Trend Micro™

OFFICESCAN™

Endpoint security from the trusted leader

The threat landscape used to be black and white – you kept the bad stuff out and the good stuff in. Now it's harder to tell the good from the bad, and traditional signature-based antivirus approaches alone are a weak defense against ransomware and unknown threats, which often slip through. Next-generation technologies help with some threats but not others, and adding multiple anti-malware tools on a single endpoint results in too many products that don't work together. To complicate matters your users are increasingly accessing corporate resources from a variety of locations and devices, and even services in the cloud. You need endpoint security that is smart, optimized, and connected, from a proven vendor you can trust .

Trend Micro™ OfficeScan™ infuses high-fidelity machine learning into a blend of threat protection techniques to eliminate security gaps across any user activity and any endpoint. It constantly learns, adapts, and automatically shares threat intelligence across your environment. This blend of threat 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 gateway and endpoint protection capabilities like application control, intrusion prevention (vulnerability protection), endpoint encryption, data loss prevention (DLP), and more, in one compelling package. Additional Trend Micro solutions extend your protection from advanced attacks with endpoint investigation and response (EDR). 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.

YOU CAN HAVE IT ALL

- **Advanced malware and ransomware protection:** Protects endpoints, on or off the corporate network, against malware, trojans, worms, spyware, ransomware, and adapts to protect against new unknown variants as they emerge.
- **Detection and response capabilities:** Advanced detection and response capabilities are included with OfficeScan. An optional investigation tool, Trend Micro Endpoint Sensor, is also available as an add-on.
- **Connected threat defense:** OfficeScan integrates with other security products locally on your network and also via Trend Micro's global, cloud threat intelligence to deliver network sandbox rapid response updates to endpoints when a new threat is detected, enabling faster time-to-protection and reducing the spread of malware.
- **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.
- **Available on-premises or as a service.** OfficeScan can be deployed on site in your network or is available as a service (SaaS).

Protection Points

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

Threat Protection

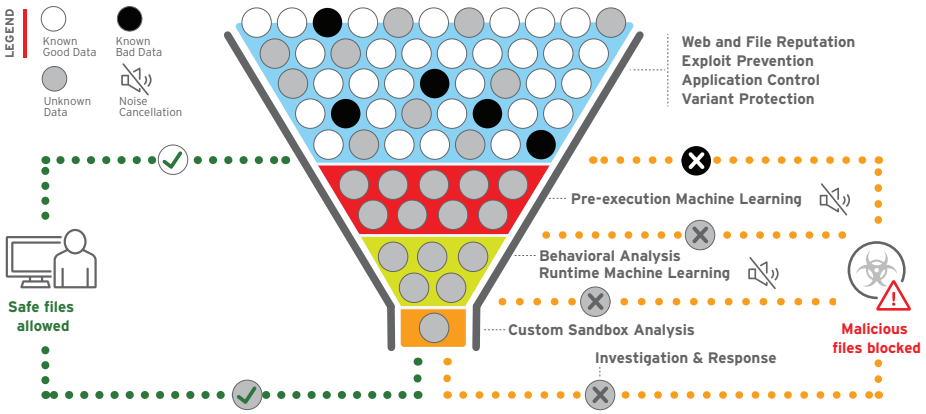
- High-fidelity machine learning (pre-execution and runtime)
- Behavioral analysis (against scripts, injection, ransomware, memory and browser attacks)
- File reputation
- Variant protection
- Census check
- Web reputation
- Exploit prevention (host firewall, exploit protection)
- Command and control (C&C) blocking
- Data loss prevention (DLP module)
- Device control
- Good file check
- Sandbox and breach detection integration
- Detection and response

See how we stack up

ADVANTAGES

Maximum XGen™ security

Infuses high-fidelity machine learning with other detection techniques for the broadest protection against ransomware and advanced attacks.



- Progressively filters out threats using the most efficient technique for maximum detection without false positives.
- Blends signature-less techniques including high-fidelity machine learning, behavioral analysis, variant protection, census check, application control, exploit prevention, and good-file check with other techniques like file reputation, web reputation, and command and control (C&C) blocking.
- Trend Micro is the first to infuse high-fidelity machine learning which uniquely analyzes files not only before execution but also during runtime for more accurate detection.
- Noise cancellation techniques like census and whitelist checking at each layer reduce false positives.
- Instantly shares information on suspicious network activity and files with other security layers to stop subsequent attacks.
- Advanced ransomware protection monitors for suspicious file encryption activities at the endpoint, terminates malicious activities, and even recovers lost files if necessary.

Minimum Impact

Reduce user impact and management costs.

- OfficeScan as a Service (only available from Smart Protection Suites) allows you to deploy and manage OfficeScan from our cloud-based service and offers feature parity with the on-premises option.
- Lightweight and optimized security uses the right detection technique at the right time to ensure minimal impact on devices and networks.
- Comprehensive central view of endpoint status lets you quickly get visibility to security risks.
- Automatic sharing of threat intelligence across security layers enables protection from emerging threats across the whole organization.
- Enable off-premises compliance and protection with the Edge relay that enables employees to work outside the corporate network and still connect to OfficeScan without a VPN.
- Customizable dashboards to fit different administration responsibilities.
- 24x7 support means that if a problem arises, Trend Micro is there to resolve it quickly.

Proven Security Partner

Trend Micro has a history of constant innovation to provide the most effective and efficient security technologies. We are always looking ahead to develop the technology needed to fight tomorrow's ever-changing threats.

- Nearly 30 years of security innovation.
- Protects over 155 million endpoints.
- Trusted by 45 of the top 50 global corporations.
- Trend Micro positioned as one of only three Leaders, amongst a field of 21 vendors in the 2018 Gartner Magic Quadrant for Endpoint Protection Platforms.

Key Business Issues

- Too many malware and ransomware threats getting through
- Need one solution to protect against all known and unknown threats on PC endpoints, Macs, and VDI
- Endpoint security solutions that don't talk to each other, lengthens time to protection and increase the management burden
- Risks of users working remotely, and sharing information in new ways via the cloud, etc.
- IT efficiency reduced when advanced threat and data protection don't integrate

> "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 Option

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 Option

Stops zero-day threats immediately on your physical and virtual desktops and laptops—on and off the network. Using host-based 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 vulnerabilities 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 Option

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
- Dynamic policies reduce management impact and allow flexibility for active user environments
- 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

Endpoint Sensor Option

Provides context-aware endpoint investigation and response (EDR), recording and reporting detailed system-level activities to allow threat analysts to rapidly assess the nature and extent of an attack. Custom detection, intelligence, and controls enable you to:

- Record detailed system-level activities
- Perform multi-level search across endpoints using rich search criteria such as OpenIOC, Yara, and suspicious objects
- Detect and analyze advanced threat indicators such as file-less attacks
- Rapidly respond before sensitive data is lost

Trend Micro™ Control Manager™ Module

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

OfficeScan Server Operating Systems:

- Windows HPC Server 2008 and HPC Server 2008 R2 (x64)
- Windows MultiPoint Server 2010 (x64) and 2012 (x64)
- Windows Server 2012 and 2012 R2 (x64) Editions
- Windows MultiPoint Server 2012 (x64) Editions
- Windows Storage Server 2012 (x64) Editions
- Windows Server 2016 (x64) Editions

OfficeScan 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 2008 family)

- 2 GB minimum with at least 500 MB exclusively for OfficeScan (on Windows 2010/2011/2012/2016 family)

Disk Space: 6.5 GB minimum, 7 GB minimum (using remote install)

OfficeScan Edge Relay Server Platform:

Processor: 2 GHz Intel Core 2 Duo (2 CPU cores) or better
Memory: 4 GB minimum
Disk Space: 50 GB minimum
Operation System: Windows Server 2012 R2
Network Card:

1. 2 network cards connect
   - One for intranet connection to OfficeScan Server
   - One for external connection to off-premises OfficeScan agents
2. 1 network card configuration to use different ports for intranet and internet connections

Database:

1. SQL Server 2008 R2 Express (or later)
2. SQL Server 2008 R2 (or later)

MINIMUM RECOMMENDED AGENT REQUIREMENTS

Agent Operating System

- Windows XP (SP3) (x86) Editions
- Windows XP (SP2) (x64) (Professional Edition)
- Windows 7 (with/without SP1) (x86/x64) Editions
- Windows 8 and 8.1 (x86/x64) Editions
- Windows 10 (32-bit and 64-bit)
- Windows 10 IoT Embedded
- 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 (SP2) (x86/x64) and 2008 R2 (SP1) (x64) Editions
- Windows Storage Server 2008 (SP2) (x86/x64) and Storage Server 2008 R2 (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 and 2012 R2 (x64) Editions
- Windows MultiPoint Server 2012 (x64) Editions
- Windows Server 2012 Failover Clusters (x64)
- Windows Server 2016 (x64) Editions
- Windows XP Embedded Standard (SP1/SP2/SP3) (x86)
- Windows Embedded Standard 2009 (x86)
- Windows Embedded POSReady 2009 (x86), Embedded POSReady 7 (x86/x64)
- Windows 7 Embedded (x86/x64) (SP1)
- Windows 8 and 8.1 Embedded (x86/x64) Editions

Agent Platform

Processor: 300 MHz Intel Pentium or equivalent (Windows XP, 2003, 7, 8, 8.1, 10 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 2016 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: 650 MB minimum

Disk Space: 650 MB minimum

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

> "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 User Protection solution is powered by XGen™, a smart, optimized, and connected security approach.

POWERED BY XGen™ SECURITY

TREND MICRO™

Securing Your Connected World