

# SmartWAF™ Web Application Firewall



# SmartWAF

SmartWAF™ is a host-based integrated Web Application Firewall (WAF) that hardens and regulates access to web applications. While traditional perimeter security controls work at the network and system layer, SmartWAF™ focuses on preventing attacks that target vulnerable web applications. As a software plug-in on the web server, it offers flexible deployment and configuration options for optimum web infrastructure security. It also integrates with the CodeSecure™ Source Code Analysis platform, importing its findings and reconfiguring its rule set to explicitly block web application exploits targeting code-level vulnerabilities. As a dynamic security control, SmartWAF™ offers a highly accurate, efficient solution where costs scale linearly with web services complexity.

## Why do we need Web Application Firewalls?

Network and system level security controls do not equate to web application security. Traditional perimeter security technologies focus on attacks written at the network and transport layer. However, web application exploits such as Cross Site Scripting (XSS) and SQL Injection are higher in the protocol stack and are typically processed as legitimate traffic bound for the web server.

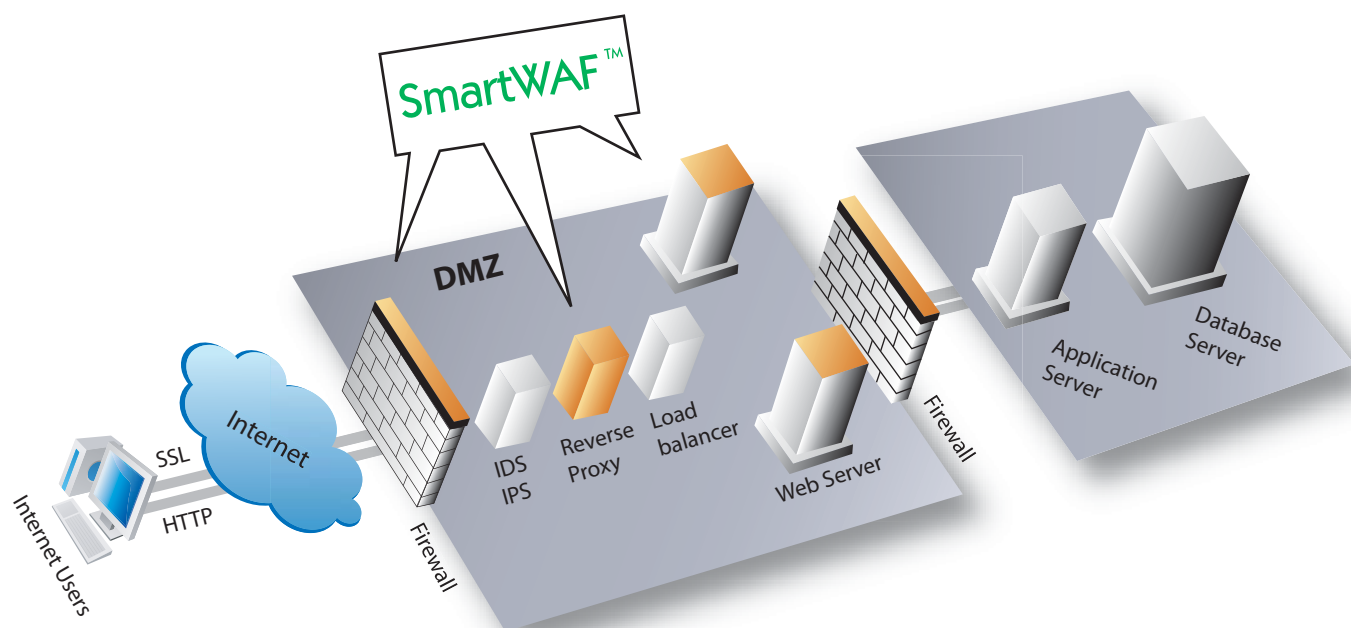
These attacks can have a devastating effect on businesses, often resulting in operational failure, client or corporate financial loss, legal liability for breach of customer confidentiality, compliance failure, untold reputation damage, and ultimately in loss of business.

As a state-of-art Web Application Firewall, SmartWAF™ focuses on the vulnerabilities that traditional perimeter security controls miss. By identifying, classifying and blocking malicious exploits embedded in the web application traffic stream, it does not replace existing network perimeter security controls such as stateful/proxy firewalls, antivirus gateways, IDS or reverse proxies but complements them in an efficient and cost-effective manner.

# SmartWAF™ Overview

## Flexible deployment

Unlike appliance-based Network WAF platforms, SmartWAF™ offers flexible deployment as it can be installed as a software plug-in directly on the web server, reverse proxy or security gateway.



It is accepted practice to install a network level firewall between the trusted network and the Internet and when it comes to protecting web applications, many businesses have used similar logic and have considered implementing a Network WAF. However, the Network WAF represents a single entry point for all traffic, and as web applications increase in number and complexity, the Network WAF requires an ever increasing list of policies which severely affect processing time creating a traffic bottleneck, slowing response-time and degrading the quality of the website. In addition, it represents a single point of failure affecting all web applications.

Installing SmartWAF™ as a web server plug-in offers obvious advantages. With web application protection mechanisms spread across all web servers, the inefficiencies of a “one-size-fits-all” rule set, traffic bottleneck and single point of failure are all removed.

## SmartWAF™ Operation

SmartWAF™ integrates with IIS, Apache or Java-based web servers running on Windows, Linux or UNIX platforms and consists of three main components as follows:

- The **Enforcer** captures every HTTP request and forwards it to the Decider for further investigation.
- The **Decider** evaluates HTTP requests based on its rule set, compiles logs and statistics and provides the interface between the Enforcer and administration interface.
- The **Administration Interface** is an easy-to-use, web-based user interface for management of single or multiple servers running SmartWAF™, security administration and access to log files and statistics.

SmartWAF™ is highly configurable and can be tuned to specifically defend against a range of web application attacks including SQL Injection, Cross Site Scripting, HTTP Response Splitting, Application Fingerprinting, Directory Indexing, Session Fixation, Content Spoofing and Web Server Fingerprinting

## SmartWAF™ Management

With its intuitive web-based user interface, SmartWAF™ provides easy-to-administer configuration and security functions. In Basic Mode, there are step-by-step guides and wizards while Expert Mode allows manual creation of specific rules to address vulnerabilities in the web application source code. The advantage of using this type of strategy is that rules can be customized not only for each application within the infrastructure, but also for specific portions of each application.



The SmartWAF™ Cluster Management feature provides centralized configuration and management across multiple SmartWAF™ instances via a single Web interface. Rules can be applied to all web applications or to particular components, and there is full support for version history allowing “Rollbacks” to earlier configurations and to facilitate auditing tasks.

The central log file analysis provides real-time information relating to incoming traffic, assisting in attack detection and mitigation, while detailed statistical reporting offers infrastructure monitoring and risk assessment.

### Integration with CodeSecure™

SmartWAF™ integrates with CodeSecure™ importing source code analysis findings and reconfiguring its rule set to explicitly block web application exploits targeted at vulnerabilities identified by CodeSecure™. This provides an extra-layer of immediate protection for those customers who do not have immediate resources to fix critical code-level vulnerabilities.

### Reporting, Logs and Analysis

SmartWAF™ features a number of reporting options facilitating compliance with legal or contractual regulations. These options also assist in analysis of common attack points or points at which security is too stringent, restricting legitimate users.

- Graphic statistical displays show the distribution of accepted and denied requests according to time and individual rules.
- Log files illustrate internal host-specific system events and error messages.
- The Audit Log lists all security-related changes.
- The Default Error Log lists events such as invalid requests, or requests with a hostname which does not match any of the configured hosts.

### Investment Optimization

SmartWAF™ optimizes the investment in information security through its unique deployment strategy.

Network WAFs (NWAFs) have a high initial cost, both in terms of price and deployment overhead. As the web server infrastructure becomes more complex, additional devices are required to address performance bottlenecks and redundancy.

As a software application, SmartWAF™ is delivered on a per web server basis, allowing security costs to scale linearly with web server infrastructure complexity.

## Supported Web Platforms

Microsoft IIS  
Microsoft ISA  
Apache  
WebSphere  
WebLogic  
Tomcat

## Supported OS

Microsoft Windows  
Linux  
FreeBSD  
OpenBSD  
Sun Solaris

## Armorize Headquarters

5201 Great America Parkway  
Suite 320, Santa Clara, CA 95054  
U.S.A.  
Office: +1-408-216-7893  
FAX: +1-408-583-4288

## Armorize Asia Pacific R&D

NanKang Software Park, San Chong Rd,  
19-13, Building E, Office 553, 5th Floor,  
Taipei, Taiwan  
Office: +886-2-6616-0100  
Fax: +886-2-6616-1100

## SmartWAF™ Summary

- Host-based integrated Web Application Firewall (WAF) installed as a software plug-in directly on the web server
- Hardens and regulates access protecting against attacks on web applications
- Inspects and analyzes web application traffic and blocks embedded application layer malicious code that network and system level security controls typically miss
- Detects and prevents malicious AJAX code execution, Cross-Site Scripting (XSS), Session Hijacking, File Inclusion, Cross-site Request Forgery, and Injection Attacks (SQL, File, XPATH, Command, Reflection)
- Rules can be created to protect the web server or a specific web application
- Centralized management of multiple SmartWAF™ applications from a single web interface
- Supports rule creation based on input from CodeSecure™ reconfiguring its rule set to explicitly block exploits targeting vulnerable entry points
- Software plug-in purchased per web server allows security costs to scale linearly with web server infrastructure complexity
- No traffic bottleneck or single point of failure

## About Armorize Technologies Inc.

Armorize Technologies provides next-generation web application security solutions traversing the System Development Life Cycle (SDLC).

From static source code analysis with CodeSecure™ to real time web application protection with SmartWAF™ and malicious code detection with HackAlert™, Armorize technologies' award-winning solutions are the culmination of years of research and innovation.

Led by a number of internationally acclaimed security veterans and financed by top Silicon Valley investors, the company was formed in 2005 with its headquarters in Santa Clara, CA, and its R&D centre in the Nan Kang Software Park in Taipei, Taiwan.

Armorize has a global customer base with clients from among finance, telecom, government and technology sector leaders.

For more information visit [www.armorize.com](http://www.armorize.com)