White Paper

Content Management and Protection Requires Deep Understanding of Hybrid Data Environments

Sponsored by: Egnyte

Sean Pike
September 2017

IDC OPINION

Organizations have fully embraced the 3rd Platform — a computing paradigm encompassing cloud, social, mobile, big data and analytics technologies. Today, organizational focus has shifted from merely capitalizing on 3rd Platform trends and is instead squarely dedicated to optimizing the use of the same 3rd platform technologies to create fully integrated, technology-driven business processes — a shift known as digital transformation. This shift requires organizations to fully embrace technology.

As a result, back-office and front-office business processes are leveraging any number of on-premises and cloud-based point solutions to move data more efficiently in attempts to satisfy line of business requirements. While accomplishing this task, these point solutions unfortunately can introduce unforeseen risk as information can quickly become out of alignment with established corporate management policies. The explosion of unstructured information that results will continue to drive demand for systems to manage all that content through its lifecycle and present it within the context of enterprise business processes. As a platform for automating and optimizing content-intensive business processes — many of which ultimately impact customer experience and revenue — enterprise content management (ECM) is taking on fresh importance as an enabler of digital transformation.

The explosion of unstructured content and the voracious appetite for leveraging cloud-enabled content collaboration tools will continue to drive demand for systems that assist enterprises in managing content throughout its lifecycle while also delivering key content management services. Such collaboration applications must be capable of peering into a myriad of on-premises and cloud content repositories in order to deliver a precise, consolidated view of enterprise content. In addition, these applications include capabilities that provide cognizable ROI for business-related functions such as content discovery, data migration services, classification, and protection. The following global business trends are driving the need for content management:

- Requirements for exchanging information with collaborators inside and outside the organization and activating it in the context of critical business processes is driving the convergence of managing content and enabling effective collaboration.
- Lines of business (LOBs) are dictating efficient means of operation and specific technologies, forcing IT functions to adapt and leverage technology to keep up with demand.
- Increasing global regulation and litigation — and the accompanying penalties, fines, or exposure — have created a general intolerance for operational risk. Since data protection, discovery, and control are so closely tied to risk exposure, organizations are making heavy

investments in technologies that are purpose-built to help reduce risk presented by unwieldy content.

- Bad actors are actively leveraging insecure data repositories to manufacture high profile data breaches in efforts to extort ransom in exchange for not releasing valuable or damaging information to the public.

IN THIS WHITE PAPER

This IDC White Paper discusses the opportunities and advantages associated with 3rd Platform content collaboration platforms and describes the content governance challenges faced by organizations as their data becomes further decentralized. The paper also examines technological trends that IT departments may leverage in order to satisfy their data protection charter while providing flexible solutions that add business value. Finally, the paper will examine the role Egnyte's Protect solution can play in enterprise content governance and control. Egnyte Protect is a solution developed to perform content management, protection, and control functions for on-premises and cloud data sources in a consolidated platform.

SITUATION OVERVIEW

While there may already be too many demands on enterprise data, content managers, and data custodians, there is no sanctuary on the horizon. In fact, the situation is quite the opposite. According to IDC, the amount of data generated by 2025 will grow to 163ZB, ten times the 16.1ZB of data generated in 2016. This trend clearly illustrates the heart of the content governance problem, namely that content volumes continue to rise. Organizations are simply creating and storing more data. With greater data volumes a reality, organizations must also attempt to satisfy the competitive factors bidding for IT data management resources. Chief among these factors is digital transformation. As businesses move through the digital transformation process, LOBs will continue to dictate the technologies and business processes necessary to efficiently meet their goals. This paradigm demands that IT functions enable business agility by allowing LOBs to select and use 3rd Platform/cloud or on-premises content sharing and storage repositories that fit the needs of an individual business process. IT no longer has the latitude to restrict business processes to one-size-fits-all solutions.

As a result, IT departments must readily support a myriad of enterprise cloud, bring your own cloud (BYOC), and on-premises collaboration applications. What's more, IT is increasingly under pressure to 1) add business value by providing single-pane-of-glass views and sophisticated search and discovery mechanisms that surface relevant enterprise content across these distributed platforms and 2) extend traditional enterprise content governance controls into third party cloud-based repositories, sharing services, and other collaborative workspaces in an effort to provide consistent data views and treatments for on-premises and distributed content. These demands have left organizations searching for consolidated content governance and protection platforms that closely integrate with any number of content repositories.

Market Environment

Enterprises are spending heavily on content services that enable business processes and spur innovation. Over the past several years, enterprises have made conscious efforts to expand their boundaries by offering solutions that support greater employee mobility and the expansion of global workforces. As a result, markets such as the worldwide enterprise file synchronization and sharing (EFSS) software market reached $1.4 billion in 2014 and will rise to $3.6 billion in 2020. ECM market revenue will grow at a CAGR of 4.3% from $4.6 billion in 2016 to $5.7 billion in 2021. IDC forecasts the data loss prevention (DLP) market will grow at a CAGR of 7.9% from 2015 to 2020, reaching nearly $1.2 billion at the end of the forecast period. While the ECM and DLP markets don't tell the entire content governance story, the trends tend to validate the new content governance paradigm: organizations are investing in agility, and the growth of distributed content systems is driving IT investment in content protection platforms. This creates a unique opportunity for vendors offering content protection solutions capable of acting as an independent control layer that overlays existing 3rd Platform enterprise solutions. These solutions grant LOBs the opportunity to choose data sharing platforms and repositories that fulfill their requirements while giving IT and compliance resources the tools necessary to execute on content management and protection strategies.

Technology Trends and 3rd Platform Adoption

Business benefits associated with 3rd Platform adoption are realized when the CIO leverages technology to achieve speed, scale and agility. Business processes no longer drive the data. Instead, data drives the business processes, which are under a constant state of optimization. The volume of data and the speed at which it is created continues to be a major challenge facing the enterprise, which is driving demand for data management, data identification, and data classification solutions. These solutions in turn address the goals set by business leaders focused on minimizing compliance risk and reducing storage costs.

Organizations engaged in digital transformation fall into three broad categories: digital transformers, technology optimizers, and technology disruptors. Digital transformers seek business process transformation and new monetization models. Technology optimizers focus on modernization to bolster efficiency and effectiveness of the IT architecture. Technology disruptors enable innovative technology to drive the business strategy. CIOs at organizations that fall into any of these categories support their companies' ability to create speed in its operational processes, including an ability to apply sensing and analysis to enable self-healing and higher levels of automation.

Regardless of which category a business falls into, all organizations must be fully engaged in converting their entire value chains to digital experiences wherein content, workflow, and interaction are enabled by the agility of 3rd Platform solutions (see Figure 1). For the CIO, embracing the 3rd Platform delivers on two key business outcomes.

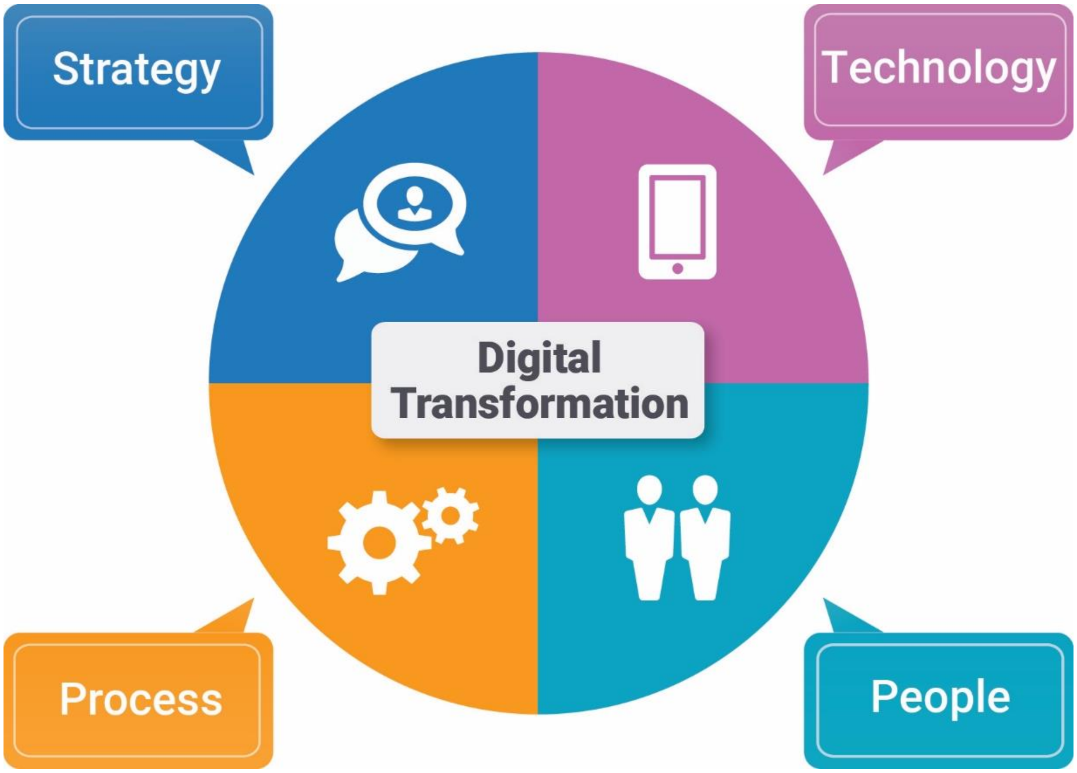
First, it allows business leaders to take an active role in the selection of underlying technologies that best fit their needs (democratizing IT decisions). Second, it offers incredible opportunity to reduce cost, create efficiencies, and drive increased ROI. Cost reduction may occur in a number of ways including:

- Reducing the amount of physical infrastructure and facilities required to operate "in-house" technologies
- Decreasing the time-to-value for applications by easing implementation and deployment cycles
- Supporting an agile marketplace which can remove the burden of developing home-grown applications

Granted, not every data store or content collaboration use-case lends itself to the cloud. Certain on-premises, regulated and sensitive information, and highly customized systems will continue to exist long after companies claim victory in their transition to 3rd Platform technologies. This means that enterprises will need to continue developing strategies to govern on-premises content and align content governance strategies during cloud transition and beyond. The most successful companies will elect multi-disciplinarians to lead cross-functional teams that understand content governance but have a focus on unlocking data potential.

FIGURE 1

Digital Transformation Influence



Source: IDC 2017

Storage Costs

As noted above, one of the major factors driving cloud adoption is the opportunity to reduce cost by eliminating the need for in-house infrastructure or leveraging economies-of-scale. Storage is a shining example. In what has become known as the "race-to-zero," cloud platform providers have been swallowing up new storage technologies that increase capacity while decreasing overall cost with the goal of providing services without the need to charge additional storage fees. While the cost of storage has decreased dramatically over the last 10 years — reaching less than $.04 per GB for consumer storage — the hardware, infrastructure components, energy, and workforce required to maintain enterprise storage systems account for the vast majority of associated cost. For the cost-conscious CIO, free/near-free storage models could mean swapping out one or more pieces of costly dedicated hardware for virtually nothing. As IT budgets continue to shrink or experience only modest year-over-year increases, the promise of virtually free storage will continue to be alluring.

Pure cost per GB isn't the only factor that CIOs must consider. While cloud applications are alluring, enterprises have invested heavily in developing existing architecture. The wholesale swap of existing, paid-for infrastructure components for cloud-based technologies isn't realistic. Nor is pulling the plug on highly customized systems that already run business processes efficiently. Businesses instead have followed a fairly predictable cloud transition playbook — moving inefficient processes and applications whose functionality or infrastructure no longer serve its purpose. Enterprises also continue to debate the utility of cloud applications for certain high value and high sensitivity data, choosing, in many cases, to retain certain data types on-premises in order to mitigate risk.

Cloud Applications Adopted by the Mobile Workforce

The number of employees in a workforce that is highly mobile is at an all-time high, and many of these professionals manage large customer portfolios with high levels of autonomy and a great deal of success. These workers view cloud-based applications as necessary tools to find balance between work/personal time. Millennials have high adoption rates for new and emerging technologies and have developed flexible workflows for finances, banking, communication, and more using cloud-based platforms. Locking these workers into stodgy inflexible systems could reduce their creativity and productivity. Finally, for geographically dispersed workforces to function as intended, they must feel intimately connected with any processes in which they participate. As a result of these trends, users as well as enterprises are adopting cloud platforms in order to achieve greater flexibility and higher levels of connectivity. More organizations are evaluating public cloud deployments to help grow their businesses and remain competitive across all industries. For the growing number of organizations that have adopted a cloud-first strategy, many are realizing that education and awareness on critical inputs should be taken into consideration around total cost of ownership (TCO) conversations. Doing so is critical in realizing compelling cloud economics. Companies that are adopting more of a cloud-first stance for net-new applications look at solutions to increase their agility and speed to market and to drive innovation spurring their digital transformation.

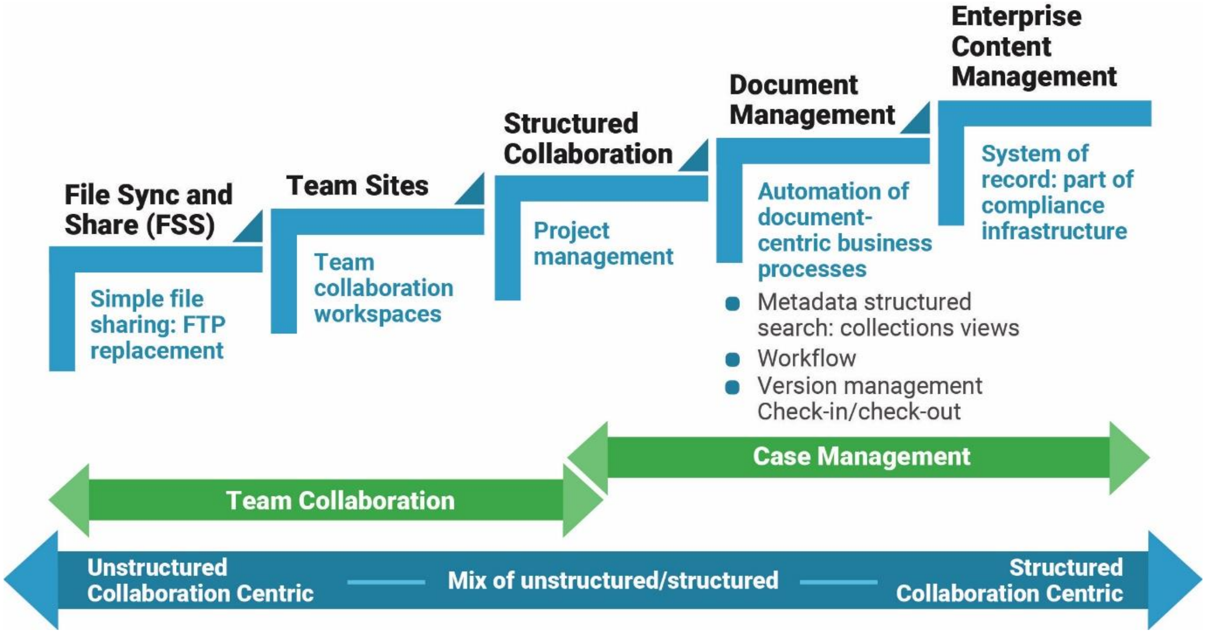
Content Governance Challenges

There is a broad continuum of needs when it comes to managing and sharing content (see Figure 2). Some needs lend themselves to cloud-based applications; others fit more naturally with on-premises application deployments. While these collaborative applications will be increasingly driven by cloud delivery and offer the vision of anytime, anyplace access, certain content will remain rooted to the enterprise. As a result, organizations will look to connect existing on-premises content repositories using cloud team collaboration applications.

Connecting customers, partners, suppliers, and other stakeholders outside the corporate domain is critical in modern business, and increasingly that collaboration occurs through third party applications. This complicates the IT and compliance mission. IT hopes to support a seamless highly productive experience. At the same time, compliance professionals must ensure the systems deliver consistent content access restrictions across applications. In fact, one of the more frequently requested initiatives from senior IT leaders is to perform an audit across both online and on-premises content platforms in order to understand how information flows between cloud and on-premises systems and identify areas of risk or policy inconsistencies.

FIGURE 2

The Content Collaboration Continuum


File Sync and Share (FSS)
Simple file sharing: FTP replacement
Team Sites
Team collaboration workspaces
Structured Collaboration
Project management
Document Management
Automation of document-centric business processes
Metadata structured search: collections views
Workflow
Version management Check-in/check-out
Enterprise Content Management
System of record: part of compliance infrastructure
Case Management
Team Collaboration
Unstructured Collaboration Centric
Mix of unstructured/structured
Structured Collaboration Centric

Source: IDC, 2017

Shadow IT

IT departments certainly have the option of deploying content protection solutions by prescribing the productivity applications to their users and dictating the flow of business processes. Unfortunately, that method has given way to shadow IT –services provisioned by LOBs or operations units without the knowledge of IT. Cloud applications make shadow IT all too common since provisioning often requires little more than a credit card. These types of services are inherently dangerous because IT organizations are unable to properly secure systems that they are unaware of, creating vulnerabilities such as unwittingly exposing sensitive data by placing it in unprotected content repositories or sharing information with the wrong people. But given the choice between slow IT reaction to changing business needs and skirting the rules for a perceptibly better technological solution, many managers choose the latter.

A better approach is for IT stakeholders to support business objectives by implementing solutions that offer visibility and control over corporate content via creation of a governance layer atop the various applications adopted with or without IT consent by the users. In this way, applications accessing and sharing content can be decoupled from content governance policies effectively granting LOBs the flexibility they desire while the organization is able to protect the intellectual property and control enterprise risk.

Privacy and Data Residence

Top of mind for many IT and compliance professionals is identifying and classifying content throughout the organization from on-premises technology and cloud-based services, to third party access. Data residence and privacy concerns are fueling these efforts. Global businesses are hyper aware that Europe is leading the charge to help consumers protect their data privacy. Among the major developments that have shaped the way that content managers and data custodians will think about data for years to come was the decision by the European Court of Justice to invalidate the Safe Harbor framework established in 2000, deeming it an inadequate measure to protect EU citizen data privacy rights. Last summer, the EU-US Privacy Shield was accepted by the EU as a replacement for the original framework. While controversy remains on its long-term viability, the new regulation is viewed as having greater protection for EU citizen personal data. The 4,400 U.S. and EU companies that leveraged the Safe Harbor framework to exchange data are now required to meet these stricter requirements in order to continue to transact business. Additionally, the EU General Data Protection Regulation (GDPR) will officially replace the European Data Protection Directive (Directive 95/46/EC) as of May 25, 2018. The new set of regulations take a much stricter view of European privacy with broad implications for businesses around the world. Among other items, the new GDPR expands regulatory reach to data controllers and processors outside of the EU whose activities relate to offering goods or services, or monitoring EU data subjects. In other words, any organization that touches EU citizen personally identifiable information (PII), regardless of its location, is subject to the new regulatory framework. Additionally, the regulation creates greater corporate accountability and stricter penalties including fines that could reach up to €20 million (US$24 million) or 4% of worldwide revenue, whichever is greater. These developments will require organizations to understand the types of data they have and where the data originated, as well as classify the data and treat each type with different policies. Only then can global businesses attempt to better execute data protection measures.

Legal, Regulatory and Compliance Challenges

Legal and regulatory challenges — in particular regulations like EU GDPR and 23 NYCRR 500 — are driving the need for greater visibility in enterprise data. As an example, under new requirements of the EU GDPR, organizations must be able to access, alter, delete and prove value of any PII related to an EU citizen. Under 23 NY CRR500, covered entities must assess risk and maintain written policies and procedures which demonstrate planning for data governance and classification specifically. These requirements introduce a range of new challenges for organizations, but the critical step in an organization's ability to be in compliance is the ability to discover specific information. Once IT leaders know where all enterprise data is located, they can then determine if and what information should be kept and for how long, based on its value to the business.

A recent IDC survey highlights the increasing demand for greater visibility and control of enterprise data environments. When asked to rank top priorities for the next 12 to 18 months, more than 63% of IT executives rated "data visibility and control" as either important or very important. This same survey found that ensuring compliance to government regulations and internal records retention policies was the number one reason for purchasing and deploying an archiving solution. This data is very telling about what the current and future needs are for enterprise IT leaders. Even with this acknowledgement and looming GDPR and 23 NY CRR500 deadlines, many enterprises are still not fully prepared. The consequences for non-compliance are extremely high from both a financial and reputational perspective. Consequently, the ability for an organization to locate, classify, identify, control and act on enterprise data in a timely fashion is critical to both the compliance department as well as to the business' performance and financial standing as a whole. It cannot be said strongly enough — data visibility is the key to any data-centric enterprise compliance initiative. There are tools that can help organizations perform critical data functions and harmonize policies across the enterprise.

FUTURE OUTLOOK

With the governance, risk and compliance software market expected to reach just under $12 billion by 2021, it is clear where business leaders will be focusing their resources over the coming years.

The ability to leverage data will become a critical differentiator among organizations. Over the next several years, global CIOs – especially those who are at highly regulated businesses like financial institutions and healthcare providers – will realize the importance of initiating a data transformation and governance framework that enables their organizations to take maximum advantage of information while minimizing associated risks and costs. Organizations using a siloed approach based on individual departmental needs will not be able to manage the high demands of data management and usage. Instead, organizations that evolve from a traditional data management approach to mastering a differentiated, well-governed information value chain will gain business leadership and competitive advantage.

The industry continues to evolve toward hybrid IT architectures that rely on a wide range of cloud and on-premises IT resources. The impact of this change cannot be understated since it affects all areas of a company's IT, particularly datacenter investments and end-to-end IT infrastructure. The growing use of off-premises resources affects all elements of long-term data and asset management, compliance, legal, security, and risk functions, elevating content governance discussions.

As it relates to content governance specifically, the immediate future likely holds more of the same – organizations are struggling to find, classify, and apply consistent data policies to their content. As business processes, software solutions, and workflows mature, enterprises will be able to leverage technology to gain visibility and consistency across all content sharing and collaboration resources.

Buyer Challenges

When considering the purchase, renewal or upgrade of enterprise content solutions, IT buyers must be concerned with usability, as well as consider data protection and security implications. Both the shift to digital and the increasing regulatory pressures demand that organizations have the ability to monitor, control and alter information in near-real time. Most single-feature, 3rd Platform data repositories and content collaboration tools were not designed with data privacy and security in mind – ever increasingly important requirements. Instead, organizations must attempt to cobble together solutions that inform security and compliance as to the whereabouts of enterprise content. Another option is for IT buyers to concentrate on locating new technologies that deliver holistic content views and support consistent data treatment and protection.

For buyers who choose to invest in holistic content governance solutions, finding the right solution can still be a challenge. Technology convergence and a desire to collect or guard market share has created a confusing landscape of products that are difficult to distinguish. In general, buyers should search for content governance solutions that are technology agnostic and capable of connecting to any number of content applications. These solutions should also be able to manage both on-premises and cloud content in a consistent manner.

Drive to ROI and Increased Business Value

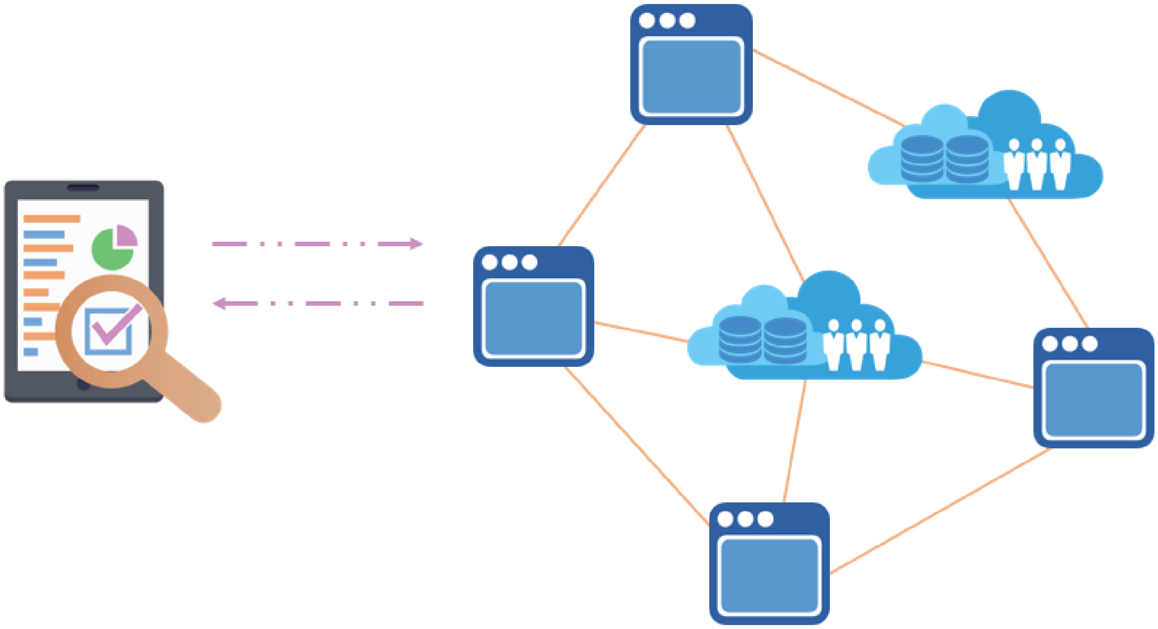
The discipline of information or data management has evolved from managing large-scale structured (machine generated) data sets to ensuring data quality and controlling user access rights. Corporations are truly striving for a holistic view of data — a deep understanding of where data is (residency), how the data should be protected (including controlled access, encryption and data retention), who created the data, and what data can be used for. That deep level of understanding is what industry professionals call information governance.

Companies endeavor to both share and publish information in a managed, governed fashion as well as to put that information to use in the context of business processes that support business-critical interactions. This means that organizations are increasingly productizing, syndicating, and distributing their information assets as "callable" IP assets or value-added content. In this way, unstructured (human generated) data is fueling a renaissance in the handling and analysis of information, resulting in a new generation of tools and capabilities that promise to offer intelligent assistance, advice, and recommendations to consumers and knowledge workers around the world. In particular, cognitive systems are providing cloud- and mobile-based platforms through which these intelligent assistants will operate, using knowledge graphs and databases built through the use of content analytics.

Some production data, however, may be hidden in data silos throughout the organization. To make this data fully visible and protected, IT buyers must search for solutions capable of connecting to a wide array of data sources and content repositories. By enabling this approach, companies will no longer need to build application integrations and will look to open platforms which provide immediate insight across disparate data sources (see Figure 3).

FIGURE 3

Visibility and Control Over Disparate On-Premises and Cloud Data Sources



Source: IDC, 2017

Data Protection

One of the chief mandates for the IT buyer and compliance professional has become data protection. While IDC surveys continue to demonstrate the importance and high level of spending on traditional IT security mechanisms, executives should not be fooled into believing that these "table stakes" are sufficient to protect data. We are in a transition. Data is more distributed and becoming more valuable than ever before. At a minimum, these data trends demand implementing appropriate access control mechanisms to ensure consistent data access and reduce the risk of unauthorized use or disclosure. At the same time, a bevy of regulatory requirements and intellectual property concerns have created additional pressure on enterprises to apply encryption to sensitive content in an effort to provide an additional layer of protection against unauthorized or inadvertent disclosure. Data protection functions become more important as this trend continues.

CONSIDERING EGNYTE PROTECT

Egnyte holds significant market share and is traditionally known for its EFSS solution, Egnyte Connect, for both on-premises and cloud environments. Founded in 2007, Egnyte is privately held, with investment backing from tech industry brands like CenturyLink as well as leading venture capital firms.

With concerns over data loss, data governance, and residency rampant, Egnyte offers an independent solution, Egnyte Protect, which is aimed at creating a holistic view of enterprise content and providing administrators with the ability to classify and enforce consistent data policies across any content repository, whether located on-premises or in the cloud.

Egnyte Protect acts as an overlay that connects to various content repositories and offers solutions such as data classification, search and discovery, and certain DLP functions in a consolidated platform. The platform dashboards provide IT with the controls to rapidly deploy or modify access control rules and permissions across all corporate content in response to business changes. In practical terms, this allows organizations to search for sensitive and/or important content, and classify it accordingly. Audit reports and monitoring support compliance and management within a hybrid IT environment. Key platform components include:

- **Access control.** Identify issues with access and permissions functions so that an organization can ensure only the people who need to access files can access them.
- **Content classification.** Scan and classify cloud and on-premises repositories and monitor them from a single pane of glass.
- **Data retention.** Control when and how long files should be retained, and who can access and modify them.

In addition, Egnyte offers end users ease of use in that no special IT or security are required. The system provides real-time alerts and is designed to be a future-proof platform. While Egnyte faces off against stiff competition in the EFSS market, the Egnyte Protect solution is intended to act as an overarching content governance platform capable of delivering insight into enterprise data no matter where the data is located (on-premises or in the cloud) and ships out-of-the-box with integrations for its own EFSS product Egnyte Connect, SharePoint and Windows File Server, as well as a host of other cloud and on-premises content repositories. That flexibility is further enhanced by Egnyte Protect's SaaS delivery model which can lower the cost of administration and maintenance.

CONCLUSION

Organizations need to understand that information transformation and governance is a work in progress, requiring long-term guidance and commitment to build strategic skills and stay ahead of the business need curve. Those organizations that have already established initiatives on data quality, data governance, and data management also must evolve these data practices to meet the requirements of both the legacy environment and the digital business under construction. Organizations need a set of structures, stakeholder accountabilities, procedures, policies, and processes that can manage information with security, consistency, and credibility. An information transformation and governance framework encompasses processes, tools, and practices aimed at managing data as an asset and delivering business value as the business evolves.

It's unlikely that a single, unified platform will emerge that spans all of the content collaboration use cases within the next few years. However, everything changes with the cloud, and embracing cloud is not entirely straightforward — at least for large organizations that have made significant investments in on-premises storage. These organizations need to manage both environments for a long time to come and will need to develop strategies around the management of information as it flows between cloud and on-premises systems. IDC expects to see considerable energy directed into integrations — between separate offerings from a particular vendor and between offerings from multiple vendors — to address the broader content collaboration needs. The Egnyte Content Intelligence analytics platform powering its content governance solution, Egnyte Protect, is focused on this objective and, as such, is well positioned for this critical and growing market.

There are many technical and semantic challenges to address as vendors unite cloud and on-premises, ad hoc workflow and structured workflow, and systems that have different metadata, security, and object models. However, vendors like Egnyte are making considerable investments here, and IDC believes that customers have everything to gain as those efforts progress.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-community.com
www.idc.com