

Web Firewall

Protect your websites, applications, APIs, and more from the Internet's worst vulnerabilities, threats, and attacks worldwide.

Websites are about attracting traffic, yet without a web application firewall both good and malicious visitors have access. With the average website being attacked 62 times per day, the chances of a threat compromising your unprotected site is inevitable. Sectigo Web Firewall protects websites and web applications from cyberthreats and harmful traffic, like cybercriminals, bad bots and DDoS attacks.

MITIGATE ATTACKS

Sectigo Firewall protects websites against all levels of DDoS threats by automatically differentiating between legitimate website visitors and automated or malicious visitors, ensuring your customers can reach your website even when under attack.

SECURITY, SPEED AND SIMPLICITY

Designed to require zero-touch configuration, and to continue getting smarter as it is used. Traffic is constantly analyzed to profile behavior, detect inconsistencies, and determine reputation, leveraging advanced intelligence algorithms and expert security analysts.

WEB FIREWALL COMPATIBILITY

Works with all popular content management systems (CMS)



WEB FIREWALL BENEFITS

- ✓ Blocks targeted attacks
- ✓ Prevents search engine blacklisting
- ✓ Helps prevent zero-day exploits and other website threats
- ✓ Enables high volumes of traffic with zero lag time
- ✓ Simplifies PCI Compliance
- ✓ Provides fully secure end-to-end encryption for SSL
- ✓ Improves SEO ranking

GLOBAL PROACTIVE PROTECTION

Sectigo Web Firewall (WAF) protects your website from data breaches, malicious traffic and harmful requests, including the OWASP Top 10. It evaluates your website's traffic and only allows good traffic to enter your site, such as customers and search engines, while blocking the bad traffic, like spam bots and hackers. Every attack is analyzed and profiled making our WAF smarter and even more secure from emerging threats.



OWASP TOP 10 PROTECTION

- Policies protecting against the top ten security threats identified by the Open Web Application Security Project active by default.

BAD BOT PROTECTION

- State-of-the-art detection technologies, including device fingerprinting, protects against automated traffic with an unparalleled level of precision and control.

BACKDOOR ACCESS PROTECTION

- Online bad actors are continuously attempting to take control of your site. Sectigo Firewall technology identifies backdoor files and blocks an attacker's access to them, giving control back to the website owner.

BRAND REPUTATION MONITORING

- Sectigo Firewall's ability to block attacks seeking to exploit the OWASP Top 10, facilitates in protecting a website's brand reputation, prevent search engine blacklisting and providing a safe customer experience.

Product Package	Pro	Premium	Enterprise
CDN: Bandwidth Usage/month	100 GB	250 GB	250 GB
# of Sites	Unlimited	Unlimited	Unlimited
CDN Requests	Unlimited	Unlimited	Unlimited
PoPs Included	Global	Global	Global
Free Private SSL	Included	Included	Included
Upload custom SSL	Free	Free	Free
SSL Traffic Metering	Inclusive	Inclusive	Inclusive
DDoS Protection Coverage	Network Layer	Network Layer	Network Layer Application Layer
Cache Policies & Handling	User Controlled	User Controlled	User Controlled
WAF Requests/month	x	x	1M
Custom Rules	x	x	5 Rules
Integrated OWASP & CMS Policies	x	x	Included
Uptime SLA	99.99%	99.99%	99.99%
Origin Shield	Included	Included	Included
Additional CDN/WAF Package	Available for Purchase	Available for Purchase	Available for Purchase
<i>Suggested MSRP</i>	\$99 / year	\$199 / year	\$299 / year