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, businesses may be under increased pressure to move their data and infrastructure to the cloud in order to achieve greater agility, responsiveness, and to cut 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 wading 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 is audit-related data that must be stored for increasingly lengthy periods of time due to new data privacy mandates. Reporting can become very slow, and in some cases, organizations can only keep

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
- Automates compliance by defining policy, streamlining the audit process, and sharing 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

30-90 days of ‘hot' data live to use for data security analytics. This is quite limiting when trying to identify threats that may have emerged over months or years. As a result, data security administrators often attempt to speed up the performance of data security platforms by adding additional hardware and processing power -this quickly becomes a constant, resource-intensive cycle as teams race to keep up with expanding volumes of data security and compliance data.

IBM Security Guardium Insights for IBM Cloud Pak for Security is a data security hub designed to help clients improve visibility into user data activity and behavioral 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, more easily automate and orchestrate security activities, and enable clients to deploy on-premises or in public or private clouds.

Guardium Insights can help users:

- Centralize data security visibility to discover data security and compliance insights across the hybrid multicloud
- Streamline audit and compliance by defining compliance policy to dictate how and what data is monitored and specifying audit milestones
- Produce data security and compliance reports in seconds, using out-of-the box and advanced, customizable reports and content
- Apply near real-time data activity monitoring and protection capabilities, agentlessly stream from Database-as-a-Service (DBaaS) sources, such as AWS Kinesis and Azure Event Hubs, and connect to data sources supported by IBM Security Guardium Data Protection central managers
- Uncover risk and threat patterns and take immediate action by leveraging advanced analytics
- Prioritize data security and compliance activities based on automated risk-based scoring and alerting
- Modernize data security infrastructure with a microservices-based, containerized solution

- Collaborate across the security operations center (SOC) by sharing data security event data with other security platforms and opening cases in IBM Cloud Pak for Security
- Quickly integrate with other critical IT and Security tools, such as Splunk and ServiceNow, to send enriched, contextual data security insights across teams

Guardium Insights for IBM Cloud Pak for Security can either work together with IBM Security Guardium Data Protection or on its own through agentless streaming directly from DBaaS sources to help customers streamline data security and compliance infrastructure and processes. This allows them to focus on increasing agility and improving response to threats and business requirements, all while supporting compliance needs.

Key Features:

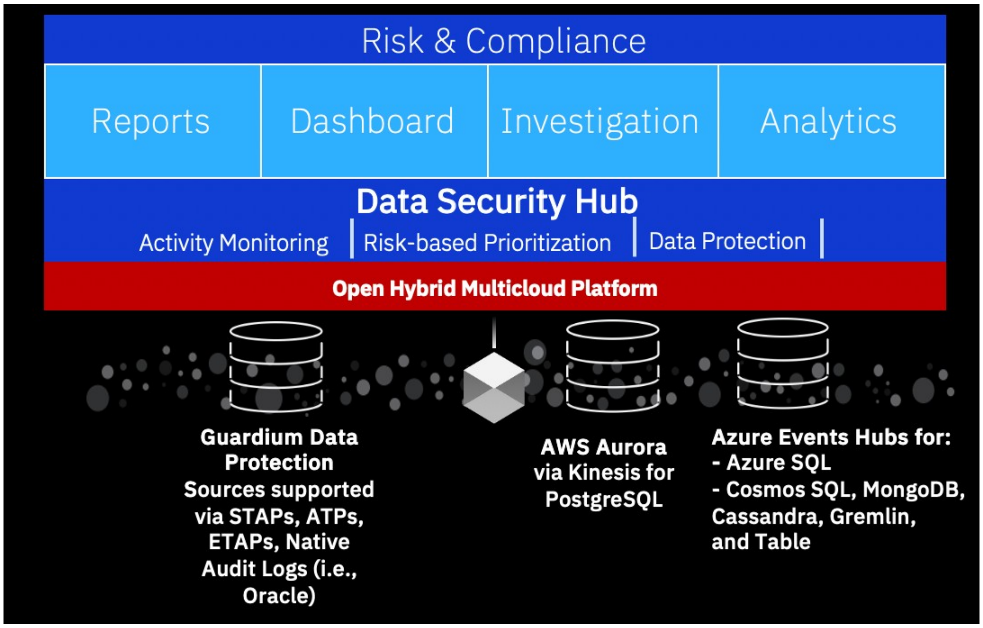
To help deliver on the vision of a modernized hybrid cloud data security hub, IBM Security Guardium Insights provides advanced data risk visualization, protection, and remediation capabilities, many of which are described below.

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 IBM 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 IBM 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 IBM 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.


Risk & Compliance
Reports
Dashboard
Investigation
Analytics
Data Security Hub
Activity Monitoring
Risk-based Prioritization
Data Protection
Open Hybrid Multicloud Platform
Guardium Data Protection
Sources supported via STAPs, ATPs, ETAPs, Native Audit Logs (i.e., Oracle)
AWS Aurora via Kinesis for PostgreSQL
Azure Events Hubs for:
- Azure SQL
- Cosmos SQL, MongoDB, Cassandra, Gremlin, and Table

Collect, analyze and act on years of data security and audit data in the Guardium Insights for IBM 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.

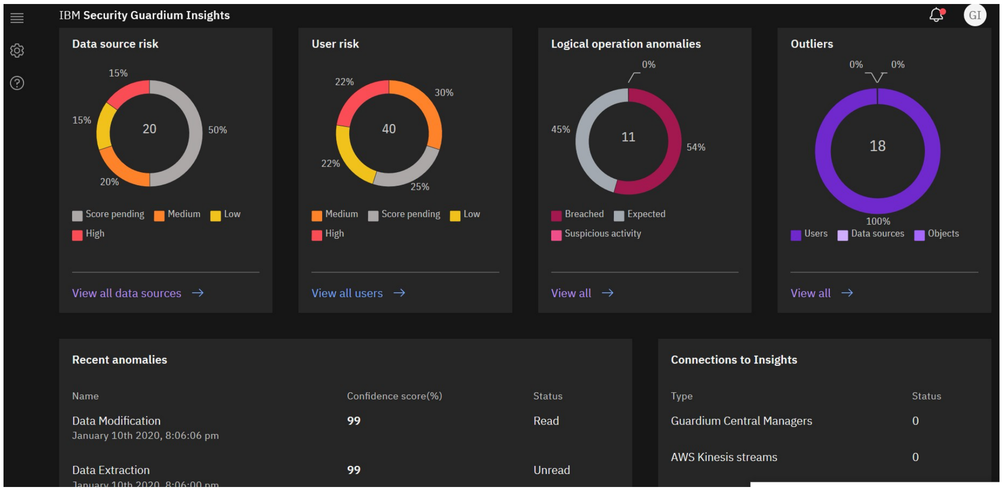
Risk-based views and alerts

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

Upon logging into Guardium Insights, administrators are immediately presented with a dashboard of information they need to understand the greatest risks currently in their environment, such as which data sources may be at risk, the potential number of risky users, and a list of risk-based alerts based on contextual analytics.

From this dashboard, users can click through for more details about risks and issues to determine root cause.

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.



Recent anomalies

Name	Confidence score(%)	Status
Data Modification January 10th 2020, 8:06:06 pm	99	Read
Data Extraction January 10th 2020, 8:06:00 pm	99	Unread

Connections to Insights

Type	Status
Guardium Central Managers	0
AWS Kinesis streams	0

The Guardium Insights for IBM Cloud Pak for Security dashboard allows data security specialiststo 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 IBM 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 can monitor user activities and generate reports based on that activity.

Role-based access control

Guardium Insights for IBM Cloud Pak for Security administrators can manage and assign access privileges to different times of users that may need access to Guardium Insights for IBM Cloud Pak for Security. Theadministrator 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 predefined roles available include roles, and appropriate levels of access for users, such as: Administrator, Accessmanager, default (no access), etc. The default role is provided so thatif a user authenticates via LDAP, but the LDAP group membership hasno matching role, they end up with 'default' access. A Guardium Insights for IBM 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 IBM Cloud Pak for Security users are interacting with data. To this end, Guardium Insights for IBM Cloud Pak for Security creates its own audit trail, where Guardium administrators can view events related to the modificationof configuration data, user actions, privileged access, system events,and more. The administrator can then export and save or share the audit log.

Compliance policy creation and audit process definition

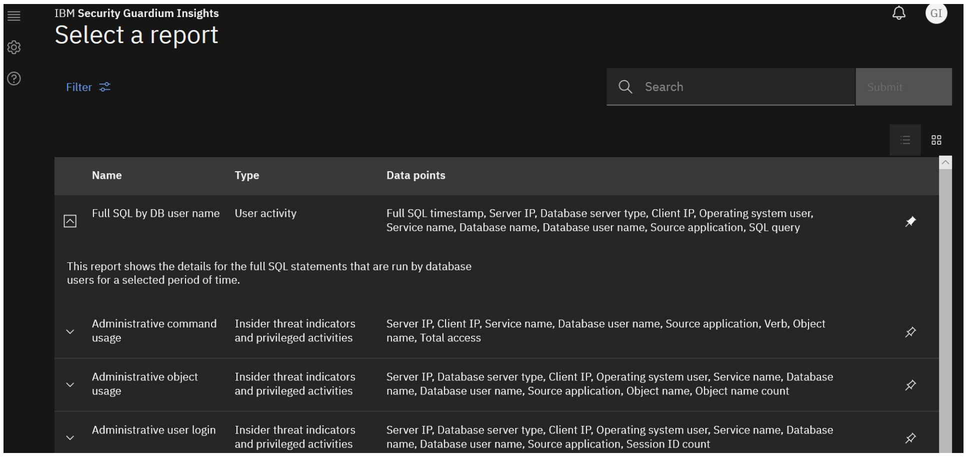
To help meet data compliance goals, Guardium Insights for IBM Cloud Pak for Security provides out-of-the-box templates for compliance policy, as well as the option to create custom policy from scratch. This allows administrators to define what and how data is monitored to meet the specific monitoring and compliance needs of their organization. Additionally, administrators 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 for IBM Cloud Pak for Security comes with many prebuilt 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 may also 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. Additionally, beyond customizing prebuilt templates, administrators may be custom reports from scratch with Guardium Insights' advanced reporting capabilities. When customizing or building custom reports, users can filter using groups or scope searching, and they can save those custom filters.

Reports may be emailed to teammates and key stakeholders, or may they 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 – custom or prebuilt – may be pinned to the overview dashboard for easier access. Delivery and distribution of reports may also be scheduled through the Guardium Insights Schedule Reports capability.



Name	Type	Data points
Full SQL by DB user name	User activity	Full SQL timestamp, Server IP, Database server type, Client IP, Operating system user, Service name, Database name, Database user name, Source application, SQL query

This report shows the details for the full SQL statements that are run by database users for a selected period of time.

Name	Type	Data points
Administrative command usage	Insider threat indicators and privileged activities	Server IP, Client IP, Service name, Database user name, Source application, Verb, Object name, Total access
Administrative object usage	Insider threat indicators and privileged activities	Server IP, Database server type, Client IP, Operating system user, Service name, Database name, Database user name, Source application, Object name, Object name count
Administrative user login	Insider threat indicators and privileged activities	Server IP, Database server type, Client IP, Operating system user, Service name, Database name, Database user name, Source application, Session ID count

Go to the Report Library for a full list of the prebuilt 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.

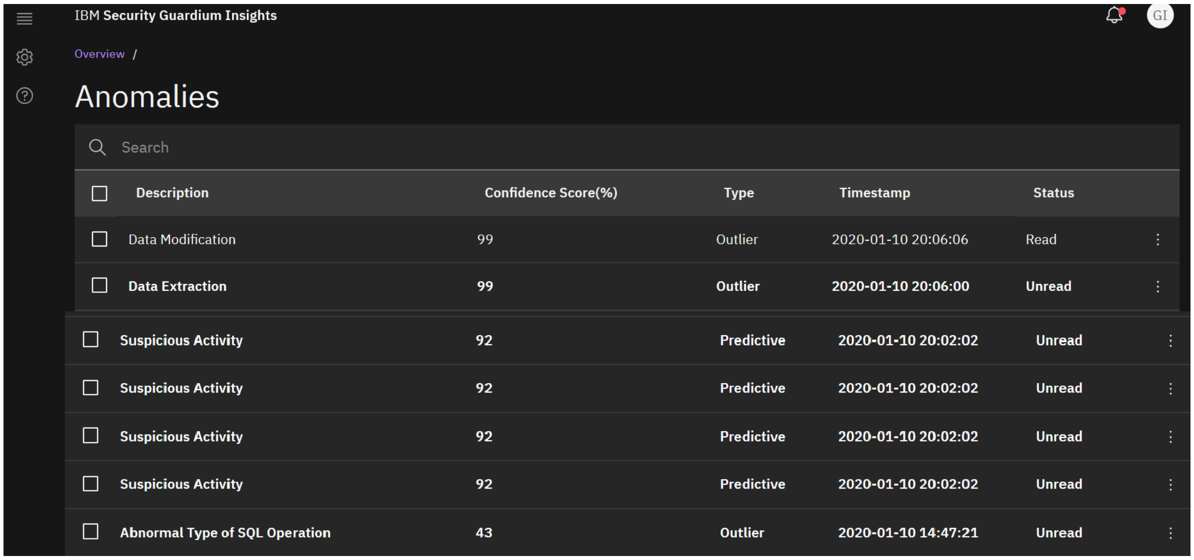
Advanced Analytics in Guardium Insights

Guardium Insights for IBM Cloud Pak for Security uses proprietary advanced analytics to help data security teams uncover areas of risk, emerging threat patterns, and potential application hijacks. Predictive analytics and outlier detection help users locate threats and anomalies within the environment. The analytics engine within Guardium Insights learns normal operations and normal data interaction patterns for a given organization and helps to identify suspicious behavior, 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 though 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, and users accessing data at unusual times can indicate insider threat activities – whether those threats come from malicious or compromised insiders. Guardium Insights for IBM Cloud Pak for Security has outlier detection analytics that rely on machine learning and statistical modeling to learn normal behavior patterns as users access and use data—integration with IBM Security Verify Privilege for privileged access management (PAM), allows Guardium Insights to even identify the risky users behind privileged credentials.

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, determine a risk score, and send an alert to the data security team for investigation and action.



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

From the IBM Guardium Insights for IBM 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.

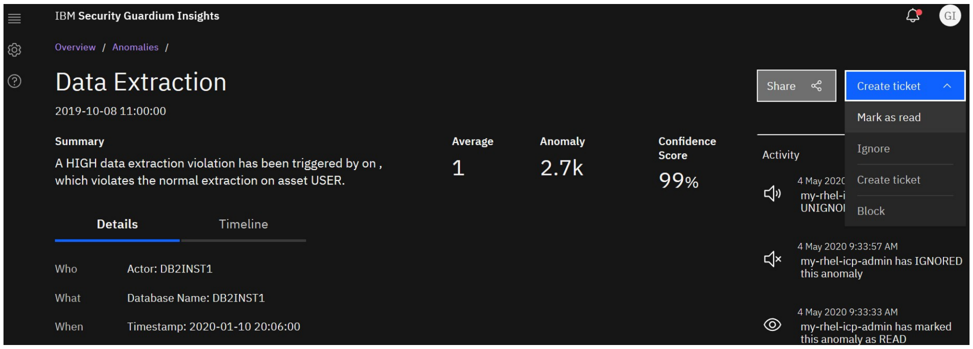
Sequential (Predictive) Analytics

Guardium Insights for IBM Cloud Pak for Security's predictive analytics – also called sequential-based analytics – use artificial intelligence andalgorithms 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. Through the Guardium Insights for IBM 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.
- Create and map tickets and cases in Guardium Insights to the corresponding Cases application in IBM Cloud Pak for Security— 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



Data Extraction

2019-10-08 11:00:00

Summary
A HIGH data extraction violation has been triggered by on , which violates the normal extraction on asset USER.

Average	Anomaly	Confidence Score
1	2.7k	99%

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

Activity

4 May 2020
my-rhel-i
UNIGNOI

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 IBM 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 IBM Cloud Pak for Security for example. Guardium Insights for IBM Cloud Pak for Security provides openREST 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, organizations often have tools that they already use for business intelligence, analytics, and visualization. If key stakeholders prefer to tap into the Guardium Insights for IBM Cloud Pak for Security data from existing tools to explore and visualize data from across the business – tools such as Kibana or Tableau – Guardium Insights for IBM Cloud Pak for Security allows integration with these typesof platforms.

Guardium Insights for IBM 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 IBM 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 IBM Cloud Pak for Security shares a common hybridmulti-cloud architecture with IBM Cloud Pak 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.

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/products/guardium-insights