WEBSCALE

DATASHEET

Webscale Cloud WAF

Powerful Protection for Ecommerce Applications

Cyber-attacks are an unfortunate reality of the ecommerce industry. Common cyber-attacks on ecommerce sites include account takeovers, hijacked gift cards, DDoS attacks, credit card theft, phishing, and malware. These attacks, and the cybercriminals perpetrating them, are becoming smarter and more sophisticated.

Cybercrime doesn't just involve stealing data, it can also be used to impact the uptime of vital systems by breaching the system through sophisticated malware or by targeting the application layer. The most sophisticated hackers today are no longer looking for open ports or launching massive DDoS attacks; instead, attacks are becoming more frequent at the application layer where most of the customer information resides.

The damage that cyber-attacks can have on an online storefront's brand, reputation, and revenue, is catastrophic. They can cause an immediate loss of user loyalty, especially if the user is directly affected by the attack. The need for advanced security to protect digital storefronts, and users identities and credit card data, is higher than ever before.

There are many different web application firewall (WAF) solutions in the market today, ranging from free to very expensive, appliance-based to SaaS, and low to high-throughput. For mid-sized and large digital commerce businesses, most of these 'front door'-type solutions prove inadequate as sophisticated cybercriminals use automation and 'back doors' to execute attacks at scale.

Webscale Cloud WAF

Webscale Cloud WAF is a SaaS-based, application-aware, programmable web application firewall (WAF) that delivers 360-degree web application security by securing transactions from the browser, to the Webscale data plane and deep into the application infrastructure, and gets rid of the need for expensive "edge" solutions. This includes monitoring and analysis through machine learning, detection, mitigation, and ongoing protection, enabling always-on security with application-aware, customized rules to protect against sophisticated attacks. The deployment is a combination of a decentralized control plane and a distributed data plane that "fronts" application traffic, and real-time backend monitoring and control that protects the application infrastructure (or origin).

Product Benefits

Application Awareness

Webscale Cloud WAF is the only WAF designed with application awareness, including specific optimizations for ecommerce and enterprise web applications. Each application may have different security needs and the ability to apply custom security policies is critical for application owners and IT. Webscale enables pre-defined security rule-sets based on the application.

SaaS Delivery Model

Webscale Cloud WAF is simple to deploy and easy to manage via an intuitive customer portal. Offering significant ROI benefits over hardware and software-based deployments, Webscale delivers a true SaaS solution, always future-proofed with new security rules and software updates automatically applied across our entire customer base instantly.

OWASP Top 10 Protection

Webscale Cloud WAF automatically protects critical web applications from the most common vulnerabilities, such as SQL Injections, Cross Site Scripting (XSS), Cross Site Request Forgery (CSRF), and other OWASP top 10 threats.

SecOps

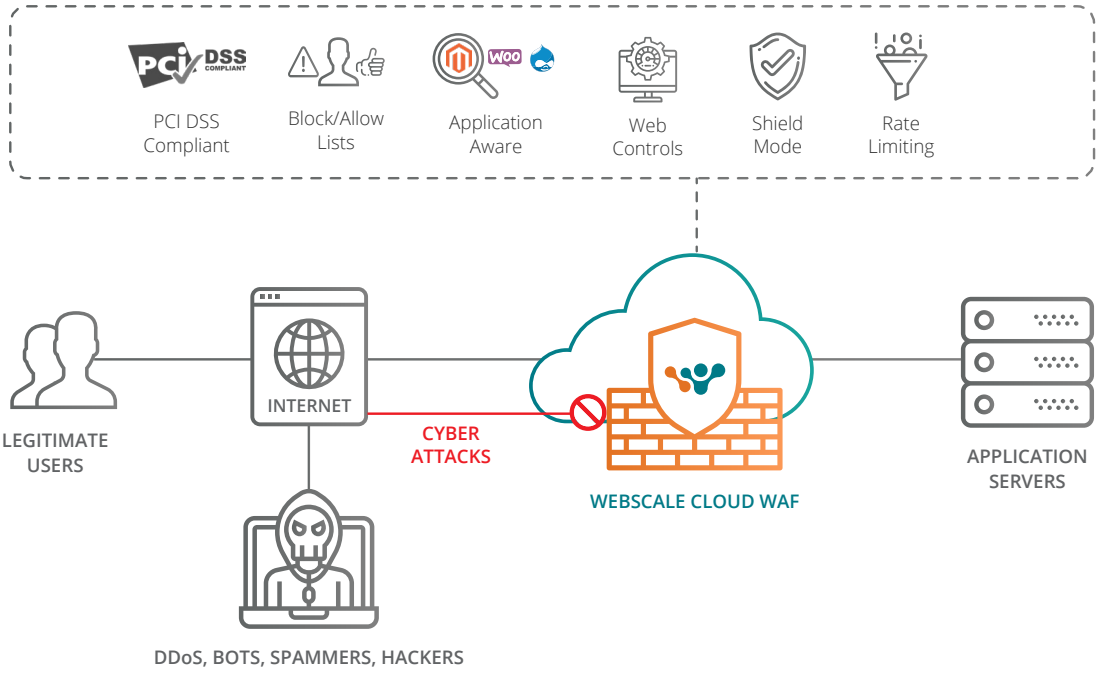
Webscale's multi-cloud-certified SecOps team delivers world-class incident management and monitors customer site security around the clock, providing customers with a fully managed security experience.

Block / Allow Listing

Webscale Cloud WAF also has standard capabilities such as block/allow listing, and geo-blocking. These features offers superior flexibility to block or allow requests and sessions by IP address, user agent, or the user's origin country. Webscale allows merchants to block known bad actors permanently, or even entire geographical regions that merchants are not serving, while building a trusted model that only allows authorized personnel to access the most secure parts of the application (such as admin sites).

Web Controls

Webscale's Web Controls enable site administrators to use pre-defined, pre-tested security rulesets based on their ecommerce application, minimizing the need to discover, define, and maintain the rules themselves. With Web Controls, site administrators can also create the equivalent of firewall rules, without having a deep technical understanding of how to build them. They have been designed to allow a user, of any skill set (technical as well as non-technical), to quickly take actions to ensure enterprise-grade security, high availability, and fast performance of their web applications.



DDoS Mitigation

Webscale identifies and blocks millions of attacks daily from all over the world, automatically learning from each new threat. Webscale's DDoS Shield Mode offers single-click protection when under a suspected Distributed Denial of Service (DDoS) attack or a flood of bots by instantly forcing a challenge that only humans can validate.

PCI Compliant

Webscale Cloud WAF is Level 1 Service Provider-grade PCI-DSS compliant, ensuring your web applications are adhering to the latest PCI security standards. With Webscale, you can quickly and easily protect your customers' sensitive data from external threats, without making any changes to your web application.

Bot Management

Webscale Cloud Bot Manager (available as an add-on) delivers advanced bot management capabilities, proactively identifying suspicious browsing and attack patterns, and mitigating malicious bots through reputation and machine learning techniques.
The unique combination of insight and management through Bot Manager, combined with the flexibility of Web Controls, allows for unprecedented security flexibility.

Key Features

SaaS Security Stack

Compliance: Level 1 PCI-DSS 3.1 service provider

Supported Web Protocols

- HTTP(S)
- HTTP/2

Protection against Common Attacks

- OWASP Top 10 protection

SSL/TLS Support and Termination

- Session encryption and authentication
- Support for TLS 1.2
- Auto-TLS – Automated procurement and renewal of certificate

Web Application Firewall

- Block / Allow Listing
- Geo-blocking
- Rate limiting
- Custom WAF rules

Unified Portal

- Real-time logging access to raw logs
- Customizable role-based administration
- Extensive monitoring, alerting and customer support

DDoS Attack Mitigation and Protection

- One-click Shield Mode

Web Access Control List

- Ability to block, suspend, allow
- Rate limit based on IP
- Restrict based on geography and user-agents

Dynamic Session Profiling

- Real-time session and traffic analysis
- Bot identification and control

Web Controls

- DIY custom policy and rules engine

Custom Rules Engine

- Application-specific rulesets (Magento, WordPress, WooCommerce and others)
- Compatible with ModSecurity

Cloud-native SaaS

- No hardware, software, installation, management, monitoring or additional costs