Top Four Considerations for Securing Microsoft SharePoint

by Chris McCormack, Product Marketing Manager, Sophos

Microsoft SharePoint is now the standard for internal and external collaboration and content management in much the same way Microsoft Exchange has become the enterprise standard for email. And like Exchange, SharePoint comes with a similar set of adoption challenges: The need to maximize ROI, protect against malware and data loss and establish policies for governance and compliance. This whitepaper examines SharePoint's key risks and recommends best practices to secure SharePoint and protect your organization's digital assets.

Top four considerations for securing Microsoft SharePoint

Microsoft Office SharePoint Server (MOSS) and Windows SharePoint Services (WSS) allows information workers to collaborate on documents, gather data from multiple sources, and publish and distribute materials through one central location. And, while its productivity and empowerment benefits can be easily realized, so can its related risks:

1. Viruses and malware: Infected files or malware is spread through SharePoint
2. Inappropriate content: Illegal or inappropriate content distribution
3. Data loss and compliance: Users obtain access to documents they shouldn't have access to
4. Data tampering: Users changing documents, files, or records without authorization

These risks are particularly critical since the majority of organizations use SharePoint to store and share vital sensitive information.

Top four security considerations

1. Viruses and malware
2. Inappropriate content
3. Data loss and compliance
4. Data tampering

Experts say SharePoint is one of the easiest-to-use tools in the Windows suite. This ease-of-use can create security issues. SharePoint's design enables potentially any user to set up a SharePoint site and often, organizations lack access control guidelines that determine what types of information can be stored, and who can access it. Furthermore, users may incorrectly assume that SharePoint is protected by the organization's corporate security defenses because it's on the company's internal network—a dangerous misconception in many environments. In other cases, employees may let external business partners and contractors access SharePoint without taking steps to secure the exchange of sensitive data. These types of decentralized SharePoint environments obviously pose a significant risk.

On the other hand, centrally-managed SharePoint environments are more contained, typically consisting of a single server farm managed by IT with established provisioning models and security guidelines. While this provides you with more control and oversight, the day-to-day administration tasks such as monitoring, reporting, user and policy configuration and quarantine management can amount to a substantial investment in time. As a result, this model has its own undesirable compromises.

What's Microsoft SharePoint Exactly?

Microsoft SharePoint comprises two components: Windows SharePoint Services (WSS) and Microsoft Office SharePoint Server (MOSS).

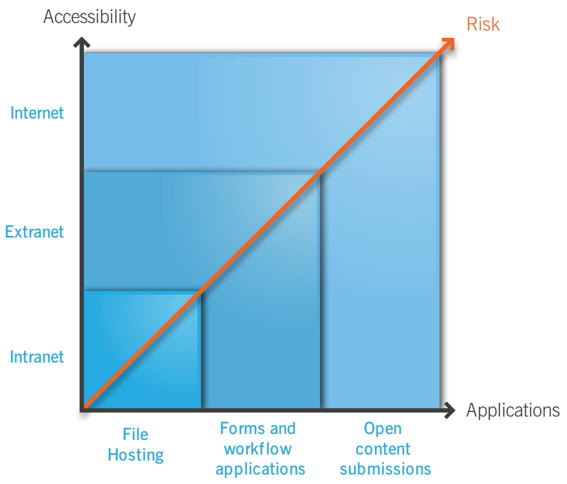
1. Windows SharePoint Services—Windows SharePoint Services is an extension of Windows Server, designed to provide collaboration tools and functions for small and medium-sized organizations. WSS lets employees create workspaces, share calendars and contacts and use Web 2.0 technologies such as blogs, wikis and RSS feeds. One of the primary reasons organizations deploy Windows SharePoint Services is for its basic document management features, which include document library services to check documents in and out, as well as Information Rights Management to control the actions users are allowed to take.

2. Microsoft Office SharePoint Server—MOSS is a collaboration and content management server that provides IT pros and developers with the platform and tools they need for server administration, application extensibility and interoperability. Microsoft Office SharePoint Server is intended for medium-sized and large organizations with more than 1,000 users.

Assessing reward versus risk

As an IT manager, you want to be able to maximize SharePoint's rich functionality. You also need to mitigate the risks that arise when you enable SharePoint to extend beyond the organizations guarded perimeter. Even when SharePoint is used predominantly by internal users (see chart 1) the malware threat remains significant.

And when outside partners and applications can access SharePoint, the risks are magnified exponentially. You must realize that maximizing SharePoint's full features increases its vulnerability to malware and data loss.



Evaluate Microsoft SharePoint's rewards and risks

So what can you do to make sure your organization's digital assets are readily available to those that can benefit, but keep them secure? You should assess the risks that apply to your operation, then use a combination of specific technologies, layered protection strategies and access controls to protect your organization's data and mitigate the risks.

What are the four primary risks?

1. Viruses and other forms of malware

Windows SharePoint Services stores documents, lists, views and other information in a Microsoft SQL Server database.

Collaborative workspaces are an easy way to share files and content with your colleagues, which increases the odds of malware and virus infection. And the threat of malware spread increases, if non-networked, unmanaged machines exchange data (for example, enabling customers to post attachments or links to untrustworthy sites in a SharePoint-based environment).

To find malware and suspicious files stored within the database we recommend that you deploy an antivirus suite designed to scan SQL Server database stores—a capability that typical endpoint/server antivirus solutions lack. Also, consider these features:

- On-access, on-demand, or on-schedule protection from malware, viruses, spyware, adware, suspicious files and potentially unwanted applications (PUAs), which ensures maximum security while offering a completely transparent end-user experience.
- Proactive zero-day detection of new malware that uses behavioral scanning technology.
- Integrated quarantine manager to delete, disinfect or authorize files.

2. Access to inappropriate content

Don't let your SharePoint portal become a vast source of inappropriate, illegal or similar content that violates legal requirements for compliance and governance. To prevent non-compliance:

- Simplify compliance with advanced content filtering.
- Make sure the third-party solution you deploy includes a comprehensive content scanning and policy engine.
- Control file types based on file name, size, or type using true-file-type technology to prevent file type masquerading.

3. Data loss of the company's competitive and business intelligence

Because SharePoint technology enables the easy exchange of files between users, even if you have deployed security policies on perimeter and mail servers, users might still try to use SharePoint to exchange files that email security solutions would normally block. You can prevent data loss if you:

- Deploy SharePoint in a secure and effective manner, utilizing the full range of policy enforcement capabilities that SharePoint 2010 and Windows Server 2008 offer.
- Establish appropriate user permissions and use the full capabilities offered by SharePoint's Information Rights Management to protect your sensitive content.
- Select a security solution that includes integrated data protection capabilities to enforce compliance on acceptable use and policies for uploading and downloading sensitive information

4. Data tampering

According to a 2009 SharePoint Security Survey, "one-quarter of 330 respondents were not confident that their organizations' electronic records or other digital content were protected when shared within the SharePoint environment. And of the respondents whose organizations had a SharePoint-related data breach, 67% said the "data tampering was at the hands of a person with access to SharePoint from inside the organization." To prevent data tampering we recommend you:

- Deploy SharePoint in a secure and effective manner and use the full range of policy enforcement capabilities that SharePoint 2010 and Windows Server 2008 offer.
- Take advantage of the encryption options available as part of SQL Server 2008 and SharePoint 2010 including Transparent Data Encryption (TDE) that encrypts the database at the disc level, using SSL between SharePoint and the SQL Server to encrypt transactions, and Information Rights Management to encrypt individual files.
- Select a security solution with integrated data protection that is fully transparent to end users, and easy to administer from a single central console.

Other security concerns

A 2010 IDC study determined that 72% of the workforce in the United States is already mobile with other geographies catching up quickly. "Underserved mobile workers across all regions stand to benefit from the reach and flexibility offered by mobile solutions. While some barriers to adoption have to be overcome, the potential market for mobility solutions is enormous." However, many IT execs don't have control over the associated risks, costs or benefits.

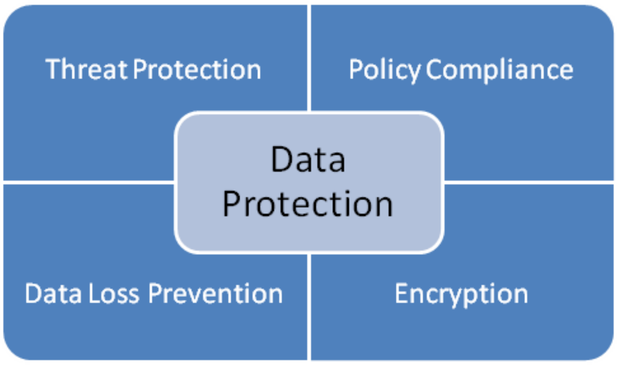
So how can you protect the critical business information that's stored in your SharePoint system? Design and roll out a data protection strategy.

What's a Data Protection Strategy?

Data protection is a general term for technologies, tools and best practices that help protect an organization's sensitive data.

An effective data protection strategy balances protection with productivity.

An ideal data protection strategy integrates key technologies with best practices and pre-packaged intelligence to make effective policies out of the box—helping you get started faster. It's also easy to deploy, simple to administer and affordable.



A comprehensive data protection strategy must include:

Threat Protection: Threat protection must include intrusion prevention, firewall, antivirus, anti-malware and anti-spam to ensure hackers don't gain a foothold on your network and compromise and steal sensitive data. Since threats are constantly evolving and are financially driven, it's critical to find a solution that can identify and block new threats before they're catalogued. With Microsoft SharePoint, it's important to implement a security solution that can scan the SharePoint data stores for threats, a capability that a typical server endpoint protection doesn't provide.

Policy Compliance: To reduce threats and legal liability. Policy compliance should provide application control (e.g., instant messaging), removable storage devices (e.g., USB keys), and corporate systems (e.g., web browsing and email). Application control lets employees use SharePoint and other tools they need to do their job and you peace-of-mind that they're not inadvertently exposing sensitive information.

Data Loss Prevention: Data Loss Prevention (DLP) provides automated oversight and monitors data movement to prevent users from accidentally exposing sensitive information via removable storage devices or Internet applications. Content control lists (CCL's) are a critical element of DLP, defining data types that need to be protected such as personally identifiable information (PII) or financial data including credit card numbers and bank accounts. The ideal solution should provide pre-packaged CCL's to make deployment and configuration quick and painless while also integrating tightly with policy compliance and other components of the data protection strategy—all while providing a seamless experience for users that minimizes impact on productivity.

Encryption: Encryption protects your data's confidentiality, integrity and authenticity at rest or on the move. It's a key requirement for many regulations. Encryption should secure data on desktops and servers, mobile devices including laptops and removable storage media, as well as data exchanged over email. The ideal solution is not only transparent to end users-to avoid productivity and workflow disruptions- but also easy to deploy and manage with flexible policies that adapt to your business. Furthermore, a solution that integrates encryption with DLP provides a significant advantage in ensuring any sensitive data that is allowed to be moved off the network for valid business reasons cannot be compromised.

Our Microsoft SharePoint product provides award-winning real-time protection for your critical business data and collaborative environment, stopping viruses, spyware, adware, suspicious files, and potentially unwanted applications (PUAs). In addition, it uses sophisticated data control capabilities to prevent the distribution of sensitive or inappropriate content.

Visit https://secure.sophos.com/products/enterprise/free-trials/sharepoint/ for a free 30-day trial.

Boston, USA | Oxford, UK