching	Managed creation and automated application of virtual patches for 100+ top applications protects system vulnerabilities from exploitation keeping your environment secure between patch cycles.	Virtual patches are automatically updated and applied on a weekly basis. For zero-day exploits that are designated emerging threats, virtual patches are released and applied as needed extraneously from the normal patching cycle to provide real-time coverage when it is needed.
Bot Management	Protection against automated attacks and data scraping.	Session anomaly detection to enforce CAPTCHA controls and lock out automated requests sent by bots probing for vulnerability or worse.
Credential Attack Protection	Puts protections in place against brute force and credential stuffing attacks that use stolen credentials, accounting for around 75% of web application compromises (Verizon DBIR 2022).	The system uses CAPTCHA, rate limiting, and blocking to detect and prevent unauthorized automated activity, such as brute force password guessing.
Adaptive Trust-based Policies	Experience increased efficiency through minimized false positives and maximized protections by dynamically applying policies of increased scrutiny based on connection trust.	The WAF increases scrutiny based on a dynamic connection trust score, applying more restrictive policies to untrusted connections. WAF violations will contribute to the connection score and trigger additional security policies to be implemented.
Fortra Threat Intelligence	Enables WAF content developers to created research-driven security policies and controls, ensuring that web application and APIs keep pace with the constantly evolving threat landscape. Content includes virtual patches, signature updates, and attacker source IPs which are automatically distributed to the Fortra Managed WAF fleet.	Fortra's Threat Intelligence unifies the portfolio's leading threat intelligence programs and insights from securing tens of thousands of customers. Fortra's Threat Intelligence is used to track the evolution of tactics and techniques in the web security space as well as maintaining a repository of active malicious actor IP addresses and attack campaigns.

For more information, please visit **alertlogic.com**