

Oracle Cloud Infrastucture Web Application Firewall

SQL injections. Cross-site scripting. Distributed denial of service (DDoS) attacks. Botnets. These are just some of the cyber-weapons increasingly being used by malicious actors to target web applications, cause data breaches, and expose sensitive business information.

Cybercriminals are leveraging advanced hacking techniques and readily available bots that exponentially grow their capabilities, making it easier for them to infiltrate web-based assets. As a result, web application security has become a must-have for every organization that does business over the internet.

Organizations facing these challenges need a powerful, cloud-based web application firewall (WAF) with global scale that can protect their websites and internet-facing applications from today's cyberattacks. Oracle and KPMG recently surveyed 456 cybersecurity and IT professionals in North America, Western Europe, and Asia and found that a whopping 86 percent rated WAFs as the most important edge service.

The Oracle Cloud Infrastructure Web Application Firewall (Oracle WAF) is a cloud-based, global security service that protects applications from malicious and unwanted internet traffic. The WAF— which is fully integrated with the Oracle Cloud Infrastructure management console—can protect any internet-facing web application and provides consistent rule enforcement across an organization's web applications.

Oracle WAF uses a multilayered approach to protect web applications from a host of cyberthreats including malicious bots, application layer (L7) DDoS attacks, cross-site scripting, SQL injection, and vulnerabilities defined by the Open Web Application Security Project (OWASP). When a threat is identified, Oracle WAF automatically blocks it and alerts security operations teams so they can investigate further.

Did You Know...

not all cloud WAF solutions are created equal? Many providers offer WAFs as a virtual machine (VM) that runs in a public cloud hypervisor service. But cloudbased VMs must still be patched and updated by the customer. Customers are responsible for scaling their VMs, whereas true, cloud-native WAFs are built to scale. When evaluating WAFs, be sure to look for a purely cloud-based solution that's supported by a global cloud infrastructure.

ORACLE

What the OCI WAF Provides

The OCI WAF is an enterprise-grade, cloud-based, globally deployed security solution designed to protect business-critical web applications from malicious cyberattacks. The OCI WAF provides a suite of security services that uses a layered approach to protect web applications against cyberattacks. This release includes over 250 predefined Open Web Access Security Project (OWASP) rules, application-specific rules, and compliance rules. The WAF also provides aggregated threat intelligence from multiple sources like Webroot BrightCloud[®]. Administrators can add their own access controls based on geolocation, whitelisted and blacklisted IPs, and HTTP URL and header characteristics. Bot management provides a more advanced set of challenges including JavaScript acceptance, CAPTCHA, device fingerprinting, and human interaction algorithms. Onboarding your applications to OCI WAF will protect against Layer 7 denial-of-service (DDoS) attacks.

How OCI WAF Works

The massively scalable Oracle WAF is supported by a global network, and the WAF's architecture creates a protective shield that serves as a security perimeter for an organization's web applications and services.

Oracle WAF security administrators can create and manage rules that will mitigate threats against business-critical web applications. The rules can also be used limit access to web applications based on geography or the signature of incoming requests. All incoming web traffic flows through the Oracle WAF network prior to arriving at your application server. This allows the WAF to inspect the traffic, compare against the pre-defined rules, and then block it or allow it to pass through as needed.

Oracle Dyn WAF offers a flexible solution that is easily deployed and continuously managed. This guarantees ongoing monitoring and tuning of WAF security policies to maintain optimal performance and effective security for your web applications.

	🖸 Seach 🔮 us-aidburn-1 👻
arnas2.test.lt	
Policy Information Tags	
WAF Policy Name: arna2.test.h Primary Domains: arna2.test.h Additional Domains: //o lokue OGID:hdsuga <u>Straw</u> <u>Copy</u> CNAME Target: arna5- test-Ita, wase, ool analideleud not Date Created: Dec 20, 2018 07.11.04 GMT	
Overview	
Origin Management Define the ports and URLs for a pool of origin servers used for cashe rules and Protection Rule settings. You can also set the response headers for outbound traffic to the origin server.	Settings Manage domain keys and SSL certificates and assign them to your application.
Destantion Poles	Access Control
FT0492-001 FT0495 These predefined rules spon various security and compliance best practices, from OWASP common rule sets for SQL injection and Colos Site Scripting (XSIS) to FCI and application-specific rules. Here you can subscrite to	ACCESS CONTROL Define explicit actions for requests that meet various conditions based on URI, request headers, client IP as or Countres and Regions. Conditions can leverage regular expression and lat comparison tools. Actions of

Figure 1. The WAF provides a custom security profile for each web application under protection, based on more than 250 rules.

Oracle WAF Features at a Glance

- Tightly integrated into Oracle Cloud Infrastructure management console
- Supports over 250 rulesets, including the OWASP top ten
- JavaScript and CAPTCHA challenges block bad traffic while allowing legitimate traffic to pass through
- Configure user access controls based on geography, IP address, URLs and other attributes
- Protects Oracle Cloud Infrastructure, onsite, hybrid cloud, and multicloud workloads
- Provides API, SDK, and Terraform support for easy integration with other systems
- 24/7 security operations centers act as an extension of users' security teams

ules	Recomm	endations Rule Settings			
Rules	0				
Acti	ens •				
	Rule ID	Protection Rule	Action		
0	941340	Cross-Site Scripting (XSS) Attempt: XSS Filters from Internet Explorer Cross-Site Scripting (XSS) Attempt: XSS Filters from IE	Block		
		OWASP OWASP-2017 CRS3 WASCTC PCI HTTP A2 A2-2017 XSS CROSS-SITE SCRIPTING			
0	941330	Cross-Site Scripting (XSS) Attempt: XSS Filters from Internet Explorer Cross-Site Scripting (XSS) Attempt: XSS Filters from IE	. Bisch		
		OWASP OWASP-2017 CRS3 WASCTC PCI HTTP AZ A2-2017 XSS CROSS-SITE SCRIPTING			
	941320	Cross-Site Scripting (XSS) Attempt: HTML Tag Handler Cross-Site Scripting (XSS) Attempt: HTML Tag Handler	Block		
		OWASP OWASP-2017 CRS3 WASCTC PCI HTTP A2 A2-2017 XSS CROSS-SITE SCRIPTING			
0	941150	Cross-Site Scripting (XSS) Attempt: XSS Filters - Category 5 Cross-Site Scripting (XSS) Attempt: XSS Filters - Category 5. HTML attributes - src, style and hed	 Block 		
		OWASP OWASP-2017 CR33 WASCTC PCI HTTP A3 A3-2017 X33 CR033-SITE SCRIPTING			
0	941101	Cross-Site Scripting (XSS) Attempt: SS Attack Detected via libinjection Cross-Site Scripting (XSS) Attampt: SS Attack Detected via libinjection	Block		
		OWASP OWASP-2017 CR83 WASCTC PCI HTTP A3 A3-2017 X88 CROSS-SITE SCRIPTING			
	941350	Cross-Site Scripting (XSS) Attempt: UTF-7 encoding XSS filter evasion for IE Cross-Site Scripting (XSS) Attempt: UTF-7 encoding XSS filter evasion for IE.	e Block		
9		OWASP OWASP-2017 CR53 WASCTC PCI HTTP A3 A3-2017 X55 CROSS-SITE SCRIPTING			

Figure 2. The security profile involves proxying traffic to establish a baseline, tuning, and moving into block mode.

Tightly Integrated into the Oracle

The OCI WAF leverages other capabilities available within OCI, including auditing of changes to WAF policies and granular access controls. OCI WAF telemetry is sent to the monitoring service for reporting and alerting. Tagging can be applied to WAF policies, just like compute, storage, DNS, and all other services for cost tracking and search.

= MBAD CRACUE				(A land	🕛 (Ö. socialitere), 🔫			
	WAP Policy Name: and Primary Dumain: amag	JavaScript Challenge	tate cance	t .				
200000	Additional Domains: //	Manage the settings that	detect and fitter abnormal and malicious bot traffic.					
ACTIVE	COID:NOn.gs	ENABLE JAVASCRIPT	CHALLENGE ()					
	CNAME Target: amas?	JS CHALLENGE ACTION	0					
	Data Greatest: Dec 20,	O DETECT ONLY	I matching execution and black on Sething action.					
		BLOCK						
		Block all matched requi	ats and return the specified response code, error page or CAPTCHA.					
WAF Policy	Bot Manage	SET HEADER FOR FA	LED REQUEST (i)					
		ACTION THRESHOLD ()						
Overview	JavaScript Challenge	10	Requests					
Orgin Management	JavaScript Challen	Due to the asynchronous in usage, and 100 for appe with	equest from the browser during page loading. It's recommended to set a threshold of 10 for web applications with basic ajas th heavy ajas usage.					
Bettings	Enable Javaforget Dha	ACTION EXPIRE TIME ()						
Protection Rules		60	Seconds					
Access Canton	O Alter of FOCE	Due to client IP address ch	anges, it's recommended that the expiry time is set to 120 seconds for apps with mobile users and 3600 seconds for apps	is insulat				
But Management		with desicop users only						
Logi				accegorin comeccora mon	cal crest are not craterigou.			
Unsublated Charges		Save Cancel						
Terra of Max and Private Council Private	Ration .							

Figure 3. Each type of vulnerability ruleset is shown within the OCI Control Center, with granular controls for each specific rule.

Protect Against Threats Identified by OWASP

Oracle WAF protects against a host of threats, including those identified by OWASP as the most serious threats facing web applications today. Oracle WAF provides rulesets to protect against each threat, and the Oracle Cloud Infrastructure management console includes granular controls for each specific rule. Some of the biggest threats identified by OWASP include:

- Injections (SQL, LDAP, OS, etc.)
- Broken Authentication and Session Management
- Cross-site Scripting
- Insecure Direct
 Object References
- Sensitive Data Exposure
- Missing Function Level Access Control



Figure 4. Set Access Rules.

Whitelisiting and Bot Blocking

Oracle WAF uses several techniques to detect and block bad blocks while allowing desirable bot and human traffic to pass through. These include JavaScript challenges and CAPTCHA challenges. Users can also whitelist certain traffic and easily customize the parameters of the challenges.

User Access Controls

User access controls enable organizations to restrict and control access to critical web applications and services. For example, regional access controls can be used to restrict users from certain geographies. Users can also restrict access based on HTTP header information and other characteristics.

Multicloud Support

In addition to providing WAF protection for Oracle Cloud Infrastructure workloads, Oracle WAF also protects onpremises, hybrid cloud, and multicloud environments.

Application Program Interface (API) support

Oracle WAF provides a RESTful API, software development kit, and Terraform support for easy integration into existing management and monitoring systems.

Oracle WAF is also supported 24/7 through Oracle's support services. Behind the scenes the Oracle WAF is kept up to date and supported by a team of security experts.

Industry-Leading Expertise

Oracle provides 24/7 security operations centers with global researchers and analysis capabilities.

Key takeaways

Oracle WAF is a cloud-based, PCI-compliant, global security service that protects applications from malicious and unwanted internet traffic. Oracle WAF can protect any internet-facing endpoint, providing consistent rule enforcement across a customer's applications.

Learn more at:

https://cloud.oracle.com/edge

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/oracle

facebook.com/oracle



Integrated Cloud Applications & Platform Services

Copyright © 2019, Oracle and/or its affiliates. All rights reserved. This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

This device has not been authorized as required by the rules of the Federal Communications Commission. This device is not, and may not be, offered for sale or lease, or sold or leased, until authorization is obtained

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group. 1020



