IBM QRadar on Cloud

Self Serve App & Ask us Anything

An open mic discussion about QRadar on Cloud (QRoC) and the Self Serve app. This Panel is hosted by QRadar on Cloud DevOps, Offering, and Support.

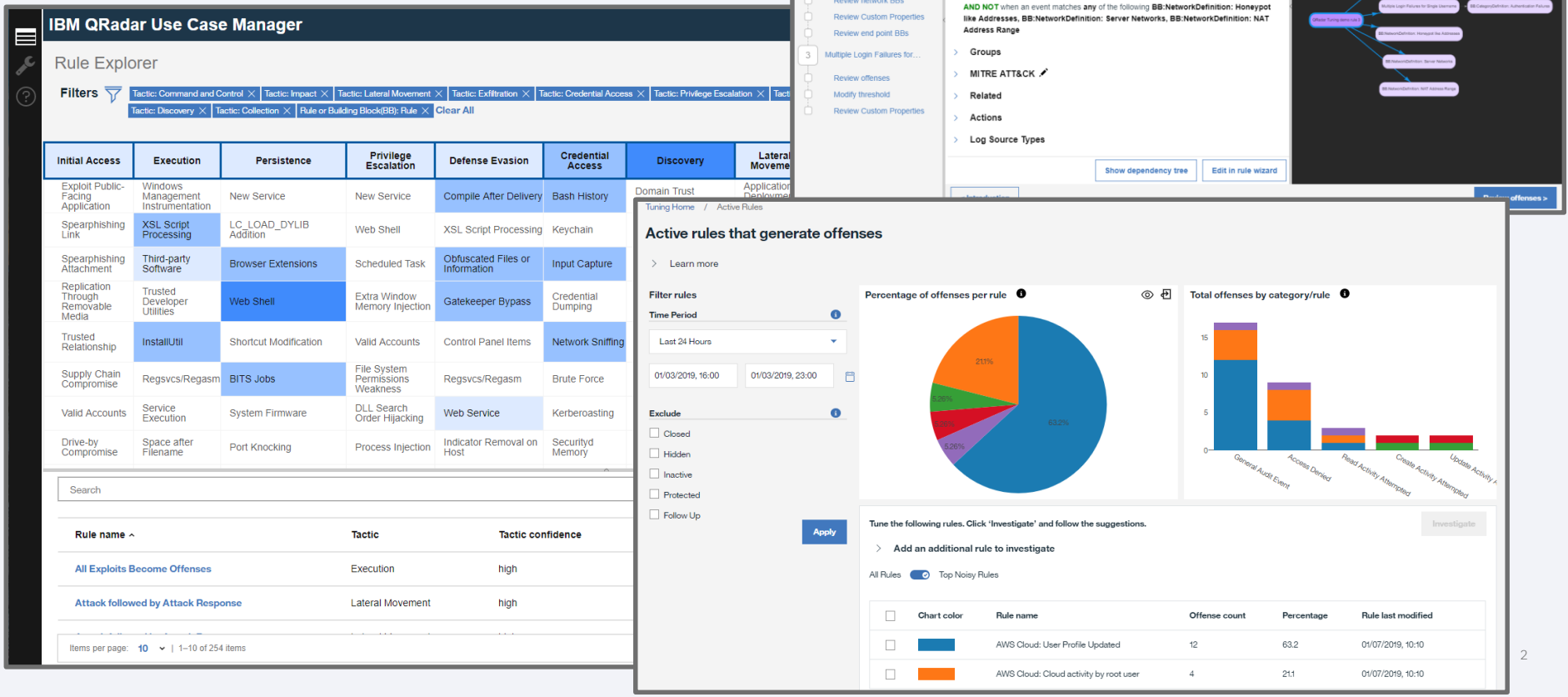
https://ibm.biz/JoinQRadarOpenMic
October 30, 2019

IBM **Security**

IBM

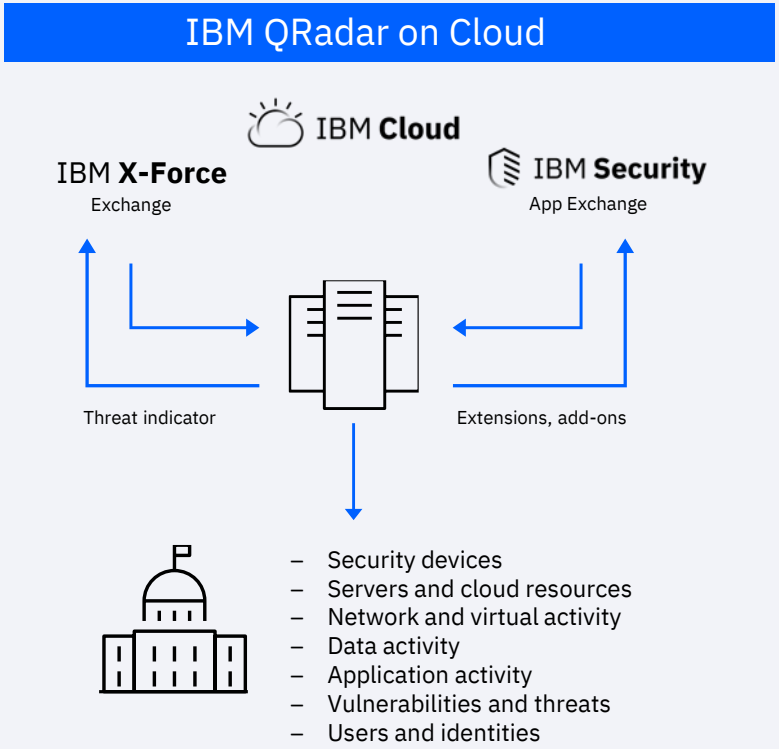
Announcement

QRadar Use Case Manager now available for QRadar on Cloud users!



About QRadar on Cloud

QRadar on Cloud offering overview



Offering highlights

- Elastic upgrades; rapid time to value
- Dedicated DevOps
- 24x7 health monitoring
- System management: upgrades, patches
- Support for 450+ security and IT integrations
- Advanced threat detection
- Configurable security operations center (SOC) and management dashboards
- Global point-of-presence coverage
- Supports multitenant mode for service providers

QRadar on Cloud: A global footprint

- Globally-distributed
- Resiliency and redundancy by default
- Built on security-rich IBM Cloud™ infrastructure

Comparing QRadar on premises and on cloud

Service component	On premises	QRadar on Cloud
Capital expense (CAPEX) budget item	✔	
OPEX budget item	✔	✔
IBM installation, deployment and upgrade		✔
IBM professionally managed infrastructure		✔
System health monitoring		✔
Configure data collection (DSMs)	✔	✔
Compliance reporting	✔	✔
Advanced attack detection	✔	✔
Incident detection and management	✔	✔
Asset modeling and vulnerability correlation	✔	✔
QVM, QFlow	✔	✔
QNI	✔	✔
IBM QRadar® Advisor with Watson™	✔	✔
App Exchange	✔	✔
Admin Access**	Root	SaaS Admin

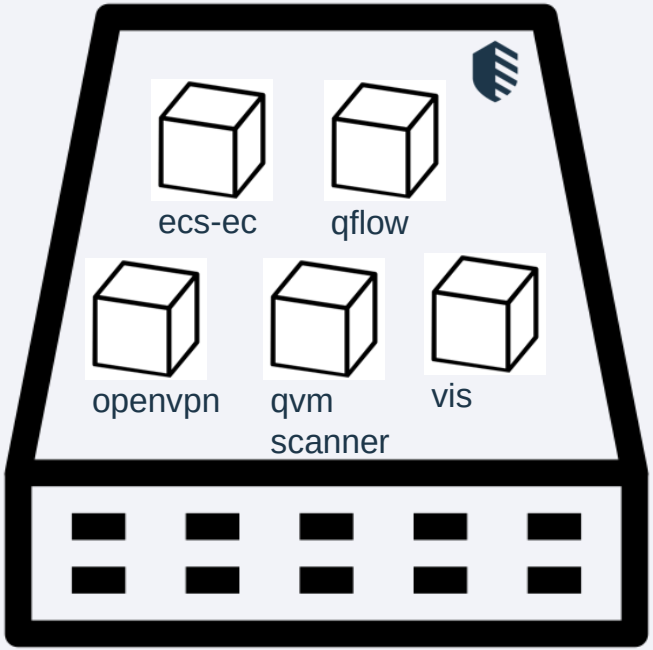
** SaaS admin doesn't include command-line interface (CLI)

DSM = device support module, QVM = QRadar Vulnerability Manager, QNI = QRadar Network Insights

What is a Data Gateway?

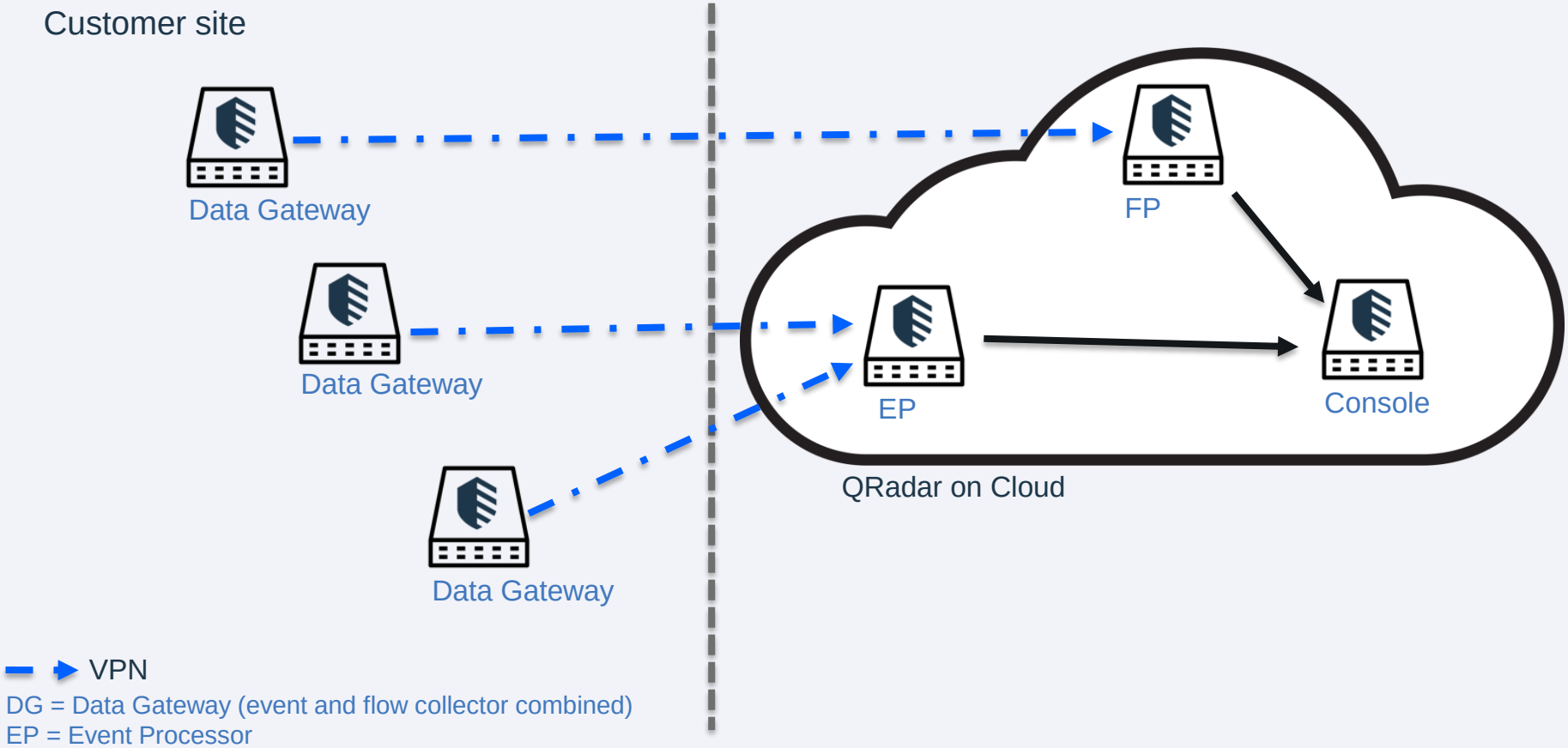
The on-premise requirement for QRadar on the Cloud is a data gateway appliance to forward the collected events and flow data to the QRadar Console running in the cloud via a secure VPN tunnel.

- Event Collector Gateway (Appliance ID 7000)
- Data Gateways install types: On-premise, VM, AWS, Azure
- 10k eps or 200k fpm or some combination
- Up to 10 Data Gateways can be installed on-premise
- Uses OpenVPN to connect to QRadar on Cloud
- 90 days of event/flow retention & 30 days offenses
- Supports all DSMs & protocols
- Incoming data buffers to disk (if required)
- Processor: 4-16 Cores
- Memory: 16GB-32GB RAM
- Disk: 500GB
- Required ports: TCP 443 Outbound



Data Gateway

Basic Architecture – Collecting From On Premise



On premises versus on cloud: Cost compare

Critical to factor in tangible and intangible costs, including opportunity cost

On premise

Requires:
- Customization
- Hardware
- Implementation
- IT staff
- Lifecycle management
- Maintenance
- Software licenses
- Training

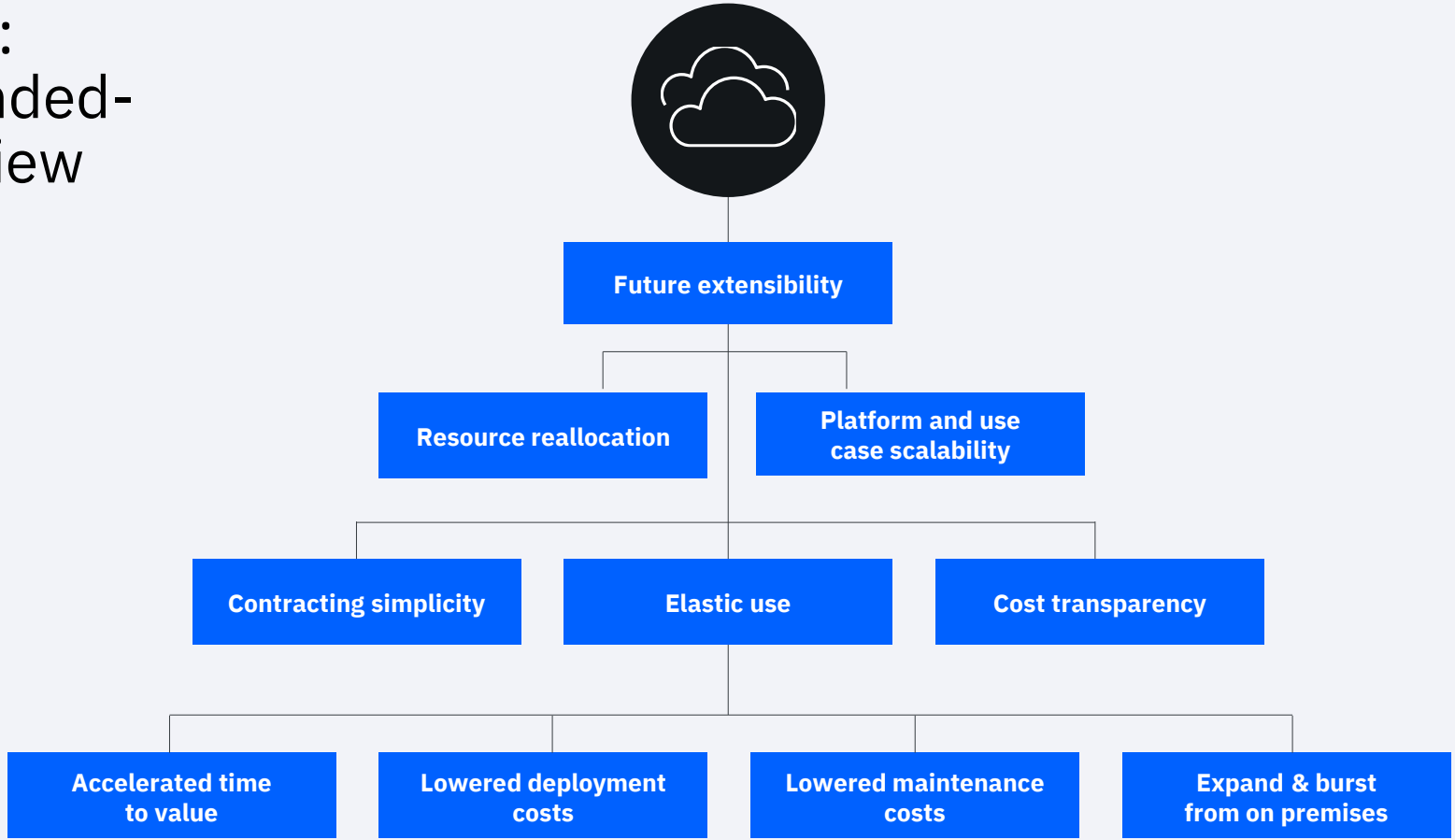
Recurring costs:
- Ongoing IT costs
- Ongoing maintenance
- Patches and fixes
- Upgrades

SaaS

Requires:
- Customization
- Implementation
- Training

Recurring costs:
- Subscription fee

On cloud: An expanded-benefit view



Self Serve App

What is the Self Serve app?

The Self Serve application is only installed on QRadar on Cloud Console appliances. It is not available on the X-Force App Exchange and is included with your Console installed.

What does the Self Serve app do?

- **App Proxy Connections** - Data gateway proxy mapping allows APPS running on the QRadar console in the cloud to reach on-prem resources via the data gateways that are installed on the customer network.
- **User Management** – Add, remove, modify users for your QRadar on Cloud instance.
- **Authorized Service Tokens** – Create, remove authorized service tokens for app or API use.
- **Whitelist hosts** - Add, remove, or modify addresses that are allows to interact with QRadar on Cloud to control access to the user interface (UI).

Demo

X-Force App Exchange

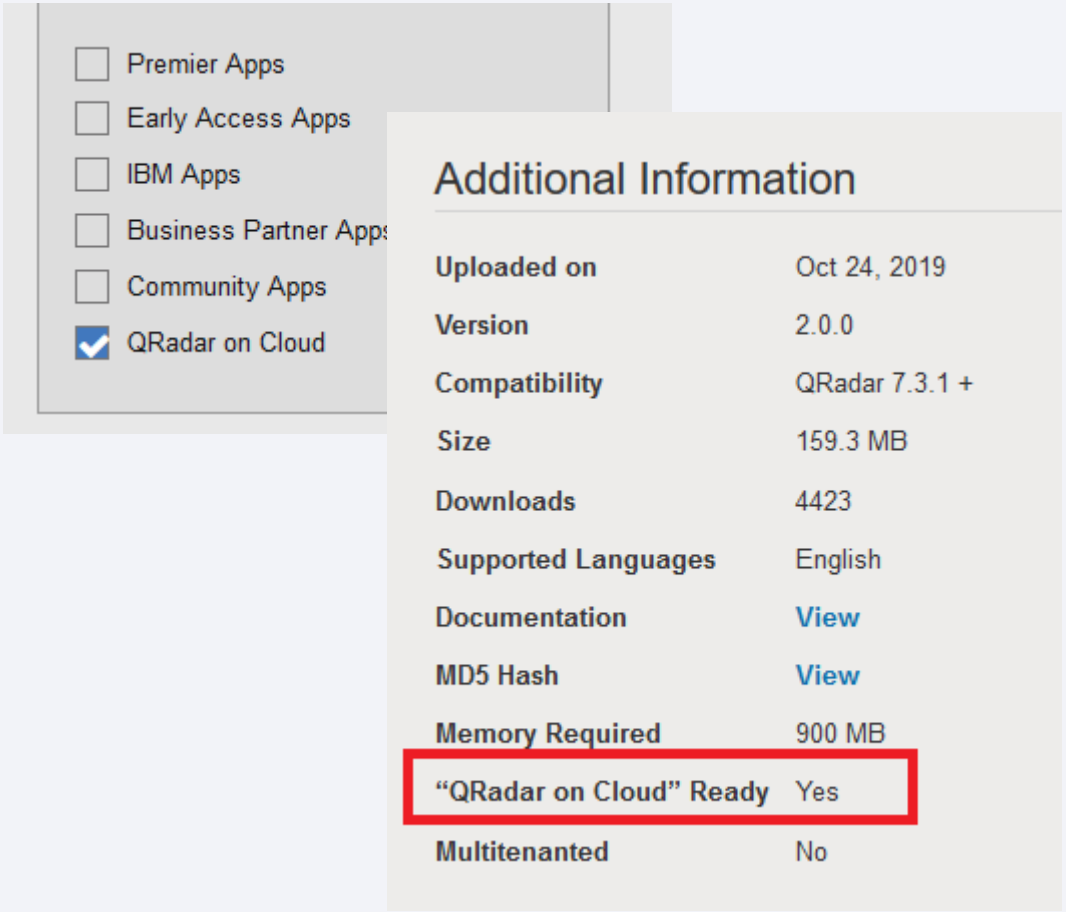
QRadar on Cloud Supported Applications

161 applications labeled as available for QRadar on Cloud currently:

- QRadar Advisor With Watson
- QRadar Cloud Visibility
- User Behavior Analytics
- IBM QRadar DNS Analyzer
- Threat Intelligence
- QRadar Pulse
- QRadar Assistant App
- QRadar Operations
- Log Source Management
- QRadar Use Case Manager
- …and more

Unsupported Applications

- QRadar Deployment Intelligence
- Incident Overview



Support

Administration or changes that requires IBM?

Work item	Description	Information that you need to provide
Auto update schedule	Selecting what time frame to receive QRadar Auto Updates or what auto update server location to use.	Time frame for your auto update and your region.
Authentication		Contact support for any authentication issues.
Whitelist changes	An asset whitelist is a collection of asset data that overrides the asset reconciliation engine logic about which data is added to an asset blacklist. When the system identifies a blacklist match, it checks the whitelist to see whether the value exists. If the asset update matches the data that is on the whitelist, the change is reconciled and the asset is updated. Whitelisted asset data is applied globally for all domains.	Provide the network range in Classless Inter-Domain Routing (CIDR) format to add to, or remove from, the whitelist.
Backup	Configuration backup occurs nightly.	The specific time to take the backup if it is scheduled outside of the normal backup time.
Restore	Restore a daily backup.	The date of the backup to restore, from the last week.
System settings	System settings are used to configure settings for databases, authentication, Consoles, and more.	Which setting and value you want to change. For more information about system settings, see the IBM QRadar SIEM Administration Guide.
Event / flow retention	Change your default retention settings in QRadar for events or flow data.	
Forwarding destinations and routing rules	You can configure QRadar systems to forward data to one or more vendor systems, such as ticketing or alerting systems. You can also forward normalized data to other QRadar systems. The target system that receives the data from QRadar is known as a forwarding destination. After you add one or more forwarding destinations, you can create filter-based routing rules to forward large quantities of data.	Details about what to forward and where to forward it. For more information about forwarding destinations and routing rules, see the IBM QRadar SIEM Administration Guide.

Common troubleshooting for access issues

- QRoC admin: SSH to their DG and telnet on port 443 to the VPN IP address? `telnet 169.48.74.49:443`

- QRoC admin: Verify if your user is attempting to VPN in from home or a non-whitelisted address. Check their IP using https://ifconfig.me/ to see their IP address details.

- Support: Can support SSH from the Console to the DG? If no, tunnels might be down from the Data Gateway. Support will determine if the vpn service requires a restart.

- Support: Try to SCP a file from the Console to the Data Gateway appliance to check bandwidth status.

What to know about installing Data Gateways?

- Your firewall to allow outgoing (and related) traffic to the console at **<HTTPS IP>** and to our VPN server at **<VPN IP>**, both on port 443.
- Your gateway must be behind a NAT firewall. Publicly-routable IPs will cause internal routing issues with the VPN server.
- When you choose an internal IP for your Data Gateway, it cannot be in the 192.168.0.0/16 range.
- The ISO to install the Data Gateway can be found on your console at Admin > Hosted QRadar.
- Your existing (and expired/consumed) tokens for installing the Data Gateway will be available at Admin > Hosted QRadar.
- If you are going to be installing more than one Data Gateway, they need to be done sequentially. Wait until the first one is completely installed, then "Deploy Changes" in the UI, then proceed to install the next one.
- Do not use the following special character(s) when creating the root password: @
- Ensure that you enter the same root password any time you are prompted for it. You may be prompted more than once, depending on your Data Gateway installation.
- Do not exit the install process at any time, even if an error message is displayed. A typical install could take more than 20 minutes once it connects to the Console and begins the add process. The installer will return to a command prompt when the install is complete, and display if it was successful or if there was an error. If there was an error, you should open a ticket with QRadar support.

Common Questions

Common questions

Question: I'm seeing issues with deploys and other general strange things happening in the UI, where do I start?
Answer: Bandwidth, is a good start. Data Gateways have a minimum bandwidth requirement and actions like a Deploy Changes can time out. During normal operation you can ask support to SCP a file from the Console to determine how fast the connection speed is in real life. On average, 0.72 Mbps is required for 1000 events per second (EPS), 7.2 Mbps for 10,000 EPS. Administrators can use the following formula to determine your bandwidth requirements:

EPS * ((average event size + 200) bytes x 8) / (1000 x 1000 x 10) = Mbps value
1000 * ((700 + 200) x 8) / (1000 x 1000 x 10) = 0.7 Mbps (EPS breakdown)

Question: Where do I find logs for communication issues?
Answer: VPN logs can be found on the Data Gateway appliance in: **`/var/log/openvpn.log`**

If you are having communication issues, submit the openvpn.log in your case so it can be reviewed.

Question: Can Data Gateway appliances forward data to other locations?
Answer: Yes, routing rules in QRadar are fully supported. However, you will be required to open a Support Case to have the destination and routing rule added to your QRadar on Cloud appliance.

Common questions

Question: Can I migrate from on-premise QRadar to QRadar on Cloud?
Answer: IBM Professional Services can review and migrate settings and data from QRadar on-premise installations. This is not an issue that DevOps or QRadar Support would take cases about.

Question: Is the QRadar REST API available to QRadar on Cloud users?
Answer: Yes, administrators can access the QRadar API.

Question: Does QRadar on Cloud support WinCollect?
Answer: Yes, but only for Stand-alone (unmanaged) WinCollect agents.

Question: Can my 90 days of data be extended?
Answer: Yes, up to 1 year of retention can be provided.

Question: How often are backups taken?
Answer: Data is backed up hourly. Configurations are backed up daily.

Question: Is “Cold” (offline storage) storage for my event/flow data available?
Answer: Yes, users can purchase offline data in 12-month increments.

Question: Is offline storage encrypted?
Answer: Yes, all data in the IBM Cloud is encrypted-at-rest and in-transit using AES-256.

IBM Security Product Professional Services

IBM specialists remotely deliver product professional services.

- **Cloud security product page:** ibm.com/security/security-intelligence/qradar/securing-the-cloud
- **IBM Security Community:** ibm.com/security/community
- **IBM Security App Exchange:** exchange.xforce.ibmcloud.com/hub/
- **IBM Knowledge Center:** ibm.com/support/knowledgecenter/en
- @ibmsecurity
- securityintelligence.com
- youtube/user/ibmsecuritysolutions

Request a trial of IBM QRadar on Cloud

Take a 14 day test drive of our detection capabilities and learn about QRadar

ibm.com/us-en/marketplace/hosted-security-intelligence

Final Questions

Thank you

Follow us on:

ibm.com/security

securityintelligence.com

ibm.com/security/community

xforce.ibmcloud.com

@ibmsecurity

youtube/user/ibmsecuritysolutions