

Trend Micro™

Endpoint Security Platform

Sicherheit, Transparenz und Verwaltung in einer einzigen, hochskalierbaren Plattform

Die Verwaltung von Netzwerksystemen zur Gewährleistung von Endpunktsicherheit war noch nie so komplex. Unternehmen bemühen sich nach besten Kräften, Software zu verteilen und zu aktualisieren, Vermögenswerte zu verwalten, Verfügbarkeit zu wahren und Daten auf allen Clients und Servern zu schützen. Hinzu kommt die Herausforderung, neue technologische Trends zu verwalten, wie zum Beispiel mobile Mitarbeiter, umweltfreundliche IT-Entwicklungen, kollaborative Web-2.0-Tools und Social-Networking-Websites – und all das in einer wirtschaftlichen Situation, die Kosteneinsparungen fordert. Unternehmen sehen sich der Herausforderung gegenüber, diese Tools effizient zu nutzen, um ihre Geschäftstätigkeit zu unterstützen, und dabei ihre Endpunkte vor immer raffinierterer Malware zu schützen.

Die zunehmende Verfügbarkeit neuer, unternehmenskritischer Endpunktanwendungen hat neue Angriffswege für Malware geschaffen und macht daher Endpunkte zur am stärksten gefährdeten Stelle im Netzwerk. Die meisten Endpunktsicherheitslösungen hinken neuen Geschäftspraktiken, die in der modernen Arbeitswelt erforderlich sind, noch hinterher. In den meisten Unternehmen werden jährlich zwei Drittel der Endpunkte mit hoher Wahrscheinlichkeit mit Malware infiziert.*

Um Bedrohungen der Endpunkte abzuwehren, kombinieren Unternehmen oft Produkte zur Sicherheits- und Systemverwaltung, um ihre Verteidigung zu stärken. Aber dieses Flickwerk bietet schlechte Sichtbarkeit und Kontrolle, so dass sich die Durchsetzung von Richtlinien an allen Endpunkten verlangsamt und kein wirksamer Schutz erfolgt. Außerdem kann es Monate dauern, bis zusätzliche Produkte auf alle Unternehmensendpunkte verteilt sind, wenn sich Bedrohungen ändern oder neue Erfordernisse des Unternehmens entstehen. Durch diese Verzögerung entsteht eine kritische Sicherheitslücke, die das Unternehmen gefährdet.

SOFORTIGE SICHTBARKEIT UND KONTROLLE AN JEDEM ENDPUNKT

Trend Micro Endpoint Security Platform verringert die Komplexität, indem Rechenleistung auf die Endpunkte verteilt wird. Der dabei eingesetzte intelligente Agent verfügt über ein bisher nicht mögliches Maß an Sichtbarkeit und Kontrolle. Durch die Technologie mit einem einzelnen Server, einem einzelnen Agent und einer einzelnen Konsole kann richtlinienbasierte Endpunktverwaltung zentral gesteuert werden. Dieses leistungsstarke System vereinfacht den Schutz für große Unternehmen, verteilte Umgebungen und sogar für externe Mitarbeiter – unabhängig von der Art der Verbindung. Für Unternehmen bedeutet dies entscheidende Vorteile bezüglich Schnelligkeit, Flexibilität und Skalierbarkeit, während die Kosten für Infrastruktur und Wartung in Verbindung mit herkömmlicher System- und Sicherheitsverwaltung reduziert werden.

DAMIT IHRE SICHERHEIT MIT IHREM UNTERNEHMEN WÄCHST

Endpoint Security Platform bildet die Basis der Lösung und erzeugt ein einheitliches System zur Sicherheits- und Systemverwaltung. Unternehmen können die Lösung dann anpassen, indem sie die speziellen Plattformmodule auswählen, die ihre jeweiligen Endpunktumgebungen unterstützen. Gewünschte Funktionen für die Sicherheits- und Systemverwaltung können einfach auf alle Endpunkte verteilt werden. Wenn sich Bedrohungen dann weiterentwickeln oder neue Erfordernisse des Unternehmens entstehen, lassen sich neue Module schnell verteilen – und die Implementierung auf allen Endpunkten erfordert nicht mehr Wochen oder Monate, sondern nur noch Tage oder sogar Stunden. Mit einer hochskalierbaren Architektur, die bis zu 250.000 Benutzer auf einem Verwaltungsserver unterstützt, können Systemverwaltungs- und Sicherheitsteams mit Endpoint Security Platform souverän und präzise ihre Endpunkte zentral schützen, Komplexität und Risiko reduzieren und Kosten sparen.

SOFTWARE

Geschützte Punkte

- Clients
- Server
- Laptops

Schutz vor Bedrohungen

- Virenschutz
- Anti-Spyware
- Anti-Rootkit
- Schutz vor Internet-Bedrohungen
- Sicherheitspatches
- Datenverlust

ENTSCHEIDENDE VORTEILE

Liefert weitreichende Sichtbarkeit und Kontrolle

- Bietet unternehmensweite Sichtbarkeit sowohl bezüglich Sicherheit als auch Abläufe
- Verwaltet mobile Computer transparent unabhängig von Netzwerk- oder Internet-Verbindung

Macht Schutz schneller verfügbar

- Verkürzt Verwaltungsaktionen von Wochen und Monaten auf Tage und Stunden
- Verteilt neuen Schutz schnell durch modulare Architektur

Erhöht die Verwaltungseffizienz

- Unterstützt Unternehmen bei der Einhaltung von Service Level Agreements und behördlichen Auflagen
- Reduziert die Anzahl von Tools sowie Lizenzkosten durch Servicekonsolidierung

* Osterman Research. Eine webbasierte Client-Architektur bietet mehr Sicherheit bei weniger Kosten. Januar 2009

FUNKTIONSMERKMALE DER ENDPOINT SECURITY PLATFORM

Endpoint Security Platform Agent

- Verwendet einen einzelnen Mehrzweck-Agent, der über einen zentralen Server eine robuste, verteilte und intelligente Infrastruktur steuert
- Bietet in Echtzeit und ohne Unterbrechung Schutz, Richtlinienverarbeitung, Wiederherstellung, Validierung und Berichterstellung
- Benötigt nur 2 bis 4 MB des Endpunkt-Systemspeichers und weniger als 2 % des Host-Prozessors
- Setzt Richtlinien sogar auf externen Geräten außerhalb des Unternehmensnetzwerks durch
- Unterstützt spontane Anfragen und Verwaltungsaktionen mit verschlüsselter Kommunikation zwischen Agent und Server

Endpoint Security Platform Server

- Verwaltet mehr als 250.000 Endpunkte auf einem Verwaltungsserver
- Hostet die Management-Konsole mit Funktionen für Richtlinien und integrierten Tools zur Berichterstellung und Analyse
- Unterstützt die automatische Synchronisierung mehrerer Server und Rund-um-die-Uhr-Service selbst im Störfall
- Verwendet eine integrierte Sicherheitsinfrastruktur zur Veröffentlichung von Richtlinien und gesammelten Daten
- Erstellt Konfigurationsstandards und Grundlagen für festgelegte Gruppen verwalteter Clients

Endpoint Security Platform Richtliniennachrichten

- Übertragen Informationen zwischen Agents und Serverumgebungen
- Ermöglichen einfache Skripte zur Richtlinienerstellung und die Verwendung logischer Kriterien zum Auslösen bestimmter Aktionen
- Geben Unternehmen die Flexibilität, vorgegebene Richtlinien auszuwählen oder eigene Richtlinien anzupassen
- Bieten eine sichere Authentifizierung und Prüfungskette

Endpoint Security Platform Relays

- Stellen Kommunikations- und Sammelpunkte dar, insbesondere für Richtliniennachrichten und gepatchte oder wiederhergestellte Daten
- Ermöglichen die Überwachung von Aufgaben, wie beispielsweise Aufdeckung von Vermögenswerten, Malware-Suche, Download von Patches usw. auf allen Computern ohne zusätzliche Beeinträchtigung des Hosts
- Reduzieren die Anforderungen an die Netzwerkbandbreite und bieten Plattformredundanz
- Unterstützen Geräte unabhängig von Standort oder Netzwerkzuverlässigkeit
- Maximieren Netzwerkressourcen mit Funktionen zum Zwischenspeichern, Beenden und Neustarten von Client-Updates

ENDPOINT SECURITY PLATFORM MODULE

Kernschutzmodul

- Bietet ein umfassendes Paket mit Funktionen zur Abwehr und Entfernung von Malware, einschließlich Schutz vor Spyware
- Sperrt den Zugriff von Benutzern und Anwendungen auf bösartige Webinhalte
- Stellt die neuen Technologien File Reputation und Web Reputation von Trend Micro im innovativen Smart Protection Network mit webbasierter Client-Architektur bereit
- Verlagert Malware-Signatordateien und Bewertungen der Web Reputation ins Internet, um die Update-Verwaltung zu reduzieren und den Endpunkt zu entlasten
- Verwendet webbasierte Bedrohungsinformationen zum sofortigen Schutz ohne verteilte Updates

Webschutzmodul

- Nutzt Web Reputation im innovativen Smart Protection Network
- Sperrt den Zugriff von Benutzern und Anwendungen auf bösartige Webinhalte in Echtzeit

Patch-Verwaltungsmodul

- Liefert Patch-Funktionen für diverse Betriebssysteme und eine Vielzahl von Software
- Gewährleistet Beibehaltung der Funktionalität auch für Netzwerke mit niedriger Bandbreite oder weltweit verteilte Netzwerke und erhöht dadurch die Erfolgsrate, Patches bereits im ersten Durchlauf zu übernehmen
- Bietet Sichtbarkeit in Echtzeit zur Gewährleistung eines aktuellen Schutzes mit detaillierten Berichten zu Patch-Verteilung und -Installation

Modul zum Schutz vor Datenlecks

- Schützt Vermögenswerte in Daten vor versehentlichem Verlust oder Diebstahl und gewährleistet Schutz und Integrität vertraulicher Daten
- Kombiniert endpunktbasierte Richtlinienumsetzung mit hochpräziser Technologie zur Authentizitätsprüfung und Abgleich von Inhalten

SYSTEMVORAUSSETZUNGEN

System- und Servervoraussetzungen

- Unterstützte Betriebssysteme für den Endpoint Security Platform Verwaltungsserver
 - Windows 2000 Server SP 2+/2003/2008
- Datenbankvoraussetzungen für den Endpoint Security Platform Verwaltungsserver
 - SQL Server 2000 SP4/2005
- Unterstützte Betriebssysteme für die Endpoint Security Platform Konsole
- Eine der folgenden Möglichkeiten:
 - Windows XP/2000/2003 Vista/2008

