Purchase and deploy security in the cloud—wherever your data may be

Now organizations moving to cloud or hybrid models can achieve efficiencies in compliance reporting and advanced threat detection

IBM Security White Paper

IBM QRadar provides visibility into your network

For any sized organization, securing data and networks today is a daunting task. 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® excels at these tasks. It 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 it 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.

And now, with IBM QRadar on Cloud, you can avoid deploying and maintaining the hardware and the software, and focus instead on using the intelligence that QRadar gathers. You'll stay in control because your team monitors what's going on. Study the environment, fine-tune your detection capabilities and collaborate with peers to deepen all of your threat detection and response skills.

QRadar cloud solutions can process up to

80,000

events per second.[1]

Read more on the web about IBM QRadar on Cloud.

[1] "IBM Security Intelligence on Cloud onboarding," *IBM Knowledge Center.*

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.

First, consider regulatory mandates. These demand properly locked-down systems and data—and documentation to prove that everything is protected. Deploying a security analytics system can lighten the workload compliance reporting can place on your security team. That's because these systems make it easier to prepare comprehensive, correctly-formatted reports, and to collect, curate, and review information about your network in audit-friendly form.

Now consider the complexity of your internal environment where critical data is created, stored and transmitted. Modern networks are loaded with assets, each of which also typically carries an exploitable security flaw. These include the network's variety of operating systems, its mix of hardware—from servers to routers, switches to firewalls—and application software, web-based or not. Each element makes it harder to secure the network as a whole, and cybercriminals exploit the weakest links to gain access.

Deploying a data collection and compliance reporting system is fairly easy, but making the auditors happy and protecting your organization's critical data is anything but. The more advanced the system—such as QRadar, backed by the IBM Sense Analytics Engine™—the more thoroughly it prepares you for managing both routine activities and unusual network breaches requiring investigation and incident response.

In 2015, hacking incidents reached a nine-year high, with an **8.4%** *jump over 2014.*[1]

▸ Get more insight into today's enterprise threats from IBM X-Force®.

[1] "Identity Theft Resource Center Breach Report Hits Near Record High in 2015," *Identity Theft Resource Center*, January 2016.

Gain deep insights to support compliance and security

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.

One way to add security analytics is to budget for a large capital expense, clear space in the data center, and spend weeks to months deploying an on-premises solution as your team schedules an auto-update service, configures a threat intelligence feed, creates a network scanning schedule, and defines data retention periods—all before realizing much value from the investment.

Another way is to deploy secure 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.

Within days, your staff won't be disturbed by a straightforward log event (Jackie Jones logged in at 2:32 p.m. from Chicago), but will be alerted by a behavioral change (Jackie Jones logged in later that week at 3:07 a.m. from southeast Asia). By eliminating needless distractions, you'll have the time to discover if there's a reasonable explanation for the difference (Jackie's traveling) or if something else is afoot.

QRadar can create more than

1,500

predefined report types, from regulatory compliance to vulnerability management.[1]

▸ Read the IBM white paper to learn more about QRadar.

[1] Lee Bell, "IBM builds QRadar Security Intelligence in the cloud," *The Inquirer*, April 2015.

Set your organization on the path to regulatory compliance

QRadar on Cloud 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. Sarbanes-Oxley (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. Even without the pressure of penalties, the process of ensuring regulatory compliance serves to encourage best practices in data storage, encryption and protection of network nodes. While no software can replace the work of designing and maintaining an infrastructure that incorporates a regulation-compliant workflow and storage architecture, QRadar on Cloud helps you look for noncompliant practices to ensure a clean bill of health for data and applications.

HIPAA violations can incur criminal penalties, as well as fines up to

USD50,000

per violation, with an annual maximum of USD1.5 million.[1]

▸ Learn more about the dos and don'ts of regulatory compliance in this white paper.

[1] "HIPAA Violations and Enforcement," *American Medical Association*. Accessed July 26, 2016.

Watch data closely to meet new and evolving threats

Some security threats can be approached tactically, using specialized tools that address individual aspects of security. These 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 can be far more valuable than point solutions because it collects a broader array of security data that is shared across 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 IP address.

QRadar also watches for connected events 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. It even looks for patterns of *non*-use, as when a particular service or asset unexpectedly disappears. This could mean an asset is offline (perhaps because of malware) or that QRadar has detected a deviation from baseline user behavior.

Criminal attacks are the leading cause of medical record data **breaches** *in healthcare.*[1]

▸ Learn more about the deep security knowledge gathered by IBM X-Force.

[1] "Sixth Annual Benchmark Study on Privacy and Security of Healthcare Data," *Ponemon Institute*, May 2016.

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.

What's more, the lifecycle of hardware for hosting on-site—from initial specification to eventual disposal—can bring an additional burden. It often means keeping enough spare parts on hand and selecting hardware with maintenance in mind. And it all typically becomes the responsibility of already-busy local staff.

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 re-allocated to analysis and planning. System upgrades and application fixes can be handled remotely, by specialists, and can take place without disrupting your local IT infrastructure. With the remote access that defines cloud applications, your local staff members don't have to spend time physically installing and provisioning servers to gain new software capabilities. Together, these factors mean that cloud-based solutions can be acquired and expanded on aggressive schedules—typically in days or weeks—without overprovisioning of on-site resources.

The QRadar on Cloud infrastructure is monitored

24x7

by trusted IBM professionals.[1]

▸ Read this IBM white paper to learn more about how adopting cloud software can help regulate expenses.

[1] "IBM QRadar on Cloud," *IBM Corp.*, April 2015.

Prepare for change—and growth—with your security investment

As with nearly any other technology, security tools rarely stand alone. Tools that work together can better address a changing threat environment or add specific capabilities—and that includes the perimeter defense tools in which you've already invested.

QRadar on Cloud inherits more than 500 existing integrations developed over the last decade, responding to requests from on-premises clients and partnering 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 receiving value in just days after an agreement is completed.

Security data gathered through IBM X-Force Threat Intelligence research, for example, is also seamlessly and continuously integrated into your QRadar on Cloud deployment, drawing on hundreds of terabytes of information about evolving threat vectors and witnessed attacks as well as previously unreported vulnerabilities.

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.

QRadar can collect log events and network flows from

500+

applications and devices.[1]

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

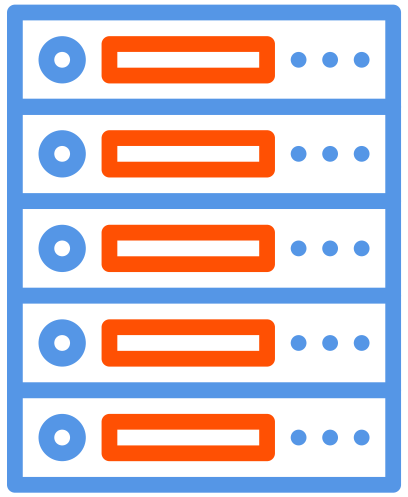
[1] "Introducing the IBM Security App Exchange," *IBM Corp.*, December 2015.

Put a scalable, flexible infrastructure to work when you need it

Buying software as a service offers advantages in scalability and flexibility, because it means that capacity changes are not tied to on-site infrastructure, and they are far less dependent on the availability of in-house personnel. To understand the advantages of security analytics software deployed in the cloud, it makes sense to consider two different kinds of scale changes:

Seasonality: Most businesses have ebbs and flows in their workload, some of them quite predictable in their scope if not their exact timing. With conventional software purchases, buying for the worst case scenario (that is, the busiest or most demanding time) may be the only option, even if it means spending for more hardware capacity than what's required for typical use.

Company growth: In the same way, organizations planning a merger, acquisition or other growth often are forced to unnecessarily "buy big" in anticipation of greater capacity needs. With cloud-based deployments, however, an enterprise can buy—or release—capacity in small increments as needed. Because the infrastructure lives in the cloud and is 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.



Many companies have employed as much as

5x

the data center space they need for steady-state business cycles.[1]

▸ Learn what analysts have to say about the financial case for moving your business data to the cloud.

[1] David Linthicum, "Cloud Economics – Are You Getting the Bigger Picture?" *Cloud Technology Partners*, May 2016.

Rely on the real-world capabilities of IBM QRadar on Cloud

Cloud-based software can help you bypass often considerable infrastructure costs—such as scoping, provisioning and testing time incurred by internal personnel or consultants—that an on-premises deployment demands. IBM QRadar on Cloud applies the experience gained from thousands of on-premises QRadar deployments to meet the needs of your environment. It's a jumpstart—in the cloud.

By deploying QRadar on Cloud, you can keep or expand the monitoring capabilities you've already developed, but allow analysts to spend more time understanding threat intelligence data or applying their skills to protecting existing assets. There's no need to maintain or tweak on-premises security software. With automatic software updates and on-demand scalability, QRadar on Cloud makes life simpler for IT security staff as it brings predictable monthly operating expenses to the organization.

A QRadar on Cloud deployment means you'll get the expertise, power and extensibility you need. The system is capable of enterprise-grade analysis, with capabilities that include:

- Web browser accessibility
- 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 for near-continuous availability
- Apps, add-ons and extensions through IBM Security App Exchange
- X-Force Threat Intelligence feed on developing situations

And 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.

Companies with a cloud strategy spent

22%

less on security than those without one.[1]

Watch this video to learn more about QRadar on Cloud.

[1] "Buying Intentions Survey: Security," *Nucleus Research*, February 2016.

Why IBM?

IBM Security solutions help enterprises prevent, detect and respond to security threats and vulnerabilities with integrated hardware, software and service offerings. Powered by deep analytics and trusted IBM Security expertise, the IBM portfolio of scalable, industry-leading tools delivers wide-ranging security intelligence.

QRadar on Cloud uses the same underlying technology to deliver log management, network flow analysis, real-time and historical analytics and vulnerability management to any size of organization looking to outsource the acquisition, deployment and management of the QRadar security intelligence infrastructure. The solution is hosted within IBM Cloud Data Centers and is available worldwide. For regions with specific in-country data storage requirements, QRadar on Cloud is currently enabled within the following locations: US – Dallas, Texas; Canada – Toronto, Ontario; European Union – Frankfurt, Germany; Latin America – Sao Paulo, Brazil. Additional locations are planned.

In addition, QRadar On Cloud has an open framework that enables easy integration with solutions posted on the IBM Security App Exchange. The IBM Security App Exchange allows partners to share applications, security application extensions and enhancements to IBM Security products. Security teams using QRadar on Cloud can download and install the solutions at their own convenience using a self-service model with no changes to existing hosting agreements (unless basic licensing terms are exceeded).

For more information

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

About IBM Security
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, offering 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. We provide full lifecycle management of IT products and services, from acquisition to disposition. For more information, visit: **ibm.com**/financing

IBM Security
Route 100
Somers, NY 10589

Produced in the United States of America
January 2017

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 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.