WEBSCALE

SOLUTION BRIEF

Webscale CloudEDGE Security

Powerful, Fully-Managed Security. Built for Ecommerce.

60% of online shoppers won't buy from a company that has had a data breach in the past 12 months. 24% of cyberattacks target retail and the industry witnesses more breaches than any other sector. These two statistics together underline why ecommerce businesses need powerful security.

Today's high traffic ecommerce sites need a comprehensive security solution that goes beyond traditional, basic WAFs, and implements a robust 360-degree security cover that has been built to address the specific needs of the segment – identify complex and evolving threats, and automatically take the necessary action to prevent them from harming the business. It's the reason we created Webscale CloudEDGE Security.

Webscale CloudEDGE Security

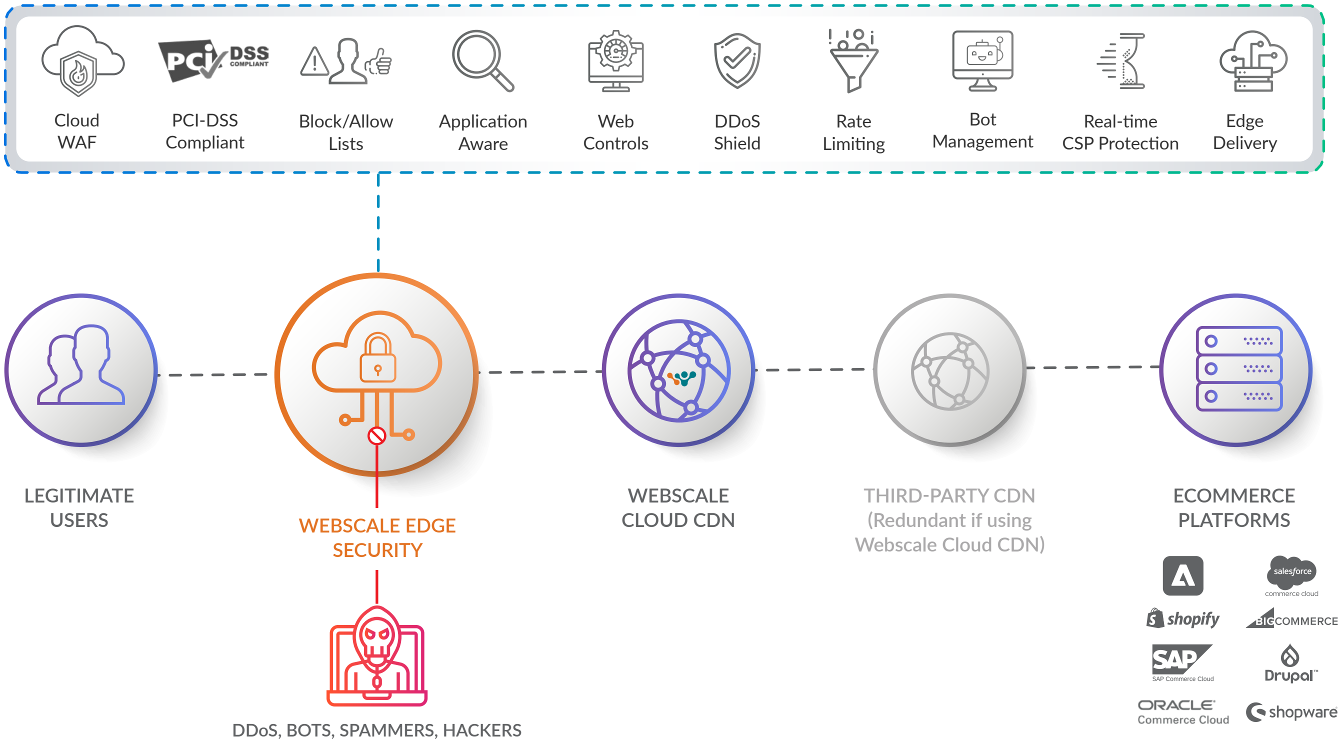
Enterprise-grade security from the origin to the edge

Webscale CloudEDGE Security is a fully-managed security suite, deployable alongside any CDN or WAF, and on top of any ecommerce platform. Leveraging deep analytics and automation, CloudEDGE Security proactively identifies sophisticated threats to modern commerce platforms – form jacking (Magecart), bots & scrapers and access breaches to carding and DDoS attacks, injection (SQL and XSS) and server-side request forgery (SSRF) – and implements the necessary controls to mitigate them before they impact your business.

How Does It Work?

Available in two plans, **Self-Managed** and **Fully-Managed**, CloudEDGE Security is deployed on top of any ecommerce platform including headless, composable and PWA environments and alongside, or as a replacement for, traditional CDNs, WAFs and other point security solutions. Merchants on fully-managed plans work alongside our DevSecOps team of ecommerce security specialists to identify and resolve any threats.

Websites protected by CloudEDGE Security have always-on security with application-aware, customized rules to protect against sophisticated attacks. In addition to a managed WAF, CloudEDGE Security includes a range of features that allow for real-time application monitoring and analysis through machine learning, fraud detection, automated mitigation, and ongoing protection.



> Would happily recommend Webscale to any ecommerce business. Their innovative security solution keeps our customers safe by proactively monitoring, detecting and defending against any attacks.

KADOKAWA AMARIN

Benefits

Protect the application from unwanted traffic

Prevent cyber criminals from circumventing the firewall and attacking the application tier and database. App Shield locks down access to the application infrastructure from any traffic not approved by the Webscale data plane.

Activate DDoS Protection with a single click

DDoS Shield Mode offers single-click protection by instantly forcing the application to grant access to real users only, while the DevSecOps team identifies the root cause.

Unmatched visibility and control

Web Controls enable site admins to use pre-defined, pre-tested security rulesets based on their ecommerce application, or create their own, minimizing the need to discover, define, and maintain the rules themselves.

Detect and mitigate bad bots in real-time

Real-time bot monitoring proactively identifies suspicious browsing and attack patterns, mitigating malicious bots through IP reputation and machine learning techniques.

Stay secure against OWASP Top 10 threats

Webscale 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.

Enhance trust between browser and application

Critical for preventing MageCart and similar attacks, our real-time Content Security Policy (CSP) protection extends security beyond traffic and application infrastructure, to the browser. There it identifies, in real-time, any script violation from a pre-established policy, and reports (or prevents) the malicious script so that administrators can take immediate action to protect the website.

Maintain PCI-DSS compliance

Webscale is a PCI-DSS Level 1 Service Provider, ensuring our customers' web applications are maintaining robust security policies, at all times, and adhering to the latest PCI security standards. Webscale also offers SOC2 and HIPAA compliance.

> We have been very impressed with the security and support offered by Webscale, which is far in advance of anything we have received before.

Tricker's

Technical Specifications

Webscale CloudEDGE Security Stack

Supported Web Protocols

- HTTP(S)
- HTTP/2
- Auto-HTTPS
  - Automatically obtains and renews certificates

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
  - Basic
  - Advanced
- Built in/bring your own rulesets

Protection Against Common Attacks

- OWASP Top 10 protection
- Origin Protection (App Shield)
  - Level 1: Server addresses are hidden behind the data plane.
  - Level 2: Security Group is managed by the control plane to allow only the proxies to connect to application servers.
  - Level 3: App servers are completely isolated from the internet, behind a dedicated data plane on the same private network as your app servers

DDoS Attack Mitigation and Protection

- One-click DDoS Shield Mode

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
- Multi-Factor Authentication
- 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
- Data Loss Prevention

Web Access Control

- Ability to block, suspend, allow
- Rate Limiting based on IP
  - Restrict based on geography and user-agents
- Secure Access
  - Role based permissions for sections of your application to protect access from the general internet.
- Trusted Proxies
  - Registration of trusted 3rd party proxies accessing the Webscale data plane

Real-time CSP Protection

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

Dynamic Session Profiling

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

Custom Rules Engine

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