IBM Security

IBM

IBM QRadar on Cloud

Rapidly detect threats and comply with regulations with a flexible, highly scalable SaaS solution

Introduction

As the threat landscape evolves, organizations can no longer rely on check-the-box compliance controls. Instead, they need comprehensive visibility into threats and risks within their environment so that they can better protect sensitive data and assets from advanced attackers. And, they need to achieve this in spite of a shrinking cyber security talent pool. Leading security intelligence solutions can help organizations gain an end-to-end security view across on-premises and cloud-based environments without requiring months of professional services or major customization investments. When delivered from the cloud, these solutions can also offer faster setup and scaling, access to dedicated DevOps resources, a lower cost of ownership and built-in resiliency and redundancy.

IBM® QRadar® on Cloud is a highly scalable Security Information and Event Management (SIEM) solution that consolidates log, event, and flow data from thousands of devices distributed across on-premises and cloud-based networks, performing immediate correlation and analysis to distinguish real threats from false positives. QRadar on Cloud helps security teams accurately detect and prioritize threats, and it provides intelligent insights that enable teams to respond quickly to reduce the impact of incidents.

This brochure explores the advantages of using an enterprise-ready security intelligence solution, delivered from the IBM® Cloud™ with optional threat monitoring capabilities provide by IBM Services or a Managed Security Service Provider (MSSP). It will look at how IBM QRadar on Cloud, a Security as a Service (SaaS) offering, enables organizations to stay ahead of the latest threats with industry-leading technology combined with trusted IBM expertise—resulting in greater flexibility, cost effectiveness, and peace of mind.

Security intelligence is vital in today’s hybrid-cloud environments

To remain ahead of attackers, security teams need actionable insights into the most critical threats occurring in their environments.

The right security intelligence and analytics tools can help:

- Reduce a large number of security events to a small number of actionable offenses
- Decrease false positives
- Inform security teams about what has been exploited and what malicious activity has taken place as a result—such as data loss, theft or fraud
- Provide quicker threat detection and accelerate incident response

Security intelligence solutions use advanced security analytics and automation to provide deeper insights into threats. These solutions are designed to collect, normalize, correlate and distill massive amounts of data – including network traffic, logs, user behavior, system configurations, vulnerability reports, and others – into actionable, prioritized alerts that notify security teams about both known and unknown threats.

System and network activities from on-premises and cloud environments can be collected and analyzed using a coherent and integrated approach. With an expectation that on-premises IT and cloud IT must co-exist, it is important to deploy a security intelligence solution that is flexible enough to fit into a mixed cloud and on-premises environment and handle data sources across a broad range of infrastructures.

IBM delivers advanced security intelligence and analytics, hosted from the cloud

The harsh reality is that today’s IT organizations must work within increasingly limited budgets. Rather than deploying another point solution, they need an integrated platform that can provide advanced security intelligence with rapid time to value—while also providing the scalability and functionality needed to quickly and easily meet new requirements.

Integrated, end-to-end visibility

IBM QRadar on Cloud provides a fast, easy, cost-effective way to meet changing needs for security intelligence and analytics. The solution delivers market-ready SIEM capabilities as a SaaS solution, eliminating the need for infrastructure management.

With IBM QRadar on Cloud, clients can spend up to 100 percent of their available time monitoring security events in their environment, investigating potential incidents, and building knowledge about normal versus suspicious activities. QRadar on Cloud is built for resiliency to help protect your organization against hardware failures. It also benefits from the IBM X-Force® Threat Intelligence data feed to provide the latest insights into newly discovered threats and attacks.

Key capabilities of the IBM QRadar on Cloud offering include:

- A single architecture for analyzing event, log, flow, vulnerability, user and asset data
- Near real-time correlation and behavioral anomaly detection to identify high-risk threats
- High-priority incident detection among billions of data points
- Insights and visibility into network, application and user activity
- Streamlined regulatory compliance with out-of-the-box collection, correlation and reporting capabilities

QRadar on Cloud delivers the key capabilities of IBM QRadar SIEM configured to customer specifications and deployed within a dedicated private cloud environment. The solution is hosted by IBM within secure IBM Cloud data centers with built-in resiliency and failover-supporting infrastructure.

How it works

QRadar on Cloud is a component of the IBM QRadar Security Intelligence Platform, which offers integrated capabilities for log management, SIEM, risk and vulnerability management, user behavior analytics and network packet inspection. Security teams can access QRadar SIEM capabilities from a web browser, just as they would if the infrastructure were deployed on-premises. But IBM experts manage the infrastructure, on-going maintenance, disaster recovery and technical support.

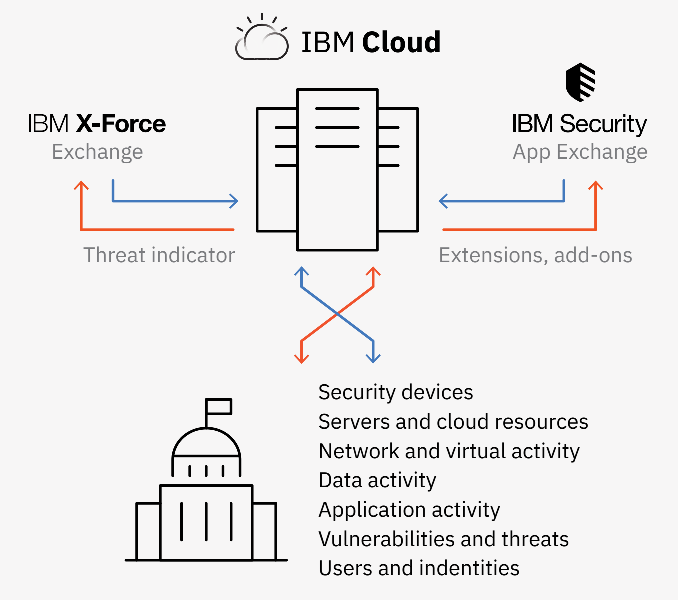
Clients can start with basic log management and compliance reporting, and then add more capabilities and services over time as their team grows. Simpler competitive solutions lack the ability to add vulnerability management, user behavior analytics (UBA) or network packet inspection, which can result in out-of-date investments that may fall over when a real cyber-attack occurs.

Optionally, IBM Global Security Services or one of IBM Security's MSSP partners can offer a wide range of complementary threat monitoring services to cover either essential or advanced use cases, or they can separately assist with emergency response services to help remediate confirmed network breaches.

QRadar on Cloud is designed to:

- Collect and correlate over 400,000 events per second from on-premises and cloud-based sources to detect malicious behavioral patterns and enable a faster response to critical threats
- Scale up and down to meet dynamically changing business needs
- Help ensure enterprise resiliency and availability with expert staff that monitors server health, installs critical patches, and upgrades software
- Align with an organization's operational expense budget model by featuring monthly billing and flexible payment options, as opposed to traditional budgeting based on large, up-front capital expenditures
- Help address the skills shortages by reducing time-to-deployment and overhead associated with appliance management
- Include comprehensive threat intelligence from IBM X-Force research and development, one of the most respected commercial security research teams

IBM QRadar on Cloud deployment model



- Cloud-based offering of #1 Security Intelligence solution
- Collects data from both on-premises and cloud resources
- Leverages real-time threat intelligence from X-Force
- Includes access to value-added features from App Exchange

Start your journey to a hosted, cloud-based SIEM solution

QRadar on Cloud provides organizations with quick access to market-leading SIEM technology, the flexibility to meet changing needs, and the trust of a world-class service team. In addition, the IBM offering enables organizations to take a phased approach to cloud-hosted security services. Organizations can start by outsourcing the core SIEM infrastructure and optionally add services or migrate to an even more comprehensive managed services engagement over time.

Flexibility

QRadar on Cloud is designed to support a wide variety of security use cases. Organizations do not have to worry about large up-front capital expenditures, burdensome infrastructure deployment and management, or IT maintenance expenses; they can simply plan for operating expenses via periodic billing.

At the same time, QRadar on Cloud enables organizations to customize the service to fit their specific needs. To help customers get up and running quickly, the solution offers over 450 out-of-the-box integrations with commercial products, as well as a custom Device Security Module (DSM) Editor to easily collect and parse custom log sources.

Once the solution is deployed, customers can leverage over 150 pre-built apps and content packs from IBM Security App Exchange to add new integrations, rules, analytics, searches, dashboards and reports. Open APIs and an SDK enable both customers and partners to optionally develop their own apps to address custom use cases and extend the value of existing solutions. With QRadar on Cloud, organizations get the flexibility to adapt to their own requirements—with the assurance that the underlying infrastructure is configured according to security best practices.

Trust

Instead of dealing with the high capital cost and complexity of an on-premises infrastructure, companies utilizing QRadar on Cloud have the help of IBM experts for a predictable cost that aligns with their operations budgets. The solution is used today and trusted by leading organizations around the world, including:

- A leading energy company that reduced two billion logs and events per day to 25 high-priority offenses
- A financial information provider that tracked 250 activity baselines and saved 50 to 80 percent on staffing
- A global bank that identified and blocked more than 650 suspicious incidents in the first six months of security operations

Conclusion

IBM QRadar enables security teams to collect, correlate and analyze information from across data silos—including the cloud—to automatically detect and prioritize threats. And now, QRadar on Cloud gives organizations a way to access QRadar capabilities without having to manage the infrastructure themselves.

QRadar on Cloud provides organizations with a starting point for cloud-delivered security intelligence—but it's a starting point that comes from a trusted vendor, delivering industry-leading SIEM technology, backed by expert services and support. Over time, organizations can optionally continue the migration to a fully outsourced solution. With deep visibility into both cloud and on-premises infrastructure, QRadar on Cloud can help organizations stay a step ahead of the latest threats.

For more information

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

About IBM Security solutions

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 and development, provides security intelligence to help organizations holistically protect their people, infrastructure, 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, monitoring greater than 60 billion security events per day in more than 130 countries, and holds more than 3,700 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 2019

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 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] "Forrester's 10 Cloud Computing Predictions For 2018." Louis Columbus. Forrester. November, 2017. https://www.forbes.com/sites/louiscolumbus/2017/11/07/forresters-10-cloud-computing-predictions-for-2018/#8e9bc914ae18

[2] "The 2017 Global Information Security Workforce Study: Women in Cybersecurity." Frost & Sullivan. March 2017. https://iamcybersafe.org/wp-content/uploads/2017/03/WomensReport.pdf