Trend Micro

OFFICESCAN

Comprehensive, high-performance endpoint protection

Organizations are looking at their endpoint security with a critical eye these days, with more awareness that traditional signature-based antivirus approaches alone are a weak defense against modern threats and targeted attacks. To defend against today's threats, it's critical to deploy advanced endpoint protection that covers the full security lifecycle to prevent, detect, analyze, and respond to threats. A connected approach across this lifecycle means fewer consoles and vendors, less expense, and a more rapid response to threats. And to protect against fast-changing threat landscapes, you require a flexible endpoint security platform that will adapt to your changing needs with an architecture optimized for network and endpoint performance.

Trend Micro™ OfficeScan™ delivers comprehensive endpoint security technology for today and the future with real-world protection against the latest advanced threats. You get modern threat protection for anti-malware, packer variants, device control, command and control (C&C) traffic, browser exploits, behavior monitoring, web threats, census-based control, and more. This broad protection is delivered via an architecture that uses endpoint resources more effectively and ultimately out-performs the competition on CPU and network utilization.

OfficeScan is a critical component of our Smart Protection Suites that deliver even more gateway and endpoint protection capabilities like application whitelisting, vulnerability shielding, endpoint encryption, data loss prevention (DLP), and more in one compelling package. Additional Trend Micro solutions extend your protection from advanced attacks with endpoint forensics + analysis. Plus, Deep Discovery network sandboxing delivers rapid response (real-time signature updates) to endpoints when a new threat is detected locally, enabling faster time-to-protection and reducing the spread of malware. All of this modern threat security technology is made simple for your organization with central visibility, management, and reporting.

Protection Points

- Physical endpoints
- Virtualized endpoints
- Windows PCs
- Mac computers
- Point of Sale (POS) and ATM endpoints

Threat Protection

- Command and control
- Anti-rootkit, antispyware, anti-ransomware, antivirus, anti-malware
- Advanced threats
- Firewall
- Behavior monitoring
- Browser exploit protection
- Anti-variant/packer protection
- Data loss prevention (DLP)
- Web threat protection
- Sandbox integration

See how we stack up

YOU CAN HAVE IT ALL

- **Advanced malware protection:** Protects endpoints, on or off the corporate network, against viruses, Trojans, worms, spyware, ransomware, and new variants as they emerge.
- **Security optimized for virtual desktop infrastructures (VDI):** Isolate control of desktop environments, streamline management, and consolidate and extend the life of existing hardware.
- **Connected threat defense:** OfficeScan integrates with Deep Discovery (via Control Manager) to deliver rapid response (real-time signature updates) to endpoints when a new threat is detected locally by the sandbox, enabling faster time-to-protection and reducing the spread of malware.
- **Integrated data loss prevention (DLP):** Protect your private data with this optional DLP module that secures the most common vectors like cloud storage, USB devices, and email for accidental and intentional data leaks. Policy can be configured to automatically encrypt information being moved to a USB or cloud storage channel.
- **Centralized visibility and control:** When deployed with Trend Micro™ Control Manager™, multiple OfficeScan servers can be managed through a single console to provide 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.

ADVANTAGES

Secures 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.

- Provides complete visibility of your security environment with by-user management across threat vectors, from a single pane of glass
- 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
- Improves web performance and privacy by synchronizing with a local server
- Prevents programs or users from disabling anti-malware protection

Secures endpoints with the broadest range of superior malware protection

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

- Reduces the burden of pattern file management and lowers performance impact
- Detects and removes active and hidden rootkits and ransomware
- 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 (both inbound and outbound)
- 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
- Monitors for suspicious file encryption activities at the endpoint and terminates malicious activities, for more extensive ransomware prevention

Empowers mobility without compromising security

When deployed with OfficeScan, Trend Micro™ Mobile Security extends your endpoint protection to smart phones and tablets—enabling centralized management, policy deployment, and visibility of all endpoint security through Trend Micro Control Manager. Trend Micro Mobile Security integrates mobile device anti-malware, mobile app management, mobile device management (MDM), and data protection to help you manage and protect a wide range of mobile user activity.

- Centralizes management via Trend Micro Control Manager, for heightened visibility and greater control
- Protects sensitive data on smart phones 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
- Decreases 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
- Empowers IT to restrict the use of USB drives, CD/DVD writers, and other removable media

Key Business Issues

- Need one solution to protect against all advanced malware on PC desktops, Macs, and VDI
- Require centralized management for IT efficiency
- Must address security risks of BYOD, employees working remotely and cloud app usage
- Integration with advanced threat and data protection is critical

> "My first objective was to get rid of the heavy overhead that the previous endpoint solution was putting on our systems," said Jamieson. "OfficeScan did that... My second objective was to introduce security that really worked. Since we replaced the previous solution, we can see that Trend Micro has stopped the infections."

Bruce Jamieson,
Network systems manager of
A&W Food Services of Canada

CUSTOMIZE YOUR ENDPOINT PROTECTION

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

Data Loss Prevention (DLP) Module

Protects your sensitive data for maximum visibility and control.

- Secures private data on- or off-network, including encrypting files before they leave your network
- Protects against data leaks via cloud storage, 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

Security for Mac Module

Provides 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
- 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

Lets 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 whitelists base images and previously scanned content to preserve the host resources

Endpoint Encryption

Ensures data privacy by encrypting data stored on your endpoints—including PCs, Macs, 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
- Manages Microsoft Bitlocker and Apple FileVault

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.

- Eliminates risk exposure by shielding vulnerablities with virtual patching
- Reduces down-time for recovery and emergency patching
- Allows patching on your own terms and timelines
- Identifies security vulnerabilities with reporting based on CVE, MS-ID, severity

Endpoint Application Control

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

- Protects users or machines from executing malicious software
- Light-weight on system resources and ideal for protecting legacy, end-of-support systems
- Locks down systems to only the applications that your organizations wants used
- Uses correlated threat data from billions of files to create and maintain an up-to-date database of validated, good applications

Deep Discovery Endpoint Sensor

Provides context-aware endpoint security monitoring that records and reports detailed system-level activities to allow threat analysts to rapidly assess the nature and extent of an attack. Deep Discovery's custom detection, intelligence, and controls enable you to:

- Detect and analyze your attackers
- Immediately adapt protection against attack
- Rapidly respond before sensitive data is lost

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-premises, 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. Control Manager also provides access to actionable threat intelligence from the Trend Micro™ Smart Protection Network™, which uses global threat intelligence to deliver real-time security from the cloud, blocking threats before they reach you.

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

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

Disk Space: 5 GB minimum, 5.5 GB 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 10 (32-bit and 64-bit)
- 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: 300 MHz 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: 256 MB minimum (512 MB recommended) with at least 100 MB exclusively for OfficeScan (Windows XP, 2003, Windows Embedded POSready 2009 family)

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

Disk Space: 350 MB minimum

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

Complete User Protection

OfficeScan is part of the **Trend Micro Smart Protection Suites**. These interconnected, multi-layered security suites protect your users and their data regardless of the device they use, or where they are working. The Smart Protection Suites combine the broadest range of endpoint and mobile threat protection capabilities with multiple layers of email, collaboration, and gateway security. And, you can manage users across multiple threat vectors from a single management console that gives you complete user-based visibility of the security of your environment.

> "With a network like ours, spread across the entire country, being able to secure mobile and desktop devices under one platform simplifies the security for our network and improves our team's productivity."

Greg Bell,
IT director
DCI Donor Services

TREND MICRO™

Securing Your Journey to the Cloud