

QVISION™

Network behavior management and analysis



“The largest security risk is typically from internal users doing things they shouldn’t be doing. QVISION allows us to look for that abnormal usage – things that wouldn’t necessarily trigger an alert.”

Mike Sullivan
Chief Information Officer, Entrust
Q1 Labs Customer

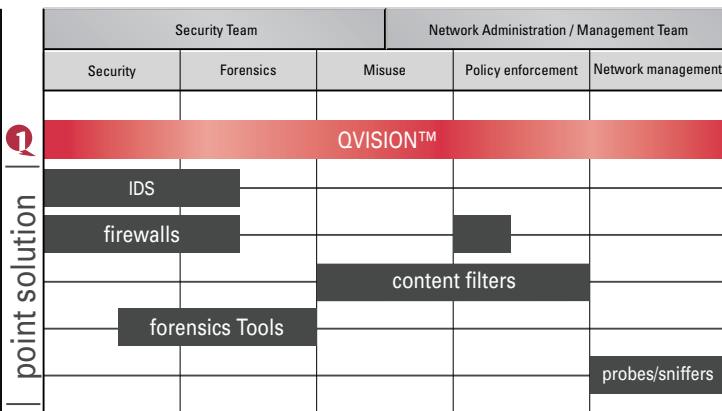
- **Provides a real time, comprehensive view of the network**
- **Easy to deploy, configure, and use for immediate impact**
- **Eliminates false positives and negatives**
- **Intuitive design for quick response and resolution**
- **Leverages and integrates existing security for more effective solution**
- **Identifies risks inside and outside the network**

QVISION – A security solution that bridges the gap

As network administrators and security professionals encounter increasingly more sophisticated threats, they are recognizing that there’s a strong need for a solution that bridges the gap between their areas. In order to respond more quickly and to be more effective, they need a solution that connects deployed point solutions and provides a comprehensive view of the network.

There has been an ongoing debate about what is the best way to detect and prevent network misuse – behavioral rules or signature-based technology. Administrators are also shifting their focus from protecting the perimeter toward solutions that can detect and prevent attacks from within.

With these challenges in mind, Q1 Labs developed QVISION, a network behavioral analysis and misuse technology with a robust user interface that presents network behavior in a variety of views. This innovative solution increases efficiency and reduces operating costs for security management.



QVISION combines the best of point solutions, so your organization can get the most impact and ROI from its security program.

Greater manageability, automation, and ease of use

QVISION provides greater manageability, automation, and ease of use in monitoring misuse and threats to an enterprise environment. Designed to monitor traffic from a wide variety of multi-dimensional projections and graphs, QVISION allows the user to instantly identify malicious activity and determine all aspects of the attack. It allows an organization to take immediate, corrective action to contain the threat before significant damage can occur.

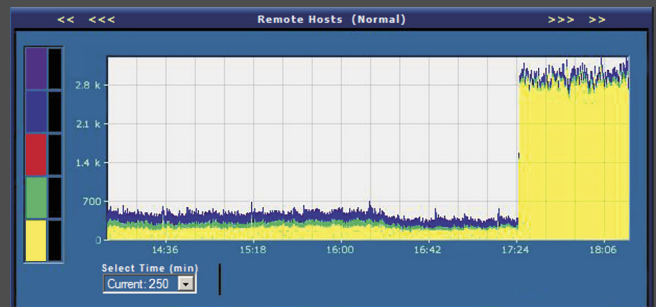
QVISION audits every activity and transaction that crosses the network. Administrators can effectively manage large volumes of security data and easily access and comprehend that data real time.

As a forensics tool, QVISION captures all information necessary to identify and track individual activity. An administrator can determine who talked to whom and for how long, what applications they were using and what kind of files they were transferring. Managers can pinpoint specific machines and remote addresses to quickly resolve network problems. In addition users can look back in time to review trends and prior abuses or security breaches.

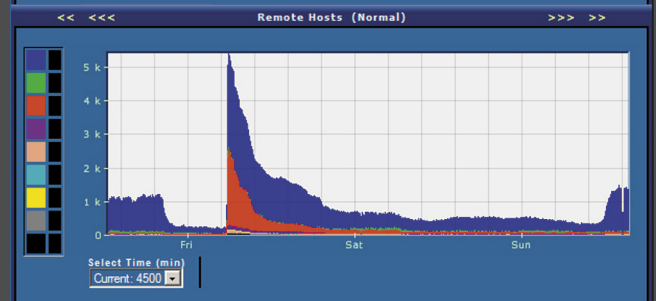
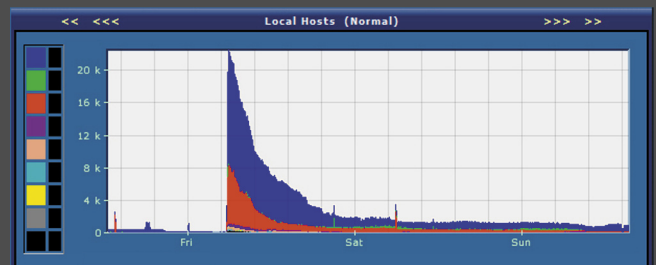
The best defense is faster knowledge

QVISION is a solution that provides greater access and promotes better communication between the security team and the network administrators. Its hierarchal nature allows both functions to see the same information so both can be better informed, and both can share responsibility for troubleshooting and resolving network and security issues.

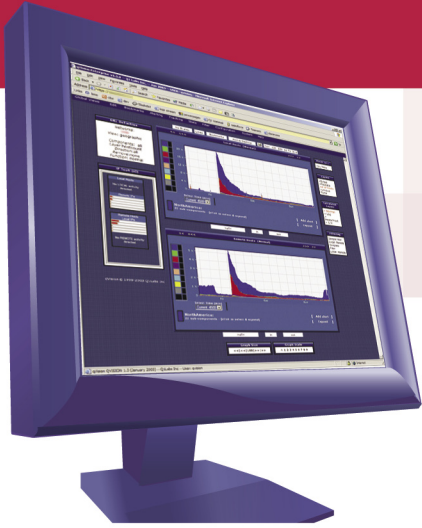
The need for enterprise corporations to share data with customers, partners, suppliers, and employees will continue to grow at an enormous rate. And, while the internet allows more effective methods of data collaboration, it also exposes organizations to a universe of new, unpredictable risks. Viruses, worms, trojans, and a variety of threats propagate, spread and wreak havoc on corporate networks, debilitating business. No one can prevent these attacks, but with QVISION you can quickly identify and resolve them.



This screen capture displays a scan gathering intelligence on the network of over 2000 hosts per second outside the network.



In this geographic view taken during the Slammer Worm incident, the blue represents North America and the red represents Asia. This view helps to determine that it can potentially be a world-wide issue.



How QVISION works

QVISION is a turn-key, appliance-based solution. Its modular design makes it simple to install, configure, and use. Because QVISION doesn't require extensive training and there are no complicated logs to decipher, administrators can begin to realize the benefits immediately.

The QVISION management console functions as the central brain for your security system. It allows you to monitor and manage potential internal and external threats and misuse for a network of any size. Users can view all traffic coming across the Internet real time, in a variety of customizable views. It can display general overviews, and through sophisticated data mining and drill down abilities, it can display network activity based on a wide variety of component combinations.

The flow generator can be positioned anywhere on the network, monitoring network traffic flows coming in and out of the network, detecting unnatural patterns and client behaviors. It collects and breaks down packet data in real time, and then a classification engine stores the components into databases based on the concept of views, both general and specific, drilled down to the IP address and packet level.

QVISION implements seamlessly with other security technologies, allowing you to better leverage existing security products, and to have multiple levels of network security management. With QVISION, you can incorporate IDS data within the context of the management console. This provides for seamless security monitoring using multiple sources, enabling a more flexible and scalable web-based interface.

Benefits of QVISION:

- **View-based solution** – QVISION classifies data flows into thousands of components to view data quickly and easily.
- **Centralized interface** – View the network from a central screen and manage your security program from QVISION's management console. QVISION integrates with multiple security data sources and visualizes security data to more effectively manage threats and misuse.
- **Effective correlation and analysis tools** – Intuitive design and quick drill-down allow for detailed analysis and effective security decisions with the right data.
- **Hierarchical multi-user access** – QVISION was designed for multiple users. Responsibility for monitoring the network can be shared.
- **Complete audit trail of total network activity** – Ensure your firewalls are doing what they are supposed to. QVISION provides a critical line of defense for traffic that has passed through the firewall and the IDS without triggering an alert.
- **Adjustable alerts** – Adjust alert levels to fit existing security management processes and procedures.
- **Constant updates not needed** – Since QVISION is based on network behaviors, signature updates are not needed. Modifications can be made immediately.
- **Scalability** – QVISION is a turn-key, appliance-based solution. Its modular design provides enterprise class scalability.
- **User activity monitoring** – Routinely monitor and report on identified suspicious users.



“If you use IDS in a vacuum and don’t have a way to make sense of it, you may as well turn it off rather than have people running around in circles. The visualization component in QVISION makes the information more palatable at all levels – from network operations to security operations and on up through management layers. It provides a useful tool to justify past and future expenditures in the next wave of security solutions.”

Dan Keldsen
Senior Analyst and Director of Information Systems
Delphi Group

QVISION – the key components

QVISION is a complete, appliance-based solution. As a result it can be implemented more quickly and easily, and the user can begin to realize the benefits immediately.

- **Management Console** – Serves as the brain and allows for a comprehensive view of the network. It includes alarms and alerts to notify a user of network behavior changes and policy violations. The audit data collected from each flow is aggregated and stored in a proprietary RDB, and the flow data is efficiently retained for long periods, allowing for historical analysis and reporting.
- **Flow Generator Appliance** – The flow generator is a passive device that monitors network traffic flows. It can be placed at one or more places in the network to capture a complete record of every transaction.
- **Third Party Event & Log Data Correlation**
IDS events are mapped to the flow data. The correlation process is unique and extremely efficient in both processing time and data storage. IDS events associated with a specific flow are tagged on the flow record.

About Q1 Labs

Q1 Labs Inc. is a leading developer of innovative network behavior management and analysis solutions. Q1 Labs’ customers come from a variety of industries including government, academic, and financial institutions, utilities, service providers, manufacturing, and healthcare.

To learn more about QVISION and how to minimize risk to your enterprise, contact us. We’d be happy to schedule a demo of QVISION and discuss setting up a test run in your network environment.

International Headquarters

One Brunswick Square, Suite 1608
Saint John, New Brunswick
Canada E2L 4V1

U.S. Headquarters

15 Piedmont Center, Suite 1040
Atlanta, Georgia
USA 30305

1.877.471.5227 Phone
info@q1labs.com
www.q1labs.com