IBM Security Guardium Insights Data Sheet

Highlights

- Improves data security and compliance visibility
- Monitors activity related to critical data in on-prem and DBaaS sources
- Enables investigation and exploration of issues and risks
- Helps users take action to protect data across different data sources
- Offers advanced analytics for enriched data security insights
- Helps users prioritize activities using risk-based scores and alerts
- Enhances flexibility of IT security and operations

Companies of all types and sizes struggle with the implementation and usability of fragmented, disconnected security tools and the specialized skills and costs required to integrate and operate them. As a result, many organizations lack a complete view of their data security and compliance landscape, which can diminish their ability to effectively assess, prioritize and respond to threats and issues.

Additionally, business may be under increased pressure to move their data and infrastructure to the cloud in order to achieve greater business agility, responsiveness, and to save costs. They may also face external and internal pressures to support data privacy and compliance requirements – which might become more complicated in the cloud. These types of organizations might be struggling to understand how to leverage their existing on-prem data security investments, while forging into the hybrid multi-cloud world.

Many traditional data security platforms have become overwhelmed by the increased volume of data security and auditing data, whether that data comes from monitoring information and events, or whether it's other audit-related data that must be stored for longer and longer periods of time due to new data privacy mandates. Reporting can become very slow, and in some cases, customers can only keep 30-90 days of 'hot' data live to use for data security analytics, which is quite limiting if you are trying to identify threats that may have emerged over months or years. As a result, data security administrators often try to speed up the performance of data security platforms by adding additional hardware and processing power – but this becomes a constant cycle and a resource-intensive way to keep up with the expanding volumes of data security and compliance data.

IBM Security Guardium Insights is a hybrid cloud data security hub designed to help clients improve visibility into user data activity and risk, protect data more efficiently, and enhance IT flexibility as organizations embrace new business paradigms - such as moving data to the cloud.

Guardium Insights can help users:

- Create and leverage centralized data security and compliance insights over long periods of time
- Produce data security and compliance reports in seconds, leveraging out-of-the-box reports and content
- Apply near real-time data activity monitoring and protection capabilities for DBaaS sources, such as AWS Kinesis, and for data sources supported by IBM Security Guardium Data Protection
- Leverage advanced analytics to help uncover risk and threat patterns and take action
- Prioritize data security and compliance activities based on automated risk-based scoring and alerting
- Modernize the data security infrastructure with a microservices-based, containerized solution
- Deploy flexibly by leveraging the Red Hat OpenShift Container Platform

Guardium Insights works together with IBM Security Guardium Data Protection and database-as-a-service sources to help customers streamline data security and compliance infrastructure and processes, allowing them to focus on increasing agility and improving response to threats and business requirements.

Key Features

To help deliver on the vision of a modernized hybrid cloud data security hub, IBM Security Guardium Insights provides advanced data risk visualization, protection, and remediation capabilities, many of which are described below.

Centralized data security and audit hub, efficiently retaining historical data

One of the challenges of traditional data security and compliance solutions is retaining and maintaining data security and audit data over long periods of time. In some cases, administrators can only store or archive data that’s between 45 and 90 days old, and short data security and compliance data retainment timeframes can make it very difficult to create detailed reports for auditors. Data security specialists also may not be able to apply data security analytics over a long enough time period to identify threats. Data infiltrations that began months ago may go undetected under constructs that only analyze the last 90 days.

IBM Security Guardium Insights is architected to provide data security administrators with a centralized hub where they can store their data security and compliance data. By redirecting data to IBM Security Guardium Insights, security organizations can streamline their IBM Security Guardium Data Protection architecture by reducing the number of aggregators, helping improve operational efficiencies, and assisting data security teams to become more focused on data security.

Guardium Insights can ingest data security and audit data from database-as-a-services (DBaaS) sources such as AWS, as well as from Guardium Data Protection (Guardium Data Protection for Databases, for Data Warehouses, and for Big Data environments). From DBaaS sources, users stream data directly to Guardium Insights. The Guardium Data Protection collectors or central managers send the data to Guardium Insights. All of this data is gathered into Guardium Insight's data mart, which is powered by the market-leading IBM Db2 Warehouse, provided as part of the Guardium Insights integrated solution.

Hybrid multi-cloud data activity monitoring and protection

As organizations move data to the cloud, they often discover that the data security capabilities inherent in a public cloud service offering typically only function within that specific environment. So if an organization has cloud projects dispersed across multiple vendors, they may lack the centralized visibility needed to monitor for threats across all of their cloud hosted and on-premises data sources.

Guardium Insights enables users to get a consolidated view of how and by whom critical data is being accessed and used across hybrid multi-cloud environments.

Risk-based views and alerts

Guardium Insights provides data security teams with risk-based views of the environment, to help them prioritize their workload and their efforts to help protect the business.

Upon logging into Guardium Insights, security analysts are presented the information they need to understand the greatest risks in their environment, such as the number of data sources that may be at risk, the potential number of risky users, and a list of risk-based analytical alerts.

From this dashboard, users can click through for more details about risks and issues to get to the root cause of potential issues.

Data security teams can quickly see and access their most recently generated reports ,as well as the status of the environment and details of errors or problems.

Out-of-the-box reports

To help simplify key activities for data security administrators, Guardium Insights comes with pre-built data security and audit reports on data related to events such as: user activity, dormant accounts, deployment health, brute force attacks, application health, insider threat indicators, privileged user activities, privilege escalation, connection detection, denial of service, and more.

Using these reports, data security admins can investigate data activity over time periods for data security and/or audit purposes and share information with teammates via CSV or a link to the report results in order to accelerate remediation efforts.

Advanced Analytics

Guardium Insights uses patented advanced analytics to help data security teams uncover areas of risk, emerging threat patterns, and potential application hijacks. Predictive analytics and outlier detection analytics help users identify, prioritize, and respond to issues and threats.

Guardium Insights learns normal operational and process patterns to help identify suspicious operations and potential fraud- or threat-related activities in near-real time. Users can view the granular data related to IP address, time, activity, confidence scores related to the analytics, and more to investigate issues.

Outlier detection analytics within Guardium Insights are designed to help users improve accuracy and spot anomalous activity such as SQL injections and credentials abuse related to databases, tables, and users. When an anomaly is detected, an alert is sent to the data security team so they can investigate the issue and take action.

In addition to monitoring activity from a central location, users can take action to protect data from across environments. The Guardium Insights dashboard, data security teams can:

- Trigger data protection policies in Guardium Data Protection
- Directly block suspect users from accessing DBaaS sources
- Create tickets in incident management solutions such as ServiceNow, Inc.
- Share issues and threats with Security Analysts for investigation

The IBM Security Guardium platform provides a data security and compliance solution designed to help clients locate, classify, and take action to protect sensitive data residing on-premises and in the cloud. It can help organizations address their data protection and compliance needs with automation and customizable workflows that deliver the visibility and actionable insights, real-time controls and scalability to help identify and protect critical data across multicloud environments.

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 IBM X-Force® research, provides security solutions to help organizations stop threats, prove compliance, and grow securely.IBM operates one of the broadest and deepest security research, development and delivery organizations. It monitors more than two trillion events per month in more than 130 countries, and holds over 3,000 security patents. To learn more, visit https://www.ibm.com/security

For more information

To learn more about the IBM Security Guardium Insights offering, please contact your IBM representative or IBM Business Partner, or visit: https://www.ibm.com/us-en/marketplace/guardium-insights.

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