COMMVAULT®

Commvault® Sensitive Data Governance

WHAT INFORMATION WOULD DO THE MOST DAMAGE TO YOU OR YOUR ORGANIZATION IF IT WERE LOST OR LEAKED?

Each year, we see a global increase in the number of cyberattacks and in the number of data loss incidents requiring data breach notifications. Therefore, it should be no surprise that governments around the world are introducing ever more stringent data privacy regulations designed to protect individuals from data theft. The latest of these is the EU's General Data Protection Regulation (GDPR) which becomes effective on May 25, 2018.

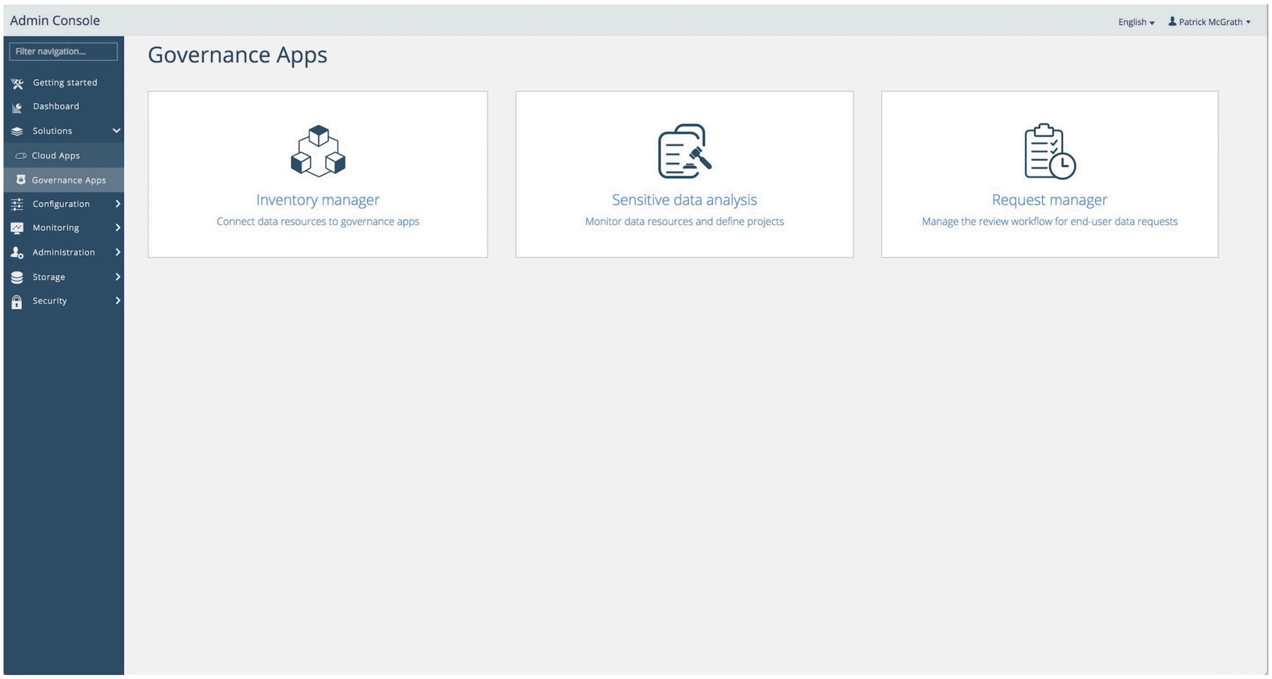
Managing confidential or sensitive data is a struggle for most organizations. It's the most common target for data thieves and usually the initial driver for information governance, data compliance and security programs. Examples could include:

- Personal data, which could be personally identifiable information (PII) or could expand to include data such as religious or political affiliations, ethnic background, union memberships, personal legal judgements, etc.
- Financial data including, credit card information (PCI), bank routing and account numbers, contracts and other financial records, etc.
- Health and clinical information (HIPAA), etc.
- Student records (FERPA), etc.
- Research or intellectual property

> "Gartner predicts that by the end of 2018, more than 50 percent of companies affected by the GDPR will not be in full compliance with its requirements."[1]
>
> GARTNER

This is a potentially long list. While many of these data types are shared by companies and highlighted by certain regulation, others can be industry or company specific. Each organization must determine their own data classification scheme and apply appropriate controls and protections for the data.

Organizations typically have high confidence in their ability to identify and manage sensitive data within structured data sources such as databases. After all, databases are designed to enable reporting and remediation. However, for many, unstructured data is a bigger challenge. While it comprises about 80% of all data stored[2], unstructured data can present a critical blind spot which is notoriously difficult to control.



Governance Apps

Inventory manager
Connect data resources to governance apps

Sensitive data analysis
Monitor data resources and define projects

Request manager
Manage the review workflow for end-user data requests

COMMVAULT® SENSITIVE DATA GOVERNANCE

[1] Gartner Says Organizations Are Unprepared for the 2018 European Data Protection Regulation, Gartner May 2017

[2] Structured vs. Unstructured Data, Datamation August 2017

REDUCE YOUR RISK, PROTECT YOUR REPUTATION, OPTIMIZE YOUR COMPLIANCE

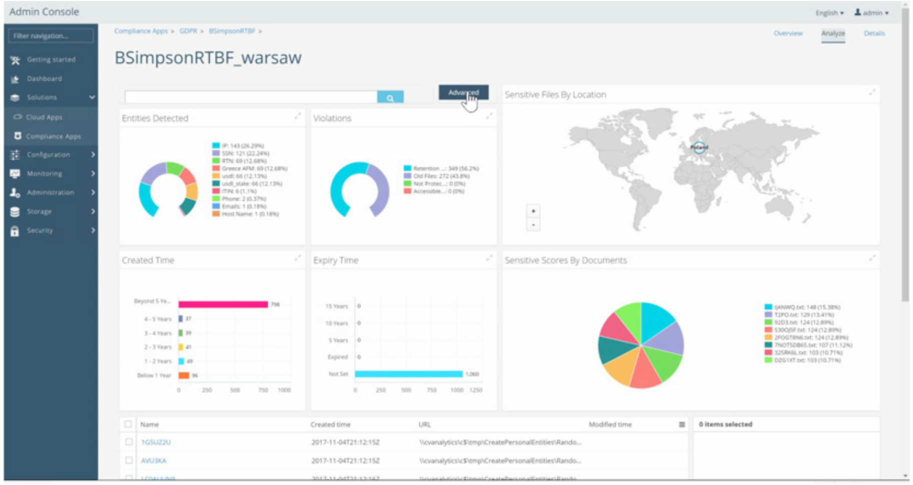
If you don't need to store sensitive data, just don't. Avoid the risk and minimize your threat vectors.

Commvault® Sensitive Data Governance simplifies the best practices of managing sensitive data at scale, starting with file servers and endpoints:

- At any point in time, find and tag sensitive data wherever it resides in your ecosystem and know who has access to it.
- Present the key information that allows you to prioritize a plan of action.
- Facilitate proactive sensitive data cleanup and automate your data policy with information lifecycle rules for retention and erasure.
- Ensure comprehensive response to data subject requests for disclosure or erasure.
- Prove compliance to your auditors.

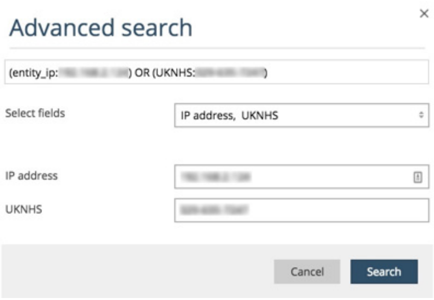
Commvault® Sensitive Data Governance performs all of these functions within a single toolset, reducing the risks and costs of relying on a variety of niche products.

> "A good starting point is to create a prioritized list of what needs to be done. In particular, make sure that 80% of the organization's unstructured data is addressed."[3]
>
> **IDC**
> *FIVE ESSENTIAL STEPS FOR GDPR COMPLIANCE*



Name	Created time	URL	Modified time
1GSUZ2U	2017-11-04T21:12:15Z	\\cvanalytics\c$\tmp\CreatePersonalEntities\Rando...	
AVU3KA	2017-11-04T21:12:15Z	\\cvanalytics\c$\tmp\CreatePersonalEntities\Rando...	

ANALYZE SENSITIVE DATA RISK

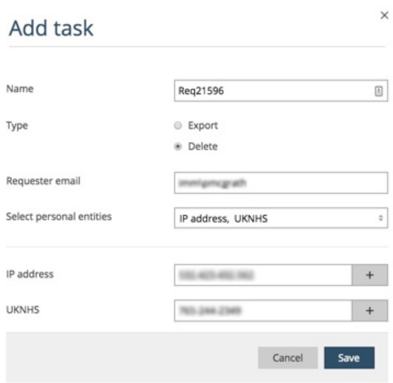


Advanced search ×

(entity_ip:[redacted]) OR (UKNHS:[redacted])

Select fields	IP address, UKNHS
IP address	[redacted]
UKNHS	[redacted]

FIND INFORMATION QUICKLY



Add task ×

Name	Req21596
Type	○ Export ● Delete
Requester email	[redacted]
Select personal entities	IP address, UKNHS
IP address	[redacted]
UKNHS	[redacted]

INITIATE DATA SUBJECT REQUESTS FOR DISCLOSURE OR ERASURE

[3] IDC White Paper, sponsored by Commvault, Five Essential Steps for GDPR Compliance, March 2017

KEY CAPABILITIES

CAPABILITY	DESCRIPTION
CENTRALIZED SEARCH INDEX	Create a centralized searchable index of your unstructured data from file servers and endpoints. Harvest file metadata and contents directly from active locations or gain efficiencies by analyzing the data you've already backed up or archived.
SENSITIVE DATA DETECTION	Eliminate blind spots and classification gaps. Detect and extract sensitive data from within file content, based on a prebuilt set of personally identifiable information (PII) data profiles. Expand the list of data profiles based on your company's requirements.
INFORMATION RISK PLANNING	Assess information risk with reports and other visualizations that illustrate where sensitive information resides across your organization's infrastructure. This allows you to focus on the most critical items first and build your remediation and protection priorities from there.
ACTIVE DIRECTORY INTEGRATION	Information sourced from Active Directory allows additional analysis of devices, users and access controls to help with risk assessments and planning.
MINIMIZE DATA RISKS	Reduce your exposure by removing sensitive data that is not critical to your organization. Preview files to determine whether they should be retained, deleted or ignored. Move files to secure locations or delete files altogether based on your review. Set retention periods for files — and in combination with Commvault® File Archiving — automate retention and disposition.
RESPOND TO DISCLOSURE REQUESTS	Support sensitive data disclosure requests from data subjects, with multi-step workflows that help to identify, validate and export files containing sensitive data specific to an individual. *Examples include GDPR Right of Access by the Data Subject [Art. 15].*
RESPOND TO ERASURE REQUESTS	Support sensitive data erasure requests from data subjects, with multi-step workflows that help identify, validate and delete files containing sensitive data from the source location, specific to an individual. *Examples include GDPR Right to Erasure ('Right to be Forgotten') [Art. 17].*
PROOF OF COMPLIANCE	Demonstrate compliance with comprehensive audit logging, detailing every action taken with the Commvault solution.
ROLE-BASED ACCESS	Role-based access enables secure processing between IT, DPO and other stakeholders.

▶ Are You GDPR Ready? Learn 5 Essential Steps to Achieving GDPR Compliance. Read the IDC REPORT.

COMMVAULT

COMMVAULT.COM | 888.746.3849 | GET-INFO@COMMVAULT.COM