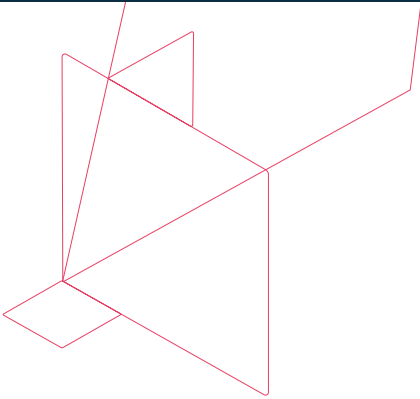


Sensitive Data Governance with Commvault Activate™

Reduce your risk, protect your reputation, optimize your compliance



Each year, we see a global increase in the number of cyberattacks and in the number of data loss incidents associated with data breaches. With your data residing on-premises, in multiple clouds, and across more locations than ever, managing confidential or sensitive information can be a struggle. Yet, it is crucial for your information governance, privacy, and cybersecurity programs.

Only 40% of respondents were very or extremely confident in knowing exactly where their data resides.¹

With more scrutiny being placed upon protecting sensitive data such as personally identifiable information (PII), you need to answer these key questions:

- What does your organization define as “sensitive” data?
- Do you know where all that data resides? Can you easily secure or delete it if needed?
- Can you proactively find and identify new data containing PII or other sensitive information?
- What reports or audit tools do you have in place to track processes related to the management of sensitive data?

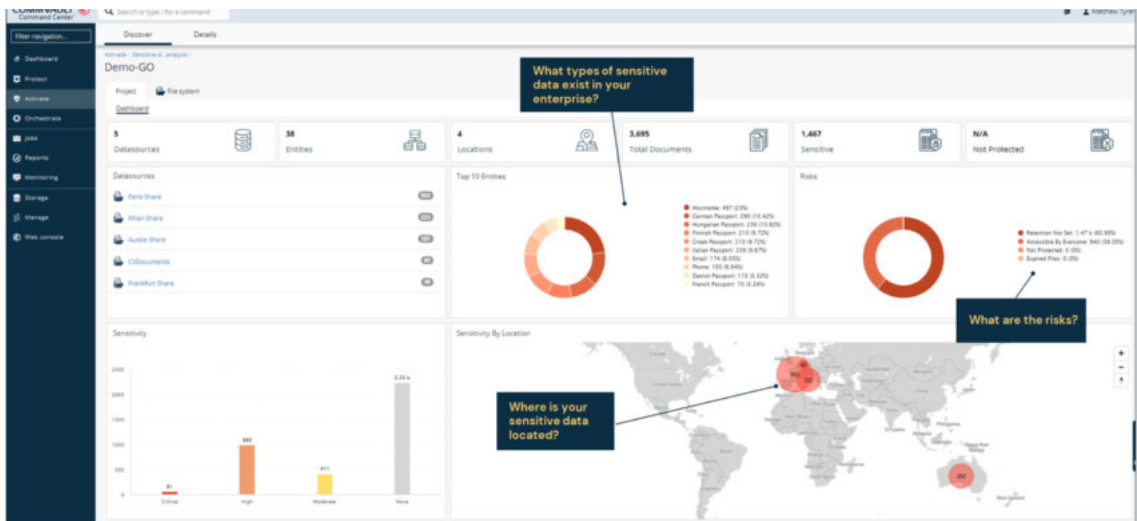
Your data. Know it. Act on it.

Commvault Activate gives you the insight you need to answer those questions and secure your sensitive data.

Powered by advanced analytics and machine learning, the information about files, email, databases and their contents are centralized in an intelligent index. This provides a consistent view of your data across your organization. Through these analytics you can quickly find sensitive data residing in both your live environment and within your Commvault backup or archive copies.

While many key data types related to HIPAA, FERPA, PCI, are common, you may have company-specific requirements. Commvault Activate allows you to leverage existing definitions or create custom ones to match your organization’s sensitive data criteria.

With those definitions in place you can quickly identify matching data sets and drive action. Using built-in workflows for review and audit, you can quarantine the live data or even delete the sensitive files from the backup copy to prevent data leakage. This level of visibility to your important data will also accelerate your ability to respond to compliance, legal, or data subject requests.



Commvault Activate key features for Sensitive Data Governance	
Gain visibility into production and backup data.	Create a full index of data from structured, unstructured, and semi-structured sources within your production environment as well as Commvault backup and archive copies. The centralized index gives you organization-wide data visibility, so you can make content-aware decisions and apply consistent data policies.
Proactively identify sensitive data and act.	Use the Entity Manager to define and customize sensitive data types for your ecosystem. Then leverage Commvault's machine learning driven algorithms to quickly find matching data sets across both your production and backup data sources.
Dynamic dashboards.	Use the out-of-the-box dashboards or customize them for different projects and uses within your organization. Search, filter, and drill down to the relevant details such as: <ul style="list-style-type: none"> • Data owner type, size, and location • Sensitivity level • Identified risks associated with the data • And more
Review and respond to disclosure and other legal or compliance requests.	Request Manager provides automated workflows for compliance tasks such as audit, review, and data subject requests directly from the dashboards. Accelerate your response to regulatory inquiries such as GDPR "Right to be Forgotten" and "Right to Disclosure".
Proof of Compliance	Maintain an auditable chain of custody to demonstrate compliance with details of every action taken within the Commvault solution.
Role-based access	Robust and granular role-based access enables secure collaboration among IT security, data privacy officers, and other stakeholders.

Complete your intelligent data management strategy

Enhance your data management by integrating Commvault Activate with a proven leader and innovator in the backup and recovery market – Commvault Complete™ Backup & Recovery.

Commvault Complete Backup & Recovery is a single, powerful solution for data protection – whatever your data is, wherever your data lives. Through automation, an intelligent policy engine, and deep integrations into one of the broadest lists of applications, hypervisors, clouds, and platforms, you can be confident your data is protected and can be recovered when and where you need it.

Commvault Activate can operate independent of Commvault Complete Backup & Recovery or as part of a combined solution to maximize data management capabilities for your business. Through Activate, you can gain insights to data that isn't necessarily managed by Commvault to drive analytics and other tasks against those data sources.

Commvault users saw up to **61%** reduction in annual exposure to compliance or audit failures and/or data theft and breach and had **48%** faster responses to discovery requests.²

1 Integris – Data Privacy Maturity Survey

2 IDC: Quantifying the Business Value of Commvault Software – Worldwide customer survey analysis

Commvault Activate can help you to better understand and act upon your data. [Learn >](#)