

Trend Micro™ Outbreak Prevention Services

Prevent and Contain Outbreaks with Attack-Specific Policies

PROBLEM

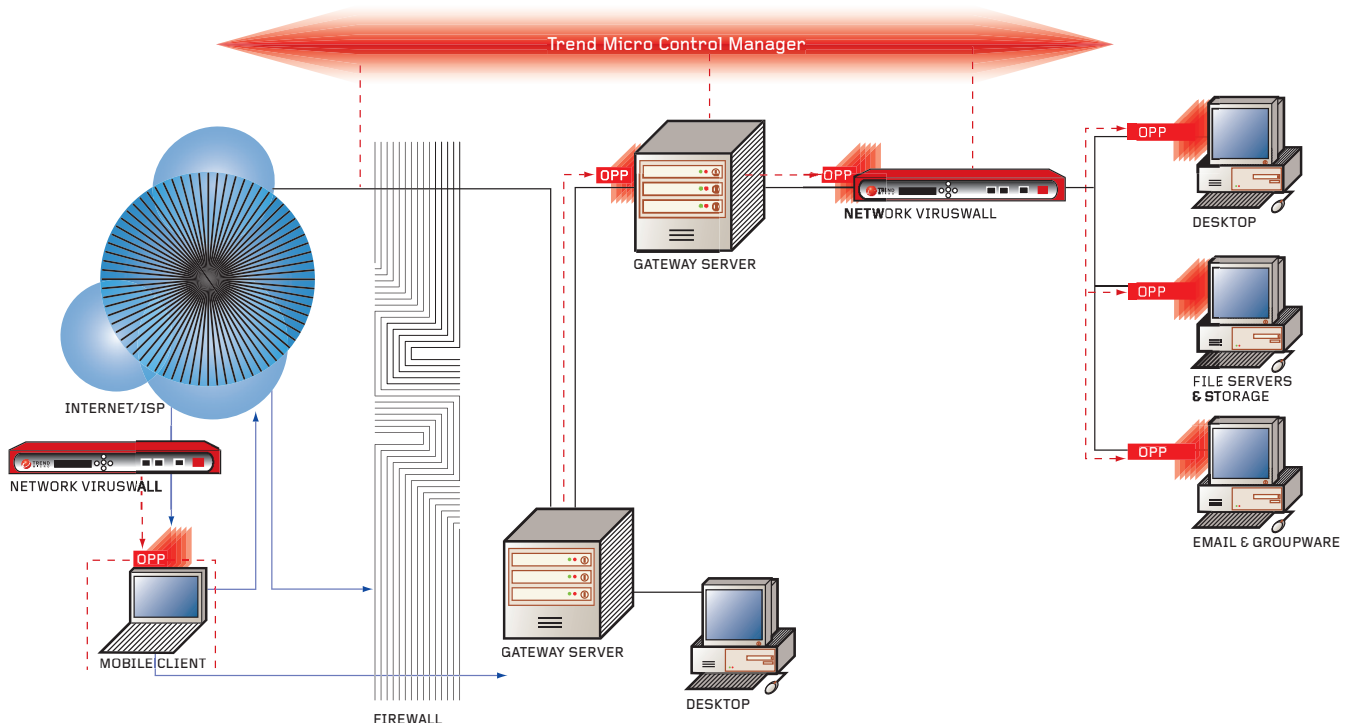
Most antivirus products are designed to respond to viruses only after infection. This reactive approach leaves organizations vulnerable to attack while waiting for pattern files to be deployed. Without reliable information about the nature of a new threat, how can IT managers contain outbreaks or even prevent them from happening? Some take drastic measures and shut down entire networks or block ports at the firewall. Others struggle to manage multiple security products from various points on the network. Decentralized management makes these networks easier to attack than those whose defenses are coordinated network-wide. Organizations need to adopt a proactive strategy to prevent or contain outbreaks during the vulnerable time between virus discovery and pattern file availability.

SOLUTION

Trend Micro™ Outbreak Prevention Services is a core component of Trend Micro Enterprise Protection Strategy (EPS) and operates in conjunction with other EPS products. Outbreak Prevention Services delivers threat-specific outbreak prevention policies from TrendLabs™ — Trend Micro's global network of over 300 security experts and engineers. Outbreak prevention policies (OPPs) are designed to give IT managers early warning of threats to help prevent or contain outbreaks before pattern files are deployed. Outbreak Prevention Services equips IT managers with a proactive defense that can block any combination of virus spreading mechanisms to prevent infection and network congestion. During outbreaks it prevents infection from spreading and can automatically activate Trend Micro™ Damage Cleanup Services to clean up virus remnants and keep viruses from propagating at unsuspected network entry points. Centrally managed from Trend Micro Control Manager™, outbreak prevention policies can be manually or automatically deployed to help ensure consistent security administration across the network.

KEY BENEFITS

- Outbreak prevention policies from TrendLabs provide early warning of specific threats to help IT managers prevent or contain outbreaks
- Outbreak prevention policies can be automatically deployed based upon virus risk profiles (high- and medium-risk alert) to help customers prioritize protection
- Centralized outbreak management accelerates the consistent deployment of outbreak prevention policies network-wide
- Blocks any combination of virus spreading mechanisms to prevent or contain infection and help prevent network traffic jams
- Can be configured to activate Trend Micro Damage Cleanup Services during outbreaks to clean up virus remnants and keep viruses from propagating at unsuspected network entry points



Blocks Virus-Spreading Mechanisms to Prevent Attacks: Outbreak Prevention Policies (OPPs) are developed by TCMC to block any combination of virus-spreading mechanisms including file extensions, executables, email attachments, IP addresses, ports, instant message channels, and file transfer protocols to prevent or contain viruses at both application and network layers.

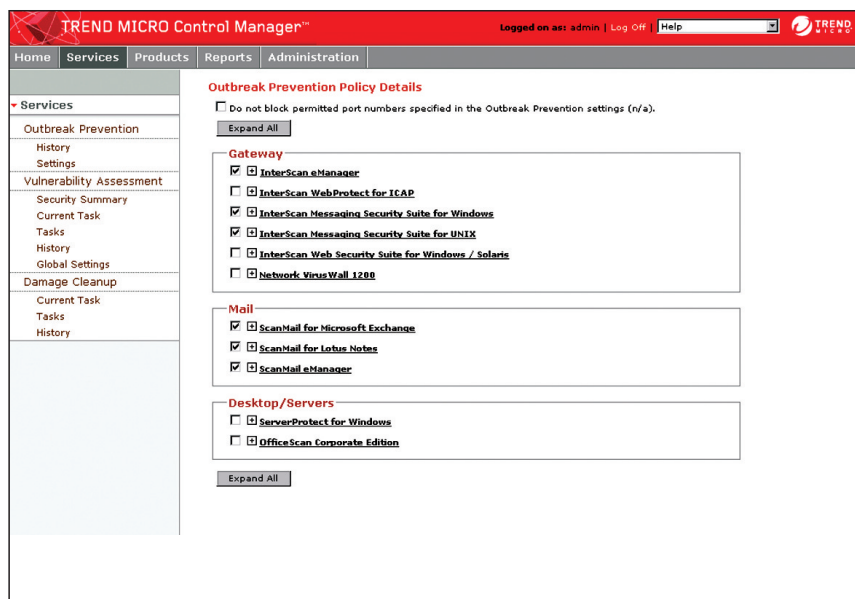
Trend Micro™ Outbreak Prevention Services

CENTRALIZED OUTBREAK MANAGEMENT AND COORDINATION

- Outbreak Prevention Services is centrally managed from Trend Micro Control Manager enabling consistent deployment of outbreak prevention policies network-wide
- Prior to the release of a virus pattern file or network virus signature, threat-specific outbreak prevention policies from TrendLabs can be automatically or manually deployed to specific points across the network
- Outbreak Prevention Services can be configured to activate Damage Cleanup Services during outbreaks to remove virus remnants and keep viruses from propagating at unsuspected network entry points

OUTBREAK PREVENTION AND VIRUS RISK PROFILING

- Outbreak prevention policies can block traffic from specific ports, protocols, and ranges of IP addresses
- Outbreak prevention policies can block specific instant message (IM) channels and files transferred by FTP, HTTP, and Microsoft Windows network file sharing
- Outbreak prevention policies can block any combination of virus spreading mechanisms including file extensions, executables, email attachments, IP addresses, ports, IM channels, and file transfer protocols
- Virus risk profiling allows IT managers to configure outbreak prevention policy and clean-up template deployments based on alert status—high or medium risk—according to TrendLabs virus infection statistics
- Outbreak prevention policies can be executed based on a specific deployment plan and configured to keep designated ports open and include or exclude deployment to specific product groups



Outbreak prevention policies can be deployed at specific points across the network

SYSTEM REQUIREMENTS

Hardware (Server)

- Intel™ Pentium™ III processor, 450MHz or higher
- 256MB RAM
- 300MB disk space for Control Manager Standard Edition
- 350 MB disk space for Control Manager Enterprise Edition
- 300MB for MSDE 2000 (optional)

Products Supported

Requires installation of one of the following Trend Micro products. Gateway: InterScan™ eManager™, InterScan Web Protect™ for ICAP, InterScan™ Messaging Security Suite for Windows/Unix, InterScan Web Security Suite for Windows/Solaris, Trend Micro™ Network VirusWall™. Mail: ScanMail™ for Exchange, ScanMail for Lotus Notes, ScanMail for eManager. Desktop: Server Protect™ for Windows, OfficeScan™

Software Requirements

Server

- Microsoft™ Windows NT™ 4 with Service Pack 6a, Microsoft Windows 2000 Server /Advanced Server with Service Pack 3, Microsoft Windows Server 2003 Standard Edition / Enterprise Edition

Web Server

- Microsoft Internet Information Server (IIS) 4.0 or higher

Databases—any of the following:

- Microsoft Data Engine (MSDE) 1.0 / 2000 (2000 + Service Pack 3 is recommended), Microsoft SQL Server 7.0, Microsoft SQL Server 2000 (2000 + Service Pack 3 is recommended)
- Others—SQL ODBC driver 3.7 or higher
- Windows Installer (included in Control Manager package)

Agent

Please refer to the managed product documentation for detailed information. To get the newest supported agents by Control Manager visit the following URL: <http://www.trendmicro.com/en/products/management/tmcm/evaluate/requirements.htm>

Management Console

Requires Trend Micro Control Manager:

- Microsoft Internet Explorer 5.5 with Service Pack 2 or higher
- Microsoft Version 5.0.0.3805 or higher

TrendLabs™

24X7 ANTIVIRUS SUPPORT

Trend Micro products are backed by timely, high-quality service from TrendLabs™, a global network of five regional antivirus research and support centers with an ISO9001:2000-certified & COPC-2000 Standards-certified headquarters. A team of more than 300 engineers and antivirus specialists operate around the clock to monitor virus activity, develop information on new threats, and deliver prompt, effective strategies.

For more information about Trend Micro service and support, contact TrendLabs at <http://www.trendmicro.com/trendlabs>.

TREND MICRO

ENTERPRISE PROTECTION STRATEGY

Trend Micro™ Enterprise Protection Strategy (EPS) is a customer-driven approach designed to manage the outbreak lifecycle, from vulnerability prevention to malicious code prevention and elimination. Through coordinated delivery of industry-leading products, services, and threat-specific expertise from Trend Micro's global network of security experts, EPS helps organizations prevent viruses from exploiting vulnerabilities on the network, enforce security policies to control network access of devices, prevent or contain and eliminate viruses and remnants spreading through application and network layers, and centrally manage and integrate outbreak security actions. EPS has helped customers worldwide prevent malicious code attacks and minimize outbreak-related costs and damages.

TREND MICRO INCORPORATED

10101 N. De Anza Blvd.
Cupertino, CA 95014, USA
toll free: 1+800-228-5651
phone: 1+408-257-1500
fax: 1+408-257-2003

www.trendmicro.com