Quantalytics

Q-Box®

The **Q-Box**® is an amalgamation of a number of open source software packages, listed below, running on an extremely small form factor, low-power-consumption server. The **Q-Box** provides system security through network device and services monitoring using **Nagios®**, and combines it with intrusion detection and prevention using **Snort®**. This creates in a single device what typically is provided with two 1U "pizza box" servers. This ultra compact design allows exceptionally flexible and creative deployment options as well as significant electricity and space savings.

Q-Box 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: 12 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-Box** includes:

- **Nagios®** – **Nagios®** is the leading open source, enterprise-class, network monitoring and alerting solution. The **Nagios** implementation includes **ModBus** over TCP monitoring and alerting for IoT devices supporting **ModBus**.

- **NagiosQL®** – **NagiosQL®** is a leading open source, enterprise-class, Web GUI configuration package for **Nagios**. **NagiosQL** also complements **Nagios** with a wide range of analytics and graphs, enabling network administrators to see problems literally at a glance.

- **Snort®** – **Snort®** is the leading open source, enterprise-class, network intrusion detection and prevention system (IDS/IPS). **Snort** is monitored through **Nagios**. Any Syslog or SIEM solution can also be used for monitoring.

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

Quantalytics. In-depth network defenses.

- **ntopng – ntopng** (“**ntop next generation**”) is the latest iteration of ntop, which is used to probe all network traffic. Some of its features include: show realtime network traffic and hosts; create long term reports for network throughput, application and application protocols; monitor and report live throughput, network and application latencies, RTT, and full TCP stats; discover application protocols (e.g. Facebook, BitTorrent, etc.) by leveraging nDPI (ntop Deep Packet Inspection); characterize HTTP traffic using characterization services provided by Google and HPPT Blacklist; provide geolocation mapping of hosts; sort all network traffic via criteria including IP address, port, L7 protocol, throughput, Autonomous Systems (ASs); analyze IP traffic and sort by source and destination; IPv6 support; full Layer 2 support, including ARP stats; and an alerts engine to capture anomalous and suspicious hosts.

- **ModSecurity® – ModSecurity®** (“**ModSec**”) is the leading open source Web Application Firewall (WAF) for cross-scripting attack protection. We have hardened the **Q-Box**’s built-in Apache web server to prevent conceivable attacks.

- **NMap – NMap** is the leading open source network mapping package for inventorying networks and security auditing.

- **Nagios Bulk Import (NBI) – NBI** is the leading open source package, which, when combined with **NMap**, automates the complete inventorying of network objects, including both network devices and services. **NBI** is accessed via **Webmin**.

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

- **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.

- **Webmin – Webmin** is the leading open source Web GUI package for server configuration and maintenance. **Webmin** also allows for the linkage of multiple **Q-Box** appliances for simplified administration.

- **HA Proxy** – **HA Proxy** is the leading open source package for automatic failover and load balancing. Up to 32 **Q-IDS** appliances may be linked for automatic failover or load balancing for coverage of extremely large networks. Configuration and administration are done through a web gui.

The **Q-Box** is completely administered through a Web GUI. All package usage is via Web interfaces, thereby opening up sophisticated intrusion detection, network forensic analysis, and network monitoring to even novice network administrators. No Command Line Interface (CLI) or Linux skill is required.

The **Q-Box** has both a Gigabit (1000 mbps) NIC and 802.11 Dual Band WiFi. (2.4 GHz and 5 GHz.) Intrusion detection can be set up on either network interface.

The **Q-Box** is also available as a Virtual Machine (VM).

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 with a module in **Webmin**, and syslog entries. **Snort®** has been integrated with **Nagios®** in the **Q-Box** as a notification route. SMS notification is available as an option. The **Q-Box** can also be integrated with the **Q-Log®** network appliance or any other Syslog or SIEM (Security Information and Event Management) solution.

Q-Box® *and all registered trademarks above are property of their respective owner(s).*