



## Meeting enterprise IT security objectives through effective log management

A White Paper on the application of QRadar for  
enterprise-wide log management

## Overview

IT organizations of all sizes face tremendous challenge keeping their computer networks secure and properly tuned for optimum performance. Most organizations leverage disparate IT technologies and software solutions to monitor and track network performance, monitor and track application security, as well as collect and manage event logs in an attempt to meet overall IT objectives. A wealth of information exists in the event data provided by computing resources, unfortunately, this information may not be utilized effectively by existing management solutions. Oftentimes critical incidents are overlooked because the information needed to recognize the incident is buried across multiple silos of information. Adding to the challenge are many external regulatory forces that dictate a formal approach to log and security management. Organizations that are struggling to maintain the integrity of their computing resources or having difficulty meeting their compliance requirements should look to deploy a comprehensive log management solution that best meets all of the organizations information security objectives. When selecting a log management solution, organizations need think strategically and consider both short and long term objectives which is prudent when making any technology decision.

## Challenge

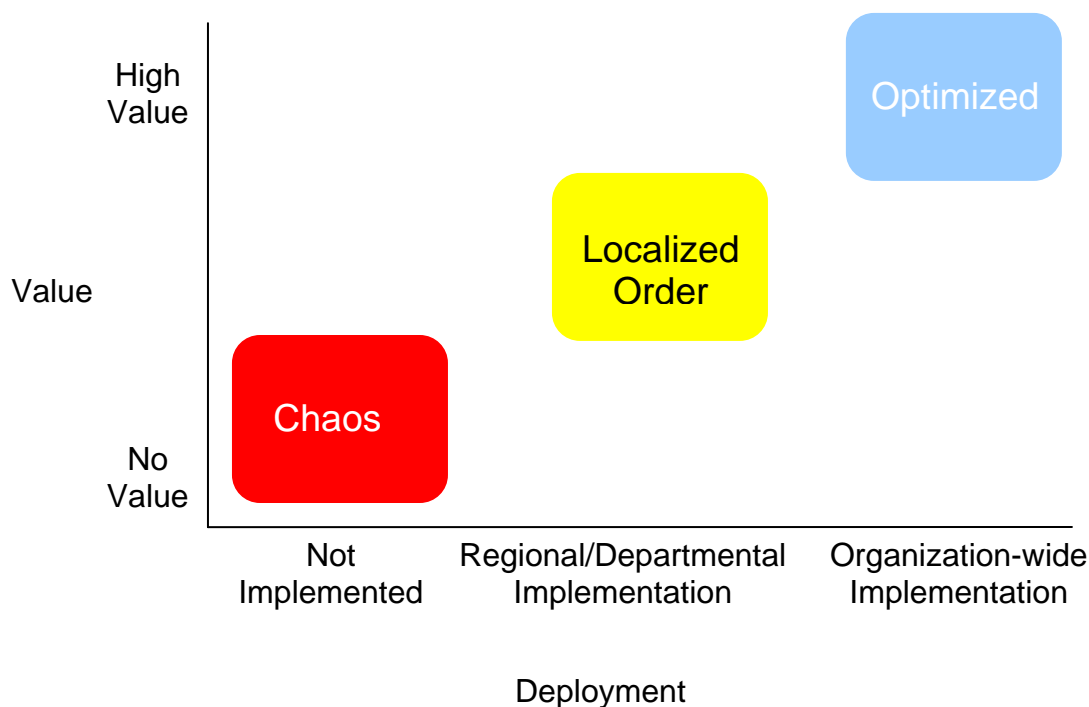
Many companies have invested in the delivery of some sort of log management infrastructure and process. These tools can vary from home grown scripts, to shareware software, to commercially available solutions. Unfortunately many security and network teams are dissatisfied with the solutions they currently have in place for a wide variety of reasons. First, existing solutions may not effectively support the wide spectrum of devices and applications on the network. A major challenge for heterogeneous event management is that log formats are complex, always changing, and lack consistency from vendor to vendor. In addition organizations may struggle with existing solutions because they only collect from a subset of the networked systems which results to incomplete visibility. Second, these tools may not scale to the volume of events that are generated daily resulting in an incomplete picture of the network and security posture. Third, only collecting and storing logs in a central location is only part of the battle. Many organizations that have taken the home grown or shareware route have abandoned the solution because it hasn't delivered the required visibility. Many companies that have made the investment in a commercial product may see some value in their choice, however may be frustrated by the lack of correlation between the different silos of information which can result in a sea of false positives and information overload.

## Compliance Mandates

There's no debating a comprehensive log management strategy provides value to an IT organization. Most regulations and IT security best practice frameworks, that impact organizations today, recognize this value and specifically dictate some form of log collection and auditing. Although some regulations are not as specific as others on the requirements around log management, a comprehensive log management solution should be implemented by any organization that is under any regulatory scrutiny. Appendix A at the end of this document gives a high level overview the log management requirements of some of the well publicized mandates and best practice recommendations. As organizations define their compliance driven IT security objectives, many quickly figure out that a log management solution alone is not sufficient to meet their requirements.

It is evident by some of the emerging regulations and security frameworks, that the guidelines are becoming more specific in their log and security management requirements. An example of a regulation where just log management is not sufficient is the Payment Card Industry – Data Security Standard (PCI-DSS) that requires surveillance into network and application use that can not be extracted from just network and security events.

Regardless off what regulation an organization must adhere to, it is important to assess the usefulness of the log management solution as part of the overall information security and compliance program. The usefulness of a log management solution can be measured by both the value to the organization and how widespread that value is obtained as shown in figure 1.



**Figure 1: Measuring log management value to the organization**

Organizations assessing the effectiveness of their log management program will usually fall somewhere across a spectrum that includes:

**Chaos** – No formalized log management solution has been implemented. The organization may leverage some limited tools, however meeting the tactical security requirements of monitoring and correlating security events is non-existent or extremely manual and the reporting requests of management and auditors go unfulfilled. Organizations in this category spend significantly more time fighting fires than strategic planning.

**Localized order** – A log management solution has been implemented, although only at a regional or departmental level. Alternatively, a company in this category may have implemented a log management solution that does not provide a comprehensive or effective set of log management features. Or, as mentioned earlier the solution may provide visibility into network and security events, but does not provide a deep understanding of application or user identity. Organizations in this position gain some value from their solution, but it is limited.

**Complete order** – A comprehensive log management solution has been implemented company-wide and all constituents across the organization are receiving significant value. The operation teams are receiving value through advanced analysis across all network and security systems which results in the quick isolation of threats. Management is receiving sufficient information to make better network and security decisions, and executives are obtaining the reporting and auditing results needed to meet internal and external information security mandates.

Deployment of a log management solution for meeting compliance mandates is a necessity in today's IT driven organization. Companies should strive to obtain corporate wide value of their technology purchase and make sure their technology investment meets all of the requirements of the business.

## Log Management Technical Considerations

There are many things to consider when an organization is making a decision on a log management solution. A few of these include:

### ***What is the breadth of data collection?***

Computing environments are made up of many disparate IT technologies. These typically include networking products like switches and routers, security solutions like firewalls, intrusion detection and prevention, and vulnerability scanners, operating systems, applications like databases, network and systems management tools, and proprietary applications. An important consideration is how capable is the solution at collecting heterogeneous network and security event data across all networked resources. In addition, it's important to understand if the solution can leverage non-event security management information, including network flow and identity data that may be required to meet security objectives. It is also important to assess how extensible the solution is for supporting proprietary applications and new technologies. Another consideration in this area is how well does the solution "normalize" events of a similar nature across devices from different vendors.

### ***Does the solution scale to my environment?***

Large global organizations generate 10's of millions of events across their network every day. An important log management consideration is whether the solution has the ability to scale to the event load of the organization. A scalable log management solution should provide the ability to distribute the collection load across multiple systems, but at the same time aggregate the monitoring and reporting capabilities in a central console. In addition, one must consider whether the management solution has the ability to support the wide number of users across a broad spectrum of responsibilities including executives, management and operational teams.

### ***Is the architecture secure?***

Many regulatory mandates require that audit logs are maintained in an unaltered state. This means that any log management solution must provide integrity in the log records from the time they are created to the time they are destroyed. Important questions to ask include does the log management solution encrypt the log data any time after it is received by the system. It is also important to ask if the integrity of the log archives is protected with integrity checks including hash functions.

### ***Does the solution provide real time event correlation?***

An effective log management solution should provide a comprehensive and scalable event correlation engine to turn the flood of events generated across the network into actionable information. Some log management solutions will provide limited filtering of events that may provide some value but will result in thousands of incidents that still must be managed.

***Does the solution enable workflow for remediation and compliance?***

Extracting value from network and security information is an important feature of any log management solution. However, understanding what is done after obtaining synthesized results is just as important. It is important to investigate whether the solution can effectively integrate with existing workflow to assist in the remediation of threats as they're uncovered. It is also important to understand how the solution will integrate with an existing security process that has been defined to meet regulatory mandates.

***Does the solution meet any audit requirements of the business?***

A solution that can collect and archive event logs is typically not sufficient to meet the regulatory and reporting requirements of the business. When selecting a log management solution a key consideration is does it integrate with and/or support detailed alert notification, forensics, auditing and compliance reporting. An optimized log management solution will provide reporting capabilities that support the requirements of all individuals across the organization.

## QRadar Solution

QRadar, from Q1 Labs, provides a comprehensive log management framework that includes scalable and secure log management capabilities integrated with real time event correlation, network visibility, threat detection, and compliance reporting.

The QRadar solution provides the ability to distribute log collection across multiple appliances, with a centralized view of the information. The appliance approach provides both unparalleled simplicity in the deployment of log management as well as security that is more difficult to achieve in a software log management solution. Flexible APIs provide the ability to support proprietary devices and applications as well as emerging network and security technologies.

The QRadar advanced monitoring and threat detection capabilities, powered through patent pending event correlation, can quickly turn the sea of events in the organization into a manageable set of actionable items. Through QRadar's correlation, network and security operation teams are quickly notified with meaningful data that enables the delivery of an improved security posture. Core to the event correlation is the ability to normalize events across thousands of network devices, security devices and applications to minimize false positives and improve the ability to recognize significant threats on the network.

Events and logs that are collected by QRadar are archived in a database that has been designed for both efficient storage and fast retrieval of information. The QRadar database enables organizations to archive event log for however long is specified by a specific regulation.

Finally, the reporting capabilities of QRadar offer a wide variety of business and compliance reporting and auditing capabilities to support the security and compliance reporting requirements of the entire organization. The reporting capability is template driven and ships with reports specific to a wide spectrum of regulations and IT best practices.

## QRadar Family – 2 solutions to meet an evolving information security program

An information security management program is constantly evolving for most organizations. When companies are developing their security program they typically need to learn how to crawl, then walk, then jog, and then run. An important first step is the deployment of an effective log management solution that is necessary to gain value from the vast amount of network and security events that are generated on the network. Recognizing that most organizations will continually evolve their log management requirements as part of a security program, Q1 Labs has introduced two solutions that can be implemented in succession as companies requirements mature and more advanced security management capabilities are needed.

There are 2 QRadar solutions that include log management capabilities:

### **QRadar Simple Log Management Information Manager (SLIM):**

QRadar Simple Log Management Information Manager (SLIM) provides a turn key log management solution for organizations that are looking to collect, archive, analyze, and correlate network and security event logs. The solution will assist an organization in getting a handle around many auditing and reporting requirements that are specified by government regulations including PCI, Sarbanes-Oxley, HIPAA, and FISMA. Important features in QRadar SLIM include:

- Heterogeneous network and security event collection
- Easy to deploy and manage appliance based log management solution
- Scalable distributed log collection and archival
- Simple to use policy driven event correlation
- Effective reporting and compliance auditing
- Reliable and tamper proof log storage

### **QRadar Network Security Manager (NSM):**

QRadar NSM is a full featured network security management platform. The solution will assist organizations that have an information security program that has matured to include advanced requirements in the area of advanced threat detection, application monitoring, advanced correlation, and support collection of network and application flow data. QRadar NSM includes all of the features included in QRadar SLIM plus:

- Collection and analysis of network and application flow data
- Collection of identity information provided by corporate directory systems (i.e. LDAP and AD)
- Integrated correlation using a context that has network, application and identity awareness
- Advanced compliance reporting on user application and protocol activity

QRadar SLIM provides a unique solution for organizations looking to deploy a log management solution, but that are not ready for a more comprehensive Network Security Management (NSM) application such as the full QRadar NSM solution. As an organization grows their ability to leverage more advanced features, QRadar SLIM customers can purchase a simple software upgrade that protects their original purchase of solutions from Q1 Labs.

## **Summary**

Organizations of all sizes that are tasked with protecting the information that traverses their network should invest in a log management solution that meets their individual log and security management requirements. There is a lot of excellent information buried in network, security and application event logs that can enable an organization to better protect and optimize the use of the resources. In many businesses corporate wide log management is no longer a nice to have, but rather is mandated by some government regulation. When considering a log management solution it is important to consider how the log data will support important business functions across all levels of the organization including:

- Does the solution integrate into an effective monitoring and threat notification capability to support the day to day operation of the network?

- Does the solution provide the ability to deliver sufficient reporting and auditing required by internal and external regulatory mandates?
- Does the solution provide the security, scalability, and workflow that should be considered with any IT technology decision?

QRadar from Q1 Labs provides an integrated Network Security Management platform that integrates log management with powerful monitoring, event correlation, threat notification, reporting and auditing to meet the requirements of any comprehensive IT security management program.

## Appendix A : Regulatory and IT best practice logging/auditing requirements

Regulation/Best Practice	Industry Represented	Log Management Requirement
Payment Card Industry Data Security Standard (PCI-DSS)	Retail/Finance	<p>Most all major credit card providers, including Visa and Mastercard, are now mandating any merchant and service provider that deals with credit card holder information must implement a security program that complies with the Payment Card Industry Data Security Standard (PCI-DSS).</p> <p>Specific security control areas provided by PCI-DSS that is supported by QRadar's log management capability include:</p> <ul style="list-style-type: none"> <li>➤ Maintaining &amp; building a secure network</li> <li>➤ Protecting card holder data</li> <li>➤ Maintaining a vulnerability assessment program</li> <li>➤ Implementing strong access controls</li> <li>➤ Regularly monitoring and testing networks</li> <li>➤ Maintaining an information security policy</li> </ul>
Health Insurance Portability and Accountability Act (HIPAA)	Healthcare	<p>The health care industry is now under the federal mandates of HIPAA and the "Security Standards for the Protection of Electronic Protected Health Information"</p> <p>Specific security control objectives dictated by HIPAA that are supported by QRadar's log and security management capability include:</p> <ul style="list-style-type: none"> <li>➤ Reduce vulnerabilities (164.308(a)(1)(ii)(B))</li> <li>➤ Information system activity review (164.308(a)(1)(ii)(D))</li> </ul>

		<ul style="list-style-type: none"> <li>➤ Protection from malicious software (164.308(a)(5)(ii)(B))</li> <li>➤ Log in monitoring (164.308(a)(5)(ii)(C))</li> <li>➤ Security incident response and reporting 164.308(a)(6)(ii))</li> <li>➤ Audit controls (164.312(b))</li> <li>➤ Integrity of records (164.312(c)(1))</li> </ul>
Sarbanes-Oxley (SOX)	Public Companies	<p>Section 404 of SOX specifies that an annual report must be delivered that</p> <ol style="list-style-type: none"> <li>1. state the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting; and</li> <li>2. contain an assessment, as of the end of the most recent fiscal year of the issuer, of the effectiveness of the internal</li> </ol> <p>In addition, it mandates an external audit of the procedures used to deliver the report.</p> <p>Although the SOX requirements are relatively broad, organizations under the scrutiny of the regulation must implement an information security program to protect the integrity of financial reports. Any prudent information security program will require a log management framework like the one provided by QRadar.</p> <p>SOX driven security management programs will typically follow a well defined set of control objectives, like CobiT, that requires more than just basic log management. There are many important CobiT control objectives including monitoring and reporting to ensure system security. More detail on this is covered below in the CobiT section of this table.</p> <p>In addition, section 802 of SOX requires supporting materials used in the delivery of the financial reports must be maintained unaltered for 5 years. Many have inferred that log data must also be maintained for the</p>

		same period of time.
Graham-Leach-Bliley Act (GLBA)	Finance	<p>GLBA was enacted by congress and mandates that financial organizations “protect the security, integrity and confidentiality of consumer information. Section 501(b) of GLBA states that organizations must “establish appropriate standards for the financial institutions subject to their jurisdiction relating to administrative, technical, and physical safeguards--</p> <p>(1) to insure the security and confidentiality of customer records and information;</p> <p>(2) to protect against any anticipated threats or hazards to the security or integrity of such records; and</p> <p>(3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer”</p> <p>GLBA driven security management programs will typically follow a well defined set of control objectives, like CobiT, that requires more than just basic log management. There are many important CobiT control objectives including monitoring and reporting to ensure system security. More detail on this is covered below in the CobiT section of this table.</p>
National Institute of Standards & Technology (NIST) North American Electric Reliability Corp (NERC) Critical Infrastructure Protection (CIP) Federal Energy Regulatory Commission	Utilities Manufacturing	<p>The control systems that manage the delivery of utilities (i.e. gas, electricity, water, etc.) and support manufacturing processes are increasingly being scrutinized because of their vulnerability to cyber-terrorism.</p> <p>There are many different control systems, including supervisory control &amp; data acquisition systems (SCADA), that are extremely susceptible to vulnerabilities because of deficiencies in architectures that have evolved over many years that have</p>

(FERC)		<p>lacked a focus of providing security controls.</p> <p>With increased use of off the off the shelf server technologies in control systems, concern over potential vulnerabilities have increased resulting in emerging security best practices and regulations focused on tightening security for control systems that, if compromised, could cause a catastrophe.</p> <p>Multiple standards have emerged including the NERC Cyber Security Standards for Critical Information Protection (CIP) that outlines 8 areas of security control:</p> <p>Specific security control objectives dictated by NERC CIP that is supported by QRadar's log and security management capability include:</p> <ul style="list-style-type: none"> <li>➤ (CIP-001-1) Sabotage Reporting</li> <li>➤ (CIP-002-1) Critical Cyber Asset Identification</li> <li>➤ (CIP-003-1) Security Management Controls</li> <li>➤ (CIP-005-1) Electronic Security Perimeter(s)</li> <li>➤ (CIP-007-1) Systems Security Management</li> <li>➤ (CIP-008-1) Incident Reporting and Response Planning</li> </ul>
CobiT	All	<p>There are multiple areas of CobiT that specify that optimal security is only achieved through "an organization wide continuous improvement program that takes into account lessons learned and industry best practices for internal control monitoring" (ME2: Monitor and Evaluate Internal Controls).</p> <p>Specific security control objectives dictated by CobiT that are supported by QRadar's log and security management capability include:</p>

		<ul style="list-style-type: none"> <li>➤ DS3 – Manage Performance &amp; Capacity</li> <li>➤ DS4 – Ensure Continuous Service</li> <li>➤ DS5 – Ensure Systems Security</li> <li>➤ DS6 – Identify and Allocate Costs</li> <li>➤ DS8- Manage Service Desk &amp; Incidents</li> <li>➤ DS9 – Manage the Configuration</li> <li>➤ DS10 – Manage Problems</li> <li>➤ ME1 – Monitor and Evaluate IT Performance</li> <li>➤ ME2 – Monitor and Evaluate Internal Control</li> <li>➤ ME3 – Ensure Regulatory Compliance</li> <li>➤ ME4 – Provide IT Governance</li> </ul>
<p>ISO 17799 Information technology- Security techniques – Code of practice for information management</p>	<p>All</p>	<p>Similar to CobiT, many areas of ISO 17799 benefit from a log and security management solution like QRadar.</p> <p>Specific security control objectives dictated by ISO 17799 that are supported by QRadar’s log and security management capability include:</p> <ul style="list-style-type: none"> <li>➤ Section 5 - Defining a security policy</li> <li>➤ Section 7 – Asset management <ul style="list-style-type: none"> <li>○ 7.1.1 Discovery and inventory of assets</li> <li>○ 7.1.3 Acceptable use of assets</li> <li>○ 7.2.1 Classification guidelines</li> </ul> </li> <li>➤ 10 Communications and operations management <ul style="list-style-type: none"> <li>○ 10.1.3 Segregation of duties</li> <li>○ 10.4.1 Protection against malicious code</li> <li>○ 10.6 Network security management</li> <li>○ 10.6.1 Network controls</li> <li>○ 10.8.1 Information exchange policies and procedures</li> <li>○ 10.8.5 Business information systems</li> <li>○ 10.10 Monitoring</li> <li>○ 10.10.1 Audit logging</li> </ul> </li> </ul>

		<ul style="list-style-type: none"><li>○ 10.10.2 Monitoring system use</li><li>○ 10.10.3 Protection of log information</li><li>○ 10.10.4 Administrator and operator logs</li><li>○ 10.10.5 Fault logging</li><li>➤ 11.1.1 Access control policy</li><li>➤ 11.5.1 Secure log-on procedures</li><li>➤ 12.6.1 Control of technical vulnerabilities</li><li>➤ 13.1.1 Reporting information security events and weaknesses</li><li>➤ 13.2 Management of information security incidents</li><li>➤ 13.2.3 Collection of evidence</li></ul>
--	--	--