Reduce Risk and Protect Privacy across Enterprise Systems

Most organizations today have content stored in business applications and system databases. This content can contain confidential information that pertains to future strategy, forecast figures and partnership plans, or sensitive data such as personally identifiable, personal credit or personal health information.

The sensitivity and privacy needs of this data is often overlooked when content becomes inactive and only referred to for reporting purposes, or is buried in file shares and SharePoint sites that remain ungoverned.

Global Regulations Are Driving Complex Requirements

With an increasing number of publicized data breaches for organizations around the world, information security and data privacy are rapidly growing priorities. The complexity of addressing these needs has increased with the creation of global regulations such as GDPR that require compliance across multiple jurisdictions and many types of content.

The risk of exposing sensitive data increases when applications are retired, databases are duplicated for development and training environments or SharePoint sites and File Shares are abandoned at the conclusion of a project. For retired applications with no suitable upgrade or migration path, this inactive but sensitive data often needs to be maintained for regulatory and business continuity reasons so must be secure, accessible and usable. Similarly unstructured content such as email, spreadsheets and documents that may be left ungoverned in less secure environments such as SharePoint sites, files shares and exchange must be identified, analyzed and protected to reduce risk of loss or theft.

Difficulties in Addressing Data Privacy Regulations

Sensitive and confidential information can reside in many different business systems including; databases for HR, Finance, Customer and Sales as well as file shares, SharePoint sites and email servers. These systems don't have to be active either, they may be retired applications or abandoned SharePoint sites. The problem is, if you don't know what information resides in these systems and you don't have the tools to identify PII, PCI, PHI and corporate records you run the very real risk of this information being exposed, lost or stolen and your organization being in breach of various regulations including privacy.

The Challenge of Balancing Collaboration and Compliance

In addition to the challenges of identifying and protecting sensitive information, you need to balance the requirements of compliance with your business goals around productivity and efficient collaboration. Today most organizations (not just highly regulated industry) have compliance as a high priority. While they need to put essential systems and processes in place to protect and govern their data they also need to improve productivity, collaboration and efficiency to grow their business in an increasingly competitive market. It's easy to forget collaboration extends well beyond the ability to work simultaneously on a document.

Efficient and effective collaboration is dependent on staff having access to the right content, in context when and where they need it. You need to have tools that facilitate the governance, protection and authorized sharing of content without negatively impacting the user experience—this means having powerful search, an intuitive user interface, navigation, automation and mobile support, to name a few.

The Ongoing Cost to Compliantly Manage and Access Data from Retired Applications

Data privacy and protection can be overlooked for application data in retired, test and training databases, it can also be costly to maintain and access. You might struggle to identify, mask and extract sensitive information from a retiring application before it is shut down, or as is the case with many organizations, you may choose to maintain an instance of the retired application for reporting purposes only. In addition to the license costs you also have to maintain costly (skilled) resources and infrastructure for as long as access and reporting is needed—even if this is sporadic and very infrequent. The difficulty in extracting data or running a report with limited resources could result in your inability to respond promptly to an FOI or e-discovery request.

With changing privacy regulations there is also a real risk that sensitive data may not be

managed in accordance with legislation and could be accidently or deliberately exposed or leaked. An industry survey suggests 20% of organizations sighted "staff negligence or bad practice is the most likely cause of data loss."*

Micro Focus Secure Content Management—Reduce Risk, Protect Privacy and Collaborate Efficiently

The Micro Focus Secure Content Management suite integrates file analysis, structured data management and governance-based enterprise content management to help you identify, analyze, manage, retain and consign both unstructured and structured data across the lifecycle. The Secure Content Management suite consists of ControlPoint (file analysis for unstructured data), Structured Data Manager (application retirement and structured data archiving) and Content Manager (governance-based ECM to manage both structured and unstructured content across the lifecycle).

Content is analyzed for sensitivity and risk, masked (if required), classified accordingly with policy applied to govern access, sharing and retention. Connected repositories, contextual relationships and powerful search coupled with policy based enterprise content management (ECM) makes it easier to find the permissible data you're after.

Unstructured content can be managed inplace or moved to a secure repository while structured data extracted from system databases has security and access controls applied prior to being intelligently archived to support future reporting and access needs.

Both the structured and unstructured data is managed by Content Manager (governance-based enterprise content management), in a unified and policy driven manner across the lifecycle to facilitate authorized access, re-use and reporting. To optimize system performance and infrastructure costs, redundant, obsolete and trivial (ROT) data is defensibly disposed while storage is tiered and the remaining content allocated according to its value and activity levels.

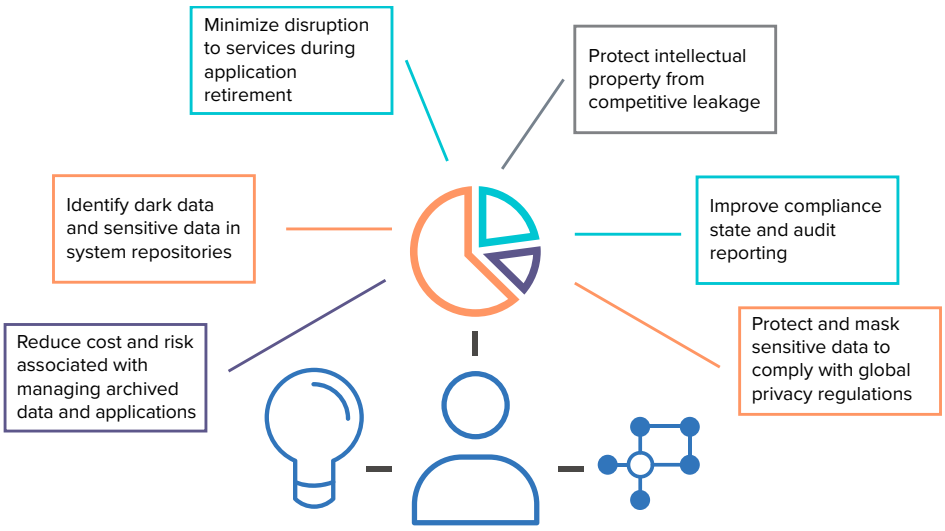

Figure 1. What do you care about?

What Are the Advantages of Secure Content Management?

Secure Content Management suite helps you balance the requirements for collaboration and productivity with information security, privacy and compliance across enterprise systems.

Authorized access, reporting and ongoing use of content from business applications such as MS Outlook and SharePoint/O365 and database applications such as PeopleSoft and SAP ERP is managed in a uniform manner with reduced risk, complexity and cost.

Secure Content Management can help you:

- Preserve data and security through application retirement
- Balance requirements for collaboration, productivity, security and privacy at a lower total cost by leveraging existing investments through
  - Interoperability with business systems
  - Integration with MS SharePoint/O365
  - Automation
- Lower data security and privacy risks with data identification, masking, access controls, redaction and defensible disposal
- Reduce the cost of managing applications and data by
  - Removing the need for legacy applications to provide secure access and reporting on data

* © AIIM 2015, aiim.org—Industry Watch, Information Governance: too important to be left to humans

Contact us at **CyberRes.com**
Like what you read? Share it.

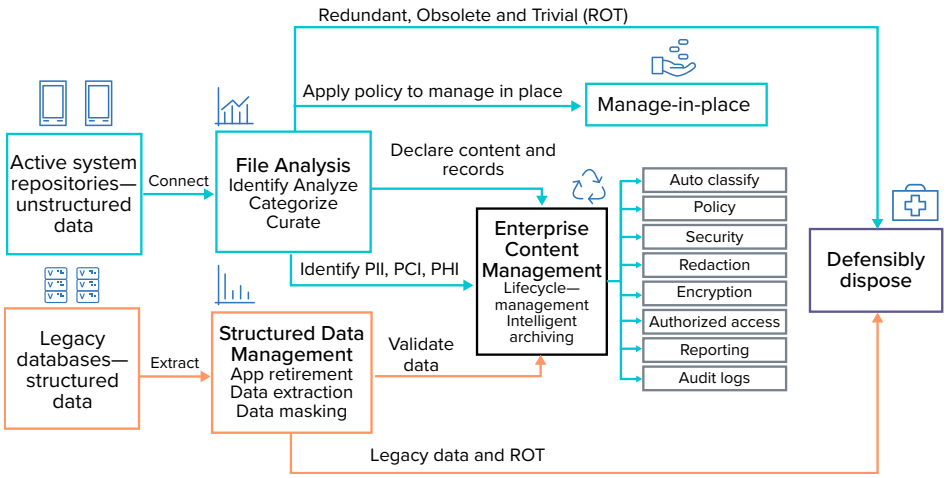

Figure 2. Secure Content Management components.

  - Simplifying the process for reporting across archived data
  - Centralizing control and access to archived data
- Reduce the cost and complexity of securely managing unstructured content with automation and integration

In simple terms the Secure Content Management suite allows you to get control, enhance compliance, improve productivity and lower cost for structured and unstructured content in both active and inactive systems.