Web Application Firewall

Protect your business with enterprise-grade web application security that scales with you.

Whether you're connecting with customers, employees or third-party suppliers, your organization needs to remain available and online at all times. Web Application Firewall (WAF) helps you accomplish that by protecting your website and apps from sophisticated attacks, including cross-site scripting (XSS), SQL injection (SQLi) and large-scale distributed denial of service (DDoS). WAF adds to your defenses while limiting complexity.

43%

Percentage of breaches involving web app attacks[1]

Challenges

The size of DDoS attacks is growing.
The largest DDoS attack on record was 2.3 Tbps of concurrent traffic, recorded in early 2020.[2] Most companies don't plan for or have the security measures in place to defend against this size of attack. And this record is likely to be broken. No matter how sophisticated your security assets are, you need large-scale protection to guard your organization.

Whack-a-mole
In 2019, an average of 33 new vulnerabilities were announced each day.[3] Not knowing you've been breached can have a severe impact on your ability to operate. On average, it takes 279 days to identify and contain a data breach, with the average cost to a business of $3.92 million.[4]

Limited security budget
Threats are pervasive, and they are increasing in frequency and impact. Protecting your web apps from the growing number of sophisticated threats, including DDoS, is a significant task. But not protecting them risks significant damage to your reputation, customer loyalty and your company's value.

Benefits of WAF

High-capacity global network
With 115 Tbps of global network capacity, we protect your business from the largest DDoS attacks. And with more than 160+ points of presence connected to 5,000+ interconnects around the world, we block attacks at the edge, before they can damage your infrastructure and your reputation.

Enterprise-grade web app security
We keep your apps protected against the most sophisticated multilayered attacks. WAF includes rulesets, HTTP rate limiting and real-time analytics, which empowers you to respond instantly to security events, increasing uptime and user loyalty, and preserving capital.

Cost-effective security
Our comprehensive WAF offering is designed to protect your web applications against a variety of dangers, including Open Web Application Security Project® (OWASP) Top 10 threats, multilayered attacks and the largest DDoS attacks.

Features

Dual Web Application Firewall
Employ current security rules and test new ones at the same time. WAF includes our unique Dual WAF, which enables security operations teams to experiment with new rules against production traffic in alert mode. Fine-tuning occurs before promotion to block mode. This system provides predictability when pushing changes to production environments, minimizing risk, downtime and delays associated with a lack of information.

Instant configuration
WAF deploys updated configurations within seconds. Feel confident knowing that your security team can roll back changes and push out updates within a few minutes, making security trials much more impactful and effective. Being able to test protection solutions minimizes downtime resulting from accidents or incorrect configurations.

verizon✓
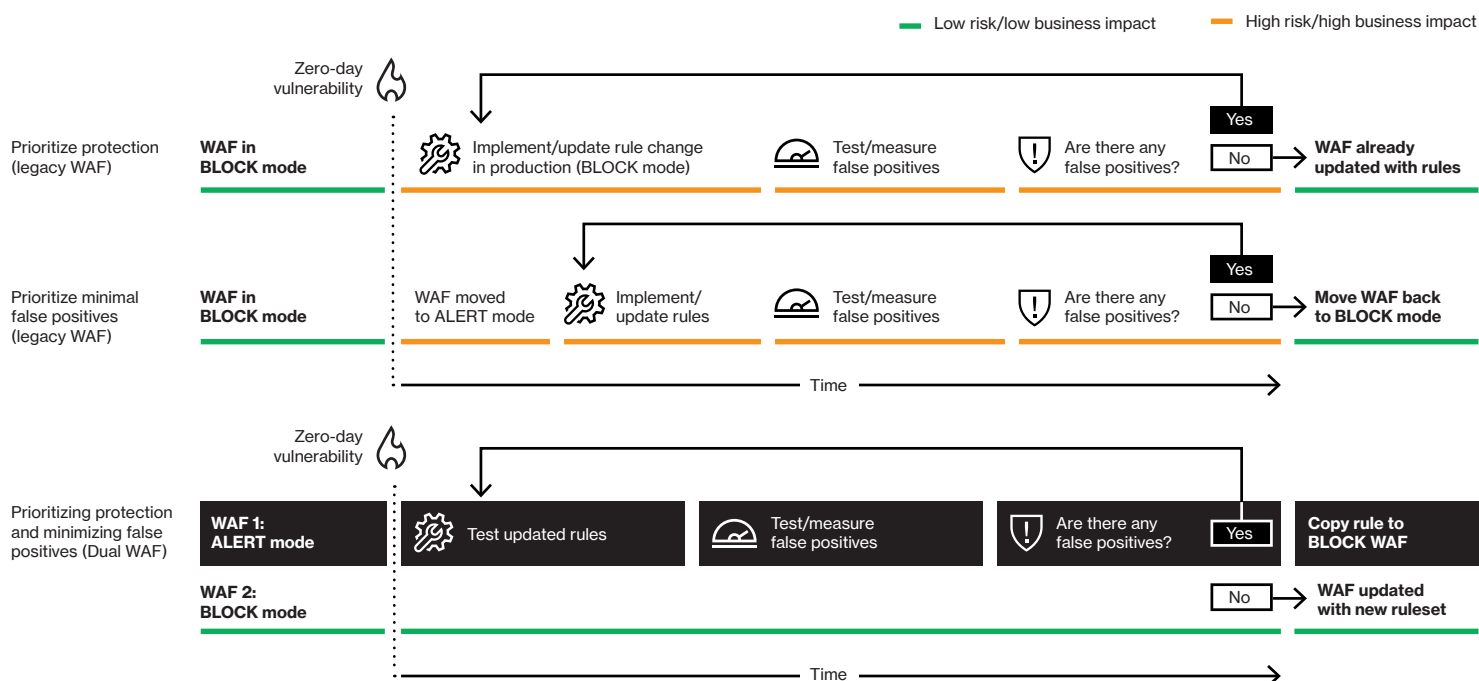
Dual Web Application Firewall

HTTP rate limiting
Enable security teams to elegantly deal with automated attacks. In addition to traditional Layer 3 and 4 DDoS protection, WAF includes HTTP rate limiting, which protects your website against Layer 7 HTTP flood attacks. With faster, configurable propagation, more accurate targeting and a flexible penalty box that allows for temporarily adding the device or bot to a deny list of threats based on URL, you can keep bad traffic out while allowing good traffic on to your site.

Global DDoS protection
Our massive globally distributed delivery network with more than 160+ points of presence absorbs attacks where they occur at the edge, freeing up your server resources to handle legitimate traffic. With over 115 Tbps of global network capacity, you'll protect your application layer, web forms and application programming interfaces (APIs) so that you can

remain online for business continuity. WAF can be combined with Verizon DDoS Shield service to ensure the most comprehensive DDoS protection, including attack detection, alerting, and granular visibility and reporting.

Get the security you need.

Web Application Firewall can help protect your online presence and data transactions to help keep your sites, content and users' data secure. Find out more ⟩

verizon✓

1 *Verizon 2020 Data Breach Investigations Report*.
2 "AWS Hit With a Record 2.3 Tbps DDoS Attack," *Computer Business Review*, June 13, 2002. https://www.cbronline.com/news/record-ddos-attack-aws
3 Browse Vulnerabilities by Date, CVE Details. https://www.cvedetails.com/browse-by-date.php
4 *Cost of a Data Breach Report 2019*, IBM Security. https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/