



White Paper

Spring 2002

TREND MICRO, INC.
10101 N. DE ANZA BLVD.
CUPERTINO, CA 95014
T 800.228.5651 / 408.257.1500
F 408.257.2003
WWW.TRENDMICRO.COM

Trend Micro PortalProtect for Microsoft SharePoint Portal

TABLE OF CONTENTS

3	INTRODUCTION
4	HOW DOES TREND MICRO PORTALPROTECT WORK?
5	MICROSOFT SHAREPOINT PORTAL SERVER
6	TREND MICRO PORTALPROTECT FOR MICROSOFT SHAREPOINT PORTAL SERVER
11	ABOUT TREND MICRO

Spring 2002
Trend Micro, Inc.

©2002 by Trend Micro, Inc.

All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the prior written consent of the publisher. InterScan, eManager, Trend VCS, Trend Micro Control Manager, ScanMail, ServerProtect, PortalProtect, OfficeScan, MacroTrap, ActiveUpdate, SoftMice, and SmartScan are trademarks or registered trademarks of Trend Micro, Inc. All other company and product names are trademarks or registered trademarks of their respective owners.

INTRODUCTION

Employees spend increasing amounts of time organizing, managing, and searching through information collected on enterprise information portals (EIP). Microsoft SharePoint Portal Server enables businesses to create corporate Web portals with powerful indexing and search functions, extensive document management features, and rich collaboration options. While the SharePoint Portal Server makes it easy for users to share information regardless of physical location, it also provides an environment where viruses and malicious programs such as Trojans and worms can replicate, spread and cause damage.

Trend Micro has recognized the need to provide security for the new platform. The first solution that Trend Micro has designed and developed for EIPs is Trend Micro PortalProtect, which specifically works with Microsoft SharePoint Portal Server. Trend Micro's PortalProtect is the first security solution integrated with Microsoft SharePoint Portal and built on proven enterprise-level technology for optimal reliability and interoperability. PortalProtect delivers effective centrally-managed virus protection and content security for Microsoft SharePoint Portal systems and their users.

HOW DOES TREND MICRO PORTALPROTECT WORK?

Using the Microsoft antivirus API, PortalProtect detects and cleans existing viruses as well as other malicious programs inside the Web Storage System. In addition, PortalProtect guards vulnerable entry points by scanning files replicated from other Microsoft SharePoint Portal Servers in real time. PortalProtect uses three types of scanning to ensure that SharePoint Portal environments are kept clean of viruses and other malicious code: real-time scans, manual scans (scan now), and scheduled scans.

Real-time Scan is a powerful feature that works in the background. Whenever a file is "checked in", "checked out", saved or retrieved, PortalProtect performs a scan for viruses or other malicious code on the file in real time.

Manual Scan (Scan Now) occurs when invoked by the user and completely scans all specified files in the Web Storage System. The length of the scan depends on the number of files and hardware resources.

Scheduled Scan automates routine scans on SharePoint Portal Servers, improves antivirus management efficiency, and gives administrators more control over antivirus policy.

The Real-time Monitor displays details about the scanned files, any viruses found, and the status of any currently running manual or real-time scan.

FACT:
Based on a September 2001 study by Computer Economics, each outbreak incident results in a cost of \$5K up to \$500K per corporation.

To offer more proactive protection, PortalProtect's file blocking capability can be used during a virus outbreak to temporarily block all files of a certain type. Based on true file types or file names, PortalProtect can proactively quarantine or delete specified files in the Web Storage System and those being introduced or "checked in" to the SharePoint Portal Server, making sure the Web Storage System is kept free of the specified file types. Since blocked files cannot enter your system, they do not need to be scanned and scanning performance remains optimal.

To make antivirus maintenance easier, PortalProtect utilizes Trend Micro ActiveUpdate which automatically searches for and downloads the latest virus pattern and scan engine update files. This powerful feature ensures that PortalProtect is using the latest technology and latest virus definitions. You can update on-demand or schedule PortalProtect to check Trend Micro's ActiveUpdate Server for new components at regular intervals.

PortalProtect also offers an intuitive Web-based management console, which gives administrators secure, convenient access to configuration, reports, logs, and customized notifications.

MICROSOFT SHAREPOINT PORTAL SERVER

Microsoft SharePoint Portal Server (SPS) is a server-based product that runs on Windows 2000 Server SP1 or later and is built on the same Web Storage System technology as Exchange 2000. SPS is designed for businesses to build portals for intranet applications such as knowledge management, document management and workflows. This section describes some of the features and technologies of SPS that are related to the PortalProtect security strategy.

SPS offers versatile indexing and search capabilities for content on SharePoint Portal Servers, Web servers, file servers, Exchange Public folders, and Notes databases, and the indexing is extensible to other databases. SPS's document management tools support document versioning, profiling, role-based security, publishing, and routing for review and approval. SPS also provides a workflow engine which allows users to build applications using any of the same tools used with Exchange 2000.

The Web Storage System is a storage platform for managing multiple types of unstructured information, such as pictures, Web pages, and documents, in one infrastructure. In addition to storing, accessing, and managing information, it provides a collaborative development platform for building and running applications. The Web Storage System provides the foundation for both Microsoft Exchange 2000 and the SharePoint Portal Server. It is utilized by SPS and Exchange 2000 for storing unstructured files and data.

The digital dashboard is a browser-based interface for corporate portals that integrates various company resources and provides single-click access to analytical and collaborative tools. Web-based information and services are delivered to a digital dashboard via Web Parts.

Web Parts are components for corporate portals that extract and present customized views of data to a desktop. Ready-made Web Parts from Microsoft and partners allow companies to plug applications and services into a digital dashboard; they can also be created and managed by a company's IT Department.

PKMCDO (Publishing and Knowledge Management Collaboration Data Objects) is the object model used to interact with SharePoint Portal Server. It includes CDO (Collaboration Data Objects) enhancements that manage documents and portals.

Microsoft Anti-Virus API: SharePoint Portal Server incorporates the antivirus API developed for Exchange Server 5.5 SP3 and 2000, which allowed antivirus solutions to scan attachments in the Exchange Server information store and selectively repair, mark as suspicious, or replace any attachment. The antivirus API architecture provides high-speed access to data in the information store for optimal performance and ensures that all files are scanned before a

client has access to them. Use of this, and other Microsoft technologies, helps to ensure a reliable solution that will not unduly impact the Microsoft application or environment.

PortalProtect Architecture

Trend Micro's PortalProtect cleans existing files inside the Microsoft™ SharePoint™ Portal Web Storage System using background scanning provided by the Microsoft antivirus API. In addition, PortalProtect scans all possible entry points with real-time scanning of all incoming and outgoing files (files being checked in and out). Figure 1 depicts how PortalProtect, the Antivirus API, and SharePoint Portal Server interact to provide a more secure portal environment.

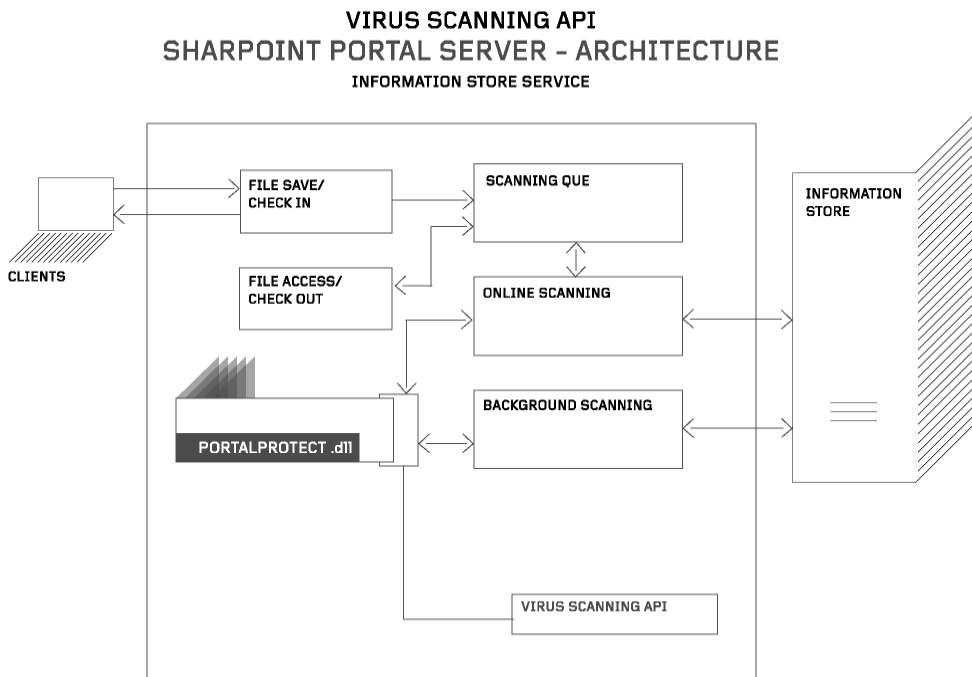


Figure 1:
PortalProtect Architecture

TREND MICRO PORTALPROTECT FOR MICROSOFT SHAREPOINT PORTAL

Trend Micro's PortalProtect is the first security solution integrated with Microsoft SharePoint Portal and built on proven enterprise security technology for optimal reliability and interoperability. The collaborative nature of enterprise portals increases the security risks from viruses. PortalProtect provides a centrally managed solution to effectively secure SharePoint Portal systems and their users.

PortalProtect is built upon Trend Micro's high-performance scan engine and the technology of ScanMail - the world's leading antivirus solution for Microsoft Exchange. PortalProtect integrates with Microsoft's latest Antivirus API and has adopted other Microsoft technologies to ensure a minimal effect on system performance.

PortalProtect is designed to shield enterprises from potential threats by scanning and cleaning, in real-time, any viruses entering or residing in SharePoint's Web Storage System. In addition, its file blocking capability can be used to enforce security policies on undesirable documents and to quickly block files identified as potential threats during a virus outbreak.

Enterprise customers are concerned with ease of management as well as the quality of protection offered by their security solutions. To enhance the manageability of PortalProtect, Trend Micro has developed an intuitive web-based management console that gives administrators secure, convenient access to configuration details, reports, logs and customized notifications. In addition, automated update mechanisms keep PortalProtect's scan technology and virus definitions current.

As a server-based solution, PortalProtect is designed for high scalability, and growing companies can easily meet their security needs by adding additional servers. Administrators can rest assured that PortalProtect will continue to provide security for the enterprise as the SharePoint Portal evolves.

Tight Integration

Regardless of the number or size of individual SharePoint Portal Servers, PortalProtect's tight integration ensures complete scalability, making it ideal for businesses of all sizes. PortalProtect uses the Microsoft Anti-Virus API v 2.0 for more effective protection. PortalProtect was developed to get maximum leverage from MS technologies including: SharePoint DOM (Document Object Model), digital dashboard, Web Parts, Web Storage System (same database technology as the Exchange Information System), CDO, PKMCDO, and the Windows NT/2000 Security Model.

High Reliability

In addition to incorporating Trend Micro's award-winning antivirus scan engine, PortalProtect is built on proven enterprise security technology to deliver optimal reliability and interoperability. PortalProtect includes the latest technology innovations to protect against recent mixed-threat viruses such as Nimda and CodeRed. Using "true file type" detection, PortalProtect is able to help enforce security policies and provide immediate added protection during virus outbreaks by blocking undesirable files.

Ease of Management

The Web-based management console gives administrators secure, convenient access regardless of physical location or platform. The Real-time Monitor and Server Status Console display current information and important events, such as the last virus found. The Real-time Monitor Web Part can be integrated into a digital dashboard to help administrators check PortalProtect status remotely.

ActiveUpdate automatically supplies PortalProtect Servers with the most current pattern files and scan engine updates. Integration with Windows 2000 installer components allows easy deployment across a Microsoft SharePoint Portal enterprise. PortalProtect Servers can collaborate to share pattern files and scan engine updates for intelligent use of corporate network bandwidth. Administrators can remotely or locally deploy PortalProtect to a single server or multiple servers simultaneously.

Automatic, customizable, real-time notifications allow administrators to identify sources of viruses or service abnormalities and deal with them quickly and effectively. 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 of infected documents and log files can be exported into CSV format.

NEW TECHNOLOGIES

In addition to common security technologies such as MacroTrap and ScriptTrap, Trend Micro has developed innovative management and other infrastructure technologies. In this release of PortalProtect, Trend Micro releases two technologies designed to deliver a formidable antivirus strategy.

IntelliScan

Most antivirus solutions today offer administrators two options in determining which files to scan for potential threats. Either all files are scanned (the safest approach), or only those files with certain extensions are scanned. But recent developments involving files being "disguised" through having their extensions changed, has made this later option almost useless.

IntelliScan is a new Trend Micro technology that identifies a files "true file type" regardless of the extension. Through IntelliScan, administrators can maintain a list of file types that they wish to have scanned, restoring the viability of this second option to help balance security needs with performance objectives.

ActiveAction

ActiveAction categorizes malicious code into categories such as viruses, Trojans, and joke programs. Administrators can, by category, configure specific primary and secondary responses. For example, they may wish to have Trojan horse and Joke programs "delete". Yet, for other categories they may prefer to attempt to "clean" the viruses code from the file first and then, if that fails, to have the file "quarantined" for later inspection.

SYSTEM REQUIREMENTS

You need the following to effectively run PortalProtect:

Hardware

Minimum:

- Intel Pentium III-compatible processor or higher
- 256MB of RAM
- 50MB of available disk space

Recommended:

- Intel Pentium III-compatible processor 1.0 GHz or higher
- Intel Pentium 4-compatible processor 1.40 GHz or higher
- 512MB of RAM
- 100MB of available disk space

Software

- Microsoft(TM) SharePoint(TM) Portal Server 2001 with SP1 or above, Microsoft hot fix Q318627
- Microsoft Windows 2000 Server or Advanced Server, with SP2 or above
- Microsoft Windows 2000 or above for remote installation
- Microsoft Internet Explorer 5.01 with SP2 or above (both Java and JavaScript must be enabled)

ABOUT TREND MICRO

Trend Micro provides centrally controlled server-based virus protection and content filtering products and services. By protecting information that flows through Internet gateways, email servers, and file servers, Trend Micro allows companies and service providers worldwide to stop viruses and other malicious code from a central point before they ever reach the desktop.

Trend Micro's corporate headquarters is located in Tokyo, Japan, with business units in North and South America, Europe, Asia, and Australia. Trend Micro's North American headquarters is located in Cupertino, CA. Trend Micro's products are sold directly and through a network of corporate, value-added resellers and service providers. Evaluation copies of all of Trend Micro's products may be downloaded from its award-winning Web site, <http://www.trendmicro.com/>.