IBM Security QRadar
Version 7.3.0

Hardware Guide

Note

Before you use this information and the product that it supports, read the information in “Notices” on page 67.

Product information

This document applies to IBM QRadar Security Intelligence Platform V7.3.0 and subsequent releases unless superseded by an updated version of this document.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. What's new for hardware installers in QRadar V7.3.0

IBM Security QRadar V7.3.0 introduces a new Event Collector appliance, an appliance that is dedicated to incident forensics, three new high-performance appliances, a network packet capture appliance, and two appliances that reconstruct network sessions in real-time to provide more detailed threat visibility.

QRadar Event Collector 1501

The IBM Security QRadar Event Collector 1501 (MTM 4412-Q4D) 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.

Learn more about the QRadar Event Collector 1501 appliance.

QRadar Incident Forensics

The IBM® QRadar® Incident Forensics appliance (MTM 4412-F1A) appliance allows you to retrace the step-by-step actions of a potential attacker, and quickly and easily conduct an in-depth forensics investigation of suspected malicious network security incidents.

Learn more about the QRadar Incident Forensics appliance.

QRadar xx05

The IBM Security QRadar xx05 (MTM 4412-Q1E) appliance is the M5 version of any xx05 appliance. For example, you can use the QRadar xx05 as a QRadar Event Processor 1605, a QRadar Flow Processor 1705, a QRadar 3105 (All-in-One), and so on.

Learn more about the QRadar xx05 appliance.

QRadar xx29

The IBM Security QRadar xx29 (MTM 4412-Q2A) appliance is the M5 version of any xx28 appliance. For example, you can use the QRadar xx29 as a QRadar Event Processor 1629, a QRadar Flow Processor 1729, a QRadar 3129 (All-in-One), and so on.

Learn more about the QRadar xx29 appliance.

QRadar xx48

The IBM Security QRadar xx48 (MTM 4412-Q3B) captures larger traffic volumes for enterprise clients that require higher levels of performance. With the faster data processing, faster availability of data for searching and analysis, and the capacity to support more IP-enabled devices, of the QRadar xx48, you use fewer appliances, saving rack space.

Learn more about the QRadar xx48 appliance.

QRadar Network Packet Capture

The IBM Security QRadar Network Packet Capture (MTM 4412-F2C) provides more storage capacity to enable users to store more packet data for a longer period of time, and improved performance. The QRadar Network Packet Capture appliance also provides more capture ports and extra configuration flexibility to support a wide range of deployment options.

Learn more about the QRadar Network Packet Capture appliance.

QRadar Network Insights 1901

The IBM Security QRadar Network Insights 1901 (MTM 4412-F4Y) appliance provides detailed analysis of network flows to extend the threat detection capabilities of QRadar. QRadar Network Insights 1901 provides the same capabilities as the QRadar Network Insights 1920 but on a lower-price hardware platform designed for 1 Gbps network connectivity.

Learn more about the QRadar Network Insights 1901 appliance.

QRadar Network Insights 1920

The IBM Security QRadar Network Insights 1920 (MTM 4412-F3F) appliance provides detailed analysis of network flows to extend the threat detection capabilities of QRadar. QRadar Network Insights 1920 reconstructs network sessions in real-time, gathering high-value indicators, and analyzing metadata and content.

Learn more about the QRadar Network Insights 1920 appliance.

Chapter 2. QRadar SIEM hardware migration scenarios

If your hardware reaches its end of life, you require upgraded processing capacity, or you are consolidating existing hardware, plan to migrate data from older IBM Security QRadar SIEM appliances to new QRadar appliances.

You have several options when you migrate:
- "Replacing a QRadar managed host"
- "Replacing a QRadar Console with an appliance that uses the same IP address" on page 5
- "Replacing a QRadar Console with an appliance that uses a new IP address" on page 9

Replacing a QRadar managed host

Migrate data from an older QRadar managed host (16xx, 17xx, or 18xx) appliance to newer hardware. Follow this process for non-HA appliances.

Before you begin

Ensure that the following conditions are met:
- You recorded the network information for the old appliance, because you must manually type this information into the network configuration for the new appliance.
- The software version of the new appliance matches the software version of the QRadar Console. You might be required to reinstall an ISO image for the appliance to downgrade or use an SFS fix pack to upgrade.
- You configured data backups to prevent potential data loss during the migration.

About this task

During migration, the IP address of the old appliance is assigned to the new hardware. The new hardware is added to the deployment and then you move data while new events are collected from the network.

Procedure

1. Prepare your new hardware:
   a. Rack the appliance and connect network connections.
   b. Review the paperwork for your appliance to determine which QRadar version is installed on the new hardware.
2. Review your software version.
   a. If your Console software version is older than the software on the appliance, re-install the appliance with the newest ISO that is less than or equal to the Console software version. Download the ISO file from Fix Central (www.ibm.com/support/fixcentral/).
   b. Follow the installation wizard to complete the installation.
   c. Type a root password for the appliance.
   d. Type a temporary IP address and network information for the new hardware.

   e. Log in as a root user, and select the appliance type during the installation process.
   f. If your Console patch version is newer than the software on the appliance, download and install the SFS (software fix/patch) from Fix Central (www.ibm.com/support/fixcentral/).
3. Remove the old appliance from the deployment.
   a. Log in to QRadar as an administrator.
   b. Click the **Admin** tab and click the **System and License Management** icon.
   c. From the Display menu, click **Systems**, and then select the old QRadar appliance.
   d. Click **Deployment Actions** > **Remove Host**.
   e. When prompted, click **Remove** to confirm the removal of the host deployment.

      Attention: Don't delete the components for the Event Collector, and Event Processor, because these components are re-used.
4. Reassign the IP addresses to ensure that the decommissioned appliance doesn't cause an IP address conflict in the network after it is powered back on.
   a. To reassign the IP address of the old appliance to any unused address:
      1) Use IMM (Integrated Management Module) for remote access, or use the local Console keyboard, to log in to the command line of the old appliance as the root user.
      2) Reassign the IP address of the old appliance by typing the following command:

         ```
         /opt/qradar/bin/qchange_netsetup
         ```
   b. Set the IP address for the new hardware:
      1) Use IMM for remote access, or use the local Console keyboard to log in to the command line of the new appliance as the root user.
      2) From the command line of the new appliance, type `/opt/qradar/bin/qchange_netsetup` to use same host name and IP address as the old appliance.

   If you want to migrate old data to the new system, leave the existing system running and connected to the network. The data is moved when the new appliance is running and collecting data.
5. Add the new appliance to the deployment
   a. Log in to QRadar as an administrator.
   b. Click the **Admin** tab and click the **System and License Management** icon.
   c. Click **Deployment Actions** > **Add Host**.
   d. If you're prompted to add old components from the deployment to the host, click **Yes**. Any deployment components that were on the old appliance are reassociated with this host so that any protocol-based sources are automatically enabled and migrated to the new appliance.
   e. Click **Save and Close**.
   f. On the **Admin** tab, click the **Deploy Changes** icon.
   g. Verify that event or flow sources that were reporting to the original host are being processed in the QRadar user interface.

After you add the host back to the QRadar deployment, the deployment process ensures that the required configuration is regenerated on the new appliance. After the new host is part of the deployment, you can only use SSH access from the Console.

6. To copy data from the old appliance, you shut down the host firewall on the new appliance by typing the command `systemctl stop iptables`.
7. Copy certificates and custom-generated key pairs from the old appliance to the new appliance to ensure that log sources and scanners can connect to remote sources.

   You must also migrate any custom generated private keys that you have by transferring the `/etc/ssh` and `/root/.ssh` directories.

   a. Log in to the old QRadar managed host as the root user.

   b. Copy the data from the old hardware to the new appliance by using the **rsync** command as in one of the following examples:

      Tip: For better performance when using a crossover cable solution, use rsync -av instead of rsync -avz.

      Use this example for certificates:

      ```
      Example: rsync -avz /opt/qradar/conf/trusted_certificates/
         root@new_appliance:/opt/qradar/conf/trusted_certificates
      ```

      Use these examples for SSH:

      ```
      Example 1: rsync -avz /etc/ssh/ root@new_appliance:/etc/ssh
      Example 2: rsync -avz /root/.ssh/ root@new_appliance:/root/.ssh
      ```
8. Transfer event and flow data to the new appliance.

   You can use either **rsync** or **SCP** to complete the data transfer. These commands might require the root user to accept SSH keys and provide the root password for the target server. The length of this process depends on how much data needs to be transferred.

   a. Log in to the old QRadar appliance as the root user.

   b. Copy the data from the old appliance to the new appliance (target server) by using the **rsync** command, as in the following example:

      Tip: For better performance when using a crossover cable solution, use rsync -av instead of rsync -avz.

      ```
      rsync -avz /store/ariel/ root@new_appliance:/store/ariel
      ```
9. Type the command `systemctl start iptables` after the configuration and data migration are complete.

What to do next

After the data transfer is complete, decommission the old appliance and unrack the obsolete hardware.

Replacing a QRadar Console with an appliance that uses the same IP address

Migrate data from an older QRadar Console to a new Console appliance that uses the same IP address. All managed host appliances stay as-is. Use this process for non-HA appliances.

Before you begin

You must complete a QRadar installation on the new Console with a matching software version to the old Console. The installation of the new appliance uses a temporary IP address until the old hardware is removed from the deployment.

About this task

It is not necessary to remove managed hosts from the old QRadar Console because the new QRadar Console takes over any existing hosts in the deployment. This procedure allows managed hosts in the deployment to continue to receive events while the Console is offline.

Procedure

1. Prepare your new hardware:
   a. Rack the appliance and connect network connections.
   b. Review the paperwork for your appliance to determine what QRadar version is installed on the new hardware.
2. Review your software version.
   a. If your Console software version is older than the software on the appliance, re-install the appliance with the newest ISO that is less than or equal to the Console software version. Download the ISO file from Fix Central (www.ibm.com/support/fixcentral/).
   b. Log in as a root user and select the appliance type during the installation process.
   c. Type a temporary IP address and network information for the new hardware.
   d. Type a root password for the appliance.
   e. Follow the installation wizard to complete the installation.
   f. If your Console patch version is newer than the software on the appliance, download and install the SFS (software fix/patch) from Fix Central (www.ibm.com/support/fixcentral/).
3. Prepare your old QRadar hardware.
   a. Log in to the old Console appliance.
   b. Click the **Admin** tab, and then click the **Backup and Recovery** icon.
   c. From the navigation menu, click **On Demand Backup**.

      Important: Configuration backups only can be restored to the same version of QRadar that they were created with. If you plan to change the overall QRadar version in the deployment, you must create a new configuration backup after any software change and keep these files in a safe place for your hardware migration. Moving from a smaller Console to a larger or newer appliance is supported by the migration or backup process. For example, a 3105 Console's configuration backup can be applied to a 3128 or a 3148 appliance.
   d. Type a name and description for the new configuration backup.
   e. Click **Run Backup** and wait for the configuration backup to complete.
   f. After the backup finishes, click the new configuration backup name that you created to download the file.
   g. Copy the configuration backup from the old QRadar Console to a safe location.

   A configuration backup file is created for the new Console to use. This file is required later on in the procedure to restore users, rules, log sources, offenses, reports, admin configurations, and other system settings to the new hardware.
4. Reassign IP addresses on the old QRadar Console.

   This process is done manually by adjusting the network configuration file directly, instead of using the `qchange_netsetup` command. You can use this method to change the system's physical IP address to avoid conflicts. If the backup restore does not complete on the new system, you can easily revert to the old address. After the IP address is changed on the existing console, it cannot affect any changes to the other hosts in the deployment unless the IP address is reverted.

Note: Complete this task by using IMM or a physical keyboard to prevent connection and lockout issues. If you are accustomed to editing network configuration files in Linux, you can use SSH and the `screen` command. Using a direct SSH session with `systemctl restart network` results in the loss of network connectivity and causes issues with the address change and service restart.

a. Use IMM for remote access, or the local Console keyboard to log in to the command line of the old appliance as the root user.

b. Verify which network interface is the management interface by typing the following command:`cat /etc/management_interface`

c. Change the directory to `/etc/sysconfig/network-scripts/`.

d. Open the file `ifcfg-` <*name*> , as listed in the `/etc/management_interface` file.

e. Change the IP address to an unused or decommissioned range by editing the IPADDR= line.

f. Save the changes to the file.

g. Depending on whether you need to migrate data from the existing Console, power off the system or type `systemctl restart network` to restart networking. Restarting the network services switches the IP address to the one you previously entered, freeing up the old IP address to use on the new console. If any QRadar processes on the system result in errors, QRadar operates normally if you switch the IP address back later. Don't unrack the old hardware because data still exists on the old appliance and that data must be transferred to the new appliance.

5. Set IP addresses on the new QRadar Console appliance.

   a. Use IMM for remote access or the local Console keyboard to log in to the command line of the new appliance as the root user.

   b. Change the IP address by typing the following command:`/opt/qradar/bin/qchange_netsetup`.

   c. Use the Configuration Wizard to change the IP address of the system to the old Console's IP address.

   d. Save and exit the Wizard to complete the address change.

6. Copy certificates and custom-generated key pairs from the old appliance to the new appliance to ensure that log sources and scanners can connect to remote sources.

   You must also migrate any custom-generated private keys that you have by transferring the `/etc/ssh` and `/root/.ssh` directories.

   a. Log in to the QRadar old managed host as the root user.

   b. Copy the data from the old hardware to the new appliance by using the **`rsync`** as in the following examples:

   Tip: For better performance when using a crossover cable solution, use rsync -av instead of rsync -avz.

   Use this example for certificates:

```
Example: rsync -avz /opt/qradar/conf/trusted_certificates/
   root@new_appliance:/opt/qradar/trusted_certificates/
```

Use these examples for SSH:

```
Example 1: rsync -avz /etc/ssh/ root@new_appliance:/etc/ssh
Example 2: rsync -avz /root/.ssh/ root@new_appliance:/root/.ssh
```

c. Wait for the transfer to complete.

d. If you are using custom SSL certificates:

1) Copy the certificate or intermediate certificate from the old Console's `/etc/httpd/conf/certs` directory.

2) Install the SSL certificate on the new Console, by using `/opt/qradr/bin/install_ssl_cert.sh -i` and follow the instructions.

The required certificate and ssh key files are transferred to the new hardware. You can now migrate event and flow data from the old appliance to the new hardware.

7. Restore the backup configuration to the new QRadar Console appliance.

a. Using SCP, copy the configuration backup file that you downloaded previously to `/store/backupHost/inbound/` of the new Console.

b. Log in to the QRadar Console as an administrator.

c. Click the **Admin** tab and select the **Backup and Recovery** icon.

d. Select the configuration backup that you copied to the Console and click **Restore**.

e. In the restore options list, click **Select All Configuration Items**.

f. In the restore options list, click **Select All Data Items**.

g. Click **Restore** to start the configuration restore process. The restore process might take a while to complete.

h. After the restore process is complete, log in to the QRadar user interface.

i. From the **Admin** tab, click **Advanced>** > **Deploy Full Configuration**.

j. Verify that event or flow sources that were reporting to the original host are being processed in the QRadar user interface.

After the host is added back to the QRadar deployment, the deployment process ensures that the required configuration is regenerated on the new appliance. Verify that log source data is being pulled and that flow data is being received by the new hardware. Any log sources that are not collecting data might require certificates to be moved to the new host.

8. Transfer event and flow data to the new hardware.

You can use either **`rsync`** or the **`SCP`** command to complete the data transfer. These commands might require the root user to accept SSH keys and provide the root password for the target server. The length of this process depends on how much data needs to be transferred.

a. Log in to the old QRadar Console as the root user.

b. Copy the data from the old hardware to the new appliance (*targetserver*) by using the **`rsync`** command as in the following example:

Tip: For better performance when using a crossover cable solution, use rsync -av instead of rsync -avz.

```
Example: rsync -avz /store/ariel/
   root@new_appliance:/store/ariel
```

Results

After the data transfer is complete, you might want to keep the old console on hand in case you to revert to the old appliance. Otherwise, after a week or two, the old Console is no longer required and can be decommissioned or repurposed for other uses.

Replacing a QRadar Console with an appliance that uses a new IP address

Migrate data from an older QRadar Console to a new Console appliance that uses a new IP address. All managed host appliances stay as-is. Use this process for non-HA appliances.

Before you begin

You must complete a QRadar installation on the new Console with a matching software version to the old Console.

About this task

You don't have to remove managed hosts from the old QRadar Console because the new QRadar Console takes over any existing hosts in the deployment. This procedure allows managed hosts in the deployment to continue to receive events while the Console is offline.

Procedure

1. Prepare your new hardware:
   a. Rack the appliance and connect network connections.
   b. Review the paperwork for your appliance to determine which QRadar version is installed on the new hardware.
2. Review your software version.
   a. If your Console software version is older than the software on the appliance, re-install the appliance with the newest ISO that is less than or equal to the Console software version. Download the ISO file from Fix Central (www.ibm.com/support/fixcentral/).
   b. Follow the installation wizard to complete the installation.
   c. Type a root password for the appliance.
   d. Type a new IP address and network information for the new hardware.
   e. Log in as a root user and select the appliance type during the installation process.
   f. If your Console patch version is newer than the software on the appliance, download and install the SFS (software fix/patch) from Fix Central (www.ibm.com/support/fixcentral/).
3. Prepare your old QRadar hardware.
   a. Log in to the old Console.
   b. Click the **Admin** tab, and then click the **Backup and Recovery** icon.
   c. From the navigation menu, click **On Demand Backup**.

      Important: Configuration-only backups can be restored to the same version of QRadar that they were created with. If you plan to change the overall QRadar version in the deployment, you must create a new configuration backup after any software changes and keep these files in a safe place for your hardware migration. Moving from a smaller Console to a larger or newer appliance is supported. For example, a 3105 Console's configuration backup can be applied to a 3128 or a 3148 appliance.

   d. Type a name and description for the new configuration backup.
   e. Click **Run Backup** and wait for the configuration backup to complete.
   f. After the backup finishes, click the new configuration backup name that you created to download the file.
   g. Copy the configuration backup from the old QRadar Console to a safe location.

   A configuration backup file is created for the new Console to use. This file is required later on in the procedure to restore users, rules, log sources, offenses, reports, admin configurations, and other system settings to the new hardware.

4. Copy certificates and custom-generated key pairs from the old appliance to the new appliance to ensure that log sources and scanners can connect to remote sources.

   You must also migrate any custom generated private keys that you have by transferring the `/etc/ssh` and `/root/.ssh` directories.

   a. Log in to the QRadar old managed host as the root user.
   b. Copy the data from the old hardware to the new appliance by using the **`rsync`** command as in the following examples:

      Tip: For better performance when using a crossover cable solution, use rsync -av instead of rsync -avz.

      Use this example for certificates:

      ```
      Example: rsync -avz /opt/qradar/conf/trusted_certificates/
          root@targetserver:/opt/qradar/conf/trusted_certificates/
      ```

      Use these examples for SSH:

      ```
      Example 1: rsync -avz /etc/ssh/ root@targetserver:/etc/.ssh
      ```

      ```
      Example 2: rsync -avz /root/.ssh/ root@targetserver:/root
      ```

   c. Wait for the transfer to complete.
   d. If you use custom SSL certificates, do the following steps:
      1) Copy the certificate or intermediate certificate from the old Console's `/etc/httpd/conf/certs` directory.
      2) On the new Console, install the SSL certificate by using `/opt/qradr/bin/install_ssl_cert.sh -i` and follow the on-screen instructions.

   The required certificate and ssh key files are transferred to the managed host. You can now migrate event and flow data from the old appliance to the new hardware.

5. Restore the backup configuration to the new QRadar Console appliance.
   a. Using **`SCP`**, copy the configuration backup file that you downloaded previously to `/store/backuphost/inbound/` on the new Console.
   b. Using SSH, log in to the old QRadar Console as the root user.
   c. To stop `IPtables` on all hosts, type the following command: `/opt/qradar/support/all_servers.sh "systemctl stop iptables"`.
   d. Log in to the new QRadar Console as an administrator.
   e. Click the **Admin** tab, and then click the **Backup and Recovery** icon.
   f. Select the configuration backup that you copied to the Console and click **Restore**.
   g. In the restore options list, click **Select All Configuration Items**.
   h. In the restore options list, click **Select All Data Items**.
   i. Click **Restore** to start the configuration restore process.

j. After the restore process finishes, click the **Admin** tab.

k. Select **Advanced** > **Deploy Full Configuration**.

l. Wait for the deployed changes to complete.

m. To start `IPtables` on all hosts, type the following command: `/opt/qradar/support/all_servers.sh "systemctl start iptables"`.

n. Verify that event or flow sources that were reporting to the original host are being processed in the QRadar user interface.

After the host is added back to the QRadar deployment, the deployment process ensures that the required configuration is regenerated on the new appliance. Verify that log source data is being pulled and that flow data is being received by the new hardware. Any log sources that are not collecting data might require certificates to be moved to the new host.

6. Transfer event and flow data to the new hardware.

   You can use either **rsync** or **SCP** to complete the data transfer. These commands might require the root user to accept SSH keys and provide the root password for the target server. The length of this process depends on how much data needs to be transferred.

   a. Log in to the old QRadar Console as the root user.

   b. Copy the data from the old hardware to the new appliance (*targetserver*) by using the **rsync** command, as in the following example:

      Tip: For better performance when using a crossover cable solution, use rsync -av instead of rsync -avz.

      ```
      Example: rsync -avz /store/ariel/ root@new_appliance:/store/ariel
      ```

What to do next

After the data transfer is complete, you might want to keep the old Console on hand in case you need to revert to the old appliance. Otherwise, after a week or two, the old Console is no longer required and can be decommissioned or repurposed for other uses.

To verify that your migration is successful, log in as an administrator, click the **Log Activity** tab and perform a search to see whether events are flowing. Then click the **Network Activity** tab and perform a search to see whether flows are being processed.

Chapter 3. 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 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 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 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 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
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
Maximum capacity	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
Maximum capacity	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
Maximum capacity	Up to 1,200,000 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 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
Maximum capacity	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
Maximum capacity	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
Maximum capacity	1,000 EPS 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
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
Maximum capacity	Up to 5,000 EPS Up to 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	6.5 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 33
- “QRadar Flow Processor 1705” on page 35
- “QRadar 1805” on page 37

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
Maximum capacity	Up to 5000 EPS Up to 200,000 FPM
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 16
- “QRadar Flow Processor 1724” on page 17

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
Maximum capacity	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
Maximum capacity	Up to 20,000 EPS
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
Maximum capacity	Up to 1000 EPS
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
Maximum capacity	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**
Maximum capacity	Up to 5000 EPS
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

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 20

- “QRadar Log Manager 1624” on page 21

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 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 19. QRadar Vulnerability Manager overview

Description	**Value**
Maximum capacity	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 4. 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 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

The IBM 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 22. QRadar QFlow Collector 1202

Description	Value
Network traffic	3 Gbps

Table 22. QRadar QFlow Collector 1202 (continued)

Description	Value
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 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 23. QRadar QFlow Collector 1202-C/1301-C specifications

Description	Value
Network traffic	3 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 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 1301

The IBM 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 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	10 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, 6.1 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	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, 39 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
Maximum capacity	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, 39 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**
Maximum capacity	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, 5.5 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

For diagrams and information about the front and back panel of this appliance, see “QRadar M4 Consoles and Processors and Data Nodes” on page 62.

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**
Maximum capacity	40,000 EPS

Table 32. QRadar Event Processor 1628 Event Processor 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 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, 34 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
Maximum capacity	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, 34 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
Maximum capacity	1,200,000 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, 5.5 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 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
Maximum capacity	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, 34 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
Maximum capacity	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, 34 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
Maximum capacity	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, 5.5 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 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
Maximum capacity	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, 34 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
Maximum capacity	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, 34 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
Maximum capacity	1,000 EPS 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
Maximum capacity	200,000 FPM 5,000 EPS

Table 41. QRadar 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, 4.9 TB usable (RAID 6)
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
Maximum capacity	300,000 FPM 15,000 EPS

Table 42. QRadar 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, 29 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
Maximum capacity	300,000 FPM 15,000 EPS
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, 29 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 43. QRadar 3128-C (All-in-One) specifications (continued)

Description	Value
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
Maximum capacity	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, 5.5 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 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
Maximum capacity	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, 34 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

Table 45. QRadar Log Manager 1628 (continued)

Description	Value
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
Maximum capacity	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, 34 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
Maximum capacity	1000 EPS

Table 47. QRadar Log Manager 2100 overview (continued)

Description	Value
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
Maximum capacity	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, 4.9 TB usable (RAID 6)
Power supply	Dual redundant 750W 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
Maximum capacity	15,000 EPS
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, 29 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 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**
Maximum capacity	15,000 EPS
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, 29 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

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 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 33

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
Maximum capacity	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

Table 51. QRadar Vulnerability Manager overview (continued)

Description	Value
Storage	9 x 3.5 inch 1 TB 7.2 K rpm NL SAS, 9 TB total, 5.5 TB usable (RAID 6)
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 62.

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, 5.5 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	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 62.

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 62.

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
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 62.

Chapter 5. QRadar M5 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 1202/1301

The IBM QRadar QFlow Collector 1202/1301 (MTM 4412-Q7C) appliance provides high capacity and scalable Layer 7 application data collection for distributed deployments. The QRadar QFlow Collector 1202/1301 also supports external flow-based data sources.

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

Table 54. QRadar QFlow Collector 1202/1301 overview

Description	Value
Interfaces	One Napatech Network Adapter, providing four 1 Gbps SFP network interfaces, including 4x SX (LC 1G short range fiber) and 4x TX (RJ-45 1G copper) transceivers Three 10/100/1000 Base-T network interfaces One 10/100/1000 Base-T QRadar management interface One 10/100 Base-T integrated remote system management interface
Memory	64 GB, 4 x16 GB truDDR4 2133MHz Memory
Storage	2 x 200 GB SSD
Power supply	Dual redundant 750 W AC
Dimensions	28.9 inches deep x 17.1 inches wide x 1.7 inches high

For battery removal steps, see Removing the coin-cell battery (also called CMOS battery) (http://www-01.ibm.com/support/knowledgecenter/api/redirect/systemx/documentation/index.jsp?topic=/com.lenovo.sysx.8871.doc/t_removing_system_battery.html)

QRadar QFlow Collector 1310

The IBM 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 55. QRadar QFlow Collector 1310 overview

Description	Value
Interfaces	One Napatech Network Adapter, providing four 10 Gbps SFP+ network interfaces, including 4x SR (LC 10G short range fiber) transceivers Three 10/100/1000 Base-T network interfaces One 10/100/1000 Base-T QRadar management interface One 10/100 Base-T integrated remote system management interface
Memory	64 GB, 4 x16 GB truDDR4 2133MHz Memory
Storage	2 x 200 GB SSD
Power supply	Dual redundant 750 W AC
Dimensions	28.9 inches deep x 17.1 inches wide x 1.7 inches high

For battery removal steps, see Removing the coin-cell battery (also called CMOS battery) (http://www-01.ibm.com/support/knowledgecenter/api/redirect/systemx/documentation/index.jsp?topic=/com.lenovo.sysx.8871.doc/t_removing_system_battery.html)

QRadar Event Collector 1501

The IBM Security QRadar Event Collector 1501 (MTM 4412-Q4D) 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.

Tip: You can configure the QRadar Event Collector 1501 appliance to be used as a QRadar QFlow Collector 1201.

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

Table 56. QRadar Event Collector 1501 specifications

Description	Value
Events per second	15,000 EPS
Network traffic	1 Gbps
Interfaces	Seven 10/100/1000 Base-T network monitoring interfaces Two 10 Gbps SFP + Ethernet ports One 10/100/1000 Base-T QRadar management interface One 10/100 Base-T integrated management module interface
Memory	64 GB, 4 x16GB truDDR4 2400MHz LP RDIMM
Storage	4 x 600GB 2.5 inch 10K rpm 12 Gbps SAS RAID 10 1.2GB total (RAID 10)
Power supply	System x 550W High Efficiency Platinum AC Power Supply
Dimensions	28.9 inches deep x 17.1 inches wide x 1.7 inches high

Table 56. QRadar Event Collector 1501 specifications (continued)

Description	Value
Included components	Event Collector

QRadar xx05

Use the IBM Security QRadar xx05 (MTM 4412-Q1E) appliance for various appliance types in your deployment.

Use the QRadar xx05 for the following appliance types:

- QRadar Event Processor 1605
- QRadar Flow Processor 1705
- QRadar 1805 Event and Flow Processor
- QRadar 3105 (All-in-One)
- QRadar 3105 (Console)
- QRadar Log Manager 1605
- QRadar Log Manager 3105 (All-in-One)
- QRadar Log Manager 3105 Console
- QRadar Risk Manager
- QRadar Vulnerability Manager

View hardware information and requirements for the QRadar xx05 in the following table:

Table 57. QRadar xx05 overview

Description	Value
Maximum capacity	QRadar Event Processor 1605: 20,000 EPS QRadar Flow Processor 1705: 1,200,000 FPM QRadar 1805 Event and Flow Processor: 5000 EPS, 200,000 FPM QRadar 3105 (All-in-One): 5000 EPS, 200,000 FPM
Interfaces	Two 8Gbps Fiber Channel HBA ports Four 10/100/1000 Base T Ethernet interfaces One 10/100 Base-T integrated management module interface Two 10 Gbps SFP + Ethernet ports
Memory	64 GB 2400 MHz DDR4 RDIMM
Storage	10 x 2.5 inch 1 TB 7.2 K rpm NL SAS, 10 TB total, 5.6 TB (RAID 6) available to store event and flow data
Power supply	Dual redundant 750W AC power supply
Dimensions	28.9 inches deep x 17.1 inches wide x 1.7 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*.

For battery removal steps, see Removing the coin-cell battery (http://publib.boulder.ibm.com/infocenter/systemx/documentation/index.jsp?topic=/com.lenovo.sysx.8871.doc/t_removing_system_battery.html).

QRadar xx29

Use the IBM Security QRadar xx29 (MTM 4412-Q2A) for various appliance types in your deployment.

The QRadar xx29 can be used for the following appliances:

- QRadar Event Processor 1629
- QRadar Flow Processor 1729
- QRadar Event and Flow Processor 1829
- QRadar 3129 (All-in-One)
- QRadar 3129 (Console)
- QRadar Log Manager 1629
- QRadar Log Manager 3129 (All-in-One)
- QRadar Log Manager 3129 (Console)

View hardware information and requirements for the QRadar xx29 in the following table:

Table 58. QRadar xx29

Description	Value
Maximum capacity	QRadar Event Processor 1629: 40,000 EPS QRadar Flow Processor 1729: 2,400,000 FPM QRadar Event and Flow Processor 1829: : 15,000 EPS, 300,000 FPM QRadar 3129 (All-in-One): 15,000 EPS, 300,000 FPM
Interfaces	Two 8Gbps Fiber Channel HBA ports Four 10/100/1000 Base-T Ethernet interfaces One 10/100 Base-T integrated management module interface Two 10 Gbps SFP + Ethernet ports
Memory	128 GB, 8 x 16 GB 2400 MHz DDR4 RDIMM
Storage	12 x 3.5 inch 6 TB SAS 7.2 K rpm, 72 TB total 3129: 48 TB (RAID 6) available to store event and flow data. All other xx29 appliances: 58 TB (RAID 6) available to store event and flow data.
Power supply	Dual Redundant 900 W AC
Dimensions	31.5 inches deep x 17.5 inches wide x 3.4 inches high

Table 58. QRadar xx29 (continued)

Description	Value
Included components	Event Collector Event Processor for processing events and flows Internal storage for events and flows

The QRadar 3129 (All-in-One) requires external QRadar QFlow Collectors for layer 7 network activity monitoring.

For battery removal steps, see Removing the coin-cell battery (also called CMOS battery) (http://publib.boulder.ibm.com/infocenter/systemx/documentation/index.jsp?topic=/com.lenovo.sysx.8871.doc/t_removing_system_battery.html).

QRadar xx48

The IBM Security QRadar xx48 (MTM 4412-Q3B) captures logs from sources that generate a large amount of traffic without a need for load balancing.

The QRadar xx48 appliance handles the higher levels of performance that are required by enterprise class clients. For example, companies can use the QRadar xx48 for the following requirements:

- A company wants faster processing to search and analyze a large amount of data.
- A company wants to reduce the footprint of an IBM Security QRadar deployment, so they install QRadar xx48 appliances to reduce rack space.

The following appliances are examples of appliance types that you can use the QRadar xx48 for:

- QRadar Event Processor 1648
- QRadar Flow Processor 1748
- QRadar Event and Flow Processor 1848
- QRadar 3148 (All-in-One)
- QRadar 3148 (Console)

View hardware information and requirements for the QRadar xx48 in the following table:

Table 59. QRadar xx48 overview

Description	Value
Maximum capacity	QRadar Event Processor 1648: 100,000 EPS QRadar Flow Processor 1748: 3,600,000 FPM QRadar Event and Flow Processor 1848: 30,000 EPS, 1,200,000 FPM QRadar 3148 (All-in-One): 30,000 EPS, 1,200,000 FPM

Table 59. QRadar xx48 overview (continued)

Description	Value
Interfaces	One 2-port Emulex 8 Gb FC Four 10/100/1000 Base-T Ethernet 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, 2133 MHz DDR4 RDIMM
Storage	6x 3.8 TB SSD
Power supply	Dual redundant 900 W AC
Dimensions	31.5 inches deep x 17.5 inches wide (19 inches with EIA) x 3.4 inches high

For battery removal steps, see Removing the coin-cell battery (also called CMOS battery) (http://publib.boulder.ibm.com/infocenter/systemx/documentation/index.jsp?topic=/com.lenovo.sysx.8871.doc/t_removing_system_battery.html).

QRadar Incident Forensics

Use the IBM® QRadar® Incident Forensics appliance (MTM 4412-F1A) to retrace the step-by-step actions of a potential attacker, and quickly and easily conduct an in-depth forensics investigation of suspected malicious network security incidents.

View hardware information and requirements for the QRadar Incident Forensics appliance in the following table:

Table 60. Incident Forensics appliance specifications

Description	Value
Interfaces	Three 10/100/1000 Base-T network interfaces One 10/100/1000 Base-T QRadar management interface One 10/100 Base-T integrated remote system management interface
Memory	128 GB, 8 x16 GB truDDR4 2400MHz LP RDIMM
Storage	12 x 6TB 3.5" 7.2K 12Gbps NL SAS RAID6
Power supply	System x 900W High Efficiency Platinum AC Power Supply
Dimensions	31.5 inches deep x 17.5 inches wide x 3.4 inches high

QRadar Network Packet Capture

IBM Security QRadar Network Packet Capture (MTM 4412-F2C) 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 Network Packet Capture in the following table:

Table 61. QRadar Network Packet Capture overview

Description	Value
Interfaces	Napatech Network Adapter for fiber, providing four 10 Gbps SFP + LR (long range) and SR (short range) network interfaces Three 10/100/1000 Base-T network interfaces One 10/100/1000 Base-T QRadar management interface One 10/100 Base-T integrated remote system management interface
Memory	Dual redundant 900 W AC
Storage	2 x 1 TB 3.5" SAS, 12x 6 TB 3.5" SAS
Power supply	Dual redundant 900 W AC
Dimensions	31.5 inches deep x 17.5 inches wide (19 inches with EIA) x 3.4 inches high

For battery removal steps, see Removing the coin-cell battery (also called CMOS battery) (http://publib.boulder.ibm.com/infocenter/systemx/documentation/index.jsp?topic=/com.lenovo.sysx.8871.doc/t_removing_system_battery.html)

QRadar Network Insights 1901

The IBM Security QRadar Network Insights 1901 (MTM 4412-F4Y) appliance provides detailed analysis of network flows to extend the threat detection capabilities of IBM Security QRadar.

The QRadar Network Insights 1901 appliance provides the same capabilities as the QRadar Network Insights 1920 appliance but on a lower-price hardware platform that is designed for 1 Gbps network connectivity.

View hardware information and requirements for the QRadar Network Insights 1901 in the following table:

Table 62. QRadar Network Insights 1901 overview

Description	Value
Interfaces	One Napatech Network Adapter for fiber, providing four 1 Gbps SFP+ 2x SX (short range) and 2x TX (copper/RJ-45) network interfaces Three 10/100/1000 Base-T network interfaces One 10/100/1000 Base-T QRadar management interface One 10/100 Base-T integrated remote system management interface
Memory	64 GB, 4 x16 GB truDDR4 2133MHz Memory
Storage	2 x 200 GB SSD
Power supply	Dual redundant 750 W AC
Dimensions	28.9 inches deep x 17.1 inches wide x 1.7 inches high

For battery removal steps, see Removing the coin-cell battery (also called CMOS battery) (http://www-01.ibm.com/support/knowledgecenter/api/redirect/systemx/documentation/index.jsp?topic=/com.lenovo.sysx.8871.doc/t_removing_system_battery.html)

QRadar Network Insights 1920

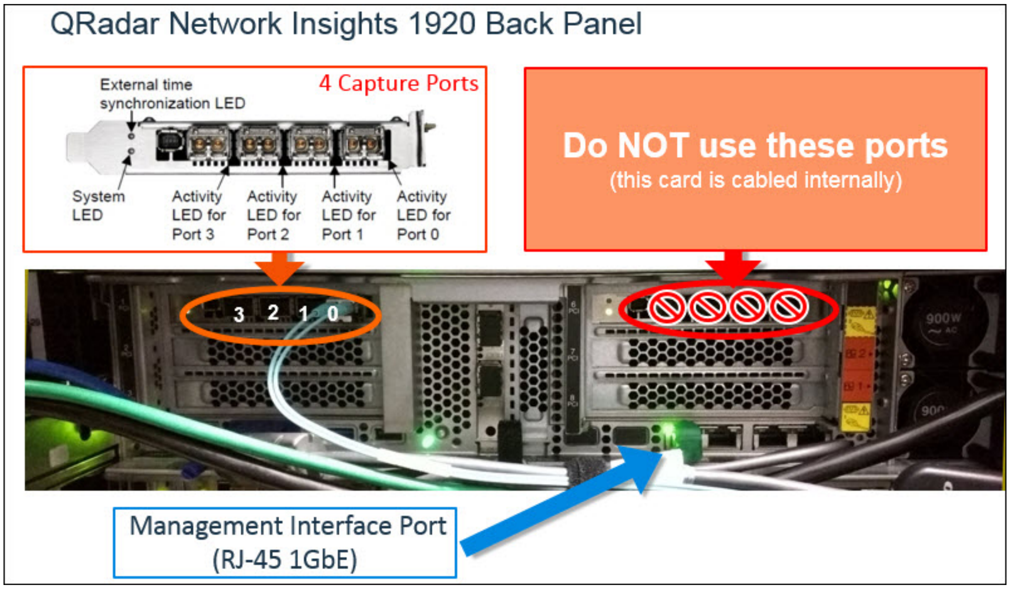
The IBM Security QRadar Network Insights 1920 (MTM 4412-F3F) appliance provides detailed analysis of network flows to extend the threat detection capabilities of IBM Security QRadar.

View hardware information and requirements for the QRadar Network Insights 1920 in the following table:

Table 63. QRadar Network Insights 1920 overview

Description	Value
Interfaces	Two Napatech Network Adapter for fiber, providing four 10 Gbps SFP+ LR (long range) and SR (short range) network interfaces Three 10/100/1000 Base-T network interfaces One 10/100/1000 Base-T QRadar management interface One 10/100 Base-T integrated remote system management interface
Memory	128 GB, 8 x16 GB truDDR4 2133MHz Memory
Storage	2 x 200 GB SSD (RAID 1)
Power supply	Dual redundant 900 W AC
Dimensions	31.5 inches deep x 17.5 inches wide (19 inches with EIA) x 3.4 inches high

Important: One of the two Napatech cards is cabled internally and should not be used. The following image shows the back panel.



For battery removal steps, see Removing the coin-cell battery (also called CMOS battery) (http://publib.boulder.ibm.com/infocenter/systemx/documentation/index.jsp?topic=/com.lenovo.sysx.8871.doc/t_removing_system_battery.html)

Chapter 6. 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

The Integrated Management Module (IMM) is a management module that is used for systems-management functions.

On the back panel of each appliance type, the serial connector and Ethernet connectors can be managed by 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 comes 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 QRadar QFlow Collector 1201 (MTM 4378-QC1)
- IBM QRadar QFlow Collector 1202 (MTM 4378-QC2)
- IBM QRadar QFlow Collector 1301 (MTM 4378-QD1)
- IBM 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 (https://lenovopress.com/tips0804).

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 24
- "QRadar Risk Manager" on page 25

For more information about IBM Security QRadar M3 Consoles, Processors and Data Nodes, including front and back panel diagrams, see IBM System x3630 M3 (https://lenovopress.com/tips0807).

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 39 (4380-Q1C).
- "QRadar QFlow Collector 1202" on page 27 (4380-Q3C).
- "QRadar QFlow Collector 1301" on page 29 (4380-Q4C).
- "QRadar QFlow Collector 1310" on page 29 (4380-Q5C).
- "QRadar Event Collector 1501" on page 32, "QRadar QFlow Collector 1201" on page 27 (4380-Q2C).
- "QRadar Log Manager 2100" on page 44 (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 (https://lenovopress.com/tips0851-system-x3550-m4-e5-2600-v2).

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 30 (4380-Q1E).
- "QRadar Event Processor 1605" on page 33 (4380-Q1E).
- "QRadar Event Processor 1628" on page 33 (4380-Q2E).
- "QRadar Flow Processor 1705" on page 35 (4380-Q1E).
- "QRadar Flow Processor 1728" on page 35 (4380-Q2E).
- "QRadar 3105 (All-in-One)" on page 39 (4380-Q1E).
- "QRadar 3105 (Console)" on page 40 (4380-Q1E).
- "QRadar 3128 (All-in-One)" on page 40 (4380-Q2E).
- "QRadar 3128 (Console)" on page 42 (4380-Q2E).
- "QRadar Log Manager 1605" on page 42 (4380-Q1E).
- "QRadar Log Manager 1628" on page 43 (4380-Q2E).
- "QRadar Log Manager 3105 (All-in-One)" on page 45 (4380-Q1E).

- “QRadar Log Manager 3105 Console” on page 46 (4380-Q1E).
- “QRadar Log Manager 3128 (All-in-One)” on page 46 (4380-Q2E).
- “QRadar Log Manager 3128 (Console)” on page 47 (4380-Q2E).
- “QRadar Vulnerability Manager” on page 48 (4380-Q1E).
- “QRadar Risk Manager” on page 49 (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 (https://lenovopress.com/tips1102-system-x3650-m4-bd).

M5 QRadar Event Collector 1501 and Network Insights 1901

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

- “QRadar Event Collector 1501” on page 52 (4412-Q4D)
- “QRadar Network Insights 1901” on page 57 (4412-F4Y)

For more information about the QRadar Event Collector 1501 and QRadar Network Insights 1901 including front and back panel diagrams, see IBM System X3550 M5 (https://lenovopress.com/lp0067-lenovo-system-x3550-m5-machine-type-8869).

QRadar xx05

Review the information about the front and back panel features for appliances to confirm proper connectivity and functioning for the IBM Security QRadar xx05 (MTM 4412-Q1E).

“QRadar xx05” on page 53 is based on the Lenovo System x3550 M5.

For more information about the front panel, see Front view (http://publib.boulder.ibm.com/infocenter/systemx/documentation/index.jsp?topic=/com.lenovo.sysx.8869.doc/c_front_view.html).

For more information about the back panel, see Rear view (http://publib.boulder.ibm.com/infocenter/systemx/documentation/index.jsp?topic=/com.lenovo.sysx.8869.doc/c_rear_view.html).

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:

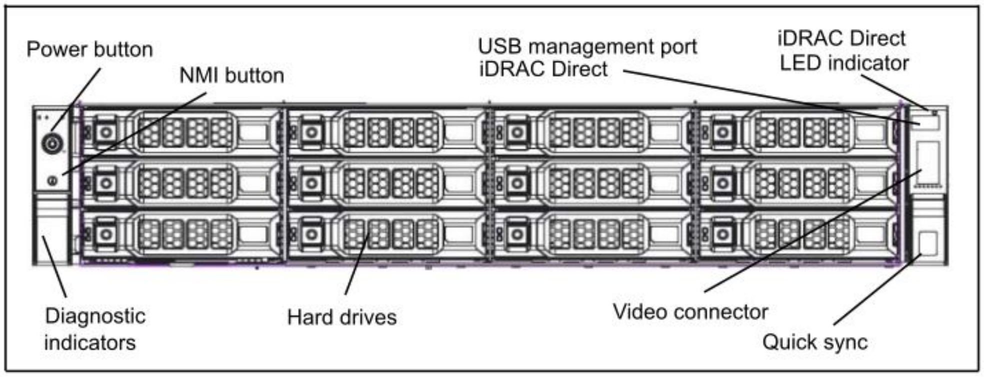
- QRadar
- QRadar Risk Manager
- QRadar Vulnerability Manager
- QRadar Incident Forensics
- QRadar Packet Capture, including QRadar Packet Capture Data Node.

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

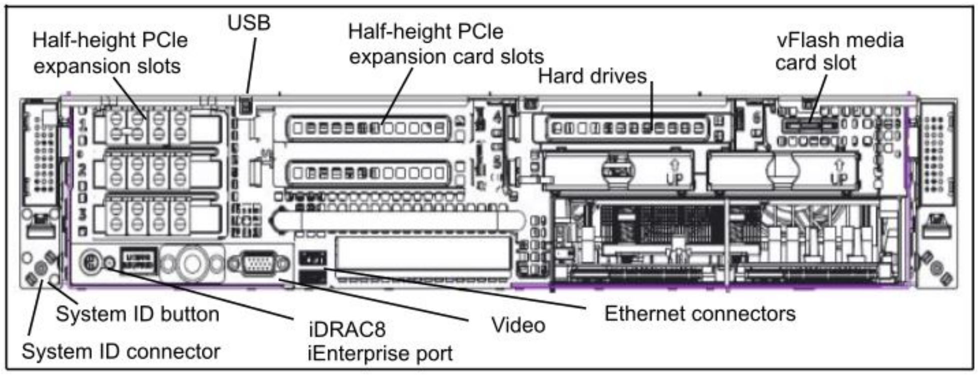
Important: To make an xx28-C appliance FIPS compliant, the QRadar release must be FIPS compliant, and your appliance must have the required physical security. For more information about physical security, see the *IBM Security QRadar Version 7.2.5 FIPS 140-2 Installation Guide*. QRadar Incident Forensics and QRadar Packet Capture are not FIPS compliant.

- “QRadar 1400-C Data Node” on page 31
- “IBM Security QRadar Event Processor 1628-C” on page 34
- “QRadar Flow Processor 1728-C” on page 36
- “QRadar Flow Processor 1828-C” on page 38
- “QRadar 3128-C (All-in-One)” on page 41
- “QRadar 3128-C (Console)” on page 42
- “QRadar Log Manager 1628-C” on page 44
- “QRadar Log Manager 3128-C (All-in-One)” on page 47
- “QRadar Log Manager 3128-C (Console)” on page 48

The following image shows the front panel.



The following image shows the back panel.



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 28
- "QRadar QFlow Collector 1310 SR-C/LR-C" on page 30

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).

QRadar xx29, xx48, Network PCAP, Network Insights 1920, and Incident Forensics

Review the information about the front and back panel features for appliances to confirm proper connectivity and functioning for the QRadar xx29, QRadar xx48, QRadar Network Packet Capture, QRadar Network Insights 1920, and QRadar Incident Forensics.

View the front and back panel diagrams for the following appliances:

- "QRadar xx29" on page 54
- "QRadar xx48" on page 55
- "QRadar Network Packet Capture" on page 56
- "QRadar Network Insights 1920" on page 58
- "QRadar Incident Forensics" on page 56

QRadar xx29, xx48, Network PCAP, Network Insights 1920, and Incident Forensics are based on the Lenovo System x3650 M5.

For more information about the front panel, see Front view (http://publib.boulder.ibm.com/infocenter/systemx/documentation/index.jsp?topic=/com.lenovo.sysx.8871.doc/c_front_view.html).

For more information about the back panel, see Rear view (http://publib.boulder.ibm.com/infocenter/systemx/documentation/index.jsp?topic=/com.lenovo.sysx.8871.doc/c_rear_view.html).

For more information, you can also see System x3650 M5 (https://lenovopress.com/lp0068-lenovo-system-x3650-m5-machine-type-8871.html).

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

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 jurisdictions 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 websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you provide 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 Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

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.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions..

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.

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 actual people or business enterprises is entirely coincidental.

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.

Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

Applicability

These terms and conditions are in addition to any terms of use for the IBM website.

Personal use

You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of IBM.

Commercial use

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

Rights

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

IBM Online Privacy Statement

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.

Printed in USA