



IBM Security Guardium Insights for IBM Cloud Pak for Security

Enhance visibility and protection, understand risk, uncover hidden threats, and help streamline operations with centralized data security and compliance data.

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 multicloud 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

Highlights

- Improves data security and compliance visibility
- Monitors activity related to data in on-prem and DBaaS sources
- Retains data over long periods of time to support compliance
- Enables users to create and share security and audit reports in seconds
- Enables key stakeholders to investigate and explore issues and risks
- Helps users take action to protect data across hybrid environments
- Offers advanced analytics to help spot threats at the first anomaly
- Helps users prioritize activities using risk-based scores and alerts
- Enhances flexibility of IT security and operations



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 for IBM Cloud Pak for Security is a data security hub that is 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 IT infrastructure to the cloud. It shares common components and a containerized hybrid multicloud architecture with IBM Cloud Pak for Security to enhance ease of use and more easily automate and orchestrate security activities and enable clients deploy on-premises or in public or private clouds.

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, using customizable out-of-the box reports and content
- Apply near real-time data activity monitoring and protection capabilities for Database-as-a-Service (DBaaS) sources, such as AWS Kinesis and Azure Event Hubs, and for data sources supported by IBM Security Guardium Data Protection
- Leverage advanced analytics to help uncover risk and threat patterns and take immediate 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

Guardium Insights for Cloud Pak for Security works together with IBM Security Guardium Data Protection and DBaaS 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, while supporting compliance needs.

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

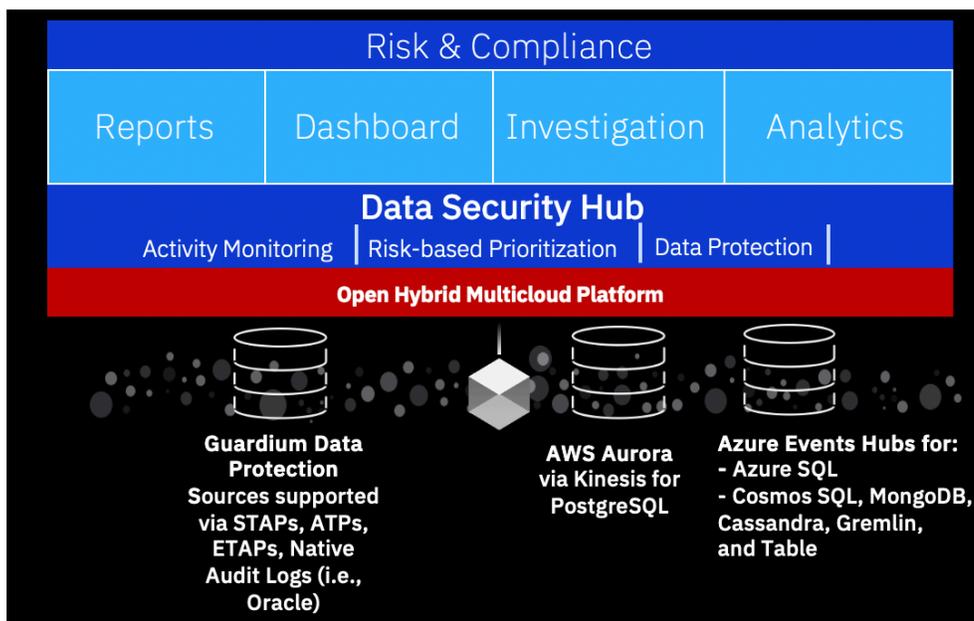
One of the challenges of traditional data security and compliance solutions is retaining and maintaining data security and audit data over long periods of time. In some cases, administrators can only store or archive data that's between 45 and 90 days old, and short data security and compliance data 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.

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

Guardium Insights for Cloud Pak for Security can ingest data security and audit data from Database-as-a-services (DBaaS) sources such as AWS Aurora via Kinesis streams for PostgreSQL and Azure Event



Hubs (and all the databases natively supported on Event Hubs, such as Azure SQL, Cosmos SQL, Cosmos MongoDB, Cosmos Cassandra, Cosmos Gremlin, Cosmos Table), 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 audit data directly to Guardium Insights without needing an agent. The Guardium Data Protection collectors send data security and audit data to Guardium Insights. All of this data is gathered into the Guardium Insights repository, which is powered by the market-leading IBM Db2 Warehouse, which is provided as a fully integrated part of the Guardium Insights solution.



Collect, analyze and act on years of data security and audit data in the Guardium Insights for Cloud Pak for Security data security hub - whether that data comes from Guardium Data Protection via collectors or is streamed directly into the hub from Cloud sources in an agentless way.

Hybrid multicloud 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. Sometimes there are multiple security functions available, but they are still only



available for that particular service. So, if an organization has cloud projects dispersed across multiple vendors or environments, they likely lack the centralized visibility needed to monitor for threats and support compliance needs 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 multicloud environments.

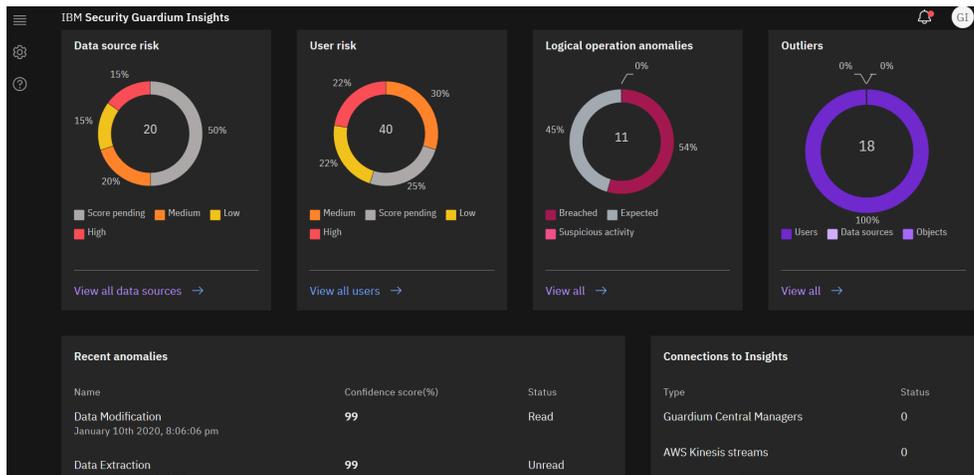
Risk-based views and alerts

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

Upon logging into Guardium Insights, data security specialists 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 also use the dashboard to quickly see and access their most frequently generated reports, as well as the status activities occurring within the Guardium Insights environment.



The Guardium Insights for Cloud Pak for Security dashboard allows data security specialists to understand their data security posture at a glance, immediately drill into the details and investigate anomalies, take action in just a few clicks, and generate reports in seconds.

Guardium Insights role-based access controls & audit trail

Guardium Insights for Cloud Pak for Security supports the separation of duties across different types of roles, to help data security teams ensure data security and audit data is secure and to provide checks and balances across different user roles. Insights provides administrators with the ability to assign and manage access controls by role. Additionally, the offering also can monitor user activities and generate reports based on activity occurring within Guardium Insights for Cloud Pak for Security.

Role-based access control

Guardium Insights for Cloud Pak for Security administrators can manage and assign access privileges to different times of users that may need access to Guardium Insights for Cloud Pak for Security. The administrator may choose from predefined roles to assign roles, as well as reading, updating and deleting users and their roles, as well as assigning roles to specific reports.

The types of pre-defined roles available include roles, and appropriate levels of access for users, such as: Administrator, Access manager, default (no access), etc. The default role is provided so that



if a user authenticates via LDAP, but the LDAP group membership has no matching role, they end up with 'default' access. A Guardium Insights for Cloud Pak for Security administrator can then change the privileges.

Audit trail

In addition to being able to monitor, understand, and create reports to show how users are accessing data in the data sources across the organization's on-premises and DBaaS environments, it's also necessary to understand how Guardium Insights for Cloud Pak for Security users are interacting with data. To this end, Guardium Insights for Cloud Pak for Security creates its own audit trail, where Guardium administrators can view events related to the modification of configuration data, user actions, privileged access, system events, and more. The administrator can then export and save or share the audit log.

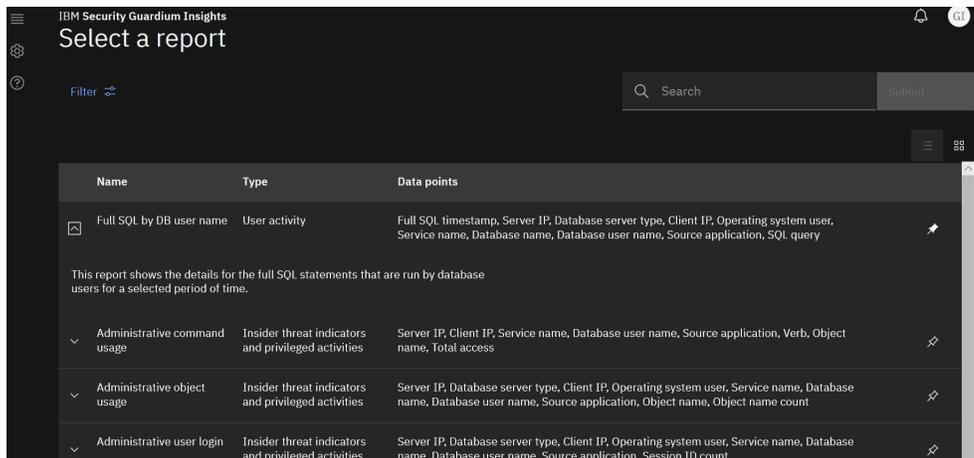
Out-of-the-box, customizable reports

To help simplify key activities for data security administrators, Guardium Insights for Cloud Pak for Security comes with many 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 specialists can understand and show key stakeholders and auditors how privileged users have been interacting with data over various time periods.

These reports also may be quickly and easily customized by copying any report, giving it a new name and description, and selecting which columns should be shown and by selecting the order of the columns, and by selecting the time range to apply to the report. When customizing reports, users can also filter using groups or scope searching, and they can save those custom filters.



Reports may be emailed to teammates and key stakeholders, or may be downloaded as a CSV. For very large numbers of reports (for example, with 10-20 million records included), users have the option to export report data in bulk. Any report – customized or pre-built - may be pinned to the overview dashboard for easier access.



Go to the Report Library for a full list of the pre-built data security and audit reports. Click the arrow for a report description or click on the pin to pin the report to the overview dashboard.

Advanced Analytics in Guardium Insights

Guardium Insights for Cloud Pak for Security 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 locate threats and anomalies within the environment. Guardium Insights analytics learn normal operational logical operations and normal data interaction patterns and 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. The results of the analytics are sent through the Guardium Insights risk-scoring engine, and are tagged with a high, medium, or low risk score based on the type of anomaly that was uncovered.

Outlier Detection Analytics



Suspicious activities such as unusual quantities of failed log ins, unexpectedly large data extraction, users accessing data at unusual times can indicate insider threat activities – whether those threats come from malicious insiders or compromised insiders. Guardium Insights for Cloud Pak for Security has outlier detection analytics that rely on machine learning and statistical modeling to learn normal behavior patterns as privileged users access and use data. Then, when outliers occur (such as credentials abuse related to databases, tables, and users or unusual levels of data extraction), the outlier detection analytics will flag these activities as anomalies, apply a high risk score, and an alert is sent to the data security team for investigation and action.

The screenshot shows the 'Anomalies' section of the IBM Security Guardium Insights dashboard. It features a search bar and a table with columns for Description, Confidence Score(%), Type, Timestamp, and Status. The table lists several anomalies, including Data Modification, Data Extraction, Suspicious Activity, and Abnormal Type of SQL Operation.

Description	Confidence Score(%)	Type	Timestamp	Status
<input type="checkbox"/> Data Modification	99	Outlier	2020-01-10 20:06:06	Read
<input type="checkbox"/> Data Extraction	99	Outlier	2020-01-10 20:06:00	Unread
<input type="checkbox"/> Suspicious Activity	92	Predictive	2020-01-10 20:02:02	Unread
<input type="checkbox"/> Suspicious Activity	92	Predictive	2020-01-10 20:02:02	Unread
<input type="checkbox"/> Suspicious Activity	92	Predictive	2020-01-10 20:02:02	Unread
<input type="checkbox"/> Suspicious Activity	92	Predictive	2020-01-10 20:02:02	Unread
<input type="checkbox"/> Abnormal Type of SQL Operation	43	Outlier	2020-01-10 14:47:21	Unread

From the Guardium Insights for Cloud Pak for Security dashboard, view the full list of anomalies uncovered by the outlier detection and predictive analytics, and then click on any anomaly to investigate.

Predictive Analytics

Guardium Insights for Cloud Pak for Security’s predictive analytics – also called sequential-based analytics – use intelligence and



algorithms to self-learn the regular logical operations that occur within an environment (such as payroll activities, banking transactions, and the sequences demonstrated by other business process patterns). Then, if the logical operation varies in any way – for example, if a step is dropped or skipped – the predictive analytics will catch the deviation upon the first anomaly (or at the first time the pattern changes). Since these types of operations do not normally vary, this type of anomaly would also be flagged with a high risk score, and an alert would also be sent to the data security team for investigation.

Take immediate action

In addition to monitoring activity from a central location, and easily spotting anomalies, data security specialists can also take immediate action to protect data from across environments. The Guardium Insights for Cloud Pak for Security dashboard, data security teams can:

- Trigger data protection policies in Guardium Data Protection to block access to connected on-premises and cloud data sources
- Directly block suspect users from accessing DBaaS sources streaming audit data to Guardium Insights
- Create tickets in incident management solutions such as ServiceNow, Inc.
- Share issues and threats with Security Analysts or other stakeholders for investigation or follow up



The screenshot displays the IBM Security Guardium Insights interface. The main heading is "Data Extraction" with a timestamp of "2019-10-08 11:00:00". Below this, a summary states: "A HIGH data extraction violation has been triggered by on , which violates the normal extraction on asset USER." To the right of the summary, three key metrics are shown: "Average" is 1, "Anomaly" is 2.7k, and "Confidence Score" is 99%. Below the summary, there are two tabs: "Details" and "Timeline". The "Details" tab is active and shows a table with the following information:

Who	Actor: DB2INST1
What	Database Name: DB2INST1
When	Timestamp: 2020-01-10 20:06:00

On the right side of the interface, there are several action buttons: "Share", "Create ticket", "Mark as read", "Ignore", "Create ticket", and "Block". Below these buttons, there is an "Activity" section with three entries:

- 4 May 2020 9:33:33 AM my-rhel-1-UNIGNOI Block
- 4 May 2020 9:33:57 AM my-rhel-icp-admin has IGNORED this anomaly
- 4 May 2020 9:33:33 AM my-rhel-icp-admin has marked this anomaly as READ

Investigate any anomaly and then take action. Use a link to share the anomaly with team members or key stakeholders or take action in just a few clicks – whether opening a ticket for remediation or blocking user access.

Unlock insights & provide self-service access for stakeholders

With all the data security and audit data available in Guardium Insights for Cloud Pak for Security, it's crucial that this data be shared across the business – with consuming applications such as IBM Security QRadar, Splunk or the IBM CloudPak for Security for example. Guardium Insights for Cloud Pak for Security provides open REST APIs and easy-to-use interactive Swagger documentation so that 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.

Additionally, often organizations already have tools that they already use for business intelligence and analytics and visualization. If key stakeholders prefer to tap into the Guardium Insights for Cloud Pak for Security data from existing tools that are in place to explore and visualize data from across the business, such as Kibana or Tableau, Guardium Insights for Cloud Pak for Security allows integration with these types of tools.



Guardium Insights for Cloud Pak for Security has also been globalized for Spanish, French, and German, and it provides backup and restore functionality.

Conclusion

IBM Security Guardium for Cloud Pak for Security 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.

Guardium Insights for Cloud Pak for Security shares a common hybrid multi-cloud architecture with IBM CloudPak for Security, helping 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](https://www.ibm.com/security).

© Copyright IBM Corporation 2020.

IBM, the IBM logo, and [ibm.com](https://www.ibm.com) are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at <https://www.ibm.com/legal/us/en/copytrade.shtml>, and select third party trademarks that might be referenced in this document is available at https://www.ibm.com/legal/us/en/copytrade.shtml#section_4.

This document contains information pertaining to the following IBM products which are trademarks and/or registered trademarks of IBM Corporation:



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

For more information

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