



# QRadar Security Intelligence Platform

No matter how large or small an organization, the demands for security intelligence are growing. Compliance mandates are on the rise and data threats and breaches continue to challenge organizations. All of this is compounded by the huge amounts of data and events generated by an ever increasing number of users and devices. Without finding new ways to stay on top of it, an organization will be left vulnerable. Security Intelligence isn't just nice to have—it's a necessity.

## Total Intelligence & Visibility For Today's Security Challenges

Q1 Labs is a global provider of high-value, cost-effective next-generation security intelligence products. The company's flagship product, the QRadar Security Intelligence Platform, integrates previously disparate functions — including SIEM, risk management, log management, network behavior analytics, and security event management — into a total security intelligence solution, making it the most intelligent, integrated and automated security intelligence solution available. 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.

Thousands of worldwide customers have chosen the QRadar as the most intelligent, integrated and automated security intelligence solution available. QRadar allows businesses to:

### Detect Threats Others Miss

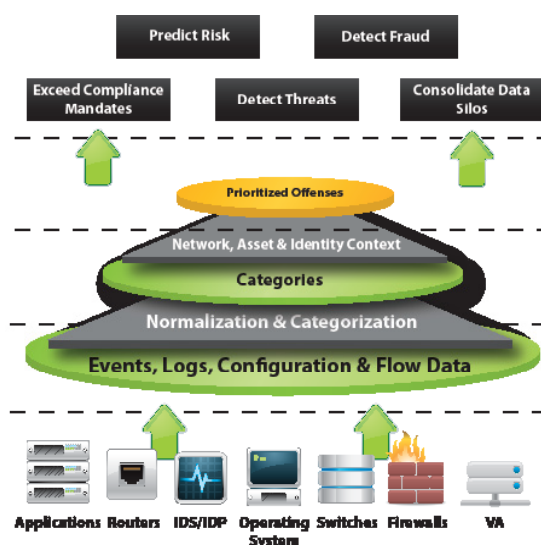
Internet-based threats and fraud continue to get more sophisticated. Intelligence is hidden in an organizations' data which can detect alarming problems that range from employees stealing proprietary information to botnets trying to break in to steal credit card information or international espionage. QRadar helps identify the high priority offenses against your corporate data and detect anomalies in user, application and network behavior.

### Consolidate Data Silos

With many companies generating millions or billions of records and events every day, a wealth of information exists in the event and log data generated by existing network devices. Unfortunately, this information is frequently in silos, often ignored and always under-utilized. QRadar converges the previously distinct network, security and operations views of the infrastructure into a sensible yet scalable intelligence platform. This lets an organization quickly respond to what is important and distill network and security information down to the identity and application awareness level to better and more efficiently resolve network threats and policy infractions.

### Detect Insider Fraud

Some of the biggest threats to an organization come from the inside and companies often lack the intelligence necessary to accurately link individuals to incidents of



Delivering Total Security Intelligence

## QRadar Security Intelligence Platform

malicious behavior. With user and application monitoring, organizations can baseline normal user activity making it easier to identify abnormal or risky behavior and weaknesses.

### Predict Risks Against Your Business

Security and IT teams are constantly challenged to better manage risk across an ever-growing spectrum of vulnerabilities before a breach actually occurs. QRadar provides a pre-exploit solution that allows for not only assessing what risks exist during and after an attack, but also answer many "What if?" questions ahead of time, which can greatly improve operational efficiency and reduce network security risks.

### Exceed Regulation Mandates

Companies today are under growing executive pressure to comply with mandates such as Sarbanes-Oxley, GPG-13, FSA, Garante, HIPAA, FISMA, GLBA, PCI, NERC. The massive amounts of data and events being generated in an organization provide the keys to the audit trail. QRadar's collection correlation and integration of all surveillance feeds yields more accurate data for an operator, more granular forensics for an incident response manager, and more complete reporting for auditors.

### Intelligent, Integrated and Automated

The QRadar Security Intelligence Platform provides a unified architecture for collecting, storing, analyzing and querying log, threat, vulnerability and risk related data. Because QRadar is a highly intelligent, integrated and automated solution, organizations benefit by having several departments and staff with a variety of roles (operators, analysts, auditors, etc) and needs seamlessly using different QRadar modules.

#### Intelligent

With more data under surveillance and more intelligent analytic techniques, QRadar will detect threats that others will miss; it will provide visibility that others can't.

#### Integrated

Designed from scratch to integrate Log Management, SIEM and Risk Management in one solution it will deliver massive log management scale without any compromise on SIEM "Intelligence."

- ▶ A common platform for all searching, filtering, rule writing, and reporting functions
- ▶ A single intuitive user interface for all log management, risk modeling, vulnerability prioritization, incident detection and impact analysis tasks

#### Automated

QRadar is simple to deploy and manage with automated security and network device discovery as well as compliance and policy functions. By automating tedious discovery and tuning functions QRadar removes the crushing complexity that cripples traditional security intelligence platforms.



## Gartner

Q1 Labs in Leaders Quadrant of 2011  
Gartner SIEM Magic Quadrant Report

Q1 Labs, an IBM company  
890 Winter Street, Suite 230  
Waltham, MA 02451 USA  
1.781.250.5800, info@Q1Labs.com

Copyright 2011 Q1 Labs, an IBM company. All rights reserved. Q1 Labs, the Q1 Labs logo, Total Security Intelligence, and QRadar are trademarks or registered trademarks of Q1 Labs, Inc. All other company or product names mentioned may be trademarks, registered trademarks, or service marks of their respective holders. The specifications and information contained herein are subject to change without notice.

DSQRSIPOV1111