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 sales 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 remotely.

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, engine monitors traffic for new specific vulnerabilities using host-based intrusion prevention filters as well as zero-day attack monitoring. So you can detect network protocol deviations, suspicious content that signals an attack, or security policy violations. Vulnerability Protection prevents these vulnerabilities from being exploited with easy and fast-to-deploy filters that provide full protection before patches can be deployed. When used in conjunction with additional Trend Micro endpoint products, Vulnerability Protection provides the industry's broadest range of protection for endpoints, whether they are on the network, travelling, or remote.

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

KEY FEATURES

Defends Against Advanced Threats

- Blocks known and unknown vulnerability exploits before patches are deployed
- Automatically assesses and recommends required virtual patches for your specific environment
- 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
- 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 and often before patches are available
- 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
- Blocks all known exploits with intrusion prevention signatures
- 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 user-based visibility with the management console
- Organizes vulnerability assessments by Microsoft security bulletin numbers, CVE numbers, or other important information
- Provides logging integration with popular SIEM tools
- Simplifies deployment and management by using your exisiting Trend Micro OfficeScan plug-in manager and Control Manager (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) filters, 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 10. 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 is very scalable with options for multiple servers to ensure endpoint deployment for even the largest of organizations. 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

SYSTEMS REQUIREMENTS FOR VULNERABILITY PROTECTION

VULNERABILITY PROTECTION MANAGER (SERVER) SYSTEM REQUIREMENTS
Memory: 4 GB (8 GB recommended)
Disk Space: 1.5 GB (5 GB recommended)
Operating System • Microsoft Windows 2012 R2 (64-bit) • Microsoft Windows 2012 (64-bit) • Windows Server 2008 R2 (64-bit) • Windows Server 2008 (32-bit and 64-bit)
Web Browser • Firefox 12+ • Internet Explorer 9.x & 10.x • Chrome 20+ Note: Cookies must be enabled on all browsers

VULNERABILITY PROTECTION AGENT SYSTEM REQUIREMENTS
Memory: 128 MB
Disk Space: 500 MB
Operating System • Windows 10 (32-bit and 64-bit) • Windows 8.1 (32-bit and 64-bit) • Windows Server 2012 R2 (64-bit) • Windows 8 (32-bit and 64-bit) • Windows Server 2012 (64-bit) • Windows 7 (32-bit and 64-bit) • Windows Server 2008 R2 (64-bit) • Windows Server 2008 (32-bit and 64-bit) • Windows Vista (32-bit and 64-bit) • Windows Server 2003 SP1 (32-bit and 64-bit) patched with "Windows Server 2003 Scalable Networking Pack" • Windows Server 2003 SP2 (32-bit and 64-bit) • Windows Server 2003 R2 SP2 (32-bit and 64-bit) • Windows XP (32 bit and 64 bit)

Complete User Protection

Vulnerability Protection is part of the Trend Micro Smart Protection Suites. These interconnected, multi-layered security suites protect your users and their data regardless of device or location. So you get the broadest range of threat protection capabilities, at multiple layers: including endpoint, application, and gateway. Plus, you can evolve your protection along with your business using flexible on-premise, cloud and hybrid deployment models. You simply make changes on the fly without the hassles of new licenses. And, you can manage users across multiple threat vectors from a single management console giving you complete user-based visibility of the security of your environment.

TREND MICRO™

Securing Your Journey to the Cloud