

Solving four primary security challenges of Microsoft SharePoint

Microsoft SharePoint has quickly become the enterprise standard for internal and external collaboration and content management much in the same way Microsoft Exchange has become the enterprise standard for email. However, along with SharePoint's acceptance comes the same challenges that enveloped Exchange: The need to maximize ROI, guard against viruses and data leakage, and establish policies for governance and compliance. This white paper examines SharePoint's benefits and risks and recommends best practices for protecting an organization's digital assets.

by Chris McCormack, Product Marketing Manager, Sophos

Solving four primary security challenges of Microsoft SharePoint

Introduction to SharePoint

Microsoft Windows SharePoint enables information workers to collaborate on documents, exchange files, problem-solve, strategize, link to live web content and create tables and reports that are culled from an organization's databases. SharePoint offers many benefits for organizations, especially those with 1,000 employees or more, because it:

- » Increases employee productivity by streamlining day-to-day business operations
- » Reduces project cycle time through collaboration
- » Empowers employees to make informed decisions by providing centralized access to information
- » Helps meet regulatory requirements through total content control
- » Simplifies access to structured and non-structured data across various systems

- » Offers a unique, integrated platform for managing business-wide intranet, extranet and internet applications

Microsoft SharePoint comprises two main components: Windows SharePoint Services 3.0 (WSS) and Microsoft Office SharePoint Server (MOSS). Read "What is Microsoft SharePoint, Exactly?" on page 5.

Microsoft SharePoint sales broke the \$1 billion revenue mark in 2008 with more than 100 million licenses sold, leading one market research analyst to proclaim that "SharePoint is the hottest-selling server-side product ever for the company." Other analysts predict the growth of the popular content management and collaboration platform will remain steady and they expect to see it grow at a remarkable average annual rate of 25% over the next 4 years.

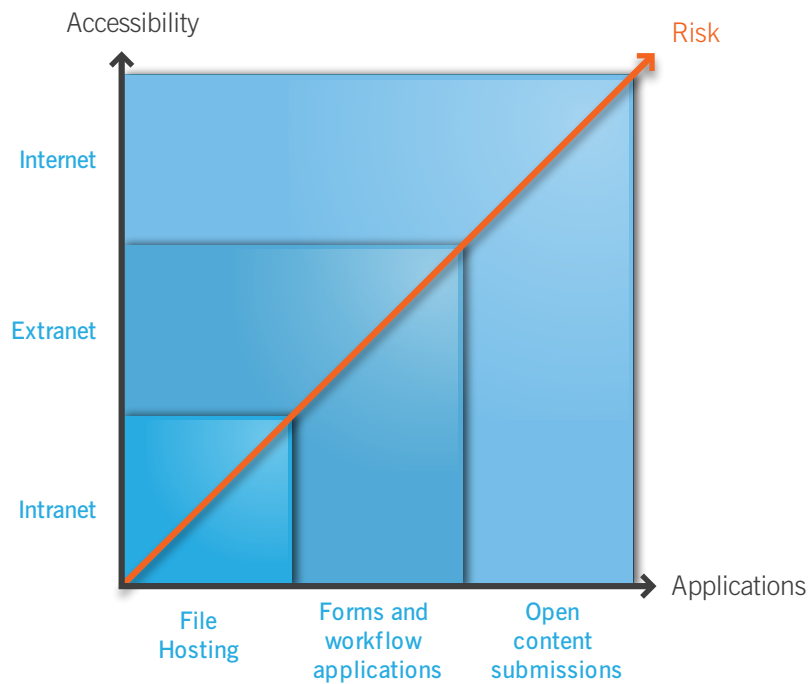
Today, a majority of organizations are using SharePoint to store and share their most vital electronic records such as strategic corporate planning documents, company financials, employee records, critical intellectual property records and personal health records.

What is Microsoft SharePoint Exactly?

Microsoft SharePoint comprises two components: Windows SharePoint Services 3.0 (WSS) and Microsoft Office SharePoint Server (MOSS).

1. Windows SharePoint Services — Microsoft's Windows SharePoint Services is an extension of Windows Server, designed to provide collaboration tools and functions for small and medium-sized organizations. WSS makes it possible for employees to 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 admin, app 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

One of the key challenges IT managers and administrators face is finding a way to balance SharePoint's rich functionality with the attendant risks that come from making interactive content more accessible beyond the organization's walled garden. Even when SharePoint is used mainly by internal users (see shaded area in the figure on page 2) the threat of malware propagating across the network is remains significant.

As access to SharePoint is broadened to include outside partners and applications, the risks are magnified exponentially. What this means for IT managers and admins is that fully leveraging the organization's investment in SharePoint also increases its vulnerability to malware, data leakage and many other concerns.

A secure deployment consists of layers of security backed with appropriate access controls so that the organization's content is well protected while at the same time accessible beyond the walls of the organization.

What are the four primary risks?

SharePoint is susceptible to a variety of existing and emerging threats:

1. Viruses and other malware
2. Access to inappropriate content
3. Data leakage of the company's competitive and business intelligence
4. Data tampering by internal and external users

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, which only increases the odds of contracting viruses and other forms of malware. This is a significant concern if content originates from outside the organization from unmanaged machines (for example, enabling customers to post attachments or links to untrustworthy sites in a SharePoint-based environment).

Recommendations

Deploy an anti-virus suite designed for scanning SQL Server database stores to find malware and suspicious files stored within the database — a capability that typical endpoint/server AV solutions lack. Other features to consider include:

- » On-access, on-demand, or on-schedule protection from malware, viruses, spyware, adware, suspicious files and potentially unwanted applications, which ensures maximum security while offering a completely transparent end-user experience.
- » Proactive zero-day detection of new malware using Behavioral Genotype technology.
- » Integrated quarantine manager for deleting, disinfecting or authorizing 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.

Recommendations

- » 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 leakage of the company's competitive and business intelligence

Because SharePoint technology enables the easy exchange of files between users, even if you've deployed security policies on perimeter and mail servers, users might still try to use SharePoint to exchange files that would ordinarily be blocked by email security.

Recommendations

- » Look for a solution that specifically ensures sensitive data is not being leaked through SharePoint or Exchange.
- » Employ content control that prohibits users from uploading or downloading sensitive information.
- » Check to see that files can be controlled by file name and by content (words and phrases) within files.

4. Data tampering

According to a recent survey, one-quarter of 330 respondents lack confidence that their organizations' electronic records or other digital content are protected when they are being shared within the SharePoint environment. Of the respondents whose organizations have suffered a data breach within their SharePoint systems, 67% indicated that the tampering was at the hands of a person with access to SharePoint from inside the organization.

Recommendations

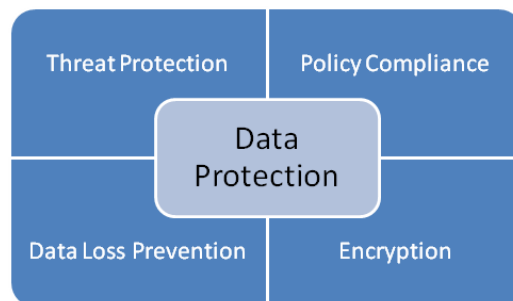
- » Look for a modular information protection control solution that enforces policy-based security for PCs and mobile devices across mixed environments.
- » It should be fully transparent to end users and easy to administer from a single central console. Finally, its modular architecture provides comprehensive data security tailored to your organization's needs and growth requirements.
- » Delivers centralized data security control across mixed IT environments.
- » Provides consistent implementation and enforcement of company-wide security policies.
- » Makes storage, exchange and recovery of keys simple and easy through centralized state-of-the-art key management

- » Provides comprehensive data protection on all kinds of devices, including: laptops, desktops, removable media, PDAs, CDs, and email
- » Offers encryption and data leakage prevention (DLP) under a single management console.
- » Fully manages Windows Vista BitLocker Drive Encryption
- » Integrates quickly and effectively with existing security infrastructures and automates administrative tasks.

Emerging concerns

- » The threats are getting greater and are not likely to subside any time soon, if ever. One reason is that employee mobility continues to rise. The 2009 Total Employee Mobility Benchmarking Report, released by Runzheimer International, notes 51% of the workforce is mobile on any given day. However, many IT execs do not have control over the associated risks, costs or benefits. The annual report was developed through interviews with executives from 90 small, mid-sized and large organizations across the U.S.
- » SharePoint is among the easiest-to-use tools in the Windows suite, experts say. The problem is any user can set up a SharePoint site, and, often, there are no guidelines for who can access it or what data can be stored there. Some users assume that because it's used on the company's internal network, SharePoint data must be protected by the standard corporate security defenses. In other cases, employees make the mistake of offering SharePoint access to business partners or contractors outside of the company, without taking steps to secure the exchange of data.

A layered approach to data protection



What do we mean by data protection?

Data protection is an umbrella term for technologies, tools, and best practices related to protecting sensitive data within organizations. An effective data protection strategy is one that balances protection with productivity — ensuring that all sensitive and confidential data is secure without preventing users from going about their daily business tasks.

For a strategy to be successful, the technologies need to be implemented in a timely fashion while being affordable, easy to deploy and simple to administer.

The ideal solution to the problem of data protection is therefore one that integrates key technologies with best practices and pre-packaged intelligence to make effective policies out of the box — helping you get started faster.

Effective data protection = Technology that embodies best practices + Pre-packaged intelligence

A comprehensive data protection strategy should cover the following four key areas:

Threat Protection: Threat protection should protect data against infection from malware and prevent hackers from gaining direct or indirect access to sensitive data on your systems and network. Thus threat protection must include: intrusion prevention, firewall, anti-virus, anti-malware, and anti-spam to ensure hackers do not gain a foot-hold on your network with which to compromise and steal sensitive data. Since threats are constantly evolving and becoming more financially driven, proactive protection that can identify and block new threats before they are cataloged is critical.

Policy Compliance: The role of policy compliance is to reduce the threat landscape, legal liability and exposure by implementing best practices in the form of policy to prevent users from inadvertently still giving them the tools they need to go about their daily work. Policy compliance should provide control over applications (e.g., instant messaging, putting themselves or the organization at risk while P2P file sharing), removable storage devices (e.g., USB keys), and corporate systems (e.g., web browsing and email). Controlling the way in which these are used means that employees can be given the tools they need to do their job without putting data at risk.

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 is essential for protecting the confidentiality, integrity, and authenticity of data at rest or on the move and is a key requirement for many regulations. It should secure data on desktops and servers, mobile devices including laptops and removable storage media, as well as data that is allowed to be sent via email. The ideal solution is one that is both transparent to the end user to avoid productivity and workflow disruptions, while also being 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.

Sophos solution

Sophos for Microsoft SharePoint provides award-winning real-time protection for your mission-critical business data and collaborative environment, stopping viruses, spyware, adware, suspicious files, and potentially unwanted applications (PUAs). In addition, Sophos for Microsoft SharePoint uses sophisticated content filtering 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
© Copyright 2009. Sophos Plc

*All registered trademarks and copyrights are understood and recognized by Sophos.
No part of this publication may be reproduced, stored in a retrieval system, or transmitted by any
form or by any means without the prior written permission of the publishers.*

SOPHOS
WWW.SOPHOS.COM