

Trend Micro™

# Endpoint Security Platform

Security, visibility, and manageability converge in a single, highly scalable platform

Managing network systems to ensure endpoint security is more difficult than ever before. Enterprises struggle with distributing and updating software, managing assets, maintaining availability, and securing data across all clients and servers. Add to this the challenge of managing new technology trends such as a mobile workforce, green IT initiatives, collaborative Web 2.0 tools, and social networking sites—all within an economy that demands lower costs. Enterprises are faced with the challenge of efficiently utilizing these tools to support their business while having to secure their endpoints against increasingly sophisticated malware.

The increasing availability of new, business-critical endpoint applications has created more avenues for malware to exploit, making endpoints the most at-risk point in the network. Most endpoint security has not caught up to new business practices required in today's workplace. Two thirds of most enterprise endpoints are likely to be infected by malware each year.\*

To combat endpoint threats, enterprises often piece together security and systems management products to create a stronger defense. But this patchwork approach provides poor visibility and control, slowing the ability to issue policy enforcement across endpoints to ensure effective protection. And when threats change or enterprise needs evolve, it can take months to deploy additional products across enterprise endpoints. This delay creates a critical security gap that puts the enterprise at risk.

## INSTANT VISIBILITY AND CONTROL OF EVERY ENDPOINT

**Trend Micro Endpoint Security Platform** reduces complexity by distributing computing power to the endpoints, using an intelligent agent that offers a level of visibility and control not previously possible. A single server, single agent, single console technology provides a unified point of control for policy-driven endpoint management. This high-performance framework simplifies protection for large organizations, distributed environments, and even remote workers—regardless of connectivity. Enterprises get significant advantages in speed, flexibility, and scalability, while reducing the infrastructure and maintenance costs associated with traditional systems and security management.

## BUILT TO EVOLVE WITH YOUR ENTERPRISE'S NEEDS

As the foundation for the solution, Endpoint Security Platform creates a unified framework for security and systems management. Enterprises then customize the solution by selecting the specific platform modules that support their unique endpoint environments, easily deploying the security and systems management functionality they need to every endpoint. Then, as threats evolve or enterprise needs change, new modules can be quickly deployed—reducing implementation across all endpoints from weeks and months to just days or hours. With a highly scalable architecture that supports up to 250,000 users on one management server, Endpoint Security Platform allows system management and security teams to centrally secure their endpoints with confidence and accuracy, reducing complexity and risk, and saving costs.

## SOFTWARE

### Protection Points

- Clients
- Servers
- Laptops

### Threat Protection

- Antivirus
- Antispyware
- Anti-rootkit
- Web threat protection
- Vulnerability patching
- Data loss

## KEY BENEFITS

### Delivers Pervasive Visibility and Control

- Provides enterprise-wide, real-time visibility into both security and operations
- Transparently manages mobile computers regardless of network or Internet connectivity

### Speeds Time to Protection

- Collapses management actions from weeks and months to hours and days
- Quickly deploys new protection through modular architecture

### Increases Management Efficiency

- Helps organizations meet their service level agreements and regulatory compliance requirements
- Reduces tool clutter and licensing costs through service consolidation

\*Osterman Research. A Cloud-Client Architecture Provides Increased Security at Lower Cost. January 2009

## ENDPOINT SECURITY PLATFORM FEATURES

### Endpoint Security Platform Agent

- Uses a single, multi-purpose agent that powers a resilient distributed intelligent infrastructure with processing from a central server
- Delivers real-time and continuous security, policy processing, remediation, validation, and reporting
- Requires only 2-4 MB of endpoint system memory and consumes less than 2 percent host CPU
- Enforces policies even when remote devices roam from the enterprise network
- Supports on-the-fly queries and management actions with encrypted agent-to-server communications

### Endpoint Security Platform Server

- Manages over 250,000 endpoints on a single management server
- Hosts the management console with policy capabilities and built-in reporting and analysis tools
- Supports automatic multi-server synchronization and non-stop services even during a disruptive event
- Uses an integrated security infrastructure to publish policies and aggregate data
- Sets configuration standards and baselines for defined groups of managed clients

### Endpoint Security Platform Policy Messages

- Communicate policy information between agents and server environments
- Allow simple scripting for policy creation, enabling the use of logical criteria to trigger specific actions
- Give enterprises the flexibility to choose from provided policies or customize their own
- Deliver a secure authentication and audit trail

### Endpoint Security Platform Relays

- Act as communication and aggregation points as well as staging areas for the Policy Messages and patch or remediation content
- Allow any computer to be designated to oversee tasks such as asset discovery, scanning, patch downloading, and more, with no additional impact on the host
- Reduce network bandwidth requirements and provide platform redundancy
- Serve devices regardless of location or network reliability
- Maximize network resources with the ability to cache, stop, and restart client updates

## ENDPOINT SECURITY PLATFORM MODULES

### Core Protection Module

- Provides a complete set of anti-malware prevention and removal capabilities, including protection against spyware
- Blocks users and applications from accessing malicious web content
- Features Trend Micro's new File Reputation and Web Reputation in the innovative Smart Protection Network, using a cloud-client architecture
- Moves malware signature files and web reputation assessments into the cloud to reduce update management and minimize the load on the endpoint
- Queries in-the-cloud threat intelligence for immediate protection without distributed updates

### Web Protection Module

- Leverages Web Reputation in the innovative Smart Protection Network
- Prevents users and applications from accessing malicious web content in real time

### Patch Management Module

- Delivers patch capabilities for multiple operating systems with coverage for a variety of software applications
- Ensures no loss of functionality over low-bandwidth or globally-distributed networks, increasing first-pass patch installation success rates
- Offers real-time visibility to ensure up-to-date protection with detailed patch deployment and installation reports.

### Data Leak Prevention Module

- Protects data assets from accidental loss or theft, ensuring the privacy and integrity of sensitive information
- Combines endpoint-based enforcement with highly accurate fingerprinting and content matching technology

## SYSTEMS REQUIREMENTS

### System and Server Requirements

- Supported Operating Systems for Endpoint Security Platform Management Server
  - Windows 2000 Server SP 2+/2003/2008

### Database Requirements for Endpoint Security Platform Management Server

- SQL Server 2000 SP4/2005

### Supported Operating Systems for Endpoint Security Platform Console

- Windows XP/2000/2003 Vista/2008

