

Microsoft White Paper



Trend Micro™ ServerProtect™ and Windows Server 2003



INTRODUCTION	3
WINDOWS SERVER 2003 – AN OVERVIEW	3
Improvements across the board	3
FEATURES AND BENEFITS	3
Security	3
Internet Information Services 6.0	5
Scalability	6
Reliability and Availability	6
Manageability	7
TREND MICRO SERVERPROTECT	9
FEATURES AND BENEFITS	10
Centralized Management and Reporting	10
Reliable and Efficient Virus Protection	10
Pattern matching	10
MacroTrap	10
Compressed files	11
OLE layer scan	11
IntelliScan	11
ActiveAction	11
Real-time scan and on-demand scan	11
Central deployment and updates	11
Scalability	11
24x7 Antivirus Support	11
Throughput Compared to Windows 2000	11
TREND MICRO ENTERPRISE PROTECTION STRATEGY	12
Outbreak Commander Scenario	13
CONCLUSION	18

“For great end-to-end antivirus coverage, with unique strengths in outbreak containment, you need look no further than Enterprise Protection Strategy.”

PC Magazine

Windows Server 2003 is the first Windows operating system to ship under the Trustworthy Computing initiative.

INTRODUCTION

Trend Micro continues its close collaboration with Microsoft Corporation by offering Trend Micro™ ServerProtect™ 5.56 on Windows Server 2003. ServerProtect is an integral part of the Trend Micro Enterprise Protection Strategy, a comprehensive approach that enables customers to minimize the impact of mixed threats to productivity and information assets.

ServerProtect works closely with core Microsoft technologies to protect enterprise-level networks supporting Windows Server 2003. It performs kernel-level scanning for viruses and malicious code via Microsoft APIs to minimize performance degradation, and uses a multi-threaded scan engine to enhance the speed of scanning files and to minimize the impact to the server.

The goal of the collaboration between Trend Micro and Microsoft is to provide comprehensive security software and services for Microsoft environments. This relationship sustains integration between Microsoft's operating system, database, and server products and Trend Micro solutions – whether in 32- or 64-bit environments.

Microsoft and Trend Micro recognize that for many enterprises that have installed Windows NT or Windows 2000, swift, cost-effective migration to Windows Server 2003 while maintaining server protection and performance is key to their long-term enterprise IT strategy.

In this white paper we discuss Windows Server 2003 and Trend Micro ServerProtect and explore how organizations can implement components of the Enterprise Protection Strategy to efficiently manage the entire outbreak lifecycle.

WINDOWS SERVER 2003 – AN OVERVIEW

Improvements across the board

The Microsoft® Windows® Server 2003 operating system represents a significant advancement over the Microsoft Windows 2000 family of operating systems. Windows Server 2003 is the fastest, most reliable, most secure Windows server operating system ever offered. It features overall enhancements in reliability, availability, and manageability, as well as scalability extending to 64 processors.

The Windows Server 2003 family builds on the strengths of Windows 2000 to provide a platform that is more productive, dependable, and connected than ever before. New and improved file, print, application, Web, and communication services provide a more robust, comprehensive platform for your mission-critical business resources. Integrated features such as the Active Directory® service and enterprise-class security services allow you to provide secure yet flexible access to all the resources your users need.

FEATURES AND BENEFITS

Security

The Trustworthy Computing initiative launched by Bill Gates in January 2002 is based on four pillars: security, privacy, reliability, and business integrity. Windows Server 2003 is the first Windows operating system to ship under the Trustworthy Computing initiative.

The security innovations in Windows Server 2003 offer customers a flexible security experience, providing both a more secure out-of-the-box foundation and extensive technologies to help customers build, deploy and manage more secure solutions. Microsoft has made engineering design changes, adjusted settings to help deliver security

by default, and delivered new features and technologies that enhance security for the Windows platform.

Secure by Design. Improved security of Windows Server 2003 reflects Microsoft's \$200 million investment in 2002 to reduce code vulnerabilities in its platform, modify the development process, and improve accountability at every level for security. Designed with a focus on improving security, Windows Server 2003 features a redesigned IIS, strong authentication protocols such as 802.1x and PEAP, and the common language runtime to create a safer computing environment.

- Internet Information Services (IIS) was redesigned in Windows Server 2003 to improve security for Web transactions. IIS 6.0 makes it possible to isolate an individual Web application into a self-contained Web service process, which prevents one application from disrupting the Web services or other Web applications on the server. IIS also provides health-monitoring capabilities to discover, recover, and prevent Web application failures. In IIS 6.0, third-party application code runs in isolated worker processes, which by default use the new lower-privileged Network Service logon account. Worker process isolation makes it possible to confine a Web site or application to its root directory through Access Control Lists (ACL).
- Improved network communication security in addition to host security. To improve the security of wireless communication, Windows Server 2003 supports strong authentication protocols such as 802.1x (WiFi) as well as Protected Extensible Authentication Protocol (PEAP). Internet Protocol Security (IPSec), a suite of cryptography-based protection services and security protocols, has been enhanced for stronger LAN data encryption.
- The common language runtime (CLR) software engine is a key element of Windows Server 2003 to improve reliability and help ensure a safer computing environment. CLR verifies that applications can run without error and checks security permissions to ensure that code only perform appropriate operations. CLR reduces the number of bugs and security holes caused by common programming mistakes, leaving fewer vulnerabilities for attackers to exploit.

Secure by Default. To secure Windows Server 2003 by default, the attack surface area has been reduced by creating stronger default policies (e.g., file system Access Control Lists (ACL)), redesigning IIS, and reducing the total number of services, the number of services running by default, and the number of services running as system.

- To reduce the default attack surface of Windows Server 2003, Microsoft disabled 19 services, and reduced several services to run under lower privileges. For example, in order to reduce the Web infrastructure attack surface, installing Windows Server 2003 does not install IIS 6.0 by default—administrators must explicitly select and install it. When a server is being upgraded to Windows Server 2003, IIS 6.0 will be disabled also. In addition, as IIS 6.0 is being installed, it is configured by default in a "locked down" state. After installation, IIS 6.0 accepts requests only for static files until configured to serve dynamic content, and all time-outs and settings are set to aggressive security defaults. IIS 6.0 can also be disabled using Windows Server 2003 group policies.
- Stronger default settings are used in ACLs, which define the criteria an operating system uses to protect network resources. For example, creating the new System Root ACL and setting it as the default means that users can no longer write files to the root of the system drive, which prevents certain spoofing attacks.

- Two additional user accounts were created to run services at lower privilege levels, which helps ensure that a vulnerability in a service cannot be exploited to take over the system. The new Network Service account is used, for example, to run DNS Client and all IIS Worker Processes. Telnet now runs using the new Local Service account.

Secure in Deployment. In addition to the secure architecture design and added security features in Windows Server 2003, Microsoft offers its customers tools, prescriptive guidance, training, and services to help them deploy a secure connected infrastructure.

- Software Restriction Policy (SRP) is a new feature in Windows Server 2003 and Windows XP that gives administrators a policy-driven mechanism to identify software running in their domain and control its ability to execute. Using a software restriction policy, an administrator can confine execution to a set of trusted applications, thus preventing the operation of unwanted applications, such as viruses or software known to cause conflicts. A software restriction policy also could be used to allow only administrators to run certain programs on shared machines.
- Security Configuration Editor (SCE) is designed to help businesses secure Windows systems operating in various roles and deployment scenarios, such as a Web server that is connected both to the Internet and to a secure internal network. The goal of SCE is to help customers maximize the security of such systems without sacrificing their required functionality. For example, services (e.g. Fax) that may not be required for file server role can be disabled. Administrators can use the Security Configuration Wizard in SCE to construct security policies for their different types of servers, and perform Lockdown Testing to verify that systems function as expected. This tool will be released in the later part of 2003.
- Microsoft Audit Collection Services (MACS) is a tool to monitor and audit systems. MACS collects security events in a compressed, signed, encrypted manner and loads the events into a SQL database for analysis. This tool works with Windows XP, Windows 2000 Server, and Windows Server 2003, and uses existing security technologies to protect against tampering and disclosure during network transit. It enables the separation of auditor and administrator roles to ensure that administrators cannot make changes to audit information. This tool will be released in the later part of 2003.

Internet Information Services 6.0

One of the key security enhancements in Windows Server 2003 is the complete redesign of Internet Information Services (IIS). Internet Information Services 6.0 is a powerful Web server available in all versions of Windows Server 2003 that provides a highly reliable, manageable, scalable, and secure Web application infrastructure.

IIS 6.0 makes it possible for organizations of all sizes to quickly and easily deploy powerful Web sites and applications, and provides a high-performance platform for all applications. Applications built with Microsoft .NET frameworks are faster and more reliable on IIS 6.0 due to the integration of the .NET frameworks into the IIS 6.0 process model. IIS 6.0 features a new fault-tolerant process architecture with health monitoring that runs all application code in an isolated environment for maximum reliability and availability.

Web server administration is simplified using an XML-based configuration file that can be modified without having to stop and restart the server. IIS 6.0 enhancements such as kernel-mode caching and "Web gardens" dramatically increase the product's scalability and performance compared to previous versions of IIS. In

Windows Server 2003 offers support for 64-bit architecture with Enterprise and Datacenter Editions.

terms of security, IIS 6.0 is not installed by default with Windows Server 2003 and is fully “locked down” when first installed to reduce attack surface area. The benefits of choosing IIS 6.0 include less planned and unplanned system downtime, increased Web site and application availability, lower system administration costs, server consolidation (reduced staffing, hardware, and site management costs), and a significant increase in Web infrastructure security.

Scalability

Windows Server 2003 takes the scalability gains on Windows 2000 Server Family to a new height. Windows Server 2003 is designed for both scale-up and scale-out scenarios. Scale-up scenarios are enabled by symmetric multiprocessing (SMP) and CC-NUMA (Cache Coherent Non-Uniform Memory Access) optimizations, and scale-out by the various types of clustering provided by Microsoft.

Windows Server 2003 scales from single processor solutions all the way up to 64 processors in a single partition and offers 8-node clustering with Enterprise and Datacenter Editions. In comparison, Windows 2000 Server scaled to 32 processors and offered up to 4-node clustering.

Internal tests indicate that, compared to Windows 2000 Server, Windows Server 2003 delivers up to 140 percent better performance in the file system and significantly better performance in various other features, including Microsoft Active Directory service, Web server, Terminal Server components, and networking services. Key scalability enhancements include:

- **64-Bit Support.** Windows Server 2003 offers support for 64-bit architecture with Enterprise and Datacenter Editions. With 64-bit architecture, Windows offers scalability up to 64 processors and 512 GB of RAM. Customers can get even more performance and scalability in high-end database and LOB (line of business) application scenarios that demand the utmost for memory-intensive or computational-intensive tasks.
- **Support for Intel Hyper-Threading.** Intel Hyper-Threading Technology (HT) allows a single physical processor to execute multiple threads (instruction streams) simultaneously, potentially providing greater throughput and improved performance. In general, multithreaded Windows applications perform better when running unmodified on an HT processor than they do on a similarly equipped single-threaded processor. Windows Server 2003 32-bit platforms provide HT support both on architectural and licensing fronts.
- **NUMA Optimization.** Windows Server 2003 provides enhanced NUMA (Non-Uniform Memory Access) support. Most Windows applications will perform optimally without modification on NUMA systems running Windows Server 2003 due to the automated NUMA features in the operating system. NUMA support is offered only on 32-bit and 64-bit Enterprise and Datacenter Editions.
- **Hot Add Memory.** This new feature allows ranges of memory to be added to a compatible computer and made available to the operating system and applications as a part of the normal memory pool. This does not require rebooting the computer or other downtime. Hot Add Memory is offered only on 32-bit versions of Enterprise and Datacenter Editions.

Reliability and Availability

Reliability and availability are woven into every aspect of Windows Server 2003 design to provide better customer experience. Key highlights include:

The addition of 8-node clustering offers increased deployment flexibility, particularly for geographically dispersed cluster configurations.

- **8-Node Clustering.** Windows Server 2003 supports 8-node clustering with 32-bit and 64-bit Enterprise and Datacenter Editions. This is an increase from 2- and 4-node support in Windows 2000 Advanced and Datacenter Servers, respectively. By increasing the number of nodes in a server cluster, an administrator has many more options for deploying applications and providing failover policies that match business expectations and risks. The addition of 8-node clustering offers increased deployment flexibility, particularly for geographically dispersed cluster configurations.
- **Majority Node Set.** Windows Server 2003 provides the traditional cluster quorum mechanism, as well as a new quorum resource called "Majority Node Set." This quorum resource allows server clusters to be built without using a shared disk as the quorum device. Using this new quorum mechanism, additional cluster topologies such as server clusters with no shared disks can be built. Majority Node Set also makes it easier to build and configure multi-site, geographically dispersed clusters.
- **Network Load Balancing Manager.** This new utility in Windows Server 2003 provides a single point of configuration and management for NLB clusters. NLB Manager can be used to create new NLB clusters and automatically propagate cluster parameters and port rules to all hosts in the cluster, add and remove hosts to and from NLB clusters, automatically add Virtual IP (VIP) addresses to TCP/IP, manage existing clusters by connecting to them or by loading their host information to a file and saving this information for later use, configure NLB to load balance multiple Web sites or applications on the same NLB cluster, and diagnose improperly configured clusters.
- **Datacenter High Availability Program.** The Datacenter Program has been expanded to meet the growing customer demand for higher availability on Windows. The new Datacenter High Availability Program strengthens the support and services model, expands the range of support providers, and merges the Joint Support Queue (JSQ) with the new Microsoft High Availability Resolution Queue (HARO). The improvements to the support and services model enable vendors to act in a unified, consistent way. This new model ensures our mutual customers they can achieve the highest levels of reliability and availability from the Datacenter Server platform. In addition, the Datacenter High Availability Support Program has added change management and configuration auditing services as required practices to participate in the program.

Manageability

Management capabilities delivered with Windows Server 2003 are designed to simplify and automate the management of Windows environments while providing the flexibility and reliability necessary to meet the business needs of customers. Windows Server 2003 includes new and enhanced management capabilities to address the challenges faced by customers and improve the manageability of Windows Server environments. Key highlights include:

- **Active Directory Enhancements.** Active Directory in Windows Server 2003 provides customers increased flexibility and manageability. Examples of the enhancements include secure credential and certificate management to provide a consistent single sign-on experience; health monitoring visibility to easily monitor trusts and replication activity; improved interfaces (e.g., multi-select and bulk-edit users, frequently save used searches, Resultant Set of Policy (RSOP), new setup wizards and DNS "self-diagnostics"); domain rename to allow customers to easily rename one or more already deployed domains and create a different domain-tree structure; design flexibility via Cross-Forest Trust, enabling autonomy with interoperable authentication and share files and

other resources across forests; schema enhancements to easily redefine attributes or class definitions and deactivate unused or no longer needed elements.

- **Policy Based Management.** Policy-based management provides fine-grained control over the definition and enforcement of IT policies. Policy-based management enables 'one-to-many' management, making it almost as easy to manage very large distributed systems environments as to manage a single system or user, once the policies have been defined. Windows Server 2003 unleashes the power of policy-based management via improved Group Policy infrastructure, new and vastly improved Group Policy management capabilities, and broad support for policy-based management across server components.
- **Automated Deployment.** Windows Server 2003 includes new and enhanced capabilities to automate the deployment and redeployment of the operating system and applications. Remote Installation Services (RIS) enables fully automated script-based or image-based deployments to servers and desktops. In conjunction with Windows PE, the new Windows pre-installation operating system environment, RIS enables complete automation of highly customized deployments. The new Automated Deployment Services (ADS) includes a new set of imaging tools developed by Microsoft and a secure, remote-able infrastructure for rapidly deploying and re-deploying servers in high-bandwidth data center environments. In addition, ADS offers a secure, reliable script execution framework that lets administrators perform script-based administration on 1,000 servers as easily as they once did on a single server.
- **Effective User Service Management.** IntelliMirror[®] – the ability to provide users with consistent access to their applications, roaming user profiles, and user data, from any managed computer – even when they are disconnected from the network, is enabled by Windows Server 2003 technologies such as Active Directory, Group Policy, Software Installation, Windows Installer, Folder Redirection, Offline Folders, and Roaming User Profiles. This also enables centralized backup of user data and configuration files by the IT organization. The volume shadow copy capabilities enable automated point-in-time backups of user data and provide self-service capabilities to allow users to find and restore lost or corrupted files. Together, these capabilities result in high levels of user productivity, satisfaction, and data safety.
- **Enhanced Security Management.** Windows Server 2003 provides powerful capabilities to establish and manage the security of your Windows environment. The ability to restrict and delegate rights for specific administration roles, software restriction policy enforcement, strong password requirement enforcement, and the ability to deliver highly managed user environments minimizes the risk of unintentional or deliberate security breaches. Also included is Software Update Services (SUS), a solution that enables automated download of security & critical operating system updates and gives administrators control over the testing, staging, distribution, and application of these updates within their organizations.
- **Scalable Operations Management.** Remote administration is enabled via Terminal Server, Windows Script Host and Windows Management Instrumentation (WMI), the management infrastructure that provides access to over 10,000 system objects in Windows Server 2003 via application, scripting, and command line interfaces. WMI allows fine-grained discovery, monitoring, control, and reporting of system and application settings and state. Windows Server 2003 also includes built-in performance monitoring, logging, tracing, and system recovery capabilities to enable quick troubleshooting and resolution of abnormal operating conditions.

With the Microsoft Services for UNIX 3.0 product (a separately licensed add-on), Windows Server 2003 delivers a complete UNIX environment on Windows and allows IT organizations to leverage their investments in UNIX scripts and expertise to do unified management of Windows and UNIX environments.

- **Windows System Resource Manager (WSRM).** WSRM enhances application availability and quality of service by providing control over application CPU and memory utilization, making it easier to run mixed application workloads on a single server. You can use WSRM to manage multiple applications on a single computer, users on a computer on which Terminal Services are installed, IIS app pools, or virtual machines. Managing resources with WSRM improves system performance and reduces the chance that applications, services, or processes will interfere with the rest of the system. This aligning of IT resources with business priorities creates a more consistent and predictable experience for users of applications and services running on the computer. WSRM's accounting tracks resource usage, which results in improved understanding of application resource utilization; this accounting data can serve as the basis for charge backs and capacity planning. WSRM is offered on 32-bit and 64-bit versions of Windows Server 2003, Enterprise and Datacenter Editions.

TREND MICRO SERVERPROTECT

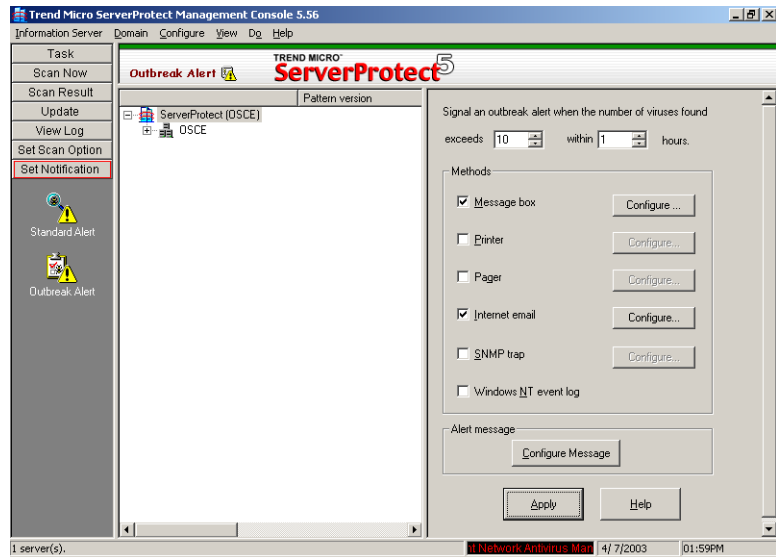
“Trend Micro continues to prove its innovation through developing robust enterprise level antivirus solutions.”

A file server can be a vulnerable, centralized point of information exchange. Even within the network, users without adequate protection can inadvertently upload infected files, which can then spread to other users who access them. Large organizations may need to consistently monitor, configure, and maintain hundreds or thousands of individual server machines with minimal time and effort. Within the enterprise, the ideal antivirus program for file servers needs to provide centralized management capabilities to simplify the administrator's job, including the ability to automatically deploy software and virus pattern file updates to detect the latest viruses, and the ability to scale from a simple multi-system network to a large distributed network.

ServerProtect delivers industry-certified virus protection, scanning and detection as well as damage cleanup services to remove malicious code and repair any resulting system injuries. Administrators can use a single Web-based management console to centrally enforce, administer, and update the antivirus program on every server throughout an organization.

ServerProtect employs a three-tier architecture: the Management Console, the Information Server, and the Normal Server. A normal server can be any server on the network on which ServerProtect is installed, for example, a file server or FTP server. The Management Console is used to configure dedicated Information Servers, which in turn control the Normal Servers.

Server antivirus history can be displayed in a central log file, which can be exported to other applications for further analysis. ServerProtect notifies predefined recipients of virus outbreak and program events. The figure below displays the ServerProtect Outbreak Alert notification setup screen:



Administrators can send notifications in multiple ways - via message box, pager, printer, Internet email, SNMP trap, or Windows event log.

ServerProtect can be configured to download virus pattern files and scan engine updates automatically and then distribute them to designated servers. It uses an incremental update mechanism so that the designated servers only download the new virus pattern files that have been added since the last version, which saves download time and preserves network bandwidth.

FEATURES AND BENEFITS

Centralized Management and Reporting

ServerProtect provides centralized management of multiple servers in one site from a Windows-based console. The console enables administrators to deploy programs and updates to servers simultaneously and monitor server status in real time. Administrators can also use ServerProtect in conjunction with Trend Micro Control Manager™, a centralized management console that integrates multiple Trend Micro antivirus and content security products and services in a single-console view.

Reliable and Efficient Virus Protection

ServerProtect combines rule-based and pattern-recognition technologies for efficient virus detection. The scan engine has been certified by both the International Computer Security Association (ICSA) and Virus Bulletin (VB) for reliable scanning.

Pattern matching

ServerProtect draws upon an extensive database of virus patterns to identify known virus signatures using a process called pattern matching. Key areas of suspect files are examined for telltale signs of virus code and compared against thousands of virus signatures that Trend Micro has on record.

MacroTrap

ServerProtect includes MacroTrap™ technology to guard against macro viruses in Microsoft Office files and templates. Since Macro viruses are harbored in files that are commonly passed around via email, they are easily spread. Macro virus code is typically contained as a part of the invisible template, for example, *.dot in Microsoft Word, that travels with the document. MacroTrap performs a rule-based examination of all Macro code that is saved in association with a document.

Compressed files

Compressed files are sometimes used to "smuggle" viruses into protected networks or computers. The Trend Micro scan engine can scan files inside compressed archives. It can even scan compressed files that are composed of other compressed files - up to a maximum of five compression layers.

OLE layer scan

Microsoft Object Linking and Embedding (OLE) allows embedding of Microsoft Office files within themselves, for example a Microsoft Word document inside an Excel spreadsheet, which in turn is embedded in a PowerPoint presentation. While OLE offers a large number of benefits, it can lead to infection. To address this issue, Trend Micro added a new scan feature, OLE Layer Scan.

IntelliScan

IntelliScan is a new method of identifying which files to scan that is both more secure and efficient than the standard "Scan all files" option. For executable files, for example, .zip, .exe, the true file type is determined by the file content. In the event that a file is not executable, for example, .txt, IntelliScan will use the file header to verify the true file type. One of the benefits of IntelliScan is that scan time is significantly less than that of other file scans. This is because only the files with a greater risk of being infected are scanned.

ActiveAction

ActiveAction is a set of pre-configured scan actions that can be performed based on different types of viruses and malware.

Real-time scan and on-demand scan

ServerProtect features two powerful scan functions: Real-time Scan and Scan Now. Real-time Scan runs continuously on a server. All "open/close" file events on the server are monitored and infected files are prevented from being copied to or from the server. Scan Now is a manual virus scan and can be used to check a machine that is suspected of being exposed to a virus or about which immediate information is required.

Central deployment and updates

A successful antivirus policy depends on the deployment of program files, scan engines, and pattern files that can deal with the latest virus threats. ServerProtect enables administrators to develop a deployment scheme based on their specific enterprise network topology. Administrators can also install ServerProtect software to new servers via the Management Console. This efficient approach simplifies the maintenance of Trend Micro software and reduces the total cost of a network's antivirus security.

Scalability

If there are multiple ServerProtect Information Servers installed on a network, administrators can use Trend Micro Control Manager to collectively manage all servers. In keeping with other Trend Micro enterprise products, ServerProtect is designed for complete integration with Trend Micro Control Manager. In addition, other Trend Micro products, for example, OfficeScan™ and ScanMail™ for Microsoft Exchange can be jointly managed via Trend Micro Control Manager.

24x7 Antivirus Support

TrendLabs, Trend Micro's global antivirus research and support center, backs Trend Micro products with timely, high-quality service. A team of engineers works around the clock to monitor virus activity, develop information on new threats, and deliver effective solutions.

Throughput Compared to Windows 2000

Enterprises upgrading to Windows Server 2003 will not have to sacrifice performance in order to ensure platform security.

ServerProtect maintains its outstanding Windows 2000 scanning performance on Windows Server 2003, providing consistent results across mixed data types, including compressed and archived files.

Trend Micro conducted ServerProtect performance tests using the following data profiles:

- 1. Document files**
Microsoft Word and Excel files (861 MB total)
- 2. Document and graphics files**
The document files described above and JPEG files (965 MB total)
- 3. Document, graphics, and compressed files**
The document and graphic files described above and ZIP files (1212 MB total)

The following table lists the results:

Platform	Profile 1	Profile 2	Profile 3
Windows 2000 SP3	6.89 Mbps	7.48 Mbps	8.85 Mbps
Windows Server 2003 Enterprise Edition, build 3790	6.83 Mbps	7.31 Mbps	8.42 Mbps

TREND MICRO ENTERPRISE PROTECTION STRATEGY

Today's enterprises are highly dependent on global, distributed computing environments to streamline operations, increase efficiency and reduce costs. Organizations are also burdened by the proliferation of mixed-threat attacks that can target multiple points on the network and leave unseen trails of damage and the potential for re-infection. For the IT security administrator, dealing with viruses and other malware has moved beyond detection to encompass minimizing the damage and costs of an outbreak through a systematic strategy for prevention, detection, and cleanup.

ServerProtect is a key component of the Trend Micro Enterprise Protection Strategy, an industry-unique approach to antivirus and content security that addresses mixed-threat attacks through coordinated delivery of products, services and expertise throughout the outbreak lifecycle. The outbreak lifecycle, the process that customers undergo in response to new security threats or outbreaks, consists of three primary phases – outbreak prevention, threat-based scanning, and assessment and restoration.

When an outbreak occurs, Outbreak Prevention Services enable IT security administrators to receive policy recommendations from Trend Micro. These policy recommendations are designed to thwart new viruses and contain the spread of virus attacks until a fully tested pattern file is available.

The Outbreak Prevention Service, a subscription-based service implemented through Trend Micro Control Manager, also provides administrators with information on new attacks as soon as they are identified. It sends a notice to every client machine, enabling the Outbreak Prevention mode. Systems in Outbreak Prevention mode can then be configured to block shared folders and specified ports, and/or to deny writing certain file types to specified directories, further containing the threat.

Once a new pattern file has been issued to detect the specific threat, ServerProtect's centralized architecture enables the rapid, automated deployment of the latest protection to all installed servers, ensuring consistency and speed at the threat-based scanning phase. Trend Micro's response times to new threats are also backed by an optional

Virus Response Service Level Agreement, offering a penalty-backed two-hour response guarantee.

Today the process of cleaning the network of virus remnants is incredibly time-consuming and expensive, because most networks rely on a manual cleanup and restoration process. The Trend Micro Damage Cleanup Services component of the Enterprise Protection Strategy provides cleanup and restoration policy templates targeting damaged registries, infected files in memory, and Trojan virus remnants, which, left undetected, could potentially re-infect the network.

The services described above can be centrally managed through the Outbreak Commander console found within Trend Micro Control Manager. Outbreak Commander acts as a central command center for outbreak management-related tasks within a single interface, including the ability to automatically download and deploy policies set forth by services such as Outbreak Prevention Services.

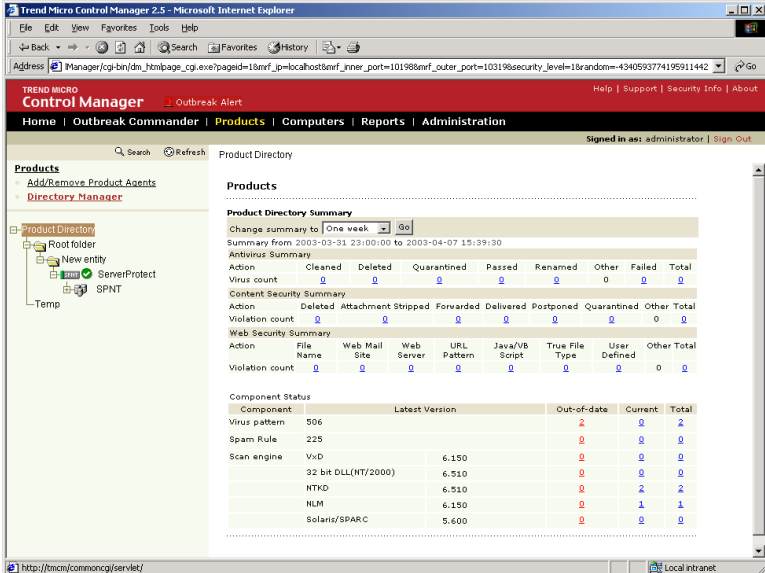
Outbreak Commander Scenario

The following procedure presents a visual example of using the Outbreak Commander to configure an outbreak prevention policy for a remote installation of ServerProtect on Windows Server 2003.

Note. This example is a brief overview and not meant to provide technical instructions for live system configuration. For technical installation and configuration details for Trend Micro Control Manager and ServerProtect, please see the appropriate product-specific documentation.

1. Ensure that Trend Micro Control Manager is configured to manage ServerProtect.

Click the **Product** link in the top menu bar. In the left frame of the Product page, expand the management hierarchy tree to display the ServerProtect node. The green circle-white checkmark icon indicates that the Trend Micro Control Manager is communicating with the ServerProtect installation properly.



The screenshot shows the Trend Micro Control Manager 2.5 interface in Microsoft Internet Explorer. The browser address bar shows a URL for the management console. The interface includes a top navigation bar with links for Home, Outbreak Commander, Products, Computers, Reports, and Administration. A search bar and refresh button are also present. The main content area is divided into a left-hand navigation pane and a right-hand main pane. The left pane shows a tree view under 'Product Directory' with 'ServerProtect' selected and marked with a green checkmark. The right pane displays several summary tables:

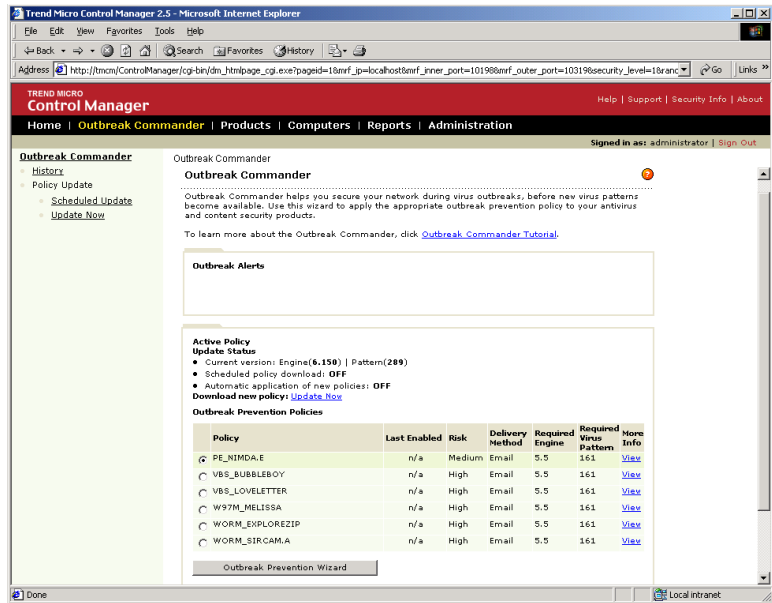
- Product Directory Summary:** A table with columns for Action, Cleaned, Deleted, Quarantined, Passed, Renamed, Other, Failed, and Total. It shows a virus count of 0.
- Content Security Summary:** A table with columns for Action, Deleted, Attachment Stripped, Forwarded, Delivered, Postponed, Quarantined, Other, and Total. It shows a violation count of 0.
- Web Security Summary:** A table with columns for Action, File Name, Web Mail Site, Web Server, URL Pattern, Java/VB Script, True File Type, User Defined, and Other Total. It shows a violation count of 0.
- Component Status:** A table listing various components and their status.

Component	Latest Version	Out-of-date	Current	Total
Virus pattern	506	2	0	2
Spam Rule	229	0	0	0
Scan engine	VxD	6.150	0	0
	32 bit DLL(NIT/2000)	6.510	0	0
	NTKD	6.510	2	2
	NLM	6.150	1	1
	Solans/SPARC	5.600	0	0

2. Start the Outbreak Commander.

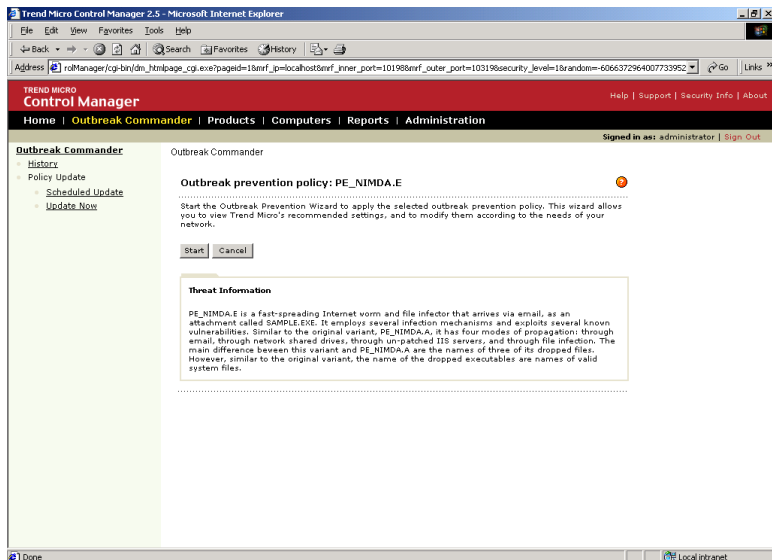
Click the **Outbreak Commander** link in the top menu bar. The Outbreak Commander page displays a list of available policies. If the policy you need is not displayed, click the **Update Now** link to

download new policies. Select the policy you want to configure and click the **Outbreak Prevention Wizard** button.



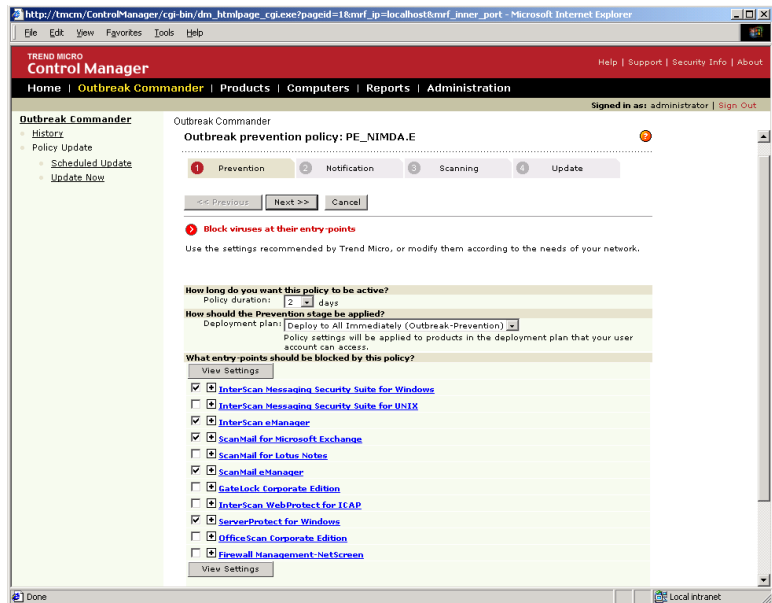
3. Review threat information.

The Outbreak Commander displays threat information about the subject of your prevention policy. Review the information and click the **Start** button to begin configuration.



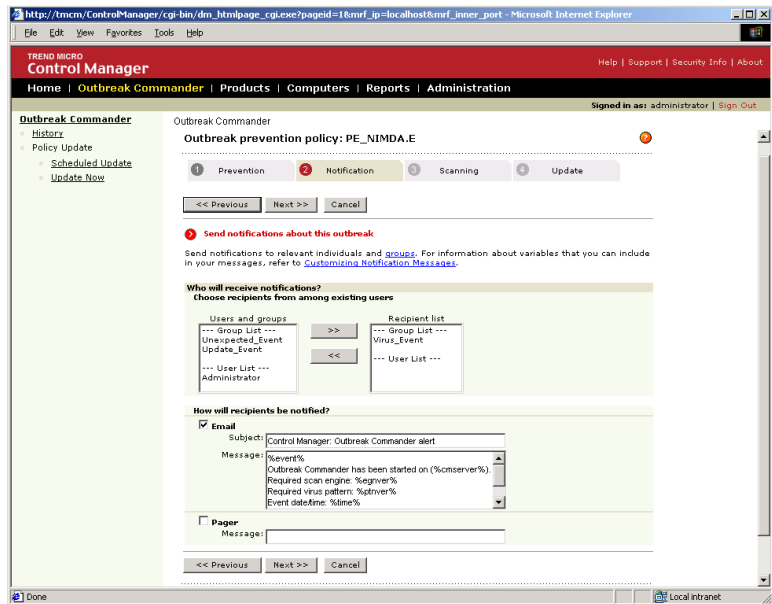
4. Configure prevention details.

The Prevention page allows you to specify the number of days to keep the policy active, the Prevention stage (when the policy should be deployed), and the entry points this policy should block. Configure the details and select the entry points, including **ServerProtect for Windows**, as required. Click the **Next** button to continue.



5. Configure Notification details.

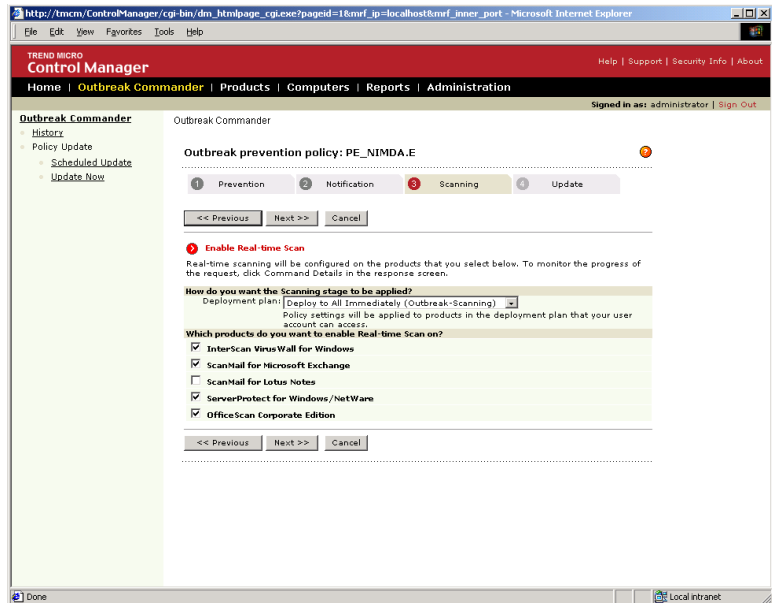
The Notification page allows you to send outbreak-prevention status information to pre-configured user and/or group recipients via email address or pager. Select the recipients and configure message details, then click the **Next** button to continue.



6. Configure Scanning details.

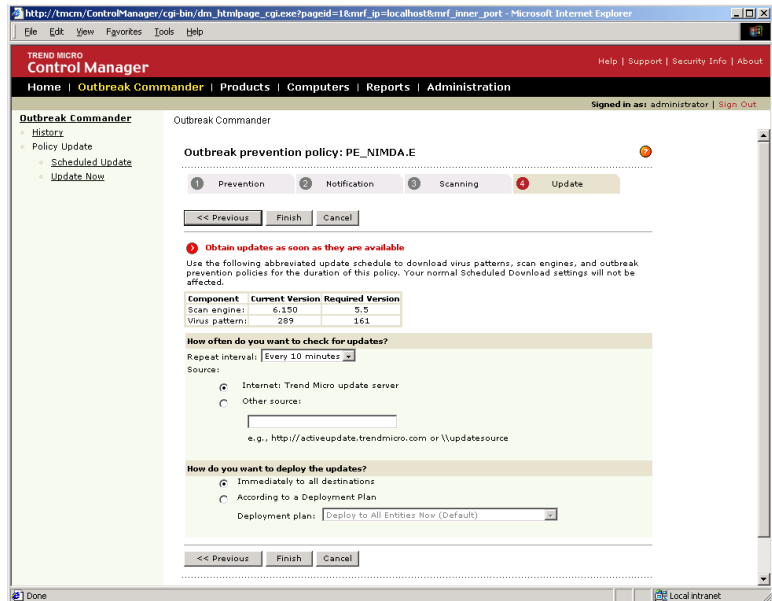
The Scanning page allows you specify the deployment plan and products for real-time scanning. Select the deployment plan and

product, including **ServerProtect for Windows**, as required, then click the **Next** button to continue.



7. Configure Update details.

On the Update page you can set a schedule for downloading virus patterns, scan engines, and outbreak prevention policies for the duration of the current policy. Specify how often to check for updates and how to deploy them, then click the **Finish** button to complete the process.



8. Configure Notification details.

The final page displays details about the configured policy. From here you can view the status of the policy (including virus activity history), view and modify policy details, stop the policy, among other operations. To return to this page in the future, click the **View** link in the More Info column of the Outbreak Prevention Policies table on the Outbreak Commander main page, as displayed in step 2 of this procedure.

The screenshot shows the Trend Micro Control Manager interface in a Microsoft Internet Explorer browser window. The page title is "Outbreak Commander" and the user is signed in as "administrator". The main content area displays the "Active Policy" section, which includes a table of active policies and an "Update Status" section.

Policy	Last Enabled	Risk	Delivery Method	Required Engine	Required Virus Pattern	More Info
PE_NIMDA.E	04/07/2003 01:26:53 PM	Medium	Email	5.5	361	View

Update Status

- Current version: Engine(6.150) | Pattern(289)
- Scheduled policy download: ON
- Automatic application of new policies: OFF
- Download new policy: [Update Now](#)

Scan Products

- Use the updated scan engine and/or virus pattern to scan your network.
- [Scan Now](#)

CONCLUSION

The Trend Micro Enterprise Protection Strategy helps minimize the impact of threats to the productivity and information assets of enterprises upgrading to Windows Server 2003. By preventing the spread of attacks, quickly deploying scanning solutions, and automating damage assessment and restoration processes, enterprises will maintain both platform security and system performance while managing the needs of long-term security strategies.

Trend Micro ServerProtect delivers innovative real-time virus protection for Microsoft file and application servers. Featuring a three-tier architecture, ServerProtect can be deployed and managed through a centralized, Web-based management console, and can scale from a simple multi-system network to a globally dispersed organization.

Through Trend Micro Control Manager, IT security administrators can consolidate ServerProtect with other Trend Micro solutions across the network and deliver policies for outbreak prevention along with the latest scan engines and virus pattern files to quickly and consistently minimize the impact of new threats. Within ServerProtect, administrators can minimize damage via port-blocking and deny-write and shared folder blocking capabilities; they can also deploy cleanup templates through Trend Micro Damage Cleanup Services to remove remnants of an attack from systems during the restoration phase.

ServerProtect enables not only the technology, but also the necessary strategy and services to effectively protect an enterprise relying on Windows Server 2003 for superior operational performance.

Microsoft, Windows, Windows NT, BackOffice, SQL Server, Windows 2000 and Windows Server 2003 are either registered trademarks of Microsoft Corporation in the United States and/or other countries. All other trademarks are held by their respective companies.

Trend Micro, ServerProtect, OfficeScan, ScanMail, TrendLabs and the t-ball logo are trademarks or registered trademarks of Trend Micro Incorporated. All other company or product names may be trademarks or registered trademarks of their respective owners.

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. Microsoft makes no warranties, express or implied, in this summary.

© 2003 Microsoft Corporation. All rights reserved.

Microsoft[®]