



Buyer's Guide to Enterprise Collaboration

With a robust enterprise collaboration solution, getting work done efficiently and securely has become easier, despite continuously evolving regulation regarding data privacy and the management of sensitive content.

intralinks.com



Buyer's Guide to Enterprise Collaboration Solutions	2
How to Use This Guide	3
What to Look for in an Enterprise Collaboration Solution Provider	4
Risk Perspective of Enterprise Collaboration Solutions	5
Enterprise Collaboration Solutions Basics	6
Evaluating Enterprise Collaboration Solutions: Underlying Platform	7
Application Security	7
Infrastructure Security	8
Process Security	9
Integration	10
Mobile Devices	11
Access, Authentication and Authorization	12
Digital Rights Management	13
Compliance Reporting	14
Support Requirements	15
Conclusion	16
Sources	16



Buyer's Guide to Enterprise Collaboration

With a robust enterprise collaboration solution, getting work done efficiently and securely has become easier, despite continuously evolving regulation regarding data privacy and the management of sensitive content. It is also now possible to extend collaboration beyond the firewall and to mobile devices without compromising security or usability.

The consumerization of Information Technology (IT) continues to change the way we work and share information. Gartner predicted that by 2017 the Chief Marketing Officer (CMO) would spend more on IT than the Chief Information Officer (CIO). In fact, many technology-buying decisions do not involve IT. Some business teams avoid IT because of lengthy deployments or restrictions on the use of various file-sharing applications altogether.

Despite the infiltration of consumer devices and applications into the enterprise, IT must continue to secure confidential information and prevent data leakage while enabling employees to work. The challenge is doing so without excessive constraints on the necessary exchange of sensitive information that allows employees and their external business partners to conduct business effectively. Even in heavily regulated industries such as life sciences, legal and finance, collaborating on highly sensitive information is possible. The key is selecting a vendor with experience operating in regulated industries that can also address the three drivers of enterprise file sharing:

1. **Risk management strategy** – deep knowledge of regulation and certifications; proven expertise and experience in managing risk and ensuring compliance. If you were audited today, would you be prepared? Would your vendor be prepared?
2. **Accelerating business productivity** – an enterprise collaboration solution must not limit productivity or be excessively restrictive; it must be an enabler of secure collaboration through effective controls.
3. **Improving IT efficiency** – an enterprise collaboration solution must efficiently leverage existing IT resources and support integration with existing applications and protocols.

This buyer's guide examines the granular file sharing aspect of enterprise collaboration solutions, as well as infrastructure and extended collaboration, including Digital Rights Management (DRM). You'll gain insight into the factors to consider when evaluating enterprise collaboration solutions, while keeping in mind evolving regulatory and business environments.



How to Use This Guide

While the guide addresses the requirements of IT relative to data control and protection, it also addresses the concerns of business users relative to data usability, visibility, auditability and compliance. The information is organized into the following sections:

- Underlying platform (infrastructure and security)
- Integration
- Mobile Devices
- Access, authentication and authorization
- Extended collaboration and file handling beyond the firewall
- Digital Rights Management
- Audit and compliance reporting
- Support requirements

As your requirements may vary, use this information to guide your RFP planning.

What to Look for in an Enterprise Collaboration Solution Provider

First and foremost, look for a provider with experience in managing secure file sharing in heavily regulated and highly secure industries such as life sciences, finance and legal. Ask your provider for a list of clients with whom they've worked and look for similarities between your industry and the needs of their existing clients.

Specifically, does the prospective file-sharing provider have a long history of working with enterprise clients in regulated industries? If so, they're likely to have been audited and/or penetration tested by some of their clients as well as by third party auditing and testing firms.

Know what certifications they've received, the volume and types of audits they've supported and how they've supported clients in your regulated environment. Also, make sure you understand their security processes such as frequency of penetration testing and file encryption.

Secondly, your provider should complement and support your IT team. Look for a vendor that not only supports the end-users within your organization, but also the end users/business partners external to your organization with whom you share information. Will your provider provision, de-provision and support all end-users regardless of time, location or language? If not, can your IT team scale quickly and cost-effectively enough to do so? Is your IT team willing to provide support to your business' external business partners? Is it in their charter?

Make your business case by selecting a provider that can leverage your existing enterprise IT investments, such as Microsoft SharePoint® and Outlook®, and reduce licensing, infrastructure and support costs associated with secure file sharing. Remember, security and ease of use are not mutually exclusive. Consider your provider's ability to enable users to work within familiar technology environments such as Microsoft SharePoint and support a variety of workflows—simple, complex, ad hoc, structured, public or confidential—yet maintain a transparent and compliant information flow.

Finally, an enterprise collaboration solution vendor should provide centralized visibility and compliance monitoring capability over the lifetime of a document. Understand what reporting capabilities are available, particularly those that show audit trails and demonstrate compliance or identify gaps before a breach occurs.



Risk Perspective of Enterprise Collaboration Solutions

Sixty four percent of data breaches were the result of human error or system glitches, according to the Ponemon Institute's "2013 Cost of Data Breach Study: Global Analysis," sponsored by Symantec. The study was based on interviews of more than 1,400 people representing 277 organizations in nine countries. What does your enterprise collaboration solution vendor do to reduce these risks?

Consider the inherent risk of sharing information across today's increasingly complex IT infrastructures — on premise, off premise, virtual and cloud — and the costs associated with maintaining data security despite shrinking IT budgets. Add to that the costs of complying with the increasingly complex regulatory landscape, and the security and compliance risks of file sharing grow exponentially.

An effective enterprise collaboration solution provider should significantly reduce these risks while enabling IT to better control and predict their costs. Starting with your existing governance framework, determine how well your provider's solution is able to meet your stringent security standards without compromising usability. Make sure to understand the deployment options your vendor provides and compare these to the ones you need in order to meet your specific industry and country regulations.

An effective enterprise collaboration solution must consider people, processes and technologies. Given the evolving regulatory environment, ongoing training and support are a must. Processes and technologies that incorporate the latest security, risk management and compliance policies can substantially reduce the human error element of data security and support your due diligence.

Keeping these considerations in mind will help you choose the most effective and compliant solution for your organization.



Enterprise Collaboration Solutions Basics

Before delving into the details of enterprise collaboration solutions, keep in mind a few basic questions that are important to ensure the security of your data and the productivity of your administrators and end users.

- **Admin Access:** Can administrators set policies that restrict access to specific files even though a user may require access to other files within the same folder?
- **File, Sync and Share:** Is file sync and share conducted in real time and can your administrators set permissions to selectively sync certain files?
- **Storage:** What is the maximum storage capacity?
- **Users:** Are there limitations on the number of users?
- **Uploading:** Are there limitations on the number of files uploaded?
- **File History:** Can you go back to previous versions even after subsequent versions have been created?
- **Audit Ready:** Is an audit trail of document and version access available?
- **Deployment:** How is the solution deployed – public, private or hybrid?
- **Cost:** What is the cost?

These basics give you a good starting point for evaluating enterprise collaboration solution providers and allow you to gain a broad understanding of their solution framework. Then, consider the following details based on your specific use cases to effectively evaluate the best solution.

Evaluating Enterprise Collaboration Solutions: Underlying Platform (Infrastructure and Security)

The platform on which an enterprise collaboration solution is built is the foundation of secure content sharing. Your provider's response to the following questions should elicit a sense of trust and confidence in the stability of their infrastructure and architecture as well as in their expertise in regulatory compliance. Look for a provider with extensive experience in operating in regulated global industries and validate that by the makeup and number of their clients.

Application Security

Desired Capability	Description	Questions to ask your vendor
Strict ID and password protocol	Prevents users from password sharing	Does your system detect and prevent a single-user ID from logging in from multiple locations at the same time?
Secure data transmission and storage	Protects data in transit and at rest, while ensuring compliance with local data regulations	- Does your data encryption support the strong commercially available ciphers, e.g., 256 bit keys and standard algorithms? - Is data encrypted by default in transit and at rest in storage? - Does your encryption scheme use algorithms designated by the NSA as standard?
Permissioning and visibility	Supports existing business governance processes and workflows giving users access and/or control only on a need-to-know basis (e.g., one person may have control in one business process, but read-only access in another).	- Does your system provide near real-time reporting of who's looking at what content and when? - Do you allow for role-based permissioning based on business processes? - Can any of these employees undo the revocation?
Document locking & protection; dynamic watermarking	Prevents saving and forwarding files in the open (unencrypted) to reduce access and the risk of accidental disclosure to unauthorized individuals	- How do I maintain control once you disclose the document to external partners? - Do you offer watermarking? - Can you digitally shred the document after the end user has downloaded it?
Strong authentication	Provides a higher level of security in order to exchange critical information	- Does your solution meet government and financial industry two-factor authentication requirements? - Does your solution allow security options for grouping information by sensitivity with appropriate protections? - Does the user authentication strength scale up and down to allow application of multi-factor challenges based on data sensitivity and user's assessed risks (e.g., end device parameters, geo-location, IP address, time of access, etc.)?
Private SaaS hosting	Ensures that you know where your data is at rest; especially significant for countries where legislation protects personal data residing within its borders, such as the UK	- Is the data housed on a public cloud such as Amazon Web Services or a private cloud? - Is the data limited to specific servers? - If public, how are multi-tenant environments secured? - Who controls the cloud stack; your file sharing provider or the host? - Do you perform onsite assessments of your key vendors? - Have your clients audited your operational controls, procedures and technology for fitness within their security standards? - Have you done vendor viability assessments of your key vendors? - If you go out of business, what happens to my data?

Infrastructure Security

Desired Capability	Description	Questions to ask your vendor
256-bit AES (Rijndael algorithm) encryption and robust encryption process	Provides the most secure commercially available encryption and is robust enough to shield against brute force attacks by high capability adversaries, such as state security agencies	• Do you offer encryption at the file level? • Is there only a single encryption key or is there a unique key for each file? • Is a multi-layer key management system in place? • Who has access to the encryption key(s)? • How robust is the encryption algorithm? • Is the encryption key randomly generated for each file or is the key generated using a template that includes known information such as the user's email address?
Geographically separated data centers	Ensures additional protection of critical data under all disaster scenarios	• Are the servers which house client data located in geographically separated data centers? • Is a failover mechanism between the sites in place? Is it tested at least annually? • Do the servers use real-time replication? • Are the servers continuously monitored with controls such as virus scanning and intrusion detection?
Certifications	Ensures that the processes in place to govern the creation and management of an online information exchange are of the highest standards relative to the industry	• Which party validations, certifications and audits do you possess? • Do you perform annual SOC 2 Type 2 audits? • Do you comply with FDA 21 CFR Part 11 (electronic records and electronic signatures used in FDA regulated environments)? • Do you undergo regular, independent 3rd party penetration tests and application vulnerability assessments? • Can you share your recent audit and penetration test reports? • Can you share your historical audit and penetration test reports going back up to ten years?
Business continuity / disaster recovery	Ensures reliability and uptime	• Do you have redundant data centers in geographically separate locations? • Do you produce daily backups? Are they stored offsite? Are they stored in a geographically separate location? • Do you test your failover capability? If so, how often? • Do you test the data centers' disaster recovery plans, and, if so, how often?
Personnel security	Provides assurance of the integrity of the people supporting your information exchange	• Do support personnel undergo background checks and are they bound by confidentiality agreements? • What training, examinations and certifications are support personnel required to undergo? Are they required to go through a recertification process?



Process Security

Desired Capability	Description	Questions to ask your vendor
Change control	Prevents the introduction of new vulnerabilities during a product release and increases infrastructure stability	• Does your organization follow strict change management processes such as ITIL or similar IT best practices? • How are product releases obtained by or distributed to end users? • Are product releases backward compatible? If so, to what extent? (i.e., will the release of new functionality require every user to update?)
Enterprise scale implementation and operational processes	Ensures system stability, availability, reliability and integrity. Reduces the risks of business disruption	• How do you ensure that vendors comply with your quality management practices? • How do you assess your vendors' processes? • Do you monitor your vendors' SLAs? • How closely do your software vendors align their product changes — functional and release timing — to your business?
Restricted access to vendor personnel	Ensures additional security by preventing the vendor's personnel from accessing your sensitive data	• Who within your organization has access to my data? • Is an audit log of such access maintained? Is it available for review (either self service or on demand)?

Evaluating Solutions: Integration

The need to quickly and easily share content makes the adoption of consumer grade file-sharing applications very appealing to end-users. However, consumer-grade solutions should not compromise the security of company sensitive information. Look for a solution that delivers ease-of-use while integrating complex workflows with existing applications.

Your vendor's solution should provide an easy, approachable and intuitive interface for end users that can also be easily deployed in your current environment. For example, your IT team should be able to use its existing identity and access management system and end-users should be able to use existing tools and workflows.

If users are accustomed to working with Microsoft SharePoint, Salesforce.com® or other enterprise collaboration and content management tools, understand how your provider can allow secure file sharing and document control in conjunction with these applications and beyond your firewall.

Desired Capability	Description	Questions to ask your vendor
Web-services ready API	Provides developers with a broad set of functionality and an API that manages and controls content, users, sessions and system administration that can be used with your own custom applications	On what architecture are your provider's APIs built?
Connector	Integrates with the APIs of other enterprise software systems to extend access beyond the enterprise firewall to external customers and business partners	- Do you offer XML-based communications between your service and external systems? - Does your solution enable data integration without hand coding? Does it shield developers from underlying complexities? - Do you integrate with popular enterprise services including, Microsoft SharePoint, EMC Documentum®, etc.? - Does your solution extend access beyond the enterprise firewall? - Does your solution include integration with file transfer, permissioning, reporting and workflow for existing enterprise software systems?
Ease of adoption	Speeds onboarding and allows associates to work from anywhere and on any device with the same inside-the-firewall security	- What is your onboarding process for both internal and external users? - Do you support collaboration tools for internal and external users and if so, how?
Single point of control	Ensures visibility and control across the platform for all sharing use cases: simple to complex, ad hoc to structured, and public to confidential	- How will your solution provide reporting in the event of an audit? - How can we know what information has been shared? - Do you provide self-service access reports? - Do you provide training?
Plug-in	Streamlines integration and workflow with familiar user-level tools including Microsoft Outlook and Internet Explorer®	Have they been tested across different Windows® operating systems and MS-Office® releases?
Content	Limits file sharing, approval and audit trails to the context of a project and collaboration group. Enables file assignment and tracking	- Can you assign people and tasks to document approvals within your file sharing application? - Does your solution allow users to set up a project and monitor content within that project? - Does your solution have the capability of creating workflows for document approval and are those workflows auditable?

Evaluating Solutions: Mobile Devices

Whether you provide corporate-issued devices (including laptops) or endorse the Bring Your Own Device (BYOD) policy, security should be as robust on the mobile devices as it is behind the firewall without sacrificing the on-the-go support that mobile users expect. You should consider an enterprise collaboration solution vendor with experience in provisioning and de-provisioning internal and external mobile users, as well as in handling sensitive data that may be accessed by mobile devices.

Desired Capability	Description	Questions to ask your vendor
Mobile device support	Enables the mobile workforce to collaborate easily and securely	• Can I prevent mobile access to some data by default, and ease restrictions based on content type? • Which devices are supported? • Are devices supported in their native applications or through browser-based access? • How do you prevent users from saving sensitive data locally onto their devices? • How do you prevent users from saving and/or copying sensitive information on their devices?
Remote data wipe capability	Wipes shared content from lost, stolen or de-provisioned mobile device	• Can you allow administrators to prevent access to the shared content? Can the shared content be wiped even when the device is not online? • In a wipe, is the file destroyed or is its access de-permissioned? • Does your solution encrypt content in transit and at rest on mobile devices? • How do you handle a compromised device?
File synchronization	Allows for policy-based synchronization to prevent compliance issues from the propagation of data on multiple devices	• Are files synced in real time? • Can files be configured to sync at intervals determined by my administrators? • Does the data sync across end point devices? • Does your solution allow administrators to set policies for file synchronization? • Can data be synced selectively? • Can your solution set who can and cannot synchronize?

Evaluating Solutions: Access, Authentication and Authorization

Any extended enterprise collaboration solution should include security measures that guard against unauthorized access. The most efficient means of ensuring appropriate access is through the use of your existing Identity and Access Management (IAM) procedures. As an added precaution, administrators should have the flexibility to invoke added security measures such as multi-factor authentication.

Desired Capability	Description	Questions to ask your vendor
Single Sign-On (SSO)	Integrates with your existing corporate identity provider, such as Active Directory®, and enables users to sign in using existing corporate credentials instead of a separate login	• Do you offer SSO without modification to the SaaS application or integration with SAML / OAUTH? • Can your system easily de-provision users by updating their corporate identity provider (e.g., Active Directory)?
Multi-factor authentication	Enables administrators to define a set of rules and user challenges to verify identity prior to accessing the shared content	• Do you offer multi-factor authentication? • What happens when the user login authentication fails on multiple back-to-back attempts? • Does it affect all users at login? • Can it be applied depending on content that the user is trying to access? • Are custom-tailored policies available, such as challenging users if their source IP address is not in the white list? • Can the challenge scale up if the user cannot pass the previous challenge (e.g., multiple failed attempts with the security question automatically switch the challenge to a one-time password)



Evaluating Solutions: Digital Rights Management

Digital Rights Management (DRM) provides lifetime access control over the content's viewing, copying, printing and alteration. Every action must be pre-configured and an audit trail may be available. DRM should be fully integrated with native file protection to control information even after it has been shared and downloaded.

DRM is an integral part of an enterprise collaboration system. Your solution should provide encryption at the document level so that content owners have granular access to documents.

Not all users require the same level of access and control for every document on every project. Your solution should be flexible. Look for lifetime control that is based on configurable policies that take into account the user's role within the context of a specific project.

Desired Capability	Description	Questions to ask your vendor
Role-based permissioning in a given context	Enables administrators to better control read, print, change and copy capabilities based on the role they assign to users	• Can users have different roles depending on the context of the project?
Document-level DRM	Enables granular control of documents within and beyond the firewall	• Can access to a mistakenly shared document be revoked and the document rendered inaccessible even when it is outside the firewall? • Can a shared document's access have a set expiration date? • Does your solution provide lifetime control at the document level? • Does the rights management policy stay with the document if the document leaves the application? • What file formats are supported? • What happens if a document saved on a PC is de-permissioned? • Can administrators apply rights management to specific content in a given folder without affecting all the content in the folder? • How do you enable projects or processes where files require differing security policies?
Version Control	Ensures the latest version is in use and retains a trail of document versions	• Are file versions maintained? • Are file versions easily accessible by users and administrators?
Lifetime control of content	Enables control of information even after it has been shared and downloaded on any computer or device	• What happens to content after it has been emailed or shared outside of the solution? • Can you determine if emailed content has been viewed? • Can you destroy emailed content or prevent it from being viewed? • How do you demonstrate when sensitive information was shared or viewed? • What is your recommended solution when information is accidentally shared? • How do you secure content that employees have access to across multiple devices?

Evaluating Solutions: Compliance Reporting

Whether your organization manages compliance in a decentralized manner or has a centralized compliance group, IT frequently provides the necessary reporting to assess risks and verify compliance against company policies. IT teams must be prepared to support the compliance teams with policies and reports that address the growing regulatory requirements. How will IT teams ensure that a proposed solution supports their company's compliance requirements? How will users know if they comply?

The most effective way to navigate through compliance issues is to build into the proposed solution the policies, regulatory standards and workflows that ensure compliance across all information-sharing activities and that such activities are tracked for each user. An enterprise collaboration solution should include readily available, self-service reports that provide a macro view of sharing activity with the capability to drill down to the file level — a typical regulatory requirement. You must know, at any given time, who is accessing what information, how many times and what they have done with it (e.g., viewed, printed, downloaded).

Desired Capability	Description	Questions to ask your vendor
Access, retention and destruction management	Ensures appropriate access and that all records are securely retained in the event of an audit or legal review, and securely destroyed in accordance with company policy	- What data and events are recorded? - What reports are available? - Can I limit exposure of potentially sensitive/confidential information to a specific user (i.e. my Compliance Officer) who has been given explicit approval to access this data? - Are the reports available in a self-service manner? Can they be exported to Microsoft Excel? - How do you configure retention and destruction policies to meet my requirements?
Future-proofing	Ensures the solution remains current with the complex and dynamic regulatory environment	- How do you remain current with my industry's regulations? - Which regulatory bodies do you actively monitor? - Which regulatory body is the most challenging for you?
Granular and comprehensive audit & compliance	Ensures compliance visibility across all sharing activity	- How do you know who is authorizing and giving access to my data? How is this tracked? - What is your process for recording and reporting on content moving within and beyond my organization? - How do I retrieve the required granular document and user-level records in the event of an audit? - How do I ensure that access is revoked when an internal or external participant leaves or changes departments?
Highly-regulated industries	Ensures vendor has a solid history and understanding of strictly-regulated industries	- How long have you served regulated industries? - Who are your clients in these regulated industries? What types of content are they sharing? - Has your solution been validated by your regulated users for 21 CFR Part 11 (Electronic Records and Electronic Signatures) compliance? - Will you support an onsite 21 CFR Part 11 based validation assessment? - If I get audited by the FDA or MHRA, will you provide supporting evidence while the audit is underway?

Evaluating Solutions: Support Requirements

Support is an essential key to increased adoption rates among users. However, many IT support operations are already at capacity, have been outsourced, or are chartered to only support internal users. You should consider a provider that can alleviate IT's support burden of onboarding your users, business partners and stakeholders to yet another product. Look for a solution that can be quickly deployed to users within and beyond the firewall. Local language support is also an effective way to speed the onboarding process and increase adoption rates globally.

Review the ability of your IT resources and help desk system to support new users beyond your firewall. Will your enterprise collaboration solution provider fill the gaps necessary to ensure a smooth onboarding and ongoing support? You should confirm that your provider offers 24-hour per day live service and support for users in multiple time zones and with different language needs.

Desired Capability	Description	Questions to ask your vendor
24/7/365 multi-lingual support	Ensures that the organization's IT department does not need to provide global, multi-lingual end-user support for the solution	- Do you offer global around-the-clock support personnel? - How many languages do you support? - Do you offer phone, email and chat support options? - What is your average time to answer the phone? - What is your average time to resolve an issue and is there an escalation process in place?
Support all users including business partners	Ensures that all users within and external to the organization collaborate efficiently and securely when and where needed	Do you extend support to my external business partners who use the solution but are not part of my organization?
Functional support and user training	Ensures that the solution is rolled out in a manner that is most effective based on your organization's structure and employees' roles and responsibilities	- How quickly can you on-board my internal team? - Do you provide additional training online and/or through self-directed online training programs? - Can you provide evidence that my users received training?
Service Level Agreements (SLAs)	Ensures accountability for your extended enterprise	- If my business partner has a problem with your solution, whom do they call? - Do you provide SLAs for system availability, recovery time and recovery point objectives, and the call center?



Conclusion

Your company, its brand and reputation are at risk when sensitive content is shared outside the organization. However, your employees still need to collaborate in order to innovate and drive your business forward. With these high stakes, it is imperative that you know your enterprise collaboration solution provider will keep your sensitive content safe regardless of where it is shared and with whom. More importantly, your solution provider should give you lifetime control of every document that is shared, including the ability to revoke access once it is beyond your firewall.

The checklists in this guide, accompanied by a discussion with potential providers, will ensure that you have done the proper due diligence needed to control the security of your sensitive information. They are based on a holistic framework of considerations important for selecting a provider that gives you end-to-end visibility and control and can withstand the rigors of a regulatory audit.

Sources:

- (<http://my.gartner.com/portal/server.pt?open=512&objID=202&mode=2&PageID=5553&resId=1871515&ref=Webinar-Calendar>)

Gartner Technology Report (page 3)

- http://www.symantec.com/content/en/us/about/media/pdfs/b-cost-of-a-data-breach-global-report-2013.en-us.pdf?om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2013Jun_worldwide_CostofaDataBreach

Ponemon Institute Sponsored by Symantec "2013 Cost of Data Breach Study: Global Analysis" (page 7)

Learn more about Intralinks: intralinks.com

North America: +1 866 473 7194

EMEA: +44 (0) 20 7549 5200

Asia Pacific: +65 6232 2040

Latin America: +55 11 4949 7700