IBM QRadar Security Intelligence Platform appliances

Comprehensive, state-of-the-art solutions providing next-generation security intelligence

IBM® QRadar® Security Intelligence Platform appliances combine typically disparate network and security management capabilities into a single, comprehensive solution. Appliance versions are offered for IBM Security QRadar Log Manager, IBM Security QRadar SIEM, IBM Security QRadar Data Node, IBM Security QRadar Incident Forensics, IBM Security QRadar Packet Capture, IBM Security QRadar Vulnerability Manager and IBM Security QRadar Risk Manager. For additional network visibility, IBM Security QRadar QFlow Collector and IBM Security QRadar VFlow Collector solutions can be added to the platform’s network analysis and content capture capabilities.

QRadar Security Intelligence Platform appliances are preconfigured, optimized systems that do not require expensive external storage, third-party databases or ongoing database administration. Deployment options include dedicated, high-performance appliances; Linux-based software packages; and virtualized appliances for VMware-based environments.

Organizations use these appliances to protect and grow with their businesses by addressing:

- Log management—Collection, archiving and analysis of events from various network and security devices, systems and applications
- SIEM—Integrated log management and network flow collection with advanced correlation, anomaly detection, workflow and reporting capabilities
• Event collector, event processor and data storage nodes—
  Event correlation, indexing, search capabilities and storage
• Flow processing—Layer 4 NetFlow and Layer 7 QFlow
collection and correlation
• Risk and vulnerability management—Proactive configuration
  audit, risk and compliance policy assessment, and advanced
  threat simulation
• Incident forensics and full packet capture—Quick and easy,
in-depth security incident investigation
• High availability and disaster recovery—Backup capabilities
to help ensure continuous operations

IBM Security QRadar Log Manager
appliances
QRadar Log Manager appliances are ideal for organizations
that need simplified capabilities for log management today, with
the ability to expand capacity for event processing and upgrade
to a full SIEM solution in the future. These appliances are
designed to meet the needs of small and midsized organizations,
as well as large businesses that are geographically dispersed
and require an enterprise-class, highly scalable solution.

The QRadar Log Manager all-in-one appliance is an entry-
level system that utilizes on-board event collection and correla-
tion. It can easily expand as the organization grows, with the
ability to support hundreds of thousands of events per second
through conversion into a console (distributed) deployment
with the addition of separate event processor appliances.

Larger organizations can utilize the QRadar Log Manager
console appliance with its external event collection and correla-
tion approach, which allows for dedicated search processing,
distributed correlation, reporting and central administration of
a distributed log management deployment. Console appliances
require at least one add-on event processor.

The scalable QRadar architecture includes distributed event
processor and event collector appliances for real-time collect-
tion, storage, indexing, correlation and analysis. Large, multi-
appliance deployments can support more than one million
events per second, with all data correlated in real time. For
situations where network connectivity is either unreliable or
temporarily unavailable, or in locations with low event volumes,
event collector appliances can be deployed to collect events and
forward them to an event processor or all-in-one appliance.

IBM Security QRadar 1605 and 1628 event processor
appliances
QRadar event processor appliances provide scalable event
collection and correlation for organizations of all sizes. The
IBM Security QRadar 1605 and 1628 event processor appli-
cances are expansion solutions that can be deployed in conjunc-
tion with QRadar Log Manager and QRadar SIEM console
appliances. They offer turnkey collection, storage, indexing
and real-time correlation of log data and can be deployed in
a distributed manner that can support some of the largest
deployments in the world.

IBM Security QRadar 1501 event collector appliances
QRadar event collector appliances provide continuous event
logging when network connectivity is unavailable. Event collec-
tor appliances simply collect events and forward them to an
event processor or all-in-one appliance for correlation, analysis
and long-term storage. Also designed to collect events and logs
in distributed locations with relatively low event volumes (such
as retail stores and satellite offices), they provide a more
economical approach than deploying event processors in
such scenarios.
IBM Security QRadar SIEM appliances

QRadar SIEM appliances deliver integrated log management and security intelligence technology for organizations of all sizes. Available in either all-in-one or distributed deployment configurations, they are ideal for growing organizations that seek maximum security and compliance. These appliances offer the ability to correlate logs, network flows, vulnerabilities, user identities, threat intelligence and other security telemetry. QRadar SIEM appliances often serve as the base platform for large, geographically dispersed businesses that require an enterprise-class, scalable solution.

The QRadar SIEM appliance architecture offers an easy-to-deploy, scalable model through the use of distributed event and flow processor appliances. An event processor appliance (see 1605 or 1628 descriptions within the QRadar Log Manager table) can perform real-time collection, storage, indexing, correlation and analysis of up to 40,000 events (logs) per second. A flow processor appliance can perform real-time collection, storage, indexing, correlation and analysis of up to 1,200,000 bidirectional flows per minute. Large, multi-appliance deployments can support more than one million events per second, and millions of flows per minute, with all data correlated in real time.

The IBM Security QRadar SIEM 2100 all-in-one appliance delivers a single appliance for small and midsize organizations. It provides an integrated security solution, and its intuitive user interface makes it easy to deploy in minutes. The QRadar SIEM 2100 all-in-one appliance also includes an embedded version of IBM Security QRadar QFlow Collector, which provides Layer 7 collection of network traffic flows and deep application visibility for advanced threat detection and forensic capabilities. No additional event processors or flow processors can be used to expand this system.

The IBM Security QRadar SIEM 3105 and 3128 all-in-one appliances utilize on-board event and flow processor and event collector appliances when network availability conditions warrant.

QRadar Log Manager solutions can begin as a single turnkey appliance and grow into highly distributed solutions, supporting multiple event processor and event collector appliances when network availability conditions warrant.
<table>
<thead>
<tr>
<th>Security QRadar Log Manager appliance features</th>
<th>2100 all-in-one</th>
<th>3105 all-in-one</th>
<th>3128 all-in-one</th>
<th>3105 console</th>
<th>3128 console</th>
<th>1501 event collector</th>
<th>1605 event processor</th>
<th>1628 event processor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single turnkey solution</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Part of distributed solution</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Event collection, correlation, analysis and storage</td>
<td>Max. 1,000 EPS (sustained)</td>
<td>Max. 5,000 EPS (sustained)</td>
<td>Max. 15,000 EPS (sustained)</td>
<td>Not applicable</td>
<td>Not applicable</td>
<td>Collection and forwarding only*</td>
<td>Max. 20,000 EPS (sustained)</td>
<td>Max. 40,000 EPS (sustained)</td>
</tr>
<tr>
<td>Long-term data storage</td>
<td>1.5 TB</td>
<td>6.2 TB</td>
<td>40 TB</td>
<td>6.2 TB</td>
<td>40 TB</td>
<td>600 GB</td>
<td>6.2 TB</td>
<td>40 TB</td>
</tr>
<tr>
<td>Support for high availability and disaster recovery</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

QRadar SIEM solutions can start small with an all-in-one solution and grow to support enterprise environments, using a centralized console and any number of distributed event and network flow collection appliances.
The IBM Security QRadar SIEM 3105 and 3128 console appliances utilize external event and flow processor appliances, allowing the console to perform dedicated search processing, offense management, reporting and central administration of the distributed SIEM deployment. At least one add-on event processor, flow processor, or combined event and flow processor appliance is required. Teamed with one or more QRadar QFlow Collector appliances, the console can also receive Layer 7 network analysis and content capture while aggregating other network activity data, such as NetFlow, J-Flow, sFlow and IPFIX. QRadar VFFlow Collector appliances provide the same visibility and network flow collection for VMware virtual environments.

<table>
<thead>
<tr>
<th>Security QRadar SIEM appliance features</th>
<th>2100 all-in-one</th>
<th>3105 all-in-one</th>
<th>3128 all-in-one</th>
<th>3105 console</th>
<th>3128 console</th>
<th>1705 flow processor</th>
<th>1728 flow processor</th>
<th>1805 event/flow processor</th>
<th>1828 event/flow processor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single turnkey solution</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Part of distributed solution</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Event collection, correlation, analysis and storage</td>
<td>Max. 1,000 EPS (sustained)</td>
<td>Max. 5,000 EPS (sustained)</td>
<td>Max. 15,000 EPS (sustained)</td>
<td>Not applicable</td>
<td>Not applicable</td>
<td>Not applicable</td>
<td>Not applicable</td>
<td>Max. 5,000 EPS (sustained)</td>
<td>Max. 15,000 EPS (sustained)</td>
</tr>
<tr>
<td>Support for expandable log source (devices) data</td>
<td>Not applicable</td>
<td>Requires console conversion</td>
<td>Requires console conversion</td>
<td>Requires 1605/1628 event processor appliances</td>
<td>Requires 1605/1628 event processor appliances</td>
<td>Not applicable</td>
<td>Not applicable</td>
<td>Not applicable</td>
<td>Not applicable</td>
</tr>
<tr>
<td>Flow collection, correlation, analysis and storage</td>
<td>Max. 50,000 bidirectional flows/minute</td>
<td>Max. 200,000 bidirectional flows/minute</td>
<td>Max. 300,000 bidirectional flows/minute</td>
<td>Not applicable</td>
<td>Not applicable</td>
<td>Max. 600,000 bidirectional flows/minute</td>
<td>Max. 1.2 million bidirectional flows/minute</td>
<td>Max. 200,000 bidirectional flows/minute</td>
<td>Max. 300,000 bidirectional flows/minute</td>
</tr>
<tr>
<td>Optional use of QFlow and VFFlow Collectors</td>
<td>On-board QFlow Collector included</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Long-term data storage</td>
<td>1.5 TB</td>
<td>6.2 TB</td>
<td>40 TB</td>
<td>40 TB</td>
<td>6.2 TB</td>
<td>40 TB</td>
<td>6.2 TB</td>
<td>40 TB</td>
<td>6.2 TB</td>
</tr>
<tr>
<td>Support for high availability and disaster recovery</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>
IBM Security QRadar 1705 and 1728 flow processor appliances

IBM Security QRadar flow processor appliances provide scalable flow collection, correlation and storage for organizations of all sizes. These appliances are expansion appliances deployed in conjunction with QRadar SIEM all-in-one or QRadar SIEM console appliances. They offer turnkey collection, storage, indexing and real-time correlation of flow data and are designed to be deployed in a distributed manner. QRadar flow processor appliances collect and analyze network flow data in a variety of formats including NetFlow, J-Flow, sFlow, and IPFIX. They can also process Layer 7 application-level data gathered by QRadar QFlow Collector appliances.

IBM Security QRadar 1805 and 1828 combined event and flow processor appliances

IBM Security QRadar 1805 and 1828 combined event and flow processor appliances provide event and network activity monitoring and correlation for remote or branch offices and for large, distributed organizations seeking scalable solutions. They are expansion appliances for use with QRadar SIEM console systems.

IBM Security QFlow and VFlow Collector appliances for Layer 7 visibility

QRadar QFlow Collector and VFlow Collector appliances offer a powerful solution for gathering rich network activity data in both physical and virtual infrastructures. They surpass traditional flow data (such as NetFlow) by using deep packet inspection to collect more detailed and revealing Layer 7 data. This enables application-level network activity analysis and the detection of anomalies, such as large spikes in traffic volumes. This information, when correlated with event data, enables a more advanced analysis of the overall security posture of the network.

QRadar QFlow Collector appliances gather network traffic passively through network taps and SPAN ports. They can detect more than 1,000 applications such as Voice over Internet Protocol (VoIP), social media such as Twitter and LinkedIn, multimedia including Skype, enterprise resource planning (ERP), and peer to peer (P2P), among many others. QFlow Collector appliances must be paired with either a 17XX flow processor, an 18XX combined event and flow processor, or an all-in-one SIEM appliance.

There are four QRadar QFlow Collector models:

- **IBM Security QRadar 1201 QFlow Collector**: Offers midrange, multi-port collection capabilities for underutilized gigabit Ethernet connections
- **IBM Security QRadar 1202 QFlow Collector**: Provides line-rate gigabit Ethernet network performance and multi-port flexibility for copper-based networks; is well suited for collecting and monitoring high rates of network traffic at the data center and core of an enterprise
- **IBM Security QRadar 1301 QFlow Collector**: Provides line-rate gigabit Ethernet network performance with multi-port flexibility for fiber-based networks; is well suited for collecting and monitoring high rates of network traffic at the data center and core of an enterprise
- **IBM Security QRadar 1310 QFlow Collector**: Delivers advanced network and application visibility and collection on 10-Gbps Ethernet networks

QRadar VFlow Collector appliances are virtual activity monitors that provide the same collection and visibility for virtual network and server resources as QRadar QFlow Collector appliances provide for physical resources. QRadar VFlow Collector appliances are virtual appliances that connect to the
virtual switch within a VMware virtual host. They can support up to four virtual interfaces and up to 10,000 bidirectional flows per minute. The product can also analyze port-mirrored traffic for a physical network switch, helping bridge the gap between the physical and virtual realms.

**IBM Security QRadar Data Node appliances**
IBM Security QRadar Data Node appliances (14XX Series) provide a cost-effective solution for increasing the data storage capacity and analytical processing performance of QRadar deployments. QRadar Data Node appliances can be clustered around event processors and flow processors, giving them access to the storage capacity and processing capability of each licensed data collection device. This allows aggregate storage deployments to grow to potentially hundreds of terabytes while simultaneously adding processing power to support data queries. Intelligent algorithms can distribute incoming data across data nodes in a manner optimal for both querying and storage. QRadar Data Node appliances are available as a software package or virtual appliance.

**IBM Security QRadar Incident Forensics appliances**
IBM Security QRadar Incident Forensics appliances are designed to significantly reduce the amount of time required to investigate a security incident. They help eliminate the need for expensive, specialized forensics training, and offer an intuitive user interface capable of rapidly searching through terabytes of network flow data. The appliances incorporate an Internet-style search engine interface, and provide clarity around what happened, when, who was involved, and what data was accessed or transferred. As a result, QRadar Incident Forensics appliances help remediate a network breach and prevent it from succeeding again.

**IBM Security QRadar Packet Capture appliances**
IBM Security QRadar Packet Capture appliances are companion offerings to QRadar Incident Forensics, designed to expand security data collection capabilities beyond log events and network flows to include full packet captures and digitally stored text, voice and image files. Packet captures contain the full context of information flowing through a network, and include useful metadata along with the full “payload” contents of the session.

**IBM Security QRadar Vulnerability Manager appliances**
IBM Security QRadar Vulnerability Manager appliances can help organizations proactively identify security weaknesses so they can take corrective action before a breach occurs. These appliances can perform network security scans, consolidate results, find vulnerabilities and help prioritize remediation efforts. Through integration with IBM Security QRadar SIEM, QRadar Vulnerability Manager appliances can add rich context and help lower costs by removing the need for an additional point product. They are available as a software package or virtual appliance.

**IBM Security QRadar Risk Manager appliances**
IBM Security QRadar Risk Manager appliances deliver proactive risk management for organizations of all sizes by extending QRadar SIEM capabilities to provide multi-vendor configuration audit, risk/compliance policy assessment, continuous monitoring and advanced threat simulation. These systems are deployed as an add-on to an existing IBM Security QRadar SIEM solution.
IBM Security QRadar high-availability and disaster-recovery appliances

Easy-to-deploy IBM Security QRadar high-availability appliances provide fully automated disk synchronization and failover for high availability of data collection, correlation, analysis and reporting.

IBM Security QRadar disaster-recovery appliances provide a means of safeguarding collected event and flow data by mirroring it to a secondary, identical backup appliance deployment. QRadar disaster-recovery appliances can be used in conjunction with QRadar high-availability solutions to achieve optimal system protection.

Why IBM?

IBM operates a worldwide security research, development and delivery organization comprising 10 security operations centers, 10 IBM Research centers, 17 software security development labs and an Institute for Advanced Security with chapters in the United States, Europe and Asia Pacific. IBM solutions empower organizations to reduce their security vulnerabilities and focus more on the success of their strategic initiatives. These products build on the threat intelligence expertise of the IBM X-Force® research and development team to provide a preemptive approach to security. As a trusted partner in security, IBM delivers the solutions to keep the entire enterprise infrastructure, including the cloud, protected from the latest security risks.

For more information

To learn more about IBM QRadar Security Intelligence Platform appliances, contact your IBM representative or IBM Business Partner, or visit: ibm.com/security

For more information about IBM Security QRadar SIEM software, please see the “IBM Security QRadar SIEM” data sheet.