INTRALINKS®

Enterprise. Strength. Collaboration.

Creating Secure, SharePoint-Based External Collaboration Portals

"CIOs are seeking easy-to-implement, low-cost solutions that allow them to securely externalize SharePoint content, so they can leverage their large existing investments in SharePoint infrastructure."

SharePoint has become a leading internal content management and collaboration platform for many enterprises. While the behind-the-firewall use of SharePoint has served many organizations well, business teams that have benefited from improved internal collaboration are now looking to extend these same productivity gains to their inter-enterprise collaboration processes.

Unfortunately, extending SharePoint for inter-enterprise applications introduces a number of IT challenges, including content protection and security, user governance and support, and initial and on-going infrastructure and license costs.

As a result, "CIOs are seeking easy-to-implement, low-cost solutions that allow them to securely externalize SharePoint content, so they can leverage their large existing investments in SharePoint infrastructure," explains former CIO Michael Hugos, who now blogs for *CIO Magazine*.

That existing SharePoint investment is large, indeed. In October 2011, IDC reported that SharePoint sales passed the $1 billion level several years ago and that SharePoint is on its way to becoming Microsoft's first new $2 billion business in a very long time.[1] Microsoft says there are more than 65,000 customers using SharePoint, 67% of which have rolled out SharePoint across their entire organization.[2]

SharePoint is right — and wrong — for external collaboration

What makes SharePoint right for external collaboration are its widespread internal enterprise deployments and the strengths that led to that use. SharePoint provides a stable and scalable foundation for document sharing, team collaboration, electronic forms and social enterprise portals.

SharePoint's extensive installed base means that IT staff has been trained in its operation and support, and business people have learned its user interface and come to depend on it for intra-company document sharing and content management. "The value of that knowledge possessed by IT and line-of-business employees is incalculable — and it's all on top of a company's hard-dollar investment," says Hugos.

[1] *IDC's view of SharePoint's marketshare numbers* - FierceContentManagement, October 18, 2011
http://www.fiercecontentmanagement.com/story/idcs-view-sharepoints-marketshare-numbers/2011-10-18

[2] *SharePoint by the numbers* - FierceContentManagement, October 10, 2011
http://www.fiercecontentmanagement.com/story/sharepoint-numbers/2011-10-10

Yet increasing global competition is forcing business requirements to evolve rapidly. Companies are increasingly looking outside their walls for new and innovative ideas, and to collaborate with a diverse set of partners — and that means outside of their firewalls, as well. This causes them to come up against SharePoint's out-of-the-box weaknesses, such as inadequate auditing and access reporting, file encryption, document locking and protection limitations, and provisioning and supporting a community of external users.

The challenge for CIOs with sizable SharePoint investments and large populations of SharePoint users (and, therefore, expertise) is to build on this existing foundation to provide secure inter-company collaboration and document sharing over the Internet — without adding unnecessary complexity and considerable cost to their IT infrastructure. This challenge is non-trivial, but not insurmountable.

A hybrid solution that leverages your SharePoint investment

Let's examine the attributes of an ideal solution for inter-company collaboration with all the appropriate security, document control and information governance CIOs are looking for:

- Secure, policy-based document-sharing control outside the firewall
- Agile response — the solution should be in place in days or weeks, not months
- Low up-front investment
- Ability to leverage existing systems without adding new complexity
- And an approach for provisioning and supporting a community of external users

To start with, IT departments are working under tight budgets and they need a way to support secure collaboration without buying more servers or investing in customization. Chris Geier, a SharePoint user since 2001 and co-author of *SharePoint Server 2010 Six in One*, recommends cloud solutions for partner and customer collaboration because they simplify identity management tasks and take workload off of internal SharePoint servers. "Getting lots of people on SharePoint doing queries and searches on content is one of the fastest ways to overload servers and degrade performance," he says.[3]

Notes Hugos: "The right cloud-based solution also enables agile response, leverages but unburdens the in-house IT infrastructure, and comes with a business model that creates a predictable cost, and lowers a buyer's up-front investment."

Also, as companies start sharing sensitive documents with their collaboration partners, they need to maintain tight access control. Sunil Arora, an experienced IT project manager who has worked for United Airlines and HSBC Bank, among others, has used SharePoint often and notes that, "SharePoint … control over document access isn't as well defined as many large enterprises might want." Companies need a comprehensive and easy way for granting appropriate document access and they need the ability to create audit trails showing who has seen what information. Ideally, they should be able to use document locking and protection tools to secure content shared outside the corporate firewall, and content tracking and controls to replace or revoke access to already deployed content.

The ideal solution, therefore, would be a hybrid. It would allow internal users to continue using their familiar SharePoint-based platform and applications with little or no change or added overhead. But it would rely on a cloud-based software-as-a-service (SaaS) application with secure document collaboration capabilities to protect sensitive content when engaging with external partners. Those capabilities should include integrated digital rights management (DRM), file encryption, virus protection, external user provisioning and management, and advanced access reporting and auditability.

"The value of that knowledge possessed by IT and line-of-business employees is incalculable — and it's all on top of a company's hard-dollar investment."

— MICHAEL HUGOS, *CIO MAGAZINE*

[3] Geier, Dew, Bertram, Clark, Mitchell, Preston, Schaefer, *SharePoint Six in One*, (Wrox Books — Programmer to Programmer, 2011)

Effective, agile solutions build on the strengths IT departments already have and focus on adding the specific new capabilities they need.

From internal document sharing to secure external document sharing

Effective, agile solutions build on the strengths IT departments already have and focus on adding the specific new capabilities they need. To this end, we've identified a hybrid approach of combining SharePoint with a SaaS-based managed file and content transfer service as the ideal solution for extended enterprise collaboration with external partners.

As a component of this hybrid solution, an external SaaS application would need to bring the following added capabilities to SharePoint:

- Simple-to-administer content access rights for external partners
- Encryption
- Digital Rights Management
- Real-time monitoring and auditing
- Reliable and secure infrastructure and support services

In addition, the system should add these security, compliance, and information governance capabilities without requiring additional SharePoint software customization, or introducing a new user interface that internal SharePoint users have to learn.

Access rights for external partners. Given the large number of potential collaboration partners and the number of documents to share, this requires a granular and dynamic document administration capability. Arora advocates having a single dashboard that gives administrators one place to manage privileges of people to see or download individual documents and groups of documents.

"Once collaboration projects start rolling they move so fast you will be glad you insisted on having a single, easy-to-use way to handle document access privileges across the various projects you are managing," Arora says.

Encryption. As soon as documents leave your SharePoint system and pass beyond your firewall, they need to be encrypted. They need to remain encrypted both as they move over the Internet and while they are at rest in the database or storage system used by the external document sharing application. Hackers can find a way into almost any system if they are determined enough, but when a system's data is encrypted, that data remains secure.

Digital Rights Management. Best-in-class DRM services let IT departments provide secure document access to any device — PC, smartphone, tablet — while dynamically managing content rights even after a document has been distributed. Such systems have the ability to let users view without downloading documents, and prevent printing or screen capture. Finally, digital watermarking identifies a document as confidential and also embeds in the document the name of the person doing the download. This helps ensure that the user will be extra careful not to lose or leak the document.

Monitoring and auditing. The fourth capability is the ability to monitor in real time which people are looking at what documents, for how long, and then to create audit reports from this information. This capability meets the need to create audit trails and reports to verify compliance with data privacy and other relevant regulations, such as the Sarbanes-Oxley Act.

Bruce Radke, a lawyer with Vedder Price P.C., has seen many situations where companies got into needless trouble simply because they could not produce competent audit reports when requested. "The inability to produce relevant information when requested can lead to sanctions and claims of destroying evidence," he explains. "Good records management is the best way to meet current and future e-discovery obligations."[4]

[1] Bruce Radke, Esq., Vedder Price P.C., from his presentation *Proactive Records Management and eDiscovery* made to Chicago SharePoint User's Group, March 18, 2010.

One firm's hybrid solution

All of these capabilities were critical to a major U.S. private equity firm that built just such a hybrid SharePoint-SaaS solution for sharing sensitive information with external investors, explains Peter Bongiorno, Vice Present, Product Marketing for IntraLinks.

"While the firm used SharePoint for their internal collaboration, they needed a secure and audit-ready option to support external client communications for fund raising and to demonstrate compliant fund reporting. This involved authorizing different levels of access to sensitive fund information as a potential investor's interest matured, and required tracking the distribution of investor fund reports to demonstrate compliance. So access rights administration and audit reporting was important," says Bongiorno. Because sensitive information was being shared over public fixed and wireless networks, encryption was an absolute requirement, he adds.

IntraLinks was able to serve the firm's extended enterprise collaboration needs by integrating the secure external collaboration capabilities of the IntraLinks SaaS-based collaboration platform with the firm's internal SharePoint environment through its own proprietary IntraLinks Connector for SharePoint. With the Connector, content is automatically replicated to IntraLinks, users can be provisioned and access rights defined, and access reports and audit trail details viewed all from within a familiar SharePoint user interface.

The result was the firm was able to rapidly implement a secure external content portal for their investors, while internal users could continue to work within their familiar SharePoint environment. This was accomplished without the delay and cost of setting up and supporting a separate SharePoint server farm for external user access.

User interface and ease-of-use considerations

An additional challenge and key consideration of an extended enterprise collaboration solution is a user interface that is familiar to internal users and intuitive and easily understood by external users. For internal users, familiarity with their existing collaboration tools will minimize disruption. For external users, where the opportunity to conduct system training may be limited, an intuitive and easy-to-use interface will be key to adoption and success.

"All the functionality people want may indeed be provided by a system, but if people can't figure out how to use it or feel intimidated by the complexity of a system, they throw up their hands and walk away," says Arora. "People don't like systems that make them feel overwhelmed; they'll find a hundred reasons why it doesn't meet their needs."

It's important that the business users inside your company experience little or no change in the way they use SharePoint.

Similarly, users at partner companies should be able to log onto the external collaboration portal you set up for them and figure out how to start using the basic functions of this new system in a matter of a few minutes, or get immediate answers to questions when this is not the case. On this point, a 24-hour helpdesk that external participants can call for help with more complicated functions is a key consideration. And for a global community of users, that helpdesk should be able to support people speaking a wide range of different languages.

The system should also be easy to implement and use for the IT and administrative staff who will support its operation. That means more configuration than custom implementation, and system administrator functions that provide a single unified view across all external collaboration projects. From a single screen or small group of screens, system administrators should be able to see and manage the status of all projects, and drill down to get greater detail.

"While the firm used SharePoint for their internal collaboration, they needed a secure and audit-ready option to support external client communications for fund raising and to demonstrate compliant fund reporting."

— PETER BONGIORNO, VICE PRESENT, PRODUCT MARKETING, INTRALINKS

Although extended enterprise content-and-collaboration via “out-of-the-box” SharePoint creates challenges in terms of content protection and security, compliance and information governance risk for most corporations, solutions do exist to enable IT departments to securely externalize SharePoint content.

Attributes of the right solution vendors

There are a few additional characteristics to look for when the time comes to select a SaaS partner to help build the hybrid solution for external document sharing via SharePoint described in this paper. Any vendor you select should:

- **Be deployed and audited in many different situations.** The vendor should provide you with audit reports from credible independent organizations that can attest to their trustworthiness and the high standards of security that are used to deliver the vendor’s SaaS offering. Ideally, this means SOC 2 and ISO 9000 compliance.
- **Have good customer evaluations.** The vendor should provide a list of current customers who have also audited their cloud data centers and related operations and satisfied themselves that the service is indeed secure.
- **Provide global coverage.** Look for offices in key locations around the world and support for all the languages you need to do business.
- **Help with installation, training and operation.** The vendor should provide assistance with all aspects of installing, training and creating operating procedures related to using the system.

Conclusion: Leveraging SharePoint for Extended Enterprise Collaboration

Although extended enterprise content-and-collaboration via “out-of-the-box” SharePoint creates challenges in terms of content protection and security, compliance and information governance risk for most corporations, solutions do exist to enable IT departments to securely externalize SharePoint content. This white paper focuses on a hybrid SharePoint-SaaS solution because it represents the ideal option for leveraging an enterprise’s existing investment in SharePoint infrastructure with extensions that are fast to deploy, easy to implement and represent an overall lower total cost of ownership.

INTRALINKS®

Enterprise. Strength. Collaboration.

IntraLinks is a leading global provider of Software-as-a-Service solutions for securely managing content, exchanging critical business information and collaborating within and among organizations. More than 1 million professionals in industries including financial services, pharmaceutical, biotechnology, consumer, energy, industrial, legal, insurance, real estate and technology, as well as government agencies, have utilized IntraLinks' easy-to-use, cloud-based solutions. IntraLinks users can accelerate information-intensive business processes and workflows, meet regulatory and risk management requirements and collaborate with customers, partners and counterparties in a secure, auditable and compliant manner. Professionals at more than 800 of the Fortune 1000 companies have used IntraLinks' solutions. For more information, visit **www.intralinks.com** or **blog.intralinks.com**. You can also follow IntraLinks on Twitter at **www.twitter.com/intralinks** and Facebook at **www.facebook.com/IntraLinks**.

AMERICAS
1 866 INTRALINKS
info@intralinks.com

EUROPE, MIDDLE EAST & AFRICA
+ 44 (0) 20 7549 5200

ASIA PACIFIC
+ 65 6232 2040

LATIN AMERICA
+ 55 0800 892 2247

Terms of use

IL-WP-SHAREPOINT COLLABORATION-120229