IBM Guardium Discover and Classify

Sensitive data intelligence for security, privacy and data governance

Highlights

Automated and continuous network approach

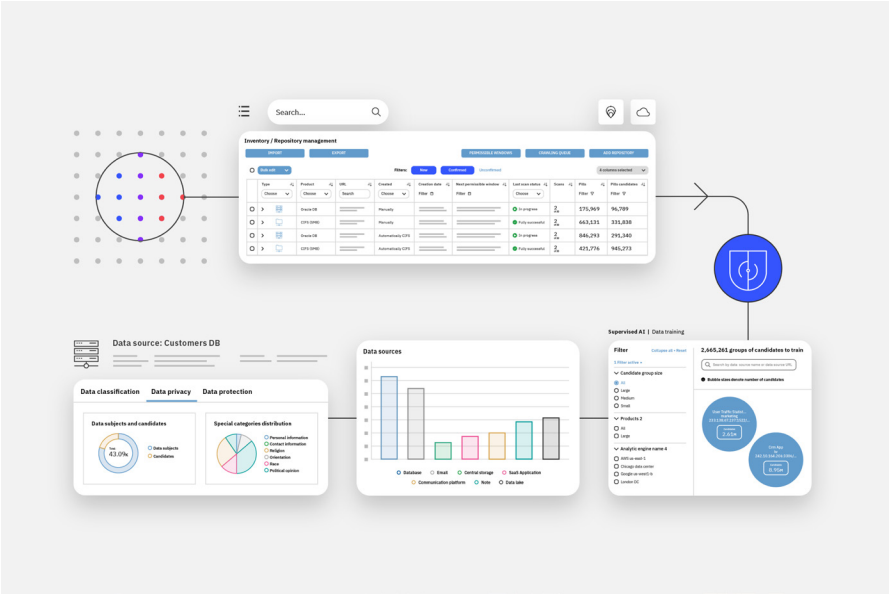
Unified security and privacy with IBM and other third-party solutions

Addressing data privacy requirements

Support for hybrid, multicloud and mainframe environments with minimal oversight required to operate

Protecting sensitive data is more complicated than protecting general data—it's more carefully regulated. Both clients and the general public respond differently to changes in sensitive data management as well as breaches that threaten this type of data. The most crucial element is awareness of how and where data enters the organizational network, and how and where it's disseminated and stored.

IBM® Guardium® Discover and Classify is an intelligence platform that uses data discovery and classification to deliver automated, near real-time discovery, network mapping and tracking of sensitive data at the enterprise level. Using techniques that include AI, machine learning (ML), natural language processing (NLP) and network analytics, the platform generates a master inventory of sensitive data down to the personally identifiable information (PII) or data element level. The inventory associates disparate data elements with the relevant data subject as well as provides data lineage, business context, transaction history and the location of all copies of every data element across on-prem, cloud and mainframe for structured or unstructured data. Guardium Discover and Classify can easily integrate with third-party solutions to use the information that the platform provides for data governance, incident response and privacy management.



Automated and continuous network approach

Failure to recognize sensitive data use within the organization exposes the enterprise to risks, such as include nonconformity to regulatory requirements and excessive hoarding of sensitive data when unnecessary. It's both a data security and privacy issue. Many organizations struggle with existing systems that can tell you where your personal data is—only after you tell the system where to look for it.

Guardium Discover and Classify uses a proprietary passive network packet capture process to assist in discovering sensitive data throughout your organization's network. This feature helps Guardium Discover and Classify identify repositories, such as databases, applications, file systems, log files and so forth, where sensitive data resides. The solution scans those locations to gain full visibility into the depth and breadth of the data. Guardium Discover and Classify then analyzes and consolidates the identified data into a master inventory that connects the information to business context. This action allows users to access, view and export the data to support a variety of business cases.

By analyzing traffic on an autonomous and continuous basis—as well as data repositories connected to the network—Guardium Discover and Classify can detect all elements on the network that are storing, processing and sharing sensitive data, both outside and inside the network. The platform can "crawl" any repository or database when it's confirmed to be or is suspected of processing sensitive data, whether it's known or unknown to the enterprise. In this way, Guardium Discover and Classify can give a truly holistic view as to how and where sensitive data is being used, whether it's data in motion or data at rest, structured or unstructured, in the cloud, on premises or on a mainframe.

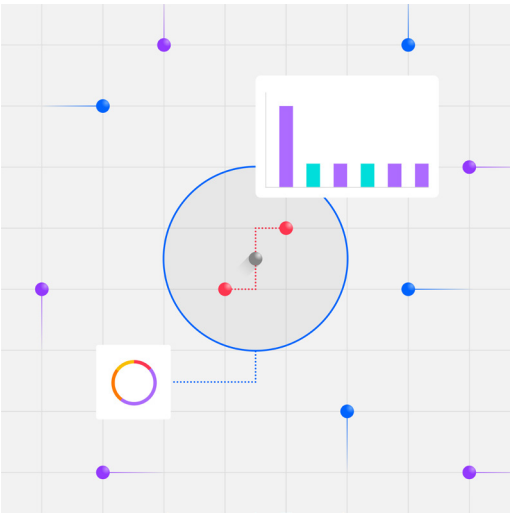
In addition to finding sensitive data, the Guardium Discover and Classify classification search function filters the cryptographic assets stored in the environment to easily determine which encryption tools and inventory crypto assets, including keys, functions and algorithms are at risk. Once inventoried, sensitive data is prioritized based on criticality to the organization. Users can export findings to the necessary tools, such as ServiceNow, security information and event management (SIEM) and security orchestration, automation and response (SOAR), to be remediated.

Guardium Discover and Classify offers comprehensive coverage of sources where sensitive data may reside, including structured, unstructured, cloud, on-prem and mainframe data stores. Gain visibility into discovery and classification scans—including statistics and results—for Common Internet File System (CIFS), Server Message Block (SMB), Network File System (NFS), Amazon S3 and Box. Recognize scan performance, how scan performance improves over time as the system learns, files that may have been skipped, total data scanned and other descriptive statistics. Optical character recognition (OCR) enables users to save time by reducing the need to manually sort or tag, improving, improve accuracy and data quality, and handling large volumes of data in unstructured documents. This OCR includes allowing users to identify and catalog sensitive data in image-based documents, such as PDF or JPG files.

Guardium Discover and Classify helps minimize your attack surface by categorizing and eliminating data that's duplicated, unused or no longer critical to protect. The platform provides a view of both the age of sensitive files and the last date modified to determine appropriate action. By keeping only necessary, sensitive data and getting rid of old or useless records and files, you can better address compliance and reporting requirements.

Guardium Discover and Classify scales with organizations, scanning and discovering both on-premises and cloud network elements. New repositories are discovered and scanned with minimal manual direction, maintaining lower operational costs—even as the organizational network gets larger.

With expansive support of data sources, Guardium Discover and Classify provides data classification on over 100 supported data sources, file types and protocols for both cloud and on-prem sources.



Unified security and privacy with IBM and other third-party solutions
Adopting a zero trust approach to data security and privacy means never assuming that anyone or anything is trustworthy. This concept requires continuously verifying whether access to personal data should be granted based on each user's contextual information. IBM can help put zero trust into action with unified data security and privacy workflows strengthened by contextual insight and connected solutions. IBM Guardium Discover and Classify platform's continuous discovery, monitoring and cataloging help round out most of the necessary security capabilities for zero trust.

Guardium Discover and Classify integrates with a variety of other products in the IBM Guardium portfolio to further enrich your data security posture. IBM Guardium Data Protection is a modern, scalable data security platform that's ready to meet the demands of today's increasingly complex environments. It helps protect sensitive and regulated data across multiple cloud environments while helping manage compliance obligations, discovering where sensitive data lives, encrypting and monitoring what's important, and helping reduce your risk while responding to threats.

A new, asynchronous bidirectional integration with Guardium Discover and Classify provides Guardium Data Protection with the location of sensitive data. It then automatically updates policies with information on the new data sources as well as identifies data sources that aren't being monitored but should be. Guardium Data Protection sends its current monitored data sources to Guardium Discover and Classify so that the solution can discover hidden data, rounding out the full data security picture.

IBM Guardium Insights is a data protection solution that uses advanced analytics to help uncover risk and threat patterns. It also works to prioritize data security and compliance activities based on automated risk-based scoring and alerting so that it can take immediate action to remediate incidents. To respond efficiently to risk and compliance issues, IBM Guardium Insights works collaboratively with the IBM SOAR Breach Response add-on to open an investigation and take mitigating actions with relevant stakeholders from security, privacy, legal and other departments.

IBM QRadar® SOAR is a breach response platform that helps guide organizations in their response with detailed tasks and instructions to comply with global, federal and state security regulations. To inform these activities, Guardium Discover and Classify provides much-needed context about the data that was compromised. Guardium Discover and Classify enriches the security and privacy analytics generated by IBM Guardium Insights and preloads critical information in breach response that's required for a thorough, targeted investigation and response plan that helps you manage a variety of compliance requirements.

Addressing data privacy requirements
Organizations need to comply with many different data security and privacy regulations, all of which are growing in complexity and scale. To help you keep pace, Guardium Discover and Classify provides near real-time visibility into the location and context of sensitive data across the network and enables you to assign exacting policies for intricate sets of data. Organizations can configure policies around sensitive data using rule sets, rule definition and business terminology, without requiring translation into technical operations or human intervention.

Guardium Discover and Classify offers a data subject access request (DSAR) workflow, entity configuration and identification, and tagging capabilities. These features allow users to associate repositories and networks in different locations with customized business, operational and alerting rules. Tags and entity rules can be easily updated and immediately applied to all scanned repositories and network elements.

Support for hybrid, multicloud and mainframe environments with minimal oversight required to operate
Guardium Discover and Classify is built on a distributed architecture that supports deployment of multiple analytic appliances that aggregate data into the console manager, creating a central inventory. Guardium Discover and Classify software can be installed on a 1touch.io physical appliance or a virtual machine (VM).

Analytic appliances can be installed as a physical or virtual appliance. Guardium Discover and Classify is agentless, combining support for security, privacy and compliance in a single platform, which helps reduce redundancies. It can also decrease the error rate by reducing manual oversight requirements. You can install the solution locally to reduce costs and increase performance. Once in production, Guardium Discover and Classify is virtually maintenance free and requires minimal action each month to maintain.

For more information
To learn more about IBM Guardium Discover and Classify, contact your IBM representative or IBM Business Partner, or visit ibm.com/products/ibm-security-discover-and-classify.

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the
United States of America
July 2024