NEXUSGUARD®
Global Leader in DDoS Mitigation

Web Application Firewall (WAF)

Bundled as an integral part of Application Protection (AP), Nexusguard Web Application Firewall (WAF) completes the DDoS mitigation platform by protecting web applications from attacks and exploits including those outlined by the Open Web Application Security Project (OWASP).

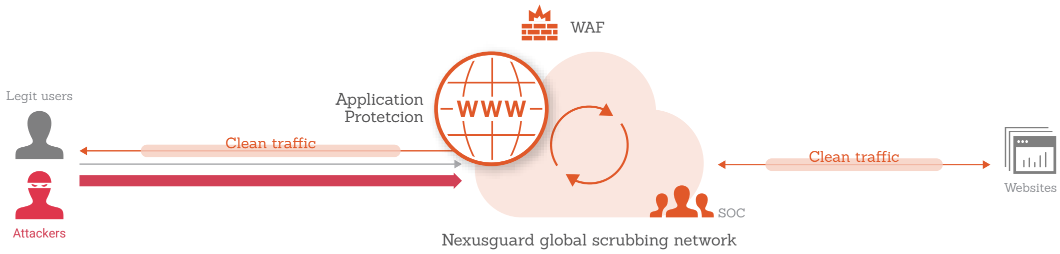
Deployed virtually through the cloud, Nexusguard WAF is centrally managed by the 24x7 SOC team and security experts. This way, we can leverage the collective intelligence of a diverse range of clients. It will also help us to constantly update the rule-set addressing latest threats and expanding its capacity whenever needed.

Nexusguard WAF also complies with the PCI DSS Requirement 6.6. This eliminates the need for investing in costly hardware necessary to meet this compliance requirement. These turn to be vital for banking and finance institutes or e-businesses that process credit card transactions on their website.

What is WAF?

WAF is deployed in the cloud to ensure maximum application security. It is centrally managed by our security experts 24x7 to rapidly detect and virtually patch vulnerabilities.

Being highly scalable and adaptive, Nexusguard WAF can block hacks or illegal intrusions that can exploit known vulnerabilities. It also prevents sensitive information leakage and controls when and where your applications are accessed by analyzing contents of HTTP/S traffic targeting applications.



nexusguard.com
contact@nexusguard.com

Who needs WAF?

Any site that has HTTP/S traffic served to the public is recommended to have a WAF setup in place. Having said that, banks, financial institutes, airlines or e-commerce businesses that process online credit card transactions and store sensitive customer information will find the Nexusguard WAF very cost-effective to meet the Payment Card Industry Data Security Standard (PCI DSS) requirements.

Specifically, the PCI DSS 6.6 Requirement stipulates that organizations must "verify that public-facing web applications are reviewed regularly using either manual or automated vulnerability assessment tools or methods". Meeting this requirement is not that easy, and that's where the Nexusguard WAF's value lies.

Why Nexusguard WAF?

Nexusguard is the worldwide leader in DDoS attack mitigation with a global scrubbing infrastructure and multi-layered defense—all built from the ground up for the sake of DDoS mitigation.

Key Features & Benefits

DDoS + Web Application Protection

- Nexusguard WAF complements the DDoS mitigation platform. Together they identify and mitigate alerts and threats on L7—especially if you have a dozen, hundreds or even thousands of applications.

Protection Against OWASP Top 10 - 2017 Vulnerabilities

- Our rule-set guards against the Top 10 threats identified by OWASP, including:
  - A1:2017-Injection
  - A2:2017-Broken Authentication
  - A3:2017-Sensitive Data Exposure
  - A4:2017-XML External Entities (XXE)
  - A5:2017-Broken Access Control
  - A6:2017-Security Misconfiguration
  - A7:2017-Cross-Site Scripting (XSS)
  - A8:2017-Insecure Deserialization
  - A9:2017-Using Components with Known Vulnerabilities
  - A10:2017-Insufficient Logging & Monitoring
- Simple, customizable and constantly updated WAF security policies and custom rules address specific security needs of your application. Our engineers can work with you to develop and refine site-/application-specific rules.

Easy Installation, Fast Deployment

- The cloud-based WAF can be deployed in minutes, supports SSL/TLS, requires no hardware and software, and incurs very low operational costs to maintain.

High Detection Rates, Low False Positives

- Nexusguard collects and analyzes threat intelligence from a large pool of clients using the WAF platform. The WAF central management helps achieve high detection rates against very low false positives.

Non-Intrusive Authentication

- Non-intrusive authentication challenges assess user behavior discreetly to identify and block malicious spammers, crawlers, hackers and bad bots and even those using malformed IP addresses.

Real-Time Reporting And Robust Logging

- Detailed security event logs and traffic summary information displayed on the Customer Portal allow your security team to gain visibility and insight into WAF and traffic analytics continuous monitoring, risk assessments and remediation paths.
- Detailed log is downloadable for every WAF event captured for post-attack analysis.
- Attack summary can also be provided to present statistics of events, site performance, other site analytics as well as detailed forensic information.

PCI DSS Compliance

- Integrating Nexusguard WAF ensures compliance with PCI DSS (requirement 6.6). It also complies with ISO27001.
- Cost-effective solution for achieving/maintaining PCI DSS compliance.
- Prevent sensitive data leakage, e.g. credit card data, customer information, customer login/password, etc.
- Hedge risks of commercial costs (i.e. legal costs, compensation, etc.) arising from failures in PCI DSS compliance audits.

24x7x365 SOC

- WAF events and attacks are monitored and handled by 24x7x365 Security Operations Center (SOC) staffed with security experts.

Maintain Search Engine Ranking & Avoid Blacklisting

- Nexusguard has patented search engine crawler identification technology that accurately segregates legitimate crawlers from spoofed or illicit ones
- Free from malware, so the site won't be blacklisted by search engines.

Low Total Cost Of Ownership (TCO)

- As a total cloud solution, Nexusguard WAF requires no hardware, software, operational and maintenance costs, nor does it need any rack space or electricity costs. No in-house WAF engineers are needed on the client side as well.