Advance to the next level of data security and compliance

Leveraging the power of a big-data platform—purpose-built for data security

Highlights

- Store and access years of compliance, risk and security data via a security data lake
- Meet expanding compliance requirements while optimizing performance and visibility
- Establish context-aware insights by easily linking relevant data sets
- Reduce costs by streamlining operational efforts and reducing infrastructure requirements
- Unleash the power of data security and compliance insights with self-service, interactive access for multiple stakeholders

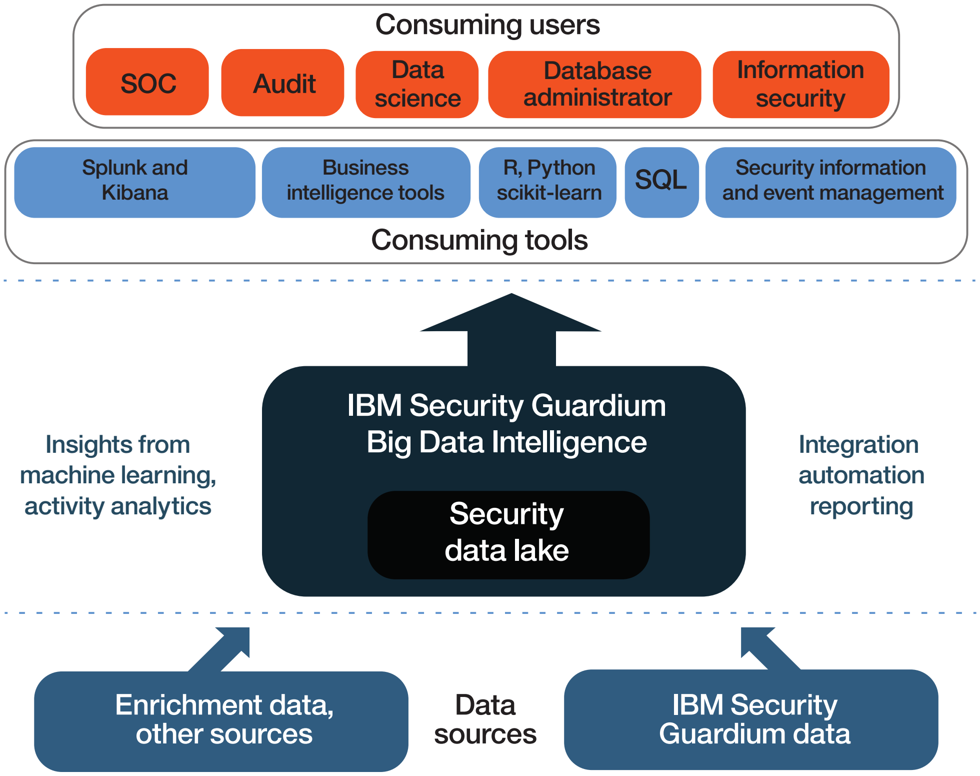
As data volumes continue to expand across databases, file systems, cloud environments and big-data platforms, and as compliance retention requirements lengthen (now up to five years for some regulations), there is increasing stress on IT organizations to address significant data management and storage requirements for data security solutions. As a result, the capacity and processing power needed to support today's data security objectives has risen dramatically—and it will only continue to rise.

At the same time, there is organizational pressure to obtain more sophisticated security and compliance insights faster, supported by prebuilt, high-performance reporting capabilities and interactive data exploration tools. Further, data security and compliance efforts—and the associated collection, storage and management of that data—must apply across the entire technology landscape, and that landscape is ever-changing and growing.

Organizations using IBM® Security Guardium® today already benefit from the ability to automatically discover and classify sensitive data; discover data source vulnerabilities and track remediation progress; monitor data access across different file systems and data sources (such as databases, mainframes, Hadoop and NoSQL environments); perform advanced analytics and gain insights from machine learning to reveal internal and external risks and threats; protect sensitive data with data encryption capabilities and dynamic data masking; and support real-time alerting, blocking and quarantining. However, data volumes—and the associated data management and storage pressures—have created the need for additional agility, support for longer retention timeframes, and the delivery of context-aware analytics. This is where IBM Security Guardium Big Data Intelligence comes into play.

Guardium Big Data Intelligence is beneficial for organizations with various sized deployments, and is especially helpful for organizations in highly regulated industries that require longer data retention periods. The solution allows organizations to give authorized users direct, real-time access to data security and compliance reports and insights, providing the Guardium administrator with the freedom to focus more on improving the organization's data security and compliance posture, and to focus less on data management and operational issues.

With Guardium Big Data Intelligence, organizations are able to enhance their Guardium deployments to achieve additional *agility* for operations and data security, cost-efficiently *retain* more data over longer time horizons, and achieve new *insights* into existing data security and compliance data.


Consuming users
SOC
Audit
Data science
Database administrator
Information security
Splunk and Kibana
Business intelligence tools
R, Python scikit-learn
SQL
Security information and event management
Consuming tools
IBM Security Guardium Big Data Intelligence
Security data lake
Insights from machine learning, activity analytics
Integration automation reporting
Enrichment data, other sources
Data sources
IBM Security Guardium data

Guardium Big Data Intelligence helps enrich data security and compliance data, reveals new insights, and provides secure self-service access and reporting for multiple teams, freeing data security and compliance insights while streamlining their management.

Agility

Improve time to value and flexibility while reducing costs

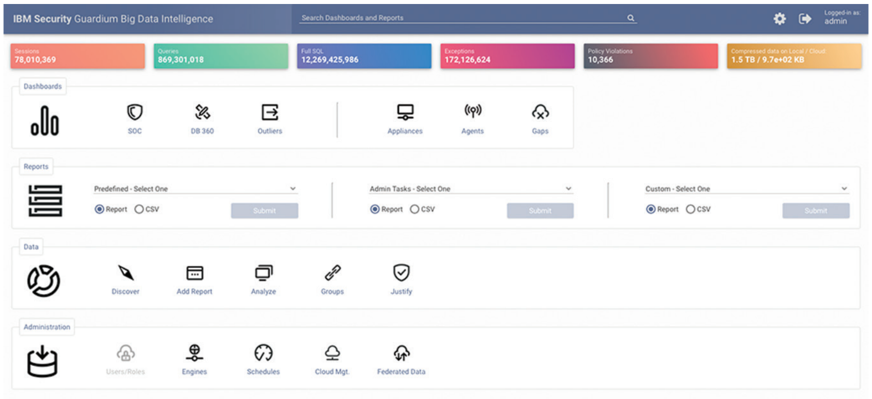
Guardium Big Data Intelligence is a security data lake that can optimize your data security architecture and streamline data collection and management processes. Because Guardium collectors are able to push data directly into the purpose-built security data lake, organizations no longer need to store large quantities of data in Guardium. This reduces stress on the system and improves processing performance and throughput. Using Guardium Big Data Intelligence and Guardium together, users can still leverage the Guardium Central Manager to manage all the Guardium collectors that feed data into the Guardium Big Data Intelligence environment, while also streamlining their collection and interaction with the highly valuable data collected by Guardium.

In this more flexible architecture, data updates are frequent. Most data is collected by Guardium Big Data Intelligence every hour; key diagnostics such as Guardium S-TAP® status and system health indicators are collected every five minutes for reliable database and file traffic monitoring. Less time-critical information is collected every 24 hours. Database administrators (DBAs) can also leverage powerful automation capabilities, such as an event-level workflow engine, enabling them to act on individual events that occur around or within their data. This process automation brings value to data consumers as well as managers, by routing important data to the appropriate personnel without requiring manual administrator intervention and reducing the time it takes to receive information. Guardium Big Data Intelligence helps you optimize your data security architecture and workflows—putting all the data you need at your fingertips—while:

- Delivering smart action- and results-oriented data security and audit workflows
- Exploiting integrated analytical services to transform massive volumes of raw activity data into actionable insights

By storing Guardium security, risk and compliance information in a security data lake, clients can also significantly reduce current data storage costs and avoid the otherwise prohibitive costs associated with meeting multi-year retention requirements. The streamlined architecture also frees Guardium to more efficiently execute data collection across broader policies, vulnerability assessment, data protection, and risk and threat detection analytics tasks.

> *One Guardium Big Data Intelligence customer reported that they were able to retrieve a report derived from 16 billion records in five seconds, down from approximately two days.*[1]



Sessions 78,010,369

Queries 869,301,018

Full SQL 12,269,425,986

Exceptions 172,126,624

Policy Violations 10,366

Compressed data on Local / Cloud: 1.5 TB / 9.7e+02 KB

Logged-in as: admin

Guardium Big Data Intelligence includes a range of built-in dashboards, reports, data views and administration tools to share new data security and compliance insights. Users can also add customized dashboards and reports as needed.

Enrich data—and set it free

Storing data security and compliance data in a highly flexible and dynamic security data lake allows that data to be enhanced with related data from other business processes and applications. For example, auditors are increasingly asking for the reconciliation of privileged account management solutions such as CyberArk with the actual activity data captured by Guardium. This is easily accomplished with Guardium Big Data Intelligence. These data integration capabilities allow the analytics to become more context-aware, and can therefore reveal new compliance and data security insights.

Additionally, new data and insights stored in Guardium Big Data Intelligence can be directly shared with authorized users and with other security and analytics applications such as IBM QRadar® SIEM, Splunk, and other applications. Guardium Big Data Intelligence is compatible with hundreds of commercial tools, from business intelligence solutions such as Tableau, Qlik and IBM Cognos®, to Microsoft Excel, SQL and other tools that meet data consumers' preferred access methods. As secure, self-service access and reporting are made available to auditors, security analysts and other teams able to leverage valuable Guardium data, Guardium administrators are free to focus on introducing more sophisticated strategies for enhancing data security, protection and compliance.

Use powerful, embedded analytical tools

Guardium Big Data Intelligence quickly makes sense of large volumes of context-aware historical views and provides near-real-time access to event data to apply big-data analytics and machine learning for richer compliance and data security insights. Users can better understand and highlight new areas of risk, discover new access and threat patterns, and quickly present more comprehensive and consumable reports to management. Embedded analytical services can help solve a variety of database security-specific challenges, resolve operational issues and more effectively manage your database environment.

Simplify deployment

And, unlike other big-data offerings, which require expensive development and ongoing maintenance, Guardium Big Data Intelligence may be deployed in days, preconfigured with the Guardium-compatible policies you need right out of the box.

Guardium Big Data Intelligence can help you reduce your infrastructure and offering costs by more than 25 percent[1] *and reduce your storage requirements by more than 80 percent.*[1]

Retention

Comply with mandates to keep data for the long term

Increasing data volumes, and the increasing costs to store them within data-security platforms, have created new pressures and stresses in the data security and compliance landscape. This is because data-security platforms are designed to support data security, protection and compliance requirements, but aren't necessarily designed as big-data lakes.

Every client struggles with a need to retain increasing amounts of data to efficiently (and effectively) tackle data security and compliance. Today, data-security professionals constantly struggle to keep up with data volumes and lifecycles, capturing more data and retaining it for longer time periods. In most cases, these longer data retention requirements are being driven and specified by regulatory requirements.

Guardium Big Data Intelligence is a NoSQL big-data analytics platform that is designed to act as a big-data lake for data security, cost-effectively storing massive quantities of data, while making the data stored in the big-data lake directly and easily accessible.

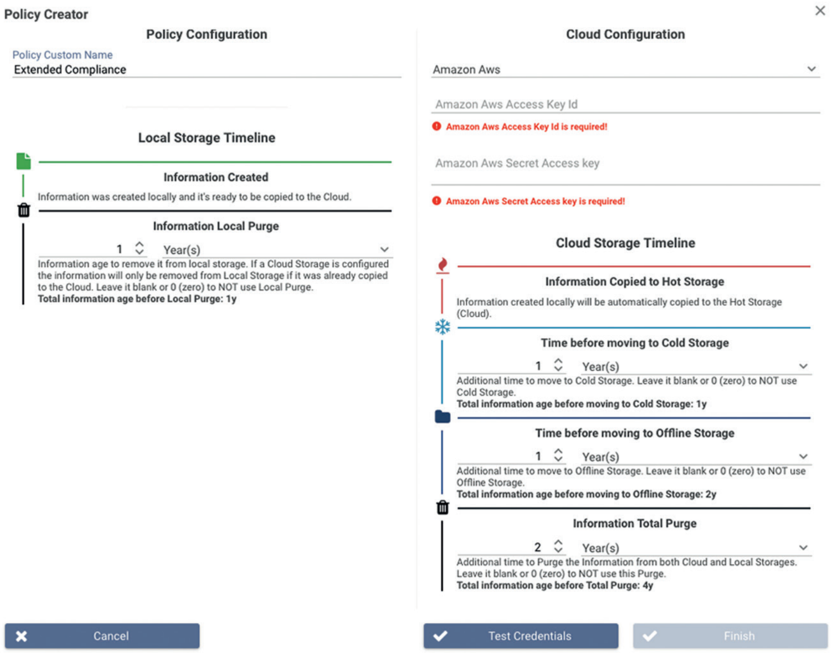
Guardium Big Data Intelligence and its architecture make it easier to meet new or expanding regulatory requirements by enabling users to retain more data over longer time periods—even years—without hindering performance.

Some clients facing challenges around big-data security and compliance volumes try the "archiving" approach, moving data into a temporary storage facility. This approach, however, is not viable, since archived data sets are encrypted and compressed, rendering them inaccessible—thus defeating the purpose of retaining them for compliance purposes. Because it is based on a NoSQL architecture, Guardium Big Data Intelligence can do this without requiring any data archiving.

The Guardium Big Data Intelligence data store is a compressed-columnar system specifically optimized for large-scale data queries that span years and terabytes of data. As a result, the performance for a query focusing on data that is a year old is roughly the same as the performance for a query focusing on data that is a week old, enabling teams to not only store more data more efficiently and longer, but also to access and use it with ease.

And, because Guardium Big Data Intelligence provides online, real-time access to years' worth of data, the solution can help you dramatically reduce false positive rates associated with identifying potential outliers, based on a much richer historical perspective.

Guardium Big Data Intelligence can help shrink collector storage requirements from 600 GB to 100 GB.[1]



Policy Creator

Policy Configuration

Policy Custom Name
Extended Compliance

Local Storage Timeline

Information Created

Information was created locally and it's ready to be copied to the Cloud.

Information Local Purge

1 Year(s)

Information age to remove it from local storage. If a Cloud Storage is configured the information will only be removed from Local Storage if it was already copied to the Cloud. Leave it blank or 0 (zero) to NOT use Local Purge.
Total information age before Local Purge: 1y

Cloud Configuration

Amazon Aws

Amazon Aws Access Key Id
Amazon Aws Access Key Id is required!

Amazon Aws Secret Access key
Amazon Aws Secret Access key is required!

Cloud Storage Timeline

Information Copied to Hot Storage

Information created locally will be automatically copied to the Hot Storage (Cloud).

Time before moving to Cold Storage

1 Year(s)

Additional time to move to Cold Storage. Leave it blank or 0 (zero) to NOT use Cold Storage.
Total information age before moving to Cold Storage: 1y

Time before moving to Offline Storage

1 Year(s)

Additional time to move to Offline Storage. Leave it blank or 0 (zero) to NOT use Offline Storage.
Total information age before moving to Offline Storage: 2y

Information Total Purge

2 Year(s)

Additional time to Purge the Information from both Cloud and Local Storages. Leave it blank or 0 (zero) to NOT use this Purge.
Total information age before Total Purge: 4y

Guardium Big Data Intelligence delivers interactive data exploration capabilities to quickly and easily visualize data and uncover new insights.

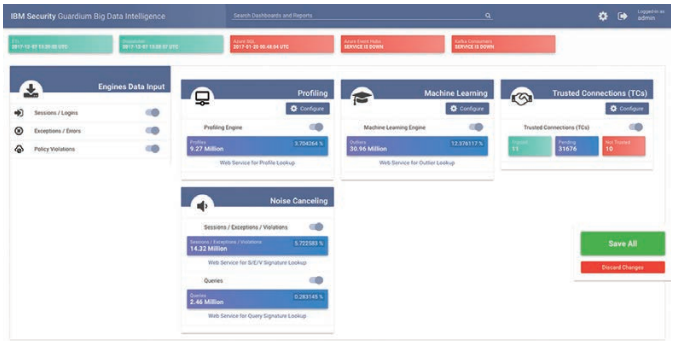
Insights

Use analytics to achieve context-aware intelligence

Guardium Big Data Intelligence is able to apply analytics and machine-learning capabilities to all the data in the newly-formed data lake to create richer insights and actionable information. It can reveal new insights derived by analyzing the data over longer time periods and performing analytics on context-aware data. Guardium Big Data Intelligence analytics can provide:

- *Noise cancelation and deduplication forensics* can sift through vast volumes of raw data to present, in a single prebuilt report, specific errors, such as failed logins and SQL errors, organized by frequency of occurrence instead of massive volumes of discrete error messages.

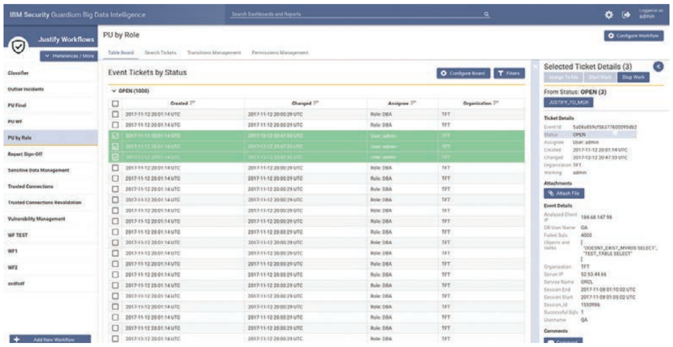
- *Data security and compliance-specific* user activity analytics apply machine learning to determine normal user activity and then persistently evaluate this activity to identify anomalies and risks. You can analyze the activity of different users on the same data source (such as a database, file system or big-data environment) to detect anomalies. Anomalies can include unusual activity patterns within a user category, such as DBAs, or activities over time in a user's history. This information is not only useful for protecting sensitive data, but also for sharing with your SIEM solution, in support of enterprise-level activity analytics initiatives.
- *Trusted connection profiling* is a key data security control that enables you to automatically identify, manage and isolate "normal" data interactions from unusual connections (i.e. lower-volume, non-application accounts) that may be exploited for unwanted behavior. By constantly evaluating who is accessing which databases, file systems, and other data sources—and what access methods, routes and tools they are using—you can significantly enhance your ability to identify unusual connections. Successfully executing a trusted connection profiling program requires significant resources because the system must constantly monitor and assess all data access connections, review them with the appropriate data and application owners and implement Guardium configuration changes as the connections are approved. Guardium Big Data Intelligence provides a complete solution for automating otherwise-cumbersome manual processes to achieve a highly efficient and effective trusted connections profiling program. With the ability to more easily recognize unusual connections, Guardium Big Data Intelligence can help strengthen your data security coverage. Furthermore, this capability brings the added benefit of increasing the effective throughput of your Guardium environment, by focusing a fine-grained monitoring lens on unusual connections versus known trusted connections.


IBM Security Guardium Big Data Intelligence
Search Dashboards and Reports
Logged in as admin
Azure SQL 2017-01-20 00:48:04 UTC
Azure Event Hubs SERVICE IS DOWN
Kafka Consumers SERVICE IS DOWN
Engines Data Input
Sessions / Logins
Exceptions / Errors
Policy Violations
Profiling
Configure
Profiling Engine
Profiles 9.27 Million 3.704264 %
Web Service for Profile Lookup
Machine Learning
Configure
Machine Learning Engine
Outliers 30.96 Million 12.376117 %
Web Service for Outlier Lookup
Trusted Connections (TCs)
Configure
Trusted Connections (TCs)
Trusted 11
Pending 31676
Not Trusted 10
Noise Canceling
Sessions / Exceptions / Violations
Sessions / Exceptions / Violations 14.32 Million 5.722583 %
Web Service for S/E/V Signature Lookup
Queries
Queries 2.46 Million 0.283145 %
Web Service for Query Signature Lookup
Save All
Discard Changes

Trusted connections profiling enables you to save time by automatically, identifying, managing and isolating "normal" data interactions from lower-volume non-application accounts that are often exploited.

- *Privileged access reconciliation* helps improve data governance by enabling Guardium Big Data Intelligence to integrate with key privilege information from external data sources, such as Cyberark, Total Privileged Access Management (TPAM), and IBM Security Privileged Identity Manager, to tighten controls and increase visibility into who is accessing sensitive data. By linking these key data sets together, critical information regarding privileged account provisioning and the actual activity associated with the privileged account can be automatically reconciled and help significantly improve data governance while also reducing the level of effort needed to achieve this reconciliation.
- *DB360* enables organizations to consolidate key data perspectives from specific data security sources (such as data discovery, classification, vulnerability assessment and entitlement reporting) to create a unified view of the data security profile for any given database (or other data source). Using DB360, you can isolate any data source and, at a glance, understand the results of the latest vulnerability assessment or classification scan, see if an S-TAP was successfully installed and is actively performing monitoring, see data or file activity monitoring exceptions, and more.

- *Data Explorer* allows users to easily and interactively explore data security and compliance details, operational information and other essential data to get instant visibility into any security and compliance-related data contained within the security data lake. Data Explorer is built on Kibana, an open-source analytics and visualization tool that allows users to rapidly drill down into vast volumes of data. Data Explorer helps users search for and find any data they want in seconds.[2] For example, users can view all failed logins, as well as all profiles by user, application or specified time period, all of which are displayed in a user-friendly graphical interface and available for dashboards and other visualizations.
- *A fully customizable security operations center (SOC) dashboard* displays data on vulnerability assessments, policy violations, errors and other valuable metrics, providing easy visualization of security-relevant events that are directly embedded into a SOC environment.



PU by Role

Event Tickets by Status

OPEN (1000)

□	Created	Changed	Assignee	Organization
□	2017-11-12 20:01:14 UTC	2017-11-12 20:00:29 UTC	Role: DBA	TFT
□	2017-11-12 20:01:14 UTC	2017-11-12 20:00:29 UTC	Role: DBA	TFT
☑	2017-11-12 20:01:14 UTC	2017-12-12 20:47:33 UTC	User: admin	TFT
☑	2017-11-12 20:01:14 UTC	2017-12-12 20:47:33 UTC	User: admin	TFT
☑	2017-11-12 20:01:14 UTC	2017-12-12 20:47:33 UTC	User: admin	TFT
□	2017-11-12 20:01:14 UTC	2017-11-12 20:00:29 UTC	Role: DBA	TFT
□	2017-11-12 20:01:14 UTC	2017-11-12 20:00:29 UTC	Role: DBA	TFT
□	2017-11-12 20:01:14 UTC	2017-11-12 20:00:29 UTC	Role: DBA	TFT
□	2017-11-12 20:01:14 UTC	2017-11-12 20:00:29 UTC	Role: DBA	TFT
□	2017-11-12 20:01:14 UTC	2017-11-12 20:00:29 UTC	Role: DBA	TFT
□	2017-11-12 20:01:14 UTC	2017-11-12 20:00:29 UTC	Role: DBA	TFT
□	2017-11-12 20:01:14 UTC	2017-11-12 20:00:29 UTC	Role: DBA	TFT
□	2017-11-12 20:01:14 UTC	2017-11-12 20:00:29 UTC	Role: DBA	TFT
□	2017-11-12 20:01:14 UTC	2017-11-12 20:00:29 UTC	Role: DBA	TFT
□	2017-11-12 20:01:14 UTC	2017-11-12 20:00:29 UTC	Role: DBA	TFT
□	2017-11-12 20:01:14 UTC	2017-11-12 20:00:29 UTC	Role: DBA	TFT
□	2017-11-12 20:01:14 UTC	2017-11-12 20:00:29 UTC	Role: DBA	TFT
□	2017-11-12 20:01:14 UTC	2017-11-12 20:00:29 UTC	Role: DBA	TFT
□	2017-11-12 20:01:14 UTC	2017-11-12 20:00:29 UTC	Role: DBA	TFT
□	2017-11-12 20:01:14 UTC	2017-11-12 20:00:29 UTC	Role: DBA	TFT
□	2017-11-12 20:01:14 UTC	2017-11-12 20:00:29 UTC	Role: DBA	TFT
□	2017-11-12 20:01:14 UTC	2017-11-12 20:00:29 UTC	Role: DBA	TFT

Selected Ticket Details (3)

From Status: **OPEN (3)**

Ticket Details

Event Id	5a08a859cf5b377600095db2
Status	OPEN
Assignee	User: admin
Created	2017-11-12 20:01:14 UTC
Changed	2017-12-12 20:47:33 UTC
Organization	TFT
Working	admin

Attachments

Event Details

Analyzed Client IP	184.68.147.98
DB User Name	QA
Failed Sqls	4000
Objects and Verbs	["DOESNT_EXIST_MYROS SELECT", "TEST_TABLE SELECT"]
Organization	TFT
Server IP	52.53.44.64
Service Name	ORCL
Session End	2017-11-08 01:10:02 UTC
Session Start	2017-11-08 01:05:02 UTC
Session_Id	1550986
Successful Sqls	1
Username	QA

Comments

Workflows in Guardium Big Data Intelligence can reveal event tickets by status and enable you to drill down for detailed event insights.

Focus on the right events and insights

Guardium Big Data Intelligence includes an event-level workflow engine that provides powerful and fully customizable tools for automatically distributing the appropriate pieces of data security, risk and compliance information from Guardium directly to the appropriate stakeholders, helping to enforce associated review and escalation processes.

For example, if one report includes 10,000 different events, not everyone in an organization needs information about each event in the report. Using key metadata attached to the events, Guardium Big Data Intelligence can parse the report and send relevant pieces of information to relevant and interested application owners and key stakeholders. Individual events may be automatically distributed to the proper stakeholders as well. The solution can also provide automatic escalation, if needed, in the event of a non-response or other issue.

This level of automation—and the ability to focus on the right insights within a report, rather than having users mine an entire report—streamlines effort, saves time and cost, and empowers users be to more impactful more quickly.

Trusted connection profiling is a good example of an area in which to leverage smart workflow capabilities. The workflow engine may be used to distribute trusted connection candidates to the appropriate owners for review and approval. And, if those connections are approved, the workflow tool can automatically build integrations and changes needed to trigger Guardium configuration changes so that Guardium understands that the newly approved connections are trusted connections. Without these workflow capabilities, a great deal of manual labor and sleuthing would be required to find new trusted connections, have them approved, and build the right integrations to add them.

Guardium features	Guardium Big Data Intelligence features
Data and file-activity monitoring across databases, Hadoop distributions, NoSQL platforms, big-data platforms, cloud deployments, file systems and more	The ability to streamline data collection and management to gather, manage and store massive data volumes while keeping infrastructure and operational costs low
Data encryption and key management	Data security, compliance and operational reporting in near-real time without impeding performance
Discovery and classification of sensitive data	Data storage over longer timeframes to support compliance requirements
Discovery of data source vulnerabilities and tracking of remediation progress over time	Interactive and self-service data accessibility that empowers a variety of authorized users to better leverage high-value data security/privacy information for expanded use cases
Advanced analytics that support dynamic data protection, including near-real-time alerting, blocking and quarantining	Built-in features to perform big-data analytics on historical, context-aware and refined data
Delivery of automated data compliance and audit capabilities for data at rest and data in motion	Seamless integration with a variety of adjacent tools, including QRadar SIEM, Cyberark, a configuration management database (CMBD), Splunk and others
Scanning and analysis of audited data to detect symptoms of a database attack from inside or outside	Trusted connections profiling, a fully embedded Kibana data explorer, traffic analyzers and other analytical engines for isolating and examining data security and privacy concerns

Why IBM?

Guardium provides powerful data security and analysis and opportunities for data insights. With Guardium Big Data Intelligence, you can easily enrich your Guardium deployment and provide greater agility, simplified installation—often in as little as two hours—longer data retention and an enhanced breadth of data insights. Fast reporting, direct access to multiple stakeholders, and support for both security and compliance initiatives make Guardium Big Data Intelligence, working hand in hand with Guardium, a robust solution for protecting, managing and optimizing your stored data.

For more information

To learn more about Guardium Big Data Intelligence, please contact your IBM representative or IBM Business Partner, or visit: **ibm.com**/us-en/marketplace/guardium-big-data-intelligence

To learn more about Guardium, please contact your IBM representative or IBM Business Partner, or visit: **ibm.com**/guardium

About IBM Security solutions

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 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, monitors more than one trillion security events per month in more than 130 countries, and holds more than 3,000 security patents.

Additionally, IBM Global Financing provides numerous payment options to help you acquire the technology you need to grow your business. We provide full lifecycle management of IT products and services, from acquisition to disposition. For more information, visit: **ibm.com**/financing

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

Actual available storage capacity may be reported for both uncompressed and compressed data and will vary and may be less than stated.

IBM Security
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
January 2018

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions.

All client examples cited or described are presented as illustrations of the manner in which some clients have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual client configurations and conditions. Contact IBM to see what we can do for you.

It is the user’s responsibility to evaluate and verify the operation of any other products or programs with IBM products and programs.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation.

♻ Please Recycle

[1] Based on an IBM customer deployment.

[2] Based on IBM lab results.