IBM Security Guardium Insights

Enhance visibility and protection to reduce risk with unified data security

Highlights

Enhances data security and compliance visibility through monitoring, retention and automation

Enables investigation, action and protection across hybrid environments

Offers advanced analytics, risk-based scoring and flexible IT security

Streamlines policy, audit and report sharing for compliance efforts and data protection

Companies struggle with fragmented security tools, lack of specialized skills and costs, limiting their view of data security and compliance workflows. Cloud migration and data privacy requirements add complexity. Traditional security platforms can be overwhelmed by data volume, often resulting in slow reporting and limited data retention.

IBM Security® Guardium® Insights is a data security platform designed to help clients improve visibility into user activity and behavioral risk, help meet compliance regulations, protect data more efficiently, and enhance IT flexibility as organizations embrace new business paradigms such as moving IT infrastructure and operations to the cloud. Whether you're looking for a software or SaaS solution, Guardium Insights can easily automate and orchestrate security and many compliance activities whether deployed on-premises or in public or private clouds.

Enhances data security and compliance visibility through monitoring, retention and automation

Guardium Insights addresses challenges inherent in traditional data security and compliance solutions by providing a centralized hub for retaining and maintaining data security and audit data for extended periods. Unlike other tools on the market, Guardium Insights allows data security specialists to store data for as long as needed, enabling them to create detailed reports for auditors and apply data security analytics over a longer time frame to identify threats.

By consolidating and retaining data in Guardium Insights, security organizations can streamline architecture, reduce the number of appliances, improve operational efficiencies and allow data security teams to focus on value-add data security activities rather than infrastructure management. Guardium Insights can ingest data from various sources, including Database-as-a-Service (DBaaS) sources such as AWS Aurora and Azure Event Hubs, as well as from Guardium Data Protection, and store it in the Guardium Insights repository.

Organizations often face limitations with data security capabilities that are confined to specific environments. Guardium Insights helps address this challenge by providing a consolidated view of critical data access and usage across hybrid multicloud environments.

Enables investigation, action and protection across hybrid environments

Guardium Insights supports the separation of duties across different roles to help data security teams ensure data security and audit data is more secure. It also provides checks and balances across different user roles. Guardium Insights helps administrators assign and manage access controls by role.

Administrators may choose from either predefined roles or bespoke roles, as well as implement more granular access control on a report-by-report basis.

In addition to analyzing and reporting on how Guardium Insights users are accessing data in on-premises and DBaaS environments, it’s also necessary to understand how they are interacting with the collected data. Guardium Insights creates its own audit trail so administrators can view events related to the modification of configuration data, user actions, privileged access, system events and more.

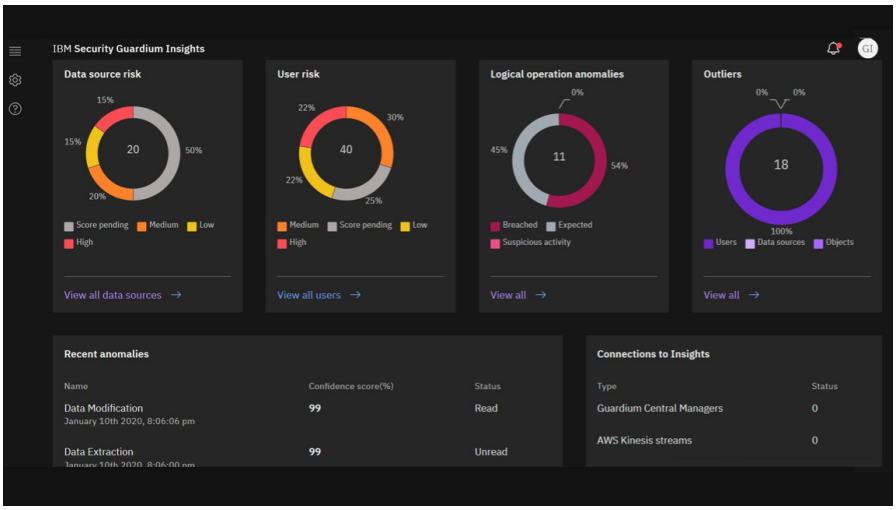

Figure 1. The dashboard allows you to understand your data security posture at a glance.

Offers advanced analytics, risk-based scoring and flexible IT security
Guardium Insights uses advanced analytics to help data security teams uncover areas of risk, emerging threat patterns and potential application hijacks. The analytics engine within Guardium Insights learns which operations and data interaction patterns are normal for a given organization, then helps identify suspicious behavior, potential fraud or threat-related activities in near-real time. Users can investigate issues by viewing granular data related to IP address, time, activity, confidence scores related to the analytics and more. The results of the analytics are processed though the Guardium Insights risk-scoring engine and tagged with a high, medium or low risk score based on the type of anomaly uncovered.

These risk events help identify patterns impacting data risk including behavior outliers, user types, database vulnerabilities, data classification, exceptions and errors, and policy violations. Users can drill down to access more details to determine a root cause. They can also access frequently generated reports and activity information within the Guardium Insights environment.

In addition to monitoring activity from a central location to more easily spot anomalies, data security specialists can also take immediate action to protect data from across environments. Through the Guardium Insights dashboard, data security teams can:

- Create tickets in incident management solutions such as ServiceNow, Inc.
- Create and map tickets and cases in Guardium Insights to the cases application in IBM Security QRadar® Suite and assign to a security analyst for escalation and remediation. Share issues and threats with security analysts or other stakeholders for additional investigation or follow-up.

Streamlines policy, audit and report sharing for automated compliance and data protection

To help meet data compliance goals, Guardium Insights provides out-of-the-box policy templates to simplify regulatory compliance. You also have the option to create your own custom policies. This allows administrators to define what data is monitored and how it's captured in order to meet the specific security and compliance needs of your organization. You can specify and schedule audit milestones and tasks to help streamline the process of conducting and reporting on a data security audit.

Out-of-the-box customizable reports

To help simplify key activities for data security administrators, Guardium Insights includes prebuilt data security and audit reports related to use cases 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.

Admins can create custom reports with the advanced reporting capabilities of Guardium Insights. The ability to create advanced custom filters for reports, including nested conditions, case sensitivity and usage of the "AND/OR" operators helps simplify reporting. These reports may be emailed to teammates and key stakeholders from within the application or they can be downloaded for later use and collaboration.

With all the data security and audit data available in Guardium Insights, it's crucial that this data be shared across the business with consuming applications such as IBM Security QRadar Suite or Splunk. Guardium Insights provides open REST APIs along with interactive API documentation so any consuming application that supports REST API integration can call Guardium Insights and get relevant data—minus the noise—to enhance their operations. Stakeholders and consuming applications can access reports, anomaly information, risk information and more.

1T+

IBM monitors more than one trillion events per month in more than 130 countries.

3K+

IBM holds over 3,000 security patents.

Conclusion

IBM Security Guardium Insights provides a data security and compliance solution designed to help clients locate, classify and take action to help protect sensitive data residing on-premises and in the cloud. Whether you're looking for a SaaS or software option to help solve your data security and compliance challenges, we have a solution to support your business. Guardium Insights helps bring security teams, data and workflows together on a single platform.

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 drive security into the fabric of their business so they can thrive in the face of uncertainty. IBM operates one of the broadest and deepest security research, development and delivery organizations. Monitoring more than one trillion events per month in more than 130 countries, IBM holds over 3,000 security patents. To learn more, visit ibm.com/security.

For more information

To learn more about IBM Security Guardium Insights, contact your IBM representative or IBM Business Partner, or visit: ibm.com/products/guardium-insights.

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the
United States of America
June 2023