ORACLE®

Cloud Infrastructure

Oracle Cloud Infrastucture Web Application Firewall

Challenges

Web application security is a growing concern for enterprises. A significant portion of all cyberattacks are directed at web applications, and that rate is increasing.

Factors such as the rise of cloud computing, use of open source technologies, the increase in data processing requirements, complexity of web applications, and an increase in the overall sophistication of attackers has led to an extremely challenging environment for IT security leadership.

When a breach occurs, it could often have been prevented. However, security budgets are not keeping up. Information technology leaders struggle to keep pace with innovation and the growing costs of breach mitigation, prevention, post-breach remediation, and cleanup.

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 cloud-based 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 Cloud Infrastructure Web Application Firewall: Cloud-Based, Globally Distributed Network

Well-intended security controls often end up becoming an enterprise security choke point when cyberattackers can make use of global networks and continuously change their threat locations.

Eventually, cybercriminals overwhelm or breach an organization's perimeter-only defenses. A global security platform is needed to extend enterprise defenses. Organizations must embrace globally scalable and distributed solutions as a starting point to thwart attacks.

The Oracle Cloud Infrastructure (OCI) Web Application Firewall (WAF) is an enterprise-grade, cloud-based, globally deployed security solution, designed to address today's web application challenges. The OCI WAF provides a suite of security services that uses a layered approach to protect web applications against cyberattacks.

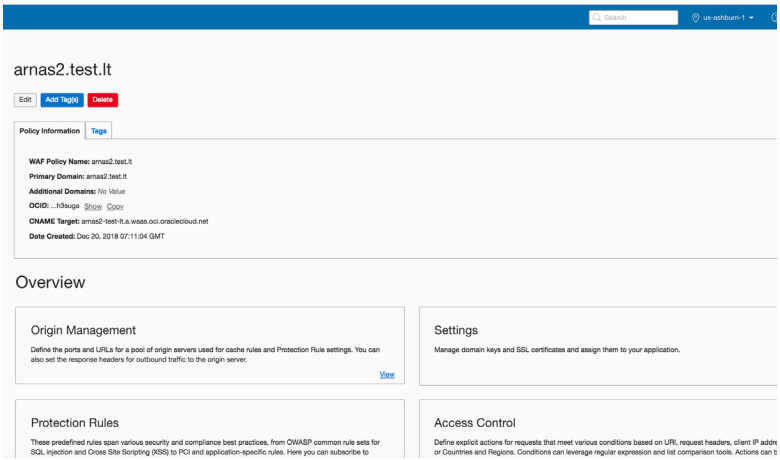
What the OCI WAF Provides

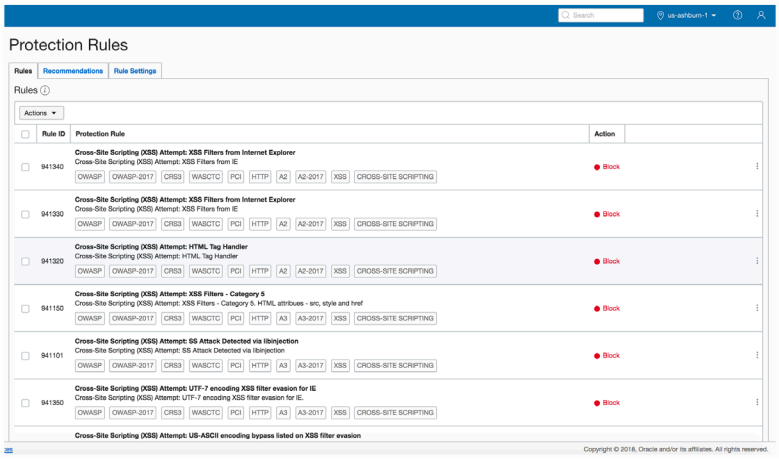
The OCI WAF is an enterprise-grade, cloud-based, globally deployed security solution designed to protect business-critical web applications from malicious cyberattacks. The OCI WAF provides a suite of security services that uses a layered approach to protect web applications against cyberattacks. This 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 OCI WAF network architecture creates a protective shield serving as the security perimeter for HTTP, adding a critical layer of web application and API protection.

All traffic flows through the OCI WAF network prior to arriving at your application server. This allows the OCI WAF to inspect the traffic and compare it to defined rules and parameters. Configured as a reverse proxy, the OCI Web Application Firewall inspects all traffic destined to your web application origin and identifies and blocks all malicious traffic. The WAF provides a custom security profile for each web application under protection, based on more than 250 rules. Developing the security profile involves proxying traffic to establish a baseline, tuning, and moving into block mode.





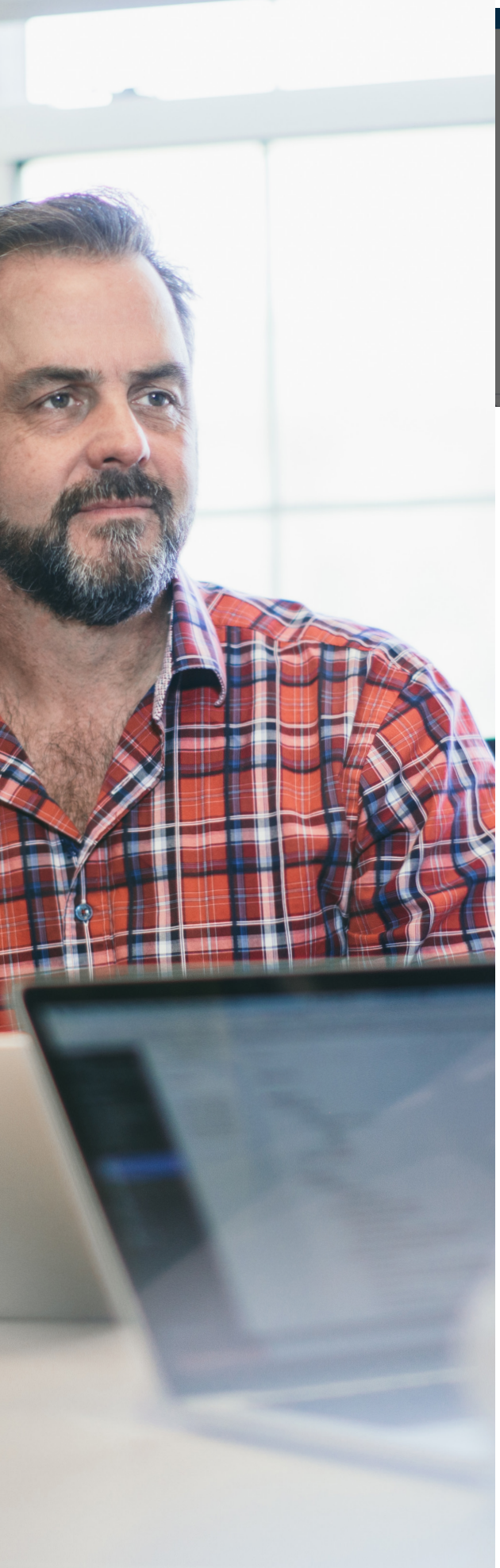
Key OCI WAF Components

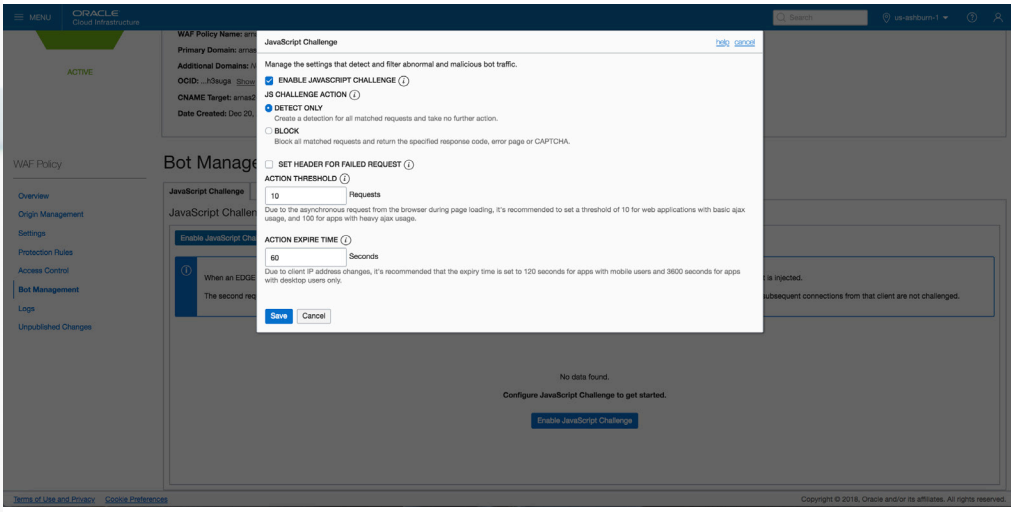
The technical functions that are critical to deliver robust and effective security services are:

- Tightly integrated into the OCI console for tight control and ease of use for your OCI setup
- Supports over 250 rulesets, as well as the OWASP rulesets to protect against SQL injection, cross-site scripting, HTML injection, and many more threats
- JavaScript Challenge, CAPTCHA Challenge, and whitelisiting capabilities work in conjunction with rulesets to further detect and mitigate bad bots and allow access to legitimate human and bot traffic
- User access controls can be configured on the basis of countries, IP addresses, URLs, and other request attributes to prohibit risky traffic
- Multicloud support provides WAF protection for any internet-facing application. OCI WAF can protect workloads in any environment: OCI, on-premises, and across hybrid or multicloud deployments
- OCI WAF has API, SDK, and Terraform support for every operation and can be orchestrated with other OCI services
- 24/7 security operations centers with global researchers and analysis capabilities

Tightly Integrated into the Oracle Cloud Infrastructure Console

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.





What kinds of rulesets does OCI WAF support?

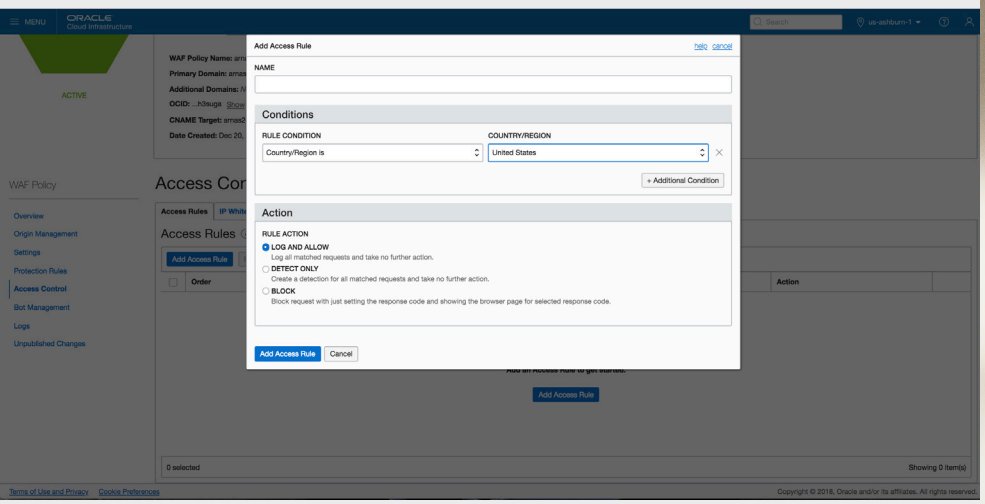
The WAF's rulesets protect critical web applications from cyberattacks and malicious actors. These rules are compared against incoming requests to determine if the request contains an attack payload. If it's determined that a request is an attack, the WAF will then block or send an alert about that request. These attacks are many and varied and include threats such as: SQL injection, cross-site scripting, HTML injection and many more—all of which can be detected and blocked by the OCI WAF rulesets.

Top OWASP 10 vulnerability groups include:

- A1 – Injections (SQL, LDAP, OS, etc.)
- A2 – Broken Authentication and Session Management
- A3 – Cross-site Scripting (XSS)
- A4 – Insecure Direct Object References
- A6 – Sensitive Data Exposure
- A7 – Missing Function-Level Access Control

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

Each client can create custom rules. We work with clients to create unique rules during the onboarding process. OCI includes the capability to create custom rules, both for all applications and at any time that custom rules are required by the web application.



Challenges and whitelisiting capabilities

Use the additional JavaScript challenge, CAPTCHA challenge, and whitelisting capabilities in conjunction with the WAF rulesets to further detect and block bad bots while allowing good bots through. Customize challenge parameters, such as number of failed attempts, expiration times, messages and more. Pick and choose which bots you want to deny and allow using bot whitelisting.

JavaScript Challenge: After receiving an HTTP request, a piece of JavaScript is sent back to the browser of every client, attacker, and real user. It instructs the browser to perform an action. Legitimate browsers will pass the challenge without the user's knowledge, while bots—which are typically not equipped with JavaScript—will fail and be blocked. This is a fast and efficient way to block a large percentage of bot attacks.

CAPTCHA Challenge: If a specific URL should be accessed only by a human, you can control it with CAPTCHA protection. You can customize the comments for the CAPTCHA Challenge for each url.

Whitelisting: Allows you to manage which IP addresses appear on the IP whitelist. Requests from the whitelisted IP addresses bypass all challenges, such as DDoS policies and WAF rulesets.

User Access Controls

Use the access controls to restrict or control access to your critical web applications, data and services. As an example, regionally-based access aligns to GDPR compliance requirements. In some cases, an offering may need to stay within a specific country. Regional access control can be used to restrict users from certain geographies. For instance, you may not do business with countries located in Asia, so you can completely block access from these countries.

- Control access, based on HTTP header information. Block requests if the HTTP header contains specific names or values or allow traffic with proper HTTP regular expression.
- Control access based on URL address matching or partial matching or match proper URL regular expressions.

Multicloud Support

Many cloud providers restrict their WAF protection to applications that reside within their own clouds. This is not the case with the OCI WAF. In addition to providing WAF protection for OCI workloads the OCI WAF will also protect on-premises and multicloud environments. Having this single OCI WAF to protect your workloads in any environment is extremely important as you move to OCI. This will provide protection for your entire environment and each phase of your OCI migration that includes cloud testing, migration, and ramp-up.

API Support for Integration

If you are an OCI customer, partner, or managed service provider who wants to integrate the OCI WAF directly into your existing management system or SIEM, WAF logs can be consumed via RESTful APIs. The log format is easy to parse and rich with request metadata. Future releases will make log files available in OCI buckets.

Industry-Leading Expertise

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

ORACLE
Cloud Infrastructure

Oracle Cloud Infrastructure is an enterprise infrastructure-as-a-service (IaaS) platform. Companies of all sizes rely on Oracle Cloud to run enterprise and cloud-native applications with mission-critical performance and core-to-edge security. By running both traditional and new workloads on a comprehensive cloud that includes compute, storage, networking, database, and containers, Oracle Cloud Infrastructure can dramatically increase operational efficiency and lower total cost of ownership. For more information, visit cloud.oracle.com/iaas.