

Data Sheet: QRadar Appliance Family

The **QRadar™ appliance family** provides, to enterprise and government customers, an unequalled platform to deploy Q1Labs flagship network security management solution QRadar, which enable a repeatable security process to improve operational efficiency, better protect IT assets from a complex landscape of threats, and assist meeting a wide array of today's IT focused regulatory mandates.

With pre-installed QRadar software, a hardened operating system, and Web-based setup, the QRadar family of appliances lets you get your network security up and running quickly and easily.

The bottom line: Simple deployment, fast implementation and improved security – all at a low total cost of ownership.

Key features and benefits*

Delivers centralized log management

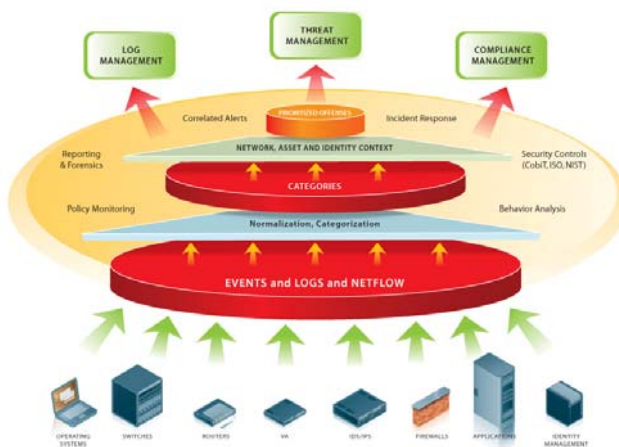
- Collect and manage network and security events
- Solution provides log management with inherent integrity and reliability

Provides threat management

- Detect threats that other solutions miss
- Enables directed remediation of security incidents

Enables regulatory compliance

- Provides comprehensive log management across all networked devices
- Enables monitoring, alerting, reporting and auditing required by most all regulations



* For more information on QRadar please see the QRadar 6.1 Data Sheet



The **Nexus** of Security and Networking

**QRadar 2100
“All-in-One” Appliance**

**Delivering the full power of
QRadar in a single device**

2100



Features:

Includes 50Mbps QFlow Collector
10/100/1000 base T Connectivity
for Monitoring

10/100/1000 base T Management
25000 to 50,000 Flows Per Sec-
ond (50,000 to 100,000 NetFlows)

1000 Events Per Second
Support for up to 750 Event
Sources (devices)

Dual Redundant Power Supplies

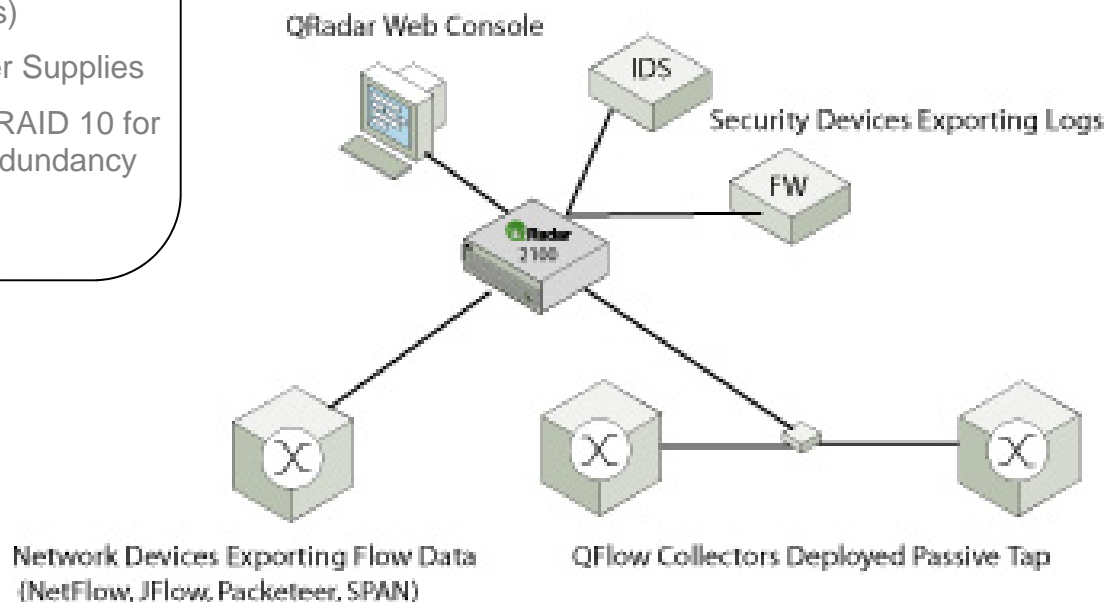
Embedded Hardware RAID 10 for
high availability and redundancy
of OS and Storage.

The QRadar 2100 All-In-One appliance combines the features and functionality of the powerful QRadar software in a single hardware offering. It provides an all-in-one security solution that plugs right into a network, making it 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 supports Q1 Labs’ Offense Resolution module and 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.

The 2100 appliance is ideal for deployments in smaller enterprises or departments that do not foresee the need to upgrade to higher EPS of Flows/Sec capacities.



QRadar 3100 Series Server Appliance

Deployed in conjunction with QRadar 1000 series QFlow Collection Appliances

3100



Features:

25,000 flows 200,000 Flows Per Second (Expandable to millions of flows with add-on 1701 Flow Processors)

1,000 to 5000 Events Per Second (Expandable to 10s of thousands events per second with add-on 1601 Event Processors)

Support for up to 750 Event Sources (devices) (Expandable)

Dual Redundant Power Supplies (Auto-Sensing)

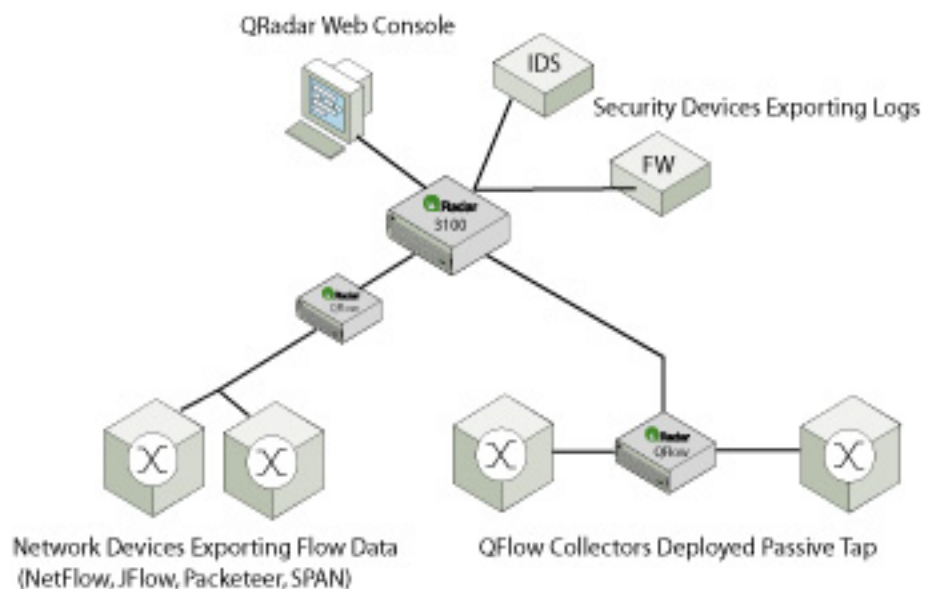
Embedded Hardware RAID 10 for high availability and redundancy of OS and Storage

The **QRadar 3100 Appliance** is an enterprise class appliance which provides a scalable Network Security Management solution for medium sized companies to large, globally deployed organizations.

The QRadar 3100 Appliance is an ideal solution for companies who are growing and who will need additional flow and event monitoring capacity in the future. It is also the base platform for large companies who may be geographically dispersed and 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 Appliances.

The QRadar 3100 Appliance utilizes QFlow Collector appliances 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, SFlow and Packeteer's Flow Data Records.



1700 Flow Processors



Features:

Up to 600,000 Flows

Multiple 1701 flow processors can be deployed for scaling

The 1701 provides on-board 2TB TB of Storage for detailed Flow data

The 1700 provides support for the QRadar Direct Attached Storage Appliance. (Sold Separately)

Dual Redundant Power Supplies (Auto-Sensing)

Embedded Hardware RAID 10 for high availability and redundancy

1600 Event Processors



Features:

Up to 10,000 EPS Per 1600 Appliance

Multiple 1601s can be deployed for scaling

Dual Redundant Power Supplies (Auto-Sensing)

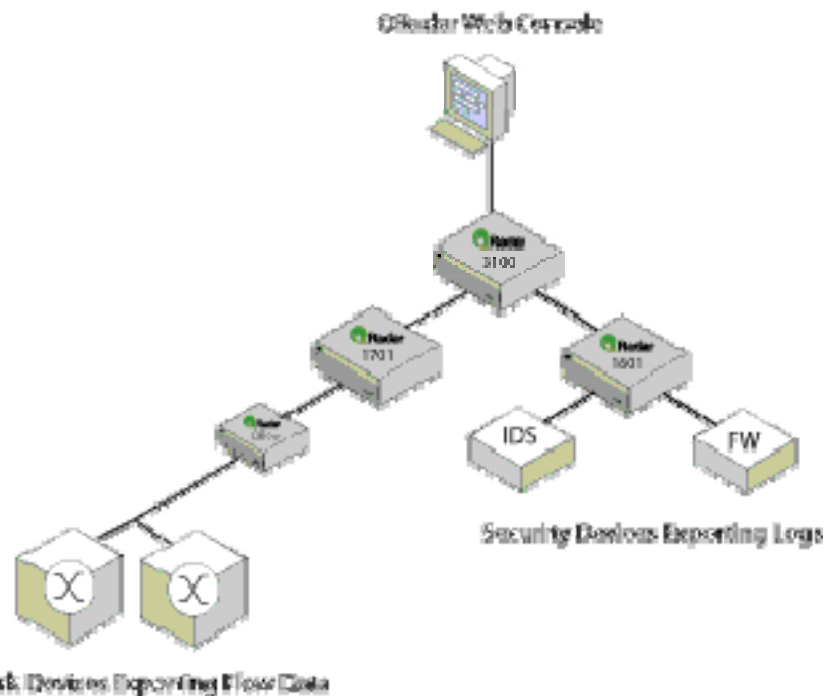
The 1601 provides on-board 2TB TB of Storage

The 1600 provides support for the QRadar Direct Attached Storage Appliance. (Sold Separately)

Embedded Hardware RAID 10 for high availability and redundancy

The QRadar 1700 and QRadar 1701 Flow Processors are expansion appliances for the QRadar 3100 Appliance. Flow Processor Appliances can scale the 3100 series from 200,000 to one million + flows per second.

The QRadar 1600 and 1601 Event Processors are expansion appliances for the QRadar 3100 Appliance that can be distributed to scale the QRadar 3100 from supporting 5000 to 10,000+ events per second.



QRadar Server and Processor Appliance Specifications

	2100	3100	1601/1701
Chassis	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
Storage	900 GB	2 TB	2 TB
RAID	Hardware RAID 10 for data storage and OS	Hardware RAID 10 for data storage	Hardware RAID 10 for data storage
Network Interfaces	1 10/100/1000 base T for management 3 10/100/1000 base T for monitoring (Span or TAP)	2 10/100/1000 base T	2 10/100/1000 base T
Power Supply	Dual Redundant Auto Sensing Power Supply	Dual Redundant Auto Sensing Power Supply	Dual Redundant Auto Sensing Power Supply

**QRadar 1000 Series
QFlow Collection Appliances**



QFlow collectors provide added security at critical points across the enterprise network for greater defense. QFlow collectors can be used with the QRadar 2100 and 3100 series appliances. The 1000 series offers a cost-effective solution for gathering the most sophisticated and actionable flow data available from your network.

QFlow goes 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.

All QFlow 1000 Series Appliances support QRadar-ICX Resolver technology for threat resolution with the add-on QRadar-ICX module.

QRadar QFlow Collection Appliance Specifications

	1101	1201	1202	1302	1301
Chassis	1U	1U	1U	1U	1U
Dimensions	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	29.31" D x 17.5" W x 3.4" H
Storage	NA	NA	NA	NA	NA
RAID	Hardware RAID 10 for OS	Hardware RAID 10 for OS	Hardware RAID 10 for OS	Hardware RAID 10 for OS	Hardware RAID 10 for OS
Network Interfaces	2 10/100/1000 baseT	1 10/100/1000 base T for management 3 10/100/1000 base T for monitoring (Span or TAP)	1 10/100/1000 base T for management 2 10/100/1000 base T for monitoring (Span or TAP)	1 10/100/1000 base T for management 2 1000 base SX Fiber for monitoring (Span or TAP)	1 10/100/1000 base T for management 2 1000 base SX Fiber for monitoring (Span or TAP)
Power Supply	Dual Redundant Auto Sensing Power Supply	Dual Redundant Auto Sensing Power Supply	Dual Redundant Auto Sensing Power Supply	Dual Redundant Auto Sensing Power Supply	Dual Redundant Auto Sensing Power Supply

QRadar QFlow Collection Appliance Specifications (continued)

QRadar 1101

(QFlow for Access)

Designed for access-layer and edge deployment, this QFlow collector supports up to 50 Megabits/second of traffic (deployed via SPAN connection, with 10/100 Connectivity)

Features:

Up to 50Mbps
50 resolvers
Deployed via SPAN connection

QRadar 1201/1302

(QFlow for Distribution)

Designed for distribution-layer deployment, this QFlow collector supports up to 200 Megabits/second of traffic (deployed via SPAN or TAP connection)

Features:

Up to 200 Mbps
Deployed via SPAN or TAP
50 resolvers

QRadar 1202/1301

(QFlow for Core)

Designed for deployment in high-speed environments, such as core and backbones, this high-end QFlow collector supports line rate Gigabit traffic (deployed via Fiber TAP)

Features:

High Speed
– Line Rate Gigabit (1301 Fiber, 1202 Copper)
Deployed via Fiber TAP
50 resolvers



The Nexus of Security and Networking

Copyright © 2008 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

info@q1labs.com