



For more information:
ReSoft International
www.re-soft.com
203 972 8462

QVISION™ Technical FAQ

What is QVISION?

QVISION is an innovative view-based network behavior management and analysis solution developed by Q1 Labs to provide greater manageability and automation in monitoring an enterprise environment for misuse and threats. It provides an additional layer of security that will make it easier for businesses such as yours to reach the next level of security.

How is QVISION different from other security products out there today, and why would it be selected as the best solution in a vendor “bake-off”?

Companies are drowning in false alarms from their intrusion detection. QVISION helps organizations manage firewalls, antivirus and intrusion detection, and it helps make sense of all the data. Q1 Labs has an established customer base and proven technology. It is an innovative and effective solution that provides an immediate and comprehensive view of activity in and out of your network. The QVISION technology was in development for two years prior to the company's inception. Q1 Labs has a unique research and development alliance with the University of New Brunswick which allows the R&D team to access seventeen live networks for product testing and research..

- QVISION monitors for unusual behavior and misbehavior and tracks activity from a high level down to an individual IP address.
- It identifies where your capacity is going. Often within minutes of installing QVISION, our customers have discovered gaming servers, illegal peer-to-peer file-sharing activity, e-mail servers, and more bandwidth-draining activity from internal sources that they had never been aware of.
- QVISION presents the data real time in a variety of easy-to-navigate and comprehensive views. Like an x-ray, it provides a snapshot of the network allowing for a true understanding of network behavior. As a result you can establish policies and alarms/alerts for behaviors and/or activities considered abnormal or unacceptable.
- You can customize the alarms and/or alerts within QVISION which reflect the rules for what is acceptable behavior on your network. Alerts may also be set for specific targeting activities such as intelligence gathering, as well as inappropriate behavior targeted against customers from outside and inside the network.
- QVISION's easy to use, graphical management console, allows administrators to quickly prioritize and respond to behaviors that trigger alarms by drilling down into the activity to uncover the details. E.g. source/destination IP, application, protocol, scan or targeted attack, etc.
- QVISION detects activities that go against usage policy (misuse), threatening (security), or abusive behaviors. Administrators can implement automated actions as a response to QVISION alarms. Coded within the QVISION alarm, a user may choose to send a command to a Firewall or IDS/IPS product to end/filter threatening activity.



Does it work with other security products and will it interfere with existing security practices?

While QVISION collects its own data (a combination of network flows and content) it can also use existing security devices to allow greater intelligence and decision making information available to users. Some organizations have found that QVISION provides a complete solution beyond the firewall, while other organizations find QVISION to be the best complement to IDS by making the data from IDS more manageable and useable.

Although QVISION's flow generators are installed passively on a network, you will need to install them using a network tap or on a mirror/span port. If you already have other security devices plugged into that port, you may need to consider other options: another mirror or span port, a network tapping device, or a high quality hub to feed both products.

I already have firewalls and IDS. Why do I need QVISION? Do you replace my firewalls or IDS?

For companies that already have Firewalls and IDS, QVISION is the next logical layer to add to your security infrastructure. Since QVISION collects its own data, however, it is not dependant on IDS or Firewalls to provide value in your environment. Many recent articles have been written about the effectiveness (or ineffectiveness) of current IDS products and other monitoring devices. While some organizations purchase QVISION to replace IDS, other organizations have found that QVISION actually makes their IDS deployments more effective.

How does QVISION collect the network information it uses and then correlate it to be able to alert security staff to take actions?

QVISION uses flow generators to collect and break down network traffic flows (packet header data) in real time. A classification engine then stores the components into databases within the management console. The data is translated into a visual representation of the activities on your network within 30 seconds of collecting the data. The information is accessed via a web browser that accesses the console from anywhere. The flows that occur from the flow generator to the console are extremely small and will not create bandwidth issues on the network being monitored.

Third party correlation – QVISION's integration with third party IDS and Firewall event information is focused on getting security analysts to the event quickly, then providing them with the underlying flow information and the ability to identify the severity of the event. Within seconds a network or security analyst can determine if a large number of IDS alerts was caused by (for example) a *script-kiddy*, or is a potentially harmful targeted attack from a professional, hostile source. 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. The result is the graphical snapshot, like an x-ray, of the customer's network which can show specific activities/flows marked as potential problems from the IDS/Firewall devices.

Monitoring events – QVISION also has the unique ability to maintain monitoring details on IDS events. A flow can be tagged and tracked when an IDS event has been identified as a potential trigger. Future flows that are associated with this IP address can be tagged with follow-up IDS tags. This is applied even if the IDS does not trigger an event on subsequent



flows. Such follow-up events may actually be more important to investigate than the actual event associated with the first triggered IDS event.

SIM products – Generally administrators rely on log information from a number of other point products placed in or running on the network. They correlate and in some cases aggregate information from the logs, attempting to increase the strength of the knowledge of the individual event. If more than one product identifies an event (for example if based on a vulnerability scan that determines that the device is in fact vulnerable), events are further categorized, or a decision is made as to the probability of success. If the device providing the information is the target of the attack (many attacks are targeted at security devices), the information may not be accurate or even be available to the SIM console. QVISION acts as an additional layer of defense. It will continue to capture and display behavioral information even if the IDS device itself is disabled.

QVISION provides cross-validation – Like the SIM products, QVISION will aid in validating events but more specifically, it will present information in context with the underlying flow that generated the event. QVISION is especially effective in situations where the security threat is new and usually (immediately) unrecognizable by the IDS devices.

Is QVISION software or an appliance?

QVISION is a software application that runs on Linux Red Hat. It can be installed on a system that meets the minimum system requirements. Hardware and software can be purchased thru Q1 Labs in a pre-configured appliance per the customer's request

What do you mean by “views” and why are they significant?

Many point solutions are cumbersome with too much data to decipher. They also require specialized training to be able to interpret the volumes of data. And by the time you do, it can be too late to take action on a current threat. QVISION makes the data available instantly and displays it in a wide variety of intuitive *views*, real time screen captures of activity across the network. These views are produced in HTML pages, no JAVA or applet add-ons, so they load quickly. You can literally navigate from a high level geographic view, through hosts and application views, and drill down to an individual IP address within a few mouse clicks.

People understand pictures more intuitively than data. The graphs that QVISION presents take advantage of this fact, enabling those who are not highly trained (i.e. expensive security experts and consultants) to have the ability to identify suspicious traffic on the network.

Is the data real-time?

Yes. All views and data presented in QVISION are occurring in real time. The only delay is the timeframes in which to refresh the HTML screen which can be configured by the user.

Does QVISION incorporate alerts and how are they set up?

QVISION comes with a base set of alerts for common, recognizable security threats. Beyond this an administrator can set his own alerts. You can use this feature to set alerts based on activities and behaviors that are against policy for your network and resources. For example, if a U.S.-based financial institution has only U.S.-based customers, they could set an alert for activities and traffic to their application server that originate from outside the U.S.

QVISION's alerting is extremely easy to set up. Alerts can be based on high or low thresholds, and alerts can be sent to a technician's pager or forwarded to an enterprise



management system. QVISION presents the data associated with an alert in a graphical format, displaying the event in context with the data collected in an easy to understand format.

Alerts are half the answer to solving a problem, however. The other half is having access to the detailed data that can aid a technician in finding and resolving the issue. QVISION's easy-to-use visual presentation of what is occurring in the network allows an administrator to quickly and easily navigate from a high level view of what is occurring, down to a precise IP address in real time to determine exactly who is causing the activity.

Is QVISION a “sniffer”?

No. QVISION is based on a different approach and technology. A sniffer monitors and analyzes network traffic by looking at packets to detect bottlenecks and problems on a network. It's effective at what it does, but it's a limited, low level tool. Administrators typically don't run sniffers continuously. The output from a sniffer typically appears in a log format and requires informed analysis.

QVISION runs continuously and displays activity real-time, in easy to understand views. QVISION doesn't look at just the packets. It looks at the flow and uses flow generators to monitor a variety of information in and out of the network. It creates a complete audit of every communication that passes the flow generator, enabling administrators to detect and resolve threats more quickly. QVISION complements sniffers, as well as signature-based, and pattern identification products that recognize known security events by detecting any unusual event.

Where do I place QVISION in the network?

QVISION is a distributed system that is typically deployed across your infrastructure from your connections to the Internet to your internal networks. We typically see clients deploy on the perimeter first, but add flow generators internally shortly after the initial install.

How many flow generations can a single management console handle?

Rule of thumb – 100,000 flows per minute per console. QVISION can be scaled to any size organization by deploying an appropriate number of flow generators. A single console is not limited, however, by the number of flow generations that can be fed to it. There are limits on the total amount of traffic a single console can manage. If you are planning on deploying in an environment where you will be feeding multiple gigabits of traffic, contact Q1 Labs for additional information on deployment scenarios.

Explain how QVISION is scalable for a large user.

QVISION has a robust, flexible architecture designed from the ground up to be scalable in large, enterprise networks. The key intellectual property within QVISION lies within the management console. This eliminates the common problems with asynchronous links experienced by most IDS and other point SIM products. The QVISION console can scale to accept data feeds from many flow generators, and the flow generators can accept data from multiple mirrored segments, working efficiently on high-bandwidth networks and optical links. The architecture has no theoretical upper boundaries other than those present in the chosen hardware appliance, plus the QVISION database is self maintaining.

Other products will typically need one sensor or collector per network segment. Determining the number of sensors requires a comprehensive interview and site survey.



QVISION does not require a flow generator appliance to be installed on every segment and can monitor multiple segments with a single appliance.

Is the flow generator detectable on the network? Will a perpetrator be able to see it and know?

The flow generators are deployed in passive mode. The monitoring ports of the flow generators do not have IP addresses, so it will be invisible on the network. However, if you have span or mirror ports configured on routers, there are methods of detecting those. The intruder will not be able to know what is connected to the port, but they can tell you are monitoring.

Can I use QVISION for forensics use?

QVISION provides detailed information on the traffic and activity on a network. It has been crucial in many organizations to identify the rogue network users and put a stop to their abuse. QVISION (version 2.0) provides selective content capture, allowing users to record data once something suspicious becomes apparent.

QVISION was designed to be an efficient and scalable solution to fit easily within operational resource constraints. Because of this, QVISION does not conduct full content capture like other forensics tools, which require significant additional costs for storing the content information. Numerous clients have used QVISION in a forensics role and the data it captures allows for a complete audit of every communication and transaction across a network. Customers who track transactions by department for billing or revenue purposes have found this to be a useful feature.

How does QVISION handle encryption? Is the communication between the flow generator and the console encrypted?

The communication between the flow generator and console can be configured to handle encryption. Communications from the QVISION web interface to the flow generators and console are encrypted. However, in the case of the flow generators, clients may choose to turn off the encryption as it adds overhead, and the data may already be traveling on encrypted networks.

What protocols do you monitor?

Unlike many monitoring tools on the market today, QVISION looks at multiple protocols. QVISION looks at all IP based protocols such as common protocols TCP, UDP, and ICMP, as well as the rarer protocols IPv6, GRE, OSPF and more. Additional protocols are being included in v2.0 of QVISION.

How can external security information be fed into the QVISION solution to help provide a total security dashboard solution?

QILabs contends that a security dashboard would be most helpful for an administrator if it were more than simply a consolidation and correlation repository for security events. A QVISION-enhanced dashboard would be configured to correlate all information required at the network flow-data level. The key goal is not simply to correlate security events, but also to map them to the underlying network activity. It is this combination that creates a management system that aids in both increasing the validity to the security event and provide real-time analysis for increased time-to-resolution.



QVISION already provides agents for the most popular IDS products and will continue to add support in (near-term, mid-2003) releases for a broader set of security products. Alternate sources of input and features can be based on customer demand and can be developed if funded.

Can you connect through the span port? If all ports are being used, how can you access?

Yes, QVISION can be connected through the span port. Use of network taps is a good method of passively tapping the network when there are no free ports. In some cases, you may need two monitoring ports on your QVISION application when using taps as they split the inbound and outbound traffic.

What is the maximum bandwidth QVISION can handle?

One of Q1 Labs' first customers was a large telco. QVISION succeeded in easily managing the massive bandwidth requirements. QVISION supports network connections from DSL to Gigabit out of the box. For connections more typical in providers such as OC-XX, we would need to determine our capabilities on an individual case basis.

Do you capture content?

QVISION (version 2.0) provides selective content capture, allowing users to record data once something suspicious is detected. QVISION is designed to be an efficient and scalable solution to fit easily within operational resource constraints. Because of this, QVISION does not do full content capture like other forensics tools which require significant additional costs for storing the content information. It scans content for protocol analysis and stores a configurable amount in our flow records.

How long do you store the data?

The length of data retention can be determined by the client for one day, one year, up to five years if needed. Storage is customizable per network, per view and per object. QVISION requires an amazingly small amount of disk space for long periods of data retention. For more specific requirements, contact support@q1labs.com.

What type of database do you use?

QVISION uses its own internal proprietary database which is included with the QVISION management console. The database scales effectively to all network sizes and can store data for years without maintenance. If needed, we can provide tools with the console to access the data directly for use in other applications and reporting tools.

How easy it to make changes to the QVISION interface?

Very easy. All changes are made through the browser with wizard-like tools. You can easily customize the parameters as well as the colors. The challenge with many networking/security tools on the market today is the difficulty of configuring the system to work optimally in every operations center. QVISION has received accolades from very large as well as medium businesses for its ease of implementation and configuration.

Can I print reports?

Yes. Information can be downloaded in CSV format to any type of report generation tool, or it can be printed directly from the web browser.



What kind of new features and improvements can we expect to see in v2.0 of QVISION?

The upcoming QVISION 2.0 release is slated for release in August 2003. This release is designed to improve on existing elements and provide additional features based on your business needs.

Protocol Analysis: A number of standard Application Protocol Signatures, including P2P signatures and IM signatures, have been added, and a signature wizard will provide assistance with specific application signature strings and port information.

QVISION is able to monitor any TCP/IP based protocol or application. QVISION currently has 70 unique signatures, which encompasses a list of 30 of the most used network applications. More specific applications will be added for monitoring purposes as they become more widely used or abused.

AIM login	HTTP Ogg/Vorbis audio file transfer	RealAudio streaming content
AIM receive message	HTTP traffic	RealAudio streaming content
AIM send message	HTTP WAV audio file transfer	RealMedia streaming content
Apple QuickTime audio/video download	HTTP WAV audio file transfer	RealVideo streaming content
DiVX/AVI file download	ICQ traffic	Shockwave Flash content
eDonkey file transfer	IMAP traffic	Shoutcast MP3 stream
eDonkey file transfer start	IMAP traffic	SMTP Hello
eDonkey files offered	IRC channel join	SSH Access
eDonkey Hello	IRC DCC chat request	Telnet access
eDonkey search	IRC DCC file transfer request	TFTP Get request
Fastrack (Kazaa/Morpheus) GET request	Java applet	TFTP Put request
Fastrack (Kazaa/Morpheus) Traffic	Java applet	VNC traffic
FTP login	Java archive file (JAR) download	WebDAV traffic
GNUTella GET Request	MS Excel file download	Windows Media 9 streamed content
GNUTella HTTP traffic	MS PowerPoint file download	Windows Media audio download
GNUTella Inbound/Outbound Client Request	MS Word file download	Windows Media streamed content
GNUTella traffic	MSN login attempt	Windows Media streamed content
GNUTella traffic	MSN message	Windows Media streamed content
Gzip compressed file download	MSN user search	Windows Media video download
HTTP binary file transfer	NFS RPC traffic (UDP)	Windows Media video download
HTTP binary file transfer	NFS TCP RPC traffic (TCP)	Zip compressed file download
HTTP MPEG audio file transfer	PDF file download	Zip compressed file
HTTP MPEG audio file transfer	POP3 traffic	file
HTTP MPEG video file transfer	POP3 traffic	download

Several new innovative views have been added to the product:

- Correlation View – will layer IDS and firewall alerts onto overall traffic.
- Unexpected Application View – within Application view, additional layers will allow easy visual identification of amount of identified Applications seen on unexpected ports.
- New Applications/Port View – new view based on application content analysis.



Additional enhancements include:

- Remote update capability – ability to update QVISION remotely.
- Encrypted connection – secure connection from console to Flow Generator
- Content capture – Configurable by customer (on/off) as well as how much of payload is to be captured. User might want to turn content on to determine details about other classified traffic.
- In QVISION v. 2.0 the administrator will have the ability to add behavioral alert conditions. The user will be able to choose from plug-in packages of alert conditions that profile denial of services, worms, and ICMP attacks. In addition to vendor-supplied templates, users will be able to add their own behavioral definitions that meet their alert conditions.
- What was previously called the *Application View*, which defines network traffic based on port and destination to known locations of concern, has been renamed *Port View*. The Port View will determine traffic based on application signatures.

Contact ReSoft for more details on the release.

How much does QVISION cost?

The QVISION pricing model consists of a console, which has ranges of prices based on IP addresses being monitored. It is also priced based on the number of flow generators deployed on a network. The price varies based on size of network and amount of network to be monitored by QVISION.

How do I get an evaluation?

In order to get the full impact of the value QVISION will bring to your network, take it for a test drive on your network. Q1 Labs can provide a standard evaluation deployment. Often within minutes of installing QVISION, you will be able to identify activity on your network that you were never aware of. Contact sales@q1labs.com to arrange a time when we can discuss the evaluation process with you.

What type of training and support is available?

Q1 Labs has several training options available to its customers and partners. Contact support@q1labs.com for details. We offer training for individuals or groups, as well as assistance with the deployment of QVISION.