



QRadar 6.1 Data Sheet

Q1 Labs™ flagship solution QRadar™ is unrivaled in its ability to provide an organization centralized IT security command and control. The unique capabilities of QRadar stem from its ability to manage all relevant network and security information required to effectively manage and monitor a company's security posture.

QRadar's integrated approach, in conjunction with unparalleled data collection, analysis, correlation and auditing capabilities, enables organizations to quickly and easily implement a corporate wide security management program that delivers security best practices including:

- Log management—Manage all relevant network and security data
- Threat management—Detect threats others miss
- Compliance management—Deliver repeatable compliance security process

Key Features:

Centralized command and control console

- ✓ Integrated log management, security information and event management (SIEM), and network behavior analysis in a single console reduces security management solution acquisition costs and improves IT efficiency

Network, security, application, & identity awareness

- ✓ Converged management of network events, security events, network and application flow data, vulnerability data, and identity information greatly improves ability to meet IT security objectives.

Advanced threat and security incident detection

- ✓ QRadar's unique "offense" management significantly reduces false positives and detect threats that other security solutions miss

Compliance-driven reporting capabilities

- ✓ QRadar provides compliance-centric reporting that enables the delivery of IT best practices which support compliance initiatives

Scalable distributed log collection and archival

- ✓ QRadar's distributed appliance architecture scales to provide event and flow log management in any enterprise network



The Nexus of Security and Networking

QRadar Enables a Repeatable Security Process including:

Log Management

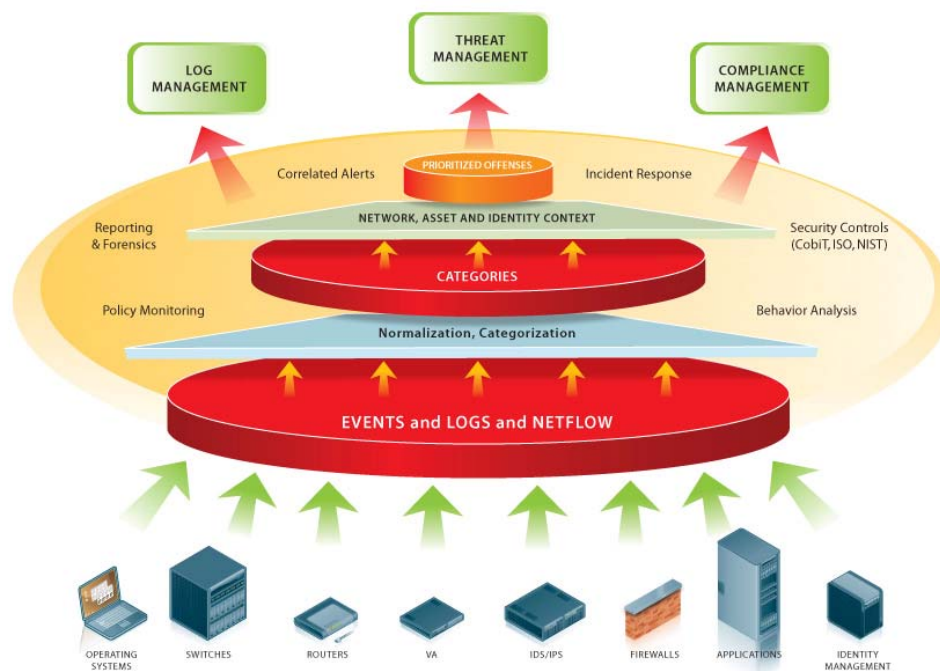
QRadar provides a comprehensive log management framework that includes scalable and secure log management capabilities integrated with real time event correlation, policy monitoring, threat detection, and compliance reporting.

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 simplicity in the deployment of log management and 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.

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 logged data. The QRadar database enables organizations to archive event and flow logs for however long is specified by a specific regulation. QRadar appliances can be easily integrated into an existing storage infrastructure for log term log retention.

Log Management Benefits

- ✓ Supports secure event & flow log collection & storage
- ✓ Provides integrated real-time correlation and historical auditing from log data
- ✓ Leverages scalable distributed appliance model
- ✓ Delivers extensible device support across network and security devices



Threat Management

The QRadar network security management solution, from Q1 Labs, takes an innovative approach to managing computer based threats in the enterprise. Recognizing that discrete analysis of security events is not enough to properly detect threats; QRadar was developed to provide an integrated approach to threat management that combines the use of traditionally silo'd information to more effectively detect and manage today's more complex "threats". Specific information that is collected:

Network events:

Includes events generated from networked resources including switches, routers, servers and desktops.

Security logs:

Includes log data generated from security devices like firewalls, VPNs, intrusion detection/prevention, anti-virus, identity management, and vulnerability scanners.

Host and application logs:

Includes log data from industry leading host operating systems (Microsoft Windows, UNIX, and Linux) and from critical business applications (authentication, database, mail and web)

Network and application flow logs:

Includes flow data generated by networking devices from vendors including Cisco, Juniper, Foundry, HP, and Extreme. Information provides the ability to build a context of network and protocol activity.

User and asset identity information:

Includes information from commonly used directories including Active Directory and LDAP.

Incorporating patent pending "Offense" management technology this integrated information is normalized and correlated by QRadar resulting in automated intelligence to quickly detect, notify and respond to threats missed by other security solutions with isolated visibility.

Threat Management Benefits

- ✓ Provides 100's of out-of-the box correlation rules
- ✓ Provides advanced threat intelligence that is network, application & identity aware
- ✓ Delivers prioritization of events through "offense" management
- ✓ Delivers extensible methods for incident resolution

Figure 2: QRadar Threat Management Process



Compliance Management

Organizations of all sizes across almost every vertical market face a growing set of requirements from IT security regulatory mandates.

Recognizing that compliance with a policy or regulation will evolve over time, many industry experts recommend a compliance program that can demonstrate, and build upon, these key factors:

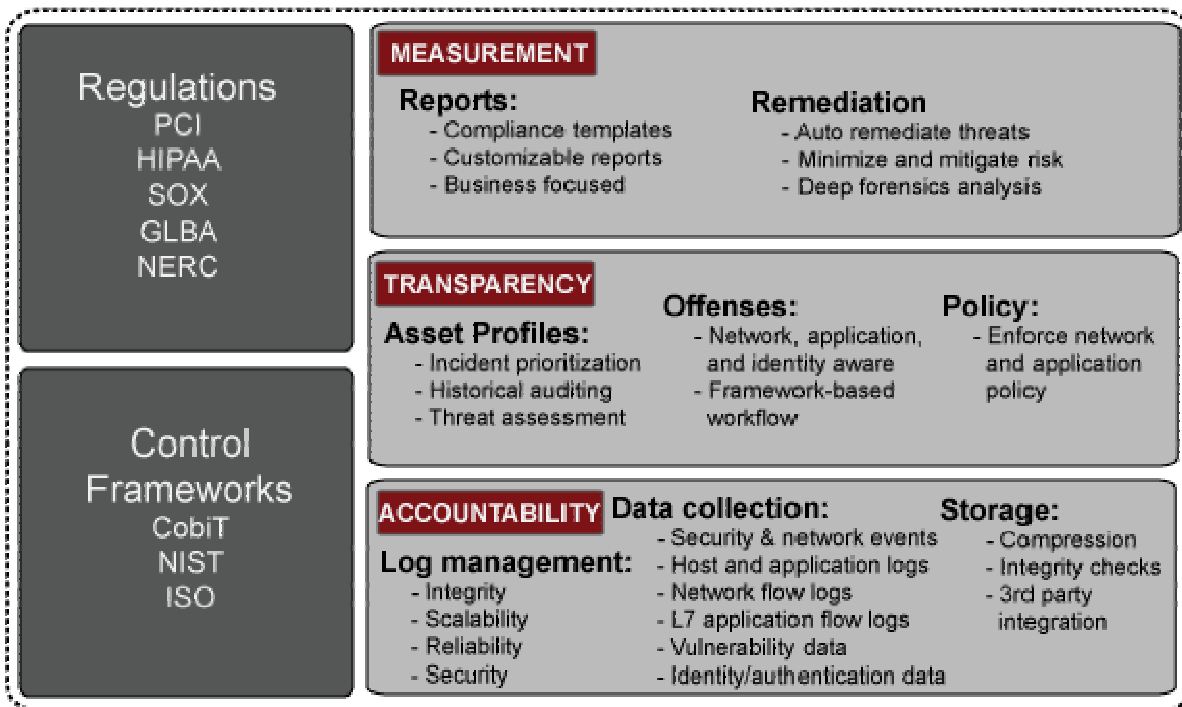
Accountability: Proving surveillance to report on who did what and when

Transparency: Providing visibility into the security controls, the business applications and the assets that are being protected

Measurability: Metrics and reporting around IT risks within a company

Although no magic tool exists to enable all aspects of compliance, QRadar's ability to provide centralized command and control for existing network and security investments across the entire IT infrastructure can play a key role in supporting compliance initiatives. Figure 2 provides an overview of the areas of compliance that QRadar Network Security Management brings to enterprises, institutions and agencies that are required to establish a comprehensive IT security program to meet specific regulatory mandates.

Figure 3: QRadar Compliance Support



QRadar provides reporting and alerting workflow for the following Control Frameworks:

- Control Objectives for Information and related Technology (CobIT)
- International Organization for Standardization (ISO) ISO/IEC 27002 (17799)
- Common Criteria (CC) (ISO/IEC 15408)
- NIST special publication 800-53 revision 1 & FIPS 200

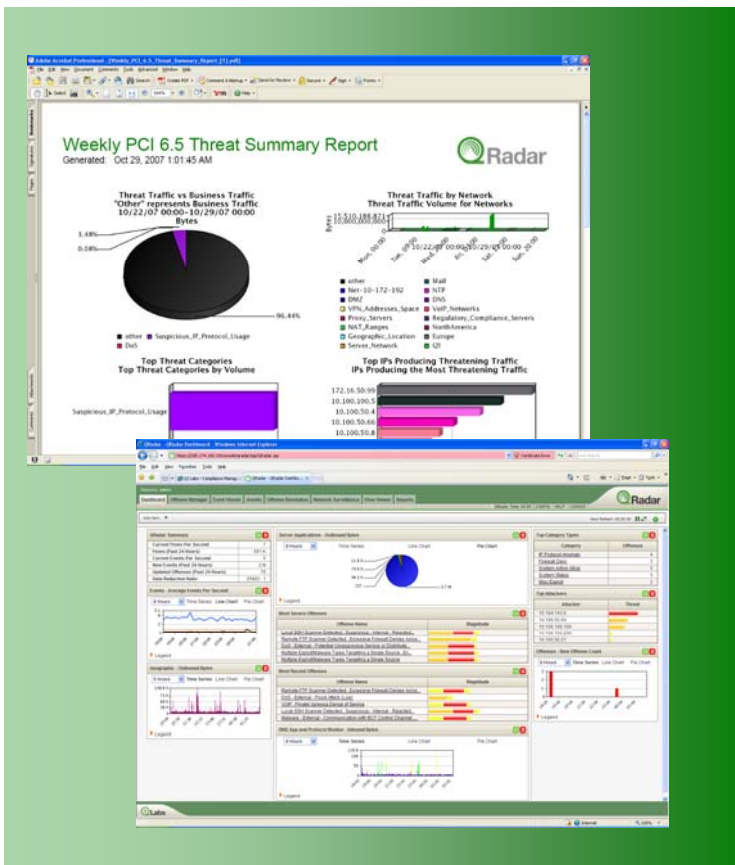
QRadar supports compliance focused workflow for the following Regulations:

- Payment Card Industry Data Security Standard (PCI-DSS)
- Health Insurance Portability and Accountability Act (HIPAA)
- Sarbanes-Oxley (SOX)
- Graham-Leach-Bliley Act (GLBA)
- Federal Information Security Management Act (FISMA)

Compliance Management Benefits

- ✓ Provides 100's of out-of-the box compliance reports
- ✓ Enables repeatable compliance monitoring, reporting and auditing process
- ✓ Supports multiple regulations and security best practices
- ✓ Delivers extensible features for advanced compliance requirements

Figure 4: Sample QRadar Compliance Monitors & Reports



- Failed server logon
- Successful server logon/logoff
- Failed application logon
- Successful application logon/logoff
- Configuration changes
- User protocol activity
- Vulnerabilities
- Attacks
- Administrative activity
- DMZ activity
- Trusted protocols
- Risky protocols
- Remote access
- Network Health

Supported Devices

QRadar SLIM supports log management for a wide variety of network and security devices including

- ✓ Routers/Switches, including network flow data
- ✓ Firewalls
- ✓ Virtual Private Networks (VPNs)
- ✓ Intrusion Detection/Prevention Systems (IDS/IPS)
- ✓ Vulnerability Scanners
- ✓ Anti-virus applications
- ✓ Host & servers
- ✓ Database, mail, and web applications
- ✓ Custom devices and proprietary applications
- ✓ QRadar application flow collectors

Please contact your Q1 Labs representative or visit www.q1labs.com for the most up-to-date list of supported devices.

For more information on the QRadar family of appliances download the QRadar Appliance Family Datasheet from www.q1labs.com.



The Nexus of Security and Networking

Copyright © 2007 Q1 Labs Inc. All rights reserved. Q1 LABS, the Q1 Logo, QRADAR and the QRADAR Logo are trademarks or registered trademarks of Q1 Labs Inc. All other trademarks and service marks are the property of their respective owners. Specifications are subject to change without notice.

Corporate Headquarters

Q1 Labs Inc.
890 Winter Street
Suite 230
Waltham, MA
02451 USA

Telephone 781.250.5800
Fax 781.250.5880