

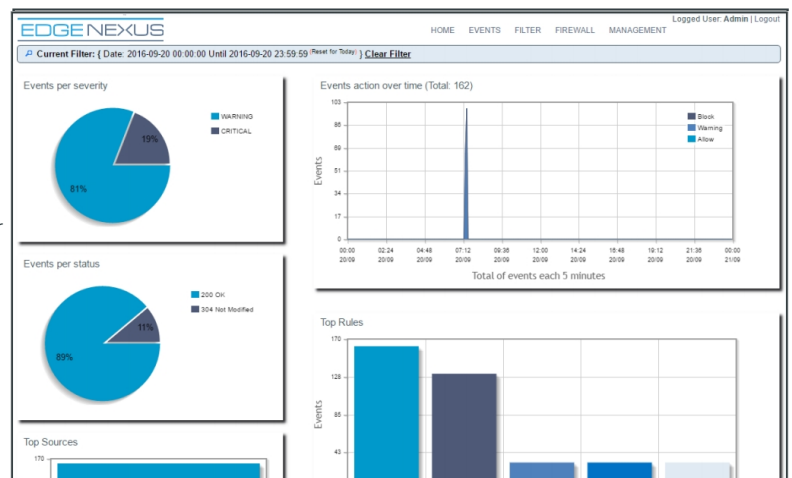
Web Application Firewall

Secure and Protect Against Application Vulnerabilities

The Edgenexus Application Firewall (WAF) Provides Layer 7 Security for Web Based Applications

Incorporating industry leading, hardened firewall technology, the Edgenexus WAF runs at the application layer to fill the security gap that traditional firewalls can fail to address.

- Eliminate application vulnerabilities
- Satisfy PCI-DSS and OWASP application firewall requirements
- Using containerisation technology to isolate each application firewall instance
- Can be used to run multiple applications or implement a multi-layered security architecture
- Fast and easy to deploy and configure
- Available for Edgenexus virtual, hardware and cloud load balancer deployments
- Free Trial Available [Here](#)



Protection Against These Attack Categories:

- Cross Site Scripting (XSS)
- SQL Injection
- DOS
- Session Hijacking
- Data Loss Prevention
- Local File Inclusion
- Remote File Execution
- HTTP Protocol Violations
- Shellshock
- Session Fixation
- Scanner Detection
- Metadata / Error Leakages
- Project Honey Pot Blacklist
- GEO IP Country Blocking

The screenshot displays the Edgenexus WAF configuration page with the following sections:

- Firewall Control:** Radio buttons for Disabled, Detection only (selected), and Detection and blocking.
- Requests Keep-Alive:** Radio buttons for Enabled and Disabled (selected).
- Logging:** Checkboxes for Store Local Logs (checked) and Store Remote Logs.
- Blocking Rules:** A list of rules including 960017 (Host header is a numeric IP address), 981203 (Inbound Anomaly Score), 981204 (Inbound Anomaly Score Exceeded), 981242 (Detects classic SQL injection), and 981318 (SQL Injection Attack).
- Whitelisted Rules:** An empty list for rules to be whitelisted.
- Manually add rule IDs to whitelist:** A text input field.
- Update configuration:** A button to save the changes.

Download a free trial of the Edgenexus WAF [here](#)

Web Application Firewall

Secure and Protect Against Application Vulnerabilities

Protection Against Cross Site Scripting, SQL Injection and Session Hijacking

The Edgenexus Application Firewall controls the input, output and access to and from an application by inspecting the HTTP conversation between the application and clients according to a set of rules.

These rules cover common attacks such as [cross-site scripting \(XSS\)](#), [SQL injection](#), [session hijacking](#) and buffer overflows which network firewalls and intrusion detection systems are often not capable of doing. The rules may be also used to enforce security policies required by PCI DSS or other security standards in order to block leakage of sensitive information like credit card numbers. By customising the rules to your application, many attacks can be identified and blocked. A Set of PCI DSS rules come as standard to the product.



Easy to Deploy, Simple to Manage

The Edgenexus Application Firewall is incredibly powerful yet simple to deploy and configure. Edgenexus utilises containerisation technology to isolate each application firewall instance. This can be used for running multiple applications, multi tenancy or implementing a multi-layered security architecture.

User Central

[Edgenexus User Central](#) is a one-stop knowledge base for everything edgenexus.

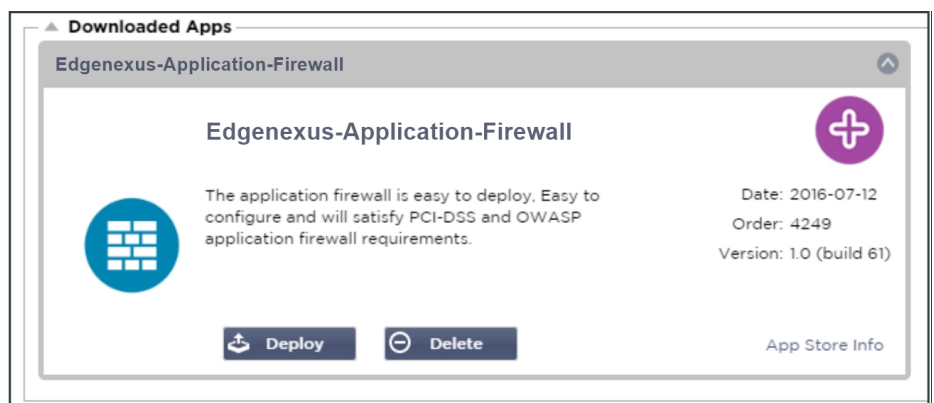
[WAF Free Trial](#)

[WAF User Guide](#)

[PCI DSS Compliance](#)

[OWASP Core Rule Set](#)

The Edgenexus Application Firewall is a virtual appliance (Isolated container) that protects Web applications by controlling the conversation between the application and clients.



Download a free trial of the Edgenexus WAF here