



QRadar Security Management Appliances

Q1 Labs' QRadar™ network security management appliances and related software provide enterprises with an integrated framework that combines typically disparate network and security information into a single, comprehensive solution. QRadar's unique approach enables organizations to deliver an unparalleled set of network security management services, including: log management, threat management, and compliance management.

QRadar also makes possible a repeatable security process to improve operational efficiencies, better protect IT assets from a complex landscape of threats, and assists meeting a wide array of regulatory mandates.

By using the high-value, cost-effective QRadar family of products, IT operations and security professionals greatly benefit from simple deployments, quick implementations, and improved security.

QRadar's Security Intelligence Platform

Provides a unified architecture for collecting, storing, analyzing and querying log, threat, vulnerability and risk related data.

Intelligent

With more data under surveillance and advanced analytic techniques, QRadar provides unparalleled visibility into network and application activity that others cannot.

Integrated

Correlating information from security logs, network flow analysis, the application layer, IAM solutions, and asset-based vulnerability assessments into one, comprehensive security management solution.

Automated

Simple to deploy and manage, QRadar automates security and network device discovery as well as compliance and policy functions.

Key features and benefits

Delivers centralized log management

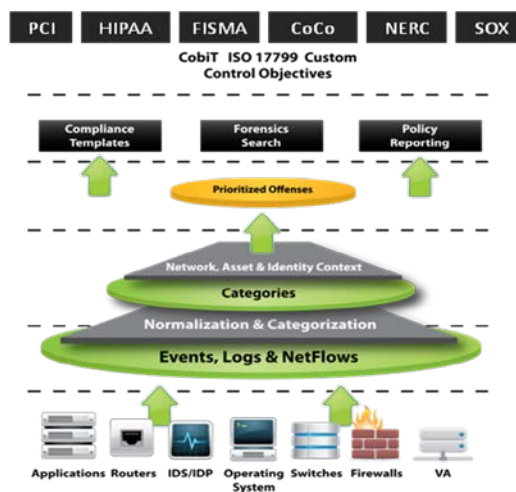
- Prioritizing millions of events and network flows into several actionable offenses
- Providing integrated analysis of network and security information
- Integrating information that provides identity and application awareness for quickly resolving network threats and policy infractions.

Detects threats that others miss

- Integrates network, security, and identity information to pinpoint threats that other security management products would miss
- Employs unrivaled data analysis that decreases time to detect and respond
- Leveraging application flow data to detect inappropriate use of networked applications and protocols.

Compliance automation

- Over 3,500 out-of-the-box reports and rules templates to address your industry compliance requirements.
- Automated device discovery and data collection identifies and profiles assets, and provides identification of noncompliance risks in your network.



The QRadar 2100 All-In-One Appliance

Combines the features and functionality of QRadar's enterprise security software in a single appliance. The QRadar 2100 provides an integrated security solution that is fast and easy to deploy. With its intuitive Web-based user interface, configuration is so simple that you can get a QRadar 2100 appliance up and protecting the network in minutes.

The QRadar 2100 Appliance includes an embedded version of Q1 Labs' QFlow Collector, which provides Layer 7 analysis of network traffic flows and enables network context for security event correlation.

The QRadar 2100 Appliance is optimized hardware that does not require expensive external storage, third-party databases, or ongoing database administration, and is ideal for deployments in smaller enterprises or departments that do not foresee the need to upgrade to higher EPS or Flows/Sec capacities.

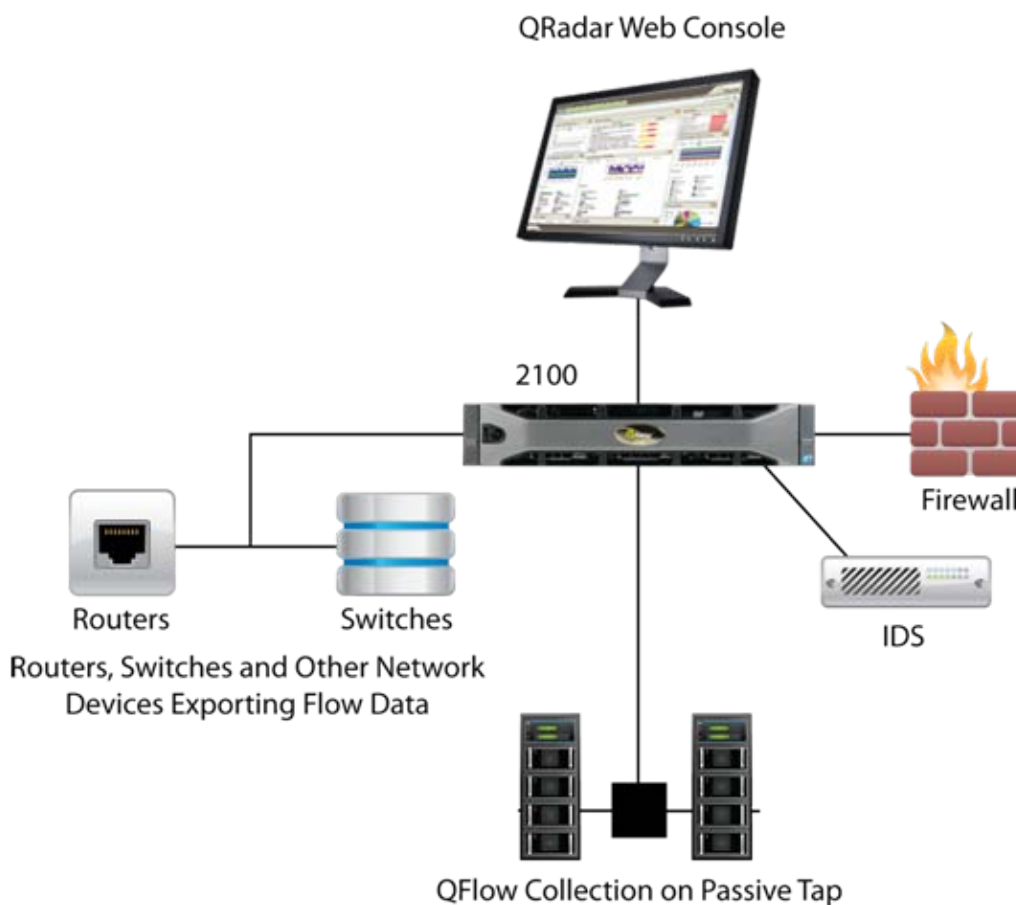
QRadar 2100 All-in-One Appliance

Delivering the full power of QRadar in one device

Features:

- Includes onboard 50Mbps QFlow Collector, collection via passive tap or span ports
- 10/100/1000 BASE-T connectivity for monitoring
- 10/100/1000 BASE-T management
- Up to 50,000 flows per minute (50,000 to 100,000 NetFlows)
- 1,000 events per second
- Support for up to 750 event sources (devices), expandable via license upgrade
- Dual redundant power supplies (auto-sensing)
- Embedded hardware RAID 10 for high availability and redundancy of OS and storage.

Sample QRadar 2100 Deployment



The QRadar 3100 Server Appliance

The QRadar 3100 is an enterprise-class network security management solution for organizations of all sizes, ranging from medium-sized companies to large, globally deployed entities.

The QRadar 3100 Appliance is an ideal solution for companies that are growing and will need additional network activity and event monitoring capacity in the future. It is also the base platform for large companies that may be geographically dispersed and are looking for an enterprise-class scalable solution.

The QRadar 3100 Appliance utilizes on-board event collection and correlation capabilities, and is expandable with 1601 Event Processor and 1701 Flow Processor Appliances.

The QRadar 3100 Appliance utilizes QFlow Collectors for the collection of network flows which provide Layer 7 analysis, as well as for the aggregation of other flow sources, such as JFlow, NetFlow and SFlow.

Sample QRadar 3100 Deployment

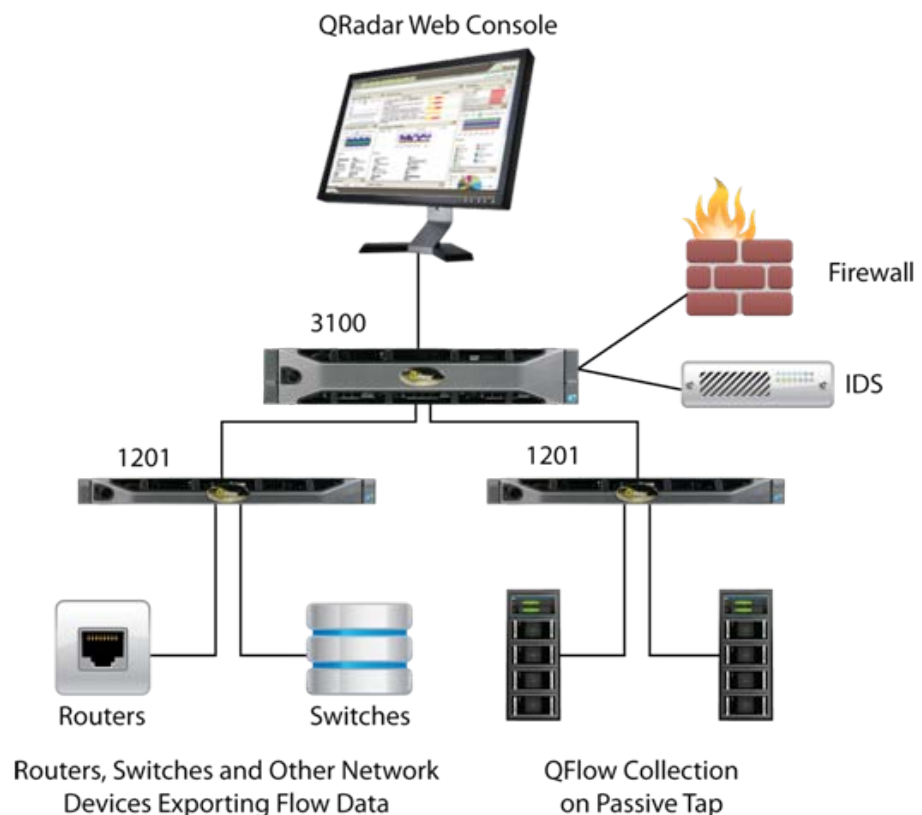
With Distributed Flow Collectors

QRadar 3100 Server Appliance

Deployed in conjunction with QFlow Collectors

Features:

- Supports 25,000-200,000 FPM, expandable to millions of flows with add-on 1701 Flow Processors
- Supports 1,000 to 5,000 events per second, Expandable to tens of thousands of events per second with add-on 1601 Event Processors
- Support for up to 750 event sources (devices), expandable via license upgrade
- Dual redundant power supplies (auto-sensing)
- Embedded hardware RAID 10 for high availability and redundancy of OS and storage



QRadar 1601 Event Processor:

The 1601 is an expansion appliance that is deployed in conjunction with QRadar 3100. Designed to integrate into Q1 Labs' Security Intelligence platform, QRadar 1601 offers real-time collection, prioritization and correlation of event data and can scale to more than 10,000 events per second.

QRadar 1605 Event Processor:

The 1605 is an expansion appliance that is deployed in conjunction with QRadar 3100. The 1605 Event Processor supports 6TB of storage, for long term retention of log data and increased capacity for event processing, and can scale to 20,000 events per second.

QRadar 1701 Flow Processor:

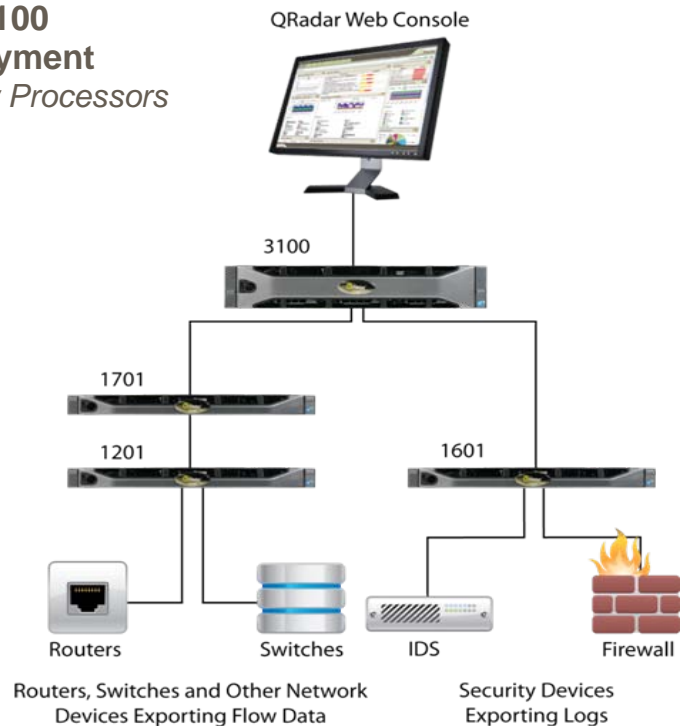
Whether extracting native flow information from the network infrastructure, or working in tandem with QFlow collectors, QRadar flow processors enable the collection, analysis and storage of a variety of flow formats including NetFlow, CFlow, JFlow, SFlow, VFlow and QFlow. The 1701 is an expansion appliance that is deployed in conjunction with QRadar 3100. QRadar's 1701 enables QRadar deployments to process and store millions of network communications each second and scales to 600,000 flows per minute.

High Availability Solution:

QRadars' easy-to-deploy high availability (HA) appliances provide fully automated failover and disk synchronization for high availability of data collection and analysis capabilities. QRadar's HA capabilities address the demand for scalable solutions that enable network and security teams to process, correlate and store more logs, events and network activities without interruption.

Sample QRadar 3100 Distributed Deployment

With Event and Flow Processors



QRadar Event and Flow Processors

Deployed in conjunction with QRadar 3100

1601 Event Processor

Features:

- 2500 EPS, expandable to 10,000 EPS with license upgrade
- Dual redundant power supplies (auto-sensing)
- Provides 3TB of storage
- Multiple 1601 flow processors can be deployed for scaling
- Embedded Hardware RAID 10, for high availability and redundancy

1605 Event Processor

Features:

- 2500 EPS, expandable to 20,000 EPS with license upgrade
- Dual redundant power supplies (auto-sensing)
- Provides 6TB of storage
- Multiple 1605 flow processors can be deployed for scaling
- Embedded Hardware RAID 5 for high availability and redundancy

1701 Flow Processor

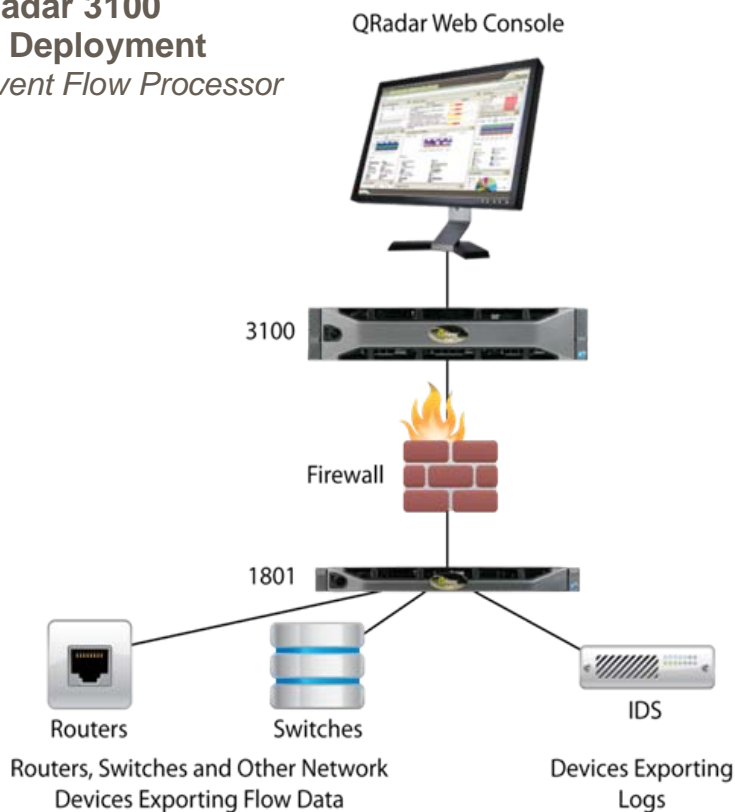
Features:

- 100,000 FPM, expandable to 600,000 FPM with license upgrade
- Dual redundant power supplies (auto-sensing)
- Provides 3TB of storage
- Multiple 1701 flow processors can be deployed for scaling
- Embedded Hardware RAID 10 for high availability and redundancy.

QRadar 1801 Combined Event Flow Processor:

The 1801 is well suited for organizations looking to provide event and network activity monitoring and processing for remote or branch offices or to larger highly distributed organizations.

Sample QRadar 3100 Distributed Deployment With 1801 Event Flow Processor



QRadar 1801

Combined Event and Flow Processor

Features:

- Provides event and flow processing on a single appliance
- Supports 1,000 events per second and up to 50,000 flows per minute
- Offers dual redundant power supplies (auto-sensing)
- On-board 1.5 TB of Storage
- Includes embedded hardware RAID 10 for high availability and redundancy.

QRadar Appliance Specifications:

	2100	3100	1601/1701	1605	1801
Chassis	2U	2U	2U	2U	2U
Dimensions	29.31" D x 17.5" W x 3.4" H	29.31" D x 17.5" W x 3.4" H	29.31" D x 17.5" W x 3.4" H	26.7" D x 17.2" W x 3.4" H	29.31" D x 17.5" W x 3.4" H
Storage	1.5 TB	3 TB	3 TB	6TB	1.5 TB
RAID	Hardware RAID 10 for data storage and OS	Hardware RAID 10 for data storage	Hardware RAID 10 for data storage	Hardware RAID 5 for data storage	Hardware RAID 10 for data storage
Network Interfaces	4X10/100/1000	2X10/100/1000	4X10/100/1000	2X10/100/1000	4X10/100/1000
Power Supply	Dual Redundant Auto Sensing	Dual Redundant Auto Sensing	Dual Redundant Auto Sensing	Dual Redundant Auto Sensing	Dual Redundant Auto Sensing

QRadar 1000 Series QFlow Collectors:

Q1 Labs offers QFlow Collector appliances that provide added security at critical points across the enterprise network for greater defense, and can be used in conjunction with the QRadar 2100 and 3100 series appliances. QFlow Collectors offer a cost-effective solution for gathering the most sophisticated and actionable network activity data available from your network.

QFlow Collectors go beyond traditional flow-based data sources to enable application-layer flow analysis and anomaly detection. Deep packet and content inspection identify threats tunneled over standard protocols and ports.

QRadar QFlow Collectors Specifications:

	1101	1201	1202	1301	1302	1310
Chassis	1U	1U	1U	1U	1U	1U
Dimensions	21.5" D x 17.6" W x 1.68" H	30.4" D x 16.7" W x 1.67" H	30.4" D x 16.7" W x 1.67" H	30.4" D x 16.7" W x 1.67" H	30.4" D x 16.7" W x 1.67" H	30.4" D x 16.7" W x 1.67" H
Traffic Rate	Up to 50 Mbps	Up to 200 Mbps	Up to 1 Gbps	Up to 200 mbps	Up to 1 Gbps	Up to 1 Gbps
RAID	H a r d w a r e R A I D 1					
Network Interfaces	2x10/100/ 1000 CX	4x10/100/ 1000 CX	1x10/100/1000 CX Mgmt 4x1000 CX Monitoring	1x10/100/1000 CX Mgmt 4x1000 SX Monitoring	1x10/100/1000 CX Mgmt 2x1000 SX Monitoring	1x10/100/1000 CX Mgmt 2x10GB SR Monitoring
Power Supply	Dual Redundant Auto Sensing Power Supply					

Q1 Labs, Inc.

890 Winter Street
Suite 230
Waltham, MA 02451
USA

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

ADS 710

Copyright © 2010 Q1 Labs, Inc. All rights reserved. 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.