# Q-ModSec®

The **Q-ModSec**® (**ModSecurity**®,"**ModSec**") network appliance is a Web Application Firewall (WAF). The **Q-ModSec** provides real-time web application monitoring, logging, and access control so as to harden Apache and Nginx Web servers against attacks, and especially, but not exclusively, against cross-scripting attacks. Cross scripting is the most common, and most dangerous, form of attack used against Web Servers. Apache powers most of the Internet's web servers. Nginx servers are also explicitly supported.

The **Q-ModSec** network appliance performs as a Web Application Firewall (WAF) doing real time application security monitoring of all HTTP traffic, plus real time inspection. This is combined with a persistent storage mechanism built into **ModSec** to track system elements over time. In turn, this creates the ability to perform correlations over time in order to look for attack patterns.

**ModSec** allows selective blocking of elements so as to cut off potential attack paths. As part of its enhanced security, **ModSec** performs continuous passive security assessments. This is a form of real-time monitoring. Instead of focusing on the behavior of external actors (hackers), a role performed by Intrusion Detection Systems (IDS), the **Q-ModSec** focuses on the behavior of the web server itself. As a result of this internal focus, the **Q-ModSec** can detect abnormalities and security weaknesses before the web server is hacked.

In order to further harden web servers and web sites, the **Q-ModSec** can sharply narrow the list of allowed http behaviors, thereby creating a smaller attack surface and in turn, heighten security. E.G. HTTP request methods. Request headers. Content types. Etc. The **Q-ModSec** also provides restriction enforcement either directly, or via interaction with other Apache web modules. Using **ModSec**, it is possible to eliminate cross-site request forgery vulnerabilities as part of web application hardening.

In addition to web server hardening, the **Q-ModSec** can be used as an XML Web service router. The **Q-ModSec** parses XML, and can apply XPath expressions while proxying server requests, thereby performing as an XML router.

The **Q-ModSec** also includes the **WAF-FLE** Security Console. The **WAF-FLE** web interface allows admins to store, view, and search events using a graphical dashboard web gui. Events are gathered by sensors. There is no limit on the number of allowed sensors, allowing **WAF-FLE** to service very large numbers of web servers and/or web sites. The **WAF-FLE** web interface eliminates the need for any command line interface (CLI) skills.



*Contact:* Richard Avery
*646-449-7810*
*Q-ModSec@quantalytics.com*

***Quantalytics. In-depth network defenses.***

# Q-ModSec®


**Q-ModSec Hardware Specifications:**

- 108 mm x 64 mm x 26 mm – 170 grams (4.25" x 2.50" x 1.125" – 6 oz)
- Power consumption under full load: 8 watts, 120v-240v
- No fan or any moving parts. Must be installed in a well-ventilated space.
- Operates 0°C–70°C (32°F–158°F)

**LED indicators:**

- Power
- Link (physical connection to network)
- Activity (network traffic)
- 1000 mbps (gigabit) NIC connection
- Dual Band WiFi. (2.4 GHz & 5 GHz)

The **Q-ModSec** includes:

- **ModSecurity® - "ModSec"** (**ModSecurity®**) is an open source, real-time web application firewall (WAF) for monitoring, logging, and access control so as to harden Apache and Nginx Web servers against attacks. **ModSec** can also be used as a router for XML service requests through XPath and its built-in proxying of web server requests. We also use **ModSec** to harden this appliance's built-in Apache web server.

- **WAF-FLE – WAF-FLE** is an open source web interface console (gui) for ModSec. It allows admins to configure and deploy **ModSe**c sensors and then see and analyze the data, using a variety of built-in filters.

- **Webmin - Webmin** is used for network appliance housekeeping and network configuration.

- **HA Proxy – HA Proxy** is the leading open source package for automatic failover and load balancing. Up to 32 **Q-ModSec** servers may be linked for automatic failover or load balancing for coverage of extremely large networks. **HA Proxy** has a web gui for monitoring the load balancer and the servers it has been setup to use.



*Contact:* Richard Avery
*646-449-7810*
*Q-ModSec@quantalytics.com*

***Quantalytics. In-depth network defenses.***

- **Tiny Honeypot (THP) - THP** fools attackers by making it appear that the attack is working, while meanwhile logging the attack info. **THP** wastes an attacker's time, and creates an opportunity to detect the network intrusion by offering to the attacker what appears to be thousands of services.

- **ClamAv® – ClamAv®** is the leading open source anti-virus package.

- The **Q-ModSec** has both a Gigabit (1000 mbps) NIC and 802.11 Dual Band WiFi. (2.4 GHz and 5 GHz.)

The **Q-ModSec** is also available as a Virtual Machine.

Using the provided **Webmin** module, two-factor authentication can be added using **Google Authenticator** or **Authy**, a commercial service with its own app. **Google Authenticator** runs on Android, IOS, and Blackberry devices, and uses the standard TOTP protocol.

Notifications are provided by e-mail using **SendMail**, which is configured through a **Webmin** module, and syslog entries. The **Q-ModSec** is integrated with **Nagios®** on the **Q-Box®** as another notification route. SMS notification is available as an option. The **Q-ModSec** can also be integrated with the **Q-Log®** or any other Syslog or SIEM (Security Information and Event Management) solution.





*Contact:* Richard Avery
*646-449-7810*
*Q-ModSec@quantalytics.com*