

Trend Micro™

# VULNERABILITY PROTECTION

## Advanced Vulnerability Shielding for Endpoints

Today's enterprise endpoints face more sophisticated attacks than ever, especially when they are outside the corporate network and no longer protected by multiple layers of security. In addition, point of sale devices and networked devices with embedded operating systems are difficult to update and patch. To keep your business fully protected from breach or targeted attack, all types of endpoints require a blended approach to protection that secures data and applications from hacking attempts, Web threats, and the increasing threat of vulnerabilities being exploited.

**Trend Micro™ Vulnerability Protection** provides earlier, stronger endpoint protection by supplementing client-level antivirus and anti-malware security with pro-active virtual patching. A high-performance, deep-packet inspection engine monitors incoming and outgoing traffic for network protocol deviations, suspicious content that signals an attack, or security policy violations. Vulnerability Protection prevents vulnerabilities from being exploited with easy and fast to deploy filters, providing full protection before patches can be deployed. When used in conjunction with additional Trend Micro endpoint products, Vulnerability Protection provides the industry's most secure protection for endpoints, whether they are on the network, mobile, or remote.

## KEY FEATURES

### Defends Against Advanced Threats

- Blocks known and unknown vulnerability exploits before patches are deployed
- Automatically assesses and recommends required virtual patches
- Dynamically adjusts security configuration based on the location of an endpoint
- Protects endpoints with minimal impact on network throughput, performance, or user productivity
- Shields endpoints against unwanted network traffic with multiple protection layers
- Protects systems that hold sensitive data, critical to regulatory and corporate policy compliance

### Removes Bad Data from Business-Critical Traffic

- Applies control filters to alert/block specific traffic such as instant messaging and media streaming

- Ensures delivery of business-critical communications with low false positives
- Uses deep packet inspection to identify content that may harm the application layer
- Filters forbidden network traffic and ensures allowed traffic through stateful inspection

### Provides Earlier Protection

- Provides protection before patches are deployed using attack blocking and vulnerability shielding
- Shields operating system and common applications from known and unknown attacks
- Detects malicious traffic that hides by using supported protocols over non-standard ports
- Blocks traffic likely to damage at-risk components using vulnerability-facing network inspection
- Prevents networking backdoors from penetrating into the corporate network

## SOFTWARE

### Protection Points

- Endpoints

### Threat Protection

- Vulnerability Exploits
- Denial of Service Attacks
- Illegitimate Network Traffic
- Web Threats

## KEY BENEFITS

- Eliminates risk exposure due to missing patches
- Extends the life of legacy and end-of-support operating systems like Windows XP
- Reduces down-time for recovery with incremental protection against zero day attacks
- Allows patching on your own terms and timelines
- Lowers potential legal exposure by improving data security compliance
- Enhances firewall protection for remote and mobile enterprise endpoints

- Blocks all known exploits with attack-facing network inspection
- Defends custom and legacy applications using custom filters that block user-defined parameters

### Deploys and Manages with Your Existing Infrastructure

- Preserves endpoint performance with light-weight agent architecture
- Simply and easily deploys with existing endpoint security solutions
- Increases convenience of implementing granular control with simplified dashboard and management console
- Easily deployed and managed from previously installed Trend Micro central management console
- Reduces the need to patch and reboot immediately causing unnecessary downtime on systems

**Vulnerability Protection** stops zero-day threats immediately on your physical and virtual desktops and laptops—on and off the network. Using host-level intrusion prevention system (HIPS), behavioral, statistical, heuristic and protocol enforcement technologies, Vulnerability Protection shields against vulnerabilities before a patch is available or deployable. This allows you to protect your critical platforms from both known and unknown threats including legacy operating systems such as Windows XP and new systems like Windows 8. To support a layered approach to security, Vulnerability Protection integrates with Trend Micro Complete User Protection solutions to deliver multiple layers of interconnected threat and information protection.

Trend Micro Vulnerability Protection can scale up to 20,000 endpoints per server. As an on-premise software application, Vulnerability Protection integrates with other Trend Micro threat protection solutions to enhance the overall threat and malware protection of your endpoints.

**Two components are required:**

- Server installs on supported Windows platforms and is managed through a web-browser
- Agent installs on supported Windows platforms

- **Complete User Protection**
- Vulnerability Protection is part of
- Trend Micro Complete User Protection,
- a multi-layer solution that provides the
- broadest range of interconnected threat
- and data protection across endpoints,
- email and collaboration, web, and
- mobile devices.

## SYSTEMS REQUIREMENTS FOR VULNERABILITY PROTECTION

VULNERABILITY PROTECTION MANAGER (SERVER) SYSTEM REQUIREMENTS
<b>Memory:</b> 4 GB (8 GB recommended)
<b>Disk Space:</b> 1.5 GB (5 GB recommended)
<b>Operating System</b> <ul style="list-style-type: none"> <li>• Microsoft Windows 2012 R2 (64-bit)</li> <li>• Microsoft Windows 2012 (64-bit)</li> <li>• Windows Server 2008 R2 (64-bit)</li> <li>• Windows Server 2008 (32-bit and 64-bit)</li> <li>• Windows 2003 Server SP2 (32-bit and 64-bit)</li> <li>• Windows 2003 Server R2 SP2 (32-bit and 64-bit)</li> </ul>
<b>Web Browser</b> <ul style="list-style-type: none"> <li>• Firefox 12+</li> <li>• Internet Explorer 9.x &amp; 10.x</li> <li>• Chrome 20+</li> </ul> <p>Note: Cookies must be enabled on all browsers</p>
VULNERABILITY PROTECTION AGENT SYSTEM REQUIREMENTS
<b>Memory:</b> 128 MB
<b>Disk Space:</b> 500 MB
<b>Operating System</b> <ul style="list-style-type: none"> <li>• Windows 8.1 (32-bit and 64-bit)</li> <li>• Windows Server 2012 R2 (64-bit)</li> <li>• Windows 8 (32-bit and 64-bit)</li> <li>• Windows Server 2012 (64-bit)</li> <li>• Windows 7 (32-bit and 64-bit)</li> <li>• Windows Server 2008 R2 (64-bit)</li> <li>• Windows Server 2008 (32-bit and 64-bit)</li> <li>• Windows Vista (32-bit and 64-bit)</li> <li>• Windows Server 2003 SP1 (32-bit and 64-bit) patched with "Windows Server 2003 Scalable Networking Pack"</li> <li>• Windows Server 2003 SP2 (32-bit and 64-bit)</li> <li>• Windows Server 2003 R2 SP2 (32-bit and 64-bit)</li> <li>• Windows XP (32 bit and 64 bit)</li> </ul>



Securing Your Journey to the Cloud

©2014 by Trend Micro Incorporated. All rights reserved. Trend Micro, the Trend Micro t-ball logo, OfficeScan, and Trend Micro Control Manager are trademarks or registered trademarks of Trend Micro Incorporated. All other company and/or product names may be trademarks or registered trademarks of their owners. Information contained in this document is subject to change without notice. [DS03\_VP\_140326US]