IBM QRadar on Cloud

Quickly add threat protection and compliance reporting without capital expenses

Highlights

- Leadership security intelligence solution protects against advanced threats, reduces compliance risks and simplifies reporting.
- Acquire and realize improved security in days with no capital purchase expenses and professional IBM installation and infrastructure management.
- Delivers broader insight collecting data from both on-premises & cloud resources including full data isolation.
- Benefit from real time threat intelligence data feeds and easily upgrade choosing from a variety of complementary offerings and service levels.
- Optional Threat Monitoring services are available to address limitations in security staff availability or skills gaps.

For organizations seeking to simplify their operations and even treat network security costs as a series of monthly operating expenses rather than any capital investments, IBM QRadar on Cloud provides a managed environment for the deployment and maintenance of IBM QRadar Security Intelligence. The solution offers an alternative to traditional on-premise deployments using cloud technology to collect, analyze and store an organization's core log source and netflow security data using a protected data gateway connection.

IBM QRadar on Cloud is configured as a highly available solution protecting 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. Clients can spend 100% of their available time monitoring the environment, investigated suspicious incidents and building knowledge about normal vs. abnormal activities.

Different from a managed SIEM environment, IBM QRadar on Cloud still relies on an organization's in-house staff to perform threat monitoring, vulnerability management, risk analyses and data breach remediation services. Many organizations are uncomfortable taking the complete leap to cloud-based security, and so QRadar on Cloud provides a stepping-stone in the process, where all the acquisition and management services for the infrastructure are performed by IBM Security experts. What this delivers is rapid time-to-value for deploying and configuring a leadership security intelligence capability, and 24x7 infrastructure maintenance services to upgrade all software to the latest available releases, apply all fix packs and critical patches, and respond to client change requests.

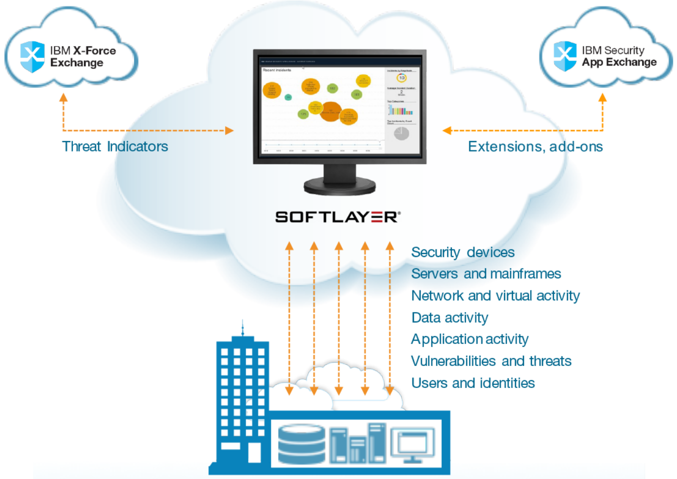
IBM QRadar on Cloud is a flexible solution that can deploy as either a true Software as a Service (SaaS) offering or combine with hybrid cloud environments to improve visibility into cloud-based applications. And as with QRadar on-premise deployments, you can avoid a rip-and-replace scenario or a situation where security teams are dealing with multiple point solution products looking at different data sets and wondering if it's all part of the same attack.

Clients can start with basic log management and compliance reporting and add more capabilities and services over time, as their team grows. Simpler, competitive solutions lack the ability to add vulnerability management and user behavioral analytics (UBA) modules and end-up being dead-end investments that fall over when a real cyber attack occurs.

IBM can also offer a wide range of complementary threat monitoring services through our Global Security Services team to cover either essential or advanced use cases or separately assist with emergency response services to help remediate confirmed network breaches.

IBM QRadar on Cloud is the logical first-step to utilizing cloud computing dynamics for network security purposes. It helps organizations begin at the beginning, and gradually build their comfort factors with outsourcing more and more security data collection, analysis and reporting capabilities.

- Collects and correlates up to 80,000 events per second from all network log source devices to detect malicious behavrioal patterns.
- Collects and analyzes up to 300K network flows per minute to understand which assets have been involved in a connection and for how long.
- Helps address any lack of in-house skills and resources to deploy and manage an on-premise SIEM solution in days rather than months.
- Infrastructure monitored 24x7 by trusted IBM service professionals with immediate application of critical patches ensuring the software is always up-to-date.
- Make temporary or permanent adjustments to monthly license capacities to adjust for seasonal changes or long-term business growth.
- Add optional threat monitoring services for even more professional protection.



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

IBM QRadar on Cloud deployment overview

Cut Costs and Add Flexibility

Organizations who are budget challenged or struggling to find and hire appropriate resources can address their immediate security and compliance reporting needs with IBM QRadar on Cloud. The SaaS licensing model converts large, upfront capital expenses on hardware and professional services engagements, to a more simplified monthly service fee, that can easily be upgraded to address evolving needs.

IBM QRadar on Cloud customers have the option to migrate to a fuller managed security services solution using even more IBM resources schooled in the latest methods of cybercrime and newly emerging attack methodologies. For example, IBM's X-Force Exchange can help alert clients to developing situations within their industry or across regional divides using a real time and collaborative threat intelligence website. Also, 24x7 threat monitoring services are available.

For more information

To learn more about this offering contact your IBM representative or IBM Business Partner, or visit: ibm.com.

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.

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
April 2016

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.

♲ Please Recycle