Richard Avery
Chief Marketing Officer
646.775.2761

Products Overview

Quantalytics is a 30 year old network and systems integration firm providing superior state-of-the-art network security solutions. Our network appliances are built with the most powerful technologies available and are custom designed to address the full range of IT, IoT and OT network cybersecurity needs.

Priced at a fraction of what other manufacturers charge, Quantalytics cyber security appliances provide small to medium-sized customers the same high-quality enterprise protection used by major organizations and Fortune 500 corporations. All of our products are administered through a user-friendly Graphical User Interface, greatly simplifying implementation and management. This feature allows all levels of IT specialists access to information security.

To enhance affordability, all Quantalytics network appliances are subscription based. A 2-year initial lease term includes all hardware, software, maintenance and required upgrades. We do not charge a mandatory upfront capital expense common to other manufacturers for comparable equipment.

Why is On-Premises Superior to Cloud Based Security?
If your Internet connection is lost for any reason, all cloud cyber security is dropped too. 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 not connected to the Internet.

Why use Open Source Software?
Open Source Software is superior because it is continuously updated and improved by thousands of developers. Modification is restricted to the developers who police each other's work. The result is highly dependable, cost-effective applications. Unlike commercial applications, Open Source Software is constantly checked and appraised by the worldwide development community. It is considered the gold standard in software development.

Richard Avery
Chief Marketing Officer
646.775.2761

Quantalytics Products:

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.

Q-DLP®
Data Loss Prevention Alarm
The Q-DLP continuously monitors data (i.e. Social Security numbers, date-of-birth and other personally identifiable information) on networks, which often change, 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 to data thieves (hackers) in the act of exfiltrating stolen data so administrators can take corrective action.

Q-OSSEC®
Ideal for Point- of- Sale (PoS) security
The Q-OSSEC is a combination of an 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®
Honey Pot Decoy Appliance for IT Networks.
The Q-Hpot camouflages 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 drop radically. Honeypots also act as an additional tripwire to notify of intrusion attempts.

Richard Avery
Chief Marketing Officer
646.775.2761

Q-ConPot®
Specialized Honey Pot 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 devices, each mimicking human activity and making them virtually impossible to spot, thereby radically reducing the odds of a successful hack. Honeypots can also act as an additional tripwire to alert an intrusion attempt.

Q-GridPot®
Specialized Honey Pot 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 (hiding in plain sight) and denies the hacker easy network access, while greatly increasing the likelihood of detecting a breach. The real devices are camouflaged by thousands of 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 an additional tripwire to alert an intrusion attempt.

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 for everything residing on a network. The Q-Log filters logs to only display entries that may indicate intrusion attempts or network device service failures.

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 web sites from being 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 blocks the commands, thereby preventing them 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.

Quantalytics, Inc. 646.449.7810 ravery@quantalytics.com

Richard Avery
Chief Marketing Officer
646.775.2761

Q-Proxy®
Proxy Server/URL redirector
The Q-Proxy filters web traffic. It blocks problematic sites (e.g. porn) and also allows custom settings to block sites (e.g. ESPN.com during working hours). The Q-Proxy is suitable 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.

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 VPNs, Quantalytics' monthly subscription charge supports unlimited VPN endpoints and users.

Q-NAC®
The Q-NAC (Network Access Control) Appliance determines which devices are allowed on a network, as well as their access privileges. It prevents unauthorized rogue laptops, thumb drives and any other devices from being attached, and blocks illegitimate user activity by denying access. This feature is crucial if a user's credentials have been compromised.

H-Box®
Network Security Testing Appliance
The H-Box (Hacking Box) is a Network Penetration (pen testing) tool. Rather than have only an annual test to determine network security holes and weaknesses, the H-Box allows users to test security with unlimited frequency. This means that new network security holes are caught quickly and remediation can happen immediately.

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

Quantalytics, Inc. 646.449.7810 ravery@quantalytics.com