

A background image showing a laptop on a desk with a speedometer overlay. The speedometer has numbers from 0 to 70 and a needle pointing towards 40. The scene is dimly lit, suggesting an office environment.

Protect Microsoft™ SharePoint™ 2003 & 2007 Environments

 A Trend Micro White Paper | July 2009

TABLE OF CONTENTS

INTRODUCTION.....	3
OVERVIEW: SHAREPOINT.....	3
• A Growing Base of Users	
• Evolving Threats	
• SharePoint Portals and User Capabilities	
• SharePoint Deployment Scenarios	
PROVEN, ENTERPRISE-CLASS SHAREPOINT SECURITY.....	5
• Highly Effective Protection	
• Scanning Options	
PORTALPROTECT™ ARCHITECTURE.....	7
• Optimal Performance	
• Minimal Impact to Administrators	
CONCLUSIONS.....	10

INTRODUCTION

Employees spend increasing amounts of time organizing, managing, and searching through the information residing on enterprise information portals (EIPs). Microsoft™ Office SharePoint Services (MOSS) 2007 helps businesses create corporate Web portals with powerful indexing and search functions, extensive document management features, and rich collaboration options. While MOSS makes it easy to provide users with access to information and individuals in real time, regardless of physical location, it also introduces new risks. Within MOSS environments, malware of all kinds can spread and sensitive information can be exposed. According to Gartner, “collaborative workspaces provide an easy mechanism for file and content sharing, which also facilitates malware propagation.”¹ The results include infected systems and lost or stolen information.

To address these risks, **Trend Micro™ PortalProtect™ for Microsoft SharePoint** helps secure collaborative environments. This proven security solution protects users and organizations from intrusion, infection, and data loss to preserve competitive advantage, reputation, and revenues. **PortalProtect** was the first solution designed for Microsoft SharePoint and currently supports the latest platforms: Microsoft SharePoint Services 2.0 & 3.0, and SharePoint Portal 2003 & 2007. Built on proven enterprise-class technology, PortalProtect offers customers highly effective protection, high scalability and reliability, and low administration.

OVERVIEW: SHAREPOINT

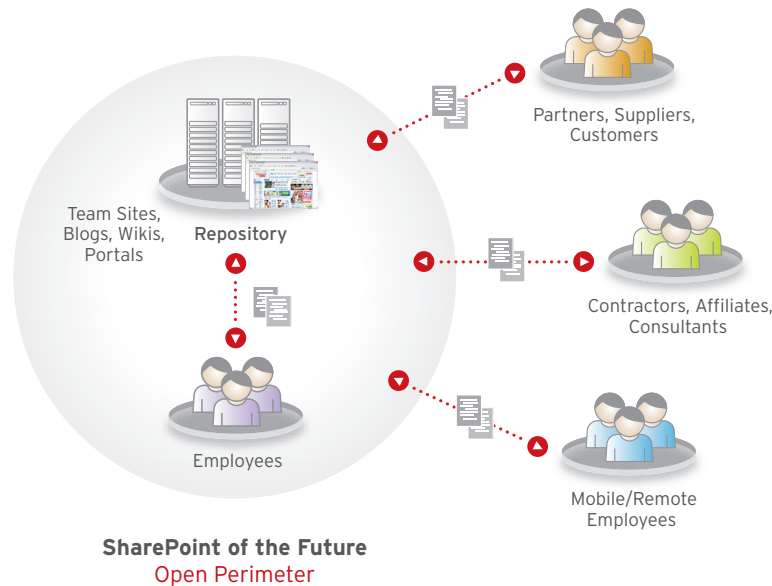
A Growing Base of Users

The use of Microsoft SharePoint continues to grow, and Gartner estimates that roughly 60% of organizations using Microsoft Exchange will also deploy Microsoft SharePoint. Its role is expanding to reach external users such as contractors, partners, affiliates, and customers. According to Osterman Research², 48% of organizations allow contractors or consultants to access their SharePoint portals, 38% give access to business partners, and 31% open them to affiliates. This same report states “the security for each of these groups is clearly outside the control of IT in most cases, leaving organizations that have not deployed SharePoint-specific security vulnerable.” In general, security risks increase as SharePoint environments expand to support larger numbers and more diverse groups of users.

¹ Gartner Research. Security Considerations and Best Practices for Securing SharePoint. February 2009.

² Osterman Research. The Need for SharePoint Security. January 2009.

Protect Microsoft™ SharePoint™ 2003 & 2007 Environments



Evolving Threats

As the user base is growing, the threat landscape is also changing. Attacks are increasingly sophisticated and targeted, and are infiltrating new avenues of propagation. In particular, threats relating to Microsoft Office increased by 300% year-over-year in 2007. Since Microsoft Office enables the primary content within information repositories, this is a significant threat for SharePoint users.

The average malware has become more sophisticated, often using social engineering to convincingly pose as legitimate business-oriented attachments such as eTicket receipts, package delivery notices, offers of business financial products, and much more. To read more about this evolution of malware, [register](#) to download Trend Micro whitepapers such as “Assessing SharePoint Risk” or [visit the Trend Micro resource center](#).

SharePoint Portals and User Capabilities

MOSS offers a broad range of capabilities in a single platform. To keep a SharePoint environment secure and operating optimally, the risks associated with the different capabilities must be identified and understood. In general, the application types and access controls used for the collaborative environment will determine the required security.

SharePoint collaboration features include document lifecycle capabilities, alerts, key task notifications, Really Simple Syndication (RSS), a basic web-based user interface, and navigation capabilities.

SharePoint portal components offer customers the ability to create, deploy, and manage intranets, extranets, team portals, and more. Information can be indexed, giving users the ability to perform automated searches for fast information retrieval. A SharePoint portal also delivers enhanced authoring, business document processing, web content management and publishing, records management, policy management, and support for multilingual publishing.

Underpinning the portals are Windows SharePoint Services (WSS) for document management. These include versioning controls, check-in/check-out document locking, rich descriptive metadata creation, workflow management, content type-based policies, auditing, and role-based-access control at the document library, folder, and individual document levels.

WSS also incorporates the Antivirus Manager (AVM), which stores file properties of the scan status from the WSS database. This helps antivirus solution vendors perform real-time scanning of documents as they are checked in or out of a SharePoint repository.

SharePoint Deployment Scenarios

Windows SharePoint provides customers with a choice of deployment scenarios. The two most commonly used are the stand-alone and server farm scenarios.

Stand-Alone Deployments

A stand-alone deployment of WSS has all Sharepoint services installed on one server. This provides a simple setup for evaluating capabilities. The stand-alone scenario can also be used for deployments of multiple websites on separate servers, allowing for easier administration especially when the sites are geographically distributed or locally managed.

Server Farms

These typically consist of at least one database or back-end server running Microsoft SQL Server 2000 or 2005, and one or more front-end servers running Internet Information Services (IIS) and Windows SharePoint Services 3.0. Front-end servers are configured as web servers, providing content and offering services such as searches. Server farms are the best SharePoint configuration choice for gaining optimum performance when hosting of a large number of websites or when supporting a large number of users. In a server farm deployment, one or more servers will be dedicated to running specific WSS applications. The front-end servers efficiently manage user access to the resources on the back-end servers.

More information on SharePoint deployments is available at: <http://technet2.Microsoft.com/windowsserver/WSS/en/library/0127769d-11aa-469d-80d7-fbd0b20e421c1033.msp?mfr=true>

PROVEN, ENTERPRISE-CLASS SHAREPOINT SECURITY

Working closely with its long-time partner, Microsoft, Trend Micro optimizes and tightly integrates its core content security technologies with the SharePoint platform. As a result, customers receive a unique combination of highly effective protection with minimal impact to servers and administrators. Trend Micro security is characterized with both enterprise-class scalability and manageability.

Highly Effective Protection

Trend Micro PortalProtect builds on the industry-leading and platform-optimized technology first introduced as part of Trend Micro ScanMail™ for Microsoft™ Exchange. This includes Trend Micro's proprietary scan engine

and pattern file technology for stopping constantly evolving threats. Working together, the scan engine and patterns detect malware of all types including viruses, Internet worms, Trojan horses, and network exploits. The Trend Micro technology can also decrypt all major encryption formats including MIME and BinHex and common compression formats such as Zip, Arj, and Cab.

PortalProtect uses Microsoft's Virus Scanning API (VSAPI) to scan documents as they are checked in, checked out, or published to the SharePoint site. It then directs the SharePoint Antivirus Manager to take any necessary action on the files, based on the results of scanning and organizational policy.

In addition to malware scanning, PortalProtect also offers file blocking based on true file type, file name, size, or other characteristics. This capability can be used to enforce standard policies concerning file types or to trigger special lockdown measures during a malware incident. PortalProtect can proactively quarantine or delete specified files located in the Web Storage System or those files being introduced or checked in to the repository. Note that blocked files cannot enter the system; therefore, they need not be scanned and do not slow down overall scan performance. It is recommended that each organization define a security policy in regard to various file types and to configure security accordingly. Special attention should be paid to configuring file type blocking, with high-risk extensions such as .exe and .com routinely blocked.

Trend Micro PortalProtect is kept up to date with the latest pattern files, which can be scheduled for automatic downloading from a designated ActiveUpdate server or other Internet/intranet sources that use HTTP.

Scanning Options

PortalProtect minimizes security risk (and the associated business risks) by detecting and blocking malware before it can impact SharePoint's Storage System. Customers can take advantage of three different scanning options: real-time, manual, and scheduled. Regardless of the scanning option used, PortalProtect's Real-time Monitor displays details about scanned files, discovered viruses and malware, and the status of any manual or real-time scan in progress.

Real-Time Scans

Real-time scanning is a powerful, multi-threaded feature that works in the background. Files are scanned at the time that they are checked in, checked out, saved, or retrieved. This scanning option is the most effective way to keep the malware from entering the repository and to ensure that files accessed by users are free of malicious, inappropriate, or unauthorized content. Trend Micro's performance tests show that PortalProtect delivers twice the throughput of other SharePoint antivirus products³. This is particularly important since throughput determines end-user latency, and therefore determines adoption rates and impacts the number of Help Desk calls.

Manual Scans

A manual scan (Scan Now) can be triggered by the administrator and inspects all specified files in the SharePoint Web Storage System. PortalProtect's manual and scheduled scans (see next section) can be granular or general in scope. The administrator can invoke a scan of the entire document store, specified sites, or just designated individual folders. The time required for a manual scan depends on the number of files to be scanned and the hardware resources available. The most common use for manual scanning is to identify specific malicious, suspect, or sensitive files that need to be removed from the repository.

³ Trend Micro. Trend Micro™ PortalProtect™ 1.7 for Microsoft™ SharePoint™ Performance Report. July 2008.

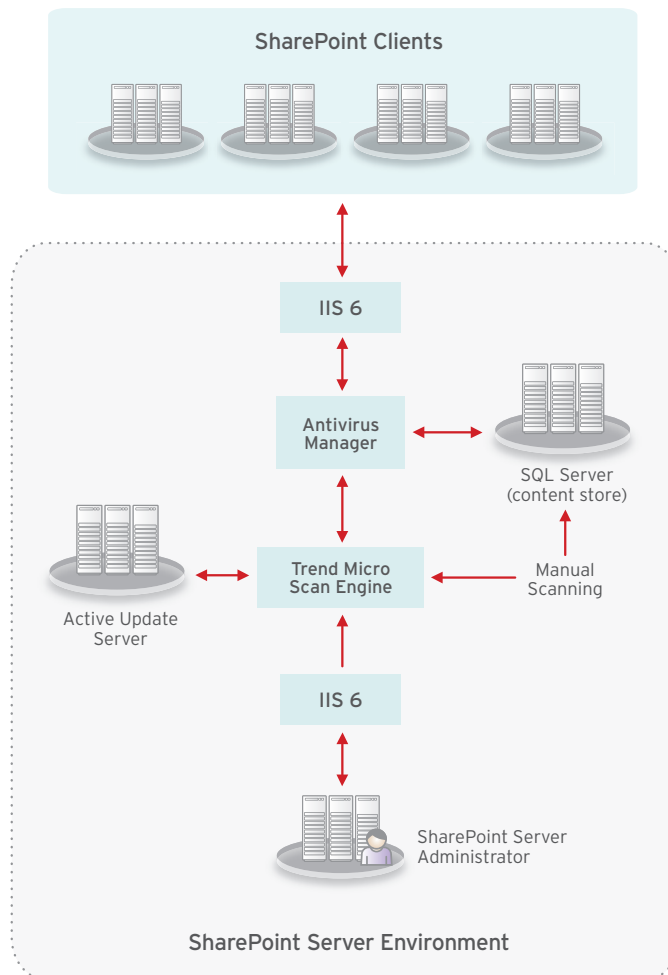
Protect Microsoft™ SharePoint™ 2003 & 2007 Environments

Scheduled Scans

Administrators can also use scheduled scans to automate routine inspection of the repository (often during off-peak hours), improving antivirus management efficiency and giving administrators more control over antivirus policy. Besides keeping the environment and users safe, scheduled scans can be used to log results for reporting, audits, and overall peace of mind.

PORTALPROTECT ARCHITECTURE

The figure that follows illustrates the Trend Micro PortalProtect architecture and shows how Microsoft Office, Internet Explorer, and other applications communicate within the SharePoint Services environment. As mentioned previously, the Antivirus Manager is responsible for sending content to PortalProtect to be scanned prior to being checked into the repository or checked out by users.

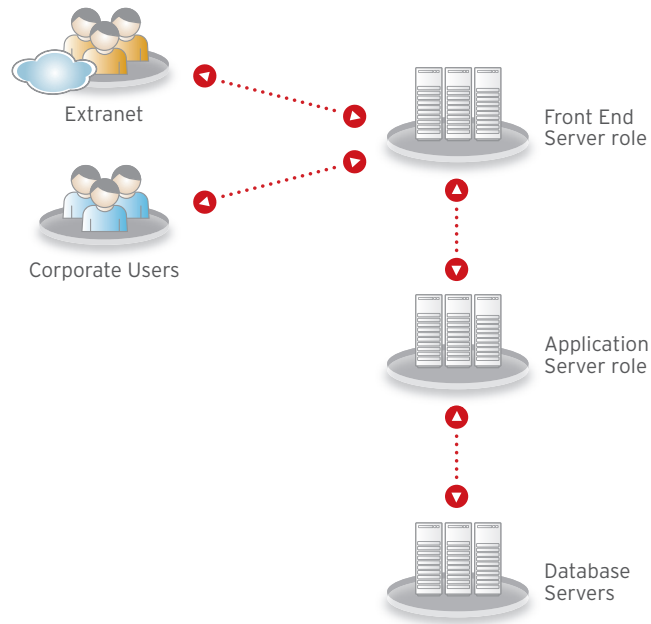


More information can be found in the [Getting Started Guide](#).

Protect Microsoft™ SharePoint™ 2003 & 2007 Environments

Optimal Performance

In addition to incorporating Trend Micro's award-winning antivirus scan engine, PortalProtect takes advantage of enterprise security technology to deliver proven, optimal performance, reliability, and scalability. As with Trend Micro ScanMail for Microsoft Exchange, PortalProtect is designed to run with little monitoring or management once deployed. It also delivers high performance by taking advantage of multi-threaded scanning and the x64-bit processing of today's hardware platforms.



Regardless of the number or size of individual SharePoint servers, PortalProtect's tight integration and agent-less scanning model ensures complete scalability, making it ideal for businesses of all sizes. PortalProtect was developed to get maximum benefits from Microsoft technologies. Future expansion of server farms has been taken into account in the design of PortalProtect, which requires installation on the front-end servers only. PortalProtect does not need to be installed anywhere else because it uses the same technology that SharePoint itself uses to communicate between the front-end and back-end servers.

For years, administrators have relied on PortalProtect to provide security for the enterprise as the SharePoint environment expands and evolves. And with 3–8% CPU utilization⁴, customers need not worry about impact to the server or latency for the end user.

⁴ Trend Micro. Trend Micro™ PortalProtect™ 1.7 for Microsoft™ SharePoint™ Performance Report. July 2008.

Minimal Impact to Administrators

The value of PortalProtect is further enhanced by its low administration requirements. To reduce the time required for deploying, configuring, and managing PortalProtect and collaboration security, Trend Micro provides many time-saving features. To start, an install wizard and powerful group management capabilities speed deployment. Administrators can remotely or locally deploy PortalProtect to a single server or multiple servers simultaneously. Installation can also be scripted for smooth, easy deployment.

Once deployed, an intuitive web-based management console gives administrators secure, convenient access to configuration details, reports, logs, customized notifications, and more—regardless of physical location or platform. Additionally, its Real-time Monitor and Server Status Console display current information and important events, such as the last virus found.

Behind the scenes, PortalProtect ActiveUpdate can be used to automatically supply PortalProtect Servers with the most current pattern files and scan engine updates. And these PortalProtect Servers can share pattern files and scan engine updates for intelligent use of corporate network bandwidth.

Automated, customizable, real-time notifications keep administrators abreast of any new malware attacks or service abnormalities. Additionally, PortalProtect automatically generates HTML system status reports on a daily, weekly, or monthly basis, and sends them via email to specified recipients. Comprehensive logs provide a recent history of service activities and details about infected documents. Log files can be exported into CSV format.

Finally, PortalProtect integrates with Trend Micro Control Manager™ enabling services-like group policy replication, configuration replication, centralized pattern and scan engine deployments, outbreak prevention services, and remote agent installation.

These usability features and more contribute to administrative effort that is half that of other SharePoint security products.⁵ To see the time savings reported by real-world users, feel free to read the TCO Report from Osterman Research.

CONCLUSIONS

Microsoft Windows SharePoint Services and Office SharePoint Server provide a powerful suite of collaborative capabilities that improve productivity by increasing access to information and individuals, while also facilitating knowledge sharing especially across geographic boundaries. However, without the requisite security solution, the platform can actually serve as a real-time platform for the spread of malicious code. Cyber criminals often take advantage of undiscovered or un-patched vulnerabilities in the SharePoint environment or Office content to spread malware.

Given increased adoption, growing use by remote, mobile, and external users (whose security is often difficult to keep current or control), it is critical that a security solution be deployed in SharePoint environments. Gartner's recommendation is to "treat all content attachment uploads from all external sources (ideally all content) as potentially hostile and scan all content, regardless of extension."⁶ It should be a solution that can provide optimum

⁵ Osterman Research. Comparing Leading Email and SharePoint Security Solutions. January 2009.

⁶ Gartner Research. Security Considerations and Best Practices for Securing SharePoint. February 2009.

Protect Microsoft™ SharePoint™ 2003 & 2007 Environments

protection—from intrusion, infection, and data theft or loss—while also minimizing impact on SharePoint servers and administrators. As with email, Trend Micro recommends a layered security model that includes protection for the SharePoint server as well as clients. A server represents a logical point for centralized inspection of incoming and outgoing files, as well as the only place to keep the repository clean. In many cases, the server is the place where security must be tightly controlled, especially when partners, affiliates, and contractors have access. Client systems are generally the ultimate target of malware, and as such must also be guarded.

Additional best practice security recommendations for SharePoint deployments, above and beyond securing the repository from malware include:

1. Protect the underlying operating system on your SharePoint servers against worms and other attacks by deploying server antivirus solutions, such as Trend Micro™ OfficeScan™ Client-Server Suite or Trend Micro ServerProtect™, and keeping them up to date with the latest patches. Also consider an Intrusion Prevention System (IPS) to protect the operating system before patches are available.
2. Define your most sensitive data and control access to it based on SharePoint permission (no administrator or user should have full permissions over all content) as well as its use by instituting content filtering or data leak prevention technology.
3. Keep your SharePoint infrastructure (back-end SQL database and front-end websites) patched and properly configured to check application and user access permissions, plus consider additional web threat protection. Contact Trend Micro for more information on new security technologies in this area, including the next major release of Trend Micro PortalProtect.
4. Deploy, configure, and routinely test a SharePoint back-up solution, whether it is a capability built into SharePoint itself or third-party software deployed with it.

TREND MICRO™

Trend Micro Incorporated is a pioneer in secure content and threat management. Founded in 1988, Trend Micro provides individuals and organizations of all sizes with award-winning security software, hardware and services. With headquarters in Tokyo and operations in more than 30 countries, Trend Micro solutions are sold through corporate and value-added resellers and service providers worldwide. For additional information and evaluation copies of Trend Micro products and services, visit our Web site at www.trendmicro.com

TREND MICRO INC.

10101 N. De Anza Blvd.
Cupertino, CA 95014

US toll free: 1 +800-228-5651

phone: 1+408-257-1500

fax: 1+408-257-2003

www.trendmicro.com

