Richard Avery
Chief Marketing Officer
646.775.2761

Quantalytics is a 30 years old network and systems integration firm which 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. T his opens up information security to all levels of IT specialists.

To enhance affordability, all of our appliances are subscription based with a 2-year initial term, which includes all the hardware, software, maintenance and upgrades as required. We have no mandatory upfront capital expense normally charged by other manufacturers for their comparable equipment.

Quantalytics Products (partial list):

Q-Box®
Foundational Network Security.
The Q-Box is a combination of a network burglar alarm and network inventorying tool. Inventorying enables identification and monitoring of all of a 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 which only look at overall network traffic, the Q-Box evaluates the *contents* of the traffic for malware.

Q-IDS®
Advanced Intrusion Detection.
The Q-IDS is a high-powered burglar alarm for networks that also includes a suite of forensic tools to help identify the exact nature of the break-in so it can be quickly fixed. We suggest the Q-IDS appliance if you don't need the inventorying and security auditing tools found in the Q-Box. The Q-IDS includes a full suite of software for automatic alerting.

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, Date of Birth and other Personally Identifiable Information data) on networks, which often change, in order to see what is open and exposed to potential hacking. The Q-DLP then automatically notifies the administrator of the potential vulnerability to their data so these issues can be corrected. The Q-DLP can also alert you of data thieves (hackers) in the act of exfiltrating the stolen data so administrators can take 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 for general use, and for PCI DSS ("Payment Card Industry Data Security Standard") auditing and compliance. It is ideal to help safeguard Point-of-Sale (PoS) terminals and networks. The data auditing tool can be used to insure 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 the real servers are not easy to spot, then the odds of a successful hack drop radically. Honeypots also act as an additional tripwire to notify of intrusion attempts.

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 1,000's of devices each mimicking human activity, making them virtually impossible to spot, thereby radically reducing the odds of a successful hack. Honeypots can also act as an additional tripwire alerting of 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 1,000's of devices each mimicking normal operational functionally, making them virtually impossible to spot, thereby radically reducing the odds of a successful hack. Honeypots can also act as an additional tripwire alerting of an intrusion attempt.

Quantalytics, Inc. 646.449.7810 ravery@quantalytics.com

Richard Avery
Chief Marketing Officer
646.775.2761

Q-Log®
Log aggregation and automated log analysis appliance
The Q-Log automates the collection and analysis of all kinds of logs. Everything on a network produces logs. The Q-Log filters these logs to only display entries that may indicate intrusion attempts or network device or 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 kinds of network hardware (e.g. routers) and software in addition to 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 legit and allowed, or illegitimate, and if illegitimate, 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") WiFi 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 wifi networks until the Evil Twin can be found, and removed.

Q-Proxy®
Proxy Server/URL redirector
The Q-Proxy filters web traffic. It keeps out 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 all libraries and schools that receive Federal aid money in order for them to meet their Federal filtering requirements. It also provides a filter for businesses and organizations that wish to enforce an Internet usage policy.

Q-VPN®
Virtual Private Network
The Q-VPN provides a secure, encrypted connection between computers at different locations. It is fully compatible with all types of VPN software. It allows scheduling as well as highly restrictive, if desired, individual user controls. Unlike most other VPNs, our monthly subscription charge supports unlimited VPN endpoints andusers.

Richard Avery
Chief Marketing Officer
646.775.2761

Q-NAC®

The Q-NAC (Network Access Control) Appliance determines what devices are allowed on a network, and with what 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 is crucial if a user's credentials have been compromised.

H-Box®

Network Security Testing Appliance

The H-Box (Hacking Box) is our Network Penetration (pen testing) tool. Rather than have only an annual test to look for network security holes and weaknesses, the H-Box allows users to test with unlimited frequency. This means that new network security holes are caught far sooner, and remediation can also happen far more quickly.

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