WEBSCALE

DATASHEET

Webscale CloudEDGE Security

Enterprise-grade Cloud Security for Any Ecommerce Platform

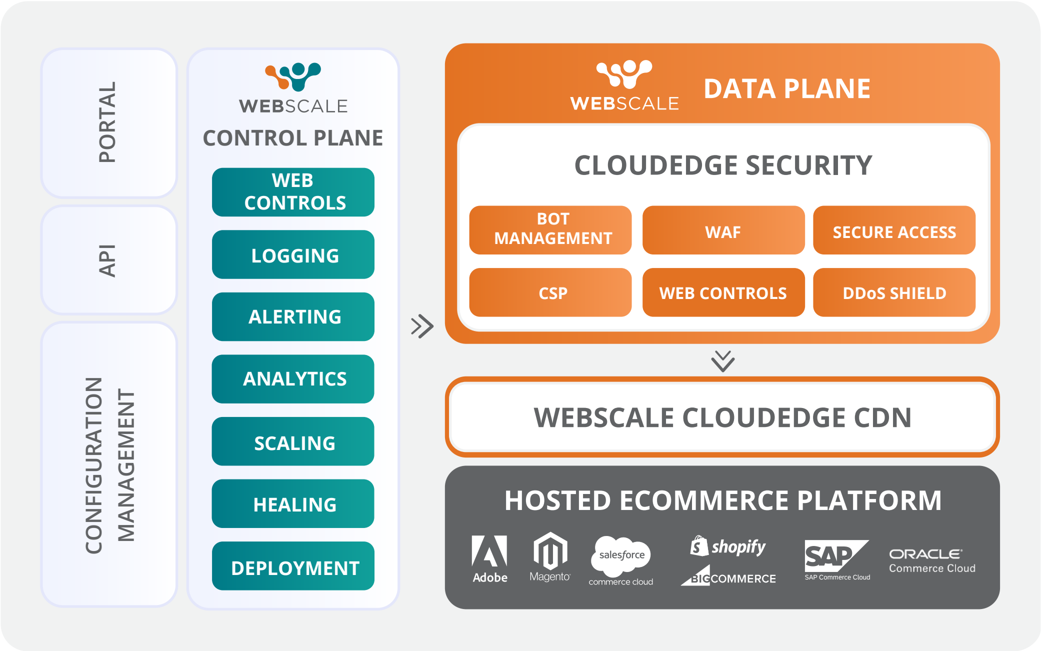
The massive growth experienced by the ecommerce segment in recent years has made it a prime target for cyber-criminals. From DDoS (Distributed Denial of Service) or cross-site scripting attacks, to credit card skimmers, malware, and content scrapers, the modern ecommerce business merchant needs a strong, highly vigilant security posture that can identify these threats, and automatically take the necessary action to prevent them from harming their business.

While merchants on self-hosted ecommerce platforms, such as Magento Open Source, WooCommerce, or SAP Hybris, have the freedom to select best-in-class security solutions, those on hosted platforms such as Adobe Commerce, Shopify or Salesforce Commerce Cloud, are limited to bundled WAFs and CDNs that lack the same breadth of features. Furthermore, if additional functionality is required, merchants are often forced to purchase premium services from pre-selected providers that are rarely the most cost-effective. The limited capabilities of these bundled solutions can seriously impact the effectiveness of a website's security, exposing storefronts and brands to high levels of risk. Ecommerce merchants, on any platform, need an advanced security solution that addresses these gaps, and effectively predicts and prevents the latest emerging security threats. These solutions must also have the ability to support design and infrastructure flexibility across hosted platforms and headless deployments, as well as on-premise web sites and applications.

Webscale CloudEDGE Security

Webscale CloudEDGE Security takes Webscale's award-winning security platform and deploys it at the traffic edge, alongside traditional CDNs and WAFs, and on top of any third party hosted ecommerce platform. This highly customizable and scalable solution, purpose-built for the ecommerce segment, uses automation and analytics to proactively identify and protect web applications from the front end through web traffic, malicious code, or from browsers executing scripts to steal sensitive information. In addition to a managed WAF, CloudEDGE Security includes a range of features that allow analysis through machine learning, detection, automated mitigation, and ongoing protection.

Key changes in the ecommerce industry are having a significant impact on hosting and infrastructure design decisions, particularly with regards to the level of integration of backend systems. Merchants want to enable seamless omnichannel experiences, which means delivering fast, secure storefronts with easy shipping and payment options. As a result, merchants are evaluating fully hosted commerce clouds, managed cloud hosting providers, and headless deployments that leverage APIs to connect a variety of backend systems. Webscale CloudEDGE Security supports all deployment models, while delivering improvements in end to end security, performance and infrastructure visibility.



Webscale sits alongside any WAF and CDN, and on top of any hosted ecommerce platform

Product Features

Programmable Cloud WAF

Webscale's programmable Cloud WAF uses a decentralized, software-defined web application delivery architecture, to monitor user traffic and application infrastructure in real-time, enabling always-on security with application-aware, customized rules to protect against sophisticated attacks.

Bot Management

Webscale CloudEDGE Security 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 CloudEDGE Bot Manager, combined with the flexibility of Web Controls, allows for unprecedented insight and security.

Real-time CSP Protection

Webscale CloudEDGE Security extends security beyond traffic and application infrastructure, to the browser level, where malicious third-party scripts can be executed. 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-allow-listed domains executing scripts on the browser.

Site Splice

With advanced features such as Site Splice and Site Cache, agencies and developers can easily route device-specific and functional needs to the appropriate services dynamically, and in turn, cache the responses, making application development and user experience faster and without third party bottlenecks.

PCI Compliance

Webscale is a PCI-DSS Level 1 Service Provider. We work with our customers to ensure their web applications are maintaining robust security policies, at all times, and adhering to the latest PCI security standards.

Web Controls

Webscale’s Web Controls is a DIY policy and rules engine that allows a user, of any skill set, to quickly take actions 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, as well as sequences of these rules capable of performing complex tasks such as dynamic whitelisting, or rate-limiting checkout attempts based on user behavior. There are no limits on how many Web Controls can be enabled at any point in time.

DDoS Mitigation

Webscale CloudEDGE Security 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 allow access to humans only, so the application can function normally, while the attacker is identified.

OWASP Top 10 Protection

Webscale CloudEDGE Security 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.

Product Benefits

Protect the Application from Unwanted Traffic

Prevent cyber criminals from circumventing the firewall and directing their attacks at the application tier and database with Webscale App Shield, which locks down access to application infrastructure from any traffic not approved by the Webscale data plane.

Activate DDoS Protection with a Single Click

Webscale's DDoS Shield Mode offers single-click protection by instantly forcing the application to grant access only to humans while the DevSecOps team works hard to identify the root cause, assuring peace of mind without overhead.

OWASP Top 10 Threats

CloudEDGE Security 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 emerging OWASP Top 10 threats.

Enhance Trust Between Browser and Application

CloudEDGE Security extends security beyond traffic and application infrastructure to the browser, where real-time CSP protection validates "trusted" domains, and prevents blocked domains from executing scripts on the browser.

Detect and Mitigate Bad Bots in Real-time

CloudEDGE Security offers real-time bot monitoring, detection and management capabilities. Proactively identify suspicious browsing and attack patterns, and mitigate malicious bots through IP reputation and machine learning.

Ensure PCI-DSS Compliance

Webscale CloudEDGE Security's WAF is Level 1 Service Provider-grade PCI-DSS compliant. With Webscale, you can quickly and easily protect your customers' sensitive data from external threats, without making any changes to your web application.

Unmatched Observability and Control

Webscale's Web Controls allow a user, of any skill set, to quickly take action to ensure enterprise-grade security of their web applications. Site administrators or Webscale's teams can create the equivalent of firewall rules, with no limits.

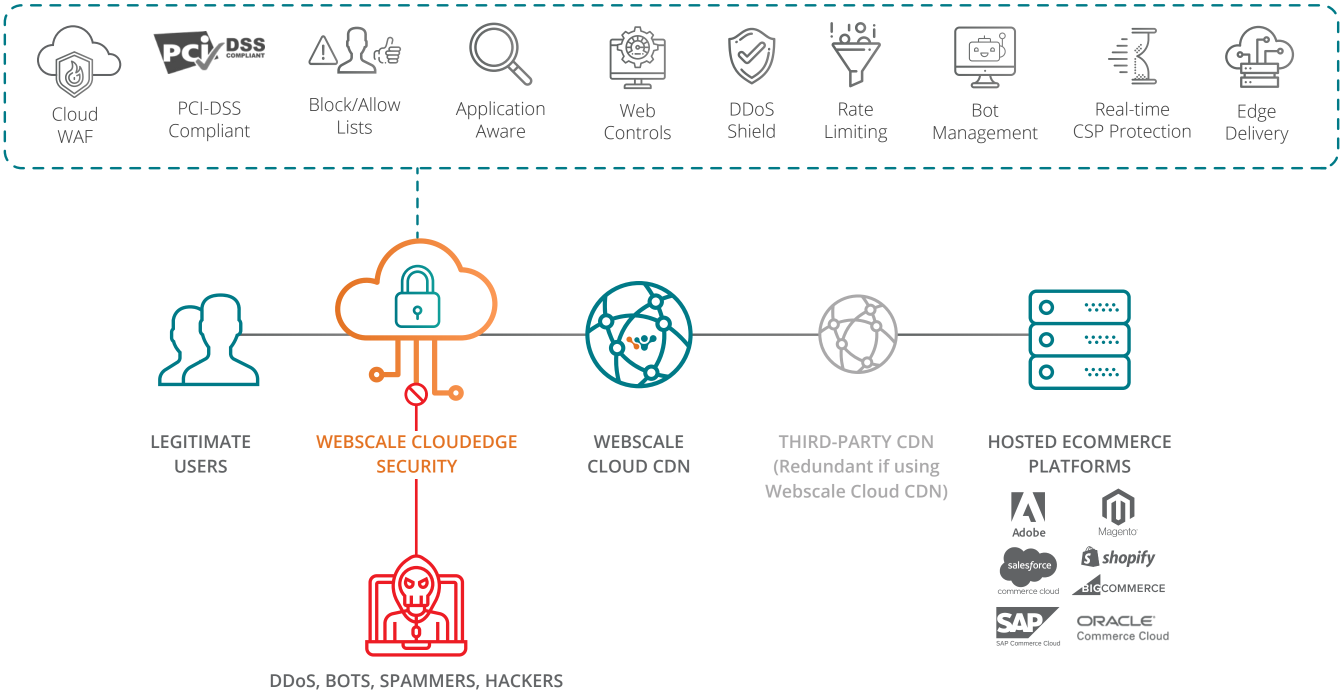
Programmable Cloud WAF

Webscale's programmable WAF uses a decentralized, software-defined web application delivery architecture, to monitor traffic and infrastructure in real-time, enabling always-on security with application-aware, customized rules to protect against attacks.

How It Works

Deployed on top of any ecommerce platform and alongside, or as a replacement for, traditional CDNs and WAFs, CloudEDGE Security uses automation and analytics to proactively identify and protect web applications from SQL injections, cross-site scripting (XSS), server side request forgery (SSRF) and other sophisticated attacks.

CloudEDGE Security is loaded with advanced features to offer bullet-proof security. In addition to a managed Cloud WAF, it includes Bot Manager, App Shield, DDoS Shield, and real-time CSP Protection, all enabled through Web Controls, a DIY policy and rules engine inside the Webscale Portal.



Technical Specifications

Webscale CloudEDGE Security Stack

Supported Web Protocols

- HTTP(S)
- HTTP/2

SSL/TLS Support and Termination

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

Programmable Web Application Firewall

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

Protection Against Common Attacks

- OWASP Top 10 protection

Real-time CSP Protection

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

Web Controls

- DIY custom policy and rules engine to deploy the equivalent of firewall rules or user defined rules
- No limit to number of rules or their complexity in terms of user behavior or traffic

Others

- No hardware, software, installation, management, monitoring or additional costs
- Real-time logging access to raw logs
- Customizable role-based administration
- Custom Templates
- Extensive monitoring, alerting and customer support
- Unified Portal

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

Custom Rules Engine

- Application-specific rulesets
- Compatible with ModSecurity
- “Bring your own ruleset”