IBM QRadar Data Store

Highlights

- Collect, normalize and store log data for a fixed and predictable price
- Simplify compliance reporting by using a single platform
- Gain deeper insights from AI-powered investigations
- Provide the necessary data to start true threat hunting operations

As the sheer volume of data continues to exponentially grow, organizations are tasked with not only protecting more data than ever before but also proving to numerous regulatory bodies and government agencies that proactive protections are in place. Not surprisingly, this requires even more data.

Despite the fact that not all data is created equally and not all data requires the same oversight, organizations are often forced to choose between either paying a significant premium to collect, store and report on all the data needed to meet their requirements or alternatively choosing to spare their limited budgets, not collect any non-critical data and accept the risks associated with incomplete audit trails. Each of these choices comes with significant tradeoffs. Modern organizations have a variety of needs, and they demand flexible options to fit the wide spectrum of security, operations, compliance and budget requirements

The Solution

IBM QRadar Data Store enables organizations to collect, normalize and store non-critical log data for future reporting and investigation. The solution offers security and operations teams a tiered approach for handling large volumes of data, enabling them to address various business and security requirements without breaking their budgets.

As an extension of the QRadar Security Intelligence Platform, customers can store noncritical security and compliance data in QRadar Data Store to gain the ability to run centralized reports, searches and in-depth investigations against enterprise-wide security and compliance data from a single console.

Unlock the Value of Log Storage

Simplify compliance reporting

As part of the QRadar Security Intelligence Platform, log data stored within QRadar Data Store can be searched and reported on alongside all other security, incident and threat intelligence data stored within the platform. Instead of using a third party data lake solution for logs, which can require additional investment and manual effort to piece together data from siloed solutions, QRadar Data Store enables you to centrally store and report on all relevant log data from a single solution and interface. In addition, operations teams can granted centralized, read-only access to log data from the systems they respectively manage, enabling them to measure performance and run their own analytics without requiring direct access to log data.

Extract additional value from QRadar Advisor with Watson

QRadar Advisor with Watson is at its best when it has deep insight into a customer's network. When an incident is discovered by IBM QRadar, Watson Advisor can use its corpus of information to automatically research the Indicators of Compromise (IOCs) and learn more about the potential threat, threat actors and related IOCs. Watson Advisor then takes what it has learned from its various research sources and compares the new information against log data stored within a customer's local QRadar environment. Watson Advisor can then uncover similar events potentially related to the same attack campaign and determine the true scope and severity of the incident. By storing enterprise-wide log data in QRadar Data Store, Watson Advisor can gain greater insight into your local environment, deliver more relevant results and uncover IOCs that may otherwise be missed, helping to both improve the speed and accuracy of investigations.

Enable threat hunting

Advanced organizations that are ready to build a threat hunting program can benefit from storing large volumes of normalized logs in a single location. By first normalizing log data, threat hunters can work from a common understanding of what happened without having to be experts in hundreds, if not thousands, of enterprise-wide technologies and log formats. When integrated with IBM i2 Analyze, threat hunters can visually map out potential threats, including the users, assets, vulnerabilities and tactics associated with each, and easily share this information with team members. As a result, teams can more easily collaborate, be more effective and better identify stealthy threats.

In Summary

QRadar Data Store, an extension of the QRadar Security Intelligence Platform, enables organizations to cost-effectively collect, normalize and store large volumes of data to enable easier compliance reporting, optimize AI-powered incident investigations and provide threat hunting teams with the data needed launch searches and investigations.

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

For more information

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

This document contains information pertaining to the following IBM products which are trademarks and/or registered trademarks of IBM Corporation:
IBM®, IBM logo, ibm.com®, IBM X-Force® and QRadar®

All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.