IBM Security Discover and Classify

Sensitive data intelligence for security, privacy, and data governance

Highlights

Automated continuous data discovery using AI/ML, NLP and network analytics to help reduce operational costs

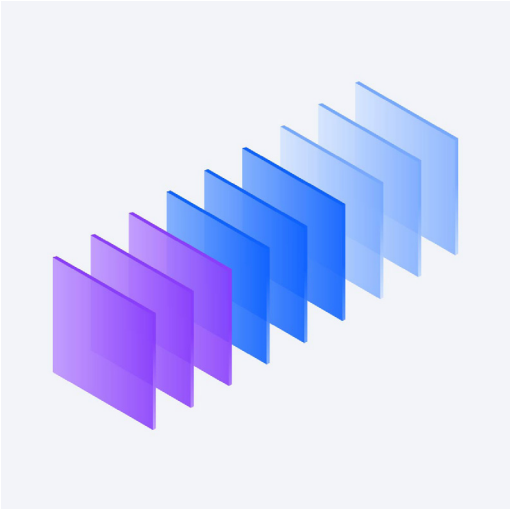
Compliance needs are addressed with full data lineage and history for near real-time visibility and context around sensitive data

Deep integrations with IBM Security and other third-party solutions

Easier to deploy with existing security infrastructure and minimal oversight required to operate

Protecting sensitive data is more complicated than protecting general data—it's more carefully regulated. Both customers 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 Security® Discover and Classify is a data discovery and classification platform that delivers automated, near real-time discovery, network mapping and tracking of sensitive data at the enterprise level. Using techniques that include AI/ML, NLP and network analytics, it generates a master inventory of sensitive data down to the PII or data element level. The inventory associates disparate data elements with the relevant data object, as well as providing data lineage, business context, transaction history and the location of all copies of every data element. IBM Security Discover and Classify can easily integrate with third-party solutions to leverage the information that the platform provides for risk management, risk assessments, incident response and privacy management.



Automated and continuous network approach

Failure to recognize sensitive data usage within the organization exposes the enterprise to risk. The risks not only include non-conformity to regulatory requirements, but can also lead to excessive hoarding of sensitive data when it's not needed. It's a security issue as well as a privacy one. Many organizations struggle with legacy systems that can tell you where your personal data is—only after you tell the system where your personal data is.

IBM Security 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 IBM Security Discover and Classify identify repositories (databases, applications, file systems, log files and so forth) where sensitive data resides. Then the solution scans those locations to get full visibility into the depth and breadth of the data. IBM Security Discover and Classify next 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—IBM Security Discover and Classify can detect all elements on the network that are storing, processing and sharing sensitive data both outside and inside the network. It can "crawl" any repository or database when it is confirmed to or suspected of processing sensitive data, whether it is known or unknown to the enterprise. In this way, IBM Security Discover and Classify can give a truly holistic view as to how and where sensitive data is being used, whether it is data in motion or data at rest, structured or unstructured, in the cloud, on-premises or on a mainframe. IBM Security Discover and Classify is especially capable at finding unknown sources such as shadow IT assets as well as known sources.

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



Unified security and privacy with IBM Security
Adopting a zero-trust approach to data security and privacy means never assuming 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 Security can help put zero trust into action with unified data security and privacy workflows, strengthened by contextual insight and connected solutions. By working with IBM Security Discover and Classify, the solution's continuous discovery, monitoring and cataloging help round out most of the necessary security capabilities for zero trust.

IBM Security Discover and Classify integrates with a variety of other products in the IBM Security Guardium® portfolio to further enrich your data security posture. IBM Security Guardium Data Protection is a modern, scalable data security platform that's ready to meet the demands of today's increasingly complex environments. It protects 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 IBM Security 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 identifying data sources that are not being monitored but should be. Guardium Data Protection sends its current monitored data sources to IBM Security Discover and Classify so the solution can discover hidden data, rounding out the full data security picture.

IBM Security Guardium Insights is a data protection solution that leverages 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 it can take immediate action to remediate incidents. To respond efficiently to risk and compliance issues, IBM Security Guardium Insights works collaboratively with IBM Security SOAR Breach Response to open an investigation and take mitigating actions with relevant stakeholders from security, privacy, legal and other departments.

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



Addressing your regulatory compliance 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, IBM Security Discover and Classify provides near real-time visibility into the location and context of sensitive data across the network and enables you to assign very exacting policies for intricate sets of data. Organizations are able to configure policies around sensitive data using rule sets, and rule definition using business terminology, without requiring translation into technical operations with human intervention.

IBM Security Discover and Classify offers 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.

IBM Security Discover and Classify scans both structured and unstructured data in the cloud and on-premises. Then it builds a relationship map between sensitive data and the data subject with which it's associated. All data sources, repositories, file systems and cloud systems are detected and scanned automatically. This feature provides autonomous visibility into sensitive data across the enterprise, allowing you to assess the risk level of security events and respond accordingly.

Flexible deployment and simplified support
IBM Security Discover and Classify is built on a distributed architecture that supports deployment of multiple analytic appliances which aggregate data into the console manager, creating a central inventory. IBM Security Discover and Classify software can be installed on 1touch.io physical appliance or a virtual machine. (This product is named Amazon VPC IBM Security Discover and Classify Data Sheet (Virtual Private Cloud).)

Analytic appliances can be installed as a physical or virtual appliance. IBM Security 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, IBM Security Discover and Classify is virtually maintenance free and requires minimal action each month to maintain.

1T+

IBM monitors more than one trillion events per month in more than 130 countries.

3K+

IBM holds over 3,000 security patents.

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.

For more information

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

© Copyright IBM Corporation 2023

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the
United States of America
April 2023

IBM, the IBM logo, Guardium, IBM Security, and X-Force are trademarks or registered trademarks of International Business Machines Corporation, in the United States 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.

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.

Statement of Good Security Practices: 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 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.

The client is responsible for ensuring compliance with all applicable laws and regulations. IBM does not provide legal advice nor represent or warrant that its services or products will ensure that the client is compliant with any law or regulation.

