ORACLE

Oracle Web Application Firewall for SaaS: Oracle Cloud's Frontline Defense

How Oracle SaaS Cloud Security can help organizations protect applications with web application firewalls as a frontline defense—building resilience against cyberthreats and reinforcing overall cloud security

November 2024, Version 1.0

Public

Purpose Statement

This document provides an overview of the features of Oracle Web Application Firewall (WAF) for SaaS to help you understand the business and security benefits for Oracle SaaS customers.

Disclaimer

This document in any form, software or printed matter, contains proprietary information that is the exclusive property of Oracle. Your access to and use of this confidential material is subject to the terms and conditions of your Oracle software license and service agreement, which has been executed and with which you agree to comply. This document and information contained herein may not be disclosed, copied, reproduced or distributed to anyone outside Oracle without prior written consent of Oracle. This document is neither part of your license agreement nor can it be incorporated into any contractual agreement with Oracle or its subsidiaries or affiliates.

This document is for informational purposes only and is intended solely to assist you in planning for the implementation and upgrade of the product features described. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, timing, and pricing of any features or functionality described in this document remains at the sole discretion of Oracle. Due to the nature of the product architecture, it may not be possible to safely include all features described in this document without risking significant destabilization of the code.

ORACLE

Table of Contents

Introduction

As organizations increasingly transition critical operations to software-as-a-service (SaaS) applications, robust security measures are essential to ensure data integrity and safeguard against cyberthreats. Web application firewalls (WAFs) have become a vital component in this defense, focusing on the application layer (Layer 7) to secure web applications by filtering, monitoring, and blocking potentially harmful HTTP/S traffic. This capability is critical, as WAFs help prevent attacks that exploit common web vulnerabilities such as SQL injections, cross-site scripting (XSS), file inclusion, and misconfigurations within the application environment.

WAF operates differently from traditional network firewalls, which focus on Layers 3 and 4 to protect data transfer and network protocols such as Domain Name System (DNS), File Transfer Protocol (FTP), and Simple Mail Transfer Protocol (SMTP). Unlike these firewalls, WAF is specifically designed to defend against attacks that target web applications over HTTP and HTTPS, which is essential in today's cloud-based, application-focused environments.

Oracle WAF for SaaS is an implementation of a WAF that's deployed and managed by Oracle SaaS Cloud Security to provide comprehensive application layer protection for Oracle's SaaS environments. Leveraging Oracle Cloud Infrastructure's (OCI) advanced WAF capabilities, WAF for SaaS provides a consistent, automated defense against a wide range of cyberthreats such as the Open Source Foundation for Application Security (OWASP) Top Ten, while meeting rigorous compliance standards such as the Payment Card Industry Data Security Standard (PCI-DSS). Seamlessly integrated into the SaaS environment, WAF for SaaS helps enable proactive, defense-in-depth security, supporting the resilience and trustworthiness of SaaS environments.

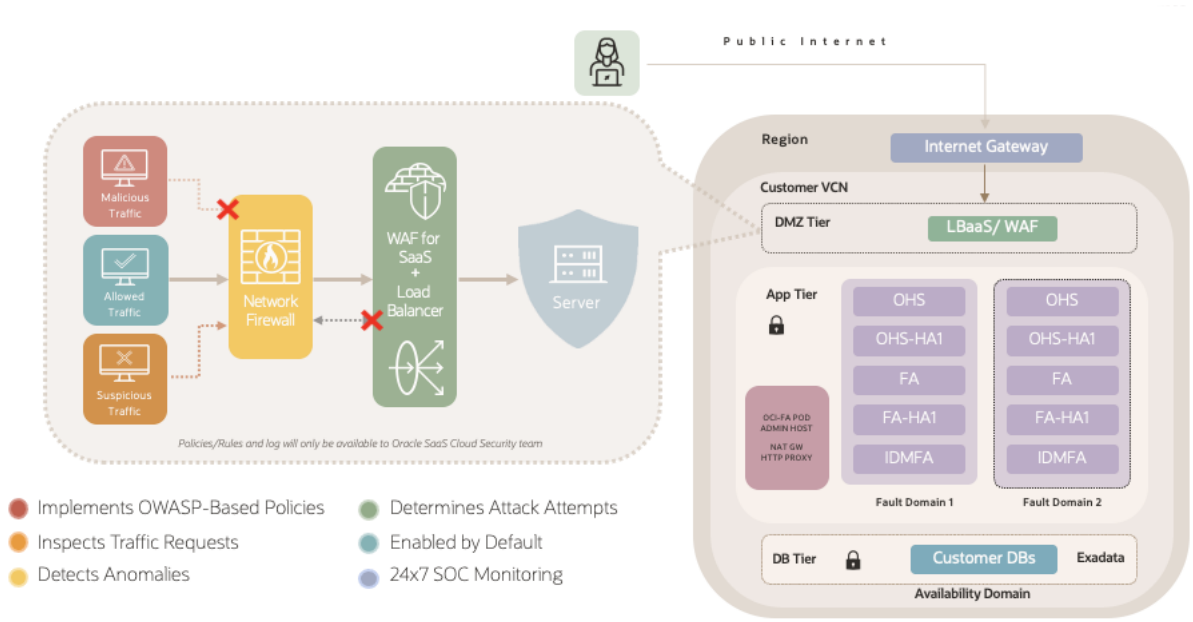

Figure 1. Oracle WAF for SaaS Filters Traffic and Protects SaaS Applications with 24x7 Monitoring

Practical Applications of Oracle WAF for SaaS

- **Protect websites and applications**: WAF for SaaS is designed to protect applications that communicate over HTTP/S, covering a wide range of use cases such as websites, API endpoints, and serverless functions. Positioned as the first layer of defense for the web, WAF for SaaS helps detect and mitigate against both known and emerging threats. Beyond traditional firewall capabilities, it defends against advanced attacks, including the OWASP Top Ten threats, supports Transport Layer Security (TLS) security mechanisms, and enforces stringent security policies.
- **Comply with security and regulatory standards**: Beyond threat prevention, WAFs are essential for regulatory compliance, particularly for websites that handle sensitive data such as credit card information. For example, the PCI-DSS mandates security assessments for systems that process credit card data (Requirement 6.6). Noncompliance can lead to significant fines and data breaches. Implementing a WAF often proves to be a cost-effective and efficient solution by meeting PCI-DSS requirements without the expense of a full code review. In addition to PCI-DSS, industries regulated by standards such as Health Insurance Portability and Accountability Act (HIPAA) and Sarbanes-Oxley Act (SOX) also benefit from the security assurances provided by WAF for SaaS.
- **Control bots and mitigate distributed denial-of-service (DDoS) attacks**: Managing bot access is essential for reducing the impact of unauthorized actions such as content scraping, spam, data theft, malware injection, API abuse, password brute-forcing, and DDoS attacks. By limiting resource overuse, WAF capabilities help to mitigate the risk of unexpected costs and operational disruptions caused by these automated threats.
- **Patch vulnerabilities**: For vulnerabilities, especially those introduced through third-party code, a WAF can help provide an internal security layer. By blocking known exploit patterns and malicious traffic, WAF assists in safeguarding applications until code patches can be applied, helping organizations maintain operations and manage risks during the remediation process.
- **Detect intrusions in real time**: Serving as a central point for logging and security metric collection, WAF supports robust real-time intrusion detection. Comprehensive traffic monitoring allows administrators to detect potential attacks as they occur, enabling a real-time response. Additionally, WAF logs are useful for diagnosing and reviewing past security events, providing insights to help improve response strategies.
- **Enforce content policies**: With the capability to inspect and filter HTTP packets, WAF enables granular control over web traffic. Service providers and organizations can set rules to allow or block content based on specific criteria such as file types, classifications, or geographic origin. This level of control supports regional content delivery, enforces geographic restrictions, and helps comply with export restrictions.

Understanding WAF Solutions: Differences Between WAF for SaaS and OCI WAF

Oracle's security ecosystem has two WAF solutions, WAF for SaaS and OCI WAF, which serve specific environments. To ensure clarity, it's essential to understand their unique capabilities and limitations. Although both solutions protect applications from web-based threats, only WAF for SaaS is tailored specifically for Oracle SaaS environments, offering an Oracle-managed security layer that's preconfigured and maintained for SaaS customers.

OCI WAF

- A customer-managed WAF solution within Oracle Cloud Infrastructure, OCI WAF provides comprehensive protection for internet-facing applications. Customers have full control over policy creation, logging, and threat management for their infrastructure-as-a-service (IaaS) and platform-as-a-service (PaaS) environments.

- Designed for customer-managed cloud services and workloads, OCI WAF isn't available for direct configuration in Oracle's SaaS applications.

WAF for SaaS

- An Oracle-managed WAF service automatically integrated into Oracle SaaS platforms. This solution is configured, maintained, and managed by the SaaS Cloud Security team and requires no setup by customers.
- WAF for SaaS leverages OCI WAF capabilities but is optimized specifically for SaaS applications, with regular policy updates and ongoing threat management, provided at no extra cost to SaaS customers.

Key Differences Between WAF for SaaS and OCI WAF

Area	WAF for SaaS	OCI WAF
Ownership	Managed entirely by Oracle's SaaS Cloud Security.	Customer-managed for IaaS and PaaS environments.
Artifacts	Automatically enabled and maintained by Oracle. Customers can't directly enable or configure WAF within SaaS.	Customers control and configure policies and rules.
Threat management	Threat detection and response through Oracle's SaaS Security Information and Event Management (SIEM), with oversight by the SaaS Cloud Security Detection and Response Team (DART) team.	Customer is responsible for threat management.

WAF for SaaS: Tailored Security for Oracle SaaS Applications

WAF for SaaS provides the following key benefits and core compatibilities and features.

Key Benefits of WAF for SaaS

- **Uniform, transparent security**: Helps provide consistent security capabilities across all SaaS customer environments, which supports a strong overall security posture
- **Integrated "defense in depth"**: Preconfigured and embedded at the SaaS platform level to serve as an essential layer within the security framework
- **Protection against common exploits**: Supports OWASP-based policies to help guard against well-known attack vectors and exploit attempts
- **Comprehensive traffic monitoring**: Inspects HTTP requests, identifies anomalies, and helps detect potential attack attempts in real time
- **24x7 security monitoring**: Supported by Oracle's Security Operations Center (SOC), with dedicated experts who understand the specific needs of Oracle SaaS applications
- **IP-based controls**: Provides IP-based controls for both IPv4 and IPv6 (inbound only), offering flexible and secure access management
- **No additional cost**: Available at no extra charge for Oracle SaaS customers, offering a cost-effective layer of security
- **Managed by Oracle Security experts:** Managed by Oracle on behalf of SaaS customers, ensuring expert oversight and support

Core Capabilities and Features of WAF for SaaS

WAF for SaaS is designed to defend against malicious attacks aimed to exploit potential vulnerabilities in web applications, such as the following:

- Injections—Structured Query Language (SQL), Lightweight Directory Access Protocol (LDAP), operating system (OS), and more
- Broken authentication and session management
- Cross-site scripting (XSS)
- Insecure direct object references
- Sensitive data exposure
- Missing function-level access control

WAF for SaaS Essentials: Detect, Alert, Act

Area	WAF for SaaS
Detect	• Monitors HTTP traffic in real time, providing both monitoring and blocking modes for full visibility into incoming threats • Implements rate-limiting and DDoS protection
Alert	• Offloads logs to SIEM for continuous log streaming and monitoring • Aggregates activity and event logs for centralized oversight • Uses a streaming service for real-time alerts
Act	• Enables IP address allowlists and blocklists • Supports geographic restrictions in compliance with Oracle's Global Information Security (GIS) policies, including IP-based and country-based restrictions

Note about geographic restrictions: WAF for SaaS includes geographic restriction capabilities that enforce country-specific embargoes and sanctions. This feature, guided by the SaaS Cloud Security Governance, Risk, and Compliance team, helps Oracle SaaS customers comply with global trade restrictions and secure applications within designated regions as necessary.

WAF for SaaS: Frequently Asked Questions

- **What is WAF for SaaS?**

  WAF for SaaS is Oracle's managed, second-generation, enterprise-grade cloud security solution. Designed as an additional security layer, it provides continuous Layer-7 protection against targeted attacks. Integrated at the SaaS platform level, WAF for SaaS monitors and detects malicious HTTP/S traffic to help safeguard Oracle SaaS applications and customer data.

- **What's the purpose of WAF for SaaS?**

  The primary purpose of WAF for SaaS is to provide seamless, consistent security for Oracle SaaS customers, focusing on high availability and performance. Key purposes include the following:

  - Enforcing standardized WAF policy templates across SaaS products, which enables consistent signals for SaaS Security Analytics

- Coordinating and standardizing response procedures across all SaaS services, to detect and defend against attack payloads aimed at exploiting publicly reported vulnerabilities in common open source and commercial software components
- Leveraging a centralized Security Incident and Event Management (SIEM) platform maintained by Oracle for log ingestion
- Enabling adherence to compliance requirements such as PCI DSS 4.0 for Cloud services

- **How does WAF for SaaS work?**

  WAF for SaaS operates as a regionally deployed security service attached to an enforcement point such as a load balancer or web application domain. It filters malicious and unwanted internet traffic, protecting any internet-facing endpoint within the SaaS environment through consistent rule enforcement. Rules are designed to block threats, including cross-site scripting (XSS), SQL injection, and other vulnerabilities, while also allowing restrictions based on geography or request signature.

- **How does WAF for SaaS protect my applications?**

  Incoming traffic to protected sites passes through WAF for SaaS, where it is inspected according to predefined rules. Based on these rules, the WAF blocks or allows traffic, providing a protective filter to secure applications from harmful flows.

- **Which types of attacks does WAF for SaaS help protect against?**

  WAF for SaaS is equipped to mitigate common attack techniques such as SQL injection and cross-site scripting (XSS). Customers can request the setup of rules to block or rate-limit traffic from specific sources, such as certain IP addresses, user agents, or request headers, by submitting a Service Request (SR).

- **Does enabling WAF for SaaS affect application performance?**

  Enabling WAF for SaaS doesn't impact application performance. Stress tests on high user loads and application workflows have validated the service for functionality and performance.

- **Which Oracle SaaS products are enabled with WAF for SaaS?**

  WAF for SaaS is available only on OCI. It's enabled for Fusion applications, and its adoption is being extended to all SaaS products and services. Contact Oracle SaaS Support to confirm whether your SaaS product is WAF-enabled.

- **What are the WAF for SaaS policies and rules and are they based on industry standards?**

  WAF policies are a set of rules that detect and block various attack patterns. These rules cover a broad spectrum of threats and are based on the ModSecurity Core Rule Set (CRS) but employ those that are relevant to SaaS technical stack and design,

- **Are the WAF for SaaS policies and rules available for customers?**

  No. Oracle doesn't provide WAF for SaaS policies or rules externally because of security considerations. Revealing these security controls could potentially enable bad actors intending to exploit.

- **How are policies managed and updated?**

  Oracle's SaaS Cloud Security team authors and maintains the WAF policies, balancing security, performance, and stability requirements. Policies are reviewed and updated regularly to reflect new threats and vulnerabilities.

- **Are there rate-limiting rules?**

  Yes, rate-limiting rules are implemented as part of the WAF configuration to protect SaaS environments from traffic overloads and as a potential defense against DDoS attacks.

- **Does WAF for SaaS leverage threat intelligence?**

  Threat intelligence feeds from multiple sources support WAF's security processes, helping to identify and block malicious IP addresses effectively.

- **How is false-positive blocking managed?**

  WAF policies undergo thorough testing to minimize false positives. If customers encounter blocked requests that appear to be false positives, they can submit a Service Request for review.

- **Are WAF for SaaS events monitored, and are customers notified of events?**

  WAF events are integrated into Oracle's SaaS Cloud Security SIEM platform, which enhances monitoring, detection, and response capabilities. Oracle's SOC teams notify customers about any events, including WAF-related ones, wherever necessary (consistent with our relevant hosting-related policy).

- **Are all requests logged?**

  Yes, all incoming requests are logged, providing a complete record of traffic and threat data.

- **Is sensitive data obfuscated in logs?**

  WAF for SaaS logs don't include any sensitive customer data.

- **Does WAF for SaaS support log forwarding?**

  WAF for SaaS logs are retained within Oracle's SIEM systems and aren't forwarded to external dashboards.

- **How long are WAF for SaaS logs retained?**

  WAF for SaaS logs are retained for a period that's consistent with Oracle's SaaS Cloud Security data retention policies.

- **Can customers configure WAF for SaaS?**

  WAF for SaaS is a managed service integrated with SaaS products, and all configuration and management is handled by Oracle. Although customers don't have direct management capabilities, they can refer to the My Oracle Support (MOS) notes for guidance on requesting customizations.

- **What is the shared responsibility model in the context of WAF for SaaS?**

  As a managed service, Oracle controls WAF for SaaS, although customers can request specific rule adjustments by submitting Service Requests. For details, see the SaaS cloud security: Know your responsibility blog post.

- **Can customers disable WAF for SaaS?**

  Disabling WAF for SaaS isn't an option because it serves to protect both customers and SaaS applications. Any issues can be addressed through a Service Request.

- **Are custom error pages supported?**

  Custom error pages aren't supported in the current configuration.

- **Can customers request logs for audits?**

  Customers can request WAF for SaaS logs for security, operational, or compliance audits through My Oracle Support (MOS).

- **How can customers contact WAF for SaaS support?**

  Customers can reach WAF for SaaS support through the Oracle Customer Support portal or their Customer Success Manager (CSM). See the following knowledge articles:

  - How to submit a Technical Service Request for WAF for SaaS? (Doc ID 2969373.1)
  - How To Request for WAF for SaaS IP Based Access Control? (Doc ID 2969290.1)
  - How To Request for WAF for SaaS Logs? (Doc ID 2969307.1)

Connect with us

Call +**1.800.ORACLE1** or visit **oracle.com**. Outside North America, find your local office at **oracle.com/contact**.

blogs.oracle.com facebook.com/oracle twitter.com/oracle