



## White Paper

# Content Management and Protection Requires Deep Understanding of On-Premises and Cloud Data

Sponsored by: Egnyte

Sean Pike  
June 2016

## IDC OPINION

---

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 applications must be capable of peering into a myriad of on-premise and cloud content repositories in order to deliver a precise, consolidated view of enterprise content. In addition, these applications include functionality that provides 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:

- The requirement to exchange information with collaborators inside and outside the organization and activate it in the context of critical business processes is driving the convergence of managing content and enabling effective collaboration.
- Lines of business (LOB) are dictating efficient means of operation and specific technologies forcing IT functions to adapt and leverage technology in order to keep up with demand.
- Enterprise document management and sharing systems continue to enable organizations to securely manage, protect, and govern business-critical unstructured information as a system of record, and they are platforms for building horizontal and vertical content-enabled applications that automate document-based business processes.
- 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 purpose-built to help reduce risk presented by unwieldy content.

## 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 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-premise 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. At the heart of the content governance problem lies the simple fact that content volumes continue to rise. Organizations are simply creating and storing more data. With greater data volumes an accepted premise, organizations must also attempt to satisfy the competitive factors bidding for IT data management resources. Chief among these factors is the new data or content governance paradigm which demands that IT functions enable business agility by allowing lines of business to select and use 3rd Platform/cloud or on-premise 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-premise collaboration applications. What's more is that 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 3rd party cloud-based repositories, sharing services, and other collaborative workspaces in an effort to provide consistent data views and treatments for on-premise 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 to offer 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 grew a remarkable 72% to \$1.4 billion in 2014 continuing its fast-paced year-over-year growth. For the same period of time, IDC sized the worldwide enterprise content management (ECM) and data loss prevention (DLP) markets at \$4.2 billion and \$725 million respectively. IDC predicts that the ECM market will grow at a 5.1% CAGR and DLP will grow at a 8.2% CAGR. 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

In 2014, IDC predicted that 90% of IT roles would change by 2018 driven by adoption of 3rd Platform cloud solutions. Of those roles, IDC predicted the most change for enterprise chief information officers (CIOs). Why? At the time, the 3rd platform was spurring innovation, creating new options and delivery mechanisms for nearly every IT function. CIOs were urged to fully embrace the change by transforming their own roles to become highly innovative themselves. Two years into the prediction and it's apparent that CIOs by-and-large received the message. Businesses are fully engaged in converting their entire value chains to digital experiences wherein content, workflow, and interaction

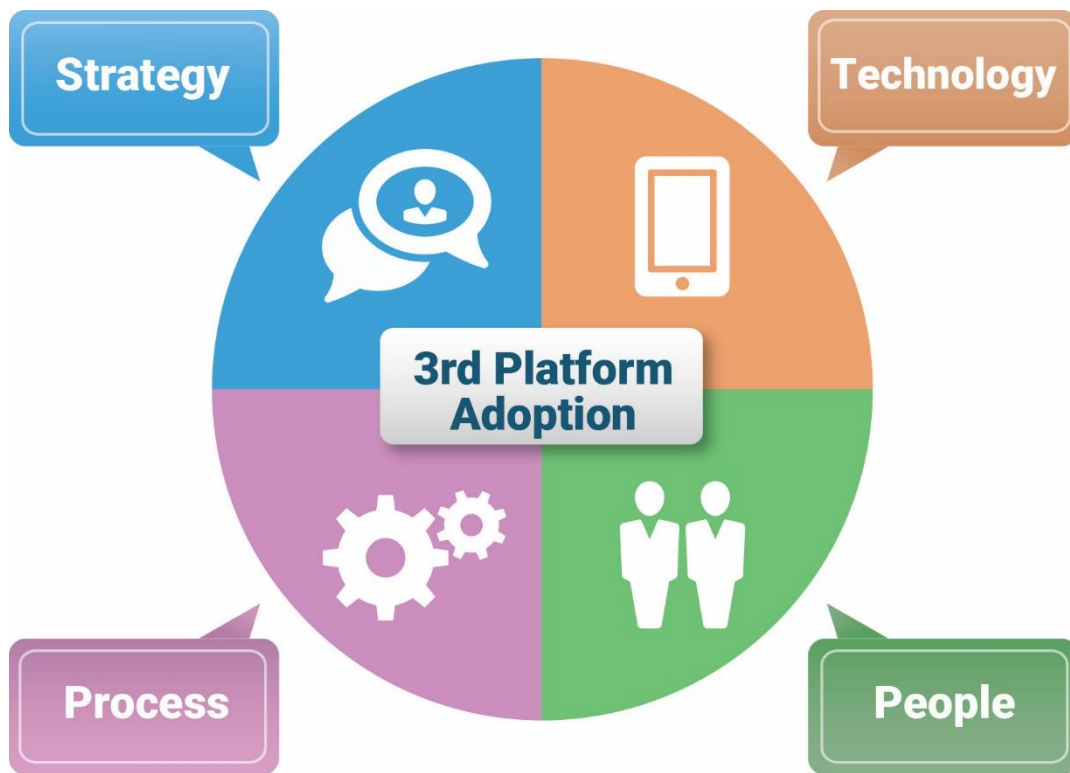
are enabled by the agility of 3rd Platform solutions (See Figure 1). For the CIO, embracing the 3rd platform delivers on two key business outcomes. First, it allows business leaders to take an active role in the selection of underlying technologies that best fit their needs (democratizing IT decisions). 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-premise, 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-premise 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**

### 3rd Platform Adoption Influence



Source: IDC 2016

## 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-premise in order to mitigate risk.

## Cloud Applications Adopted by the Mobile Workforce

The advent of smartphones, tablets, and focused collaboration applications have created a shift in how managers and individual contributors view corporate locations and connectivity. Just a few years ago, working from home-based offices was still frowned upon as enterprises felt disconnected from employees who chose to work remotely. In part, this was representative of a technological challenge whereby managers felt that employees lacked the ability to access critical systems or key data quickly and easily. In another sense, it was cultural. Employees and managers alike needed to change their mindset and workflow to create processes that incorporate disparate workforces. Third platform solutions offer this opportunity in spades. Fast-forwarding to the present day, three groups of employees continue to drive demand for flexible collaborative workflows: 1) highly mobile and seasoned home-based workers, 2) technology- attached Millennials, and 3) distributed workforces stationed in far-flung geographies.

The highly mobile workforce 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.

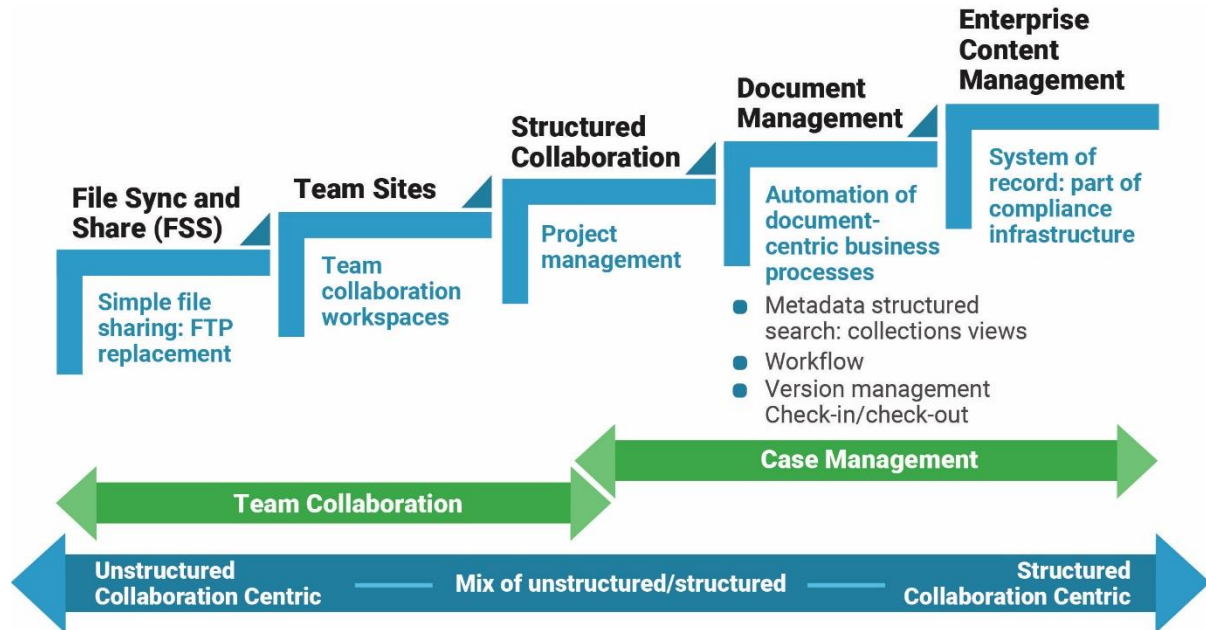
## 3rd Platform Adoption and Content Governance Challenges

While cloud solutions can offer a great deal of value, 3rd Platform technologies are not without their challenges and perhaps nowhere is this more evident than in modern enterprise content governance

and control or information governance efforts. 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-premise 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-premise content repositories using cloud team collaboration applications.

**FIGURE 2**

**The Content Collaboration Continuum**



Source: IDC 2016

In a recent IDC survey of LOB users across sales, marketing, HR, and service, more than 50% communicate outside the corporate domain weekly or daily. 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-premise content platforms in order to understand how information flows between cloud and on-premise systems and identify areas of risk or policy inconsistencies.

Microsoft SharePoint installations provide a textbook example. Many organizations have large, highly customized, and behind-the-firewall installations of this content management platform. To retain identical functionality, for highly customized installations, it may not be possible for an organization to move its entire platform to the cloud (e.g. SharePoint online). Instead, the organization may end up keeping their most complex instances of SharePoint on-premise and migrating the others to the cloud. These organizations will end up managing multiple heterogeneous environments for a long time to

come and will need to develop strategies to ensure consistent content treatment and permissions as content flows between cloud and on-premise systems.

## Shadow IT

Certainly IT departments 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 will likely give way to shadow IT – IT services provisioned by lines of business or operations units without the knowledge of IT. Cloud applications have made 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 creating 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 meaning that lines of business are granted 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-premise technology and cloud-based services, to third party access. Data residence and privacy concerns are fueling these efforts. Global businesses are already hyper aware that Europe is leading the charge to help consumers protect their data privacy and over just the last 6 months two major developments have shaped the way that content managers and data custodians will think about data for years to come. First, the European Court of Justice invalidated the Safe Harbor framework established in 2000 which permitted some 4,400 U.S. and EU companies to exchange data on agreement that the U.S. companies would offer data protection/privacy rights to EU citizens in the same manner as EU-based companies. Second, Europe's new General Data Protection Regulation (GDPR) officially replaced the 20-year old Data Protection Directive. In general, the GDPR takes a stricter view of European privacy and will be enforced in 2018. 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. Additionally, the regulation creates greater corporate accountability and stricter penalties including fines that could reach up to 4% of worldwide revenue. 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

Among the top drivers for improved content visibility are legal and regulatory challenges. At the root of these concerns lies one simple truth; organizations don't understand their content well enough to make intelligent and confident content determinations. Can a document be deleted? Is there any more data related to a given legal matter? Has an organization accounted for every data repository or sharing



mechanism? All of these questions can be answered through greater visibility across all corporate content. In fact, a recent IDC survey highlighted a data visibility gap. Only 8% of companies surveyed proclaimed success in automating data classification and only about 7% could claim success in the areas of data deduplication and incorporating new data sources. These numbers are eye-opening. If organizations are unable to classify data or, worse yet, gain a holistic view into every content source or repository, how can they be deterministic about data-centric compliance efforts? They can't. Certain regulations require the ability to monitor communications. Legal actions require good faith attempts to preserve content relevant to an ongoing or anticipated legal matter. Step one in completing either task is developing visibility.

## FUTURE OUTLOOK

---

In a clear sign that data governance has risen to the top of the business risk food chain, IDC recently predicted that 80% of global CIOs will initiate a data transformation and governance framework initiative to turn information into a competitive business differentiator over the next 18-24 months. As a result, IT teams must shift their focus from maintaining components to delivering policy-based services across dynamic hybrid architectures and securing data no matter its location.

The ability to leverage data will become a critical differentiator between organizations. Over the next several years, global CIOs, especially those that 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 them 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 is rapidly evolving toward hybrid IT architectures that rely on a wide range of cloud and on-premise 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-premise 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 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

IT buyers must be concerned with an array of near-equal forces when considering the purchase, renewal, or upgrade of enterprise content solutions. The shift to digital and 3rd Platform technologies demand democratization of IT and business agility while expanding an organization's ability to track and control information. Most single-feature, 3rd Platform data repositories and content collaboration tools don't have native capabilities designed to deliver enterprise-wide data analytics. 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-premise 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, 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.

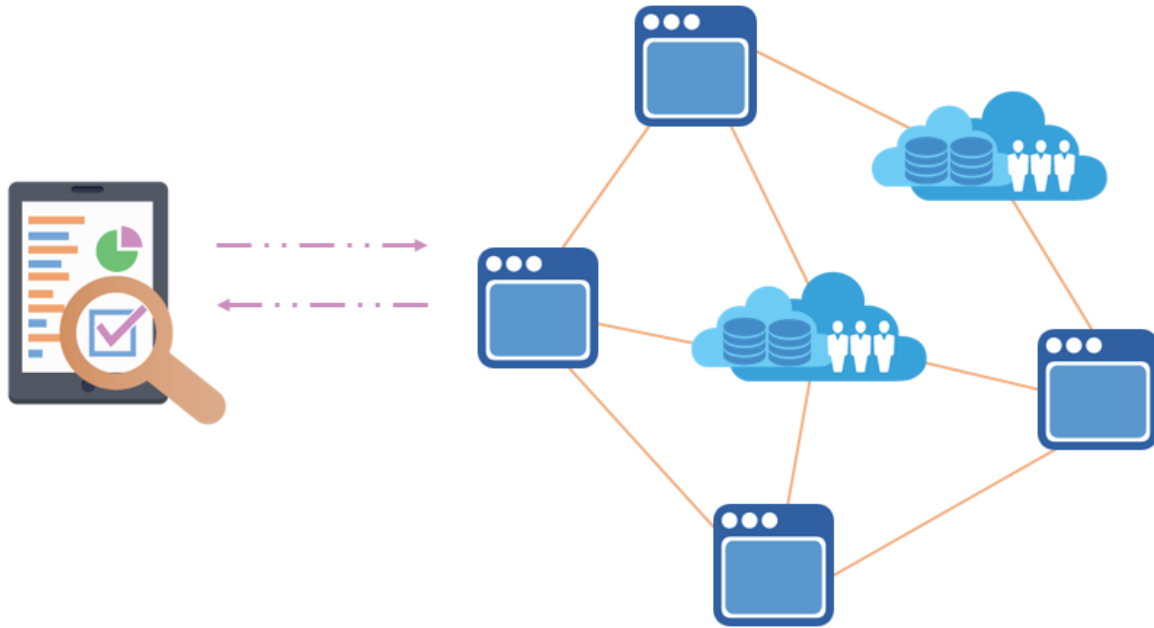
Companies endeavor to not just share and publish information in a managed, governed fashion but also to put that information to use in the context of business processes that increasingly support business-critical interactions. This means that organizations are increasingly productizing, syndicating, 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. In order to make it 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, 2016

**Data Protection**

One of the chief mandates for the IT buyer and compliance professional has become data protection. While recent 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 the midst of a transition. Data is more distributed and becoming more valuable than ever before. At a minimum, these data trends demand the institution of 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 EFSS solution, Egnyte Connect, for both on-premise 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 has introduced a new 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-premise or in the cloud.

Egnyte Protect acts as an overlay that connects to various data repositories like NAS servers, EFSS or SharePoint 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. Audit reports and monitoring support compliance and management, covering a hybrid IT environment. Key platform components include:

- **Access control.** Identify issues with your access and permissions functions so that you can ensure only the people who need to access files can access them.
- **Selective encryption.** Keep a select subset of your files encrypted at all times, even after they leave your system – and your control – to prevent unauthorized viewing of sensitive, confidential or regulated content.
- **Data residency.** Control the location of your content, between cloud or on-premise repositories, across geographical boundaries and even different vendors to comply with data sovereignty laws and other regulations.
- **Data retention.** Control when and how long your files should be retained, and who can access and modify them.

While Egnyte competes against stiff competition in the EFSS market, the new 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-premise or in the cloud) and ships out-of-the-box with integrations for its own EFSS product Egnyte Connect and major EFSS competitors, as well as a host of other 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-premise 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-premise 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. Egnyte Content Intelligence 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-premise, 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

---

### Copyright Notice

This IDC research document was published as part of an IDC continuous intelligence service, providing written research, analyst interactions, telebriefings, and conferences. Visit [www.idc.com](http://www.idc.com) to learn more about IDC subscription and consulting services. To view a list of IDC offices worldwide, visit [www.idc.com/offices](http://www.idc.com/offices). Please contact the IDC Hotline at 800.343.4952, ext. 7988 (or +1.508.988.7988) or [sales@idc.com](mailto:sales@idc.com) for information on applying the price of this document toward the purchase of an IDC service or for information on additional copies or Web rights.

Copyright 2016 IDC. Reproduction is forbidden unless authorized. All rights reserved.

