

IBM Security Guardium Data Protection

Centralize visibility, automate compliance
and continuously monitor data in real time



Highlights

Reduce risk with
real-time visibility and
actionable intelligence

Address regulatory
compliance with
automated workflows

Enforce granular
access control down
to the data level

Minimize the total
cost of ownership and
performance impact

As enterprises adapt to changes in the business and technological landscapes, data sources continue to proliferate over geographical and organizational boundaries. Data stored across on-premises and cloud environments is increasing in volume, variety and velocity, making it critical for security teams to have complete visibility into the “who, what, when, where and how” of all data access.

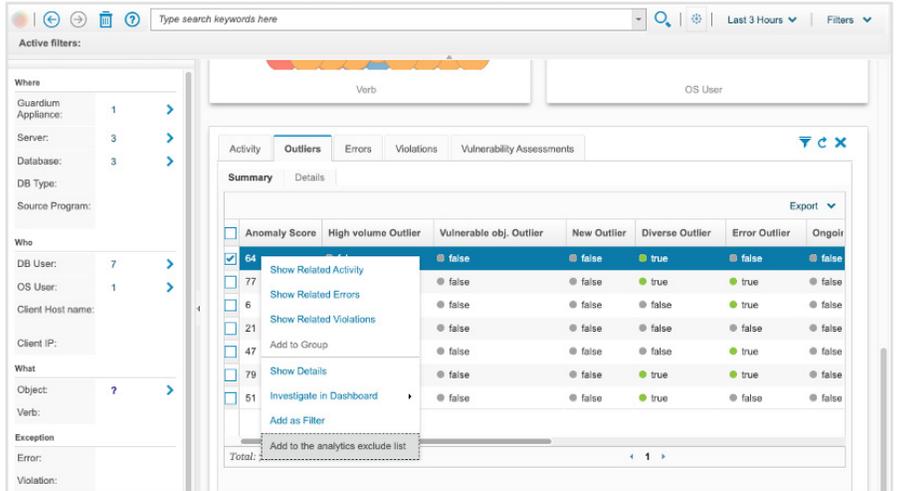
IBM Security® Guardium® Data Protection is a data security platform that empowers security teams to safeguard sensitive data through automated and continuous discovery and classification, in-depth vulnerability assessments and advanced threat detection. It extends comprehensive data protection across disparate data environments, including all of the following:

- Databases
- Data platforms
- Data warehouses
- File shares
- File systems
- Mainframes

IBM Security Guardium offers a centralized control console to help you streamline management and security of your data—both on-premises and in the cloud—to meet security and compliance requirements.

Reduce risk with real-time visibility and actionable intelligence

With IBM Security Guardium Data Protection, you can use real-time analytics and machine learning (ML) models to detect and respond to anomalies. This solution offers advanced analytical tools with a combination of rules-based policies and symptom analysis to detect patterns and behaviors that map to known industry attack vectors, thereby identifying internal and external threats. Security policies can also be configured to customize data activity monitoring to provide detailed audit trails and risky user profiles, streamlining compliance and investigation processes.

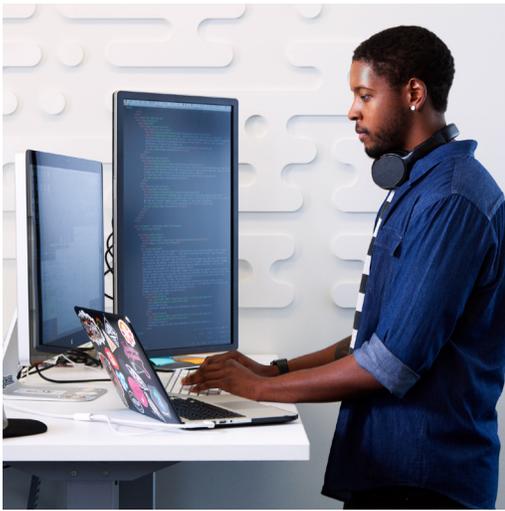


Add outliers to exclude list from Investigation Dashboard

IBM Security Guardium Data Protection evaluates risk based on severity, helping analysts remain up to date on suspicious user access or connections to data sources. The platform also identifies the presence of sensitive objects in data traffic related to monitored sources. The insights generated from these and other processes inform and enhance the following additional capabilities:

- User access profiling
- Real-time forensics search and analytics
- Outlier detection algorithms
- Detailed investigative dashboard

This platform provides an enriched understanding of risk to help security teams easily build and update data and user groups for closer monitoring and auditing; block or quarantine users or sessions for flagged suspicious activity; and remediate threats more quickly.



Address regulatory compliance with automated workflows

You can customize the predefined security and compliance templates of IBM Security Guardium Data Protection based on your specific audit and regulatory requirements. Policies can also be custom-built to detect any threat scenario related to targeted data, backed by IBM® research into the most common audit constructs and other contextual information.

To automate compliance tracking and reporting, easily create, update and tag policies and rules for specific data security and privacy regulation standards, all without doubling administrative efforts. IBM Security Guardium Data Protection also offers many quick start guides to help accelerate audit and compliance reporting timelines.

Build custom reports with drill-down capabilities using an intuitive drag-and-drop interface to further support your audit processes and regulatory compliance needs. This customizable reporting can provide granular visibility into user entitlements, dormant accounts and excessive privileges so that your organization can demonstrate proof that it has effective access governance controls in place.

Enforce granular access control down to the data level

IBM Security Guardium Data Protection empowers you to protect your data both where users, applications and services consume it and at the infrastructure level, where data is stored in databases, data warehouses, DBaaS sources and more. It does so by identifying policies and rules that are created by governance solutions like IBM Watson® Knowledge Catalog and automatically and consistently enforcing the same policies and rules in backend datastores.

IBM Security Guardium Data Protection also helps ensure that the right user or application has the right level of access to the right data under the right conditions at the right time. And intelligent automations minimize the level of skill needed for oversight, providing better, more comprehensive security and protection of data throughout the enterprise.

Minimize the total cost of ownership and performance impact

IBM Security Guardium Data Protection is built to scale seamlessly from one data source to tens of thousands with little to no impact on performance. To support this immense scalability and facilitate better management of load balancing, the platform automatically adapts to changes in the data center, an ideal feature when you need to support large deployments and frequent changes.

Centralized management of operations, policies and auditing further supports scalability by simplifying the aggregation and normalization of multiple data sources for enterprise reporting.

The platform's agent and agentless connections to data sources help to reduce the workload of infrastructure teams without affecting the performance of data sources or applications. Use IBM Security Guardium S-TAP to conduct source monitoring of sensitive data as well as external Universal Connector plugins to monitor less sensitive data. This approach offers an agentless architecture that imports native audit logs, normalizes the data and prepares said data for reporting and analytics, streamlining the process of connecting it to modern, cloud-based data environments.



IBM Security Guardium Data Protection can be deployed to protect both structured and unstructured data sources, platforms and cloud infrastructure. It also supports enterprise databases or data warehouses running on major operating systems and helps monitor data sources deployed as LaaS or DBaaS across major providers.

This platform also integrates with and provides detailed analytics and insights to your existing security solutions, including IBM Security QRadar®, Splunk and ArcSight. Identity access management solutions like Active Directory/LDAP, RADIUS, CyberArk, AWS Secrets Manager and Hashicorp Vault to streamline authentication and centralize management of data source credentials and privileged access.

Conclusion

As data continues to grow in both volume and importance across industries, major security challenges will continue to arise for enterprises. IBM Security Guardium Data Protection meets that need by showing you where critical data is stored, how it's being accessed and providing recommendations for how best to protect it—all while helping you meet compliance and privacy requirements in the process. Reduce the risk of data breaches, provide real-time data security and visibility, and put this intelligent system to work.

Why IBM?

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services available. The portfolio, supported by world-renowned IBM X-Force® research, provides security solutions to help organizations drive security into the core of their business and thrive in the face of uncertainty.

IBM operates one of the broadest and deepest security research, development and delivery organizations in the world. IBM holds over 3,000 security patents and monitors more than one trillion events per month in more than 130 countries.

For more information

To learn more about IBM Security Guardium Data Protection, contact your IBM representative or IBM Business Partner or visit ibm.com/products/ibm-guardium-data-protection.

© Copyright IBM Corporation 2023

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the
United States of America
September 2023

Guardium, IBM, the IBM logo, IBM Security, IBM Watson, QRadar, and X-Force are trademarks or registered trademarks of International Business Machines Corporation, in the U.S. and/or other countries. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on [ibm.com/trademark](https://www.ibm.com/trademark).

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 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.

