Brochure

Find and Control Enterprise Content

ControlPoint

opentext™

ControlPoint: a Better Way to Manage Data

If your business is like most today, you store data in a number of systems and information repositories—an approach that has become the norm over the past two decades with rapid advancements in information technology. But as data volumes continue to increase, you face significant business risks and loss of efficiency because you simply can't control all the information contained in siloed repositories. Time is wasted looking for a specific document that has not been managed appropriately—and you may not be fully aware of what other information you actually have.

Key Benefits

OpenText™ ControlPoint helps you to:

- Gain visibility and understanding of business risk associated with information stored in enterprise systems and dark data.
- Automate compliance, legal hold, and retention management based on policy and the conceptual understanding of information across various file formats.
- Perform enterprise data cleanup and defensible disposal by identifying, categorizing, and applying policy to data across enterprise information repositories.
- Set policy to drive more secure management of valuable business content and records either in place or in a secure records repository.
- Better manage content based on business value and lifespan for both compliance and performance improvements.
- Drive your future information governance strategy with better business insight.

Identify, Connect, and Control Data across Your Systems

With OpenText™ Information Governance and file analysis solutions, you can connect and better manage the data in your systems to gain control over information assets across your enterprise. ControlPoint uses the Intelligent Data Operating Layer (OpenText™ IDOL) Connector framework to identify, analyze, and control diverse types of information stored in enterprise repositories and dark data. ControlPoint helps you to categorize and apply policy to content indexed by IDOL. A dashboard-style display provides valuable business insight into the themes, locations, and value of your information.

An advanced file analysis tool facilitating information governance for connected data sources, ControlPoint simplifies the definition and application of policy—regardless of data format or location. There is no need for source-specific policies, which become difficult to manage and unify across the enterprise, and no need for staff to learn multiple system tools and user interfaces. Role-based security allows you to delegate different tasks to reduce the likelihood of errors and bottlenecks, and can be used to control user access to repositories, policies, IDOL categories, and administrative tasks.

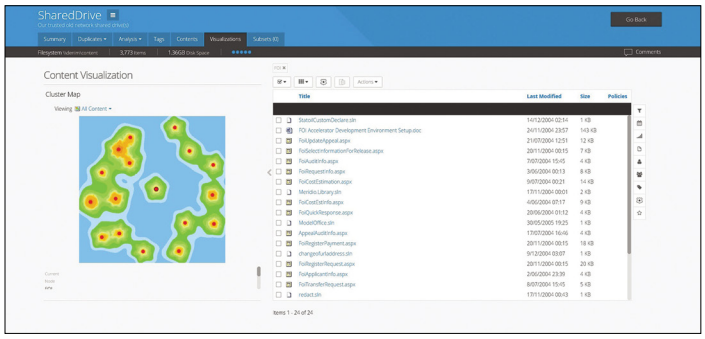

Figure 1. ControlPoint visualization page with 2D cluster map showing hot zones

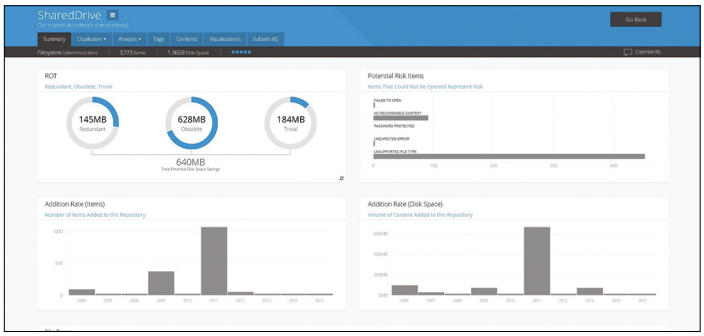

Figure 2. ControlPoint summary page displaying statistical summaries

ControlPoint provides a range of file analysis capabilities, including:

- Advanced, graphical visualization of information clusters based on meaning make it easy for executives to identify trends or popular concepts and themes.
- Two-dimensional cluster maps show heat zones of information grouped by concepts. You can click on the graph to see the underlying documents within that zone.
- Three-dimensional spectrographs display how clusters change over a period of time, and provide insight about the evolution of your enterprise information to use in training policies or in applying defensible disposal management rules.

ControlPoint summary pages present the analysis of indexed data graphically with statistical summaries and data categorization. This file analysis allows you to understand the breakdown of data types and categories across the enterprise or specific repositories. A range of tools and reports support a policy-driven and compliant clean-up process, enabling you to:

- Generate reports on items marked for deletion
- Maintain audit trails of policy selection criteria and execution
- Review and approve policy application and execution

Navigational tools allow you to drill down to explore different areas of policy application. For instance, a compliance officer can learn how much data is potentially on hold across all enterprise systems or what potential policy violations are occurring. Comprehensive reporting brings critical transparency to your compliance condition.

Using the IDOL Platform

IDOL works at the core of ControlPoint to index connected information, making it visible, transparent, and available to be analyzed, acted upon, controlled, and governed. Information sources such as file shares, SharePoint, and Microsoft Exchange are indexed through the IDOL connector framework. IDOL forms a conceptual and contextual understanding of the content, giving you the ability to index and analyze information from over 1,000 different content formats. IDOL's mature connector framework allows users to search across the entire enterprise using a Web interface, providing an unprecedented view of information assets and enabling searches that are compliant with FRCP requirements. IDOL also supports eduction or entity extraction so as to find personally identifiable information (PII), personal credit information (PCI) and personal health information (PHI) in documents and emails, etc.

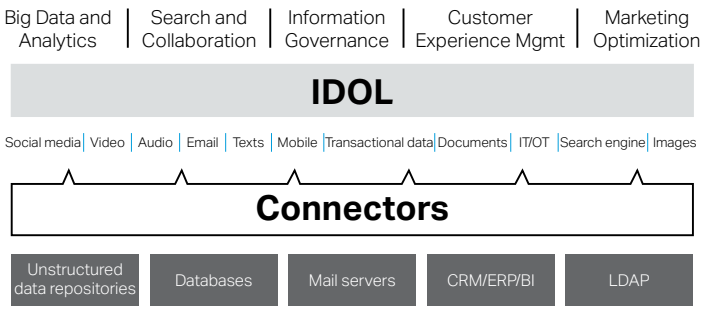

Figure 3. IDOL connectors make information accessible across devices and applications

IDOL Connector Framework

Through IDOL's connector framework, ControlPoint can access and analyze data from a range of sources—including dark data. Standard connectors provided with ControlPoint, include file shares, Microsoft SharePoint, Microsoft Exchange, and Content Manager.

Know Your Data for Better Insight and Better Decisions

Information contained in multiple systems and repositories provides little insight into business performance and practices if you don't manage it in a holistic manner. Siloed information provides tactical value to a small segment of the overall enterprise, but rarely delivers strategic value to executives or the enterprise as a whole.

The Emergence of Dark Data

Dark data is the data that you may not know you have. This currently unmanaged, often unknown electronic content resides in various repositories across the organization and is mostly human-readable, unstructured, unindexed, inactive, and orphaned. Proliferation of dark data can result from the bring your own device (BYOD) and Big Data trends that generate unstructured data types such as audio, video, and social media. Because so little is known about this dark data, it places your organization at risk.

Redundant, Obsolete, and Trivial Data

Your information footprint can be significantly reduced to provide measurable returns, if redundant, obsolete, and trivial (ROT) data can be identified.

- **Redundant data** consists of duplicates such as unauthorized copies of documents, emails, records, or database information residing in file shares, SharePoint sites, mail systems, and databases.
- **Obsolete data** consists of information that is no longer in use, or is out of date. When determining whether data is obsolete, you can identify its creation date, last modified date, or access date and then assess this information in conjunction with an appropriate retention policy.
- **Trivial data** is determined by file type, where the file type has no content value, such as executables, system files, and thumbnails.

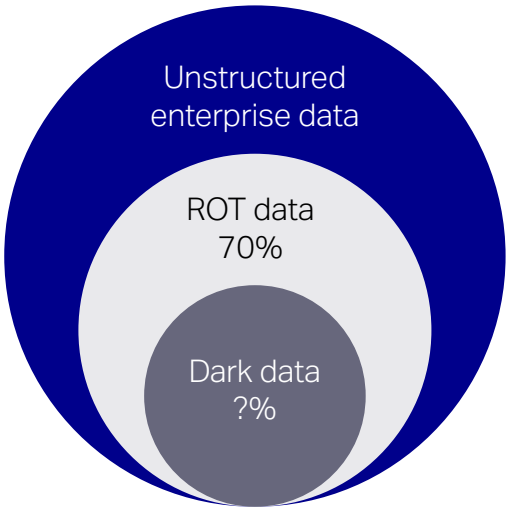

Figure 4. Unstructured enterprise data consists of: valuable content and records, ROT data and dark data

Defining ROT Data

Different areas of the business may have different definitions of what constitutes ROT; for example, the definition of obsolete data would vary greatly between the Finance and HR departments. With ControlPoint, you can define the criteria for ROT on a per-repository basis to better serve the needs of different business units. Detailed and targeted ROT analysis makes it easier and faster for information analysts to plan clean-up activities and provide the business with a more accurate assessment of its compliance state.

Clean Up to Reduce Cost and Risk

Once enterprise data is analyzed and identified by ControlPoint, you can begin the clean-up process to delete data with no business value (ROT) so you can reduce your information footprint, storage costs, and the data volume to be migrated to another system or to the cloud. Identifying dark data and assessing its value and sensitivity allows you to either delete it according to policy or migrate it into your Information Governance program for more secure management, reducing the risk of non-compliance and accidental or malicious misuse.

Enterprise Data Clean-Up

Organizations often look to enterprise data clean-up to address a number of information governance issues. The process may be undertaken as a standalone activity to address a specific problem such as onboarding applications and information acquired during merger and acquisition activities. It may also be part of an ongoing business project to improve efficiency and reduce information footprint. Another use is to gain greater insight into data holdings and the categories they fall into, helping to inform a suitable information governance plan.

ControlPoint lets you analyze and tag data in system repositories so that policy can be applied and appropriate action taken for defensible disposal or ongoing management. ControlPoint conducts analysis on a range of data attributes, including date fields, file properties (type and size), creator, category matching, custom fields, and duplicate assessment against defined masters. The process consists of five stages moving from identification, through to policy application and action.

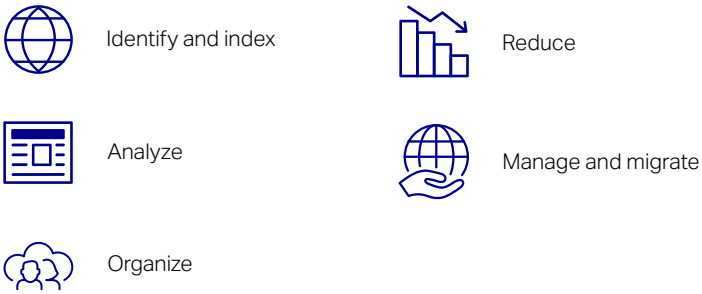

Figure 5. The five stages of enterprise data clean-up with ControlPoint

Streamlining Data Migration and Preparing for the Cloud

The process of identifying and deleting data with no business value not only improves day-to-day search and retrieval efficiency, but can also positively impact your data migration projects. You can reduce the volume of data and the number of systems to be migrated, and simplify the process of data tagging, mapping, exporting and importing. This reduces the duration and complexity of the migration project and the time it takes to be fully operational again. For cloud initiatives it is paramount to clean your data prior to migrating it, to maximize the cost savings and return on investment promised by cloud. This process can reduce the volume of data migrated and the associated amount you pay for cloud storage. With the cloud options available today coupled with data security and privacy regulations you want to make sure you migrate the right data to the right cloud. A public cloud offering may not be suitable for highly sensitive or personal data so you want to ensure that this data is correctly identified and not accidentally migrated to a public cloud but instead moved to your private cloud solution.

In addition to removing data of no value, ControlPoint can also identify valuable data that meets the criteria for migration to another system or secure repository, categorizing it and applying policy to help ensure it is migrated accordingly. ControlPoint helps you accurately and efficiently migrate data by reducing the manual tasks of identification, tagging, and mapping.

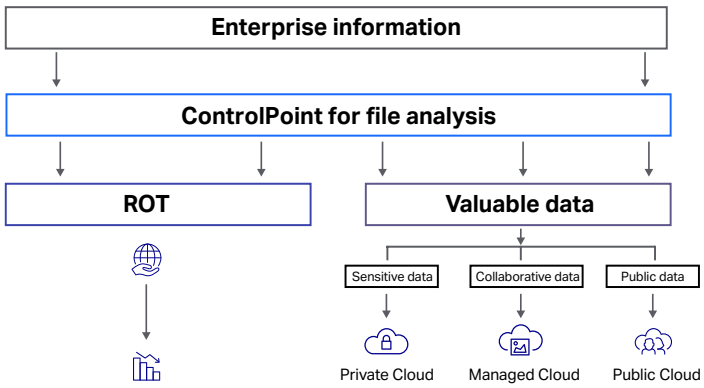

Figure 6. Determining which data is suitable for which cloud

Enhancing Information Governance and Control

The risk of non-compliance can be high for organizations with information silos or SharePoint site proliferation. In these scenarios, there is a high risk of creating volumes of inactive enterprise data and dark data. However, approaching each challenge separately is costly and leads to a disjointed information governance implementation that is likely to have gaps. Using IDOL's unified and consolidated view of enterprise repositories via its connectors, ControlPoint can apply standardized policies from a central policy engine. In this way, your data can be effectively managed through a central information governance tool.

ControlPoint offers policy-driven categorization, auto-declaration, manage-in-place capabilities, and seamless integration with Content Manager software to help you bring information under control within a robust information governance framework.

Meet the Demands of Regulation with Reduced Risk

Meeting internal governance and regulatory compliance requirements and responding to legal discovery, external investigation, and audit inquiries are challenging business obligations. Non-compliance is a risk that could result in financial penalties, interruption to your business operations, and negative publicity, which means it is essential to adopt a proactive approach to information management. With a proper program in place, you can foresee areas of risk and address them before they become real problems.

Records Management and Defensible Disposal

Many organizations keep their content well beyond its expiration date or inadvertently delete valuable business documents. These information management practices often result from disconnected information silos, a lack of understanding about what content exists and where, poor policy application and enforcement, and a lack of information security. ControlPoint allows you to manage and dispose of content wherever it resides on subscribing systems, or declare the content as records and move them to Content Manager for ongoing, policy-driven and compliant management.

Seamless Integration with Content Manager

Integration with Content Manager facilitates robust, compliant, governance-based content management for declared business content and records. ControlPoint's auto-declaration capability simplifies the flow of content from enterprise systems into Content Manager.

ControlPoint with Content Manager provides full document and records management functionality, automating the retention and disposal of this information. Content Manager applies security to manage and provide controlled access to corporate records in business context, ensuring authenticity, integrity, and reliability.

A range of audit logs and reports supplied out of the box, allows you to keep a defensible history of policy changes as well as the effects of policy application to managed content. These reports, which can be either user-driven or automated, help you monitor the application and effect of policies on your information. Content Manager manages content according to applied retention schedules with event triggers, to simplify its management and defensible disposal.

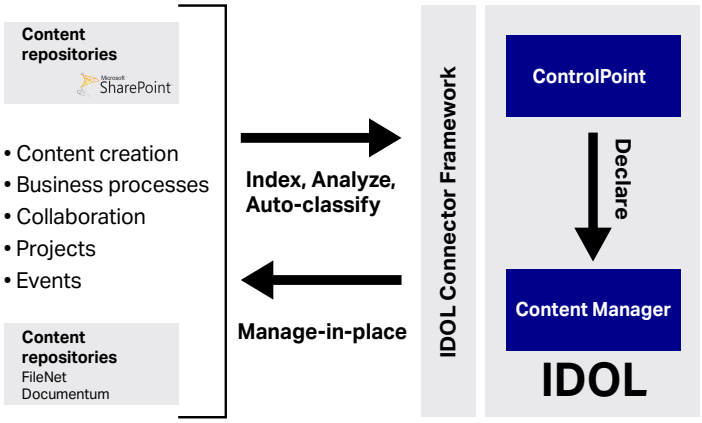

Figure 7. Manage-in-place with ControlPoint and Content Manager reduces

Increase Efficiency and Productivity through Automation

ControlPoint automates the consistent application of policy to content based on a conceptual understanding of information in a multitude of file formats. Additionally, you can use document/location metadata to assign policy, and you can automate information policy enforcement and audits.

Train ControlPoint Categories

The ability to train ControlPoint categories based on existing IDOL categories or content within Content Manager removes much of the burden of having users manually create or map categories. A selection of documents from system repositories is used for training and benchmarking, ensuring categories are based on meaningful concepts and real business context. This capability improves the efficiency and accuracy of categories and the application of policy to content.

You can prepare draft categories without affecting documents in production systems and refine and test them to determine the impact they are likely to have on enterprise documents. You can refine a category by adjusting the weighting of a term, the selection threshold, or by adding field text. These activities can be done individually or in combination. The category can be published, making it available for use in automatic policy execution against content managed by ControlPoint.

Automate Categorization

Categorization is critical to the application of policies. Traditional collaboration and ECM systems rely on users to categorize and tag information on an individual basis, but ControlPoint uses IDOL to analyze information, arranging it into self-similar groups or clusters and matching the data against trained categories. Through duplicate and near-duplicate identification, storage costs are reduced while documents identified as records can be declared into Content Manager. You can file content using a single click, or you can automatically classify it based on rules and the system's understanding of the concepts and context contained in the documents.

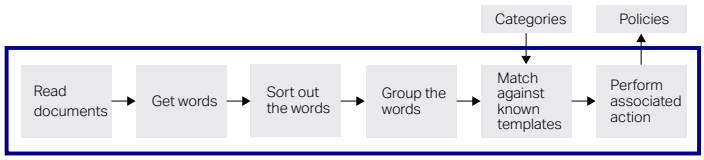

Figure 8. Simplified view of the categorization pipeline

Automate Policy-Driven Classification

Once data is categorized, you can apply policies for ongoing management. Policies can be created with keywords, metadata, and/or example documents using a simple wizard-rich dashboard. Policy creation is intuitive and allows automatic enforcement. Policies can be linked to the classification scheme within Content Manager, ensuring the appropriate retention and disposal schedules are applied to declared records.

ControlPoint enables you to:

- Automate policy application to govern the information lifecycle, including deletion prevention, storage management, and ultimately disposition management by applying meaning-based policies at data creation
- Rely on a user-friendly dashboard to create policies
- Deduplicate data across repositories to reduce storage costs and reduce discovery times

Manage-in-Place

ControlPoint gives you the flexibility to perform specific actions on content in place. These in-place capabilities simplify the management of enterprise content according to business value and lifespan, making it easy to identify and categorize content from any subscribing system. Then, based on policy, you can move the content into an enterprise content management system (Content Manager), the archive, or indicate it as ready for destruction.

ControlPoint uses IDOL indexes and categories to apply policy to information via the connector framework. The policy can dictate a number of actions to be carried out, including:

- Hold
- Release hold
- Copy
- Secure copy
- Move (between repositories)
- Apply tags
- Delete
- Declare record
- Secure link/shortcut

You can move content that has not been accessed for a defined period of time to more cost-efficient storage, eliminating the need to license costly SQL servers in SharePoint environments (inactive SharePoint sites) and alleviating the strain on network resources. Both of these capabilities can bring substantial savings.

You can also check email that falls under an automatic clean-up rule to see if it matches a records category before deletion, minimizing the risk of important information being deleted inadvertently if the user hasn't actively declared it as a record. The efficient management of these information platforms throughout their lifecycle greatly reduces storage and infrastructure costs.

Three Choices for Deploying ControlPoint

ControlPoint and its advanced file analysis capability offer you three pathways to information governance:

- You can implement ControlPoint to provide a snapshot of information contained within enterprise repositories to inform your information governance strategy for the future.
- You can implement it to identify, categorize, and apply policy to facilitate the deletion of content with no value to solve a specific problem and serve as a point solution.
- You can use it to support an end-to-end approach to information governance so you never lose valuable content again. Continuous monitoring of enterprise repositories for unmanaged content lets you identify and categorize, then apply policy to facilitate manage-in-place, defensible disposal or migration.

Learn more at
www.microfocus.com/controlpoint
www.microfocus.com/opentext

Connect with Us

OpenText CEO Mark Barrenechea's blog

opentext™