Osterman Research

WHITE PAPER

White Paper by Osterman Research
Published **January 2022**
Sponsored by **Micro Focus**

Does a Microsoft-Only Approach to Information Governance Make Sense?

Executive Summary

As organizations explore new cloud services for productivity and collaboration, mature information governance capabilities do not become less important. Microsoft and various other third-party vendors offer capabilities for governing information, albeit with strengthens in different areas. Ensuring the right information governance capabilities are available to the various organizational groups with shared responsibility for this area is essential.

This report compares and contrasts the respective approaches to information governance in Microsoft 365 and what Osterman Research considers to be best practice. It is offered to enable professionals with responsibility for information governance evaluating the move to Microsoft 365 to gauge suitability to task of the information governance tools offered by various vendors.

This white paper is intended for IT professionals, cybersecurity teams, compliance and risk professionals, and legal teams – including CISOs, CIOs, general counsel and others who need to gain a better understanding of information governance, particularly in the context of how they will handle information governance in Microsoft 365 environments.

This report compares and contrasts the respective approaches to information governance in Microsoft 365 and what Osterman Research considers to be best practice.

About Information Governance

Organizations face the relentless growth of both structured and unstructured information. While structured information is stored in curated database containers, unstructured information – the emails, documents, files of all kinds, conversation transcripts and chat messages that make up at least 80 percent of the information volume in an organization – are scattered across multiple data repositories, devices and cloud services. Few organizations have a strong grip on the fundamentals of governing this burgeoning collection of unstructured information, even though an increasing proportion of organizations across the world face privacy and other compliance regulations that demand heightened care.

For the purposes of this paper, "information governance" covers the processes that focus on:

- Determining the types of information that exist across the organization's datascape, classifying it properly, and weeding out the fluff from that which requires special protections.
- Deciding what information needs to be kept beyond its initial, ephemeral point of creation, and how to store and otherwise manage it.
- Ensuring that only authorized individuals have access to different groupings of data, including the ability to audit access and mitigate over-exposure through automated mechanisms.
- Providing the ability to audit communication for compliance.
- Filtering through the various repositories of data to identify specific data elements that are potentially responsive to an eDiscovery request (including things like regulatory audits), and excluding all irrelevant data before creating a collection for external review.

Different Fundamentals

Every successful organization has a rallying cry: a vision, a mission, a purpose. The rallying cry of each organization infuses product and service decisions, dictates employee hiring profiles, and defines how well they are likely to serve specific customers. The shape of go-to-market strategies and product decisions across comparable organizations are heavily influenced by these fundamentals. A comparative awareness of how different organizations define their fundamentals assists in deciding which is better placed to address specific customer requirements. Figure 1 offers a high-level comparison of best practice vs. Microsoft's approach to information governance (which may be best practice in some cases).

Figure 1
Best Practice vs. Microsoft Approaches to Information Governance

	Best Practice	Microsoft
Product Focus	Products that enable effective information governance—supporting customers across multiple platforms and data repositories.	Any product that could help a person or organization "achieve more," including collaboration services, productivity tools, enterprise servers, developer tooling, cloud services, mobile apps and even gaming.
Approach to Retaining Customers	Offer best-in-class tools that enable customers to work across a diverse and heterogeneous data landscape, using open formats to eliminate vendor lock in.	Offer a broad selection of tools that can meet the generalized needs of several billion people, using Microsoft-controlled file formats to discourage mobility between vendors.
Belief About Classification	Information governance professionals in security, compliance and legal are best placed to classify content sensitivity, including retroactive classification and reclassification.	The individual creating the content is best placed to classify its sensitivity at the point of creation. This can make the job of information governance professionals more efficient.

Source: Osterman Research (2022)

Are you comfortable with porting and storing all your data in Microsoft's cloud services?

When evaluating vendors to support information governance solutions, consider:

- **Industry factors**
  Are you in a highly regulated or highly litigated industry?
- **Classification approach**
  Does your organization require a focused and detailed approach to managing, protecting and classifying data for information governance, or is a more general, broader approach good enough?
- **Repository diversity**
  Are you comfortable with porting and storing all of your data in Microsoft's cloud services, or do you prefer a blended and heterogenous strategy?

Information Governance: What Information Exists?

Identifying, cataloguing and classifying the information that exists within an organization's data repositories is an early and essential task in information governance. Data specialists are likely to have a sense of what information is likely to exist, but an automated analysis of what really exists removes any uncertainty. A strong analysis of what information exists underpins each of the successive aspects of information governance.

There are various approaches to the discovery task, but important differences are evident, as shown in Figure 2.

Figure 2
Approaches to Consider in Data Discovery and Data Mapping

Best Practice	Microsoft 365
Connects with multiple repositories, both on-premises and in the cloud, including but not limited to Microsoft 365. Works across data repositories, services and file formats.	Focuses on the data stored in Microsoft 365 workloads (e.g., Exchange Online, SharePoint Online, Teams chats, etc.), and contained in supported Microsoft file types. Organizations with the higher-priced Microsoft 365 plans also gain access to data discovery capabilities for multiple cloud services (through Microsoft Cloud App Security) and on-premises Microsoft data repositories and file shares (through Azure Information Protection).
Sensitive information, specifically PHI (health), PII (identity) and PCI (financial), can be detected using machine learning algorithms across multiple repositories. The algorithms use keyword, pattern and regex matching as one of several inputs; and support confidence levels. If required, classified data sets can also receive a Microsoft label.	Approximately 100 sensitive information types are used to analyze and label content in files and email messages. Many of the types are country- and region-specific. The types rely on keyword and regex matching, along with confidence levels.
Identifies and classifies ROT (redundant, obsolete and trivial) information. Focus is on reducing the storage of ROT and determining cost levels for departmental chargeback.	Identifying ROT is supported when migrating data repositories to Microsoft 365, but few options are provided for ongoing analysis. Key focus is on storing everything in Microsoft 365; the structured removal of ROT is a far lower priority.

Source: Osterman Research (2022)

Identifying, cataloguing, and classifying the information that exists within an organization's data repositories is an early and essential task in information governance.

When evaluating the move to Microsoft 365, it is essential that decision makers ask the following questions:

- **Repository diversity**
  Does your organization have diverse data repositories? Tools that support more than just Microsoft 365 will be essential if repositories beyond Microsoft 365 will continue to be used.

- **Vendor effectiveness**
  How effective have respective vendors been in classifying your sensitive information across the data corpus, for both on-premises and cloud-based repositories?
- **Finding ROT**
  How actively is your organization required to identify and remove ROT across all data repositories?
- **Capabilities of Microsoft 365 plans**
  Does the Microsoft 365 plan your organization intends to purchase include data discovery capabilities for multi-cloud and on-premises analysis, or will a higher-priced plan be required to obtain these capabilities?
- **Time and cost to migrate data to Microsoft 365**
  What level of time, effort and cost will be required to migrate terabytes or petabytes of data to Microsoft 365 if migration is necessary?

Information Governance: What's Kept? What's Not?

Determining what information must be retained—and what can be defensibly deleted immediately or at a pre-scheduled point in the future—impacts data volumes, storage requirements, backup costs and approaches, and even the threat quantum from cyber criminals. Systematic analysis of data for erasure, based on regulatory-appropriate criteria, is essential.

There are different approaches to questions of retention and deletion, as shown in Figure 3.

How effective have respective vendors been in classifying your sensitive information across the data corpus?

Figure 3
Different Approaches to Retention and Deletion

Best Practice	Microsoft 365
Emphasize the systematic analysis for and removal of ROT, which is estimated to make up 40% to 70% of all content. Removal of ROT streamlines what data is retained, thus reducing litigation risks, the attack footprint against sensitive data, and storage costs. It eliminates information with no ongoing business value.	Microsoft emphasizes its options for unlimited storage and self-expanding archival services against in-place in Microsoft 365. However, having a separate backup of email, document and file data outside its source, including the Microsoft cloud, should be a key decision point for information governance professionals.
Reports on ROT provide detailed analysis to support collaborative decision-making on ROT removal among the various organizational groups with shared responsibility for information governance (e.g., IT, legal, risk and compliance, data security and business groups)	A general statement on the existence of ROT when migrating data into Microsoft 365 provides unilateral power for an IT administrator to act, without shared decision-making with other groups with vested interests and regulatory responsibilities
Address the information lifecycle for both essential information that must be retained and ROT that can be erased to reduce the data footprint and security/legal exposure	Microsoft 365's Data Governance capabilities focus on applying retention labels to content that must be kept for a pre-scheduled duration (or subject to an event happening at an unknown point in the future), but largely ignores the rest of the data corpus, much of which is ROT. Users are expected to select the correct retention label
Creates a separate backup of email, document and file data for long-term retention and archival. Archived data is stored in a non-editable format, signed and held in a separate location from the original source	Archival is managed through retention and deletion rules for data stored in place in Microsoft 365. A single source architecture in Microsoft 365 for current and archived data means that incorrect classification of pertinent email, document and file data leads to indefensible early deletion

Source: Osterman Research (2022)

Many organizations have poorly organized file servers with decades worth of unstructured data in a complete tangle.

When evaluating the move to Microsoft 365, consider the following questions:

- **Identify non-essential data**
  Do you currently have a way to identify non-essential data across multiple data repositories for defensible deletion?
- **Future ROT**
  How will you identify future ROT for defensible erasure, so as to ensure that what must be retained is kept in protected locations while trimming all that is unnecessary?
- **Verifying user classification**
  If users are selecting the retention label, how will classification decisions be verified to ensure users haven't just chosen the longest rate so as to keep their data for as long as possible?
- **Archival approach**
  Will an in-place archival or separate archival approach better enable you to meet your compliance and legal obligations?

Information Governance: Who Has Access?

Without a strong approach to governing who has rights to access the data stored within the organization's data corpus, the threat of insider data breaches through inadvertent data access is high, along with flow-on negative effects of credential compromise by cyber criminals. Many organizations have poorly organized file servers with decades worth of unstructured data in a complete tangle, and it's no different with modern collaboration tools introduced using viral adoption and poor information architecture. For example, the Share button in Microsoft 365 is fundamentally flawed since there are few provisions to prevent sharing of content within the organization to users who should not have access to that content, and both access validation and automatic revocation of access rights is missing. Mitigating the mess and planning a new path forward relies on auditing data access, along with automated content classification for reviewing the appropriateness of content access, and also automated remediation capabilities to revoke inappropriate levels of data access.

There are different approaches that will enable organizations to improve data access governance, as shown in Figure 4.

Figure 4
Various Approaches to Data Access Governance

Best Practice	Microsoft 365
Scopes data access analysis across data repositories, both on-premises and cloud-based	Scopes data access analysis across applications where identity and access are managed through Azure AD (Azure Active Directory); requires Azure AD Premium P2 licensing
Offer a user-centric analysis of the data that people are able to access (including access levels or rights), along with automated remediation of inappropriate access privileges	Azure AD Access Reviews provides a group-centric method of certifying whether each group member should still have access to a specific Microsoft 365 Group. Azure AD Entitlement Management provides for policy-based provisioning and deprovisioning of access. There are no provisions for to prevent "sharing" of content with users who shouldn't have it, it is not possible to validate why somebody has access to data, and access is not revoked after something changes to make ongoing access inappropriate.
Presupposes that existing access rights across multiple repositories are a tangled mess, and provides the tools for initial clean-up and ongoing monitoring and remediation	Presupposes that a well-ordered access approach to Microsoft 365 already exists, and provides the tools to keep it that way

Source: Osterman Research (2022)

When evaluating the move to Microsoft 365, consider the following questions:

Does the Microsoft 365 plan your organization intends to purchase include the Azure AD data access capabilities, or will a higher-priced plan will be required?

- **Access rights currency**
  How current are the access rights to data across your multiple repositories, particularly for those that will not be migrated to a workload in Microsoft 365 that is managed by a Microsoft 365 Group?
- **Capabilities of Microsoft 365 plans**
  Does the Microsoft 365 plan your organization intends to purchase include the Azure AD data access capabilities, or will a higher-priced plan will be required?
- **Splitting data during divestiture**
  How will data rights be enforced correctly in divestiture situations, since relying on security inheritance is unreliable—because inheritance rules are interrupted or broken when sites are divided?

Information Governance: What's Responsive? (eDiscovery)

When facing litigation, a data subject access request under new data protection regulations, or even an employee complaint of malfeasance by a senior leader, the ability to quickly, appropriately and accurately discover the presence of data relevant to the case is essential. Charges of wrongdoing can be quickly verified when the right data is located, and in cases where evidence shows the charges to be erroneous, an alternative pathway to a resolution proposed.

Microsoft 365 offers eDiscovery capabilities for organizations, but there are important differences in scope, speed and design between their offerings and what we consider to be best practice, as shown in Figure 5.

Content searches should use standard indexing processes for quick and responsive presentation of search results.

Figure 5
Best Practice vs. Microsoft eDiscovery Capabilities

Best Practice	Microsoft 365
eDiscovery is scoped to work across multiple on-premises and cloud-based data repositories simultaneously, interacting with data in-place to determine responsiveness to a case	eDiscovery is scoped to workloads in Microsoft 365 only, or if Advanced eDiscovery in the higher-priced plans is used, to any data that has also been imported into an Azure container for the case
Content searches should use standard indexing processes for quick and responsive presentation of search results	Content searches in an eDiscovery case force a re-indexing of all selected data locations in Microsoft 365 for a custodian, adding time and slowing discovery processes
Emphasis is on pre-processing potentially responsive content to remove irrelevant data through in-place content review. Only responsive content is assembled for external legal review, so as to substantially decrease the cost of the external review process	eDiscovery search results do not offer the ability to pre-process potentially responsive content. Search results must be exported before they can be reviewed
Legal holds on responsive content are created by safeguarding data in a separate tamper-proof repository for each case. Multiple legal holds can be applied to the same content	Responsive content is put under legal hold wherever it is stored in production Microsoft 365 workloads. Multiple legal holds can apply to the same content and the same workload for a custodian

Source: Osterman Research (2022)

When evaluating the move to Microsoft 365, decision makers should consider the following questions:

- **Repository diversity**
  How many different data repositories holding information that will be subject to eDiscovery searches exist across the organization?
- **Unified eDiscovery**
  How important is the ability to search across all repositories through a single eDiscovery interface (as opposed to requiring separate, disjointed searches using multiple eDiscovery platforms)?
- **System responsiveness**
  How much waiting time does an eDiscovery manager face when creating, configuring and executing cases in the respective eDiscovery systems offered by both vendors?
- **Legal hold approach**
  What is your preference for creating legal holds: a separate repository of responsive information for each legal hold, or an in-place approach that locks production data?
- **External legal counsel costs**
  What cost savings would you achieve by reducing the volume of content subject to review by external legal counsel by half?
- **Downgrading Microsoft 365 plans**
  An organization may decide at some point that it has overprovisioned some or all of its users, such as by providing them with Microsoft 365 E5 instead of E3, and so may opt to "downgrade" these users to reduce its costs, or because the organization has opted to use a third party's information governance, security or other capabilities. While it is not explicit in the Microsoft licensing terms, downgrading an online Microsoft 365 plan is extremely difficult, if not impossible.

While it is not explicit in the Microsoft licensing terms, downgrading an online Microsoft 365 plan is extremely difficult, if not impossible.

Information Governance: Endpoint Backup

Employees engage with enterprise data through a myriad of endpoints—laptops, smartphones, and tablets. They create enterprise data, store it, share it, access it, and make modifications to it. An endpoint is a facilitator of productive work and the gateway to the intellectual property storehouse of the organization. Many work processes in the modern organization have been designed based on the availability and capabilities of endpoints.

Endpoints are also a risk and threat vector. Lost or stolen devices result in loss of capability to work—and data breaches. Ransomware attacks lock data and documents from usage, rendering devices useless and unique data inaccessible. Data responsive to eDiscovery requirements and internal investigations is scattered across network servers, cloud services, and endpoint devices, and while the first two are generally easy to search, securing physical access to a custodian's endpoint device is a more difficult and expensive proposition. Safeguarding the endpoint as an enabler of productive work and protecting the data stored on endpoints are critical considerations in enterprise IT strategy.

Microsoft offers OneDrive for synchronizing some content in Office 365 with an endpoint. Any content not stored in OneDrive is excluded from wider information governance responsibilities. This is different to what we consider best practice, as shown in Figure 6.

Figure 6
Endpoint Backup Best Practice vs. Microsoft Capabilities for OneDrive Sync

Best Practice	Microsoft 365
Policy-based enterprise endpoint backup solutions safeguard all the data on an enrolled endpoint, offering a succession of historically accurate restore points	Content in OneDrive and SharePoint can be synchronized to an endpoint for simple access and document collaboration.
Data retention on endpoints is a policy-based decision. All endpoint data is captured and preserved.	Individuals can avoid data retention requirements by simply storing documents outside of the OneDrive folder hierarchy.
Compliance with organizational policies is "set and forget."	The ease of storing content outside of OneDrive means that the organization's compliance posture is best described as "set and worry continually."
Defensible and systematic capture of data to support eDiscovery and enterprise search requirements includes all endpoint data by design	Data stored on endpoints outside of the OneDrive sync hierarchies are excluded from eDiscovery and enterprise search, creating areas of dark data
Organizations can define how long deleted files should be kept available in historical backup data sets using a policy-based enterprise endpoint backup solution, providing a defensible and systematic means of supporting compliance and litigation requirements	OneDrive automatically captures deleted files in a couple of tiered duration recycle bins, enabling files to be recovered after several months of being deleted. But once the file is actually removed from the second stage recycle bin, it is unrecoverable

Source: Osterman Research (2022)

When evaluating the move to Microsoft 365, decision makers should consider the following questions:

- **Employee compliance with data retention policies**
  What percentage of employees never make careless mistakes, protect nascent ideas by storing them outside of OneDrive, and never deliberately do anything wrong?
- **Employee efficacy at maintaining endpoint backups**
  What percentage of employees are regularly and consistently backing up their endpoint to a local backup drive? How easy is it to gain access to that backup drive if an endpoint was compromised, lost, or stolen?
- **Cost of recovering a lost or compromised device**
  If policy-based enterprise endpoint backup is not used, what is the productivity loss and help desk cost of recreating a device after one is compromised, lost, or stolen?
- **Sync-only versus capturing everything on an endpoint**
  Does the business risk of using sync-only for OneDrive outweigh the cost of a policy-based enterprise endpoint backup solution?

Endpoints enable productive work and connect employees to the organization's intellectual property. Endpoints are also a risk and threat vector.

Cost Model

We produced a cost model for this white paper for the following 1,000-user environments:

- Microsoft 365 E5 using only the eDiscovery and compliance capabilities provided within that platform. The monthly, per-user cost is US$57.00
- Microsoft 365 E3 using a third-party eDiscovery and compliance platform. The monthly, per user cost is US$32.00 for Microsoft 365 E3 and US$20.00 per month for the third-party eDiscovery and compliance platform.

For purposes of analyzing the costs of information management, we have assumed that there will be three key requirements of an information governance system for either environment, although the first two elements are quite small relative to eDiscovery and compliance costs and so have little impact on overall costs:

- Storage and management of emails
- Storage and management of files
- Management of eDiscovery and compliance processes

We have made assumptions about the volume of email and files generated by employees per day, annual growth in the number and size of emails and files, the cost of Tier 1 and Tier 2 storage in an Azure environment, the length of time that files must be retained, and the investment of time required to manage the eDiscovery process. With regard to the last point, we have made the following assumptions for the two environments:

- 50 eDiscovery searches per year
- 10 content repositories that must be searched per eDiscovery effort

For the Microsoft 365 E5 environment, we have assumed that IT staffers will need to invest 12 hours per data repository per eDiscovery effort, that 10 percent of the files will be responsive to each eDiscovery effort, and that reviewers can process an average of 50 culled documents per hour. However, for the Microsoft 365 E3 environment with a third-party eDiscovery and compliance platform, we have assumed three important differences because of the greater efficiency of the third-party platform:

- IT staffers will need to invest only four hours per eDiscovery effort per data repository because of better search performance and process management in the third-party solution.
- A smaller set of files will be culled for review because of improved search capabilities across a larger set of indexed file types, resulting in a 10 percent improvement, or a cull rate of nine percent.
- The use of more efficient review workflow capabilities will result in a 10 percent improvement in the average number of documents that can be reviewed per hour.

Based on these assumptions, we find that there are significant differences in the costs associated with Microsoft 365 E5 and Microsoft 365 E3 in combination with a third-party eDiscovery and compliance platform, as shown in the figures below.

We find that there are significant differences in the costs associated with Microsoft 365 E5 and Microsoft 365 E3 in combination with a third-party eDiscovery and compliance platform.

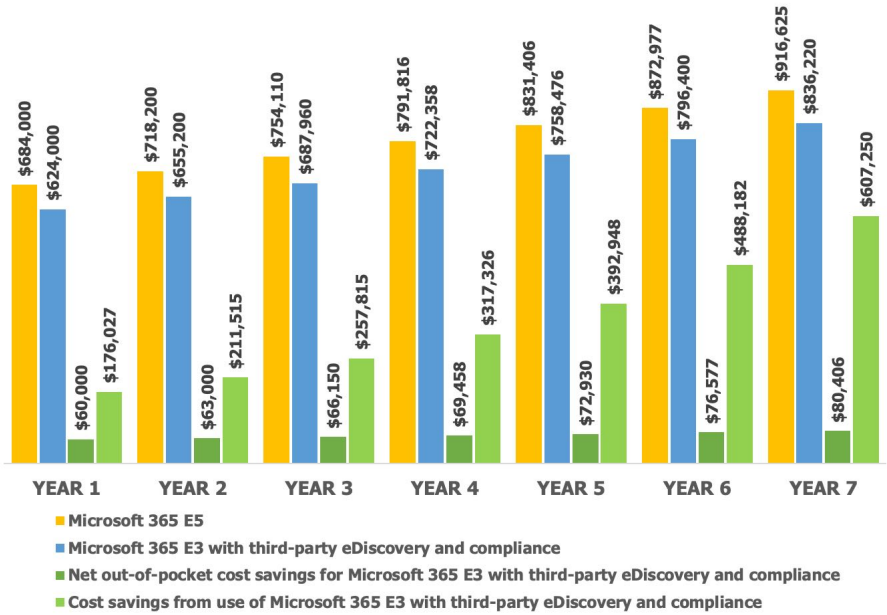
The monthly, per-user costs for Microsoft 365 E5 and Microsoft 365 E3 used in conjunction with a third-party eDiscovery and compliance platform are shown in Figure 7.

Figure 7
Monthly, Per-User Cost

Source: Osterman Research (2022)

Figure 8 shows the costs and cost savings for a 1,000-user organization over the seven-year retention period assumed in the cost model. While there are modest savings from the use of the less expensive Microsoft 365 platform, the more significant savings are the result of a) less time spent by IT staffers on managing the eDiscovery process, and b) the greater efficiency for content reviewers resulting from fewer culled files and faster review.

Figure 8
Annual Costs and Cost Savings



Source: Osterman Research (2022)

Having mature capabilities available to address information governance responsibilities reduces data risks, decreases security exposure, and increases productivity.

Implications for Practice

For mid-market, regulated firms, having mature capabilities available to address information governance responsibilities reduces data risks, decreases security exposure, and increases productivity for those responsible for various aspects of information governance. Benefits include:

- **IT professionals**
  For IT professionals, the ROT analysis reduces long-run storage and backup costs, while automated monitoring and remediation capabilities streamline ongoing processes, enabling IT professionals to invest in other strategic business technology initiatives.
- **Cybersecurity teams**
  For cybersecurity teams, the ability to reduce vulnerabilities across the potential attack surface. One example is by tightly governing data access rights, the effects of insider data breaches and credential compromise via a phishing or spear-phishing attack are minimized.
- **Compliance and risk professionals**
  For compliance and risk professionals, reliable identification of sensitive and personal data across all data repositories, including automated remediation of data stored in the wrong place.
- **Legal teams**
  For legal teams, faster identification of responsive material to assist with early case assessment, along with the ability to cull irrelevant materials before sending a collection for external review, hence saving significant litigation fees.

While Microsoft 365 offers some capabilities for information governance, the product offerings from some third-party vendors complement and extend what Microsoft offers, as well as addressing critical areas that have not been fully addressed in Microsoft's tools.

Microsoft 365 is a compelling cloud service offering, but due to organizations continuing to use multiple data repositories both on-premises and in various cloud services, having access to an integrated offering for information governance is essential. Organizations should examine their information governance needs, and look to third-party providers to complement and extend what Microsoft offers, as well as addressing the critical areas ignored in Microsoft's tools.

For mid-market, regulated firms, having mature capabilities available to address information governance responsibilities reduces data risks, decreases security exposure, and increases productivity.

Summary

Figure 9 summarizes some of the important differences that decision makers should consider when evaluating the native Microsoft 365 tools for information governance versus third-party tools.

Figure 9
Summary of Microsoft 365 and Third-Party Information Governance Offerings

Consideration	Third-Party Solutions	Microsoft
Data Repositories	Diverse, non-Microsoft repositories on-premises and in the cloud, including Microsoft's offerings	Microsoft 365, SharePoint on-premises and Microsoft file servers
eDiscovery Search Scope (for litigation, subject access request, or internal audit)	Microsoft 365 and other, non-Microsoft solutions	Microsoft 365 only
eDiscovery Search Time	Faster as a result of reliance on pre-indexed custodial locations	Slow as a result of re-indexing all custodial locations
Costs for External Legal Counsel	Lower as a result of greater culling of non-responsive material	Higher as a result of less culling of potentially responsive material
Legal Hold	Copies responsive material from multiple data repositories to a legal hold repository	Locks responsive material in source Microsoft 365 workloads
Access Rights	Assumes access rights need initial clean-up and ongoing management, including automated remediation	Assumes access rights are well-governed, and that data owners will maintain accuracy
Backup	Creates separate backup of email, documents and data for governance, retention, archival and recovery	Email, documents, and data are not backed up; original source only
Future migration to non-Microsoft platforms	Less difficult and less time-consuming because data sources and information governance are from different vendors	Difficult and time-consuming because of reliance on Microsoft for data management and information governance

Source: Osterman Research (2022)

For regulated organizations that are Microsoft-centric and at which eDiscovery cases are an infrequent occurrence, a Microsoft-only approach makes sense. When these conditions are not true for regulated organizations, complementing Microsoft's capabilities with third-party information governance tools provides a "better together" experience.

Complementing Microsoft's capabilities with third-party information governance tools provides a "better together" experience.

Sponsored by Micro Focus

Micro Focus is a global enterprise software company that provides the critical software you need to build, operate, secure, and analyze your enterprise in the race to digital transformation. The company's Information Management & Governance product group is designed to help organizations acquire data governance insights, streamline policy implementation, automate compliance monitoring, and protect information from creation to destruction. Within this product group, the Micro Focus Archiving and Risk Management Portfolio provides information governance, automated archiving, and supervision solutions for organizations of all sizes to access, govern, search, analyze, and centrally manage data. The Secure Content Management Portfolio enables organizations to discover, protect, and manage sensitive data across its lifecycle while reducing risk, complexity, and cost. Micro Focus IDOL provides unstructured data analytics for organizations that need to extract maximum value from all their text, audio, video, and image data. Finally, Micro Focus Data Protector provides backup and disaster recovery solutions for diverse, dynamic, and distributed enterprises. One of the world's largest enterprise software providers, Micro Focus generates $3.0 billion in annual revenue and serves over 40,000 customers worldwide, including 98 Fortune 100 companies. Micro Focus is headquartered in Newbury, United Kingdom.

www.microfocus.com

@MicroFocus

+1 877 686 9637