WEBSCALE

DATASHEET

Webscale Cloud Security Suite

360° Cloud Security from The World's Most Secure Cloud Platform for Ecommerce

The rapid growth of the ecommerce industry continues unabated, and while its popularity is turning many consumers into predominantly online shoppers, it is also making the segment an increasingly attractive target for cyber-criminals. From DDoS (Distributed Denial of Service) or cross site scripting attacks, to credit card skimmers, malware, and content scrapers, the modern ecommerce business merchant needs a strong, highly vigilant security posture that can identify these threats and automatically take the necessary action to prevent them from harming their business.

When cyber-attacks occur, the damage caused to a business can take many forms. It's not only about the where a breach could result in a loss of customer data, causing irreparable damage to a customer's trust and a brand's reputation.

Ecommerce storefronts with significant traffic and high average cart sizes especially, need a security solution adapted to their specific needs. Off-the-shelf WAFs (web application firewalls), and other "one-size-fits-all" security solutions simply don't cut it. Online businesses need a solution that is designed for their needs, offering robust protection for transactions all the way from the browser to deep within the application infrastructure.

Webscale Cloud Security Suite

Webscale Cloud Security Suite is a comprehensive security solution that provides the ecommerce industry's most robust protection against attacks from the frontend through web traffic, malicious code inserted into the backend, or browsers executing scripts stealing sensitive information. Websites protected by Cloud Security Suite have always-on, 360° security with application-aware, customized rules to protect against sophisticated attacks. In addition to a managed WAF, Cloud Security Suite includes a range of features that allow for real-time application monitoring and analysis through machine learning, detection, automated mitigation, and ongoing protection. Cloud Security Suite is available as an add-on to all Webscale Cloud Delivery plans.

Product Benefits

Bot Management

Webscale Cloud Security Suite delivers real-time bot monitoring, detection and management capabilities. It proactively identifies suspicious browsing and attack patterns, and mitigates malicious bots through IP 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.

Application Shield

Cyber-criminals will often attempt to circumvent the security layer provided by the firewall and direct their attacks at the application tier and database. Webscale Cloud Security Suite delivers an App Shield which locks down access to application infrastructure from any traffic not passing through the Webscale Data Plane.

Intrusion Detection

Zero-day attacks exploit known vulnerabilities, typically by inserting malicious files in the backend, before a patch can be applied. Webscale Intrusion Detection constantly monitors and detects any unexpected code and asset changes to application infrastructure, alerts in real-time, and automatically quarantines “infected” servers and/or keeps out malicious agents from infecting the site.

DDoS Mitigation

Webscale Cloud Security Suite identifies and blocks millions of attacks daily from all over the world, automatically learning from each new threat. When under a suspected DDoS attack or a flood of bots, Webscale’s DDoS Shield Mode offers single-click protection by instantly forcing the application to only allow humans in, keeping the bad bots out, so the application can function normally, while Webscale identifies the attacker more precisely.

PCI Compliance

Webscale Cloud Security Suite’s 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.

OWASP Top 10 Protection

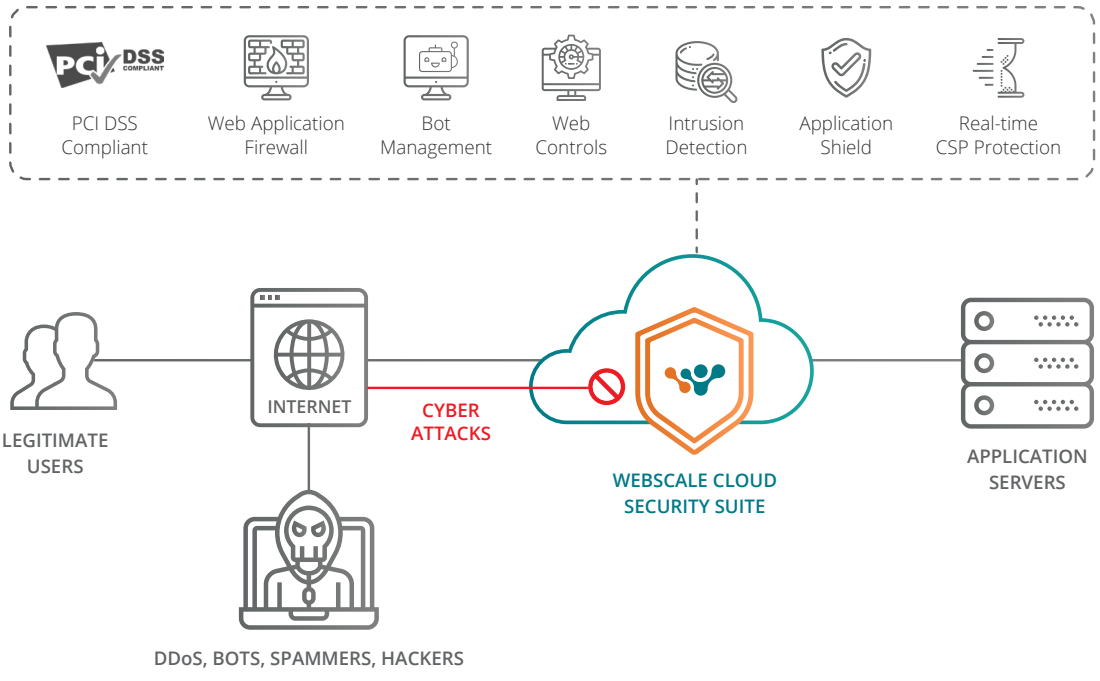
Webscale Cloud Security Suite automatically protects critical web applications from the most common vulnerabilities, such as SQL Injections, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), and other OWASP Top 10 threats.

Web Controls

Webscale's Web Controls consist of a DIY policy and rules engine that allows a user, of any skill set (technical as well as non-technical), to quickly take action to ensure enterprise-grade security, high availability, and fast performance of their web applications. Webscale enables 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, with no limits on how many Web Controls can be enabled at any point in time.

Real-time CSP Protection

Webscale Cloud Security Suite extends security beyond traffic and application infrastructure, to the browser, because mailicious third-party scripts can be executed at this level. Content Security Policy (CSP) is a HTTP security standard introduced to prevent XSS (cross-site scripting) attacks. Our real-time CSP protection enhances trust between the browser and application server by validating "trusted" domains executing scripts, and blocks or reports any non-whitelisted domains executing scripts on the browser.



Key Features

Webscale Cloud 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

Programmable Web Application Firewall

- Block and Allow by IP address, User Agent
- Geo-blocking
- Rate Limiting
- Built in/bring your own rulesets

Real-time CSP Protection

- Report-only mode and validate domains executing scripts
- Block any non-allow-listed domains from executing scripts on browser

Intrusion Detection

- Automatically detect file changes
- Malware scanners identify malware insertions
- Quarantine, self-heal and block access to suspect or blocklisted file changes

App Shield

- App Shield "locks" access to application infrastructure
- Only Webscale data plane can allow traffic through to infrastructure

Unified Portal

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

Bot Management

- Attack detection techniques
  - IP reputation-based filtering
  - User agent based identification
  - Good bot validation
  - Behavioral analysis based on machine learning
- Bot classification
  - IP reputation – dynamic database of ~10M dangerous IPs
  - Address Sets – identify trusted sources and block certain threats
- Real-time Bot Mitigation
  - Bad bots blocked proactively
  - Drop requests / Delay responses
  - Limit suspicious sessions (Rate Limiting)
  - Suspect bots given human challenge
  - Scrapers sent to an alternate backend
- Real-time Traffic Viewer
- Dynamic Site Cache
  - Serves good bot traffic through cache

DDoS Attack Mitigation and Protection

- One-click DDoS Shield Mode

Web Access Control List

- Ability to block, suspend, allow
- Rate Limiting 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 engine

Custom Rules Engine

- Application-specific rulesets (Magento Open Source, SAP Hybris, Wordpress, WooCommerce and others)
- Compatible with ModSecurity
- "Bring your own ruleset"

Cloud-native SaaS

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