OTAVA

DATA SHEET

WEB APPLICATION FIREWALL

Mitigate threats to your web-application data

Protect your web servers, databases and web based applications from malicious online attacks by utilizing Otava's web application firewall (WAF). A network firewall's open port allows internet traffic to access your websites, but it can also open up servers to potential application attacks, such as database commands to delete or extract data sent through a web application to the backend database. Sounds bad, right? No worries. WAF is here to save the day.

WAF is an appliance that resides in front of your virtual or dedicated firewall and scans any incoming traffic to web-facing servers and applications for malicious attacks that might compromise the security of the application, including Cross-site Scripting (XSS) and SQL injection attacks.

You're a perfect fit for Otava Web Application Firewall if...

- Your business desires greater control and protection of web based applications, data, and backend databases.
- You're an e-commerce, online healthcare, insurance or financial services business that handles sensitive records or customer data.
- Your business requires application level security to assure HIPAA and PCI compliance.
- Your IT/Security team requires WAF vs code review to assure better protection against newly emerging and constantly evolving threats.
- Your IT/security team requires policy based web application security that provides monitoring and notification of potential attacks.

Why Otava Web Application Firewall?

Reduce complexity and cost

Code review is an alternative option to WAF that satisfies similar requirements but does not offer the added layer of security that WAF provides. Depending exclusively on code review can be costly, complex and more difficult to manage than a WAF.

Required for PCI DSS compliance

If you are a merchant that needs to meet PCI DSS compliance (Payment Card industry Data Security Standards) because you collect, store or process credit cardholder data, then you need to install a WAF in front of all public-facing web applications.

Meets HIPPA compliance mandate

For healthcare, healthcare support, or insurance organizations that collect, store or transmit electronic protected health information (ePHI) and are required to meet HIPAA compliance, WAF addresses Technical Safeguards of the HIPAA Security Rule mandate.

How is Web Application Firewall Configured?

Protects incoming traffic

WAF is an appliance that sits in front of your virtual or dedicated firewall and scans incoming traffic to web servers for malicious attacks that may affect the web application server security, performance, or availabilty.

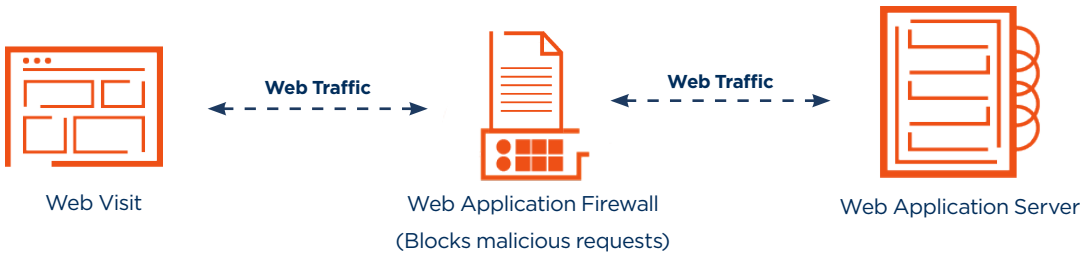
Dynamic profiling at a global scale

A WAF uses dynamic profiling to learn what kind of traffic and users are normal, and what could potentially be malicious traffic. AI-based intelligence at a global scale increases detection accuracy and reduces false positives

Action on suspicious requests

Suspicious requests can be blocked, challenged or logged as per the needs of the user while legitimate requests are routed to the destination, agnostic of whether it lives on-premise or in the cloud.

How Web Application Firewall Works



Otava's Web Application Firewall meets Compliance

PCI DSS & HIPAA

PCI requirement 6.6 states:

Verify that a web-application firewall is in place in front of public-facing web applications to detect and prevent web-based attacks. - PCI DSS Requirements and Security Assessment Procedures, Version 2.0.

For public-facing web applications, ensure that either one of the following methods are in place as follows:

They are reviewed using manual or automated vulnerability security assessment tools or methods:

- at least annually
- after any changes
- by an organization that specializes in application security
- after vulnerabilities are corrected

HIPAA §164.312(e)(1)- Transmission Security:

Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.

Bolster your defense in depth strategy with a Web Application Firewall.

- Detect and block unknown attacks, prevent data leaks, and enforce content policies
- Lock down insecure systems and mitigate the risk of inadequately configured servers compromising your business

Otava's Web Application Firewall Benefits:

- **Provides an extra layer of protection that a network firewall and IDS cannot.**
- **Can prevent attacks & data exposure before it happens by detecting malicious users & requests for information.**
- **Dynamic profiling sets accepted traffic criteria based on user behavior; custom-fit to the client's site & application.**
- **Can identify malicious sources to stop automated attacks.**
- **Fulfills PCI DSS requirement 6.6 to install a WAF in front of public-facing web application.**

OTAVA

EXPECT EXCEPTIONAL

OTAVA provides secure, compliant hybrid cloud solutions for service providers, channel partners and enterprise clients. By actively aggregating best-of-breed cloud companies and investing in people, tools, and processes, Otava's global footprint continues to expand. The company provides its customers with a clear path to transformation through its highly effective solutions and broad portfolio of hybrid cloud, data protection, disaster recovery, security and colocation services, all championed by its exceptional support team. Learn more at www.otava.com.

DON'T WAIT TO LEVERAGE THE COMPLIANCE & ADDED SERCURITY OF A WEB APPLICATION FIREWALL. Talk to a specialist now.

OTAVA.com (877) 740-5028 solutions@otava.com