Regaining Control of Enterprise Content

Bringing Governance to Consumerized IT

Accellion

Table of Contents

01 | Executive Summary

The mission of any IT department comes down to managing content, devices, and connections. In recent years, IT departments have lost control in each of these areas, largely because of changes caused by the consumerization of IT and the rise of Bring Your Own Device (BYOD) computing. Once consumers began doing work on their own devices, they began selecting cloud services for syncing files across these devices. Enterprise content, once closely controlled on internal services, began to be shared widely and freely over public Wi-Fi networks and consumer cloud services, otherwise known as shadow IT solutions. Content began traveling everywhere employees went—not just during business hours, but also wherever they carried their smartphones and tablets after hours and on weekends.

Shadow IT —users adopting IT services without authorization— increases security and compliance risks, including the risk of:

- Data breaches on unsecure networks.
- Data breaches from lost or stolen devices.
- Data breaches from consumer cloud File Sync and Sharing services.
- Mobile malware infections.
- Compliance violations for lack of data security, data governance, and data sovereignty.

As data breaches become more common and more damaging, C-suite executives have taken notice. CEOs in particular understand that their job security depends on preventing serious data breaches from damaging their organizations' brand and reputation, customers, and the public's trust.

To minimize their exposure to data breaches, enterprise IT organizations need to re-take control. Employees are not about to give up their BYOD devices—and many enterprises are interested in preserving the productivity gains those devices have enabled.

To regain control, enterprises should do the following:

1. **Use private clouds as a part of a hybrid cloud strategy to enhance cloud security.**
   As enterprises migrate to more secure clouds, they should ensure that the enterprise itself keeps control of the encryption keys used for securing confidential data.

2. **Balance security and convenience in a BYOD world.**
   BYOD devices and cloud services are convenient ways of managing enterprise content. But that content needs to be secure. By adopting a secure Enterprise File Sync and Sharing (EFSS) solution, enterprises can reduce the risk of data breaches and make it easier for employees to quickly, easily, and securely access content in disparate Enterprise Content Management (ECM) systems and data stores.

To support these strategies, an enterprise-class secure content solution should provide:

- Access controls for content on desktops and on mobile devices
- Auditing and reporting across devices
- Data sovereignty and geo-fencing for enterprise content
- Encryption and encryption key management
- Data Loss Prevention (DLP)
- Anti-malware protection
- Enterprise-ready authentication
- Universal access to content stored on ECM platforms and the Cloud
- User-friendly Digital Rights Management (also known as DRM)
- Secure containers on mobile devices
- Support for remote wipe of devices

This ebook also includes a checklist of features for Enterprise File Sync and Sharing solutions.

The secure content solution should also support compliance with strict industry regulations, such as FedRAMP, Graham-Leach-Bliley and HIPAA in the United States and data sovereignty and data governance laws, such as the European Union Data Protection Directive.

Secure content management represents a new phase in the evolution of IT. It preserves the productivity gains of today's mobilized workforce while re-establishing the security and compliance practices essential to any well-run enterprise.

Imagine an employee...

in 1995 waving good-bye to his boss on Friday night, loading his desktop computer and the department server into a van, driving home, and copying whatever files he wanted to a server at a location known only to the employee.

As far as data governance goes, this situation, which was utterly implausible two decades ago, is quite normal today. Mobile devices with enterprise content are taken everywhere and used to connect to whatever local network is handy. Internal files are loaded onto cloud-based services selected by the users, and these services could be located anywhere, run by anyone with varying, but likely limited, security expertise. IT is left totally in the dark.

02 | What Happened to Enterprise IT?

In a sense, the mission of any IT department comes down to managing enterprise content, devices, and connections.

Content includes everything from Microsoft Office files to customer records to product designs to financial statements. Devices include servers of all kinds, desktop computers, mobile computing devices, and special-purpose machines such as those that might be used in a hospital or on a manufacturing floor. Connections cover everything from Internet trunk lines to LANs, WANs, and WLANs—from 100G connections down to Wi-Fi radio waves in a conference room.

It's remarkable, in each of these areas, to consider just how much the typical IT department has lost control. Data volumes have exploded, networks are faster, and devices are both smaller and more powerful than ever before. But despite these advances, IT has less visibility and ability to act decisively than ever before, creating major risks in the areas of security and compliance.

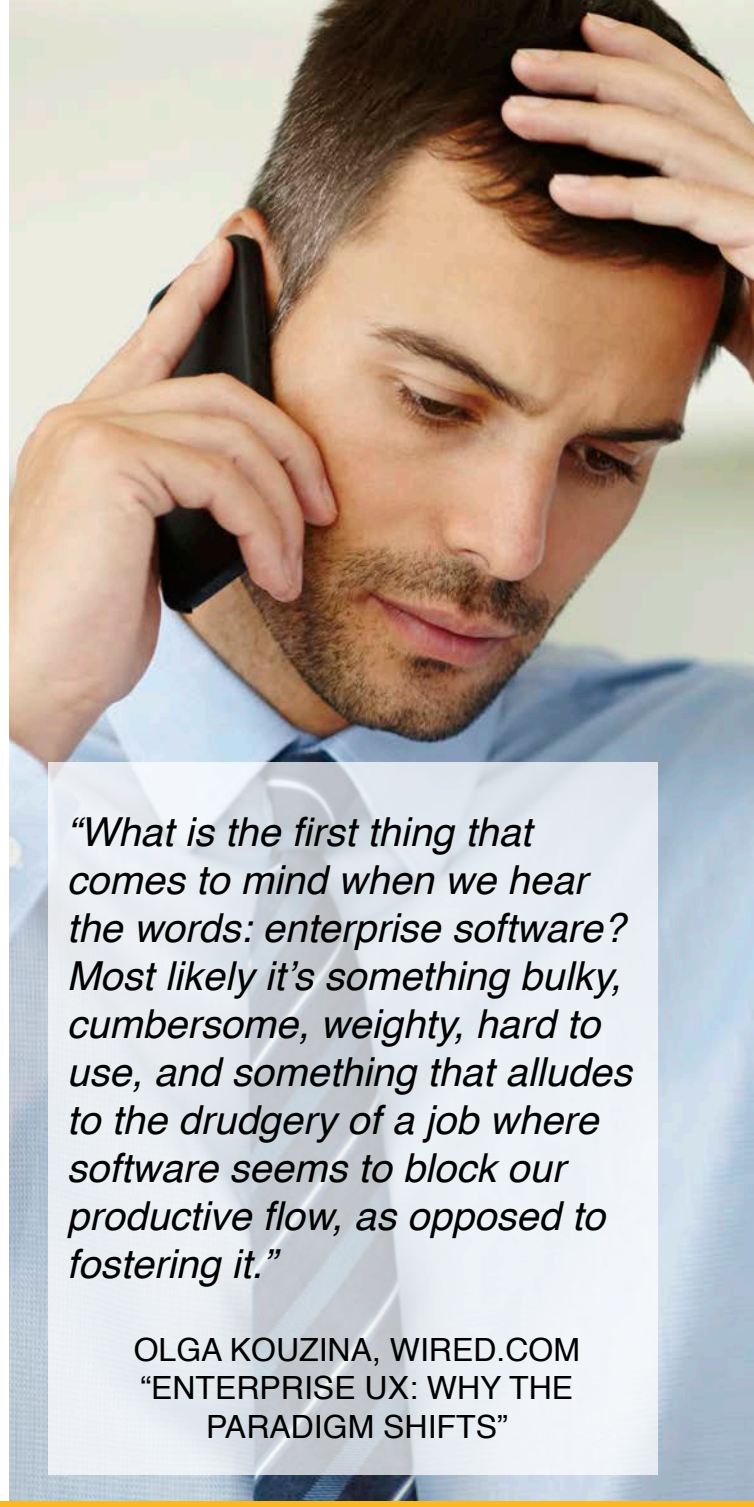
What caused IT to lose control? The chief culprit is shadow IT, the use of off-the-shelf consumer products for business use. IT has been "consumerized" primarily by the Bring Your Own Device (BYOD) movement in which employees supply their own mobile devices—primarily smartphones and tablets but also now wearables such as the Apple Watch—and use these devices for both personal activities and work.

Once employees started bringing their own devices to work, everything changed.

Suddenly, IT departments were no longer carefully selecting, configuring, or provisioning the devices that would connect employees to enterprise networks and enterprise content. Suddenly devices of unknown provenance and condition could connect to networks and access all sorts of proprietary information – from confidential product plans to patient data to internal emails.

Because these devices are portable, they go everywhere employees go. They commute home with their owners at night. They go to restaurants and bars and soccer games and airports. Some of them get left in taxis and in restaurants. Others end up being stolen from hotel rooms and parked cars.

Because these devices have to be useful wherever they go, they need data services wherever they go. These services include File Sync and Sharing services that automatically copy and synchronize files across all the devices belonging to a user. Other services include email, calendaring, and task management and project management, along with special-purpose applications suited to the user's specific job. Today, most of these services, like the devices themselves, are selected by the employee, not the IT department.



"What is the first thing that comes to mind when we hear the words: enterprise software? Most likely it's something bulky, cumbersome, weighty, hard to use, and something that alludes to the drudgery of a job where software seems to block our productive flow, as opposed to fostering it."

OLGA KOUZINA, WIRED.COM
"ENTERPRISE UX: WHY THE PARADIGM SHIFTS"

The willingness of employees who use BYOD to sign up for this or that public-cloud service without IT's knowledge or permission has lead to the phenomenon of Bring Your Own Cloud (BYOC), also known as "rogue clouds." These can include Dropbox, Evernote, Google Drive, and iCloud. The majority of cloud services used in an enterprise—about 86 percent according to a recent survey—are unauthorized by the IT department. Another survey, which focused on U.S. healthcare organizations (HCOs), found that even in this highly regulated industry, rogue clouds outnumbered authorized services by over 10 to 1. In fact, the typical healthcare employee was found to be using 26 different cloud services. On average, HCO IT departments estimated they had authorized 60 cloud services, but over 950 were in use.

One reason that employees are so quick to adopt public-cloud services is that they have had difficulty accessing traditional IT content stores from mobile devices. The content employees need daily for their jobs is distributed over disparate "silos," including Enterprise Content Management (ECM) platforms such as Microsoft SharePoint and EMC Documentum. To collect files from different sources requires navigating from one silo to another, entering credentials on a small screen, and downloading or copying files, perhaps in violation of the organization's security policies. Not only are these content silos distinct from one another (i.e., not synced to one another), they are also notoriously difficult to access on mobile devices, especially on remote devices that are required to VPN through an organization's firewall.

From a security point of view, rogue IT becomes a tail wagging the dog scenario. Employees adopt mobile devices for convenience. On these devices, basic tasks like messaging and Web surfing are easy, but accessing enterprise content is difficult. To overcome this difficulty, employees replicate enterprise content on public-cloud services, which are easy to use on mobile devices. Unfortunately, these shadow IT services are operating outside the purview and control of the IT organization. For any organization concerned about security and compliance—and

this should be every company—that's a problem. But risky shadow IT solutions aren't the only way that consumerized IT is having an affect on IT organizations.

Consumerized IT and End User Expectations

Employees think nothing of signing up for new cloud services, in part because signing up for those services has become so easy. Just fill out a Web form—which might require only an email address—and begin using the service. "Freemium" services, which offer basic features to anyone who signs up, might not even ask for payment information until a trial period expires or the user needs more advanced features. All in all, the standard user experience with popular cloud services is fast, frictionless, and sometimes even a bit fun.

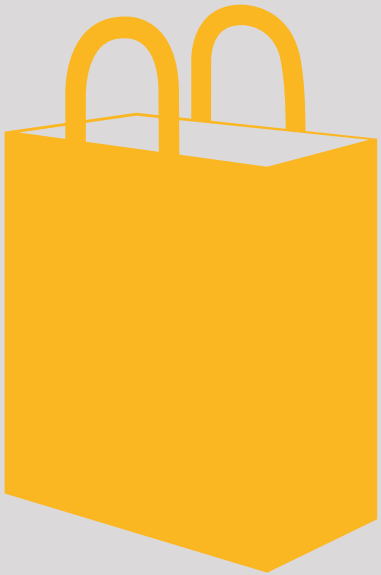
Employees now carry these expectations over to the workplace. And when they encounter traditional enterprise software, including colossal software suites that have their legacy in the 1990's, they balk at the uninspiring interfaces, the clunky procedures, and the lack of intuitive design. The disparity between slow, complicated enterprise software and the sleek, easy-to-use mobile apps only drives employees further in the direction of consumerized IT. After all, why strain yourself steering a barge when you can make the same journey more quickly on a Jet Ski? New apps are easy to use, so naturally employees are drawn to them.

The implication for IT departments is clear: As long as enterprise applications are more difficult to use than new, cloud-generation mobile apps, employees will yield to the siren call of consumer devices and public-cloud services. It's incumbent upon responsible IT and security professionals to ask, then:

What are the risks and repercussions of this new consumerized IT?

03 | Risks and Repercussions of Consumerized IT

Employees today decide which devices to use, which data services to pay for, and which networks to connect to. Mobilizing workers may boost productivity, but mobilizing them through BYOD carries significant risks and repercussions for security, which enterprises must address.



These risks include:

- **Increased risk of data breaches from unsecure networks.**
  When employees connect to enterprise services from public Wi-Fi hot spots, they risk having their communications intercepted by man-in-the-middle attacks and other forms of eavesdropping that cull login credentials and other valuable information.

- **Increased risk of data breaches from lost or stolen devices.**
  Smartphones and tablets go everywhere. Sometimes they don't come back. Over a million smartphones were stolen in the U.S. in 2014. In fact, about 15% of all data breaches are the result of devices being lost or stolen, according to Verizon.

- **Increased risk of data leaks through consumer cloud File Sync and Sharing software.**
  Consumer cloud file sharing services such as Dropbox and Google Drive can lead to data breaches, either through the careless distribution or storage of files or by the services themselves suffering security outages, such as when Dropbox disabled passwords on all accounts for 4 hours.

- **Increased risk of malware infection.**
  Mobile devices make great targets for hackers, because they contain valuable information such as login credentials and contacts lists, are running comparatively immature operating systems, and are often used quickly and haphazardly with little thought of security—these devices after all are frequently glanced at, tapped, and tucked away. Many employees are quick to download apps from unknown vendors, unaware that those apps may contain adware or malware. Mobile malware variants in fact are growing quickly. Mobile security firm Lookout reported that incidents of mobile malware grew 75% from 2013 to 2014, and over 16 million devices were infected with mobile malware in 2014, according to Alcatel-Lucent.

- **Non-compliance with industry regulations.**
  Industry regulations such as FINRA and HIPAA require that organizations closely manage confidential data. That typically involves knowing exactly where data is being stored, ensuring that it is encrypted in storage, that only authorized users gain access to it, and that all access and transmission of that data is monitored and logged. When BYOD users use public-cloud services to handle confidential data, most or all of those requirements end up being violated. Public-cloud services were designed for convenience—for consumers to upload personal files, photos, and videos, not for business users whose content must be continuously secured, monitored, and tracked.

- **Loss of data sovereignty.**
  Many countries have laws mandating that customer data be stored within the nation's boundaries. When employees sign up for public-cloud services, they usually have no idea of where the data will reside. Many public-cloud services are not designed to track or monitor where data is stored or where processes

are run; in the name of efficiency, data and services migrate from data center to data center based on resource availability and load balancing. (Amazon Web Services and other cloud service providers often make no promises about where a process might be run; they migrate workloads automatically in the name of efficiency). When employees load enterprise data into these services, they are likely to end up violating data sovereignty regulations.

These risks could produce a number of longer-term repercussions:

- **Loss of intellectual property and competitive advantage.** Data breaches, along with data leaks from lost or stolen devices or the careless use of public-cloud file sharing services, can lead to data leaks that forever erode an organization's competitive advantage. When IBM conducted a security audit a few years ago, it found confidential documents such as future product plans widely distributed over the Internet through services such as Dropbox and Evernote. To stem these losses, the company promptly banned these services from its networks. But competitive data can be lost in other ways, too, such as hackers stealing credentials from mobile devices and using those credentials to gain access to internal file servers and other data sources. In its annual investigation of data breaches, Verizon discovered that about 28% of cyber espionage breaches were directed at manufacturing companies—a clear indication that hackers are interested in stealing trade secrets and erasing competitive advantages.

Hybrid clouds are going mainstream. "[We] saw a spike in multi-cloud strategies in 2014, and that will continue into 2015," says Chris Wolf, CTO of the Americas, VMware. "CIOs will continue to seek out the flexibility that [hybrid clouds offer]. And senior IT decision makers will invest in hybrid cloud architectures to future-proof their applications and services."

JENNIFER LONOFF SCHIFF,
CIO.COM
"8 ENTERPRISE SOFTWARE PREDICTIONS FOR 2015"

- **Regulatory fines.**
  When regulators discover, either through audits or publicized data breaches, that data security and governance mandates have been violated, they are not shy about imposing stiff penalties. Penalties for HIPAA violations, for example, have reached multiple millions of dollars.

- **Loss of funds.**
  In some cases, hackers have used stolen login credentials to divert funds from corporate bank accounts. For example, hackers were able to hijack the company payroll service of Tennessee Electric Company, Inc. and siphon $327,804 from the company's bank account. The funds were transferred to 55 different accounts belonging to money mules, who in these situations are typically instructed to promptly wire the funds to foreign accounts beyond the reach of the law.

- **Loss of brand equity.**
  When news of a data breach reaches customers and the public, the affected enterprise usually suffers a loss in brand equity. Some customers will close their accounts and take business elsewhere while prospective customers will give more consideration to industry competitors. Crisis communications navigating customers and other stakeholders through the breach and its fallout require time, money, and tact. In a recent study of data breaches, the Ponemon Institute found that activities resulting from a data breach included "abnormal turnover of customers, increased customer acquisition activities, reputation losses and diminished good will," leading to a total average "lost business" cost per breach of $1.57 million in 2015.

Given these high stakes, it's worth taking a closer look at data breaches: their prevalence, their causes, and their costs.

Data Breaches: A Closer Look

Data breaches are becoming increasingly common and costly. They begin with security breach attempts—what Verizon and other security researchers refer to as security incidents. There were 42.8 million detected security incidents in 2014, and the number of detected incidents has been rising on average 66% year-over-year since 2009.

All those security incidents keep network defense solutions like Intrusion Detection Systems (IDS) busy. Enterprise IT teams find themselves deluged with daily IDS alerts, and many enterprises have teams dedicated full time to determining which alerts are merely false alarms and which truly signal that an attack is under way, leading to an actual data breach. The sophistication of attacks and the inaccuracy of alerting systems make detecting and stopping attacks a drawn-out affair. For example, the average time to discover a data breach is 256 days (about 8.5 months), giving hackers plenty of time to steal data such as customer records or product plans.

When breaches occur, they prove very costly. In a recent report they published with IBM, surveying 350 companies and spanning 11 countries, the Ponemon Institute found:

> The average consolidated total cost of a data breach is $3.8 million representing a 23 percent increase since 2013.
>
> The study also found that the average cost incurred for each lost or stolen record containing sensitive and confidential information increased six percent from a consolidated average of $145 to $154. Healthcare emerged as the industry with the highest cost per stolen record with the average cost for organizations reaching as high as $363. Additionally, retailers have seen their average cost per stolen record jump dramatically from $105 last year to $165 in this year's study.

In the U.S., the average number of records stolen in a breach was 28,070, resulting in an average cost of $4,322,780 per breach. This cost includes both direct costs and indirect costs.

> Direct costs refer to the direct expense outlay to accomplish a given activity such as engaging forensic experts, hiring a law firm or offering victims identity protection services. Indirect costs include the time, effort and other organizational resources spent during the data breach resolution. It includes the use of employees to help in the data breach notification efforts or in the investigation of the incident. Indirect costs also include the loss of goodwill and customer churn.

The ratio of direct costs to indirect costs varies by country. In the U.S., direct costs typically account for 65% of total costs. Indirect costs weigh in at 35%. The study also found that hackers and criminal insiders were responsible for 47% of the data breaches reported. Verizon, in its own study, discovered that external actors were responsible for over 80% of data breaches. What's clear from both studies is that enterprises should assume that they will be attacked by external parties and ready their defenses accordingly.

Data Breaches and the C-Suite

With data breaches so frequently in the news and so sweeping in their effects—over 1 in 4 Americans had personal data compromised in 2014—C-suite executives are under pressure to drive security initiatives and make sure that data governance is more than a checkbox item.

Consider Sony Pictures Entertainment. When hackers broke into Sony's IT systems and published a number of embarrassing emails, Sony chairman Amy Pascal found herself under pressure to resign, which she eventually did. The breach at Ashley Madison led to the resignation of Avid Life Media's CEO, Noel Biderman. And in the public sector, Katherine Archuleta, the director of the U.S. Office of Personnel Management, was forced to resign after Chinese hackers stole personal data belonging to millions of federal employees.

1 in 4 Americans
had their personal security compromised in 2014

Several well-publicized data breaches such as Anthem, Ebay, Adobe, Dropbox, The Home Depot, JP Morgan Chase, and others seem to have put C-suites and boards of directors on notice. In its survey, 79% of C-level executives in the US and UK surveyed by the Ponemon Institute say executive level involvement is necessary to achieving an effective incident response to a data breach, and 70% believe board level oversight is critical.

An even better result would be boards and C-suite executives driving IT organizations to regain control of content, devices, and networks to greatly reduce the odds of a breach occurring in the first place.

Which raises the question, how can enterprise IT organizations regain control of consumerized IT?

The Enterprise Strategy Group's ROI Assessment of Accellion's Private Cloud Solution

An Economic Value Analysis (EVA) from industry analyst firm Enterprise Strategy Group (ESG) shows that a private cloud deployment of Accellion's kiteworks solution provides five times the ROI over a public cloud file sharing solution for a typical enterprise.

The ESG EVA comprises an ROI calculator and accompanying report that compares the annual cost of ownership and annual cost benefits of deploying the kiteworks by Accellion private-cloud EFSS solution compared to public cloud alternatives. The improved ROI from kiteworks results from a lower annual cost of ownership, greater cost benefits from increased productivity, and IT operations improvements and also a significantly lower risk of data breaches.

"Deploying kiteworks offers the opportunity for enterprise organizations to drastically increase their IT and user productivity at a significantly lower total cost of ownership compared with EFSS alternatives," said Terri McClure, Senior Analyst at ESG. "In fact, ESG's analysis of a typical enterprise use case demonstrates kiteworks results in an impressive estimated ROI of nearly 400%, thanks primarily to kiteworks' productivity benefits. This compares with less than 75% ROI for generic consumer-grade cloud solutions that don't have some of the advanced productivity and deployment options such as those kiteworks offers."

Don’t Overlook Encryption Key Management

Encryption key management is often an overlooked area of Enterprise File Sync and Sharing (EFSS) security. Encryption is needed to protect content in all three possible states: at rest (in storage), in transit (for example, when moving between a cloud storage service and a mobile device), and in use (for example, when accessed through search engines or APIs). The entity that has access to the encryption keys, controls access to the encrypted content.

Enterprises should recognize the strengths and weaknesses of cloud architectures vis-à-vis encryption key management:

- On-premises cloud EFSS solutions run in an internal data center and give enterprises full control of the encryption keys for data in all three states: in transit, at rest, and in use.
- Dedicated private-cloud EFSS solutions, which provide each organization its own dedicated application instance in a hosted cloud platform, offer the capital expenditure benefits of a hosted environment while still providing better security than multi-tenant public cloud solutions.
- Multi-tenant public cloud EFSS services run in a hosted cloud platform where all customer data is co-mingled in one shared environment. Many public cloud EFSS solutions fail to protect data in use, while some offer optional key management services that give customers control over encryption keys, without an added cost.
- Not all public-cloud EFSS solutions offer encryption. Those that do offer encryption usually manage the keys themselves. In turn, enterprises must accept the fact that they don’t control the security of their content in the cloud.

To maintain full control over the encryption keys—and hence full control over confidential content—without added cost, enterprises should deploy a private-cloud EFSS solution, which includes built-in key management controls, and expand that solution in a hybrid cloud environment if a strong business case can be made.

04 | Retaking Control of Enterprise IT

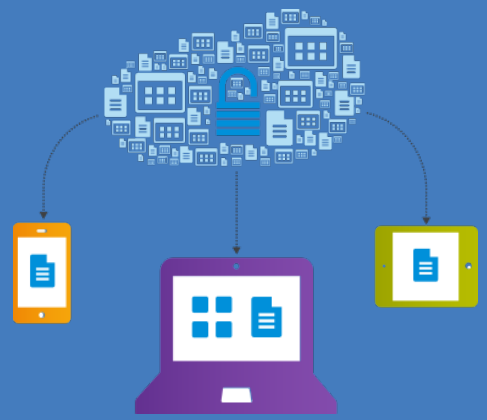
Retaking control of enterprise IT does not mean abandoning cloud architectures and mobile computing. These technologies are too promising—and by now, too entrenched—to ignore.

Instead, retaking control of enterprise IT means managing these powerful technologies in a way that serves the goals of the enterprise in terms of business agility, efficiency, and security, while also meeting the needs of users to have fast, convenient access to the content and tools they need to do their jobs.

Retaking control means adjustment and refinement, not replacement. It involves adding monitoring capabilities and control functionality to the cloud services installed by employees but otherwise unauthorized and unsupported by an organization's IT department, aka shadow IT. It brings these cloud services out of the shadows and onto the illuminated dashboards of administrators and compliance officers, while ensuring that content and features remain a just a click away for users.

It also involves simplifying IT, improving connections, eliminating the hassle of content silos and creating a new IT experience that is not just more secure, but also more efficient, effective, and seamless.

Since cloud computing is becoming the de facto model for application execution and data storage, let's consider how this transformation can be effected in the world of cloud services, which today comprise public clouds, private clouds, and hybrid clouds.



Strategy #1: Use Private Clouds as a Part of a Hybrid Cloud Strategy

Without question, public clouds like Microsoft Azure and Amazon Web Services are popular with enterprises. Enterprises spent $152 billion on public clouds in 2014, and by 2019, annual spending will reach $316 billion. Gartner forecasts that over the next five years, enterprises will spend a total of $1.2 trillion on public cloud services, representing a 16% CAGR.

Given the popularity of SaaS business applications like Salesforce and Amazon Web Services (AWS) for internal projects, the billions being spent on public cloud services should surprise no one. But while investments in public cloud services are increasing in absolute terms, their comparative share of cloud spending overall is expected to decline, according to Gartner.

In contrast, investments in private clouds will remain steady, and investments in hybrid clouds that combine private and public clouds are expected to rise sharply. In fact, cloud architectures that rely on private clouds in some way—either exclusively or in a hybrid configuration—will end up with 66% of the market by 2017.

A 2015 survey by cloud provider RightScale found strong evidence for the emergence of hybrid computing. “Eighty-two percent of enterprises have a hybrid cloud strategy, up from 74 percent in 2014.” They also found that while public clouds have been more widely adopted than private clouds, private clouds are running more workloads.

Why the growing interest in private and hybrid clouds? In large part, because enterprises remain skeptical about the security of public clouds. When Gartner asked enterprises why they were not using public clouds today, the most cited reason by far—cited by 63% of respondents—was concern about data security and privacy.

The Promise of Private Clouds and Hybrid Clouds

Private clouds give enterprises full control of their content. They enable enterprises to enforce encryption and other security controls to protect sensitive content. Enterprises can take full control over the issuing, management, and revocation of encryption keys rather

To regain control over enterprise IT, enterprise IT departments must provision a new generation of services that combine the ease-of-use of consumerized IT with the rigorous security and control of traditional enterprise software.

than ceding control of the keys to a third-party vendor. The end result is a more defensible IT network and less risk of a data breach or a compliance violation. An added bonus is stronger compliance and data sovereignty. Because the enterprise knows which content is in which of its data centers, and can enforce policies assigning specific data center locations to specific users, enterprises using private clouds can comply with data sovereignty regulations, such as those enforced in the EU.

Hybrid clouds are increasingly popular because they allow enterprises to create the secure environments they want in private clouds, then scale those environments as needed using trusted, carefully designed and vetted public-cloud resources.

If private clouds offer security and control, their combination with public clouds offers the path to a hybrid cloud strategy offering agility, scale and security.

Debunking the Myth of Public Cloud ROI

One final consideration for adopting a hybrid cloud strategy: return on investment (ROI). Public clouds are famous for their ease-of-use, quick start-up times, and impressive ROI. Without doubt, public clouds can deliver impressive ROI, especially compared to traditional server farms comprising on-premises hardware.

But as impressive as the returns from public clouds can be, the ROI from private clouds can be even greater. A well-designed private-cloud offering has the potential to deliver superior ROI by optimizing user productivity and overall manageability and control. The ROI of public and private clouds has been studied and compared by analyst firms such as the Enterprise Strategy Group, who now recommend private clouds for organizations focused on ROI from cloud deployments. Of course, if you factor in the financial and reputational costs associated with a data breach, which is heightened with a public cloud architecture, the ROI of a private cloud solution is even more attractive.

For the majority of employees today, mobile computing is simply computing

Mobile devices have become the platform of choice for checking email and messaging, and they're increasingly popular for Web surfing, watching videos, and listening to music.

Facebook, messages from friends, photos, and the rest of the Web are always just a click away. Through consumer apps like Facebook, employees grew to expect information to be delivered quickly, concisely, and with strong visual content. They wonder why business applications cannot convey information with the same power and simplicity.

If immediacy and convenience are going to be part of an IT strategy for increasing productivity—and perhaps employee job satisfaction along the way—then it makes sense for enterprises to embrace BYOD and strive to bring enterprise content and tools to the world of mobile computing.

Smartphones have completely permeated our lives—at work, at home and everywhere else.

This is an important opportunity for enterprise IT organizations—a chance to replace comparatively slower and more cumbersome legacy applications with a new generation of business solutions that leverage the UI advantages common in today's popular mobile apps.

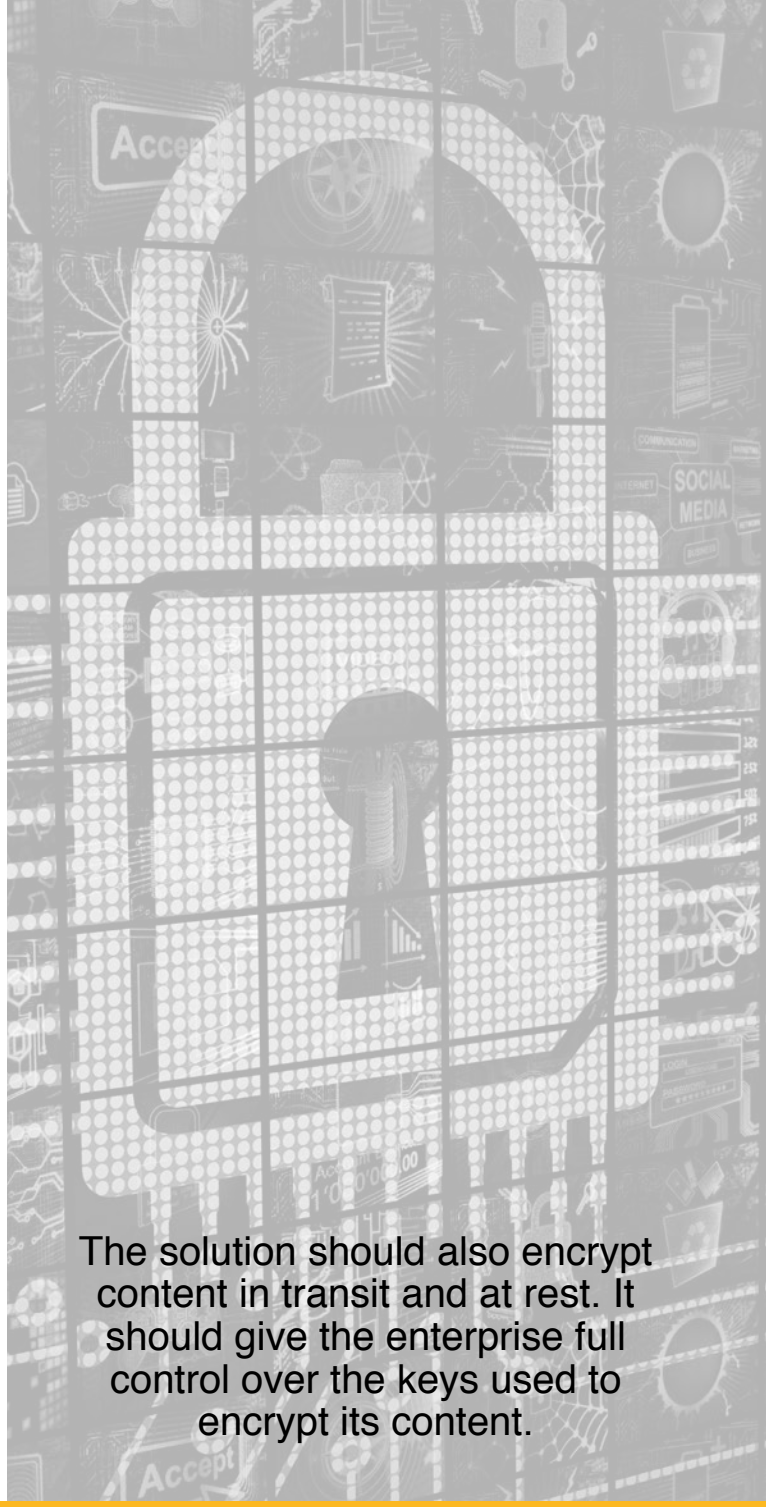
And if the mobile solutions selected by IT are truly powerful and easy to use, then employees will not be tempted to seek "rogue cloud" alternatives. They will already have a fast, easy, and (now) secure solution right in their hands.

Strategy #2: Balance Security and Convenience in a BYOD World

Moving toward hybrid-cloud services promises to restore much of an IT department's control over content and connections. But to regain even more control, it's necessary to consider not just the cloud services and connections employees are using, but also their devices. After all, many employees first signed up for public-cloud services as a way of syncing work documents across all their mobile devices (laptops, tablets, smartphones and now wearables), so they would always have the files and other content they wanted on hand. These devices, which are taken everywhere, are storing enterprise content and login credentials and as long as these devices are unprotected, enterprise content is at risk.

The world of BYOD won't change. There will continue to be iPhones, iPads, Android devices, and whatever other mobile devices, such as wearables like Apple Watch, are made available to consumers. What enterprises can change and control is the applications running on these mobile devices and the cloud-based software that interacts with those applications, creating a new generation of secure, mobile-first enterprise solutions.

A secure EFSS solution or "mobile content management" solution can bring security to the work employees do, namely creating, editing, and sharing content on mobile devices. Such a solution has the opportunity to bring security and policy enforcement to



The solution should also encrypt content in transit and at rest. It should give the enterprise full control over the keys used to encrypt its content.

users “where they live”—on their mobile devices and in the cloud. In effect, it creates a layer of security, control, and monitoring over the wild, ungoverned terrain of today’s consumerized IT. It secures devices which are unsecured today, and completes the mantle of IT’s control over content, connections, and devices.

Productivity Whenever and Wherever

The promise of such a mobile security solution depends on its breadth. It must work with whatever devices employees happen to be carrying, including the ever-broadening array of Android and iOS devices available to consumers today.

The solution should work consistently and seamlessly across all devices, including desktops. Ideally, it will become the workspace employees are comfortable using on any device, regardless of its location or screen size.

Security that Works for Employees

One of the best ways of ensuring that employees adopt a secure mobile content solution is to make the solution not just easy to use but also empowering. It should make common tasks easy, even on devices like smartphones that have small screens and limited typing capabilities.

One way to empower users is to simplify their access to content stored on an enterprise content management (ECM) platform. Especially when working remotely, employees struggle to access ECM platforms such as Microsoft SharePoint through VPNs that are slow and cumbersome on smartphones and tablets. To access files from three different platforms, they might need to log in four times: once to the VPN, then once to each of the three platforms.

Ideally, authenticated users should be able to log in to a single, secure content environment that gives them convenient access to whatever content they need from whatever ECM platform or content repository it resides in.

Employees should be able to set up their content apps and work environment themselves, using the same self-service provisioning models that have become so common in consumer mobile apps.

And employees should be able to manage and share their content easily and securely.

Specifically, employees should be able to:

- Sync content across all their mobile devices and desktop systems.
- Collect and organize content in whatever folder hierarchy they want.
- Share comments about content so colleagues can quickly understand the context of content being shared.
- Share content easily with other employees and with trusted external users, such as business partners.
- Restrict some content to View-Only mode, so that it can be read but not copied or forwarded by other users. View-Only mode should even prevent users from taking screenshots of protected content.
- Withdraw confidential content that has been shared inadvertently, so that mistakes of the moment do not have lasting repercussions.
- Through the same secure solution, access content in public-cloud EFSS services such as Dropbox or Google Drive.

Empowered by a secure content management solution like this, IT is now back in control. And the solution's ability to connect securely to ECM platforms and public-cloud services such as Dropbox, enables IT departments to bring security, monitoring, and control to the rogue clouds that have become so prevalent in today's BYOD culture.

Security Best Practices

To guard against data breaches and protect valuable enterprise content, the mobile content management solution should support these security best practices:

- **Access controls for content**
  Administrators should be able to control which users can access which content. These security controls should extend to users who are outside the organization—users such as business partners and, when appropriate, customers. Administrators should be able to define role-based access controls, so security policies can be broadly enforced.

- **Auditing and reporting**
  The solution should log user activity and enable IT administrators and security teams to audit the access and distribution of content. Administrators should be able to generate reports for trend analysis and compliance.

- **Data sovereignty and geo-fencing**
  The solution should support data sovereignty laws. Private cloud deployments enable enterprises to know exactly where their data is residing—namely, on-premise. "Geo-fencing" rules go a step further and can limit content by location. For example, certain pieces of content might be accessible only by a division in the U.K. Employees in a specific country might be permitted only to access services running within that country's borders.

- **Encryption and Encryption Key Management**
  The solution should encrypt content in transit and at rest. It should give the enterprise full control over the keys used to encrypt its content.

- **Data Loss Prevention (DLP)**
  The solution should integrate with an enterprise's existing DLP solutions, so that DLP policies can be enforced consistently across cloud services and applied to business communications on mobile devices. Integrating DLP into mobile content management helps ensure that confidential data is not inadvertently leaked.

- **Anti-malware protection**
  The solution should provide built-in AV scanning on mobile devices, so that enterprise content and apps are safe from mobile malware.

- **Enterprise-ready authentication**
  The solution should meet enterprise requirements for authentication, including supporting two-factor authentication (2FA) and single-sign-on (SSO). Naturally, the solution should integrate with 2FA and SSO solutions an enterprise has already deployed. The solution should also allow administrators to enforce the use of PINs or passcodes on mobile devices, enforcing authentication on devices known to be storing mission-critical content.

- **Uniform Access to all ECM platforms through a "single pane of glass"**
  The solution should provide a single, universal mobile-ready interface to all ECM platforms an employee is authorized to access. It should enable ECM security policies to be enforced by user and by content, while hiding the complexities of content access from users.

- **User-friendly Digital Rights Management (DRM)**
  The solution should enable employees to define strict digital rights for the content they share, so that recipients of shared content have only the rights that are appropriate for their roles. For example, the solution should enable employees to prevent shared content from being forwarded to unauthorized users. It should support View-Only roles for content, providing recipients with an image of a file, rather than content that can be forwarded or copied and pasted. The solution should also enable employees to easily watermark content as confidential, so that recipients are reminded of the content's sensitivity.

- **Secure containers**
  The solution should provide protected storage areas, known as "secure containers," to protect files on mobile devices from unauthorized access, and from malware contamination by other files on the device. All files in secure containers should be encrypted, and accessed in a separate secure memory space available only to authorized apps. In addition, IT administrators should be able to track and manage all files in secure containers.

- **Support for remote wipe**
  The solution should enable authorized administrators to remotely delete content from specific mobile devices. If an employee leaves an organization, administrators should be able to remotely delete enterprise content from every mobile device under management. Similarly, if a device is lost or stolen, administrators should be able to delete all enterprise content on that particular device, and prevent the device from having access to enterprise resources such as file servers.

Supporting Compliance with Industry Regulations and Laws

The mobile content solution should also support an organization's compliance processes with strict industry regulations, and data sovereignty and data governance laws, including:

- FedRAMP, which establishes data security standards for U.S. federal agencies adopting cloud services.
- FIPS 140-2, which sets general data security standards for U.S. federal agencies.
- Graham-Leach-Bliley, which requires financial services organizations to protect customer records.
- HIPAA and the HITECH Act, which require U.S. HCOs and their business partners to protect Protected Health Information (PHI).
- Sarbanes-Oxley, which requires public companies to monitor and control the distribution of financial information.
- The European Union Data Protection Directive, which establishes data privacy guidelines for individuals in all EU member states.
- The Canadian Personal Information Protection and Electronic Documents Act (PIPEDA), which describes individuals' rights to know who is collecting their personal data and how it is being used, and which stipulates that individuals have a right to expect that their data is managed securely.

The mobile content security solution should also be capable of complying with new data sovereignty rules, such as those pending in Brazil, Canada, Germany, and Russia.

05 | Conclusion

Consumerized IT is not going away. In the coming years, mobile devices will only increase in importance. Enterprise services will continue their migration to clouds, public and private. And data breaches will continue to occur, threatening these mobilized IT infrastructures and the organizations that depend on them.

To regain control, IT organizations need security solutions that work with the mobile devices and cloud services already in place. A secure mobile content management solution—comprising on-device security features, integration with ECM platforms and enterprise IT services such as DLP and SSO, and top-down monitoring and policy features for administrators—can restore the visibility and control that IT organizations have been missing. By securing content, connections, and mobile devices, such a solution enables enterprises to leverage the productivity advances of consumerized IT, while minimizing the security and compliance risks of ad hoc, employee-driven IT provisioning.

Secure content management represents a new phase in the evolution of IT, preserving the productivity gains of today's mobilized workforce while re-establishing the security and compliance practices essential to any well-run enterprise.

For more information about Accellion's kiteworks solution for secure content management, please visit www.accellion.com.

kiteworks™

by Accellion

Summary: Your EFSS Data Security Checklist

The remainder of this document presents a checklist of features that SMBs and large enterprises should look for in a secure content management solution. The features are organized into the following categories:

- ☐ **1. Architecture and Deployment Models**
- ☐ **2. Encryption**
- ☐ **3. Security Controls and Compliance**
- ☐ **4. Integration**

Architecture and Deployment Models

Deployment Models should include on-premises and hosted solutions, offering organizations a range of options for optimizing security, operational costs, and scalability.

- [ ] **100% On-Premise**
  The solution should be deployable completely in an on-premises environment, offering complete control over the availability, integrity, and confidentiality of data. The solution should support popular private cloud platforms, such as VMware, Citrix XenServer, and Microsoft Hyper-V.

- [ ] **Private cloud**
  To minimize the risk of data leakage or service outages from public clouds, the solution should be optionally deployable on a hosted private cloud, under the complete control of the organization's IT department. Private cloud hosted deployment provides the flexibility and scalability of a managed service offering, while ensuring high levels of security and control.

- [ ] **Hybrid cloud**
  The solution should also support increasingly popular hybrid cloud architectures, seamlessly spanning on-premises private clouds and hosted environments, to provide an optimal combination of security, control, and flexibility.

- [ ] **Multi-tier architecture**
  The solution should feature a modular architecture, enabling functionality to be divided into multiple tiers for increased security and scalability. Industry best practices typically call for a presentation tier, an application tier, and a database tier. Each tier should be able to be placed anywhere in the network (for example, the presentation tier in the DMZ, while the application and database tier reside behind the internal firewall). Furthermore, each tier should be able to scale independently to meet the specific workload requirements of the enterprise using the solution.

Encryption

The solution should include encryption technology to protect the confidentiality and integrity of files on mobile devices, and in transit.

- [ ] **Encryption at rest and in transit**
  The solution should apply industry-standard encryption to protect data at rest on servers and mobile devices, and in transit to and from end points.

- [ ] **Ownership of encryption keys**
  Ownership of the encryption keys used to encrypt data should reside with the enterprise, not with the cloud service provider. Enterprises should have full access to data and control over the means of that data being encrypted at all times.

Security Controls

The security controls should be rigorous enough to support compliance with industry regulations, such as the Healthcare Insurance Portability and Availability Act (HIPAA) and Sarbanes-Oxley (SOX). In addition, governance capabilities such as eDiscovery should be available natively.

- [ ] **Data sovereignty support**
  Administrators should be able to control the physical storage location of specific workspaces and files for specific users. For example, IT administrators should be able to ensure that files belonging to German users are stored in Germany, while files belonging to American users are stored in the United States.

- [ ] **FIPS 140-2 Certification (Encryption)**
  To allow use by U.S. federal agencies, the solution should support FIPS 140-2 certified encryption.

- [ ] **Workspace-specific access controls**
  The solution should also support workspace-specific access controls so that permissions for workspaces can easily be assigned to teams or departments.

- [ ] **AV protection**
  The solution should provide real-time malware scanning of content each time a file is uploaded or downloaded. Malware-infected files should be automatically quarantined, and prevented from being uploaded to shared workspaces. The AV scanning feature should automatically update with new signature files when new forms of malware are reported by security researchers.

- [ ] **Two-factor authentication**
  The solution should provide two-factor authentication, preferably via integration with existing strong authentication systems.

- [ ] **User-friendly DRM**
  The solution should be able to protect files from unauthorized downloads, be able to withdraw a file already sent, and provide deterrence against taking screen shots of sensitive documents.

- [ ] **eDiscovery**
  The solution should be able to meet requests for legal holds by providing the ability to preserve and collect all relevant files, emails, and metadata, as well as the ability to enforce content retention policies.

- [ ] **DLP integration**
  The solution should be able to integrate natively with leading Data Loss Prevention solutions to automatically detect and quarantine documents that violate regulatory requirements.

- [ ] **Secure containers**
  The solution should provide protected storage areas, known as “secure containers,” to protect files on mobile devices from unauthorized access, and from malware contamination by other files on the device. All files in secure containers should be encrypted and accessed in a separate secure memory space available only to authorized apps. (See “Mobile app whitelisting” below.) IT administrators should be able to track and manage all files in secure containers.

- [ ] **Support for remote wipe**
  The solution should enable authorized administrators to remotely delete content from specific mobile devices. If an employee leaves an organization, administrators should be able to remotely delete that employee’s content from every mobile device under management. If a device is lost or stolen, administrators should be able to promptly delete all enterprise content on that particular device, and prevent it from being used to access enterprise resources, such as file servers in the future.

- [ ] **Mobile app whitelisting**
  The solution should support a whitelist of mobile apps approved by the IT organization. Only mobile apps on the whitelist should be allowed to be downloaded, opened, viewed, or used.

- [ ] **Support for prevalent mobile platforms (Android, iOS, Windows)**
  The solution should support the most popular mobile platforms in use by businesses and government agencies, including Android, iOS, and Windows.

Integration

To re-establish the IT department's control over content, the solution should integrate with all content stores, on-premises and in the cloud, official and unofficial, being used by enterprise employees.

Integration with Enterprise Content Management (ECM) Platforms such as Microsoft SharePoint

Enterprise Content Management systems help businesses store, organize, and protect files. The most popular ECM platform, Microsoft SharePoint, is used by over 78% of the Fortune 500. Other ECM platforms like Documentum are popular as well. By integrating secure file sharing with ECM systems, IT organizations can bring ECM content and ECM security policies to the workforce.

- ☐ **VPN-less secure access to ECM files**
  Users should be able to access files stores in ECM systems, such as Microsoft SharePoint, securely and directly through mobile devices, without requiring a VPN connection.

- ☐ **Maintain ECM as system of record**
  If ECM administrators want to maintain an ECM platform as the system of record, ECM administrators should be able to ensure that files are saved only to the ECM platform, not to other file shares.

- ☐ **External sharing of ECM files**
  Users should be able to share ECM files with authorized external users.

Integration with Cloud Storage Systems, such as Dropbox and Google Drive

Cloud storage systems such as Box, Dropbox, Google Drive, and Microsoft OneDrive are popular

with end users for storing and sharing documents. However, when used without IT authorization and supervision, they pose a significant risk for organizations. By deploying an IT approved solution that provides secure monitored access to these systems, organizations can achieve peace of mind while delivering end user productivity.

- [ ] **Secure access to cloud storage files**
  The solution should enable users to securely access files stores in cloud storage systems in real-time, while also enabling IT to disable network access to these systems.

- [ ] **Auditing and logging of cloud storage access**
  All content accessed and shared via the cloud system should be logged and monitored.

- [ ] **DLP and AV integration**
  IT should be able to add an additional layer of security upon cloud content access by integrating with the solution's DLP and AV capabilities.

Integration with Enterprise Infrastructure

Secure solutions should integrate with important IT services, such as user directory services, single sign-on services, and Data Loss Prevention (DLP) systems in order to streamline operations and reduce operational overhead.

- [ ] **Integration with LDAP and Active Directory (AD)**
  The solution should integrate with industry-standard directory services, such as LDAP and Active Directory. Organizations should not have to maintain a separate directory system just for secure file sharing if there are other standard directories services in place.

- [ ] **Integration with Single Sign-On (SSO) services**
  The solution should integrate with industry standard single sign-on services, such as services based on SAML, Kerberos, and LDAP. Organizations that have deployed single sign-on services should not have to maintain a separate sign-on service for file sharing.

- [ ] **Integration with DLP systems**
  The solution should integrate with industry-standard DLP services, so that file sharing adheres to an organization's existing DLP policies.

- [ ] **Integration with Mobile Device Management (MDM) systems**
  With an MDM solution in place, there is an added layer of device protection. The solution should integrate with popular MDM systems to simplify the provisioning, management, and securing of mobile devices accessing an organization's files.

- [ ] **Plugins**
  To simplify access to secure file sharing and discourage users from seeking unmanaged and unmonitored channels for distributing files, the solution should offer plug-ins for popular communication applications, including Microsoft Outlook and Microsoft SharePoint.

About Accellion

Accellion, Inc. enables enterprise organizations to collaborate on content with external partners securely via private cloud. Enterprises can leave existing content where it lives today, and extend it outside the firewall without having to migrate content or disrupt their business workflows. Accellion's solutions are used by more than 15 million users and 2,500 of the world's leading corporations and government agencies including Procter & Gamble; KPMG; Kaiser Permanente; Latham & Watkins; National Park Service; Pacific Life Insurance; Cargill; and the National Institute for Standards and Technology (NIST). For more information please visit www.accellion.com or call (650) 249-9544.

Follow Accellion's Blog, Twitter, Facebook and LinkedIn.

Email: info@accellion.com
1804 Embarcadero Road | Palo Alto, CA 94303 USA | (650) 249-9544 | www.accellion.com