Solution Brief

StoredIQ InstaScan™

February 2021

BREAKWATER

BREAKWATER

Table of Contents

BREAKWATER

Introduction to StoredIQ InstaScan™

Privacy and data protection regulations are growing and evolving around the world. The General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), and Brazil's General Data Protection Law (LGPD) are some of the largest privacy regulations to impact global organizations. Other countries are following the trend to develop privacy regulations. As a result, the regulatory landscape continues to shift almost weekly.

As organizations are faced with more data privacy regulations, they must also look more holistically at how they store and use data. Organizations must now enact, comply and sustain readiness to these regulations by implementing a comprehensive enterprise-scale data privacy program. Data privacy regulations can function as a roadmap for organizations to establish a strong information and data governance program.

According to an IBM study, data discovery and ensuring data accuracy are the biggest focus areas for organizations when preparing for the GDPR. Organizations use techniques like discovery and mapping to identify the risk associated with sensitive and personal data that they use and store.

Ungoverned sensitive data may lead to regulatory penalties, and a data breach can impact consumer trust. To govern and protect data, global organizations need tools to review petabytes of data and apply the correct policies and regulations of how that data can be used.

In the US, at least 25 states have laws focused on data security and how organizations treat user data. Many of these laws state that organizations must enact "reasonable" security procedures and practices to avoid the unauthorized use of personal information. One way organizations can achieve reasonable data privacy is to perform data discovery and mapping and then apply analytics to accelerate compliance readiness. StoredIQ InstaScan is a containerized unstructured data management and privacy solution that identifies risk hot spots on an organization's data sources and reduces the time for compliance data collection.

StoredIQ InstaScan™ is an intelligent file analysis tool that leverages automation and statistical sampling models to quickly identify risk hot spots in unstructured cloud data. The tool helps accelerate regulatory compliance and data governance as part of an information governance practice by providing unique capabilities, such as:

- Risk assessment and remediation recommendations
- Support for multiple cloud sources, including MS 365 and Box
- Audit-ready compliance checks

How StoredIQ InstaScan Works

Define the scope

The first step in discovering and mapping your data is to define which data sets need analysis. A best practice is to conduct user interviews to determine which areas should be prioritized for analysis. The interviews provide details on what information is stored on which data sources, like Box, Google Drive, Microsoft OneDrive, or SharePoint, and helps establish the project scope. Different organizations have various policies and regulations with which they must comply. With StoredIQ InstaScan, you can use the possible data source scoping feature and ensure you have the correct policies defined for each analysis.

Visualize the data source

The next step is to make sure the documents can be searched and accessed quickly. StoredIQ InstaScan uses the existing metadata index in cloud repositories such as Box and Office 365 to provide an overview of the data. Using the Native Index for Cloud Sources, you can skip the need to do a metadata scan and assess the total number of documents.

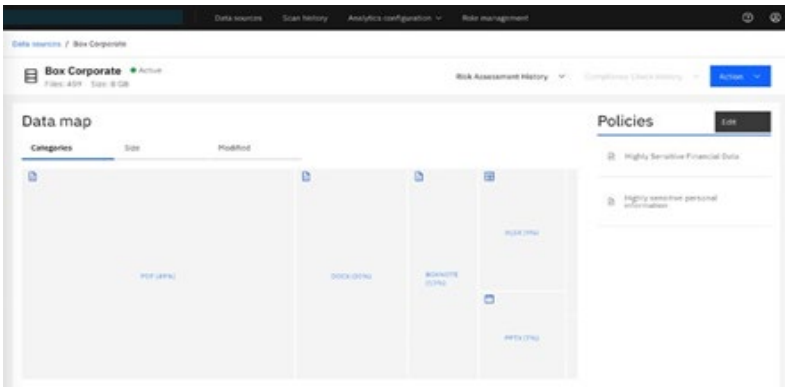

Figure 1: A data map organizing data based on extension.

StoredIQ InstaScan provides a meaningful visual representation of an organization's data repositories to help take appropriate analytics action.

Risk Assessment

StoredIQ InstaScan uses a statistical sample to analyze the chosen data source. It provides three scans of varied intensity—basic scan, intermediate scan, and rigorous scan. StoredIQ InstaScan picks a random sample from the data source and performs a Risk Assessment on the data by scanning for policy violations. The amount of sample data being analyzed depends on the type of scan the user chooses. A more intense scan leads to a higher amount of sample data and requires more time, but you will also have higher confidence in the results.

While running the Risk Assessment or after it is complete, you can view which policy violations exist within the sampled data and determine where they are the most prevalent. This step helps identify sensitive and personal data and can be used to prioritize data clean-up activities.

Figure 2: The Risk Assessment console provides three scanning options based on intensity.

Identify policy violations

When you perform a Risk Assessment scan using the above options, StoredIQ InstaScan reads a sample set of data from the selected data source. The documents within the data source remain in place—no data moves to a separate repository. Analysis plugins, also known as cartridges from StoredIQ, identify personal data and enrich the local data store regarding the risk associated with this data. These analysis plugins will contain analytics logic based on different technologies ranging from simple regular expressions to full-blown cognitive approaches like natural language processing (NLP).

These analysis plugins are designed to assist organizations in preparing and complying with various data privacy regulations. The following personal data types are just some of those supported by StoredIQ InstaScan, right out of the box:

- Bank account numbers, credit card numbers, international (IBAN) and national versions
- National identification numbers like tax ID, national ID card, or passport numbers
- Phone numbers, email addresses, and IP addresses
- Person names
- Organization names Locations and addresses
- Dates

You can customize these analysis plugins and extend them to include additional data types.

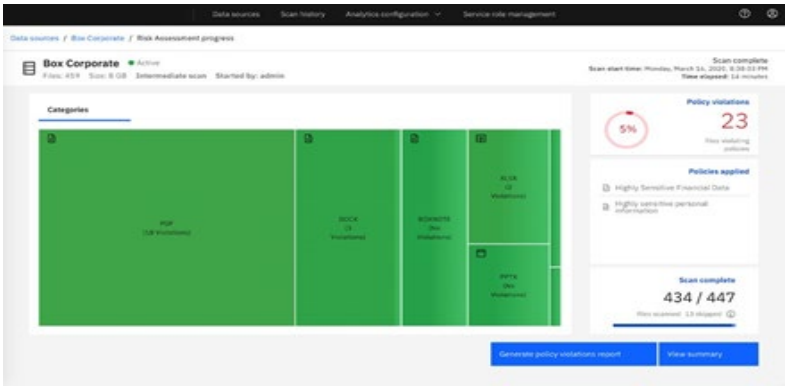

Figure 3: This Risk Assessment visualization shows policy violations across different data types for the chosen data sample.

The Risk Assessment can be used to prioritize clean-up activities. By performing Risk Assessment regularly, you can be more confident about your organization's data. After the Risk Assessment is complete, StoredIQ for Information Governance, licensed separately, can be used for in-depth analysis and data remediation.

Compliance Check

You can run a Compliance Check on a presumed clean data source – this can be when interviews have told you the source is clean, when a Risk Assessment comes back without issues or when remediation actions have been performed. When starting a Compliance Check, users will choose the desired confidence level and acceptable error rate. StoredIQ InstaScan then calculates how many documents need to be reviewed and uses a statistical sampling algorithm to perform an analysis.

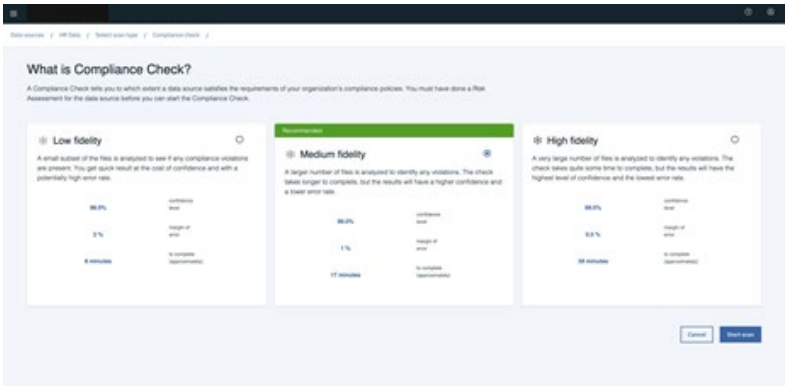

Figure 5: The Compliance Check console displays various levels of fidelity.

Passing the Compliance Check gives the user confidence that the selected data source is compliant and generates a report that can be used for audit and regulatory purposes. A failed Compliance Check will signify that additional remediation needs to occur.

With StoredIQ InstaScan, you can:

- Define your organization's policies for assessing cloud data sources
- Perform a Risk Assessment to quickly identify the risk spots within your data and prioritize remediation action
- Gain confidence in clean-up efforts with a Compliance Check
- Download reports after performing Risk Assessments and Compliance Checks
- Reduce time in gathering compliance data to help prepare for audit and regulatory checks

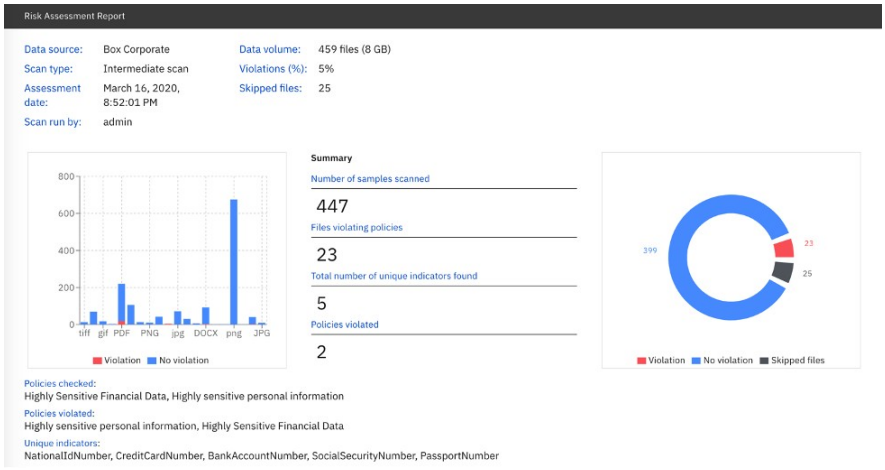

Figure 6: A sample Risk Assessment report.

Conclusion

To maximize operational efficiency, control costs, and reduce risks, organizations should use file analysis as part of a comprehensive information governance program. StoredIQ InstaScan is an intelligent file analysis tool that leverages automation and statistical sampling models to identify risk hot spots in unstructured cloud data quickly. The tool helps accelerate regulatory compliance and data governance as part of an information governance practice by providing unique capabilities for risk assessment and remediation recommendations.

Learn more at www.breakwatersolutions.com.

Why Breakwater

Breakwater helps mitigate risk and gain insight from sprawling information by combining technology automation and human expertise. Our expert consulting, software, and managed services address the challenges within information governance, disputes and investigations, regulatory compliance, privacy, and cybersecurity. Our solutions allow governance, legal, and risk professionals to locate, access, analyze, and manage information by making data transparent and actionable. Breakwater helps clients in public and private sectors mitigate risk, improve productivity, and increase profitability by transforming how they use data.

Expert Consulting and Advisory

At Breakwater, we know there is always a better way. We innovate process and automation to create efficient and effective approaches to information intelligence. Our solutions drive speed to insight for our clients, enabling them to act quickly and confidently with their information, whether responding to legal discovery, improving compliance, or protecting sensitive data. And our results deliver measurable value—reducing risk, improving quality, and saving money.

Our consulting expertise includes:

- Information Governance
- Litigation & Disputes
- Investigations & Regulatory Response
- Cybersecurity, Privacy, Data Risk

Supported by Managed Services

The investment in technology automation supporting legal, compliance, security, and governance requirements can be maximized by leveraging experts during implementation and ongoing operation. Engaging an experienced managed services team with direct access to application developers is key to achieving your business objectives.

Breakwater offers flexible managed services solutions based upon your requirements, from implementation and transition to your team to full daily management and operation. Working with organizations worldwide in every industry, the Breakwater Managed Services team offers decades of experience in information governance and management. Companies use managed services to augment their internal teams to balance workload spikes and mitigate the risk of service disruption.

Notice: Clients are responsible for ensuring compliance with various laws and regulations, including the European Union General Data Protection Regulation. Clients are solely responsible for obtaining advice from competent legal counsel as to the identification and interpretation of any relevant laws and regulations that may affect the clients' business and any actions the clients may need to take to comply with such laws and regulations. The products, services, and other capabilities described herein are not suitable for all client situations and may have restricted availability. Breakwater does not provide legal, accounting, or auditing advice or represent or warrant that its services or products will ensure that clients are in compliance with any law or regulation.