Trend Micro™

OFFICESCAN™

Trend Micro™ XGen™ Endpoint Security vom bewährten Sicherheitsexperten

Bisher war die Bedrohungslandschaft klar gegliedert: Man wehrte alles Böse ab und ließ alles Gute hindurch. Mittlerweile aber ist es nicht mehr so einfach, Gut und Böse zu unterscheiden und Unternehmen betrachten ihre Endpunktsicherheit zunehmend kritisch. Sie wissen, dass die herkömmlichen, signaturbasierten Antiviren-Ansätze allein nicht mehr ausreichen, um Ransomware und unbekannte Bedrohungen, die sich gerne unbemerkt einschleichen, abzuwehren. Sogenannte Next-Generation-Technologien sind bei einigen dieser Bedrohungen wirksam, bei anderen hingegen nicht. Wer zudem diverse Anti-Malware-Tools auf einem einzigen Endpunkt installiert, hat schnell eine Vielzahl von Produkten, die gar nicht kompatibel miteinander sind. Aber es wird noch komplizierter, denn immer mehr Benutzer greifen von den unterschiedlichsten Standorten und Geräten – manchmal sogar über cloudbasierte Services – auf Unternehmensressourcen zu. Sie brauchen also eine Endpunktsicherheit, die mehrdimensionalen Schutz vor sämtlichen Bedrohungsarten bietet. Und zwar von einem Anbieter, dem Sie wirklich vertrauen.

Trend Micro™ OfficeScan™ mit XGen™ Endpoint Security bietet ein äußerst zuverlässiges maschinelles Lernverfahren mit einer Reihe verschiedener Technologien zum Bedrohungsschutz, um Sicherheitsrisiken bei sämtlichen Anwenderaktivitäten und auf allen Endpunkten zu minimieren. Die Lösung lernt anhand von Bedrohungsdaten kontinuierlich hinzu, adaptiert diese Daten nach Bedarf und verbreitet sie automatisch über Ihre gesamte Umgebung hinweg. Dieser kombinierte Bedrohungsschutz wird über eine Architektur bereitgestellt, die Endpunktressourcen effektiver nutzt und eine deutlich bessere CPU- und Netzwerkauslastung bietet als Produkte von Marktbegleitern.

OfficeScan ist eine Kernkomponente unserer **Smart Protection Suites**, die in einem einzigen, praktischen Paket weitere Funktionen für Gateway- und Endpunktsicherheit liefern, darunter Applikationskontrolle, Schutz vor Eindringlingen (Schwachstellenschutz), Endpunktverschlüsselung, Schutz vor Datenverlust (DLP) und mehr. Zusätzliche Lösungen von Trend Micro ergänzen Ihren Schutz vor komplexen Angriffen durch gezielte Untersuchungen und Endpunktforensik. Darüber hinaus ermöglicht das Netzwerk-Sandboxing von Deep Discovery eine beschleunigte Reaktion (Signatur-Updates in Echtzeit) am Endpunkt, wenn eine neue Bedrohung lokal erkannt wird. Dies gewährleistet einen schnelleren Bedrohungsschutz und verhindert die Ausbreitung von Malware. Dank zentraler Transparenz, Verwaltung und Berichterstellung kann Ihr Unternehmen diese modernen Sicherheitstechnologien ganz unkompliziert einsetzen.

Geschützte Punkte

- Physische Endpunkte
- Virtualisierte Endpunkte (Add-on)
- Windows PCs und Server
- Mac Computer
- Point of Sale (PoS)- und ATM-Endpunkte

Schutz vor Bedrohungen

- Äußerst zuverlässige maschinelle Lernverfahren (vor der Ausführung einer Datei und während der Laufzeit eines Prozesses)
- Verhaltensanalysen (von Skripts, Injection, Ransomware, Speicher- und Browser-Angriffen)
- File Reputation
- Schutz vor Bedrohungsvarianten
- Prüfung der globalen Verbreitung einer Datei
- Web Reputation
- Abwehr von Exploit-Code (Host-Firewall, Exploit-Schutz)
- Sperrung von Command-and-Control (C&C)-Kommunikation
- Schutz vor Datenverlust (DLP-Modul)
- Gerätezugriffssteuerung
- Prüfung auf bekannt harmlose Dateien
- Integration von Sandboxing und Erkennung von Datensicherheitsverstößen

Erfahren Sie, wie wir im Vergleich abschneiden

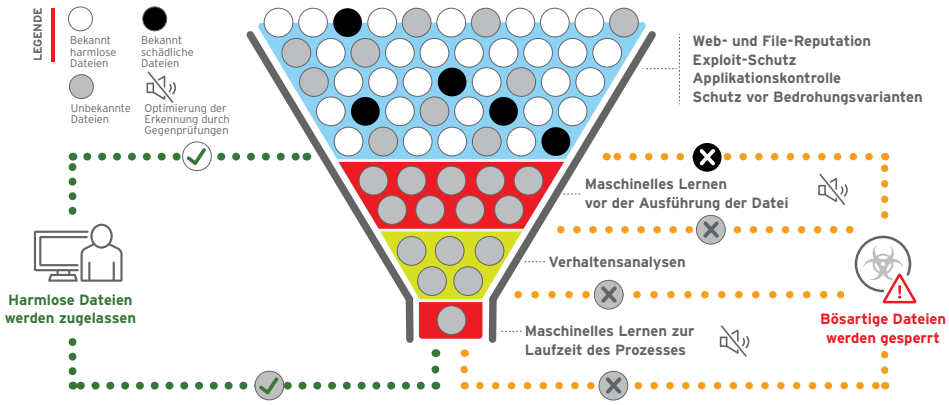
EINE LÖSUNG – ZAHLREICHE VORTEILE

- **Erweiterter Schutz vor Malware und Ransomware:** Schützt Endpunkte innerhalb und außerhalb des Unternehmensnetzwerks vor Malware, Trojanern, Würmern, Spyware und Ransomware. Treten neue Varianten auf, wird der Schutz angepasst.
- **Miteinander kommunizierende Schutzmechanismen:** OfficeScan lässt sich in andere Sicherheitsprodukte integrieren – entweder lokal in Ihrem Netzwerk oder über die globale, cloudbasierte Bedrohungserkennung von Trend Micro. Dadurch kann die Lösung schnelle Reaktionsupdates aus dem Netzwerk-Sandboxing an die Endpunkte senden, sobald eine neue Bedrohung erkannt wurde. Das ermöglicht einen schnelleren Bedrohungsschutz und verhindert die Ausbreitung von Malware.
- **Zentrale Transparenz und Kontrolle:** In Kombination mit dem Trend Micro™ Control Manager™ können mehrere OfficeScan Server über eine zentrale Konsole verwaltet werden und einen vollständigen Überblick über alle Anwenderaktivitäten liefern.
- **Integration von Mobile Security:** Über den Control Manager kann Trend Micro™ Mobile Security in OfficeScan integriert werden. So profitieren Sie von einer zentralen Verwaltung und Richtlinienverteilung über alle Endpunkte hinweg. Mobile Security umfasst einen Bedrohungsschutz für mobile Geräte, die Verwaltung mobiler Apps, Mobile Device Management (MDM) sowie Datensicherheit.

VORTEILE

Maximale XGen™ Endpoint Security

Schützt umfassend vor Ransomware und komplexen Angriffen durch die Kombination äußerst zuverlässiger maschineller Lernverfahren mit anderen Erkennungsmethoden.



- Liefert maximale Erkennungsraten ohne Fehlalarme durch kontinuierliches Filtern von Bedrohungen mithilfe der effizientesten Methode.
- Kombiniert signaturlose Methoden wie hochpräzises maschinelles Lernen, Verhaltensanalysen, Schutz vor Bedrohungsvarianten, Prüfung der globalen Verbreitung, Applikationskontrolle, Abwehr von Exploit-Code und Prüfung auf bekannt harmlose Dateien mit weiteren Methoden, einschließlich File Reputation, Web Reputation und Sperrung von C&C-Kommunikation.
- Trend Micro ist der erste Anbieter, der solche maschinellen Lernverfahren einsetzt, die Dateien nicht nur vor deren Ausführung, sondern auch während der Laufzeit analysieren. Dadurch wird eine noch präzisere Bedrohungserkennung erzielt.
- Reduziert Fehlalarme durch den Einsatz von Methoden zur Gegenprüfung, wie die Prüfung der globalen Verbreitung der Datei und Abgleiche mit Listen bekannt harmloser Dateien auf jeder Ebene.
- Ein sofortiger Austausch von Informationen über verdächtige Netzwerkaktivitäten und Dateien mit anderen Sicherheitsebenen wehrt nachfolgende Angriffe ab.
- Der erweiterte Ransomware-Schutz überwacht Endpunkte auf verdächtige Datei-verschlüsselungsaktivitäten, beendet bösartige Prozesse und kann bei Bedarf sogar verlorene Dateien wiederherstellen.

Minimale Leistungsbeeinträchtigung

Reduziert Verwaltungskosten und die Beeinträchtigung von Anwendern.

- Ressourcenschonende und optimierte Sicherheit nutzt die richtige Erkennungsmethode zur richtigen Zeit und gewährleistet damit minimale Belastungen von Geräten und Netzwerken.
- Umfassende, zentrale Transparenz der Endpunktsicherheit ermöglicht die schnelle und effiziente Analyse von Sicherheitsrisiken.
- Automatischer Austausch von Bedrohungsdaten zwischen Sicherheitsebenen bietet Schutz vor neuen Bedrohungen im gesamten Unternehmen.
- Über das Edge Relay können sich Mitarbeiter auch ohne VPN und außerhalb des Netzwerks mit OfficeScan verbinden. Dadurch können Sie die Compliance und Datensicherheit mobiler Mitarbeiter sicherstellen.
- Anpassbare Dashboards ermöglichen die Ausführung unterschiedlicher administrativer Aufgaben.
- Support rund um die Uhr gewährleistet, dass Trend Micro Ihnen bei Problemen unmittelbar mit der richtigen Lösung zur Seite steht.

Bewährter Sicherheitspartner

Trend Micro entwickelt ständig innovative Technologien, um die wirksamsten und effizientesten Sicherheitslösungen zu bieten. Wir denken stets voraus, um bereits heute die erforderlichen Technologien zur Abwehr der Bedrohungen von morgen zu liefern.

- Über 25 Jahre Erfahrung im Bereich Sicherheitsinnovationen.
- Schutz von mehr als 155 Millionen Endpunkten.
- 45 der 50 weltweit führenden Unternehmen vertrauen Trend Micro.
- Seit 2002 durchgehend führender Anbieter im „Gartner Magic Quadrant for Endpoint Protection Platforms“ und 2016 führend in der Kategorie „Umfassendste Vision“.

Die wichtigsten Unternehmensanforderungen

- Es gelangt zu viel Malware und Ransomware in das Unternehmen.
- Unternehmen brauchen eine Lösung, die sie vor allen bekannten und unbekannten Bedrohungen auf PC-Endpunkten, Macs und VDI schützt.
- Nicht kompatible Endpunkt-sicherheitslösungen behindern den Bedrohungsschutz und erhöhen den Verwaltungsaufwand.
- Mobile Mitarbeiter können ein Risiko darstellen. Sie tauschen Informationen auf neuartigen Wegen aus, zum Beispiel über die Cloud usw.
- Die IT-Effizienz ist eingeschränkt, wenn sich der erweiterte Bedrohungs- und Datenschutz nicht integrieren lässt.

> „Mein Hauptziel war, die massive Systembelastung unserer bisherigen Endpunktsicherheit zu eliminieren. Genau das hat OfficeScan geschafft. Außerdem wollte ich eine Sicherheitslösung implementieren, die wirklich funktioniert. Seitdem wir auf Trend Micro setzen, sind keine Infektionen mehr aufgetreten.“

Bruce Jamieson,
Network Systems Manager von A&W Food Services of Canada

INDIVIDUALISIEREN SIE IHREN ENDPUNKTSCHUTZ

Weiten Sie Ihre Trend Micro Endpunktsicherheit durch optionale Sicherheitsmodule und ergänzende Endpunktlösungen aus:

Modul zum Schutz vor Datenverlust (DLP, optional)

Schützt Ihre vertraulichen Daten für maximale Transparenz und Kontrolle.

- Schützt vertrauliche Daten innerhalb und außerhalb des Netzwerks, beispielsweise indem Dateien verschlüsselt werden, bevor sie Ihr Netzwerk verlassen
- Verhindert Datenabfluss über Cloud-Speicher, USB-Geräte oder verbundene Mobilgeräte, Bluetooth-Verbindungen und andere Medien
- Schützt eine Vielzahl von Geräten, Anwendungen und Dateitypen
- Unterstützt die Compliance durch mehr Transparenz und bessere Durchsetzung

Security for Mac Modul (optional)

Schützt Apple Macintosh Clients in Ihrem Netzwerk, indem der Zugriff der Clients auf bösartige Websites und die Verbreitung von Malware verhindert wird, auch wenn sie nicht auf Mac OS X Betriebssysteme abzielt.

- Reduziert die Anfälligkeit für webbasierte Bedrohungen einschließlich sich schnell verbreitender Mac-spezifischer Malware
- Bietet ein positives Anwendererlebnis durch Anlehnung an das Erscheinungsbild von Mac OS X
- Spart Zeit und Aufwand durch die zentrale Verwaltung über alle Endpunkte hinweg (einschließlich Macs)

Virtual Desktop Infrastructure (VDI) Modul (optional)

Ermöglicht die Konsolidierung Ihrer Endpunktsicherheit als Lösung für physische sowie virtuelle Desktops.

- Erkennt, ob sich ein Agent auf einem physischen oder einem virtuellen Endpunkt befindet, und kann Schutz und Leistung für seine spezifische Umgebung optimieren
- Führt Suchen und Updates nacheinander durch und vermerkt Basis-Images sowie bereits durchsuchte Inhalte in einer Whitelist, um Host-Ressourcen zu sparen

Endpoint Encryption (optional)

Schützt vertrauliche Daten zuverlässig durch Verschlüsselung der Daten auf Ihren Endpunkten (einschließlich Laptops, Macs, DVDs und USB-Laufwerken), die leicht verloren gehen oder gestohlen werden können. Trend Micro™ Endpoint Encryption stellt mit der Festplatten-, Ordner- und Dateiverschlüsselung sowie der Verschlüsselung von Wechselmedien die Datensicherheit bereit, die Sie benötigen.

- Schützt ruhende Daten mittels Software zur Festplattenverschlüsselung
- Automatisiert die Datenverwaltung mittels eigenständiger Verschlüsselung von Festplatten
- Verschlüsselt Daten in bestimmten Dateien, Freigabeordnern und auf Wechselmedien
- Legt gezielte Richtlinien zur Gerätezugriffssteuerung und Datenverwaltung fest
- Verwaltet Microsoft Bitlocker und Apple FileVault

Vulnerability Protection (optional)

Schützt Ihre physischen und virtuellen Desktops sofort vor Zero-Day-Bedrohungen, innerhalb und außerhalb des Netzwerks. Trend Micro™ Vulnerability Protection nutzt ein hostbasiertes Intrusion Prevention System (HIPS), um bekannte und unbekannte Schwachstellen abzuschirmen, bis Patches verfügbar sind und installiert werden können. Weitet den Schutz auf kritische Plattformen aus, auch auf ältere Betriebssysteme wie Windows XP.

- Eliminiert das Risiko, indem Schwachstellen mittels virtueller Patches abgeschirmt werden
- Reduziert Ausfallzeiten für Wiederherstellung und Notfall-Patching
- Ermöglicht die Installation von Patches ganz nach Ihren eigenen Bedingungen und Ihrem eigenen Zeitplan
- Identifiziert Sicherheitsschwachstellen mit Berichten zu CVE, MS-ID und Schweregrad

Endpoint Application Control (optional)

Erweitern Sie Ihren Schutz vor Malware und gezielten Angriffen, indem Sie die Installation und die Ausführung unerwünschter und unbekannter Anwendungen auf Unternehmensendpunkten verhindern.

- Schützt Benutzer und Geräte vor unwissentlicher Ausführung bösartiger Software
- Dynamische Richtlinien reduzieren den Verwaltungsaufwand und bieten mehr Flexibilität für aktive Anwenderumgebungen
- Sperrt Systeme, sodass nur die Anwendungen verwendet werden können, die in Ihrem Unternehmen zulässig sind
- Erstellt und verwaltet anhand korrelierter Bedrohungsdaten aus Milliarden von Dateien eine aktuelle Datenbank validierter, harmloser Anwendungen

Endpoint Sensor (optional)

Kontextsensitive Untersuchungen von Endpunkten und Forensikfunktionen, die Aktivitäten auf Systemebene genau protokollieren und detaillierte Berichte erstellen. So können Bedrohungsanalysten Eigenschaften und Ausmaß eines Angriffs schnell einschätzen. Die benutzerdefinierten Erkennungsfunktionen, Bedrohungsinformationen und Sicherheitskontrollen von Deep Discovery bieten Ihnen folgende Möglichkeiten:

- Erkennung und Analyse Ihrer Angreifer
- Sofortige Anpassung des Schutzes an aktuelle Angriffe
- Zeitnahe Reaktion, bevor vertrauliche Daten verloren gehen

Trend Micro™ Control Manager™ (optional)

Diese zentrale Management-Konsole sorgt für eine einheitliche Sicherheitsverwaltung, umfassende Transparenz und lückenloses Reporting über mehrere Schutzschichten ineinandergreifender Trend Micro Sicherheitslösungen hinweg. Transparenz und Kontrolle werden auch über lokale, cloudbasierte und hybride Verteilungsmodelle hinweg erweitert.

Eine zentralisierte Verwaltung in Kombination mit anwenderbasierter Transparenz erhöht den Schutz, senkt den Verwaltungsaufwand und beseitigt redundante Aufgaben in der Sicherheitsverwaltung. Control Manager bietet außerdem Zugriff auf wertvolle Bedrohungsdaten aus dem Trend Micro™ Smart Protection Network™, das globale Bedrohungsdaten nutzt, um in Echtzeit cloudbasierte Sicherheit bereitzustellen, die Bedrohungen abwehrt, noch bevor sie Ihr Netzwerk erreichen.

SYSTEMVORAUSSETZUNGEN FÜR OFFICESCAN

MINDESTVORAUSSETZUNGEN FÜR DEN SERVER

OfficeScan Serverbetriebssysteme:

- Windows Server 2008 (SP2) und 2008 R2 (SP2) (x64) Edition
- Windows Storage Server 2008 (x86/x64), Storage Server 2008 R2 (SP1) (x64) Edition
- Windows HPC Server 2008 und HPC Server 2008 R2 (x64)
- Windows MultiPoint Server 2010 (x64) und 2012 (x64)
- Windows Server 2012 und 2012 R2 (x64) Edition
- Windows MultiPoint Server 2012 (x64) Edition
- Windows Storage Server 2012 (x64) Edition
- Windows Server 2016 (x64) Edition

OfficeScan Serverplattform:

Prozessor: 1,86 GHz Intel Core 2 Duo (2 CPU-Kerne) oder besser

Arbeitsspeicher: mindestens 1 GB (2 GB empfohlen), mit mindestens 500 MB ausschließlich für OfficeScan (Windows 2008 Familie)

- Mindestens 2 GB mit mindestens 500 MB ausschließlich für OfficeScan (Windows 2010/2011/2012/2016 Familie)

Festplattenspeicher: mindestens 6,5 GB, mindestens 7 GB (bei Remote-Installation)

OfficeScan Edge Relay Serverplattform:

Prozessor: 2 GHz Intel Core 2 Duo (2 CPU-Kerne) oder besser

Arbeitsspeicher: mindestens 4 GB

Festplattenspeicher: mindestens 50 GB

Betriebssystem: Windows Server 2012 R2

Netzwerkkarte:

1. Zwei Netzwerkkarten
   - eine Karte für die Intranetverbindung mit dem OfficeScan Server
   - eine Karte für die Verbindung mit externen OfficeScan Agenten
2. Eine Netzwerkkarten-Konfiguration zur Nutzung unterschiedlicher Ports für Intranet- und Internet-verbindungen

Datenbank:

1. SQL Server 2008 R2 Express (oder höher)
2. SQL Server 2008 R2 (oder höher)

MINDESTVORAUSSETZUNGEN FÜR DEN AGENTEN

Betriebssystem des Agenten

- Windows XP (SP3) (x86) Edition
- Windows XP (SP2) (x64) (Professional Edition)
- Windows Vista (SP1/SP2) (x86/x64) Edition
- Windows 7 (mit oder ohne SP1) (x86/x64) Edition
- Windows 8 und 8.1 (x86/x64) Edition
- Windows 10 (32 und 64 Bit)
- Windows 10 IoT Embedded
- Windows Server 2003 (SP2) und 2003 R2 (x86/x64) Edition
- Windows Compute Cluster Server 2003 (aktiv/passiv)
- Windows Storage Server 2003 (SP2), Storage Server 2003 R2 (SP2) (x86/x64) Edition
- Windows Server 2008 (SP2) (x86/x64) und 2008 R2 (SP1) (x64) Edition
- Windows Storage Server 2008 (SP2) (x86/x64) und Storage Server 2008 R2 (x64) Edition
- Windows HPC Server 2008 und HPC Server 2008 R2 (x86/x64) Edition
- Windows Server 2008/2008 R2 Failover Cluster (aktiv/passiv)
- Windows MultiPoint Server 2010 und 2011 (x64)
- Windows Server 2012 und 2012 R2 (x64) Edition
- Windows Storage Server 2012 und 2012 R2 (x64) Edition
- Windows MultiPoint Server 2012 (x64) Edition
- Windows Server 2012 Failover Cluster (x64)
- Windows Server 2016 (x64) Edition
- 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 und 8.1 Embedded (x86/x64) Edition

Plattform des Agenten

Prozessor: 300 MHz Intel Pentium oder vergleichbarer Prozessor (Windows XP, 2003, 7, 8, 8.1, 10 Familie)

- Mindestens 1 GHz (2 GHz empfohlen) Intel Pentium oder vergleichbarer Prozessor (Windows Vista, Windows Embedded POS, Windows 2008 (x86) Familie)
- Mindestens 1,4 GHz (2 GHz empfohlen) Intel Pentium oder vergleichbarer Prozessor (Windows 2008 (x64), Windows 2016 Familie)

Arbeitsspeicher: mindestens 256 MB (512 MB empfohlen), mit mindestens 100 MB ausschließlich für OfficeScan (Windows XP, 2003, Windows Embedded POSReady 2009 Familie)

- Mindestens 512 MB (2 GB empfohlen), mit mindestens 100 MB ausschließlich für OfficeScan (Windows 2008, 2010, 2011, 2012 Familie)
- Mindestens 1 GB (1,5 GB empfohlen), mit mindestens 100 MB ausschließlich für OfficeScan (Windows Vista Familie)
- Mindestens 1 GB (2 GB empfohlen), mit mindestens 100 MB ausschließlich für OfficeScan (Windows 7 (x86), 8 (x86), 8.1 (x86), Windows Embedded POSReady 7 Familie)
- Mindestens 1,5 GB (2 GB empfohlen), mit mindestens 100 MB ausschließlich für OfficeScan (Windows 7 (x64), 8 (x64), 8.1 (x64) Familie)

Festplattenspeicher: Mindestens 650 MB

Ausführliche Systemvoraussetzungen finden Sie unter http://docs.trendmicro.com/de-de/home.aspx.

> „Bei einem Netzwerk wie dem unseren, das sich über das ganze Land erstreckt, reduziert der Schutz von mobilen Geräten und Desktops über eine einzige Plattform den Verwaltungsaufwand für unsere Netzwerksicherheit erheblich. Dadurch kann unser Team deutlich effizienter arbeiten."
>
> Greg Bell,
> IT Director
> DCI Donor Services

TREND MICRO™

Securing Your Journey to the Cloud