Web Application Firewall

Enhanced Application Security to Protect Your Web Applications

BLOCKDOS
Your Business, Our Protection

Most organizations today rely on mission critical applications which contain sensitive information their clients, business activities and corporate data. They know application security is essential but they usually don't have the time, financial resources or necessary experience to manage complex tools and customized rulesets which traditional application security suites provide. Our cloud-based Web Application Firewall (WAF) contains a perfect solution for these organizations. With intuitive management interface, detailed statistics, threat map, DNS panel and encryption settings, Blockdos WAF is extremely user friendly. It's a managed service which protects your web infrastructure from application layer attacks including zero-day vulnerabilities and OWASP top 10 threats. It cost effectively makes you fulfill 100% PCI compliance by adhering to PCI DSS 2.0 and 3.0 requirements. With more than 2.9 million requests per second, our WAF is identifying and blocking every potential threat. The combined intelligence propagates throughout our entire network, so if a threat is identified and blocked in our US Point of Presence (PoP), the same threat will be blocked in our UAE PoP or any other access point in the world.

Prevent Downtime, Data Theft and Defacement

Blockdos global WAF network is able to process more than 2.9 million requests every second. This enables Blockdos to continually identify and block new potential threats and even zero day vulnerabilities. The best part about our WAF is automatic updates. Our system is able to mitigate majority of the threats on the network by applying patches and automatically updating whenever new vulnerability is discovered anywhere. This is especially helpful for large-scale businesses since propagation of patches is instantaneous thereby covering their entire digital infrastructure rapidly. We have dealt with quite a lot of zero-day vulnerabilities for more than a decade. Our advanced security system empowers us to track state-of-the-art hacking techniques and make sure you focus on growing your business.

A robust rules engine to customize to your needs

Our WAF runs ModSecurity rule sets out of the box, protecting you against the most critical web application security flaws as identified by OWASP. It can also handle your existing rule sets and custom rules. Rules become effective in under 30 seconds.

Benefits to your Business

- **Drastically reduce the risk** of website defacement, downtime and data theft.
- **Cut down operational overhead** associated with application maintenance.
- **Reduce costs** associated with frustrated customers and regulatory fines.
- **Reduce expenditure** on expensive security software and hardware.
- **Improve Customer Satisfaction** while thwarting complex attack vectors.

Technical Benefits

- **Intuitive interface** equals to rapid deployment and configuration
- **Reduce time** to setup and configure the WAF
- **Built-in protection** against OWASP top 10 vulnerabilities
- **Minimize false positives** through automatic rule deployments
- **Expand your security features on-demand** through custom rule sets and policies.

Web Application Firewall

Key features	Benefit
Security	
Deep Packet Inspection, covering applications / Layer 7	Ensures your standard and custom web applications are always protected from SQL injection, cross-site scripting attacks and thousands more
SSL	Terminate SSL connections without any overhead or additional latency. Apply your WAF policy to SSL encrypted traffic without having to upload certificates or invest in costly hardware solutions.
For GET and POST HTTP/S requests	Covers range of HTTP/S traffic
URL-specific custom rule sets	Allows you to include/exclude specific URLs or subdomains for WAF protection to test domains or include/ exclude specific subdomains
DDoS mitigation integration	Allows full-stack protection against DDoS — no extra implementation required
IP reputation database integration	Real-time intelligence on over 1 billion unique IPs used to block malicious traffic — no extra implementation required
Virtual patching	Fixes a vulnerability before you patch your server or update your code, allowing you more time to patch and test updates.
Restrict by IP or geolocation	Can blacklist/whitelist traffic from specific IP addresses or countries to protect against hackers from specific IPs or countries
Low false positive	Overall 1/50M false positive rate ensures legitimate traffic reaches you
Full integration with CDN service, offering outbound content transformation	Reduces web latency for your site visitors — no extra implementation required
Rule Sets	
Automatic learning paired with security-driven research	Protects against zero-day vulnerabilities or new threats with patches automatically deployed by our security team
Compatibility with ModSecurity logic and format	Allows you to easily import existing rule sets to maintain existing protection
Core OWASP ModSecurity rule sets	Protects against OWASP vulnerabilities, the most critical flaws as identified by The Open Web Application Security Project (OWASP) — included as default with no extra fees
Zero-day BlockDOS rule sets	Rely on BlockDOS's security team to protect you against threats identified across our customer base — included as default with no extra fees
Platform-specific rule sets for major CMS and eCommerce platforms	Receive protection out of the box with no extra fees for platforms such as WordPress, Joomla, Plone, Drupal, Magneto, IIS, etc.
Custom rules	Cover situations unique to your web application included as default with no extra fees for Business and Enterprise customers

Web Application Firewall

WAF settings	
Block	Blocking an attack will stop any action before it is posted to your website.
Simulate	To test for false positives, set the WAF to Simulate mode, which will record the response to possible attacks without challenging or blocking.
Challenge	A challenge page asks visitors to submit a CAPTCHA to continue to your website.
Threshold / sensitivity setting	Set rules to trigger more or less depending on sensitivity
Customizable block pages	Customize the page a visitor sees when they're blocked, e.g. "Call this telephone number for help." Available for Enterprise customers.
Reporting	
Real-time logging	Gain visibility to help you fine-tune the WAF
Access to raw log files	Enterprise customers can conduct in-depth analysis covering all WAF requests
Administration	
High availability — built on service offering SLAs	Business and Enterprise customers enjoy 100% uptime guarantee and financial penalties if not met
No hardware, software or tuning required	Sign up with a simple change in DNS
PCI certification	BlockDOS's service has received Level 1 service provider certification

BLOCKDOS
Your Business, Our Protection

BlockDoS is a leading Canadian organization, established in 2005 as the most Secured Dedicated Hosting and Distributed Denial of Service (DDoS) Mitigation Service provider. We guarantee 99.9% uptime SLA on Enterprise Protection solution. Once your website is secured by BlockDoS, all the traffic will be routed through our global network of high-powered servers that inspect all incoming traffic, keeping hackers out while accelerating your traffic. BlockDoS delivers state of the art IT security solutions and excellence in business performance by ensuring a high level of security of the IT services; delivering a cost effective and sustained level of security that is aligned with needs of our clients; and developing and maintaining high levels of confidentiality, integrity and availability.