As the security threats facing organizations have grown exponentially, the need for greater visibility into network activity has become an imperative. Attacks and breaches have become more sophisticated, attackers now pursue targets of choice (rather than targets of opportunity), and the consequences can include significant brand and financial damage or risk to critical infrastructure.

Distinguishing itself from first-generation log management and SIEM (security information and event management) solutions, QRadar® SIEM delivers total security intelligence through the use of network flow data. QRadar SIEM with QRadar® QFlow and QRadar® VFlow is the only SIEM solution that provides the Layer 7 application visibility and flow analysis required to fully understand and respond to the activity taking place in your network. With the Q1 Labs solution, you can detect threats others miss, ensure policy and regulatory compliance, and minimize risks to mission-critical services, data and assets.
What is Flow Data and QRadar QFlow?

Network flow data covers the set of conversations between devices on a network. A network flow record provides information about a specific conversation between two devices using a specific protocol and can include many fields that describe the conversation. These characteristics include source and destination IP address, protocol transport (i.e., UDP or TCP), source and destination port, application information, traffic statistics, quality of service, and in some cases actual packet payload.

While a number of flow formats exist today (e.g., NetFlow, J-Flow and sFlow), they typically stop at Layer 4 and only provide network level IP address and UDP/TCP port level information. This is useful for obtaining a general understanding of the conversations occurring on well defined protocols; however the pre-summarized and static data from sources such as NetFlow and J-Flow does not provide deep visibility into network activity and applications.

QRadar QFlow, the most advanced flow collection and analysis solution, provides Layer 7 visibility and stateful classification of applications and protocols such as voice over IP (VoIP), multimedia, ERP, database, and thousands of other protocols and applications. Application-aware flow data is obtained from a deep examination and inspection of every packet, which also allows for advanced threat detection through analysis of packet content. Correlating this flow information with network and security events is the only way to obtain a complete and accurate view of a network’s security posture.

Virtual Flow Data and QRadar VFlow

As the use of server virtualization has become pervasive, the need has grown to monitor the traffic traversing virtual environments, which can't be collected via traditional monitoring technologies. Only QRadar VFlow provides application layer visibility of all virtual network traffic for advanced security intelligence. QRadar VFlow supports VMware virtual environments, enabling the profiling of more than 1,000 applications out-of-the-box. It can also analyze port-mirrored traffic for a physical network switch, which helps bridge the gap between the physical and virtual realms. QRadar VFlow runs on the virtual server and does not require additional hardware, making it a highly cost-effective solution.

QRadar QFlow Use Cases and Customer Successes:

QRadar SIEM with QRadar QFlow is the only solution that fully supports five key use cases:

- **Detection of zero-day threats through traffic profiling**
  Detection of malware and virus/worm activity through behavior profiling and anomaly detection across all network traffic (applications, hosts, protocols, areas of the network)

- **Compliance with policy and regulatory mandates via deep analysis of application data and protocols**
  Alerting on out-of-policy behavior and traffic, such as traffic being sent to untrustworthy geographical regions or unsecure protocols

- **Social media monitoring**
  Anomaly detection and DPI-based content capture that identify and alert on social media-related threats and risks

- **Advanced incident analysis via correlation of flow data with log data**
  Accurate prioritization of incident data and reduction of false positives by correlating security events with actual network traffic

- **Continuous profiling of assets**
  Collection and monitoring of continuous information feed from hosts, assets and services, allowing QRadar SIEM to automatically identify and classify new assets and discover what ports and services they are running
Detection of Zero-Day Threats That Others Miss

QRadar QFlow uses flow data to detect new security threats without the use of vulnerability signatures. As a result, you can rely on it to identify threats missed by antivirus and other security systems. Flow data can be used to detect changes in network traffic that may suggest a threat. Examples include a new service or protocol never seen before, such as a mail server being installed in the DMZ or an FTP service being installed on a server that has not had FTP running on it; a failed service, such as a web server that is active 100% of the day but then stops responding to communications; and a change in the activity level of commonly used services. For example, SSH might be installed on the corporate mail server, but only used a few times a week. If a malicious user were to exploit the server and then utilized the SSH service as a jumping point to exploit other servers this would be immediately detected and alerted on. Only QRadar QFlow provides the visibility and context needed to identify these risks.

CUSTOMER SUCCESS

A global auto manufacturer used QRadar SIEM with QRadar QFlow to detect a worm outbreak affecting its production facility using only flow data. This worm was not detected by other signature-based sources. The company’s security analyst was able to see how telnet sessions on the local hosts rapidly decreased during the attack, while activity through Windows network ports dramatically increased. The analyst worked with his IT operations colleagues to immediately remediate the vulnerability, preventing widespread damage.

Policy and Regulatory Compliance

First-generation log management and SIEM products helped organizations meet compliance needs in the past, but they are no longer sufficient. Newer compliance standards such as PCI DSS, as well as a greater focus on internal policy compliance, require application-aware monitoring and visibility, which simply isn’t attainable through log analysis alone. Only QRadar SIEM with QRadar QFlow provides the ability to detect applications running over non-standard ports, to identify users logging on to critical servers using clear-text user names and passwords, and to ensure that encrypted protocols are properly deployed in sensitive areas of the network.

A common example detected in customer environments is botnet communication channels (IRC traffic) running over port 80 (Web traffic). Through content inspection, covert IRC channel and communications are detected and captured for forensic evidence, and alerts are issued on the behavior. Solutions using only NetFlow data would simply view this as Web traffic and completely miss the botnet activity.
CUSTOMER SUCCESS

A major healthcare provider significantly reduced its financial and reputational risk through the use of QRadar SIEM with QRadar QFlow. The system detected unencrypted patient data being passed in the clear after a patch was applied to a critical system. Due to the rapid detection, the organization quickly remediated this risk and avoided potential penalties.

Social Media Monitoring

Social media is an increasing risk to your organization’s data and assets, as employees can easily fall victim to social engineering-based threats and unwittingly serve as entry points for advanced persistent threats. In response, you need new tools to combat these threats. QRadar QFlow addresses this through native capabilities for deep packet inspection (DPI) and content capture, which allow you to see social media usage on your networks and determine the risks arising from these applications.

The combination of QRadar SIEM and QRadar QFlow allows you to monitor activity on social media platforms and multimedia applications such as Facebook, Twitter, Gmail, LinkedIn, Skype and many others. The solution’s anomaly detection and DPI-based content capture make it easy to detect Web-based malware; identify vulnerabilities introduced to the environment from social media applications; and monitor and alert on the information users are making public – all in real-time. You can identify which users are accessing each social media service, determine their patterns of usage, and monitor and alert on the content being transmitted to those services.

Social media usage can also be correlated against other network and log activity within an enterprise. For example, the transmission of data to a social media site immediately following a user’s unusual accessing of a sensitive internal resource might signal a questionable activity to investigate. Only QRadar SIEM with QRadar QFlow combines flow-based application visibility and advanced in-memory correlation capabilities. With this solution, you gain the most complete, accurate and actionable view of the security threats and risks affecting your network.

CUSTOMER SUCCESS

F.W. Webb Company, the largest plumbing, heating, HVAC and industrial pipe distributor in New England and New York, originally deployed the QRadar Security Intelligence Platform in order to meet PCI compliance mandates and ease the auditing process. With the release of QRadar 7.0, the company expanded the scope of this deployment to monitor social networking usage, which posed a clear risk to its business. F.W. Webb now uses QRadar SIEM with QRadar QFlow to see if its customers’ personally identifiable information is at risk of being shared outside of the company. In doing so, it moved from “check box” compliance to proactive security intelligence and threat detection.
Advanced Incident Analysis and Insight

Application flow data can also be compared with events being seen from security devices in real-time to understand what is actually occurring on the network. This correlation between log data and flow data enables the identification of serious threats that would otherwise go undiscovered. An example of this is a typical backdoor exploit event from an IDS. Information from the event, such as the attacking IP, target IP and port information, can be used to automatically start filtering on actual network communications. Flow data can be analyzed to see if this type of traffic between the two hosts is normal, and if the target is communicating back to the attacking IP using a new service that has never been observed by flow data in the past. Not only can this flow-based correlation rule out most false positives, but it can also raise the relevance and credibility of real attacks to bring them to the forefront of your attention.

CUSTOMER SUCCESS

A leading multinational corporation with an 80,000-host network used QRadar SIEM with QRadar QFlow to discover a botnet infection that existing antivirus and anti-malware solutions did not detect. The QRadar solution identified a small number of .gif transfers to external hosts every day, and combined this with the knowledge that the target was a known botnet command-and-control server, to detect the infection. The company re-imaged the hosts and the activity disappeared.

Continuous Profiling of Assets

QRadar SIEM with QRadar QFlow collects and monitors a continuous feed of traffic information from hosts, assets and services, which provides additional insight into the state of your network. You may know how your network devices, assets, applications and other resources are supposed to be configured, but are you certain they are configured properly? Would you know if new systems or services were deployed? The Q1 Labs solution automatically identifies and classifies new assets found on the network and discovers what ports and services they are running. This ensures a complete view of your network, provides insight into configurations and also improves the prioritization of security incidents.

CUSTOMER SUCCESS

A major US utility company deployed QRadar SIEM with QRadar QFlow to improve its enterprise-wide security posture, and within hours of starting to monitor flow traffic, the Q1 Labs solution automatically identified and tracked thousands of devices and assets. The company found a number of servers and security risks it was unaware of, which would not have been discovered through log event monitoring alone. It now relies on this solution to continuously identify new assets and risks, and respond appropriately.

If we didn’t have QRadar SIEM with QRadar QFlow to help analyze the mountains of application traffic coming into and out of our network, it would have been nearly impossible to identify the anomalies that the company viewed as threats. With QRadar SIEM, we can take any network behavior and look back to get information about its relative importance to the company’s overall security posture.

– RON PORRITT,
Information Security Engineer for Gordon Food Service
Summary

With the sophistication and frequency of threats growing every day, you need deep visibility and actionable intelligence for your network environment. Only QRadar SIEM with QRadar QFlow and QRadar VFlow uses network- and application-aware flow data to deliver an advanced security intelligence solution, encompassing physical and virtual resources. The solution accurately detects and prioritizes security incidents by leveraging all relevant network and security information and placing it in the appropriate context. Combining Layer 7 flow data, log/event data, asset data and other types of data, QRadar SIEM with QRadar QFlow and QRadar VFlow presents prioritized and actionable offenses to your network and security operations teams within a single console. This advanced yet easy to implement solution can help you better detect and remediate threats, enforce policies, and minimize risk to mission-critical IT systems.

Application activity monitoring is important because application weaknesses are frequently exploited in targeted attacks, and because abnormal application activity may be the only signal of a successful breach or of fraudulent activity.

MARK NICOLETT,
Vice President and Distinguished Analyst for Gartner