IBM Security Discover and Classify

Sustainable data discovery for privacy, security, and data governance

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

IBM Security Discover and Classify (also known as 1touch.io Inventa™) is a data discovery and classification platform that delivers automated, near real-time discovery, network mapping, and tracking of personal sensitive data at the enterprise level with the help of techniques that include AI/ML, NLP, and network analytics. It generates a master catalog of personal data that 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 3rd party solutions that can leverage the information IBM Security Discover and Classify provides for risk management, risk assessments, incident response, and privacy management.

Highlights

- Automated continuous data discovery that can help reduce operational costs
- Platform driven by AI/ML for contextualized and enriched data
- Identification of new and/or unknown data repositories
- Discovery of structured and unstructured data at rest or data in motion, across the hybrid multicloud environment
- Full data lineage and history for complete visibility

The network approach

Blindness to personal data usage within the organization exposes the enterprise to risk, not only from non-conformity to regulatory

requirements, but also due to excessive hoarding of personal data when not needed. It's a security issue as well, not just a privacy one. Many organizations struggle with legacy systems that can tell you where your personal data is...once you can 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 the organizational network. This helps IBM Security Discover and Classify to identify repositories (DB, applications, file systems, log files, etc.) where sensitive data resides and scan them to get full visibility into the depth and breadth of the data. IBM Security Discover and Classify then analyzes and consolidates the identified data into a master catalog that connects the information to business context, and 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 personal data, both outside and inside the network. It can crawl any repository or database either confirmed to or suspected of processing personal 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 personal data is being used, whether it is data in motion or data in rest, structured or unstructured, in the cloud or on-premises, and especially if known or unknown.

IBM Security Discover and Classify scales with the organization, scanning and discovering both on-premise and cloud network elements. New repositories are discovered and scanned with minimal manual direction, maintaining low labor costs even when the organizational network grows.

Addressing your regulatory compliance needs

Organizations need to comply with different data security and privacy regulations, which are growing in complexity and scale. To 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 policies on the data asset levels. Organizations will be able to configure policies around personal data via rule sets, and rule definition uses business terminology, without requiring translation into technical operations.

IBM Security Discover and Classify offers DSAR workflow, entity configuration and identification, and tagging capabilities that allow users to associate repositories and networks in different locations with different 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, and builds a relationship map between personal data and the data subject with which it is associated. All data sources, repositories, file systems, and cloud systems are detected and scanned automatically. This provides visibility into sensitive personal data across the enterprise, allowing you to assess the risk level of security events and respond accordingly.

Flexible deployment and easy to support

IBM Security Discover and Classify's distributed architecture supports deployment of multiple Analytic Appliances that aggregate data into the Console Manager, which creates a central inventory. IBM Security Discover and Classify software can be installed on 1touch.io physical appliance(s) or a virtual machine (Amazon VPC

(Virtual Private Cloud)). Analytic Appliances can be installed as a physical or virtual appliance.

IBM Security Discover and Classify is agentless. It combines support for privacy, security, and compliance in a single platform reducing redundancies. It also decreases 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 only requires a few hours each month to maintain.

Unified security and privacy with IBM Security

Adopting a zero trust approach to data privacy and security means never assuming anyone or anything is trustworthy, but continuously verifying whether access to personal data should be granted based on 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 necessary security capabilities for zero trust.

IBM Security Guardium Insights is a data protection solution that leverages advanced analytics to help uncover risk and threat patterns, prioritize data security and compliance activities based on automated risk-based scoring and alerting, and take immediate action to remediate incidents. To respond efficiently to risk and compliance issues, Guardium Insights works with *IBM Security SOAR Breach Response* to open an investigation and take mitigating actions collaboratively with relevant stakeholders from security, privacy, legal, etc. The Breach Response platform helps guide organizations in their response with detailed tasks and instructions, to comply with global, federal, and state 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 from Guardium Insights and preloads critical information in Breach Response that is required for a targeted and thorough investigation and response plan that meets compliance requirements.

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.

This document contains information pertaining to the following IBM products which are trademarks and/or registered trademarks of IBM Corporation:

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 IBM Security's collaboration with 1touch.io, please contact your IBM representative or IBM Business Partner, or visit the following website: https://www.ibm.com/products/guardium-insights