# Stay in control with IBM QRadar on Cloud

QRadar

IBM Security

# Contents

## Introduction

## Key benefits of IBM QRadar on Cloud

## Next steps

# Intelligent SIEM as-a-service

Securing data and networks on premises and in the cloud is a daunting task for any sized organization. New vulnerabilities are discovered almost daily; new malware strains are developed as soon as a detection script is written for the old ones; and cybercriminals can buy prepackaged exploit kits on the darknet backed by professional support teams. As a security analyst, you need more than a few point solutions designed to defend the network's edge. You need visibility, perspective and an innate sense of when things just don't seem right.

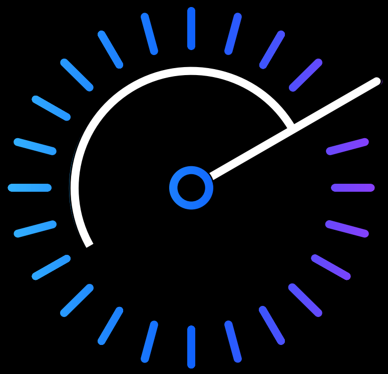
IBM® QRadar® on Cloud excels at these tasks. With robust security information and event management (SIEM) capabilities, the solution helps guard data and networks with a wide range of capabilities that can show you who's doing what, where and when. It uses dashboards and advanced visualizations, compressing thousands or millions of discrete incidents into simple indications of suspected trouble, and preserves detailed records of any suspicious activity for future analysis. At the same time, its advanced logging capabilities and report generation tools help you quickly comply with basic requirements, such as regulatory reporting mandates.

Learn more about IBM QRadar on Cloud →

QRadar on Cloud can process greater than

500,000

events per second.[1]



# Key business benefits of IBM QRadar on Cloud

> “CIOs must change their line of questioning from **‘Is the cloud secure’** to **‘Am I using the cloud securely?’** ”

Gartner
Gartner.com

Explore the benefits →

# Meet regulatory and security demands at the same time

Chances are, you've deployed basic security measures at the perimeter of your network to prevent simple attacks, but most endpoints have security flaws and some users just can't resist clicking on bad links. Devices and credentials are too frequently compromised, opening the door to data loss and potential business disruption.

Deploying a data collection and compliance reporting system is fairly easy but making the auditors happy and protecting your organization's critical data can be anything but easy. The more advanced the system the more thoroughly it prepares you for managing routine activities and unusual network breaches, requiring investigation and incident response.

Get more insight into today's enterprise threats from IBM X-Force Threat Intelligence® →

Watch and discover more about advanced persistent threats →

> "The processing and correlation of unstructured data using cognitive capabilities will give us more context for even more accurate, actionable recommendations, and will make the lives of security analysts easier on a day-to-day basis."

**Christophe Bianco**
Managing Partner and
Chief Technology Officer,
Excellium Services

Read the case study →

**What QRadar on Cloud offers:**

- Shift from CAPEX to OPEX model
- Addresses skills gap
- High visibility, compliance and security
- Over 500 out-of-the-box integrations
- Data-driven insights using AI
- Flexibility and scalability

# Gain deep insights to protect your critical assets on cloud

Detecting and eradicating malware and establishing firewall rules to guard subnets are important. That's why you've probably invested in perimeter security. But security analytics software is based on the fundamental concept that no perimeter connected to the internet is truly secure, and that organizations must be able to detect behavioral changes and anomalies.

With the cloud model, your organization can deploy security-rich data gateways and send your security data into an expertly deployed and managed cloud environment with predictable monthly operational fees. The cloud model leaves you in control—and allows your staff to spend the bulk of its time monitoring the environment, tuning threat detection rules, and customizing regulatory or management reports rather than applying software patches and performing data backups.

Keep up with compliance and regulations →

An IT decision maker spends nearly

2 hours daily looking for relevant data.[2]

69% of companies

see compliance mandates driving spending.[3]

# Get your organization compliance-ready

The QRadar on Cloud solution serves a major business-driven function. By protecting data and preserving in audit-ready form a record of the security practices and events that enable protection, it helps organizations comply with government and industry regulations. If ignored, these mandates can snag an organization with penalties just as surely as malware can snag it with data loss.

A host of requirements and best-practice standards, designed to protect consumer's personal and financial information and increase corporate transparency, govern how customer and organizational data is gathered, stored, and secured. The Sarbanes-Oxley Act (SOX), the Payment Card Industry Data Security Standard (PCI DSS), the Health Insurance Portability and Accountability Act (HIPAA), the European Union's General Data Protection Regulation (GDPR), and other regulations mean that enterprises could face civil or criminal penalties, bans on the use of payment cards, and other risks that can include devastating business interruptions for noncompliant practices.

Check out the IBM QRadar Content Extension for GDPR →

HIPAA violations can incur criminal penalties, as well as fines up to USD 50,000 per violation, with an annual maximum of

USD 1.5 million.[4]

88% of companies

spent more than USD 1 million on preparing for the GDPR.[3]

# Help prioritize threats

Some security threats can be approached tactically, using specialized tools that address individual aspects of security. These tools can be useful in addressing defined threats and known problems, and they might generate responses as simple as selectively blocking network ports, removing an instance of malware, or patching an identified vulnerable asset.

But QRadar software is far more valuable than point solutions because it collects a broader array of security data that's shared across essentially all security intelligence modules. Once it observes and calculates thresholds for data flow norms on your network, it automatically senses events that violate these thresholds and alerts your security staff. Threshold rules can help detect unusually large outbound data transfers, bandwidth use, changes in applications or a suspiciously high number of login attempts from an unexpected Internet Protocol (IP) address. QRadar also watches for connected events, for example comparing user identities, source and destination IP addresses, and geographic locations where the activity originated. It examines these linked events for context to better distinguish true offenses from one-off instances of new behaviors.

Read more about IBM X-Force security predictions for 2020 →

Cybersecurity is becoming more complex than ever. In 2019, the average time to identify and contain a breach was

279 days

with the global average cost of data breach estimated at

USD 3.9 million.[5]

Healthcare is the most expensive industry with data breaches costing organizations

USD 429 per lost or stolen record.[5]

# Adopt a new expense model with cloud-based security software

Software may be critical to enabling IT and enterprise operations, but for most organizations, keeping security software in-house adds an extra workload that can actually get in the way of their core security tasks. Reducing and simplifying the mix of roles security personnel need to play can be a significant motive for adopting a cloud-based alternative.

Achieving better security will always |require some level of human and technical resources—but with a hosted, cloud-based solution, the time and associated expenses security staff spend on routine duties can be reallocated to analysis and planning.

Read this white paper to learn more about QRadar on Cloud, a flexible and highly scalable SaaS solution →

## Cost compare

On premises versus on cloud

| **Startup costs** | On premises | SaaS |
|---|---|---|
| Customization | ● | ● |
| Hardware | ● | |
| Implementation | ● | ● |
| IT staff | ● | |
| Lifecycle management | ● | |
| Maintenance | ● | |
| Software licenses | ● | |
| Training | ● | ● |
| **Recurring costs** | | |
| Ongoing IT costs | ● | |
| Ongoing maintenance | ● | |
| Patches and fixes | ● | |
| Upgrades | ● | |
| Subscription fee | | ● |

> “Our average, total cost has increased but we don’t look at these increases as necessarily bad. We are investing in the protection of data for the long term because we know data breaches are not going away.”[6]

An IT Supervisor/South Africa/Industrial in 2018 Cost of Data breach Study, Ponemon Study

Read the study →

# Extend QRadar with other security tools

QRadar on Cloud inherits more than 500 existing integrations developed over the last decade, responding to requests from on-premises clients and aligning with third-party solutions that complement the security intelligence platform. The experienced professionals rolling out your cloud deployment will rarely have to develop any new support modules to begin accepting data from your assets and applications. Most clients will begin realizing value in just days after an agreement is completed.

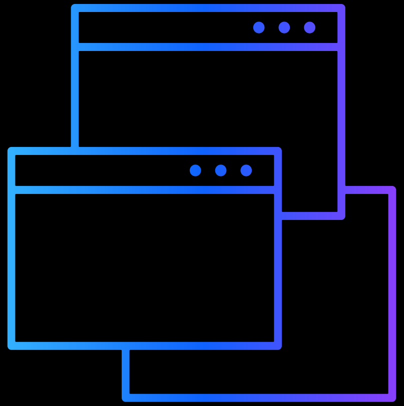
You can download and install new extensions or apps from the IBM Security App Exchange that will enhance your network monitoring capabilities, and your IBM Cloud™ maintenance team will support the technology extension. There are already dozens of these supported extensions, including new visualizations, integrations, patches, custom rules and complete new apps, such as the IBM QRadar User Behavior Analytics app. All content on the site is reviewed by IBM Security through its Ready for IBM Security Intelligence validation process.

Learn more about QRadar plug-ins and extensions through the IBM Knowledge Center →

QRadar can collect log events and network flows from

500+

applications and devices.[7]



# Address skills gap with AI

In recent years, there has been a sharp increase in cybersecurity skills gap. IBM QRadar Watson Advisor App is designed to help your organization detect threats faster.

The app uses artificial intelligence (AI) to assist users with incident and risk analysis, triage and response, and enables security operations teams to do more with greater accuracy. The result? A drastic reduction in the time spent investigating incidents from days and weeks to minutes or hours.

Additionally, security teams will spend less time working on routine security operations center (SOC) tasks and more time on other strategic priorities.

See how QRadar Advisor with Watson can help your SOC team do more with greater accuracy. Watch the video →

Discover QRadar Advisor with Watson Version 2.5.0 →

Unfilled cybersecurity jobs are expected to reach

1.8 million

by 2022.[8]

According to a recent study, the global cybersecurity workforce needs to

grow by 145%

to close skills gap. In the US, it needs to grow 62%.[9]

"Cargills Bank was able to leapfrog these limitations by using IBM QRadar SIEM and QRadar Advisor with Watson to receive real-time, prioritized alerts. IBM's best-in-class cognitive security portfolio will help us pre-empt threats and mitigate risk, thereby supporting our position as a leading digital bank."

**Rohan Muttiah**
Chief Operating Officer,
Cargills Bank

Read the case study →

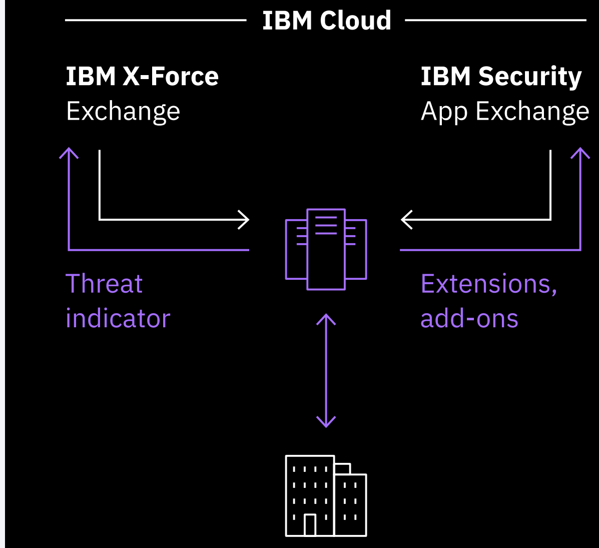
# Achieve more flexibility and scalability

Buying software-as-a-service (SaaS) offers advantages in scalability and flexibility because it means that capacity changes aren't tied to onsite infrastructure and are far less dependent on the availability of in-house personnel. Companies can change very rapidly in this economy. Be it occasional spikes in traffic or permanent changes in workloads due to mergers and acquisitions, with the QRadar on Cloud solution, they can scale up their computing power as needed. Because the infrastructure lives in the cloud and designed with capacity changes in mind, there's no need to change the software locally. Capacity can be dialed up or down on short notice and with minimal need for customer involvement.

**QRadar on Cloud 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 SOC and management dashboards
- Global point-of-presence coverage
- Multitenant model support for service providers

## IBM QRadar on Cloud



**IBM Cloud**

**IBM X-Force** Exchange

**IBM Security** App Exchange

Threat indicator

Extensions, add-ons

**Client on premises or on cloud assets**

- Security devices
- Servers and cloud resources
- Network and virtual activity
- Data activity
- Application activity
- Vulnerabilities and threats
- Users and identities

> "Before, we always felt like we were on the back foot when it came to security, but now we're much more proactive."

**Michael Warrer**
CIO, NRGi

Read the case study →

# Gain access to managed services

For organizations that need help beyond the capabilities their security staff has the time or expertise to provide, optional additional management services also are available. QRadar on Cloud offers integration with IBM Managed Security Services, offering fully managed services with 24x7 eyes-on-glass security threat monitoring and response. Optionally, organizations can outsource their security operations to a third-party IBM Managed Security Service Provider (MSSP) partner. The MSSPs offer comprehensive security management and monitoring solutions, and a wide range of complementary threat monitoring services to cover either essential or advanced use cases.

IBM has been selected once again in the 2019 Gartner Magic Quadrant for Managed Security Services, Worldwide.

Download the report →

IBM offers managed security at a global scale with local delivery capabilities to help secure your hybrid cloud and multicloud environments.

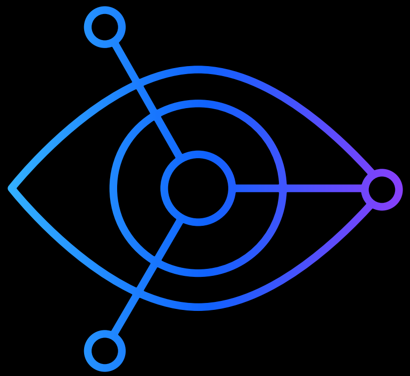
Learn more about IBM Managed Security Services →

The QRadar on Cloud infrastructure is

monitored

24x7

by trusted IBM professionals.[10]



# Move to a cloud-first operating expense model

IBM QRadar on Cloud applies the experience gained from thousands of on-premises QRadar deployments to meet the needs of your environment.

There’s no need to maintain or tweak on-premises security software. With automatic software updates and on-demand scalability, QRadar on Cloud helps make life simpler for IT security staff by moving from a large capital expenditures (CAPEX) model to a more flexible model based on operating expenses (OPEX).

The system is capable of enterprise-grade analysis, with capabilities that include:

- Data collection, correlation, and reporting capabilities to achieve regulatory compliance
- Large event per second (EPS) maximums, meeting the needs of clients with hundreds of global locations
- Highly available system configuration with committed service levels and uptime guarantees
- Apps, add-ons and extensions through IBM Security App Exchange
- Enriched alerts with included X-Force Threat Intelligence feed

**What’s next?**
Take this 14-day test drive of the QRadar on Cloud solution and learn about its sophisticated detection capabilities.

Start my no-cost trial →

# Why IBM?

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned X-Force Research, provides security intelligence to help organizations holistically protect their infrastructures, data and applications. It offers solutions for identity and access management, database security, application development, risk management, endpoint management, network security, and more.

These solutions enable organizations to effectively manage risk and implement integrated security for mobile, cloud, social media, and other enterprise business architectures. IBM operates one of the world's broadest security research, development and delivery organizations, monitors 15 billion security events per day in more than 130 countries, and holds more than 3,000 security patents.

Additionally, IBM Global Financing provides numerous payment options to help you acquire the technology you need to grow your business. IBM provides full lifecycle management of IT products and services, from acquisition to disposition. For more information, visit ibm.com/financing.

To learn more about IBM QRadar Security Intelligence Platform in the cloud, please contact your IBM representative or IBM Business Partner, or visit ibm.com/software/products/en/qradar-on-cloud.

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
February 2020

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

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. THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation.

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.

[1] IBM Knowledge Center. https://www.ibm.com/support/knowledgecenter/SS42VS_7.3.2/com.ibm.qradar.doc/c_siem_vrt_ap_ov.html

[2] “Data management challenges are having a severe impact on profitability.” Help Net Security, March 13, 2019. https://www.helpnetsecurity.com/2019/03/13/data-management-challenges/

[3] Josh Fruhlinger. “Top cybersecurity facts, figures and statistics for 2018.” CSO, October 10, 2018. https://www.csoonline.com/article/3153707/top-cybersecurity-facts-figures-and-statistics.html

[4] “HIPAA Violations and Enforcement, American Medical Association. Accessed December 2019. https://www.ama-assn.org/practice-management/hipaa/hipaa-violations-enforcement

[5] 2019 Cost of a Data Breach Report: https://www.ibm.com/security/data-breach

[6] 2018 Cost of a Data Breach Study: Global Overview. Conducted by Ponemon Institute. https://www.intlxsolutions.com/hubfs/2018_Global_Cost_of_a_Data_Breach_Report.pdf

[7] QRadar On Cloud Overview. YouTube. https://www.youtube.com/watch?time_continue=53&v=dCTnR_hHToU&feature=emb_logo

[8] Marten Mickos, “The Cybersecurity Skills Gap Won't Be Solved in a Classroom.” Forbes, June 2019. https://www.forbes.com/sites/martenmickos/2019/06/19/the-cybersecurity-skills-gap-wont-be-solved-in-a-classroom/#353d37bd1c30

[9] “Cybersecurity Workforce Needs to Grow 145% to Close Skills Gap”, SECURITY, November 2019, https://www.securitymagazine.com/articles/91224-cybersecurity-workforce-needs-to-grow-145-to-close-skills-gap

[10] IBM Managed Services - https://www.ibm.com/security/services/managed-security-services