

Four Reasons Your Content Is More Secure in the Cloud

Why You Should Migrate Now



There's no question that business is embracing the cloud as a key IT strategy. According to the market intelligence firm IDC, at least half of IT spending in 2018 will be for cloud-based projects. IDC also predicts that by 2020, cloud computing will account for 60% of all IT infrastructure and as much as 70% of all software, services, and technology spending. Clearly, IT leaders recognize the value of cloud-enabled gains in operational efficiency and business collaboration, especially across an increasingly extended enterprise.

Even with the appealing benefits of the cloud, however, moving business content, processes, workflows, and custom applications from on-premises systems is a big step. And sometimes IT hesitates to take this step, because of concerns about control, governance, and compliance for stored content. Often the biggest worry is security: Will highly sensitive business information and intellectual property be protected from increasingly sophisticated cyberthreats?

The answer is yes. Cloud content management technologies continue to advance, and cloud providers continue to strengthen their security measures. These improvements mean that IT can now look to the cloud to provide a centralized, highly secure content platform that:

- 1 *Delivers an improved, more secure user experience*
- 2 *Enables increased collaboration and productivity across the extended enterprise*
- 3 *Simplifies information governance and compliance*
- 4 *Leverages innovations such as machine learning to put user data to work*

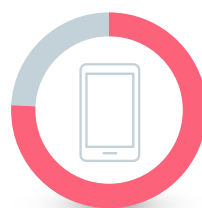
This paper explores reasons that today's cloud technologies—and, specifically, cloud content management platforms—can deliver these advantages to your business.



1. Provide Security That Enables a Seamless User Experience

Information is at the heart of nearly all business activity. Consider financial statements that are prepared by a team, design specifications for new products under development, or employee records that must be stored for many years. These are just three examples of vital business content that must be easy to access by users who need it, while being protected from access by unauthorized parties.

The mix of different security measures and user interfaces in traditional, siloed systems often makes it difficult for employees to work with and share business content. Out of frustration, they may turn to unmanaged shadow IT services and devices. Employees don't necessarily want to circumvent IT controls, but doing so may be the best or fastest way to do their job effectively.



76%

of employees think it is acceptable to move confidential documents to personal devices.¹


In contrast, a cloud content management platform provides a centralized architecture, with security embedded throughout the infrastructure and

services. This means that employees can share business content directly and securely from the cloud, eliminating the reasons to use unauthorized shadow IT.


With a cloud solution, employees also have an easier time with knowledge transfer. One IT manager says the intuitive, user-friendly interface on his cloud content management platform enables him to offer a “latte training” program—he can teach any colleague how to use the system in the time it takes to drink a cup of coffee.

A cloud management platform provides secure capabilities that IT can use to integrate content in custom applications and back-end systems and to embed content management into any application. This flexibility for content integration and custom app development helps IT deliver rich, engaging experiences for customers and employees.

Actual shadow cloud use was at least

15x 
as high as the levels estimated by CIOs.²

By 2020,

1/3 
of successful attacks experienced by enterprises will be on their shadow IT resources.³

IT Takeaway: A multinational food and beverage company had a three-day approval period for employees who wanted to collaborate externally. This restriction frustrated employees and dramatically degraded productivity. After implementing Box—the leading cloud content management solution—in a few weeks, the company waived the approval process, opening the door for users to collaborate in new and creative ways.

2. Enable the Extended Enterprise

Work is no longer bound to only one physical location or only to employees. Today business is done through a digitally connected, extended enterprise of on-site and remote users, employees, customers, suppliers, and partners. Secure access to corporate content is essential for the extended business to function successfully. The ubiquitous nature

of the cloud, combined with flexible security controls, makes using it the best way to deliver that access.

IT teams are creating new digital services and custom applications to support the increasing interconnection and digitization of business activity. But the pressure to move fast can mean that information security doesn't receive full review. IT must consider many variables, including:

- *Protection for sensitive information*
- *Central storage that simplifies access to all content*
- *Visibility and control over who is sharing what*
- *A seamless user experience*
- *How to integrate security into automated business processes and digital services*

A cloud content management platform can address these needs, by securing access for everyone in the extended enterprise. With the confidence that corporate information is secure, employees can use digital business processes to work more flexibly and creatively with partners and customers to deliver more-innovative products and services.

Storing content in the cloud also supports the “single source of truth” model: Everyone is always working with the latest version of information. This means that automated workflows are easier to implement and can operate more smoothly, as content is no longer scattered across multiple systems with their own structure and interfaces. The cloud also reduces the management burden for technical teams, instead enabling them to focus on business activity and shorten time-to-market for new digital services.

46% of respondents plan to invest in new security technology related to evolving business models.⁴

IT Takeaway: Using email is one of the most common ways employees collaborate with customers and partners, but securing it often involves deploying multiple email and web security appliances to protect information, which can create delays and degrade operations. A prominent financial services company chose the Box solution to help it

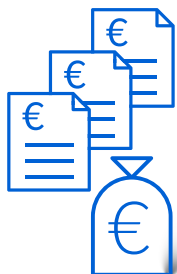
move away from using email and attachments to exchange sensitive information between advisors and clients. The new platform provides a rich user experience and enables users to securely share internal and external enterprise content while maintaining strong access controls, ensuring data security, and supporting mobile collaboration.



3. Simplify Compliance and Information Governance

The impending European Union General Data Protection Regulation (GDPR) is the latest IT compliance concern for any organization handling personal information of EU citizens. But it won't be the last. Information privacy will likely become more regulated, with individual regulations adopted by industries and countries around the world.

Data storage locations aren't the only regulatory consideration. Many businesses, not just those in regulated industries, need data retention and eDiscovery strategies. General business content, such as employee information or financial records, must be properly retained. Failure to maintain this content appropriately can result in heavy fines from regulatory bodies, such as the SEC, OSHA, or EEOC.



Companies can face fines of **€20 million** or 4% of the enterprise's total worldwide annual revenues, whichever is higher, for noncompliance with GDPR.⁵

Similar challenges can arise in preserving and presenting content for litigation. Organizations can be sanctioned and fined millions of dollars if they fail to present all relevant legal documents—not to mention the risk of an unfavorable ruling if a business can't find the evidence to prove its position.

As these examples illustrate, maintaining compliance for security and data privacy is now a key mandate for IT. The truth is, compliance and governance are



Three Questions to Ask Your CSP About GDPR

- Do you meet the cross-border processing obligations of the GDPR?
- Which certifications do you have that prove your support for these obligations?
- How can you help meet data protection obligations to an organization's customers, employees, and partners, including the right to be forgotten, transparency into info use, handling subject access requests, and security?

To learn more about GDPR, read the white paper "[Get GDPR-Ready with Box.](#)"

easier when all content is stored in a secure, centrally managed repository instead of siloed systems across the company. IT can offload many compliance requirements to the cloud service provider, which can keep pace with changing compliance requirements around the world. What's more, strong compliance also means strong protection for enterprise content when it is stored in a certified cloud.

No matter where it is stored, content should be easy to manage according to the organization's own and/or externally imposed governance principles and practices. Governance goes beyond a focus on compliance; it also addresses challenges for data retention and disposition, classification and management of records, audit trails, and support for eDiscovery. These challenges become more complex when content is scattered across multiple systems.

IT Takeaway: Security and governance go hand in hand and, as such, should work in tandem. A professional sports team in the United States uses the Box platform's governance capability to ensure that mission-critical operations content is retained as long as the team needs it. The platform provides real-time access to coaching notes, houses player records, and uses security classifications to help protect personal health information.



4. Putting User Data to Work

Data exfiltration is an important concern, one that is largely perceived as an external threat. But internal users, intentionally or not, can also pose a significant risk. Common practices such as downloading confidential files to personal devices or unsecured servers, sharing files with an unauthorized party, or sending data over an unencrypted connection can expose sensitive data to breaches.

Traditional approaches often create a large volume of alerts—and recent studies show that more than 50% of security alerts are false positives and more than 60% are redundant. Given these statistics, it's easy to see why security teams can be easily overwhelmed by a high number of false positives or struggle to differentiate between real and false threats.



58%
of organizations monitor user behavior to catch insiders who may have malicious intent.⁶

Having all content centralized in one system—versus storing content across multiple disconnected systems—can make it easier to detect real threats. The cloud also enables security professionals to collect data to track patterns of user/content interactions and behavior. New approaches to the problem, such as machine learning, can help address alert fatigue, by first establishing what “normal” user behavior is and then detecting anomalies. Today’s technologies can process logs quickly to detect irregular activity such as malicious data exfiltration attempts or inadvertent data loss caused by an inattentive user.

Even better, machine learning technology can apply insights to automatically strengthen security measures over time, based on increased activity. This approach incrementally increases protection for intellectual property and sensitive information in the cloud. It also helps IT identify the focus for user training on secure practices for information access and sharing.

Enterprises are increasingly concerned about compromised credentials, human error, and data exfiltration attempts by malicious insiders. With the cloud’s ability to rapidly adopt recent innovations such as machine learning, capabilities for detecting suspicious activity and reporting indicators of compromise become easier to integrate and help ensure that customer data remains protected.

IT Takeaway: Organizations often deal with the issue of “security alert fatigue.” In this scenario, security teams can become desensitized to alerts, leading to longer response times; in some cases, this fatigue can cause them to miss actual alerts, leading to significant data loss. But there’s good news: Customers from a variety of industries—including retail, financial services, and media and entertainment—have implemented cloud content management solutions to leverage greater control of cloud content.

The Bottom Line: Moving Content with Confidence

A robust cloud content management platform centralizes and protects content and extends security controls across the extended enterprise. This approach empowers IT to securely improve content management and collaboration, reduce data loss, maintain compliance, and simplify governance—all while taking advantage of innovations in cloud security.

Explore the cloud for content.
Click to learn more about secure content management in the cloud.

Sources: ¹ Ponemon Research ² Cisco ³ Gartner ⁴ “IDG 2017 Security Priorities Survey” ⁵ Official Journal of the European Union ⁶ IDG “2017 U.S. State of Cybercrime Survey