

ControlX 1.4

Robust multi-aprover remediation workflows

Business Challenges:

The volume of data is growing rapidly. TechJury reports that more than 11.145 trillion MB of new data is created every day. With the advent of the Information Age, data can now be shared, stored, and transmitted with the click of a mouse. One difficulty of this trend is that the storage and transmission of sensitive data across computer systems can be difficult to secure, raising the need for vigilance. Organizations must protect their customers' personal information and sensitive data to avoid data exposure, breaches, and non-compliance with national and international regulations.

A sensitive data leak occurs when a company unknowingly exposes sensitive data or when an incident causes sensitive data to be accidentally destroyed, lost, altered, or accessed in an unauthorized way by others. **Unauthorized exposure of sensitive data can result in financial damage and competitive threats, as well as damage to your reputation and brand.** Among the types of data that can be exposed are financial reports, bank account numbers, credit card numbers, usernames, passwords, personal details, and healthcare records.

A data breach and data exposure can be more than just a temporary issue; it can affect the entire future of your company. Companies should therefore strive to protect sensitive data at all times to protect their business and reputation and help protect their customers from problems such as these.

Eliminate Data Exposure Risks with ControlX 1.4

When enterprises are aware of the personal data that exists within their environment, they can safeguard the information of their users and that of the company and minimize the risk of non-compliance with privacy laws, such as GDPR in the European Union or HIPAA in the United States. Knowing what data you have allows you to act on that knowledge and resolve potential issues within your environment.

Your data may need to be remedied in several ways, depending on the issues you find and the nature of your environment. Potential issues can be remedied in the following ways:



**Quarantine
Sensitive Data**



**Restrict Access to
Sensitive Data**



**Provide a scalable,
immutable audit
trail.**

ControlX 1.4, an integral part of Insight Analytics 1.4, facilitates all the above.

Important features of ControlX 1.4.

- **Ensures data remediation of potentially sensitive information**

By utilizing this feature of the product, your organization will mitigate the risk of sensitive data access and misuse through a robust, multi-approver remediation workflow. With this workflow, all necessary stakeholders are assigned tasks to request, approve, and execute different types of Remediation assignments, and all users can easily see the status of each Remediation project as it proceeds.

- **Quarantine your sensitive data into a secure, accessible location**

With the new Remediation workflow, users can quickly and securely migrate sensitive data from their current storage location to a more secure location, such as a share on a file storage resource or an object storage bucket. Sensitive files may be moved from one file-share to another file-share and a file-share to an object-store location, including NFS and SMB based storage technologies. Object storage includes any S3 compliant object store and support for Azure-Blob.

- **Enables creating an audit trail for files using blockchains**

This function allows you to create an immutable audit trail based on the metadata and attributes of a set of files using ControlX's built-in blockchain functionality. Insight AnalytiX can then create and display an audit trail report for the set of files that are guaranteed to be accurate and real, including any instances in which a file has been accessed or modified by a user.

- **Enables users to secure sensitive files**

The Remediation Analyst may secure files from unnecessary access by excluding public access to reported sensitive files. The Secure remediation action of ControlX 1.4 allows the user to use the StorageX application to change the Access Control List (ACL) for a set of files in the environment to permissions defined in a Secure remediation template. This release supports securing files in SMB-based storage on a single Microsoft Windows Active Directory domain.

This latest upgrade in Insight AnalytiX 1.4 is focused on enhancing the product's Data Protection and Security Functionalities and will help customers with flexible and scalable PII discovery, deep analytics, and reduced data vulnerability.

The ControlX 1.4 solution empowers enterprises to mitigate risk and drive data security remediation proactively.

Book a Demo to See ControlX 1.4 in Action

Find answers to your questions by contacting solutions@datdyn.com

About Data Dynamics

Data Dynamics is a leader in intelligent file management solutions that empower enterprises to analyze seamlessly, move, manage and modernize critical data across hybrid, cloud, and object-based storage infrastructures for true business transformation. For more information, please visit www.datadynamicsinc.com.



© 2023 Data Dynamics. The trademarks Data Dynamics, StorageX, Insight AnalytiX, ControlX, Universal Data Engine, UDE, Insight Analytics, Manage Your Data, Champion of Data, and Dynamic File Management are the registered or unregistered trademarks of Data Dynamics, Inc. All other trademarks are the property of their respective owners.