IBM Security QRadar
Version 7.2.6

Hardware Guide

Note
Before using this information and the product that it supports, read the information in "Notices" on page 47.

Product information

This document applies to IBM QRadar Security Intelligence Platform V7.2.6 and subsequent releases unless superseded by an updated version of this document.

Contents

About this guide

The IBM® Security QRadar® SIEM Hardware Guide provides QRadar appliance descriptions, diagrams, and specifications.

Intended audience

This guide is intended for all QRadar SIEM users responsible for investigating and managing network security. This guide assumes that you have QRadar SIEM access and a knowledge of your corporate network and networking technologies.

Technical documentation

For information about how to access more technical documentation, technical notes, and release notes, see Accessing IBM Security Documentation Technical Note (http://www.ibm.com/support/docview.wss?rs=0&uid=swg21612861).

Contacting customer support

For information about contacting customer support, see the Support and Download Technical Note (http://www.ibm.com/support/docview.wss?uid=swg21616144).

Statement of good security practices

IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

Please Note:

Use of this Program may implicate various laws or regulations, including those related to privacy, data protection, employment, and electronic communications and storage. IBM Security QRadar may be used only for lawful purposes and in a lawful manner. Customer agrees to use this Program pursuant to, and assumes all responsibility for complying with, applicable laws, regulations and policies. Licensee represents that it will obtain or has obtained any consents, permissions, or licenses required to enable its lawful use of IBM Security QRadar.

Chapter 1. QRadar M3 appliance overview

Review information about IBM Security QRadar to understand hardware and license requirements.

Review this overview of QRadar appliances, including capabilities, and license limitations.

QRadar QFlow Collector 1201

The IBM Security QRadar QFlow Collector 1201 (MTM 4378-QC1) appliance provides high capacity and scalable Layer 7 application data collection for distributed deployments. The QRadar QFlow Collector 1201 also supports external flow-based data sources.

View hardware information and requirements for the QRadar QFlow Collector 1201 in the following table:

Table 1. QRadar QFlow Collector 1201

Description	Value
Network traffic	200 Mbps
Interfaces	Six 10/100/1000 Base-T network monitoring interfaces One management interface
Memory	6 GB
Storage	146 GB
Power supply	Dual Redundant 460W AC Power Supply
Dimensions	28" D x 17.3" W x 1.69" H
Included components	QRadar QFlow Collector 1201

QRadar QFlow Collector 1202

The IBM Security QRadar QFlow Collector 1202 (MTM 4378-QC2) appliance provides high capacity and scalable Layer 7 application data collection for distributed deployments. The QRadar QFlow Collector 1202 also supports external flow-based data sources.

View hardware information and requirements for the QRadar QFlow Collector 1202 in the following table:

Table 2. QRadar QFlow Collector 1202

Description	Value
Network traffic	2 Gbps
Interfaces	Four 10/100/1000 Base-T network monitoring interfaces One System Management Ethernet Connector

Table 2. QRadar QFlow Collector 1202 (continued)

Description	Value
Memory	6 GB
Storage	146 GB
Power supply	Dual Redundant 460W AC
Dimensions	28" D x 17.3" W x 1.69" H
Included components	QRadar QFlow Collector 1202 NT4E-STD Napatech Network Adaptor

QRadar QFlow Collector 1301

The IBM Security QRadar QFlow Collector 1301 (MTM 4378-QD1) appliance provides high capacity and scalable Layer 7 application data collection for distributed deployments. The QRadar QFlow Collector 1301 also supports external flow-based data sources.

View hardware information and requirements for the QRadar QFlow Collector 1301 in the following table:

Table 3. QRadar QFlow Collector 1301

Description	Value
Network traffic	2 Gbps
Interfaces	Four 10/100/1000 Base-T network monitoring interfaces One System Management Ethernet Connector
Memory	6 GB
Storage	146 GB
Power supply	Dual Redundant 460W AC Power Supply
Dimensions	28" D x 17.3" W x 1.69" H
Included components	QRadar QFlow Collector 1301 NT4E-STD Napatech Network Adaptor

QRadar QFlow Collector 1310

The IBM Security QRadar QFlow Collector 1310, -SR (MTM 4378-QSR) or -LR (MTM 4378-QLR), appliance provides high capacity and scalable Layer 7 application data collection for distributed deployments. The QRadar QFlow Collector 1310 also supports external flow-based data sources.

View hardware information and requirements for the QRadar QFlow Collector 1310 in the following table:

Table 4. QRadar QFlow Collector 1310

Description	Value
Network traffic	3 GBps

Table 4. QRadar QFlow Collector 1310 (continued)

Description	Value
Interfaces	Two 10 Gbps XFP One System Management Ethernet Connector
Memory	8 GB
Storage	300 GB
Power supply	Dual Redundant 460W AC Power Supply
Dimensions	28" D x 17.3" W x 1.69" H
Included components	QRadar QFlow Collector 1310 NT20E Napatech Network Adaptor

QRadar Event Collector 1501

The IBM Security QRadar Event Collector 1501 (MTM 4378-Q21) appliance is a dedicated event collector. By default, a dedicated event collector collects and parses event from various log sources and continuously forwards these events to an event processor. You can configure the QRadar Event Collector 1501 appliance to temporarily store events and only forward the stored events on a schedule. A dedicated event collector does not process events and it does not include an on-board event processor.

View hardware information and requirements for the QRadar Event Collector 1501 in the following table:

Table 5. QRadar Event Collector 1501

Description	Value
Events per second	2500 EPS
Log Sources	750
Interfaces	Six 10/100/1000 Base-T network monitoring interfaces One 10/100/1000 Base-T management interface
Memory	24 GB
Storage	1.3 TB dedicated storage
Power supply	Dual Redundant 675W AC Power Supply
Dimensions	28" D x 17.3" W x 1.69" H
Included components	QRadar Event Collector 1501

QRadar Event Processor 1605

The IBM Security QRadar Event Processor 1605 (MTM 4379-Q05) appliance is a dedicated event processor that you can scale your QRadar deployment to manage higher EPS rates. The QRadar Event Processor 1605 appliance includes an on-board event collector, event processor, and internal storage for events.

The QRadar Event Processor 1605 is a distributed event processor appliance and requires a connection to a QRadar 3105 (Console) or QRadar 3124 (Console) appliance.

View hardware information and requirements for the QRadar Event Processor 1605 in the following table:

Table 6. QRadar Event Processor 1605

Description	Value
Basic license	2,500 EPS
Upgraded license	Up to 20,000 EPS
Interfaces	Four 10/100/1000 Base-T network monitoring interfaces One 10/100/1000 Base-T management interface
Memory	48 GB
Storage	6.2 TB or larger dedicated event storage
Power supply	Dual Redundant 675W AC Power Supply
Dimensions	29.5" D x 19.2" W x 3.4" H
Included components	Event Collector, Event Processor

QRadar Event Processor 1624

The IBM Security QRadar Event Processor 1624 (MTM 4379-Q24) appliance is a dedicated event processor that you can use to scale your QRadar deployment to manage higher EPS rates. The QRadar Event Processor 1624 appliance includes an on-board event collector, event processor, and internal storage for events.

The QRadar Event Processor 1624 is a distributed event processor appliance and requires a connection to a IBM Security QRadar 3124 (Console) (MTM 4379-Q24) Console appliance.

View hardware information and requirements for the QRadar Event Processor 1624 in the following table:

Table 7. QRadar Event Processor 1624 Event Processor overview

Description	Value
Basic license	2,500 EPS
Upgraded license	Up to 20,000 EPS
Interfaces	Two 10/100/1000 Base-T network monitoring interfaces One 10/100/1000 Base-T management interface
Memory	64 GB
Storage	16 TB or larger
Power supply	Dual Redundant 675W AC Power Supply
Dimensions	29.5" D x 19.2" W x 3.4" H
Included components	QRadar Event Processor 1624 Event Processor

QRadar Flow Processor 1705

The IBM Security QRadar Flow Processor 1705 (MTM 4379-Q05) appliance is a flow processor that can scale your QRadar deployment to manage higher FPM rates. The QRadar Flow Processor 1705 includes an on-board Flow processor, and internal storage for flows.

View hardware information and requirements for the QRadar Flow Processor 1705 in the following table:

Table 8. QRadar Flow Processor 1705

Description	Value
Basic license	100,000 FPM
Upgraded license	Up to 600,000 FPM
Interfaces	Four 10/100/1000 Base-T network monitoring interfaces One 10/100/1000 Base-T management interface
Memory	48 GB
Storage	6.2 TB or larger dedicated flow storage
Power supply	Dual Redundant 675W AC Power Supply
Dimensions	29.5" D x 19.2" W x 3.4" H
Included components	QRadar Flow Processor 1705

QRadar Flow Processor 1724

The IBM Security QRadar Flow Processor 1724 (MTM 4379-Q24) appliance is a flow processor that can scale your QRadar deployment to manage higher FPM rates. The QRadar Flow Processor 1724 includes an on-board Flow processor, and internal storage for flows.

View hardware information and requirements for the QRadar Flow Processor 1724 in the following table:

Table 9. QRadar Flow Processor 1724

Description	Value
Basic license	100,000 FPM
Upgraded license	Up to 1,200,000 FPM
Interfaces	Two 10/100/1000 Base-T network monitoring interface One 10/100/1000 Base-T management interface
Memory	64 GB
Storage	16 TB or larger dedicated flow storage
Power supply	Dual Redundant 675W AC Power Supply
Dimensions	29.5" D x 19.2" W x 3.4" H
Included components	QRadar Flow Processor 1724

QRadar 1805

The IBM Security QRadar 1805 (MTM 4379-Q05) appliance is a combined Event Processor and Flow Processor that can scale your QRadar deployment to manage more events and flows. The QRadar 1805 includes an on-board Event Processor, an on-board Flow Processor, and internal storage for events and flows.

View hardware information and requirements for the QRadar 1805 in the following table:

Table 10. QRadar 1805 overview

Description	Value
Basic license	1,000 EPS 25,000 FPM, 750 log sources
Upgraded license	Up to 2,500 or 5,000 EPS. Up to 50,000, 100,000, or 200,000 FPM
Interfaces	Four 10/100/1000 Base-T network monitoring interfaces One 10/100/1000 Base-T management interface
Memory	48 GB
Storage	6.2 TB or larger
Power supply	Dual Redundant 675W AC Power Supply
Dimensions	29.5" D x 19.2" W x 3.4" H
Included components	QRadar 1805

QRadar 2100

The IBM Security QRadar 2100 (MTM 4378-Q21) appliance is an all-in-one system that combines Network Behavioral Anomaly Detection (NBAD) and Security Information and Event Management (SIEM) to accurately identify and appropriately prioritize threats that occur on your network.

View hardware information and requirements for the QRadar 2100 in the following table:

Table 11. QRadar 2100 overview

Description	Value
Basic license	1,000 EPS 25,000 FPM
Upgraded license	50,000 FPM
Interfaces	Six 10/100/1000 Base-T network monitoring interfaces One 10/100/1000 Base-T management interface
Memory	24 GB
Storage	1.3 TB or larger

Table 11. QRadar 2100 overview (continued)

Description	Value
Power supply	Dual Redundant 675W AC Power Supply
Dimensions	28" D x 17.3" W x 1.69" H
Included components	Event Collector, Event Processor, Single QRadar QFlow Collector, which supports up to 50 Mbps

Additional QRadar QFlow Collectors are sold separately.

QRadar 3105 (All-in-One)

The IBM Security QRadar 3105 (Base) (MTM 4379-Q05) appliance is an all-in-one QRadar system that can profile network behavior and identify network security threats.

View hardware information and requirements for the QRadar Log Manager 3105 (All-in-One) in the following table:

Table 12. QRadar Log Manager 3105 (All-in-One)

Description	Value
Basic license	1,000 EPS 25,000 FPM
Upgraded license	Up to 5,000 EPS Up to 200,000 FPM
Log sources	750
Interfaces	Four 10/100/1000 Base-T network monitoring interfaces One 10/100/1000 Base-T management interface
Memory	48 GB
Storage	6.5 TB
Power supply	Dual Redundant 675W AC Power Supply
Dimensions	29.5" D x 19.2" W x 3.4" H
Included components	Event Collector and Event Processor with internal event storage (6.5 TB or larger)

The QRadar 3105 (All-in-One) appliance requires external QRadar QFlow Collectors for layer 7 network activity monitoring.

QRadar 3105 (Console)

Understand and expand the capacity of the QRadar 3105 (All-in-One).

You can expand the capacity of the QRadar 3105 (All-in-One) beyond license-based upgrade options by upgrading to the IBM Security QRadar 3105 (Console) (MTM 4379-Q05) appliance and adding one or more of the following appliances:

- "QRadar Event Processor 1605" on page 21

- "QRadar Flow Processor 1705" on page 23
- "QRadar 1805" on page 25

The QRadar 3105 (Console) appliance you can use to manage a distributed deployment of Event Processors and Flow Processors to profile network behavior and identify network security threats.

QRadar 3124 (All-in-One)

The IBM Security QRadar 3124 (Base) (MTM 4379-Q24) appliance is an all-in-one QRadar system that can profile network behavior and identify network security threats.

View hardware information and requirements for the QRadar 3124 (All-in-One) in the following table:

Table 13. QRadar 3124 (All-in-One)

Description	Value
Basic license	1000 EPS 25,000 FPM
Upgraded license	Up to 5000 EPS Up to 200,000 FPM
Log sources	750
Interfaces	Two 10/100/1000 Base-T network monitoring interface One System Management Ethernet Connector
Memory	64 GB
Storage	16 TB or larger
Power supply	Dual Redundant 675W AC Power Supply
Dimensions	29.5" D x 19.2" W x 3.4" H
Included components	Event Collector and Event Processor

The QRadar 3124 (All-in-One) requires external QRadar QFlow Collectors for layer 7 network activity monitoring.

QRadar 3124 (Console)

Understand expansion options for the IBM Security QRadar 3124 (Console) (MTM 4379-Q24)

You can expand the capacity of the IBM Security QRadar 3124 (Base) (MTM 4379-Q24) appliance beyond license-based upgrade options by upgrading to the QRadar 3124 (Console) appliance and adding one or more of the following appliances:

- "QRadar Event Processor 1624" on page 4
- "QRadar Flow Processor 1724" on page 5

The QRadar 3124 (Console) appliance you can use to manage a distributed deployment of Event Processors and Flow Processors to profile network behavior and identify network security threats.

QRadar Log Manager 1605

The IBM Security QRadar Log Manager 1605 (MTM 4379-Q05) appliance is a distributed Event Processor appliance and requires a connection to a QRadar Log Manager 3124 Console appliance.

The QRadar Log Manager 1605 is a distributed Event Processor appliance and requires a connection to a QRadar Log Manager 3105 Console appliance.

View hardware information and requirements for the QRadar Log Manager 1605in the following table:

Table 14. QRadar Log Manager 1605

Description	Value
Basic license	2,500 EPS
Upgraded license	Up to 20,000 EPS
Interfaces	Four 10/100/1000 Base-T network monitoring interfaces One System Management Ethernet Connector
Memory	48 GB
Storage	6.5 TB or larger
Power supply	Dual Redundant 675W AC Power Supply
Dimensions	29.5" D x 19.2" W x 3.4" H
Included components	Event Collector, Event Processor

QRadar Log Manager 1624

The IBM Security QRadar Log Manager 1624 (MTM 4379-Q24) appliance is a dedicated Event Processor that you can use to scale your QRadar Log Manager deployment to manage higher Event Per Second (EPS) rates. The QRadar Log Manager 1624 appliance includes an on-board Event Collector, Event Processor, and internal storage for events.

The QRadar Log Manager 1624 is a distributed Event Processor appliance and requires a connection to a QRadar Log Manager 3124 Console appliance.

View hardware information and requirements for the QRadar Log Manager 1624 in the following table:

Table 15. QRadar Log Manager 1624

Description	Value
Basic license	2,500 EPS
Upgraded license	Up to 20,000 EPS

Table 15. QRadar Log Manager 1624 (continued)

Description	Value
Interfaces	Two 10/100/1000 Base-T network monitoring interfaces One System Management Ethernet Connector
Memory	64 GB
Storage	16 TB or larger
Power supply	Dual Redundant 675W AC Power Supply
Dimensions	29.5" D x 19.2" W x 3.4" H
Included components	Event Collector, Event Processor

QRadar Log Manager 2100

The IBM Security QRadar Log Manager 2100 (MTM 4378-Q21) appliance is an all-in-one system that can manage and store events from various network devices.

View hardware information and requirements for the QRadar Log Manager 2100 in the following table:

Table 16. QRadar Log Manager 2100 overview

Description	Value
Basic license	500 EPS
License upgrade	Up to 1000 EPS
Log sources	750
Interfaces	Six 10/100/1000 Base-T network monitoring interfaces One System Management Ethernet Connector
Memory	24 GB
Storage	1.3 TB or larger
Power supply	Dual Redundant 675W AC Power Supply
Dimensions	28" D x 17.3" W x 1.69" H
Included components	Event Collector, Event Processor

QRadar Log Manager 2100 includes external flow collection.

Additional QRadar QFlow Collectors are sold separately.

QRadar Log Manager 3105 (All-in-One)

The IBM Security QRadar Log Manager 3105 (Base) (MTM 4379-Q05) appliance is an all-in-one system that you can use to manage and store events from various network devices.

View hardware information and requirements for the QRadar Log Manager 3105 (All-in-One) in the following table:

Table 17. QRadar Log Manager 3105 (All-in-One) overview

Description	Value
Basic license	500 EPS
Upgraded license	Up to 1000 EPS
Interfaces	Two 10/100/1000 Base-T network monitoring interfaces One System Management Ethernet Connector
Memory	48 GB
Storage	6.2 TB
Power supply	Dual Redundant 675W AC Power Supply
Dimensions	29.5" D x 19.2" W x 3.4" H
Included components	Event Collector and Event Processor

You can upgrade your license to migrate your QRadar Log Manager 3105 (All-in-One) to QRadar 3105 (All-in-One). For more information, see the *Migrating QRadar Log Manager to QRadar SIEM Technical Note*.

QRadar Log Manager 3105 Console

You can expand the capacity of the QRadar Log Manager (all-in-one) appliance beyond license-based upgrade options by upgrading to the IBM Security QRadar Log Manager 3105 (Console) (MTM 4379-Q05) appliance. You must also add one or more QRadar Log Manager 1605 or IBM Security QRadar Log Manager 1624 (MTM 4379-Q24) appliances.

The QRadar Log Manager 3105 Console appliance manages a distributed deployment of Event Processors to collect and process events. You can upgrade your license from QRadar Log Manager 3105 Console to IBM Security QRadar 3105 (Console) (MTM 4379-Q05).

QRadar Log Manager 3124 (All-in-One)

The IBM Security QRadar Log Manager 3124 (Base) (MTM 4379-Q24) appliance is an all-in-one system that you can use to manage and store events from various network devices.

View hardware information and requirements for the QRadar Log Manager 3124 (All-in-One) in the following table:

Table 18. QRadar Log Manager 3124 (All-in-One)

Description	Value
Basic license	1000 EPS
Upgraded license	Up to 5000 EPS
Log sources	750
Interfaces	Two 10/100/1000 Base-T network monitoring interface One System Management Ethernet Connector

Table 18. QRadar Log Manager 3124 (All-in-One) (continued)

Description	Value
Memory	64 GB
Storage	16 TB or larger
Power supply	Dual Redundant 675W AC Power Supply
Dimensions	29.5" D x 19.2" W x 3.4" H
Included components	Event Collector and Event Processor

You can upgrade your license to migrate your QRadar Log Manager 3124 (All-in-One) appliance to QRadar 3124 (All-in-One). For more information about migrating QRadar Log Manager to QRadar SIEM, see the *Migrating QRadar Log Manager to QRadar SIEM Technical Note*.

QRadar Log Manager 3124 Console

The IBM Security QRadar Log Manager 3124 (Console) (MTM 4379-Q24) appliance manages a distributed deployment of Event Processors to collect and process events. Expand and upgrade the QRadar Log Manager 3124 Console.

You can expand the capacity of the QRadar Log Manager 3124 (All-in-One) appliance beyond license-based upgrade options by upgrading to the QRadar Log Manager 3124 Console appliance and adding one or more of the following appliances:

- "QRadar Log Manager 1605" on page 9
- "QRadar Log Manager 1624" on page 9

You can upgrade your license to migrate your QRadar Log Manager 3124 Console appliance to QRadar 3124 (Console). For more information, see the *Migrating QRadar Log Manager to QRadar SIEM Technical Note* .

The QRadar Log Manager 3124 Consoleappliance manages a distributed deployment of Event Processors to collect and process events.

QRadar Vulnerability Manager

The IBM Security QRadar Vulnerability Manager appliance scans and reports on network vulnerabilities. QRadar Vulnerability Manager provides a vulnerability management workflow that is fully integrated with QRadar SIEM and is available as a software option, appliance, and virtual appliance.

QRadar Vulnerability Manager provides the following capabilities:

- Scans inside and outside your network, network infrastructure, servers, and end points for bad configurations, weak settings, unpatched products, and other key weaknesses.
- Uses network usage, threat environment, security configuration information, virtual patch, and patch availability to bring real context to vulnerability management, which drives efficient remediation processes
- Integrates all vulnerability information from external systems to provide a single view.

- Full integration with the QRadar asset profile database to provide intelligent event-driven scans.
- Unlimited QRadar Vulnerability Manager discovery scans
- Use of hosted scanner for DMZ scanning

The QRadar Vulnerability Manager appliance supports:

Table 19. QRadar Vulnerability Manager overview

Description	Value
Basic license	255 assets
Upgraded license	Up to 32, 768 assets
Interfaces	Two 10/100/1000 Base-T network monitoring interfaces System Management Ethernet Connector
Memory	48 GB
Storage	6.5 TB dedicated storage
Power supply	Dual Redundant 675W AC Power Supply
Dimensions	29.5" D x 19.2" W x 3.4" H
Included components	QRadar Vulnerability Manager

QRadar Risk Manager

The IBM Security QRadar appliance delivers a fully integrated risk management, vulnerability prioritization, and automated configuration solution that is integrated into the IBM Security QRadar platform. QRadar Log Manager enables tightly integrated features in QRadar SIEM that enhance incident management, log and network activity searches, threat visualization, and reports.

View hardware information and requirements for the QRadar Risk Manager in the following table:

Table 20. QRadar Risk Manager in the following table

Description	Value
Interfaces	Two 10/100/1000 Base-T network monitoring interfaces One System Management Ethernet Connector
Memory	48 GB
Storage	6.5 TB dedicated storage
Power supply	Dual Redundant 675W AC Power Supply
Dimensions	29.5" D x 19.2" W x 3.4" H
Included components	QRadar Risk Manager

Chapter 2. QRadar M4 appliance overview

Review information about IBM Security QRadar to understand hardware and license requirements.

Review this overview of QRadar appliances, including capabilities, and license limitations.

QRadar QFlow Collector 1201

The IBM Security QRadar QFlow Collector 1201 (MTM 4380-Q2C) appliance provides high capacity and scalable Layer 7 application data collection for distributed deployments. The QRadar QFlow Collector 1201 also supports external flow-based data sources.

View hardware information and requirements for the QRadar QFlow Collector 1201 in the following table:

Table 21. QRadar QFlow Collector 1201

Description	Value
Network traffic	1 Gbps
Interfaces	Five 10/100/1000 Base-T network monitoring interfaces Two 10 Gbps SFP + ports One 10/100/1000 Base-T QRadar management interface One 10/100 Base-T integrated management module interface
Memory	16 GB, 4 x 4GB 1600 MHz RDIMM
Storage	2 x 2.5 inch 600 GB 10 K rpm SAS, 600 MB total (Raid 1)
Power supply	Dual Redundant 550 W AC
Dimensions	28.9 inches deep x 16.9 inches wide x 1.7 inches high
Included components	QRadar QFlow Collector

QRadar QFlow Collector 1202-C/1301-C

The IBM Security QRadar Core Appliance QFlow Collector 1202-C and 1301-C (MTM 4380-Q1G) appliance provides high capacity and scalable Layer 7 application data collection for distributed deployments. The QRadar QFlow Collector 1202-C/1301-C also supports external flow-based data sources.

View hardware information and requirements for the QRadar QFlow Collector 1202-C/1301-C in the following table:

Table 22. QRadar QFlow Collector 1202-C/1301-C specifications

Description	Value
Network traffic	3 Gbps

Table 22. QRadar QFlow Collector 1202-C/1301-C specifications (continued)

Description	Value
Interfaces	Two 10/100/1000 Base-T network monitoring interfaces Two 10 Gbps SFP + ports One 10/100/1000 Base-T QRadar management interface One 10/100 Base-T integrated management module interface Four 1 Gbps NT4E-STD SFP+ Napatech card. Supported SFP+ 1 Gbps Copper, 1 Gbps Short Range Fiber, 1 Gbps Long Range Fiber
Memory	16 GB, 4 x 4GB 1600 MHz RDIMM
Storage	600 GB 10 K rpm SAS, 600 MB total (Raid 1)
Power supply	Dual Redundant 750 W AC
Dimensions	27.57 inches deep x 18.99 inches wide x 1.68 inches high
Included components	QRadar QFlow Collector

For information about battery replacement, see Battery Replacement (http://www.dell.com/support/manuals/us/en/19/poweredge-r630/R630_OM_Publication_v3-v3/Replacing-the-system-battery?guid=GUID-364314C7-E137-4FC1-9B63-F9DD3BC9E582&lang=en-us).

QRadar QFlow Collector 1202

The IBM Security QRadar QFlow Collector 1202 (MTM 4380-Q3C) appliance provides high capacity and scalable Layer 7 application data collection for distributed deployments. The QRadar QFlow Collector 1202 also supports external flow-based data sources.

View hardware information and requirements for the QRadar QFlow Collector 1202 in the following table:

Table 23. QRadar QFlow Collector 1202

Description	Value
Network traffic	3 Gbps
Interfaces	Napatech Network Adapter, providing four 1 Gbps 10/100/1000 Base-T network interfaces Two 10 Gbps SFP + ports One 10/100/1000 Base-T QRadar management interface One 10/100 Base-T integrated management module interface
Memory	16 GB, 4 x 4GB 1600 MHz RDIMM
Storage	2 x 2.5 inch 600 GB 10 K rpm SAS, 600 MB total (Raid 1)
Power supply	Dual Redundant 550 W AC
Dimensions	28.9 inches deep x 16.9 inches wide x 1.7 inches high
Included components	QRadar QFlow Collector NT4E-STD Napatech Network Adaptor

QRadar QFlow Collector 1301

The IBM Security QRadar QFlow Collector 1301 (MTM 4380-Q4C) appliance provides high capacity and scalable Layer 7 application data collection for distributed deployments. The QRadar QFlow Collector 1301 also supports external flow-based data sources.

View hardware information and requirements for the QRadar QFlow Collector 1301 in the following table:

Table 24. QRadar QFlow Collector 1301

Description	Value
Network traffic	3 Gbps
Interfaces	Napatech Network Adapter, providing four 1 Gbps 1000 Base SX Multi-Mode Fiber network monitoring interfaces Two 10 Gbps SFP + ports One 10/100/1000 Base-T QRadar management interface One 10/100 Base-T integrated management module interface
Memory	16 GB, 4 x 4GB 1600 MHz RDIMM
Storage	2 x 2.5 inch 600 GB 10 K rpm SAS, 600 MB total (Raid 1)
Power supply	Dual Redundant 550 W AC
Dimensions	28.9 inches deep x 16.9 inches wide x 1.7 inches high
Included components	QRadar QFlow Collector NT4E-STD Napatech Network Adaptor

QRadar QFlow Collector 1310

The IBM Security QRadar QFlow Collector 1310 (MTM 4380-Q5C) appliance provides high capacity and scalable Layer 7 application data collection for distributed deployments. The QRadar QFlow Collector 1310 also supports external flow-based data sources.

View hardware information and requirements for the QRadar QFlow Collector 1310 in the following table:

Table 25. QRadar QFlow Collector 1310

Description	Value
Network traffic	7.5 Gbps
Interfaces	Napatech Network Adapter for fiber, providing two 10 Gbps SFP + network monitoring interfaces One 10/100/1000 Base-T QRadar management interface One 10/100 Base-T integrated management module interface
Memory	16 GB, 4 x 4GB 1600 MHz RDIMM
Storage	2 x 2.5 inch 600 GB 10 K rpm SAS, 600 MB total (Raid 1)
Power supply	Dual Redundant 550 W AC
Dimensions	28.9 inches deep x 16.9 inches wide x 1.7 inches high

Table 25. QRadar QFlow Collector 1310 (continued)

Description	Value
Included components	QRadar QFlow Collector NT20E2 Napatech Network Adaptor

QRadar QFlow Collector 1310 SR-C/LR-C

The IBM Security QRadar Core Appliance QFlow Collector 1310SR-C and LR-C (MTM 4380-Q2G) appliance provides high capacity and scalable Layer 7 application data collection for distributed deployments.

View hardware information and requirements for the QRadar QFlow Collector 1310 SR-C/LR-C in the following table:

Table 26. QRadar QFlow Collector 1310 SR-C/LR-C specifications

Description	Value
Network traffic	10 Gbps
Interfaces	Two 10/100/1000 Base-T network monitoring interfaces Two 10 Gbps SFP + ports One 10/100/1000 Base-T QRadar management interface One 10/100 Base-T integrated management module interface Napatech Network Adapter for fiber, providing two 10 Gbps SFP + network monitoring interfaces.
Memory	16 GB, 4 x 4GB 1600 MHz RDIMM
Storage	600 GB 10 K rpm SAS, 600 MB total (Raid 1)
Power supply	Dual Redundant 750 W AC
Dimensions	27.57 inches deep x 18.99 inches wide x 1.68 inches high
Included components	QRadar QFlow Collector NT20E2 Napatech Network Adaptor

For information about battery replacement, see Battery Replacement (http://www.dell.com/support/manuals/us/en/19/poweredge-r630/R630_OM_Publication_v3-v3/Replacing-the-system-battery?guid=GUID-364314C7-E137-4FC1-9B63-F9DD3BC9E582&lang=en-us).

QRadar 1400 Data Node

The IBM Security QRadar 1400 Data Node (MTM 4380-Q1E) appliance provides scalable data storage solution for QRadar deployments. The QRadar 1400 Data Node enhances data retention capabilities of a deployment as well as augment overall query performance.

View hardware information and requirements for the QRadar 1400 Data Node in the following tables:

Table 27. QRadar 1400 Data Node when used with XX05 appliances

Description	Value
Interfaces	Two 10/100/1000 Base-T network monitoring interfaces One 10/100/1000 Base-T QRadar management interface One 10/100 Base-T integrated management module interface Two 10 Gbps SFP + ports
Memory	64 GB 8x 8 GB 1600 MHz RDIMM
Storage	Storage: 9 x 3.5 inch 1 TB 7.2 K rpm NL SAS, 9 TB total, 6.2 TB usable (Raid 5)
Power supply	Dual Redundant 750 W AC
Dimensions	29.5 inches deep x 17.7 inches wide x 2.4 inches high
Included components	QRadar Data Node appliance

Table 28. QRadar 1400 Data Node when used with XX28 appliances

Description	Value
Interfaces	One 2-port Emulex 8Gb FC Two 10/100/1000 Base-T network monitoring interface One 10/100/1000 Base-T QRadar management interface One 10/100 Base-T integrated management module interface Two 10 Gbps SFP + ports
Memory	128 GB, 8 x 16 GB 1866 MHz RDIMM8
Storage	40 TB or larger dedicated event storage: 12 x 3.5 inch 4 TB SAS 7.2 K rpm, 48 TB total, 40 TB usable (Raid 6)
Power supply	Dual Redundant 900 W AC
Dimensions	29.5 inches deep x 17.7 inches wide x 2.4 inches high
Included components	QRadar Data Node appliance

QRadar 1400-C Data Node

The IBM Security QRadar 1400-C Data Node FIPS-compliant appliance provides scalable data storage solution for QRadar deployments. The QRadar 1400-C Data Node enhances data retention capabilities of a deployment as well as augment overall query performance.

View hardware information and requirements for the QRadar 1400-C Data Node in the following table:

Table 29. QRadar 1400-C Data Node specifications

Description	Value
Basic license	2,500 EPS
Upgraded license	40,000 EPS

Table 29. QRadar 1400-C Data Node specifications (continued)

Description	Value
Interfaces	One 2-port Emulex 8 Gbps FC Three 10/100/1000 Base-T network monitoring interfaces One 10/100/1000 Base-T QRadar management interface One 10/100 Base-T integrated remote system management interface Two 10 Gbps SFP + ports
Memory	128 GB, 8 x16 GB 2133 MT/s DDR4 RDIMM
Storage	12 x 3.5 inch 4 TB SAS 7.2 K rpm, 48 TB total, 40 TB usable (Raid 6)
Power supply	Dual redundant 750 W AC
Dimensions	29.5 inches deep x 17.7 inches wide x 2.4 inches high
Included components	Data Node

QRadar Event Collector 1501

The IBM Security QRadar Event Collector 1501 (MTM 4380-Q2C) appliance is a dedicated event collector. By default, a dedicated event collector collects and parses event from various log sources and continuously forwards these events to an event processor. You can configure the QRadar Event Collector 1501 appliance to temporarily store events and only forward the stored events on a schedule. A dedicated event collector does not process events and it does not include an on-board event processor.

View hardware information and requirements for the QRadar Event Collector 1501 in the following table:

Table 30. QRadar Event Collector 1501 specifications

Description	Value
Events per second	15,000 EPS
Network traffic	1 Gbps
Interfaces	Five 10/100/1000 Base-T network monitoring interfaces Two 10 Gbps SFP + ports One 10/100/1000 Base-T QRadar management interface One 10/100 Base-T integrated management module interface
Memory	16 GB, 4 x 4GB 1600 MHz RDIMM
Storage	2 x 2.5 inch 600 GB 10 K rpm SAS, 600 MB total (Raid 1)
Power supply	Dual Redundant 550 W AC
Dimensions	28.9 inches deep x 16.9 inches wide x 1.7 inches high
Included components	Event Collector

QRadar Event Processor 1605

The IBM Security QRadar Event Processor 1605 (MTM 4380-Q1E) appliance is a dedicated event processor that you can scale your QRadar deployment to manage higher EPS rates. The QRadar Event Processor 1605 appliance includes an on-board event collector, event processor, and internal storage for events.

The QRadar Event Processor 1605 is a distributed event processor appliance and requires a connection to a IBM Security QRadar 3105 (Console) or QRadar 3128 (Console) appliance.

View hardware information and requirements for the QRadar Event Processor 1605 in the following table:

Table 31. QRadar Event Processor 1605

Description	Value
Basic license	2,500 EPS
Upgraded license	20,000 EPS
Interfaces	Two 10/100/1000 Base-T network monitoring interfaces One 10/100/1000 Base-T QRadar management interface One 10/100 Base-T integrated management module interface Two 10 Gbps SFP + ports
Memory	Memory: 64 GB 8x 8 GB 1600 MHz RDIMM
Storage	Storage: 9 x 3.5 inch 1 TB 7.2 K rpm NL SAS, 9 TB total, 6.2 TB usable (Raid 5)
Power supply	Dual Redundant 750 W AC
Dimensions	29.5 inches deep x 17.7 inches wide x 2.4 inches high
Included components	Event Collector Event Processor

For diagrams and information about the front and back panel of this appliance, see "QRadar M4 Consoles and Processors and Data Nodes" on page 42.

QRadar Event Processor 1628

The IBM Security QRadar Event Processor 1628 (MTM 4380-Q2E) appliance is a dedicated event processor that you can use to scale your QRadar deployment to manage higher EPS rates. The QRadar Event Processor 1628 appliance includes an on-board event collector, event processor, and internal storage for events.

The QRadar Event Processor 1628 is a distributed event processor appliance and requires a connection to a QRadar 3128 (Console) appliance.

View hardware information and requirements for the QRadar Event Processor 1628 in the following table:

Table 32. QRadar Event Processor 1628 Event Processor overview

Description	Value
Basic license	2,500 EPS

Table 32. QRadar Event Processor 1628 Event Processor overview (continued)

Description	Value
Upgraded license	40,000 EPS
Interfaces	One 2-port Emulex 8Gb FC Two 10/100/1000 Base-T network monitoring interfaces One 10/100/1000 Base-T QRadar management interface One 10/100 Base-T integrated management module interface Two 10 Gbps SFP + ports
Memory	128 GB, 8 x 16 GB 1866 MHz RDIMM8
Storage	12 x 3.5 inch 4 TB SAS 7.2 K rpm, 48 TB total, 40 TB usable (Raid 6)
Power supply	Dual Redundant 900 W AC Power Supply
Dimensions	29.5 inches deep x 17.6 inches wide x 3.4 inches high
Included components	Event Collector Event Processor

IBM Security QRadar Event Processor 1628-C

The IBM Security QRadar Event Processor 1628-C FIPS-compliant appliance is a dedicated event processor that you can use to scale your QRadar deployment to manage higher events per second (EPS) rates. The IBM Security QRadar Event Processor 1628-C appliance includes an onboard event collector, event processor, and internal storage for events.

The IBM Security QRadar Event Processor 1628-C is a distributed event processor appliance and requires a physical connection to a QRadar 3128-C (Console) Console appliance.

View hardware information and requirements for the IBM Security QRadar Event Processor 1628-C in the following table:

Table 33. IBM Security QRadar Event Processor 1628-C FIPS-compliant Event Processor specifications

Description	Value
Basic license	2,500 EPS
Upgraded license	40,000 EPS
Interfaces	One 2-port Emulex 8Gb FC Three 10/100/1000 Base-T network monitoring interfaces One 10/100/1000 Base-T QRadar management interface One 10/100 Base-T integrated remote system management interface Two 10 Gbps SFP + ports
Memory	128 GB, 8 x16 GB 2133 MT/s DDR4 RDIMM
Storage	12 x 3.5 inch 4 TB SAS 7.2 K rpm, 48 TB total, 40 TB usable (Raid 6)
Power supply	Dual redundant 750 W AC
Dimensions	29.5 inches deep x 17.7 inches wide x 2.4 inches high

Table 33. IBM Security QRadar Event Processor 1628-C FIPS-compliant Event Processor specifications (continued)

Description	Value
Included components	Event Collector Event Processor

QRadar Flow Processor 1705

The IBM Security QRadar Flow Processor 1705 (MTM 4380-Q1E) appliance is a flow processor that can scale your QRadar deployment to manage higher FPM rates. The QRadar Flow Processor 1705 includes an on-board Flow processor, and internal storage for flows.

View hardware information and requirements for the QRadar Flow Processor 1705 in the following table:

Table 34. QRadar Flow Processor 1705

Description	Value
Basic license	100,000 FPM
Upgraded license	600,000 FPM, depending on traffic types
Interfaces	Two 10/100/1000 Base-T network monitoring interfaces One 10/100/1000 Base-T QRadar management interface One 10/100 Base-T integrated management module interface Two 10 Gbps SFP + ports
Memory	64 GB 8x 8 GB 1600 MHz RDIMM
Storage	9 x 3.5 inch 1 TB 7.2 K rpm NL SAS, 9 TB total, 6.2 TB usable (Raid 5)
Power supply	Dual Redundant 750 W AC
Dimensions	29.5 inches deep x 17.7 inches wide x 2.4 inches high
Included components	Flow processor

QRadar Flow Processor 1728

The IBM Security QRadar Flow Processor 1728 (MTM 4380-Q2E) appliance is a flow processor that can scale your QRadar deployment to manage higher FPM rates. The QRadar Flow Processor 1728 includes an on-board Flow processor, and internal storage for flows.

View hardware information and requirements for the QRadar Flow Processor 1728 in the following table:

Table 35. QRadar Flow Processor 1728 overview

Description	Value
Basic license	100,000 FPM
Upgraded license	1,200,000 FPM

Table 35. QRadar Flow Processor 1728 overview (continued)

Description	Value
Interfaces	One 2-port Emulex 8Gb FC Two 10/100/1000 Base-T network monitoring interfaces One 10/100/1000 Base-T IBM Security QRadar management interface One 10/100 Base-T integrated management module interface Two 10 Gbps SFP + ports
Memory	128 GB, 8 x 16 GB 1866 MHz RDIMM8
Storage	12 x 3.5 inch 4 TB SAS 7.2 K rpm, 48 TB total, 40 TB usable (Raid 6)
Power supply	Dual Redundant 900 W AC Power Supply
Dimensions	29.5 inches deep x 17.6 inches wide x 3.4 inches high
Included components	Flow Processor

QRadar Flow Processor 1728-C

The IBM Security QRadar Flow Processor 1728-C FIPS-compliant appliance is a flow processor that can scale your QRadar deployment to manage higher flows per minute (FPM) rates. The QRadar Flow Processor 1728-C appliance includes an onboard flow processor, and internal storage for flows.

View hardware information and requirements for the QRadar Flow Processor 1728-C in the following table:

Table 36. FIPS-compliant QRadar Flow Processor 1728-C

Description	Value
Basic license	100,000 FPM
Upgraded license	1,200,000 FPM
Interfaces	One 2-port Emulex 8 Gbps FC Three 10/100/1000 Base-T network monitoring interfaces One 10/100/1000 Base-T QRadar management interface One 10/100 Base-T integrated remote system management interface Two 10 Gbps SFP + ports
Memory	128 GB, 8 x16 GB 2133 MT/s DDR4 RDIMM
Storage	12 x 3.5 inch 4 TB SAS 7.2 K rpm, 48 TB total, 40 TB usable (Raid 6)
Power supply	Dual redundant 750 W AC
Dimensions	29.5 inches deep x 17.7 inches wide x 2.4 inches high
Included components	Flow Processor

QRadar 1805

The QRadar 1805 (MTM 4380-Q1E) appliance is a combined Event Processor and Flow Processor that can scale your QRadar deployment to manage more events and flows. The QRadar 1805 includes an on-board Event Processor, an on-board Flow Processor, and internal storage for events and flows.

View hardware information and requirements for the QRadar 1805 in the following table:

Table 37. QRadar 1805 overview

Description	Value
Basic license	25,000 FPM 1,000 EPS
Upgraded license	200,000 FPM 5,000 EPS
Interfaces	Two 10/100/1000 Base-T network monitoring interfaces One 10/100/1000 Base-T QRadar management interface One 10/100 Base-T integrated management module interface Two 10 Gbps SFP + ports
Memory	64 GB 8x 8 GB 1600 MHz RDIMM
Storage	9 x 3.5 inch 1 TB 7.2 K rpm NL SAS, 9 TB total, 6.2 TB usable (Raid 5)
Power supply	Dual Redundant 750 W AC
Dimensions	29.5 inches deep x 17.7 inches wide x 2.4 inches high
Included components	Event processor Flow processor

QRadar Flow Processor 1828

The IBM Security QRadar Flow Processor 1828 (MTM 4380-Q2E) appliance is a combined Event Processor and Flow Processor that you can scale your QRadar deployment to manage more event and flows. The QRadar Flow Processor 1828 includes an on-board Event Processor, an on-board Flow Processor, and internal storage for events and flows.

View hardware information and requirements for the QRadar Flow Processor 1828 in the following table:

Table 38. QRadar Flow Processor 1828 overview

Description	Value
Basic license	25,000 FPM, 1000 EPS
Upgraded license	300,000 FPM 15,000 EPS

Table 38. QRadar Flow Processor 1828 overview (continued)

Description	Value
Interfaces	One 2-port Emulex 8Gb FC Two 10/100/1000 Base-T network monitoring interfaces One 10/100/1000 Base-T IBM Security QRadar management interface One 10/100 Base-T integrated management module interface Two 10 Gbps SFP + ports
Memory	128 GB, 8 x 16 GB 1866 MHz RDIMM8
Storage	12 x 3.5 inch 4 TB SAS 7.2 K rpm, 48 TB total, 40 TB usable (Raid 6)
Power supply	Dual Redundant 900 W AC Power Supply
Dimensions	29.5 inches deep x 17.6 inches wide x 3.4 inches high
Included components	Flow Processor

QRadar Flow Processor 1828-C

The IBM Security QRadar Flow Processor 1828-C FIPS-compliant appliance is a combined Event Processor and Flow Processor that you can scale your QRadar deployment to manage more event and flows. The QRadar Flow Processor 1828-C includes an onboard event processor, an onboard flow processor, and internal storage for events and flows.

View hardware information and requirements for the QRadar Flow Processor 1828-C in the following table:

Table 39. QRadar Flow Processor 1828-C FIPS-compliant Flow Processor specifications

Description	Value
Basic license	25,000 FPM, 1000 EPS
Upgraded license	300,000 FPM 15,000 EPS
Interfaces	One 2-port Emulex 8 Gbps FC Three 10/100/1000 Base-T network monitoring interfaces One 10/100/1000 Base-T QRadar management interface One 10/100 Base-T integrated remote system management interface Two 10 Gbps SFP + ports
Memory	128 GB, 8 x16 GB 2133 MT/s DDR4 RDIMM
Storage	12 x 3.5 inch 4 TB SAS 7.2 K rpm, 48 TB total, 40 TB usable (Raid 6)
Power supply	Dual redundant 750 W AC
Dimensions	29.5 inches deep x 17.7 inches wide x 2.4 inches high
Included components	Flow Processor

QRadar 2100

The IBM Security QRadar 2100 (MTM 4380-Q1C) appliance is an all-in-one system that combines Network Behavioral Anomaly Detection (NBAD) and Security Information and Event Management (SIEM) to accurately identify and appropriately prioritize threats that occur on your network.

View hardware information and requirements for the QRadar 2100 in the following table:

Table 40. QRadar 2100 overview

Description	Value
Basic license	25,000 FPM 1000 EPS
Upgraded license	50,000 FPM
Interfaces	Three 10/100/1000 Base-T network monitoring interfaces One 10/100/1000 Base-T IBM Security QRadar management interface One 10/100 Base-T integrated management module interface Two 10 Gbps SFP + ports
Memory	32 GB, 4 x 8GB 1600 MHz RDIMM
Storage	6 x 2.5 inch 500 GB 7.2K rpm SATA, 3 TB total, 1.5 TB usable (Raid 10)
Power supply	Dual Redundant 750 W AC
Dimensions	28.9 inches deep x 16.9 inches wide x 1.7 inches high
Included components	Event Collector Event Processor Single QRadar QFlow Collector

Additional QRadar QFlow Collectors are sold separately.

QRadar 3105 (All-in-One)

The IBM Security QRadar 3105 (All-in-One) (MTM 4380-Q1E) appliance is an all-in-one QRadar system that can profile network behavior and identify network security threats.

View hardware information and requirements for the QRadar 3105 (All-in-One) in the following table:

Table 41. QRadar 3105 (All-in-One) overview

Description	Value
Basic license	25,000 FPM 1000 EPS
Upgraded license	200,000 FPM 5,000 EPS
Network objects	1000

Table 41. QRadar 3105 (All-in-One) overview (continued)

Description	Value
Log sources	750
Interfaces	Two 10/100/1000 Base-T network monitoring interfaces One 10/100/1000 Base-T QRadar management interface One 10/100 Base-T integrated management module interface Two 10 Gbps SFP + ports
Memory	64 GB 8x 8 GB 1600 MHz RDIMM
Storage	9 x 3.5 inch 1 TB 7.2 K rpm NL SAS, 9 TB total, 6.2 TB usable (Raid 5)
Power supply	Dual Redundant 750 W AC Power Supply
Dimensions	29.5 inches deep x 17.7 inches wide x 2.4 inches high
Included components	Event Collector Event Processor for processing events and flows Internal storage for events and flows

The QRadar 3105 (All-in-One) appliance requires external QRadar QFlow Collectors for layer 7 network activity monitoring.

QRadar 3105 (Console)

Understand and expand the capacity of the QRadar 3105 (All-in-One).

You can expand the capacity of the QRadar 3105 (All-in-One) beyond license-based upgrade options by upgrading to the IBM Security QRadar 3105 (Console) (MTM 4380-Q1E) appliance and adding one or more of the following appliances:

- QRadar Event Processor 1605
- QRadar Flow Processor 1705
- QRadar 1805

The QRadar 3105 (Console) appliance you can use to manage a distributed deployment of Event Processors and Flow Processors to profile network behavior and identify network security threats.

QRadar 3128 (All-in-One)

The IBM Security QRadar 3128 (All-in-One) (MTM 4380-Q2E) appliance is an all-in-one QRadar system that can profile network behavior and identify network security threats.

View hardware information and requirements for the QRadar 3128 (All-in-One) in the following table:

Table 42. QRadar 3128 (All-in-One)

Description	Value
Basic license	25,000 FPM 1000 EPS

Table 42. QRadar 3128 (All-in-One) (continued)

Description	Value
Upgraded license	300,000 FPM 15,000 EPS
Network objects	Up to 1,000, depending on the license
Log sources	750 (add more devices with a licensing option)
Interfaces	One 2-port Emulex 8Gb FC Two 10/100/1000 Base-T network monitoring interface One 10/100/1000 Base-T QRadar management interface One 10/100 Base-T integrated management module interface Two 10 Gbps SFP + ports
Memory	128 GB, 8 x 16 GB 1866 MHz RDIMM8
Storage	12 x 3.5 inch 4 TB SAS 7.2 K rpm, 48 TB total, 40 TB usable (Raid 6)
Power supply	Dual Redundant 900 W AC
Dimensions	29.5 inches deep x 17.6 inches wide x 3.4 inches high
Included components	Event Collector Event Processor for processing events and flows Internal storage for events and flows

The QRadar 3128 (All-in-One) requires external QRadar QFlow Collectors for layer 7 network activity monitoring.

QRadar 3128-C (All-in-One)

The IBM Security QRadar 3128-C (All-in-One) FIPS-compliant appliance is an all-in-one QRadar system that can profile network behavior and identify network security threats.

View hardware information and requirements for the QRadar 3128-C (All-in-One) in the following table:

Table 43. QRadar 3128-C (All-in-One) specifications

Description	Value
Basic license	25,000 FPM 1000 EPS
Upgraded license	300,000 FPM 15,000 EPS
Network objects	Up to 1,000, depending on the license
Log sources	750 (add more devices with a licensing option)

Table 43. QRadar 3128-C (All-in-One) specifications (continued)

Description	Value
Interfaces	One 2-port Emulex 8 Gbps FC Three 10/100/1000 Base-T network monitoring interface One 10/100/1000 Base-T QRadar management interface One 10/100 Base-T integrated remote system management interface Two 10 Gbps SFP + ports
Memory	128 GB, 8 x16 GB 2133 MT/s DDR4 RDIMM
Storage	12 x 3.5 inch 4 TB SAS 7.2 K rpm, 48 TB total, 40 TB usable (Raid 6)
Power supply	Dual redundant 750 W AC
Dimensions	29.5 inches deep x 17.7 inches wide x 2.4 inches high
Included components	Event Collector Event Processor Internal storage for events and flows

The QRadar 3128-C (All-in-One) requires external QRadar QFlow Collectors for layer 7 network activity monitoring.

QRadar 3128 (Console)

Understand expansion options for the IBM Security QRadar

You can expand the capacity of the QRadar 3128-C (All-in-One) appliance beyond license-based upgrade options by upgrading to the IBM Security QRadar 3128 (Console) (MTM 4380-Q2E) appliance and adding one or more of the following appliances:

- QRadar Event Processor 1628
- QRadar Flow Processor 1728
- QRadar Flow Processor 1828

The QRadar 3128 (Console) appliance you can use to manage a distributed deployment of Event Processors and Flow Processors to profile network behavior and identify network security threats.

QRadar 3128-C (Console)

Use the QRadar 3128-C (Console) FIPS-compliant appliance to manage a distributed deployment of Event Processors and Flow Processors so that you can profile network behavior and identify network security threats.

You can expand the capacity of the IBM Security QRadar 3128-C (All-in-One) FIPS-compliant appliance beyond license-based upgrade options by upgrading to the QRadar 3128-C (Console) appliance and FIPS compliant flow and event processor appliances. For example, add one or more of these appliances:

- IBM Security QRadar Event Processor 1628-C

- IBM Security QRadar Flow Processor 1728-C
- IBM Security QRadar Flow Processor 1828-C

QRadar Log Manager 1605

The IBM Security QRadar Log Manager 1605 (MTM 4380-Q1E) appliance is a distributed Event Processor appliance and requires a connection to a QRadar Log Manager 3105 Console appliance.

View hardware information and requirements for the QRadar Log Manager 1605 in the following table:

Table 44. QRadar Log Manager 1605

Description	Value
Basic license	2,500 EPS
Upgraded license	20,000 EPS
Interfaces	Two 10/100/1000 Base-T network monitoring interfaces One 10/100/1000 Base-T QRadar management interface One 10/100 Base-T integrated management module interface Two 10 Gbps SFP + ports
Memory	64 GB 8x 8 GB 1600 MHz RDIMM
Storage	9 x 3.5 inch 1 TB 7.2 K rpm NL SAS, 9 TB total, 6.2 TB usable (Raid 5)
Power supply	Dual Redundant 750 W AC
Dimensions	29.5 inches deep x 17.7 inches wide x 2.4 inches high
Included components	Event Collector Event Processor

QRadar Log Manager 1628

The IBM Security QRadar Log Manager 1628 (MTM 4380-Q2E) appliance is a dedicated Event Processor that you can use to scale your QRadar Log Manager deployment to manage higher Event Per Second (EPS) rates. The QRadar Log Manager 1628 appliance includes an on-board Event Collector, Event Processor, and internal storage for events.

The QRadar Log Manager 1628 is a distributed Event Processor appliance and requires a connection to a QRadar Log Manager 3128 (Console).

View hardware information and requirements for the QRadar Log Manager 1628 in the following table:

Table 45. QRadar Log Manager 1628

Description	Value
Basic license	20,000 EPS
Upgraded license	40,000 EPS

Table 45. QRadar Log Manager 1628 (continued)

Description	Value
Interfaces	One 2-port Emulex 8Gb FC Two 10/100/1000 Base-T network monitoring interfaces One 10/100/1000 Base-T QRadar management interface One 10/100 Base-T integrated management module interface Two 10 Gbps SFP + ports
Memory	128 GB, 8 x 16 GB 1866 MHz RDIMM8
Storage	12 x 3.5 inch 4 TB SAS 7.2 K rpm, 48 TB total, 40 TB usable (Raid 6)
Power supply	Dual Redundant 900 W AC
Dimensions	29.5 inches deep x 17.6 inches wide x 3.4 inches high
Included components	Event Collector Event Processor

QRadar Log Manager 1628-C

The IBM Security QRadar Log Manager 1628-C FIPS-compliant appliance is a dedicated Event Processor that you can use to scale your QRadar Log Manager deployment to manage higher event per second (EPS) rates. The QRadar Log Manager 1628-C appliance includes an onboard event collector, event processor, and internal storage for events.

The QRadar Log Manager 1628-C is a distributed Event Processor appliance and requires a connection to a QRadar Log Manager 3128-C (Console) appliance.

View hardware information and requirements for the QRadar Log Manager 1628-C in the following table:

Table 46. QRadar Log Manager 1628-C FIPS-compliant specifications

Description	Value
Basic license	20,000 EPS
Upgraded license	40,000 EPS
Interfaces	One 2-port Emulex 8 Gbps FC Three 10/100/1000 Base-T network monitoring interfaces One 10/100/1000 Base-T QRadar management interface One 10/100 Base-T integrated remote system management interface Two 10 Gbps SFP + ports
Memory	128 GB, 8 x16 GB 2133 MT/s DDR4 RDIMM
Storage	12 x 3.5 inch 4 TB SAS 7.2 K rpm, 48 TB total, 40 TB usable (Raid 6)
Power supply	Dual redundant 750 W AC
Dimensions	29.5 inches deep x 17.7 inches wide x 2.4 inches high
Included components	Event Collector Event Processor

QRadar Log Manager 2100

The IBM Security QRadar Log Manager 2100 (MTM 4380-Q1C) appliance is an all-in-one system that can manage and store events from various network devices.

View hardware information and requirements for the QRadar Log Manager 2100 in the following table:

Table 47. QRadar Log Manager 2100 overview

Description	Value
Basic license	1000 EPS
Log sources	750
Interfaces	Three 10/100/1000 Base-T network monitoring interfaces One 10/100/1000 Base-T IBM Security QRadar management interface One 10/100 Base-T integrated management module interface Two 10 Gbps SFP + ports
Memory	32 GB, 4 x 8GB 1600 MHz RDIMM
Storage	6 x 2.5 inch 500 GB 7.2K rpm SATA, 3 TB total, 1.5 TB usable (Raid 10)
Power supply	Dual Redundant 750 W AC
Dimensions	28.9 inches deep x 16.9 inches wide x 1.7 inches high
Included components	Event Collector Event Processor

QRadar Log Manager 2100 includes external flow collection.

Additional QRadar QFlow Collectors are sold separately.

QRadar Log Manager 3105 (All-in-One)

The IBM Security IBM Security QRadar Log Manager 3105 (All-in-One) (MTM 4380-Q1E) appliance is an all-in-one system that you can use to manage and store events from various network devices.

View hardware information and requirements for the QRadar Log Manager 3105 (All-in-One) in the following table:

Table 48. QRadar Log Manager 3105 (All-in-One) overview

Description	Value
Basic license	25,000 FPM 1000 EPS
Upgraded license	200,000 FPM 5,000 EPS

Table 48. QRadar Log Manager 3105 (All-in-One) overview (continued)

Description	Value
Interfaces	Two 10/100/1000 Base-T network monitoring interfaces One 10/100/1000 Base-T QRadar management interface One 10/100 Base-T integrated management module interface Two 10 Gbps SFP + ports
Memory	64 GB 8x 8 GB 1600 MHz RDIMM
Storage	9 x 3.5 inch 1 TB 7.2 K rpm NL SAS, 9 TB total, 6.2 TB usable (Raid 5)
Power supply	Dual Redundant 750 W AC Power Supply
Dimensions	29.5 inches deep x 17.7 inches wide x 2.4 inches high
Included components	Event Collector Event Processor for processing events Internal storage for events

You can upgrade your license to migrate your QRadar Log Manager 3105 (All-in-One) to QRadar 3105 (All-in-One). For more information, see the *Migrating QRadar Log Manager to QRadar SIEM Technical Note*.

QRadar Log Manager 3105 Console

You can expand the capacity of the QRadar Log Manager 3105 (All-in-One) appliance beyond license-based upgrade options by upgrading to the IBM Security QRadar Log Manager 3105 (Console) (MTM 4380-Q1E) appliance. You must also add one or more QRadar Log Manager 1605 or QRadar Log Manager 1628 appliances.

The QRadar Log Manager 3105 Console appliance manages a distributed deployment of Event Processors to collect and process events. You can upgrade your license from QRadar Log Manager 3105 Console to QRadar 3105 (Console).

QRadar Log Manager 3128 (All-in-One)

The IBM Security QRadar Log Manager 3128 (All-in-One) (MTM 4380-Q2E) appliance is an all-in-one system that you can use to manage and store events from various network devices.

View hardware information and requirements for the QRadar Log Manager 3128 (All-in-One) in the following table:

Table 49. QRadar Log Manager 3128 (All-in-One)

Description	Value
Basic license	1,000 EPS
Upgraded license	15,000 EPS
Network objects	Up to 1,000, depending on the license
Log sources	750 (add more devices with a licensing option)

Table 49. QRadar Log Manager 3128 (All-in-One) (continued)

Description	Value
Interfaces	One 2-port Emulex 8Gb FC Two 10/100/1000 Base-T network monitoring interface One 10/100/1000 Base-T QRadar management interface One 10/100 Base-T integrated management module interface Two 10 Gbps SFP + ports
Memory	128 GB, 8 x 16 GB 1866 MHz RDIMM8
Storage	12 x 3.5 inch 4 TB SAS 7.2 K rpm, 48 TB total, 40 TB usable (Raid 6)
Power supply	Dual Redundant 900 W AC
Dimensions	29.5 inches deep x 17.6 inches wide x 3.4 inches high
Included components	Event Collector Event Processor Internal storage for events

You can upgrade your license to migrate your QRadar Log Manager 3128 (All-in-One) appliance to QRadar 3128 (All-in-One). For more information about migrating QRadar Log Manager to QRadar SIEM, see the *Migrating QRadar Log Manager to QRadar SIEM Technical Note*.

QRadar Log Manager 3128-C (All-in-One)

The IBM Security QRadar Log Manager 3128-C (All-in-One) FIPS-compliant appliance is an all-in-one system that you can use to manage and store events from various network devices.

View hardware information and requirements for the QRadar Log Manager 3128-C (All-in-One) in the following table:

Table 50. QRadar Log Manager 3128-C (All-in-One) FIPS-compliant specifications

Description	Value
Basic license	1,000 EPS
Upgraded license	15,000 EPS
Network objects	Up to 1,000, depending on the license
Log sources	750 (add more devices with a licensing option)
Interfaces	One 2-port Emulex 8 Gbps FC Three 10/100/1000 Base-T network monitoring interface One 10/100/1000 Base-T QRadar management interface One 10/100 Base-T integrated remote system management interface Two 10 Gbps SFP + ports
Memory	128 GB, 8 x16 GB 2133 MT/s DDR4 RDIMM
Storage	12 x 3.5 inch 4 TB SAS 7.2 K rpm, 48 TB total, 40 TB usable (Raid 6)
Power supply	Dual redundant 750 W AC

Table 50. QRadar Log Manager 3128-C (All-in-One) FIPS-compliant specifications (continued)

Description	Value
Dimensions	29.5 inches deep x 17.7 inches wide x 2.4 inches high
Included components	Event Collector Event Processor Internal storage for events

You can upgrade your license to migrate your QRadar Log Manager 3128-C (all-in-one) appliance to QRadar 3128-C (all-in-one). For more information about migrating QRadar Log Manager to QRadar SIEM, see the *Migrating QRadar Log Manager to QRadar SIEM Technical Note*.

QRadar Log Manager 3128 (Console)

The IBM Security QRadar Log Manager 3128 (Console) (MTM 4380-Q2E) appliance manages a distributed deployment of Event Processors to collect and process events.

You can expand the capacity of the QRadar Log Manager 3128 (All-in-One) appliance beyond license-based upgrade options by upgrading to the QRadar Log Manager 3128 (Console) appliance and adding one or more of the following appliances:

- QRadar Log Manager 1605
- QRadar Log Manager 1628

You can upgrade your license to migrate your QRadar Log Manager 3128 (Console) appliance to QRadar 3128 (Console). For more information, see the *Migrating QRadar Log Manager to QRadar SIEM Technical Note*.

QRadar Log Manager 3128-C (Console)

The IBM Security QRadar Log Manager 3128-C (Console) FIPS-compliant appliance manages a distributed deployment of Event Processors to collect and process events.

You can expand the capacity of the QRadar Log Manager 3128-C (all-in-one) appliance beyond license-based upgrade options by upgrading to the QRadar Log Manager 3128-C (Console) appliance and adding one or more of the following appliances:

- "QRadar Event Processor 1628" on page 21

You can upgrade your license to migrate your QRadar Log Manager 3128-C (Console) appliance to QRadar Log Manager 3128-C (Console). For more information, see the *Migrating QRadar Log Manager to QRadar SIEM Technical Note* .

The QRadar Log Manager 3128-C (Console) appliance manages a distributed deployment of Event Processors to collect and process events.

QRadar Vulnerability Manager

The IBM Security QRadar Vulnerability Manager appliance scans and reports on network vulnerabilities. QRadar Vulnerability Manager provides a vulnerability management workflow that is fully integrated with QRadar SIEM and is available as a software option, appliance, and virtual appliance.

QRadar Vulnerability Manager provides the following capabilities:

- Scans inside and outside your network, network infrastructure, servers, and end points for bad configurations, weak settings, unpatched products, and other key weaknesses.
- Uses network usage, threat environment, security configuration information, virtual patch, and patch availability to bring real context to vulnerability management, which drives efficient remediation processes
- Integrates all vulnerability information from external systems to provide a single view.
- Full integration with the QRadar asset profile database to provide intelligent event-driven scans.
- Unlimited QRadar Vulnerability Manager discovery scans
- Use of hosted scanner for DMZ scanning

The QRadar Vulnerability Manager appliance supports:

Table 51. QRadar Vulnerability Manager overview

Description	Value
Basic license	255 assets
Upgraded license	32,768
Interfaces	Two 10/100/1000 Base-T network monitoring interfaces One 10/100/1000 Base-T QRadar management interface One 10/100 Base-T integrated management module interface Two 10 Gbps SFP + ports
Memory	64 GB 8x 8 GB 1600 MHz RDIMM
Storage	9 x 3.5 inch 1 TB 7.2 K rpm NL SAS, 9 TB total, 6.2 TB usable (Raid 5)
Power supply	Dual Redundant 750 W AC Power Supply
Dimensions	29.5 inches deep x 17.7 inches wide x 2.4 inches high
Included components	QRadar Vulnerability Manager

For diagrams and information about the front and back panel of this appliance, see "QRadar M4 Consoles and Processors and Data Nodes" on page 42.

QRadar Risk Manager

The IBM Security QRadar appliance delivers a fully integrated risk management, vulnerability prioritization, and automated configuration solution that is integrated into the IBM Security QRadar platform. QRadar Log Manager enables tightly integrated features in QRadar SIEM that enhance incident management, log and network activity searches, threat visualization, and reports.

View hardware information and requirements for the QRadar Risk Manager in the following table:

Table 52. QRadar Risk Manager in the following table

Description	Value
Interfaces	Two 10/100/1000 Base-T network monitoring interfaces One 10/100/1000 Base-T QRadar SIEM management interface One 10/100 Base-T integrated management module interface Two 10 Gbps SFP + ports
Memory	64 GB 8x 8 GB 1600 MHz RDIMM
Storage	9 x 3.5 inch 1 TB 7.2 K rpm NL SAS, 9 TB total, 6.2 TB usable (Raid 5)
Power supply	Dual Redundant 750 W AC
Dimensions	29.5 inches deep x 17.7 inches wide x 2.4 inches high
Included components	QRadar Risk Manager

For diagrams and information about the front and back panel of this appliance, see "QRadar M4 Consoles and Processors and Data Nodes" on page 42.

QRadar Incident Forensics

Use IBM Security QRadar Incident Forensics to retrace the step-by-step actions of a potential attacker, and conduct an in-depth forensics investigation of suspected malicious network security incidents. QRadar Incident Forensics reduces the time it takes security teams to investigate offense records. It can also help you remediate a network security breach and prevent it from happening again.

QRadar Incident Forensics shares hardware with QRadar XX28 appliances. For more information about XX28 appliances, see "QRadar M4 Consoles and Processors and Data Nodes" on page 42.

QRadar Packet Capture

IBM Security QRadar Incident Forensics offers an optional IBM Security QRadar Packet Capture appliance to store and manage data that is used by QRadar Incident Forensics when no other network packet capture (PCAP) device is deployed. Any number of these appliances can be installed as a tap on a network or sub-network to collect the raw packet data.

View hardware information and requirements for QRadar Packet Capture in the following table:

Table 53. QRadar Packet Capture overview

Description	Value
Interfaces	Two 10/100/1000 Base-T network monitoring interfaces One 10/100/1000 Base-T IBM Security QRadar management interface One 10/100 Base-T integrated management module interface Four 10 Gbps SFP + ports

Table 53. QRadar Packet Capture overview (continued)

Description	Value
Memory	128 GB, 8 x 16 GB 1866 MHz RDIMM8
Storage	12 x 3.5 inch 4 TB SAS 7.2 K rpm, 41 TB total, 32 TB usable (Raid 5)
Power supply	Dual Redundant 900 W AC Power Supply
Dimensions	29.5 inches deep x 17.6 inches wide x 3.4 inches high
Included components	Flow Processor

For diagrams and information on the front and back panel of this appliance, see "QRadar M4 Consoles and Processors and Data Nodes" on page 42.

Chapter 3. Appliance Diagrams

View the diagrams and descriptions for the back and front panels of your appliance. These diagrams are representations of an IBM Security QRadar appliance. Your system might vary, depending on the version of appliance you purchased.

Integrated Management Module

On the back panel of each appliance type, the serial connector and Ethernet connectors can be managed using the Integrated Management Module (IMM). You can configure the IMM to share an Ethernet port with the IBM Security QRadar management interface; however, you can configure the IMM in dedicated mode to reduce the risk of losing the IMM connection when the appliance is restarted. To configure the IMM, you must access the System BIOS settings by pressing the F1 key when the IBM splash screen is displayed. For further instructions on how to configure the IMM, see the *Integrated Management Module User's Guide* that is located on the CD that was shipped with your appliance.

M3 QRadar 2100, QRadar Event Collector 1501, and all QRadar Flow Processor Appliances

Review the information about the front and back panel features for appliances to confirm proper connectivity and functionality.

- IBM Security QRadar QFlow Collector 1201 (MTM 4378-QC1)
- IBM Security QRadar QFlow Collector 1202 (MTM 4378-QC2)
- IBM Security QRadar QFlow Collector 1301 (MTM 4378-QD1)
- IBM Security QRadar QFlow Collector 1310-SR (MTM 4378-QSR), -LR (MTM 4378-QLR)
- IBM Security QRadar Event Collector 1501 (MTM 4378-Q21)
- IBM Security QRadar 2100 (MTM 4378-Q21)

For more information about QRadar M3 2100, QRadar Event Collector 1501, and all QRadar Flow Processor appliances, including front and back panel diagrams, see IBM System x3550 M3 (http://www.redbooks.ibm.com/abstracts/tips0804.html?Open).

QRadar M3 Consoles and Processors

Review the information about the front and back panel features for appliances to confirm proper connectivity and functionality.

- IBM Security QRadar Event Processor 1605 (MTM 4379-Q05)
- IBM Security QRadar Event Processor 1624 (MTM 4379-Q24)
- IBM Security QRadar Flow Processor 1705 (MTM 4379-Q05)
- IBM Security QRadar Flow Processor 1724 (MTM 4379-Q24)
- IBM Security QRadar 1805 (MTM 4379-Q05)
- IBM Security QRadar 3105 (Base) (MTM 4379-Q05)
- IBM Security QRadar 3105 (Console) (MTM 4379-Q05)
- IBM Security QRadar 3124 (Base) (MTM 4379-Q24)

- IBM Security QRadar 3124 (Console) (MTM 4379-Q24)
- IBM Security QRadar Log Manager 1605 (MTM 4379-Q05)
- IBM Security QRadar Log Manager 1624 (MTM 4379-Q24)
- IBM Security QRadar Log Manager 3105 (Base) (MTM 4379-Q05)
- IBM Security QRadar Log Manager 3105 (Console) (MTM 4379-Q05)
- IBM Security QRadar Log Manager 3124 (Base) (MTM 4379-Q24)
- IBM Security QRadar Log Manager 3124 (Console) (MTM 4379-Q24)
- "QRadar Vulnerability Manager" on page 12
- "QRadar Risk Manager" on page 13

For more information about IBM Security QRadar M3 Consoles, Processors and Data Nodes, including front and back panel diagrams, see IBM System x3630 M3 (http://www.redbooks.ibm.com/Redbooks.nsf/RedbookAbstracts/tips0807.html).

M4 QRadar 2100, QRadar Event Collector 1501, and all QRadar Flow Processor Appliances

Review the information about the front and back panel features for appliances to confirm proper connectivity and functionality.

- "QRadar 2100" on page 27 (4380-Q1C).
- "QRadar QFlow Collector 1202" on page 16 (4380-Q3C).
- "QRadar QFlow Collector 1301" on page 17 (4380-Q4C).
- "QRadar QFlow Collector 1310" on page 17 (4380-Q5C).
- "QRadar Event Collector 1501" on page 20, "QRadar QFlow Collector 1201" on page 15 (4380-Q2C).
- "QRadar Log Manager 2100" on page 33 (4380-Q1C).

For more information about QRadar M4 2100, QRadar Event Collector 1501, and all QRadar Flow Processor appliances, including front and back panel diagrams, see IBM System X3550 M4 (http://publib-b.boulder.ibm.com/abstracts/tips0851.html?Open).

QRadar M4 Consoles and Processors and Data Nodes

Review the information about the front and back panel features for appliances to confirm proper connectivity and functionality.

- "QRadar 1400 Data Node" on page 18 (4380-Q1E).
- "QRadar Event Processor 1605" on page 21 (4380-Q1E).
- "QRadar Event Processor 1628" on page 21 (4380-Q2E).
- "QRadar Flow Processor 1705" on page 23 (4380-Q1E).
- "QRadar Flow Processor 1728" on page 23 (4380-Q2E).
- "QRadar 3105 (All-in-One)" on page 27 (4380-Q1E).
- "QRadar 3105 (Console)" on page 28 (4380-Q1E).
- "QRadar 3128 (All-in-One)" on page 28 (4380-Q2E).
- "QRadar 3128 (Console)" on page 30 (4380-Q2E).
- "QRadar Log Manager 1605" on page 31 (4380-Q1E).
- "QRadar Log Manager 1628" on page 31 (4380-Q2E).
- "QRadar Log Manager 3105 (All-in-One)" on page 33 (4380-Q1E).
- "QRadar Log Manager 3105 Console" on page 34 (4380-Q1E).

- "QRadar Log Manager 3128 (All-in-One)" on page 34 (4380-Q2E).
- "QRadar Log Manager 3128 (Console)" on page 36 (4380-Q2E).
- "QRadar Vulnerability Manager" on page 37 (4380-Q1E).
- "QRadar Risk Manager" on page 37 (4380-Q1E).

For more information about IBM Security QRadar M4 Consoles, Processors and Data Nodes, including front and back panel diagrams, see IBM System X3650 M4 BD (http://www.redbooks.ibm.com/abstracts/tips1102.html?Open).

QRadar xx28-C Appliances

Review the information about the front and back panel features for appliances to confirm proper connectivity and functionality.

IBM Security QRadar xx28-C appliances are manufactured by Dell, and can be used for the following appliances:

- QRadar
- QRadar Risk Manager
- QRadar Vulnerability Manager
- QRadar Incident Forensics
- QRadar Packet Capture, including QRadar Packet Capture Data Node.

You can also use the QRadar xx28-C appliances for FIPS-compliance.

Important: To make an xx28-C appliance FIPS-compliant, the QRadar release must be FIPS-compliant, and your appliance must have the required physical security. For more information about physical security, see the *IBM Security QRadar Version 7.2.4 FIPS 140-2 Installation Guide*. QRadar Incident Forensics and QRadar Packet Capture are not FIPS-compliant.

- "QRadar 1400-C Data Node" on page 19
- "IBM Security QRadar Event Processor 1628-C" on page 22
- "QRadar Flow Processor 1728-C" on page 24
- "QRadar Flow Processor 1828-C" on page 26
- "QRadar 3128-C (All-in-One)" on page 29
- "QRadar 3128-C (Console)" on page 30
- "QRadar Log Manager 1628-C" on page 32
- "QRadar Log Manager 3128-C (All-in-One)" on page 35
- "QRadar Log Manager 3128-C (Console)" on page 36

Front panel indicators and features

View the front panel diagram and descriptions for the IBM Security QRadar FIPS-compliant appliance to understand the hardware features.

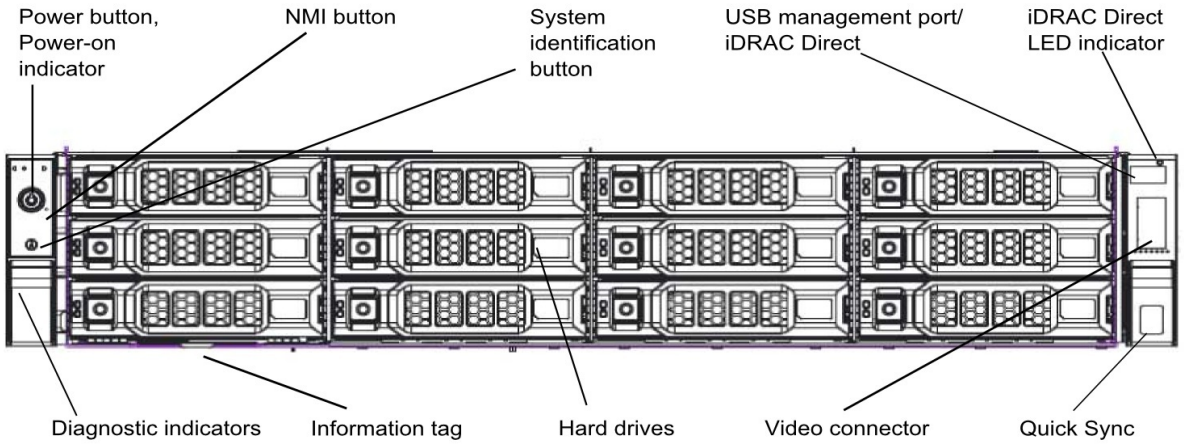

Figure 1. FIPS appliance front panel

Table 54. Front Panel Features of IBM Security QRadar FIPS Appliances

Feature	Description
Diagnostic indicators	The diagnostic indicators display error status.
System identification button	The identification buttons on the front and back panels can be used to locate a particular system within a rack. When one of these buttons is pressed, the system status indicator on the back flashes until one of the buttons is pressed again. Press to toggle the system ID on and off. If the system stops responding during POST, press and hold the system ID button for more than five seconds to enter BIOS progress mode. To reset the iDRAC (if not disabled in F2 iDRAC setup) press and hold the button for more than 15 seconds.
Power-on indicator, power button	The power-on indicator lights when the system power is on. The power button controls the power supply output to the system. **Note:** On ACPI-compliant operating systems, turning off the system using the power button causes the system to perform a graceful shutdown before power to the system is turned off.
NMI button	Used to troubleshoot software and device driver errors when running certain operating systems. This button can be pressed using the end of a paper clip. Use this button only if directed to do so by qualified support personnel or by the operating system's documentation.

Table 54. Front Panel Features of IBM Security QRadar FIPS Appliances (continued)

Feature	Description
Information tag	A slide-out label panel records system information such as Service Tag, NIC, MAC address, and so on.
Hard drives	Up to twelve 3.5 inch hot-swappable hard drives.
USB management port/iDRAC Direct	Connects USB devices to the system or provides access to the iDRAC Direct features. The USB management port is USB 2.0-compliant.
iDRAC Direct LED indicator	The indicator displays error status.
Video connector	Connects a VGA display to the system.
Quick Sync (optional)	Indicates a Quick Sync enabled system. The Quick Sync feature is optional and requires a Quick Sync bezel. This feature allows management of the system using mobile devices. This feature aggregates hardware and firmware inventory and various system level diagnostic and error information that can be used in troubleshooting the system.

Back panel indicators and features

View the back panel diagram and descriptions for the IBM Security QRadar FIPS-compliant appliance to understand the hardware features.

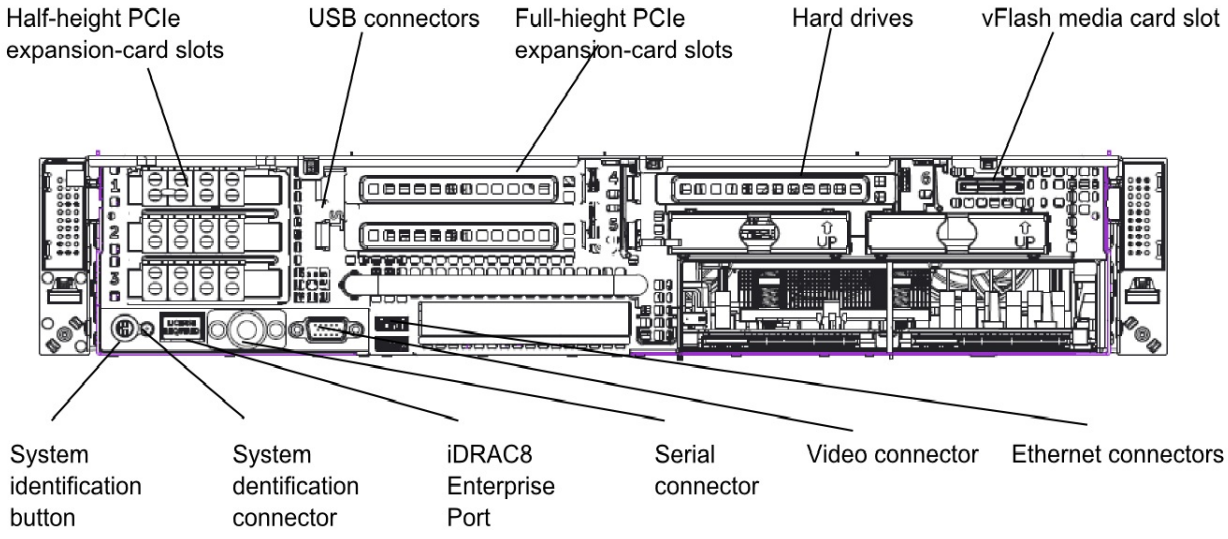

Figure 2. FIPS appliance back panel

Table 55. Back Panel Features of IBM Security QRadar Core Appliances

Feature	Description
System identification button	The identification buttons on the front and back panels can be used to locate a particular system within a rack. Press to toggle the system ID on and off. If the system stops responding during POST, press and hold the system ID button for more than five seconds to enter BIOS progress mode. To reset iDRAC (if not disabled in F2 iDRAC setup) press and hold the button for more than 15 seconds.
System identification connector	Connects the optional system status indicator assembly through the optional cable management arm.
iDRAC8 Enterprise port	Dedicated management port.
Half-height PCIe expansion-card slot	Connects up to three half-height PCI Express expansion cards.
Serial connector	Connects a serial device to the system.
Video connector	Connects a VGA display to the system.
USB connector	Connects USB devices to the system. The ports are USB 3.0-compliant.
Full-height PCIe expansion-card slot	Connects up to four full-height PCI Express expansion cards.
Ethernet connector	Integrated 10/100/1000 Mbps NIC connectors
Power supply unit	AC 495 W, 750 W, or 1100 W or DC 750 W or 1100 W
vFlash media card slot	Holder for a vFlash media card.

QRadar Core Appliance QFlow Collectors

Review the information about the front and back panel features for appliances to confirm proper connectivity and functionality for the QRadar Core Appliance QFlow Collector 1201-C/1301-C and 1310 SR-C/LR-C appliances.

View front and back panel diagrams for the following appliances:

- "QRadar QFlow Collector 1202-C/1301-C" on page 15
- "QRadar QFlow Collector 1310 SR-C/LR-C" on page 18

For information about the front panel, see Front Panel (http://www.dell.com/support/manuals/us/en/19/poweredge-r630/R630_OM_Publication_v3-v3/Front-panel-features-and-indicators?guid=GUID-D3EF7B11-B91A-4972-9DD6-BC89CC94D811&lang=en-us).

For information about the back panel, see Back Panel (http://www.dell.com/support/manuals/us/en/19/poweredge-r630/R630_OM_Publication_v3-v3/Back-panel-features-and-indicators?guid=GUID-C0B66403-F253-407C-B50C-90391617E03A&lang=en-us).

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 U.S.A.

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
170 Tracer Lane,
Waltham MA 02451, USA

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Trademarks

IBM, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.

Other company, product, and service names may be trademarks or service marks of others.

Privacy policy considerations

IBM Software products, including software as a service solutions, (“Software Offerings”) may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering’s use of cookies is set forth below.

Depending upon the configurations deployed, this Software Offering may use session cookies that collect each user’s session id for purposes of session management and authentication. These cookies can be disabled, but disabling them will also eliminate the functionality they enable.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, See IBM’s Privacy Policy at http://www.ibm.com/privacy and IBM’s Online Privacy Statement at http://www.ibm.com/privacy/details the section entitled “Cookies, Web Beacons and Other Technologies” and the “IBM Software Products and Software-as-a-Service Privacy Statement” at http://www.ibm.com/software/info/product-privacy.

Glossary

This glossary provides terms and definitions for the [product name] software and products.

The following cross-references are used in this glossary:

- *See* refers you from a nonpreferred term to the preferred term or from an abbreviation to the spelled-out form.
- *See also* refers you to a related or contrasting term.

For other terms and definitions, see the IBM Terminology website (opens in new window).

A

accumulator
A register in which one operand of an operation can be stored and subsequently replaced by the result of that operation.

active system
In a high-availability (HA) cluster, the system that has all of its services running.

Address Resolution Protocol (ARP)
A protocol that dynamically maps an IP address to a network adapter address in a local area network.

administrative share
A network resource that is hidden from users without administrative privileges. Administrative shares provide administrators with access to all resources on a network system.

anomaly
A deviation from the expected behavior of the network.

application signature
A unique set of characteristics that are derived by the examination of packet payload and then used to identify a specific application.

ARP See Address Resolution Protocol.

ARP Redirect
An ARP method for notifying the host if a problem exists on a network.

ASN See autonomous system number.

asset A manageable object that is either deployed or intended to be deployed in an operational environment.

autonomous system number (ASN)
In TCP/IP, a number that is assigned to an autonomous system by the same central authority that assigns IP addresses. The autonomous system number makes it possible for automated routing algorithms to distinguish autonomous systems.

B

behavior
The observable effects of an operation or event, including its results.

bonded interface
See link aggregation.

burst A sudden sharp increase in the rate of incoming events or flows such that the licensed flow or event rate limit is exceeded.

C

CIDR See Classless Inter-Domain Routing.

Classless Inter-Domain Routing (CIDR)
A method for adding class C Internet Protocol (IP) addresses. The addresses are given to Internet Service Providers (ISPs) for use by their customers. CIDR addresses reduce the size of routing tables and make more IP addresses available within organizations.

client A software program or computer that requests services from a server.

cluster virtual IP address
An IP address that is shared between the primary or secondary host and the HA cluster.

coalescing interval
The interval at which events are bundled. Event bundling occurs in 10 second intervals and begins with the first event that does not match any currently coalescing events. Within the coalescing interval, the first three matching events are bundled and sent to the event processor.

Common Vulnerability Scoring System (CVSS)
A scoring system by which the severity of a vulnerability is measured.

console
A display station from which an operator can control and observe the system operation.

content capture
A process that captures a configurable amount of payload and then stores the data in a flow log.

credential
A set of information that grants a user or process certain access rights.

credibility
A numeric rating between 0-10 that is used to determine the integrity of an event or an offense. Credibility increases as multiple sources report the same event or offense.

CVSS See Common Vulnerability Scoring System.

D

database leaf object
A terminal object or node in a database hierarchy.

datapoint
A calculated value of a metric at a point in time.

Device Support Module (DSM)
A configuration file that parses received events from multiple log sources and coverts them to a standard taxonomy format that can be displayed as output.

DHCP See Dynamic Host Configuration Protocol.

DNS See Domain Name System.

Domain Name System (DNS)
The distributed database system that maps domain names to IP addresses.

DSM See Device Support Module.

duplicate flow
Multiple instances of the same data transmission received from different flow sources.

Dynamic Host Configuration Protocol (DHCP)
A communications protocol that is used to centrally manage configuration information. For example, DHCP automatically assigns IP addresses to computers in a network.

E

encryption
In computer security, the process of transforming data into an unintelligible form in such a way that the original data either cannot be obtained or can be obtained only by using a decryption process.

endpoint
The address of an API or service in an environment. An API exposes an endpoint and at the same time invokes the endpoints of other services.

external scanning appliance
A machine that is connected to the network to gather vulnerability information about assets in the network.

F

false positive
A test result classed as positive (indicating that the site is vulnerable to attack), that the user decides is in fact negative (not a vulnerability).

flow A single transmission of data passing over a link during a conversation.

flow log
A collection of flow records.

flow sources
The origin from which flow is captured. A flow source is classified as internal when flow comes from hardware installed on a

managed host or it is classified as external when the flow is sent to a flow collector.

forwarding destination
One or more vendor systems that receive raw and normalized data from log sources and flow sources.

FQDN
See fully qualified domain name.

FQNN
See fully qualified network name.

fully qualified domain name (FQDN)
In Internet communications, the name of a host system that includes all of the subnames of the domain name. An example of a fully qualified domain name is rchland.vnet.ibm.com.

fully qualified network name (FQNN)
In a network hierarchy, the name of an object that includes all of the departments. An example of a fully qualified network name is CompanyA.Department.Marketing.

G

gateway
A device or program used to connect networks or systems with different network architectures.

H

HA See high availability.

HA cluster
A high-availability configuration consisting of a primary server and one secondary server.

Hash-Based Message Authentication Code (HMAC)
A cryptographic code that uses a cryptic hash function and a secret key.

high availability (HA)
Pertaining to a clustered system that is reconfigured when node or daemon failures occur so that workloads can be redistributed to the remaining nodes in the cluster.

HMAC
See Hash-Based Message Authentication Code.

host context
A service that monitors components to ensure that each component is operating as expected.

I

ICMP See Internet Control Message Protocol.

identity
A collection of attributes from a data source that represent a person, organization, place, or item.

IDS See intrusion detection system.

Internet Control Message Protocol (ICMP)
An Internet protocol that is used by a gateway to communicate with a source host, for example, to report an error in a datagram.

Internet Protocol (IP)
A protocol that routes data through a network or interconnected networks. This protocol acts as an intermediary between the higher protocol layers and the physical network. See also Transmission Control Protocol.

Internet service provider (ISP)
An organization that provides access to the Internet.

intrusion detection system (IDS)
Software that detects attempts or successful attacks on monitored resources that are part of a network or host system.

intrusion prevention system (IPS)
A system that attempts to deny potentially malicious activity. The denial mechanisms could involve filtering, tracking, or setting rate limits.

IP See Internet Protocol.

IP multicast
Transmission of an Internet Protocol (IP) datagram to a set of systems that form a single multicast group.

IPS See intrusion prevention system.

ISP See Internet service provider.

K

key file
In computer security, a file that contains public keys, private keys, trusted roots, and certificates.

L

L2L See Local To Local.

L2R See Local To Remote.

LAN See local area network.

LDAP See Lightweight Directory Access Protocol.

leaf In a tree, an entry or node that has no children.

Lightweight Directory Access Protocol (LDAP)
An open protocol that uses TCP/IP to provide access to directories that support an X.500 model and that does not incur the resource requirements of the more complex X.500 Directory Access Protocol (DAP). For example, LDAP can be used to locate people, organizations, and other resources in an Internet or intranet directory.

link aggregation
The grouping of physical network interface cards, such as cables or ports, into a single logical network interface. Link aggregation is used to increase bandwidth and network availability.

live scan
A vulnerability scan that generates report data from the scan results based on the session name.

local area network (LAN)
A network that connects several devices in a limited area (such as a single building or campus) and that can be connected to a larger network.

Local To Local (L2L)
Pertaining to the internal traffic from one local network to another local network.

Local To Remote (L2R)
Pertaining to the internal traffic from one local network to another remote network.

log source
Either the security equipment or the network equipment from which an event log originates.

log source extension
An XML file that includes all of the regular expression patterns required to identify and categorize events from the event payload.

M

magistrate
An internal component that analyzes network traffic and security events against defined custom rules.

magnitude
A measure of the relative importance of a particular offense. Magnitude is a weighted value calculated from relevance, severity, and credibility.

N

NAT See network address translation.

NetFlow
A Cisco network protocol that monitors network traffic flow data. NetFlow data includes the client and server information, which ports are used, and the number of bytes and packets that flow through the switches and routers connected to a network. The data is sent to NetFlow collectors where data analysis takes place.

network address translation (NAT)
In a firewall, the conversion of secure Internet Protocol (IP) addresses to external registered addresses. This enables communications with external networks but masks the IP addresses that are used inside the firewall.

network hierarchy
A type of container that is a hierarchical collection of network objects.

network layer
In OSI architecture, the layer that provides services to establish a path between open systems with a predictable quality of service.

network object
A component of a network hierarchy.

O

offense
A message sent or an event generated in response to a monitored condition. For example, an offense will provide information on whether a policy has been breached or the network is under attack.

offsite source
A device that is away from the primary site that forwards normalized data to an event collector.

offsite target
A device that is away from the primary site that receives event or data flow from an event collector.

Open Source Vulnerability Database (OSVDB)
Created by the network security community for the network security community, an open source database that provides technical information on network security vulnerabilities.

open systems interconnection (OSI)
The interconnection of open systems in accordance with standards of the International Organization for Standardization (ISO) for the exchange of information.

OSI See open systems interconnection.

OSVDB
See Open Source Vulnerability Database.

P

parsing order
A log source definition in which the user can define the order of importance for log sources that share a common IP address or host name.

payload data
Application data contained in an IP flow, excluding header and administrative information.

primary HA host
The main computer that is connected to the HA cluster.

protocol
A set of rules controlling the communication and transfer of data between two or more devices or systems in a communication network.

Q

QID Map
A taxonomy that identifies each unique event and maps the events to low-level and high-level categories to determine how an event should be correlated and organized.

R

R2L See Remote To Local.

R2R See Remote To Remote.

recon See reconnaissance.

reconnaissance (recon)
A method by which information pertaining to the identity of network resources is gathered. Network scanning and other techniques are used to compile a list of network resource events which are then assigned a severity level.

reference map
A data record of direct mapping of a key to a value, for example, a user name to a global ID.

reference map of maps
A data record of two keys mapped to many values. For example, the mapping of the total bytes of an application to a source IP.

reference map of sets
A data record of a key mapped to many values. For example, the mapping of a list of privileged users to a host.

reference set
A list of single elements that are derived from events or flows on a network. For example, a list of IP addresses or a list of user names.

reference table
A table where the data record maps keys that have an assigned type to other keys, which are then mapped to a single value.

refresh timer
An internal device that is triggered manually or automatically at timed intervals that updates the current network activity data.

relevance
A measure of relative impact of an event, category, or offense on the network.

Remote To Local (R2L)
The external traffic from a remote network to a local network.

Remote To Remote (R2R)
The external traffic from a remote network to another remote network.

report In query management, the formatted data that results from running a query and applying a form to it.

report interval
A configurable time interval at the end of which the event processor must send all captured event and flow data to the console.

routing rule
A condition that when its criteria are satisfied by event data, a collection of conditions and consequent routing are performed.

rule A set of conditional statements that enable computer systems to identify relationships and run automated responses accordingly.

S

scanner
An automated security program that searches for software vulnerabilities within web applications.

secondary HA host
The standby computer that is connected to the HA cluster. The secondary HA host assumes responsibility of the primary HA host if the primary HA host fails.

severity
A measure of the relative threat that a source poses on a destination.

Simple Network Management Protocol (SNMP)
A set of protocols for monitoring systems and devices in complex networks. Information about managed devices is defined and stored in a Management Information Base (MIB).

SNMP
See Simple Network Management Protocol.

SOAP A lightweight, XML-based protocol for exchanging information in a decentralized, distributed environment. SOAP can be used to query and return information and invoke services across the Internet.

standby system
A system that automatically becomes active when the active system fails. If disk replication is enabled, replicates data from the active system.

subnet
See subnetwork.

subnet mask
For internet subnetworking, a 32-bit mask used to identify the subnetwork address bits in the host portion of an IP address.

subnetwork (subnet)
A network that is divided into smaller independent subgroups, which still are interconnected.

sub-search
A function that allows a search query to be performed within a set of completed search results.

superflow
A single flow that is comprised of multiple flows with similar properties in order to increase processing capacity by reducing storage constraints.

system view
A visual representation of both primary and managed hosts that compose a system.

T

TCP See Transmission Control Protocol.

Transmission Control Protocol (TCP)
A communication protocol used in the Internet and in any network that follows the Internet Engineering Task Force (IETF) standards for internetwork protocol. TCP provides a reliable host-to-host protocol in packet-switched communication networks and in interconnected systems of such networks. See also Internet Protocol.

truststore file
A key database file that contains the public keys for a trusted entity.

V

violation
An act that bypasses or contravenes corporate policy.

vulnerability
A security exposure in an operating system, system software, or application software component.

W

whois server
A server that is used to retrieve information about a registered Internet resources, such as domain names and IP address allocations.

Printed in USA