Accellion

The Risky Business of Online Collaboration

Six Principles for Securing Sensitive Enterprise Content

To succeed in today's hyper-connected world, businesses, governments and NGOs must enable easy online collaboration across the extended enterprise. Employees, suppliers, partners, investors, customers, doctors, patients, constituents and other stakeholders expect smooth online workflows enabled by simple, easy sharing of digital content—even when that information is highly confidential.

- Hospitals must provide lab results to doctors and patients directly over the Web
- Financial institutions must offer investors digital account statements and contracts
- Law Firms must share case information with outside counsel and clients
- Insurance companies must provide claim details to agents and policy holders
- Government agencies and contractors expect to share RFPs, contracts, and plans by email
- Global manufacturers share product designs and proprietary IP across international borders

Alongside these new requirements of transparency and immediacy are heightened concerns of privacy and security. The conflicting demands to both provide and protect this shared, sensitive information has led to a surge in government regulations, such as HIPAA, FISMA, 23 NYCRR 500, PCI and GDPR. While competitive organizations must provide easy online access to account statements, contracts, policies, health records, product designs and the like, they must also secure this highly sensitive data against unauthorized use and theft.

The Goal of This eBook

CISOs must enable secure online collaboration that balances the protection of sensitive content with the overwhelming need to share it, easing access while preventing breaches, ensuring privacy alongside transparency, and adhering to complex regulations without getting in the way of efficient communication. Each trade-off entails risks. This eBook explores these trade-offs and offers six guiding principles for creating a secure content sharing channel that enables work across the extended enterprise and protects your most sensitive digital assets.

PRINCIPLE #1:

Visibility

Begin with The End in Mind

What if you could see every exchange of sensitive content between your organization and your customers, your vendors, your partners, your attorneys, your investors, and all other external parties? Where is it going to? Where is it coming from? Who is sending it? Who is receiving it? How sensitive is it? Is it infected? What if you had a dashboard that could analyze those communications along relevant dimensions, such as content sensitivity, origin and destination, time of day, and file type. What if you could implement dynamic security and governance policies based on that information, such as blocking a transfer of unusually sensitive information to a specific country by a specific user at a specific time of day? Security, privacy, transparency, governance and compliance all rely on visibility. If you don't measure it, then you can't manage it. Therefore, you should begin with the end in mind: total visibility to all activity across your secure content sharing channel, including a complete, real-time audit trail of all shared content that can be recorded, aggregated, sliced, diced and archived.

The simplest way to accomplish total visibility would be to force all sensitive content communications through a single user application attached to a single content repository, e.g., a consolidated private cloud storage and file sharing service. Then, you'd have a single point of data collection. Unfortunately, people don't work this way. They use email, web browsers, mobile apps and even SFTP clients to exchange sensitive content. And, that content gets stored all over the place in local drives, network file servers, enterprise applications, ECM systems and cloud storage services. Moreover, the most sensitive content will likely be segregated and maintained on premise. While some consolidation of user sharing applications and enterprise storage locations is certainly beneficial, it will always be limited in any reasonably large, complex organization.

Security, privacy, transparency, governance and compliance all rely on visibility. If you don't measure it, then you can't manage it.

Total visibility to all shared sensitive content is clearly much easier said than done. However, it is not simply an aspiration. With rigorous data privacy laws like HIPAA and GDPR, it's a requirement. In the real world, total visibility entails tapping into all the endpoints where users share content, as well as all the locations where content is stored. Whatever the final system architecture, an essential requirement of your secure content sharing channel will be a connection to every content repository and sharing application that monitors and governs each request to save, retrieve, send or receive a file. Every missing connection will be a blind spot that enables a potential breach.

PRINCIPLE #2:

Security

Prevent Breaches While Enabling Workflows

User apps, such as email and file sharing, define an external perimeter where content enters and exits your organization. Enterprise apps and storage repositories define an internal perimeter around your most sensitive and valuable content. Access through these perimeters should be both simple and secure to ensure seamless workflows across your extended enterprise. Given the variety of applications and user workflows, however, providing simple access is actually a very complex challenge. Users can range from internal senior executives to trusted suppliers to external consumers and workflows can range from distributing a board of directors' presentation to signing customer contracts. Preventing breaches while enabling workflows requires the implementation of very complex access rights and privileges across many user roles. Therefore, consolidating access management through single sign-on and a directory service should be high on the list of requirements for building out a secure content sharing channel.

Securing authorized access, however, is just the first step. Just as much attention must be given to preventing unauthorized access, especially to your most sensitive content. All content sharing should be encrypted from origin to destination. Sensitive enterprise content should also be encrypted in storage and access should be further restricted with multi-factor authentication. Your most sensitive content, such as legal documents, health records and proprietary IP should only be stored on premise. Public cloud storage not only exposes data to unauthorized access by unknown third parties, but the consolidation of data creates a honey pot for attackers and increases the risk of a large-scale breach. In addition, the US Federal Cloud Act of 2018 allows US law enforcement to compel technology companies via subpoena to provide data stored on their servers, regardless of whether the data is stored in the U.S. or on foreign soil. In plain English, your sensitive data can be collected in bulk without your knowledge or approval. On-premise or private cloud repositories should be the standard for truly sensitive information and IP. If on-premise storage is not possible and cloud storage must be used, then encryption keys should be unique to your organization and stored in a separate, secure location.

Public cloud storage not only exposes data to unauthorized access by unknown third parties, but the consolidation of data creates a honey pot for attackers and increases the risk of a large-scale breach.

Access controls can lock out unauthorized users, but they can't protect you against unauthorized content, such as incoming malicious email attachments or outgoing leaks of proprietary IP. Therefore, your security architecture must extend beyond securing users to securing content. At a minimum, every inbound file should be cleared by anti-virus software prior to storage in an enterprise content repository. Outbound files should be scanned using data loss prevention (DLP) software to block leaks of sensitive content. Both inbound and outbound content scans can be accelerated to ease access by taking a stratified approach. More suspicious files can be queued for advanced threat protection (ATP) processing to isolate and execute them in a secure environment. By implementing a data classification standard, DLP scans can be performed offline while sharing requests can be processed in real-time.

PRINCIPLE #3:

Confidentiality

Balance Privacy with Transparency

Every CISO knows that you can't have privacy without security, however, you can have security without privacy. Multi-factor authentication, encryption, and threat protection defend against external threats, but they do nothing to ensure sensitive content is handled correctly by authorized users. While users across your extended enterprise expect easy access to their sensitive content, they also expect complete confidentiality: transparent collaboration comprised of private communications.

To govern data in motion as it enters and leaves your organization, policy controls need to incorporate sharing metadata, such as sender, receiver, origin, destination, time of transfer, and window of availability.

Confidentiality means ensuring only authorized users can access, modify and share specific content in specific ways. It cannot be enforced at the network level—where most security controls are implemented, because it requires information like who, what, where, when, and how. It must be enforced at the user-application-content level, because that is where this information resides. For example, preventing a finance manager from sharing audited statements publicly prior to an earnings announcement requires an understanding of user roles, content type and timing of the request. These requirements echo our previously stated requirements for total visibility: connection to every user sharing endpoint and every content repository. Only now we need more than just a connection—confidentiality requires control.

Your secure content sharing channel must have very granular policy controls based on a wide array of inputs, including user roles and privileges, as well as content metadata, such as file size, type, location, read and write permissions, and content sensitivity. Consider file access at a hospital. Should a podiatrist have access to an obstetrics patient's records? Should an admitting clerk be able to edit a patient's prescription dosage? Not unless the hospital wants to draw a HIPAA violation. This is the baseline to govern data at rest. To govern data in motion as it enters and leaves your organization, policy controls need to incorporate sharing metadata, such as sender, receiver, origin, destination, time of transfer, and window of availability. The more granular the governance, the greater your ability to enforce confidentiality and strike the right balance between privacy and transparency.

PRINCIPLE #4:

Simplicity

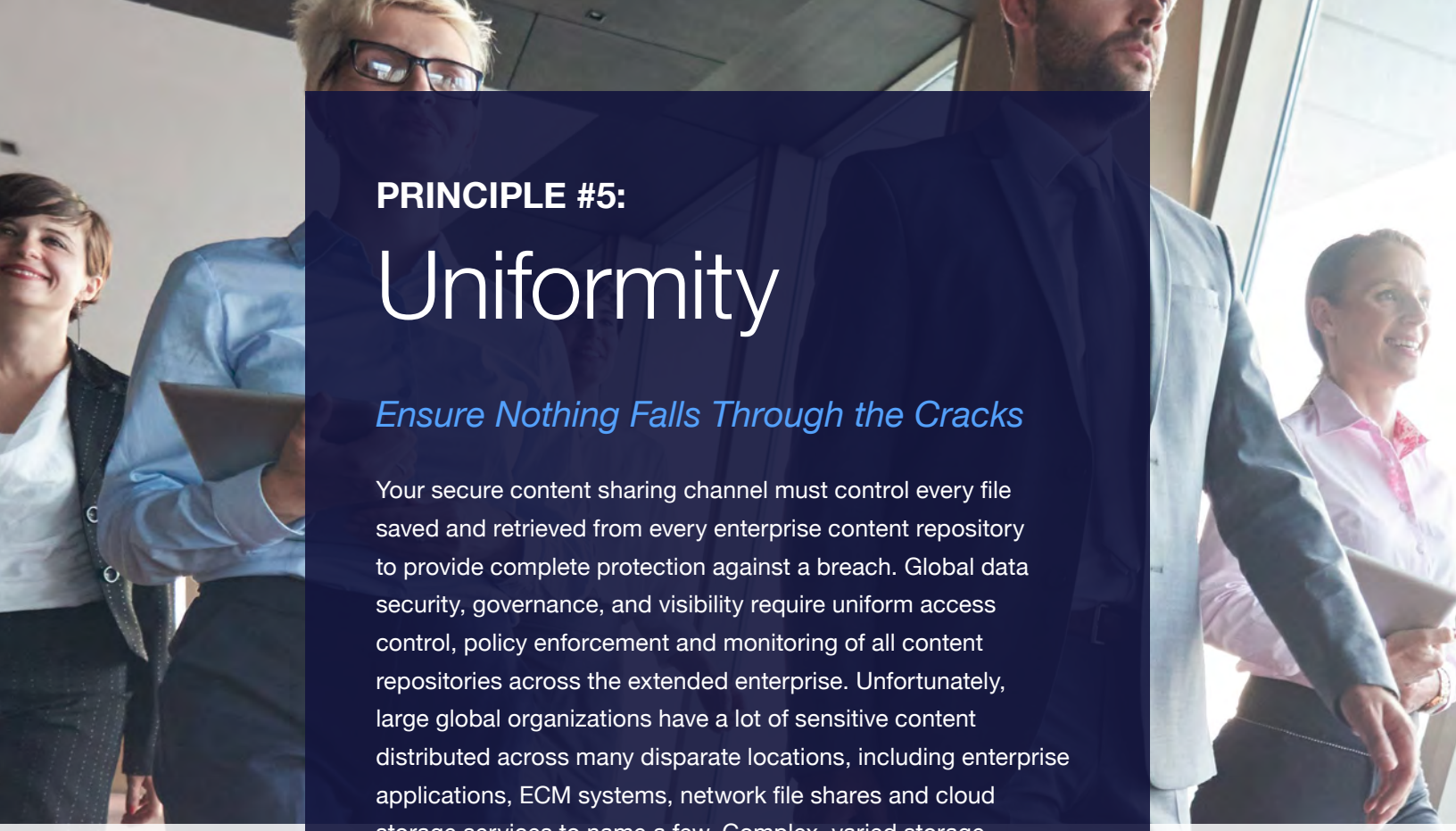
Eliminate Shadow IT

Securing sensitive data cannot sacrifice the simplicity of sharing it, otherwise users will circumvent the security. Users expect easy online access to the sensitive information they need to get work done. For them, the cloud is a panacea and a privilege. For CISOs, the cloud is a double-edged sword. Every minute and penny saved on the cloud comes at the price of increased risk. However, if you make the mistake of providing a complex channel for sharing information securely, users will seek out simple, insecure alternatives to accomplish their goals—building their own shadow IT out of easily accessible, consumer cloud applications.

Every frustrated employee who takes IT into his or her own hands to get work done increases the risk of a breach, leaving the CISO responsible. Alternatively, blocking common consumer cloud services runs the risk of alienating everyone with complex communication processes. You must provide a secure communication channel for sharing sensitive content that is also incredibly simple and easy to use. Simplicity is just as important as security.

Users share content from a wide array of applications: email, Web browsers, office apps, mobile apps, and enterprise apps. Your secure content sharing channel must extend to every one of these endpoints. This can be achieved with plugins for each application that route content sharing through your secure channel. Plugins should make sending, receiving, saving and retrieving sensitive content as easy as clicking a button inside each target application. Once you have made it simple to share sensitive content securely, then you can shut down the alternatives with confidence. Restrict sharing to authorized applications by controlling software installation and deploy a cloud access security broker (CASB) to block unauthorized cloud services.

Every frustrated employee who takes IT into his own hands to get work done increases the risk of a breach, leaving the CISO responsible.



PRINCIPLE #5:

Uniformity

Ensure Nothing Falls Through the Cracks

Your secure content sharing channel must control every file saved and retrieved from every enterprise content repository to provide complete protection against a breach. Global data security, governance, and visibility require uniform access control, policy enforcement and monitoring of all content repositories across the extended enterprise. Unfortunately, large global organizations have a lot of sensitive content distributed across many disparate locations, including enterprise applications, ECM systems, network file shares and cloud storage services to name a few. Complex, varied storage locations increase the risk that sensitive information will leak undetected.

The bad news is that the simplest solution to this problem—consolidating all enterprise content into a single repository—is not feasible for most organizations. Existing, distributed content stores are often too integrated into existing workflows and too expensive to migrate. Enterprise applications often require content in specific data formats. Regulatory requirements, such as national or regional data sovereignty rules, may prohibit the consolidation of content across international boundaries. And, highly sensitive content should be segregated to implement tighter security, such as multi-factor authentication. The good news is that you don't need to consolidate content physically. You just need to consolidate it virtually through metadata and controls to unify content access, security, governance, and visibility.

By deploying connectors to content repositories that intercept, monitor, and manage storage and retrieval requests, you can create a secure inner perimeter around your most valuable digital assets that complements the secure external perimeter created by plugins to end user sharing applications. As files pass through this perimeter, granular permissions and detailed content scans can ensure that only authorized files are retrieved and sent externally, and only safe files are received and stored internally. Nothing falls through the cracks.

Complex, varied storage locations increase the risk that sensitive information will leak undetected.

PRINCIPLE #6:

Auditability

Prevent Compliance Failures

The main goal of your secure content sharing channel is to protect your IP, PII, PHI, and other sensitive information. It is critical that you have complete confidence in this outcome. Moreover, the modern CISO must provide proof of protection to internal auditors, to government regulators, and in many cases to external parties, such as consumers, investors, attorneys, and so forth. To prevent compliance failures, you must have complete auditability of all content, all content sharing, and all content-related systems, policies and procedures.

Since we began with the end in mind, our first principle gives us total visibility. We already know who shared what with whom, when, where, and how. We also know what content passed or failed AV, DLP and ATP scans. Auditability requires keeping a historical record of everyday visibility. Audits can be very cumbersome and time-consuming, so audibility also entails supporting compliance processes with accurate, timely reporting. Specific requirements will vary by sector, such as healthcare, financial services, government, and consumer, but the end goal is the same: prove that sensitive information is handled in compliance with IT policy and the law.

About Accellion

The Accellion platform enables organizations to securely share sensitive information beyond enterprise borders while maintaining the controls and visibility needed to demonstrate compliance. Accellion's solutions have been used by more than 25 million end users and have been installed at more than 3,000 of the world's leading corporations and government agencies including NYC Health + Hospitals; KPMG; Kaiser Permanente; Latham & Watkins; National Park Service; Umpqua Bank; 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 on LinkedIn, Twitter, and Accellion's Blog.