The Business Case for a Next-Generation SIEM:

Delivering operational efficiency and lower costs through an integrated approach to network security management

Q1Labs.com

Executive Overview

The selection of the most effective IT technology is a major concern for companies of all sizes, across almost every industry. In the current economic climate, organizations face the difficult task of prioritizing where to best spend their limited budgets so that they emerge from these uncertain times as strong, viable companies.

Feeling this pain most acutely are those who deliver critical network services and applications. Despite adverse economic conditions, they must still meet a variety of requirements, such as:

- Meeting evolving and increasing numbers of regulatory mandates
- Securing IT assets from continually evolving threats
- Delivering security controls for existing and emerging technology solutions

There will be difficult, economically-driven choices to be made, and organizations need to be strategic in selecting the solutions they will deploy.

Challenge: Regulatory Burdens Will Grow

Over the last few years the burden of regulatory compliance has grown significantly and affected nearly every industry. The list of regulations is long and the potential penalties for non-compliance are significant. This list includes:

- Payment Card Industry Data Security Standard (PCI-DSS)
- Health Insurance Portability and Accountability Act (HIPAA)
- Sarbanes-Oxley (SOX)
- Gramm-Leach-Bliley Act (GLBA)
- North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP)
- Federal Information Security Management Act (FISMA).

Many of these regulations continue to evolve with significant impact across organizations.

Penalties for non-compliance vary from industry to industry. However, a common thread across all industries is that non-compliance can significantly impact the bottom line. As the financial penalties and inherent security risk have become easier to quantify, organizations have become more acutely aware of the risks and costs of non-compliance. Conventional wisdom dictates that organizations “do the right thing” and implement common sense controls to best protect corporate IT assets − not only to meet regulatory requirements, but also to protect mission-critical business data.

Challenge: Network Threats Will Increase

Security professionals are keenly aware of the growing risk of threats from both inside and outside the organization. News stories have emerged about complex and sophisticated crime operations that are behind some of the more significant breaches that have occurred. And the lengths to which criminals have gone to steal computer-based information in the past few years are almost unimaginable. As a result, significant resources have been invested to investigate and respond to major security breaches that have compromised millions of confidential records, including credit card data, healthcare information, and proprietary intellectual property.

> "It's official: Today's security managers are more worried about insiders leaking sensitive corporate data than they are about outsiders breaking in to steal it."
>
> Source: Dark Reading, March 2009

The ramifications of any network security breach to an organization are far-reaching, and post-breach cleanup costs are significant. Organizations need to be prudent and implement proper security controls that will put them ahead of criminals and provide the ability to detect complex, integrated attacks on their networks.

Challenge: Operational Costs Continue to Escalate

An ongoing challenge to IT organizations is that networks are in a constant state of change. New technologies arrive as old technologies depart. Organizations must continually assess how new technologies impact their IT security program and ensure the proper controls are in place to meet the security requirements of the business.

In a challenging economic climate, organizations must look to solutions that not only meet the security requirements of their business, but also reduce overall costs.

In their report titled "Worldwide Security 2009 Top Ten Predictions: Security Trends," Industry research firm IDC predicts:

> "Although 2008 was tumultuous, the security market maintained its historically strong growth. In 2009, security products should be able to weather the economic uncertainty because threats are not going on holiday during this time, compliance requirements will probably grow, and businesses will be looking for security to enable technologies that can reduce costs."

Compounding the issue are operational challenges that many organizations currently face, including:

- A need to provide better collaboration between network and security teams, often leading to operational convergence
- Budgetary constraints across IT departments resulting in the need to deploy tools that streamline operations and lower overall cost
- Lack of staff expertise which requires the selection of tools that minimize the need for advanced training and skill sets

There is no doubt that organizations will need to be extremely selective in the acquisition of new technologies. One technology specifically cited in the aforementioned IDC report is *automated security management*.

The Solution

Q1 Labs is a global provider of high-value, cost-effective network security management products. The company's next-generation security information and event management (SIEM) offering, QRadar, integrates functions typically segmented by first generation solutions − including log management, SIEM and network activity monitoring − into a total security intelligence solution. QRadar provides users with crucial visibility into what is occurring with their networks, data centers, and applications to better protect IT assets and meet regulatory requirements. By deploying QRadar, organizations greatly enhance their IT security programs and meet the following specific security requirements.

Compliance Management – Out-of-the-box Compliance Content without Sacrificing Security

Recognizing that compliance with a policy or regulation often works on a sliding scale, QRadar provides:

- **Accountability:** Proving who did what and when
- **Transparency:** Providing visibility into the security controls, the business applications, and the assets that are being protected
- **Measurability:** Metrics and reporting around risk within a company

A monitoring and management solution that spans the network and security technologies in your environment plays a key part in supporting and validating compliance initiatives. QRadar brings to enterprises, institutions, and government agencies the accountability, transparency, and measurability that are critical to the success of any IT security program tasked with meeting regulatory mandates.

Customer Example

Profile:	Worldwide Food Franchiser
Environment:	1000+ remote locations monitored for PCI compliance validation Internal security infrastructure also monitored for centralized threat management
Results:	***Effective validation of PCI compliance efforts; QRadar subsequently replaced existing SIEM solution***

> "S1's goal was to meet the PCI DSS compliance mandate and replace a system that required too much work to maintain. Under severe time constraints, Q1 Labs' QRadar enabled S1 to deploy and implement a solution in an efficient and straightforward fashion..."
>
> ***S1, Inc. Case Study***

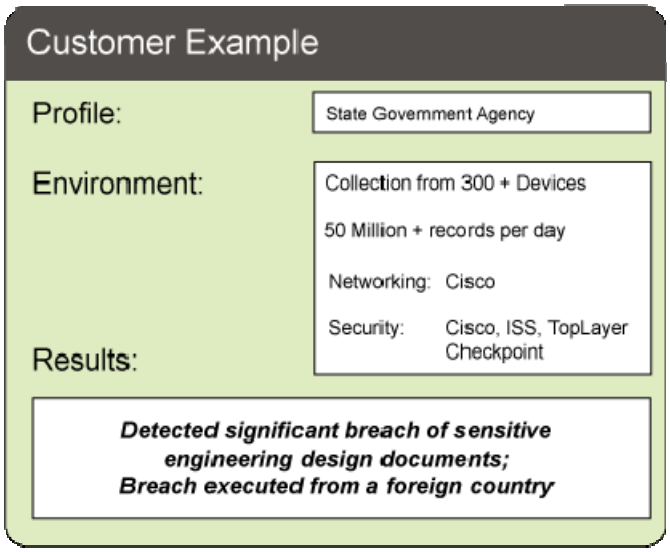
Specific benefits of a QRadar compliance management solution include:

- Out-of-the-box compliance reports to assist meeting specific regulations, including PCI, HIPAA, NERC, GLBA, and SOX
- An easy-to-use reporting engine that does not require advanced database and report writing skills, resulting in an improved ability of staff to produce required compliance reports
- Delivery of compliance workflow and security controls, resulting in decreased financial risk to the organization for non-compliance

For more information on how QRadar addresses specific regulations, please read the White Paper, "How QRadar Addresses Regulatory Compliance Requirements," available at www.Q1labs.com.

Threat Management – Detecting Complex External Attacks and Internal Fraud That is Otherwise Missed

Information-centric organizations continue to struggle to stay ahead of the evolving threat landscape. Traditional security information and event management solutions fall short because they lack truly broad surveillance. As a result, they cannot piece together all the information necessary to effectively correlate and detect threats. To detect more complex threats like fraud, it is important to leverage the available information across all deployed network and security solutions to enable improved correlation between network and security operational teams.



QRadar's threat management features bridge the gap between network and security operations and deliver the requisite surveillance on the network to detect today's more complex and sinister IT-based threats. Most of the existing SIEM solutions available today might turn millions of events into thousands of correlated alerts. Unfortunately, those thousands of alerts still need to be manually analyzed and correlated. QRadar takes traditional correlation one step further by helping to connect the dots across the entire infrastructure. It delivers to security operators a manageable and prioritized list of the most significant security threats that must be addressed, along with the information necessary to remediate the situation.

"Without QRadar, identifying the source of the problem would take a fleet of guys going through the logs."

Liz Claiborne, Inc.*

"If we didn't have QRadar to help analyze the mountains of application traffic coming into and out of our company network, it would have been nearly impossible to identify the anomalies that the company viewed as threats."

Gordon Food Service Case Study

* Wall Street Journal, "Looking for Trouble: SIEM Software Combs Log-in Records For Signs of Intruders," Michael Totty, 10/27/2008

Specific benefits of a QRadar threat management solution include:

- Integration of all relevant network and security data, enabling improved recognition of threats and reducing false positives
- Powerful security intelligence, including behavior analysis, which detects threats missed by other solutions
- Industry-leading event correlation, resulting in the detection of security incidents with pinpoint accuracy (down to the end-user in the case of internal fraud), thereby minimizing efforts of staff to manage security incidents

For more information on how Q1 Labs helps organizations detect threats missed by other solutions, please read the White Paper, "A Proactive Approach to Battling Today's Complex Network Threats," available at www.Q1labs.com.

Customer Example

Profile:	Fortune 500 Retailer
Environment:	27 locations monitored for PCI & SOX compliance 900 devices under management
Results:	140 million records per day

Detection (and successful forensic prosecution) of attempted intellectual property theft by trusted internal user

QRadar Improves Operational Efficiencies and Lowers Costs

In the absence of a centralized security management solution, organizations must rely on a set of processes that are labor intensive, reactive, and prone to missing potentially harmful security incidents. In addition, organizations that are affected by one or more compliance regulation, but lack a centralized log management and/or SIEM solution, run the risk of not being able to validate compliance efforts or pass compliance audits. The QRadar security information and event management solution helps reduce costs and provides multiple areas of operational improvement.

Customer Example

Profile:	Fortune 50 Energy Organization
Environment:	Enterprise-wide security management across 3000 + devices
Results:	

QRadar is the lynchpin of organization's security incident response

Improved operational efficiency
QRadar enables doing more with less

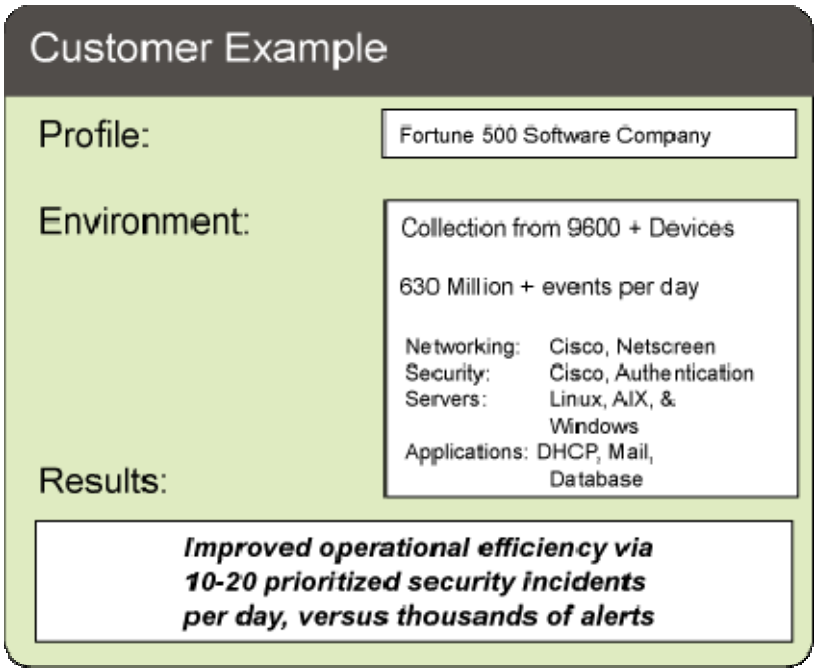
QRadar is the foundation for validating a diverse set of compliance mandates including: PCI, SOX, and NERC

"Our saving grace is that, with QRadar, we can easily respond to issues which would previously have gone unnoticed. We do our best, but when you have limited security resources, with more than 10K hosts on a normal day, it's virtually impossible to find and address all issues. QRadar provides us with a prioritized ranking of what needs to be addressed first based on how important a host is, the severity of an event, and how credible the event is."

Wayne State University Case Study

Log Management – Billions of Events Distilled into Tens of Prioritized Incidents

QRadar's comprehensive security management framework includes the ability to deliver scalable and secure log management capabilities across all networked systems and applications. While it is imperative to collect and store all original data that is relevant for your log, threat, and compliance initiatives, nobody can possibly sift through all of this information to spot and solve problems. Distilling and prioritizing millions of event records down into a handful of actionable offenses is the key value of a solution like QRadar. QRadar provides intelligent reduction of all of the information collected through integrated real-time event correlation, threat detection, compliance reporting and auditing. QRadar provides a complete log management solution for organizations tasked with collecting, retaining, and managing event logs in their environment.



"The advantages to using QRadar were overwhelming. Not only did the system come with a pre-installed set of log management capabilities, but the offering was also flexible and easily programmable so that we could modify the existing rules, or simply use the rules wizard to create new ones."

S1, Inc. Case Study

Specific benefits of a QRadar log management solution include:

- Automated collection and management of event logs across the entire organization, helping to minimize traditionally manual tasks
- Powerful event analysis and forensics search of archived logs, enabling fast investigation of security incidents and meeting specific compliance audit requirements
- Secure log management features to ensure the integrity of collected event logs
- Solution scales from organizations with 50 events per second to 300,000 events per second

For more information on how Q1 Labs helps organizations implement centralized log management, please read the White Paper, "Leveraging Log Management to Boost Enterprise IT Security," available at www.Q1labs.com.

Three Solutions In One

QRadar combines log management, security information and event management, and network behavior analysis in a single solution. Not only is there a decrease in cost of ownership, cost of deployment, and cost of operation, but the intersection of all of QRadar's surveillance feeds (logs, events, and network flows) actually yields more accurate data for an operator, more granular forensics for an incident response manager, and more complete reporting for auditors.

Network and security teams are converging, or at the very least collaborating, in all types of enterprises. Delivering visibility that matches this operational convergence, while enabling full monitoring capabilities across the network and security fabric, is a key value proposition for the QRadar solution.

Automation of Manual Tasks

Core to QRadar are its log management features that automate the collection and analysis of information across the entire IT infrastructure. QRadar provides support for hundreds of heterogeneous systems, including network solutions, security solutions, servers, hosts, operating systems, and applications. The solution is easily extended to support proprietary applications and new systems that are deployed as the IT landscape changes. Further automation includes powerful, real-time correlation that prioritizes security incidents for security operators and detailed auditing and reporting to meet the security information needs of regulatory auditors and security professionals.

Optimizing Staff Efficiency

Most IT staffs are already stretched to their limits, and this condition is unlikely to change any time soon. There are many areas in which QRadar improves the operational efficiencies of IT personnel. Traditionally, the task of collecting and managing event logs was extremely manual. QRadar delivers significant automation to log management across an entire heterogeneous network, without the need for advanced training. The ability of QRadar to prioritize network-based threats helps optimize staff efforts to effectively manage potentially harmful threats to the organization. The robust, out-of-the-box capabilities of QRadar minimize the time and effort needed to manage the security management solution, freeing up time for other important security projects.

Supporting Future Growth

The architecture, packaging, and out-of-the-box features of QRadar mean that the solution is uniquely capable of scaling from the largest, Fortune 10-sized corporations with thousands of devices and millions of events per day, to small colleges, hedge funds, and regional utilities whose logging, monitoring, and analysis needs can be met with a single appliance.

A comprehensive security management program typically develops and grows over time. In many cases, an organization will implement a log management solution at the outset to meet a specific security or compliance objective, but will quickly evolve that initiative to require advanced capabilities.

The QRadar family of security information and event management solutions provides a comprehensive migration path that can align with the maturity of an organization's network security management program, and easily supports growth from an initial project to a large, distributed global deployment.

> "When my CEO or CIO approach me and ask about network issues, I can quickly describe the problem and provide accurate traffic updates. I look smart, my team looks smart, and everyone benefits. Our QRadar investment was well worth the money spent. It was actually a bargain when compared to all other solutions we evaluated."
>
> ***UDR, Inc. Case Study***

Conclusion

The job of delivering an effective IT network security management program is not trivial for organizations. The motivation for improving overall IT security comes from many directions, including operational improvements and compliance mandates, but all lead in the same direction – protecting IT assets from those that wish to do them harm. Historically, organizations have invested in many point solutions in an attempt to mitigate specific IT risks. Moving forward, organizations need to look at ways to capitalize on their existing investments and integrate the value from the information that these solutions already provide.

Q1 Labs' next-generation security information and event management solution, QRadar, provides organizations with improved operational efficiencies and the ability to lower costs through an integrated approach to network security management, which provides unique and differentiated value in the areas of log management, threat management, and compliance management.

890 Winter Street
Suite 230
Waltham, MA 02451 USA

Telephone: 781.250.5800
Fax: 781.250.5880
Email: info@Q1Labs.com
Web: Q1Labs.com

WP052609B

Q1 Labs is a global provider of high-value, cost-effective, security information and event management (SIEM) products. The growing company's flagship offering, QRadar, integrates previously disparate functions – including log management, network behavior analytics, and security event management – into a total security intelligence solution. QRadar provides users with crucial visibility into what is occurring with their networks, data centers, and applications to better protect IT assets and meet regulatory requirements. Q1 Labs' customers include healthcare providers, energy firms, retail organizations, utility companies, financial institutions, government agencies, and universities, among others.