Trend Micro

OFFICESCAN

Endpoint protection for physical and virtual desktops

In the "bring-your-own-device" (BYOD) environment, protecting your endpoints against ever-evolving threats has become a costly juggling act for IT managers. With mobile devices and cloud computing, protecting your data from loss or theft is top of mind. Add to that the performance issues associated with trying to apply traditional security to virtual desktop infrastructures and it's clear, IT needs a flexible endpoint security platform that will adapt to changing needs with a light and lean architecture geared for performance.

Trend Micro™ OfficeScan™ endpoint security delivers real-time protection against the latest threats, in a light and lean client optimized for physical and virtual endpoint deployments. OfficeScan enhances your endpoint protection with cloud-based global threat intelligence, integrated data loss prevention (DLP), and a virtualization-aware client that reduces the endpoint footprint, protects sensitive data, and improves endpoint performance across the enterprise.

To support a layered approach to security, OfficeScan integrates with Trend Micro Complete User Protection solutions to deliver multiple layers of interconnected threat and data protection. Security modules for data loss prevention, virtual desktop infrastructure (VDI), and Mac can be immediately deployed—without having to roll out additional management or client infrastructure. OfficeScan also works in conjunction with proactive security technologies like application control, vulnerability protection, mobile security, and endpoint encryption to further enhance your threat protection.

Superior malware protection
Protects endpoints, on or off the corporate network, against viruses, Trojans, worms, spyware, and new variants as they emerge

Easy to deploy and manage
Centralizes management capabilities, for heightened visibility and greater control

Security optimized for virtual desktop infrastructures (VDI)
Isolate control of desktop environments, streamline management, and consolidate and extend the life of existing hardware

Extensible architecture
Leverage flexible architecture to add security services as needed, and, apply future updates, without having to redeploy the entire solution

Integrated data loss prevention (DLP)
Protect your private data with this optional DLP module that secures the two most common vectors for accidental and intentional data leaks: USB devices and email

Centralized Visibility and Control
When deployed with Trend Micro™ Control Manager™, multiple OfficeScan servers can be managed through a single console providing complete user visibility

Mobile Security Integration
Integrate Trend Micro™ Mobile Security and OfficeScan by using Control Manager to centralize security management and policy deployment across all endpoints; Mobile Security includes mobile device threat protection, mobile app management, mobile device management (MDM), and data protection

Protection Points

- Physical endpoints
- Virtualized endpoints
- Windows PCs
- Macintosh computers
- Sensitive data

Threat Protection

- Command and control
- Anti-rootkit
- Antispyware
- Antivirus/antimalware
- Advanced Persistent Threats (APTs)
- Firewall
- Browser exploit protection
- Anti-variant/packer protection
- Data loss prevention
- Web threat protection

ADVANTAGES

Secure data on physical and virtual desktops from a central management platform

OfficeScan endpoint security defends against the growing number of attacks on endpoints, including virtual desktops, while delivering full user visibility from a single console that integrates with your existing endpoint infrastructure.

- Manage by user across threat vectors from a single pane of glass, giving you complete visibility to the security of your environment
- Reduces the burden of client updates, decreases agent footprints, and minimizes performance impact
- Queries up-to-the-second data on the safety of a file or web page before it's accessed
- Secures endpoints, on or off the corporate network, as new threats emerge
- Improves web performance and privacy by synchronizing with a local server
- Detects and removes active and hidden rootkits
- Safeguards endpoint mail boxes by scanning POP3 email and Outlook folders for threats
- Identifies and blocks botnet and targeted attack Command and Control (C&C) communications using global and local threat intelligence

Secures endpoints with the broadest range of superior malware protection

Protects endpoints, on or off the corporate network, against viruses, Trojans, worms, spyware, advanced persistent threats (APTs) and new variants as they emerge.

- Reduces the burden of pattern file management and lowers performance impact
- Improves web performance and privacy by synchronizing with a local server
- Detects and removes active and hidden rootkits
- Safeguards endpoint mail boxes by scanning POP3 email and Outlook folders for threats
- Queries up-to-the second data on the safety of a file before it's accessed
- Identifies and blocks botnet and targeted attack Command and Control (C&C) communications using global and local threat intelligence
- Secures users and endpoint systems from accessing malicious web content without relying on updates to assure zero-day protection (browser exploit protection)
- Proactively detects malware variants, reducing the number of required signatures via anti-variant/packer protection

Enable consumerization and BYOD without compromising security

When deployed with OfficeScan, Trend Micro™ Mobile Security extends your endpoint protection to smartphones and tablets—enabling centralized management, policy deployment, and visibility of all endpoint security through Trend Micro Control Manager. As a 4-in-1 solution, Trend Micro Mobile Security integrates mobile device antimalware, mobile app management, mobile device management (MDM), and data protection to help you manage BYOD.

- Centralizes management via Trend Micro Control Manager, for heightened visibility and greater control
- Protects sensitive data on smartphones and tablets by enforcing use of passwords and encryption, enforcing app restrictions, and remotely locking and wiping lost or stolen devices
- Reduces helpdesk and IT costs by simplifying device provisioning and management
- Reduces data loss by providing visibility and control of mobile apps, enabling you to determine which apps employees can use
- Identifies risky mobile apps by utilizing the cloud-based Trend Micro Mobile Application Reputation Service, enabling IT to set policies restricting app use
- Integrates with Active Directory to synchronize endpoint data and report on policy compliance
- Empowers IT to restrict the use of USB drives, CD/DVD writers, and other removable media
- Offers granular device control, including the ability to create specific rules based on make and serial number of the device
- Educates employees on corporate data usage policies through alerts, blocking and reporting

Key Benefits

- Recognizes if an agent is on a physical or virtual endpoint for optimum targeting
- Offers a flexible, modular architecture, quick updates, and instant deployments when needed
- Prevents network, CPU, and storage conflicts by serializing scan and updates per virtual server
- Reduces scan times of virtual desktops by white-listing images and previously scanned content
- Light and lean cloud-client architecture increases performance to boost productivity
- User-based visibility of your environment

CUSTOMIZE YOUR ENDPOINT PROTECTION

Expand your existing Trend Micro endpoint security with optional security modules and complementary endpoint solutions:

Data Loss Prevention (DLP) Module

Plugs into OfficeScan to protect your sensitive data with the integrated Data Loss Prevention (DLP) module, for maximum visibility and control.

- Protects private data—on or off network
- Advanced device control capability protects against data leaks via USB drives or connected mobile devices, Bluetooth connections, and other media
- Covers the broadest range of devices, applications, and file types
- Aids compliance with greater visibility and enforcement
- Data discovery provides visibility to confidential information stored on the local hard drive

Security for Mac Module

Plugs into OfficeScan to provide a layer of protection for Apple Mac clients on your network by preventing them from accessing malicious sites and distributing malware—even if the malware is not targeted at Mac OS X.

- Reduces exposure to web-based threats, including fast-spreading Mac-targeting malware such as Flashback
- Adheres to Mac OS X look and feel for positive user experience
- Saves time and effort with centralized management across endpoints, including Macs

Virtual Desktop Infrastructure (VDI) Module

Plugs into OfficeScan to let you consolidate your endpoint security into one solution for both physical and virtual desktops.

- Recognizes whether an agent is on a physical or virtual endpoint and optimizes protection and performance for its specific environment
- Serializes scans and updates, and white lists base images and previously scanned content to preserve the host resources

Endpoint Encryption

Ensure data privacy by encrypting data stored on your endpoints—including PCs, Macintoshes, DVDs, and USB drives, which can easily be lost or stolen. Trend Micro™ Endpoint Encryption provides the data security you need with full disk encryption, folder and file encryption, and removable media encryption.

- Protects data at rest with full disk encryption software
- Automates data management with self-encrypting hard drives
- Encrypts data in specific files, shared folders, removable media
- Sets granular policies for device control and data management

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), Trend Micro™ Vulnerability Protection shields against known and unknown vulnerabilities before a patch is available or deployable. Extends protection to critical platforms, including legacy operating systems such as Windows XP and new systems like Windows 8.

- Eliminates risk exposure due to missing patches with virtual patching
- Reduces down-time for recovery with incremental protection against zero day attacks
- Allows patching on your own terms and timelines
- Enhances firewall protection for remote and mobile enterprise endpoints

Endpoint Application Control

Enhances your defenses against malware and targeted attacks by preventing unwanted and unknown applications from executing on your corporate endpoints.

- Protects against users or machines executing malicious software
- Further simplifies management and deployment when used with OfficeScan
- Provides advanced whitelist and blacklist features to enforce corporate policies
- Uses correlated threat data from billions of records daily

Trend Micro Control Manager™

This centralized security management console ensures consistent security management and complete visibility and reporting across multiple layers of interconnected security from Trend Micro. It also extends visibility and control across on-premise, cloud, and hybrid deployment models. Centralized management combines with user-based visibility to improve protection, reduce complexity, and eliminate redundant and repetitive tasks in security administration—all of which make your organization more secure, and your life easier. Control Manager also provides access to actionable threat intelligence from the Trend Micro Smart Protection Network cloud data mining framework.

OFFICESCAN SYSTEMS REQUIREMENTS

MINIMUM RECOMMENDED SERVER REQUIREMENTS

Server Operating System

- Windows Server 2003 (SP2) and 2003 R2 (SP2) (x86/x64) Editions
- Windows Storage Server 2003 (SP2), Storage Server 2003 R2 (SP2) (x86/x64) Editions
- Windows Compute Cluster Server 2003
- Windows Server 2008 (SP1/SP2) and 2008 R2 (With/Without SP1) (x86/x64) Editions
- Windows Storage Server 2008 and Storage Server 2008 R2 (x86/x64) Editions)
- Windows HPC Server 2008 and HPC Server 2008 R2 - (x86/x64)
- Windows MultiPoint Server 2010 and 2012 - (x64)
- Windows Server 2012 and 2012 R2 (x64) Editions
- Windows MultiPoint Server 2012 - (x64) Editions
- Windows Storage Server 2012 - (x64) Editions

Server Platform

Processor: 1.86 GHz Intel Core 2 Duo (2 CPU cores) or better

Memory: 1 GB minimum (2GB recommended) with at least 500MB exclusively for OfficeScan (on Windows 2003/2008 family)

- 2 GB minimum with at least 500MB exclusively for OfficeScan (on Windows 2010/2011/2012 family)

Disk Space: 5 GB minimum, 5.5GB minimum (using remote install)

MINIMUM RECOMMENDED AGENT REQUIREMENTS

Agent Operating System

- Windows XP (SP3) (x86) Editions
- Windows XP (SP2) (x64) (Professional Edition)
- Windows Vista (SP1/SP2) (x86/x64) Editions
- Windows 7 (with or without SP1) (x86/x64) Editions
- Windows Embedded POSReady 2009, Embedded POSReady 7
- Windows 8 and 8.1 (x86/x64) Editions
- Windows Server 2003 (SP2) and 2003 R2 (x86/x64) Editions
- Windows Compute Cluster Server 2003(Active/Passive)
- Windows Storage Server 2003 (SP2), Storage Server 2003 R2 (SP2) (x86/x64) Editions
- Windows Server 2008 (SP1/SP2) and 2008 R2 (With/Without SP1) (x86/x64) Editions
- Windows Storage Server 2008 and Storage Server 2008 R2 (x86/x64) Editions
- Windows HPC Server 2008 and HPC Server 2008 R2 (x86/x64) Editions
- Windows Server 2008/2008 R2 Failover Clusters (Active/Passive)
- Windows MultiPoint Server 2010 and 2011 (x64)
- Windows Server 2012 and 2012 R2 (x64) Editions
- Windows Storage Server 2012 (x64) Editions
- Windows MultiPoint Server 2012 (x64) Editions
- Windows Server 2012 Failover Clusters (x64)

Agent Platform

Processor: 300MHz Intel Pentium or equivalent (Windows XP, 2003, 7, 8, 8.1 family)

- 1.0 Ghz minimum (2.0 Ghz recommended) Intel Pentium or equivalent (Windows Vista, Windows Embedded POS, Windows 2008 {x86} family)
- 1.4 Ghz minimum (2.0 Ghz recommended) Intel Pentium or equivalent (Windows 2008 {x64}, Windows 2012 family)

Memory: 256MB minimum (512MB recommended) with at least 100MB exclusively for OfficeScan (Windows XP, 2003, Windows Embedded POSready 2009 family)

- 512MB minimum (2.0GB recommended) with at least 100MB exclusively for OfficeScan (Windows 2008, 2010, 2011, 2012 family)
- 1.0GB minimum (1.5GB recommended) with at least 100MB exclusively for OfficeScan (Windows Vista family)
- 1.0GB minimum (2.0GB recommended) with at least 100MB exclusively for OfficeScan (Windows 7 {x86}, 8 {x86}, 8.1 {x86}, Windows Embedded POSReady7 family)
- 1.5GB minimum (2.0GB recommended) with at least 100MB exclusively for OfficeScan (Windows 7 {x64}, 8 {x64}, 8.1 {x64} family)

Disk Space: 350MB minimum

Detailed requirements are available online at **docs.trendmicro.com**.

Complete User Protection

OfficeScan 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.

TREND MICRO™

Securing Your Journey to the Cloud