Richard Avery
Chief Marketing Officer
646.775.2761

Quantalytics Product Overview

Quantalytics® is a 30 years old network and systems integration firm that offers superior state of the art network security solutions. Our network appliances are built with some of the most powerful technologies available and are custom-designed to address the full range of IT, IoT or OT network cyber-security needs.

Our appliances offer small- to medium-sized customers the same enterprise protection as major organizations and Fortune 500 corporations for a fraction of what other manufacturers charge. All of our products are administrated through an easily used Graphical User Interface, so implementation and management are greatly simplified. This opens up information security to all levels of IT specialists.

To enhance affordability, Quantalytics appliances are subscription-based with a 2-year initial term. This includes all hardware, software, maintenance and upgrades. Unlike other manufacturers, we do not require any upfront capital expense ("CapEx") for hardware purchase.

Why is On-Premises Superior to Cloud Based Security?

If your Internet connection is lost for any reason, all cloud-based cyber security protection is also dropped. Having on-premises security systems and appliances eliminates this potentially major cyber security vulnerability. Your network is protected during blackouts using local appliances like **HoneyPots** that hide network assets by presenting thousands of decoys and **Network Access Controls** (NAC) that detect any unauthorized devices when connected. Both provide security for your network even when your network is not connected to the Internet.

Why use Open Source Software?

Open Source Software is favorable because it is continuously updated and improved by thousands of developers. The result is highly dependable, cost-effective applications. Unlike commercial applications, Open Source Software is constantly checked and appraised by the worldwide development community. More than 80% of all commercial software contains open source components. It is considered the gold standard in software development.

Richard Avery
Chief Marketing Officer
646.775.2761

About Quantalytics Subscription Based Products:

- We have **NO** initial capital expense ("CapEx") charges.
- All appliances are subscription-only, which includes all hardware, upgrades, maintenance and technical support (no hidden fees).
- Quantalytics always maintains ownership of our Network Security Appliances. As a result, we are always responsible for software updates and the appliance hardware itself.
- All of our appliances are fully covered by our warranties as long as they are under subscription.
- Our products are designed to be used both individually as stand-alone network security products and as part of a synergistic ecosystem to maximize Cybersecurity effectiveness.
- Quantalytics products are also compatible with our competitors' products, thereby allowing customers to "mix and match".
- All of our appliances are also available as **Virtual Machines** if required.

Quantalytics Product Overview

Q-Box®

Foundational Network Security.

The Q-Box combines a network burglar alarm with a network inventorying tool. Inventorying enables identification and monitoring of the entire network's running services and assets. The Q-Box includes a suite of forensic tools to help find and diagnose the exact nature of a break-in so it can be quickly fixed. Unlike firewalls that only look at overall network traffic, the Q-Box evaluates the contents of the traffic for the presence of malware.

Q-IDS®

Advanced Intrusion Detection.

The Q-IDS is a high-powered burglar alarm coupled with a suite of forensic tools to automatically alert and identify the exact nature of a network breach so it can be quickly fixed. Quantalytics recommends the Q-IDS appliance if the inventorying and security auditing tools found in the Q-Box are not required.

Richard Avery
Chief Marketing Officer
646.775.2761

Q-DLP®

Data Loss Prevention Alarm

The Q-DLP continuously monitors data (i.e. Social Security numbers, dates of birth, and other personally identifiable information) on networks to determine exposure to potential hacking. The Q-DLP then automatically notifies the administrator of the potential vulnerability so the issues can be corrected. The Q-DLP also alerts administrators to data thieves (hackers) in the act of exfiltrating stolen data so that corrective action can be taken.

Q-OSSEC®

Ideal for Point- of- Sale (PoS) security

The Q-OSSEC is a combination Intrusion Detection System (burglar alarm) and auditing tool. Both are for general use, as well as PCI DSS (Payment Card Industry Data Security Standard) auditing and compliance. The Q-OSSEC is ideal for safeguarding Point-of-Sale (PoS) terminals and networks. The data auditing tool can ensure credit card companies are compliant with mandatory card issuers' regulations.

Q-Hpot®

Honeypot Decoy Appliance for IT Networks.

The Q-Hpot uses a honeypot to camouflage the real servers and workstations in a network by presenting potentially thousands of false ("decoy") network devices. If real servers are difficult to spot, the odds of a successful hack decrease radically. Honeypots also act as an additional tripwire to notify of intrusion attempts.

Q-ConPot®

Specialized Honeypot for ICS and SCADA networks

The Q-Conpot is a honeypot for Industrial Control Systems (ICS) and SCADA networks. The real devices are camouflaged by thousands of phantom devices, each mimicking human activity and making the real ones virtually impossible to spot, thereby radically reducing the odds of a successful hack. Honeypots can also act as a tripwire to alert an intrusion attempt.

Q-GridPot®

Specialized Honeypot for Electric Power Grids and Substations

The Q-Gridpot is a honeypot for Industrial Control Systems (ICS) and SCADA used in electric power grid OT networks and substations. Honeypots provide network obfuscation and deny the hacker easy network access while greatly increasing the likelihood of detecting a breach. The real devices are camouflaged by thousands of phantom devices, each mimicking normal operational functionally. The camouflage makes the real devices virtually impossible to spot, thereby radically reducing the odds of a successful hack. Honeypots can also act as a tripwire to alert administrators to an intrusion attempt.

Richard Avery
Chief Marketing Officer
646.775.2761

Q-GasPot®

Specialized for Veeder-Root Gas Systems

Veeder-Root Guardian Tank Gauges are widespread in the oil and gas industry and are used for, among other things, inventorying fuels. The Q-GasPot was designed to randomize the gauges as much as possible so that no two instances look exactly alike. This makes it possible for the Q-GasPot to display hundreds of realistic attack surfaces ("decoys") on a network, which, in turn, can help catch and stymie a hacking attempt. To the hacker, it appears to be a very large fuel depot. If the hacker probes an attack surface, the hacking incident is caught and an alert is issued. The only limiting factor on the number of decoy attack surfaces is the number of available LAN IP addresses.

Q-GM®

Passive Network Monitoring appliance

GrassMarlin relies on passive scanning, unlike most network monitoring systems, including the Quantalytics Q-Box. This makes it ideal for older networks were latency potentially introduced by active scanning is a concern. GrassMarlin produces a variety of graphical reports grouped by the following topical areas: Network, Country, Manufacturer, Role, Category, and ICS Protocol. This gives network operators critical information at a glance. The data analysis tools built into GrassMarlin can be used to identify devices that are acting out of role, due to infection or misconfiguration.

Q-Log®

Log aggregation and automated log analysis appliance

The Q-Log automates the collection and analysis of all types of logs. Logs are provided by everything residing on a network. The Q-Log filters these logs to only display entries that may indicate intrusion attempts or network device service failures.

Q-SOAR® – for 2 required appliances for failover.

Ideal for fully or partially automating responses to cyber security alerts.

The Q-SOAR (Security Orchestration, Automation, and Response) automates the detection and response to security breaches, using The HIVE, a highly scalable, 4-in-1 open source Security Incident Response Platform. The Q-SOAR augments, and can replace, cyber security employees in dealing with alerts from SIEM systems such as the Q-OSSEC. The Q-SOAR relies on playbooks - predefined rules to respond to predefined network events such as a detected breach that can be customized to each customer's network. The Q-SOAR playbooks are created from customers' incident response plans.

Richard Avery
Chief Marketing Officer
646.775.2761

Q-Vul®

Vulnerability Assessment System Appliance

The Q-Vul scans networks to identify unpatched, open vulnerabilities that can lead to security breaches. It examines all types of network hardware (e.g. routers) and software, as well as workstations and servers.

Q-ModSec®

Web Application Firewall

The Q-ModSec is a specialized Web Application Firewall ("WAF") that prevents websites from becoming compromised. It examines web commands sent by browsers to determine if they are legitimate and allowed or illegitimate. If they are illegitimate, the Q-ModSec alerts Cyber Security personnel and blocks the commands, thereby preventing the illegitimate commands from reaching the web server.

Q-WiFi®

Detects and Defeats false Wi-Fi Networks ("Evil Twins")

The Q-WiFi detects and defeats imposter ("Evil Twin") Wi-Fi networks by preventing users from logging into fake, look-alike wireless networks used by hackers to steal user credentials. The Q-WiFi blocks access to Wi-Fi networks until the Evil Twin can be found and removed. This prevents innocent "guest" users from logging onto fraudulent networks, thereby protecting users' various website login credentials from exposure to hackers. Q-WiFi is ideal for all public WiFi environments.

Q-Proxy®

Proxy Server/URL redirector

The Q-Proxy filters web traffic. It blocks problematic sites (e.g. porn) and includes settings that allow custom site blocking (e.g. ESPN.com during working hours). The Q-Proxy is ideal for libraries and schools that receive Federal Aid money to meet federal filtering requirements. The Q-Proxy also provides a filter for businesses and organizations requiring enforcement of internet usage policies.

Richard Avery
Chief Marketing Officer
646.775.2761

Q-VPN®

Virtual Private Network

The Q-VPN provides a secure, encrypted connection between computers at varied, diverse locations and is fully compatible with all types of VPN software. It allows scheduling, as well as highly restrictive individual user controls. Unlike most other VPN solutions, Quantalytics' flat monthly subscription charge supports over 4,000 simultaneous users per Q-VPN, if the customer has the necessary bandwidth. Q-VPNs can also be connected together through load balancing and automatic failover to simultaneously support over 200,000 users.

Q-NAC®

The Q-NAC (Network Access Control) determines which devices are allowed on a network, as well as their access privileges. It prevents unauthorized rogue laptops, thumb drives, and any other physical or wireless devices from being attached, in addition to blocking illegitimate user activity by denying access. This feature is crucial if a user's credentials have been compromised. This appliance provides continuous protection even if internet service is interrupted.

H-Box®

Network Security Testing Appliance

The H-Box (Hacking Box) is a Network Penetration ("pen testing") tool. Rather than only testing for network security holes and weaknesses once per year, the H-Box allows users to test security with unlimited frequency. This means that new network security holes are caught quickly and action can be taken immediately.

For a full list and more details on our line of network security appliances,
please visit our website at https://www.quantalytics.com or contact us directly.