

360-DEGREE WEB APPLICATION SECURITY

Webscale offers a converged and comprehensive multi-cloud security platform that enables web applications across any vertical to be protected against a wide range of cyber attacks, from exploits using web traffic to those that target the backend infrastructure.

Like any of the other products in its portfolio, Webscale's security solutions are delivered as a true cloud-based software as-a-service (SaaS), with a simple subscription plan. It enables any web application (HTTP/HTTPS) to be hosted and secured in a cloud environment, with no hardware, software or cloud instance to deploy, configure and maintain.

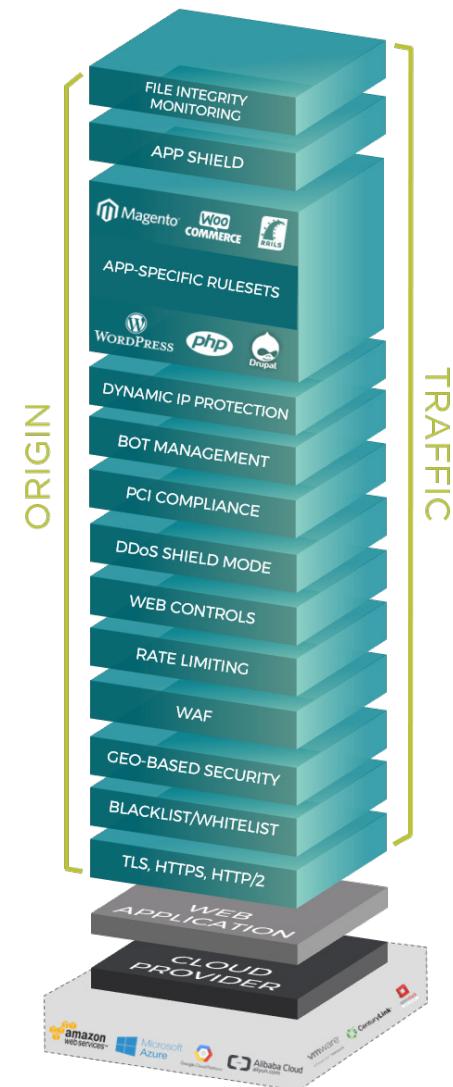
WEBSCALE ENTERPRISE CLOUD SECURE

Traditional hardware and cloud security solutions target traffic-based attacks. Other monitoring solutions exist that provide analytics around application infrastructure. Webscale Enterprise Cloud Secure is automatically deployed in close proximity to the application infrastructure, giving it deep insight into web traffic accessing the application as well as application events. It is this combination of that enables complete protection for web applications, not just from traffic accessing the application but also from exploits targeting the backend file systems and databases.

A SOLUTION STACK FOR ALL LEVELS OF SECURITY

Webscale is the industry's first multi-cloud SaaS providing a comprehensive security solution stack that offers 360-degree protection for an application. The security stack is built on a foundational layer that provides the latest standards of PCI compliance and TLS security, ensuring all web requests pass through security checkpoints. In addition, a programmable web application firewall (WAF) "fronts" the application, pre-built with application-specific rule-sets to build a base security capability against known targeted threats; additionally, custom rule-sets can deliver further protection against threats that may be unique to the customer environment.

Access control mechanisms like Blacklisting and Whitelisting allow administrators to easily block (or allow) specific requesters based on IP address, user agent or geography. The Web Controls feature adds a DIY, custom policy engine that makes it easy to configure complex security policies with easy to use interface and API options.





With an inbuilt attack shield, DDoS attacks used to bring down a web application can be easily prevented with a single-click, by identifying and only allowing humans to access applications.

In addition to protection against traffic, Webscale Enterprise Cloud Secure constantly monitors the backend infrastructure in real-time to ensure illegitimate traffic cannot bypass Webscale, access the application and make changes to the file structure. It alerts on any unexpected file or content changes in the application infrastructure, with the ability to automatically prevent access and execution of such changes within the application. Finally, the Webscale 24x7 SecOps team constantly monitors security feeds and addressing any known web application vulnerabilities, by applying virtual patches to applications as soon as they are identified, and distributing these learnings across all Webscale managed applications.

PRODUCT HIGHLIGHTS



DDoS Mitigation

Distributed Denial of service (DDoS) attacks are targeted, sophisticated attacks generated from multiple disparate sources with no immediate identifiable patterns, that are intended to inundate or bring down the application. Webscale's **DDoS Shield Mode** is a single-click protection when under a DDoS attack, that instantly keeps all bots away by forcing a challenge that only humans can validate.



Application Shielding

Any attacker who knows the application server IPs, which are public-addressable, can bypass a WAF and send traffic directly to the application servers. **Webscale App Shield**, when enabled, ensures the backend infrastructure only accepts traffic from the Webscale data plane and rejects all other requests. This enhances the end-end security across data traffic and the application backend.



Webscale Dynamic IP Protection

Many cyber attacks come from well-known bad bots identifiable by their IP addresses. Such attacks unnecessarily use up computational power, cause undue scaling of resources, increase costs, and more importantly expose the application to exploits that may cause irreparable damage to revenue and brand. **Webscale Dynamic IP Protection**, powered by the [WebRoot BrightCloud® IP Reputation Service](#), enables discovery of these bots, and other known threats, to permanently block them before they can access the application. Dynamic IP protection is programmable through Web Controls, and activated in real-time.



Backend Protection

Webscale Enterprise Cloud Secure, outside of focusing on traffic accessing the application, also protects the backend infrastructure. It integrates a **file integrity monitoring (FIM)** module that gets alerted on any changes to file and content. This is especially critical during zero-day exploits that start with the insertion of an executable in the backend. Once alerted, Webscale can take many actions including automatically blacklisting any traffic requesting the executable, quarantining servers that have suspect file changes and replacing them with pristine images.





WEBSCALE ENTERPRISE CLOUD SECURE	
COMPLIANCE	<ul style="list-style-type: none">• Level 1 PCI-DSS 3.2 service provider
SSL/TLS	<ul style="list-style-type: none">• HTTP/2, HTTP(S) protocols supported• Certificate lifecycle management – procurement, deployment and renewal• SSL/TLS Offload• TLS 1.1 support, TLS 1.2 (recommended)
WEB APPLICATION FIREWALL (WAF)	<ul style="list-style-type: none">• Ability to manage custom WAF rules• OWASP Top 10 Protection• Application-specific rule-sets: Magento, Wordpress, WooCommerce and more• Compatible with Modsecurity• Bot identification and control through WAF rules
DDOS MITIGATION AND PROTECTION	<ul style="list-style-type: none">• One-click Shield Mode
ACCESS CONTROL	<ul style="list-style-type: none">• Ability to block, suspend, allow• Rate limit sessions based on IP• Restrict based on geography and user-agents
TRAFFIC ANALYTICS	<ul style="list-style-type: none">• Powerful real-time monitoring of traffic with graphs and searchable log data• Custom filters for granular threat detection• Export Log data to multiple formats
WEB CONTROLS	<ul style="list-style-type: none">• Simple DIY custom policy engine
APP SHIELD	<ul style="list-style-type: none">• Restricts traffic from bypassing Webscale and accessing the application directly
BACKEND PROTECTION	<ul style="list-style-type: none">• Active File Integrity Monitoring of backend infrastructure changes• Automated quarantining and replacement of affected servers• Security incident creation for administrators
IP REPUTATION BASED PROTECTION	<ul style="list-style-type: none">• Real-time Bad Bot protection• Powered by Webroot BrightCloud® IP Reputation Service

ABOUT WEBSCALE

Webscale is the E-Commerce Cloud company. We are the only multi-cloud solution that enables e-commerce businesses to rapidly migrate their storefronts to the cloud, enabling 100% uptime at peak demand. The E-Commerce Cloud platform delivers enhanced visibility and control over web applications, as well as improved security, performance and user experience, designed to help e-commerce businesses focus on building their brands, not managing their infrastructure. The world's leading experts in cloud technology and e-commerce platforms, Webscale keeps users loyal and engaged by delivering a fast, reliable and secure web presence. Webscale has offices in Silicon Valley, CA, Boulder, CO and Bangalore, India.

