PRODUKT GUIDE

Trend Micro

Produkte
Service & Support

XGen™ Security

WHAT'S YOUR X? Lösen Sie es mit Trend Micro.

XGen™

ist mehr als Next-Gen

Ihr Kontakt zu Trend Micro:

TREND MICRO Deutschland GmbH
Zeppelinstraße 1 • 85399 Hallbergmoos
Tel: +49 811 88990-700 • Fax: +49 811 88990-799

TREND MICRO (Schweiz) GmbH
Husacherstrasse 3 • CH-8304 Wallisellen
Tel: +41 43 233 77 81

www.trendmicro.com

Ihr kostenfreier* Kontakt zu TREND MICRO:
D: 0800 330 4533 oder sales_info@trendmicro.de
AT: 0800 880 903 oder sales_info@trendmicro.at
CH: 0800 330 453 oder sales_info@trendmicro.ch

* Kostenfrei aus dem Festnetz des jeweiligen Landes. Abweichende Gebühren aus dem Mobilfunknetz.

INHALT

Management

Eva Chen
CEO

Wael Mohamed
President

Mahendra Negi
CFO

Akihiko Omikawa
Executive Vice President für
Japan und globales Verbrauchergeschäft

Kevin Simzer
Executive Vice President für
Vertrieb und Marketing

Oscar Chang
Executive Vice President
für Forschung und Entwicklung

Max Cheng
Executive Vice President Core Technology und CIO

Steve Quane
Executive Vice President,
Network Defense and Hybrid Cloud Security

Unsere Vision

Eine Welt ohne Gefahren beim Austausch digitaler Daten

In modernen Unternehmen sind Daten zum größten strategischen Wert geworden, da sie Wettbewerbsvorteile fördern und optimierte Betriebsabläufe ermöglichen. Mit dem sprunghaften Anstieg bei der Nutzung von mobilen Geräten, sozialen Netzwerken und Cloud-Technologien stellt der Schutz dieser Daten eine immer größere Herausforderung dar.

Als weltweit führender Anbieter von Sicherheitssoftware und -lösungen hat Trend Micro das Ziel, eine sichere Welt für den Austausch digitaler Daten zu schaffen. Seit über 25 Jahren schützen unsere Lösungen Einzelpersonen, Familien, Unternehmen und Behörden, während sie das Potenzial moderner Technologien und neuer Methoden zum Datenaustausch ausschöpfen.

Börsengehandelt:
Tokyoter Börse 4704

Gegründet:
1988 in den Vereinigten Staaten

Hauptsitz:
Tokyo, Japan

Eva Chen
CEO

Unsere Mission

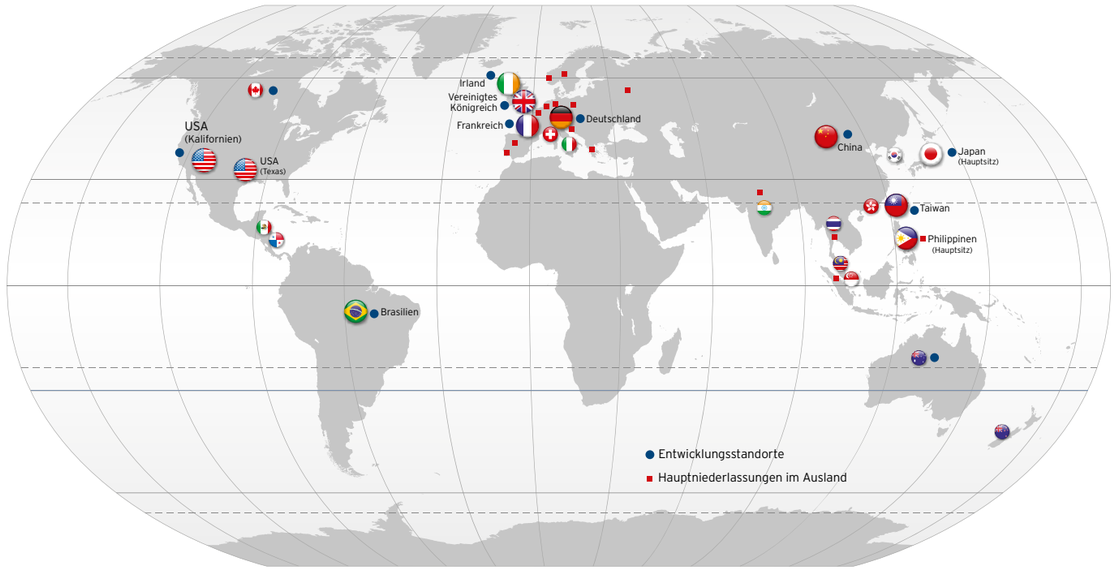
Optimale Lösungen durch kontinuierliche Innovationen

Lösungen von Trend Micro bieten mehrschichtigen Schutz für Anwender und digitale Inhalte, sei es auf mobilen Geräten, Endpunkten, Servern, an Gateways oder in der Cloud. Die innovativen Sicherheitslösungen lassen sich einfach verteilen und verwalten und fügen sich nahtlos in sich ständig wandelnde Umgebungen ein. Unsere Mission ist die kontinuierliche Innovation, um auf Veränderungen schnell mit optimalen Lösungen reagieren zu können.

Für eine sorgenfreie Sicherheit – über Landesgrenzen hinweg

Trend Micro wurde 1988 in Kalifornien (USA) gegründet. Seitdem wächst das Unternehmen mit Sitz in Tokyo stetig und wurde zu einem weltweit agierenden Unternehmen. Mit Standorten auf der ganzen Welt hat Trend Micro ein Netzwerk geschaffen, das Bedrohungen global und regional kontinuierlich überwacht, um Kunden entsprechende Lösungen schnell bereitzustellen.

Das weltweite Trend Micro Netzwerk



TrendLabs Philippines ist zur Einhaltung der IT-Servicequalität seiner Malware-Informationen, der Erkennung / Säuberung und des technischen Supportservices nach ISO 20000-1 2005 zertifiziert.

Hauptsitz	Japan										
TrendLabs (regional)	Deutschland	Philippinen (Hauptsitz)	USA	Japan	Taiwan	Irland	China	Frankreich	Vereinigtes Königreich	Brasilien	
Entwicklungsstandorte	Deutschland	USA	Kanada	Japan	Vereinigtes Königreich	Taiwan	China	Australien	Irland	Frankreich	Brasilien
Niederlassungen	Deutschland	USA	Irland	China	Taiwan	Frankreich	Kanada	Thailand	Malaysia	Singapur	
	Schweiz	China (Hongkong)	Indien	Korea	Italien	Vereinigtes Königreich	Australien	Mexiko	Neuseeland	Brasilien	

02 XGEN™ SECURITY

Die Antwort auf die ständig wachsende IT- und Bedrohungslandschaft

XGen™ Security

Während einige Anbieter der sogenannten „nächsten Generation" ausschließlich auf eine einzige Methode wie zum Beispiel Verhaltensanalyse oder maschinelles Lernen setzen, sind wir bei Trend Micro davon überzeugt, dass es kein Wundermittel gibt, um Unternehmen vor der gesamten Palette bekannter und unbekannter Bedrohungen zu schützen. Ihr Unternehmen braucht eine gesamtheitliche Lösung, um die Sicherheits-Probleme zu bewältigen.

XGen™ Security nutzt bewährte Methoden, um die große Menge an bekannt harmlosen oder schädlichen Dateien zu erkennen. Mithilfe fortschrittlicherer Technologien können dann unbekannte Bedrohungen schneller und präziser identifiziert werden. Standortunabhängige Erkennung in einem vernetzten System und die umgehende Anwendung der richtigen Abwehrtechnologie zum richtigen Zeitpunkt sorgen für maximale Transparenz und Performance. Diese Kerntechnologien unterstützen alle Trend Micro Lösungen – jeweils optimiert für die entsprechende Schutzschicht: hybride Cloud-, Netzwerk- und Anwenderumgebungen.

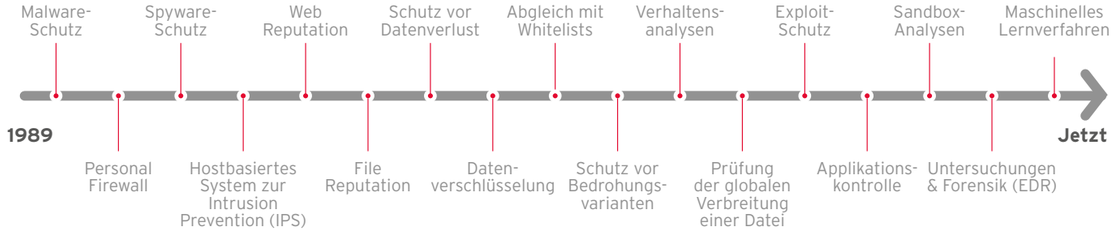
Maximale Sicherheit bei minimaler Systembeeinträchtigung

Trend Micro bietet intelligente, optimierte und miteinander kommunizierende Schutzmechanismen – alle unterstützt durch XGen™ Security. Mit der generationsübergreifenden Kombination aus Technologien zur Bedrohungsabwehr profitieren Unternehmen in der heutigen dynamischen Bedrohungslandschaft von maximaler Sicherheit bei minimaler Systembeeinträchtigung.

Trend Micro: Vorreiter im Bereich IT-Sicherheit

155 Millionen Endpunkte. Mehr als 5.000 Experten weltweit. Seit fast 30 Jahren verfolgt Trend Micro seine Vision, eine sichere Welt für den Austausch digitaler Daten zu ermöglichen. Sicherheit steht bei uns im Mittelpunkt. Und das merkt man. Diese konzentrierte Leidenschaft hat zu Innovationen geführt, die mit der sich wandelnden IT-Landschaft, riskanterem Benutzerverhalten und sich ständig verändernden Bedrohungen Schritt halten. Dabei bieten wir eine unerreichte Expertise: Wir schützen Sie vom Endpunkt über das Netzwerk bis in die Cloud – durch miteinander kommunizierende Schutzmechanismen,die von Analysten, Kunden und Branchenexperten gleichermaßen geschätzt werden.

Innovative und zeitnahe Reaktionen auf die dynamische Bedrohungslandschaft von heute



Intelligent

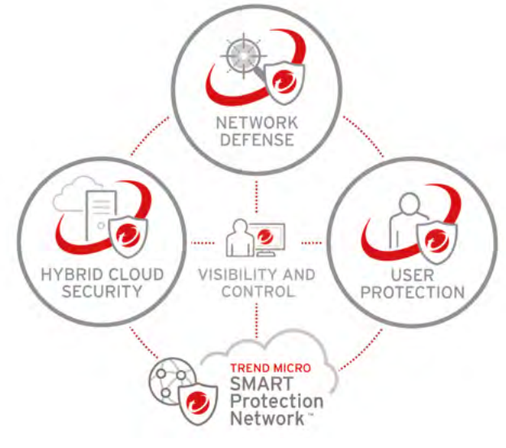
Durch eine einzigartige Kombination aus verschiedenen Technologien und marktführenden, globalen Bedrohungsinformationen sorgen die Lösungen für maximalen Schutz.

Optimiert

Die Lösungen lassen sich nahtlos in führende Kundenplattformen und -anwendungen auf Endpunkten, in Netzwerken, Rechenzentren und der Cloud integrieren und minimieren so den IT-Aufwand.

Vernetzt

Zentrale Transparenz und Kontrolle sowie der automatische Austausch von Bedrohungsinformationen über Sicherheitsebenen, Endpunkte, Netzwerke, Rechenzentren und die Cloud verkürzen die Reaktionszeit.



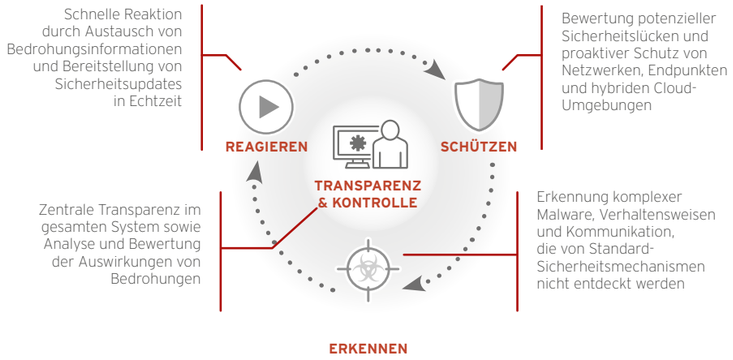
XGEN™ SECURITY

Die Antwort auf die ständig wachsende IT- und Bedrohungslandschaft

Connected Threat Defense

Optimierter Schutz vor neuen Bedrohungen

Trend Micro Connected Threat Defense ist ein mehrschichtiger Sicherheitsansatz, mit dem Sie neue und gezielte Bedrohungen besser und schneller erkennen, verhindern und darauf reagieren können. Gleichzeitig bietet der Ansatz mehr Transparenz und Kontrolle im gesamten Unternehmensnetzwerk.



Connected Threat Defense in Aktion

Im Folgenden ist die Funktionsweise bei einem Connected Threat Defense Ansatz beispielhaft beschrieben:

• Der Angriff beginnt mit dem Eingang einer E-Mail im Postfach eines Benutzers. Diese E-Mail enthält einen Anhang mit einer Zero-Day-Bedrohung*, die es auf das Entwenden von Informationen abgesehen hat. Die Bedrohung könnte in der Schutzphase von einer der vielen erweiterten Scan-Technologien gestoppt werden.
• Die Zero-Day-Bedrohung wurde jedoch so programmiert, dass sie traditionelle Techniken umgeht. Deshalb kommt hier die Erkennungsphase ins Spiel. Die Messaging-Ebene sendet den Anhang an die Sandbox, die die Datei als bösartig identifiziert und darüber hinaus C&CKommunikation feststellt.
• Nach der Analyse einer komplexen Bedrohung erfolgt die Reaktion in Form von Echtzeitsignaturen, die nach der Erstellung sofort an alle Endpunkte und Gateway-Sicherheitskomponenten weitergeleitet werden. Geschieht dies nicht, wird die Bedrohung beim nächsten Auftreten nicht automatisch abgewehrtund das Risiko multipliziert sich. In dieser Phase erfolgt auch die Beseitigung, bei der automatisch alle Malware-Instanzen von den Computern entfernt werden. Dadurch wird die Anwenderproduktivität maximiert.

Vorteile

Besserer Schutz vor komplexen Bedrohungen
- Verbesserte Transparenz von Angriffen und Bedrohungen in allen Netzwerken, Endpunkten und hybriden Cloud-Umgebungen
- Automatische Identifizierung von neuen Bedrohungen, die bei benutzerdefiniertem Sandboxing und Netzwerkanalysen entdeckt wurden
- Schnelle Reaktion und Bereitstellung von Sicherheitsupdates über mehrere Schutzebenen hinweg

POWERED BY XGen™ SECURITY

* Unter „Zero Day Bedrohung" versteht man allgemein eine Bedrohung die zum Zeitpunkt Ihres Eintretens noch unbekannt ist bzw. geeignete Gegenmaßnahmen noch nicht entwickelt wurden. Der Verteitiger hatte deshalb Null (Zero) Tage Zeit sich auf die Bedrohung vorzubereiten.

Schutzquadrant

Der Schutzquadrant schützt Ihre Netzwerke, Endpunkte und hybriden Cloud-Umgebungen proaktiv. Keine einzelne Technik kann vor allen Bedrohungsarten schützen. Deshalb garantiert der Einsatz unterschiedlicher Technologien den zuverlässigsten Bedrohungsschutz.
Die Lösungen von Trend Micro beinhalten viele Sicherheitstechnologien wie Malware-Schutz, Verhaltensüberwachung, Intrusion Prevention, Whitelists, Applikationskontrolle, Verschlüsselung und Schutz vor Datenverlust.

Erkennungsquadrant

Trotz der Stärke seiner Technologien kann der Schutzquadrant nicht jede Malware oder jeden Angriff abwehren. Daher nutzt der Erkennungsquadrant Verfahren, mit denen Sie komplexe Malware, bösartiges Verhalten und bösartige Kommunikation identifizieren können, die den Standardabwehrmaßnahmen verborgen bleiben. Dieser Quadrant ist besonders effektiv bei der Erkennung von Zero-Day-Angriffen, Command-and-Control-Kommunikation (C&C) und komplexen, zielgerichteten Bedrohungen.

Überwachung des Netzwerks

Das umfassende Monitoring des Netzwerkverkehrs überprüft mehr als 100 Protokolle im gesamten Netzwerk auf verdächtige Aktivitäten, C&C-Kommunikation und die laterale Ausbreitung von eingehender, ausgehender und interner Netzwerkkommunikation, sodass Sie sehen können, was im Netzwerk vor sich geht, um schließlich entsprechende Abwehrmaßnahmen ergreifen zu können.

Benutzerdefiniertes Sandboxing

Entdeckt eine der Techniken des Schutzquadranten etwas Verdächtiges, wird dieses Element automatisch in eine benutzerdefinierte, virtuelle Sandbox gesendet. Da die Sandbox Ihre Systemkonfigurationen widerspiegelt, um eine präzise Analyse zu gewährleisten, können Sie die Erkennung optimieren. Wenn der verdächtige Inhalt sicher ausgeführt wird, können Sie dessen potenzielle Auswirkungen bewerten und feststellen, ob er tatsächlich bösartig ist.

Reaktionsquadrant

Nach der Erkennung und/oder Abwehr einer Bedrohung müssen Sie in der Lage sein, schnell zu reagieren.
Die Reaktionsphase liefert den anderen Quadranten Echtzeitsignaturen und Sicherheitsupdates, um zukünftige Angriffe zu verhindern, die Ursache zu identifizieren und deren Beseitigung zu beschleunigen. Dieser Quadrant setzt auf eine schnelle Reaktion, die auf den Erkenntnissen des Erkennungsquadranten basiert. Wird beim Sandboxing eine Bedrohung, eine bösartige Datei oder C&C-Datenverkehr identifiziert, muss Ihre Sicherheitslösung eine Echtzeitsignatur für diese Datei bzw. den C&C-Server erstellen und diese umgehend an alle Endpunkte und Gateway-Sicherheitskomponenten weiterleiten. Wenn ein solcher Angriff oder eine solche Bedrohung dann das nächste Mal auftritt, erfolgt die automatische Abwehr dann bereits im Schutzquadranten.

Der Reaktionsquadrant umfasst Folgendes:
- Schnelle Reaktion
  Wenn in diesem Quadranten ein Angriff entdeckt wird, werden gezielte Informationen zu bösartigen Dateien, IP-Adressen und C&C-Kommunikation mit dem Schutzquadranten geteilt, um Echtzeitschutz bereitzustellen. Werden diese Objekte das nächste Mal entdeckt, können sie automatisch gesperrt werden. So kommen die Vorteile von Connected Threat Defense optimal zum Einsatz.
- Beseitigung
  Um die Produktivität zu maximieren, ist eine automatische Beseitigung von dateibasierter Malware, Netzwerkviren und den Rückständen von dateibasierter Malware und Würmern auf Ihren Computern erforderlich.
- Transparenz und Kontrolle
  Es ist wichtig, Techniken einzusetzen, die den gesamten Lebenszyklus einer Bedrohung abdecken. Gleichzeitig müssen diese Techniken in einer einzelnen Lösung mit zentraler Verwaltung und Berichterstellung integriert und koordiniert sein, in der alle Komponenten Hand in Hand arbeiten. Durch die Integration können die verschiedenen Sicherheitsebenen Informationen austauschen und Ihnen einen konsolidierten Überblick über die Aktivitäten in Ihrem Netzwerk liefern. Die zentrale Transparenz über alle Sicherheitsebenen hinweg bietet einen umfassenden Überblick über die Sicherheit von Netzwerken, Endpunkten und hybriden Cloud-Umgebungen. Dies vereinfacht sowohl die Untersuchung von Angriffen als auch die tagtäglichen Verwaltungsaufgaben. Dank der anwenderspezifischen Transparenz können Sie nachvollziehen, wie sich Bedrohungen, die auf bestimmte Benutzer ausgerichtet sind, über unterschiedliche Übertragungswege, Geräte und Anwendungen ausbreiten. Ein visuelles Dashboard liefert eine Echtzeitübersicht über wichtige Performance-Metriken sowie Priorisierungsindikatoren für eine einfachere und effektivere Sicherheitsverwaltung. Die wichtigste Konstante besteht darin, die Bedrohungslandschaft regelmäßig zu bewerten und Ihre Sicherheitskontrollen an die neuesten Taktiken, Techniken und Verfahren der Angreifer anzupassen. Connected Threat Defense wurde entwickelt, da das traditionelle Sicherheitsmodell angesichts der heutigen Angriffe und Bedrohungen ausgedient hat. Dieser neue Ansatz ermöglicht Unternehmen, von den neuesten und fortschrittlichsten Schutzmaßnahmen zu profitieren, die über Netzwerke, Endpunkte und hybride Cloud- Umgebungen hinweg integriert und koordiniert werden. Zudem erhalten Sie die nötige Kontrolle und Transparenz, um Angriffe schnell zu identifizieren und auszuhebeln.

ZERO DAY INITIATIVE

Bug-Bounty-Programm fördert verantwortungsvolle Offenlegung von Schwachstellen

Zero Day Initiative

Weltweit größtes, herstellerneutrales Bug-Bounty-Programm fördert verantwortungsvolle Offenlegung von Schwachstellen

In der Informationssicherheitsbranche werden Schwachstellenforscher teilweise noch immer für bösartige Hacker gehalten, die Schäden anrichten wollen. Zweifelsohne gibt es dort draußen begabte bösartige Hacker. Sie machen jedoch nur eine sehr kleine Minderheit der großen Anzahl von Menschen aus, die neue Sicherheitslücken in Software aufspüren. Eine große Gruppe bilden hingegen wohlmeinende Forscher mit dem nötigen Fachwissen, die bei ihrer täglichen Sicherheitsarbeit immer wieder Schwachstellen entdecken. Hierzu schreibt Gartner: „IPS Anbieter sollten über F&E-Fähigkeiten verfügen, um primäre Bedrohungen, Schwachstellen und weitere Bedrohungen zu erforschen. Hierbei handelt es sich um eine wichtige Unterstützungsfunktion, die es Anbietern erlaubt, die Mechanismen bei der Ausnutzung von Schwachstellen vollständig zu verstehen und so Bedrohungen für Ihr Unternehmen sinnvoll abzuwehren. Eine Methode zur Beurteilung von Anbietern ist deren Fähigkeit, Bedrohungsfilter bereitzustellen noch bevor überhaupt eine Schwachstelle ausgenutzt werden kann. Dies muss mit Investitionen in die Forschung einhergehen.“[1] TippingPoint verfügt mit den Digital Vaccine® Labs (DVLabs) bereits über eine der weltweit führenden Organisationen für die Sicherheitsforschung. Trotzdem erschien es sinnvoll, DVLabs zu erweitern und zusätzliche Erkenntnisse zu Zero-Day-Bedrohungen aus einem globalen Netzwerk unabhängiger Forscher einzubinden. Aus diesem Gedanken heraus entstand die am 25. Juli 2005 ins Leben gerufene Zero Day Initiative (ZDI). Die Zero Day Initiative (ZDI) war wegweisend auf dem „weißen Markt“ für Schwachstellen. Ihr Ziel war es, den Schwarzmarkt zu sprengen, indem sie die Ergebnisse der Schwachstellenforschung rechtmäßig erwarb und den betroffenen Anbietern bereitstellte. Schwachstellen werden vom Markt genommen und sind für eine etwaige missbräuchliche Verwendung nicht mehr verfügbar. Die betroffenen Anbieter können die Schwachstelle dann beheben, bevor die zugehörige Information veröffentlicht wird. Die ZDI ermöglicht die koordinierte, an ein Bonusprogramm gekoppelte Meldung an die betroffenen Anbieter, um unerwartete Angriffe auf Unternehmensumgebungen zu verhindern.

Die wichtigsten Ziele der ZDI

- Erweiterung unserer internen Forschungsteams durch Nutzung der Methoden, Fachkompetenz und Zeit anderer Experten
- Förderung der verantwortungsvollen Meldung von Zero-Day-Schwachstellen an die betroffenen Anbieter, indem Forscher durch Bonusprogramme finanziell entlohnt werden
- Schutz von Trend Micro/TippingPoint-Kunden, während der betroffene Anbieter an einem Patch arbeitet

DER WEISSE MARKT

Bug-Bounty-Programme, Hacking-Contests und die direkte Kommunikation mit Anbietern bieten Möglichkeiten für eine verantwortungsbewusste Offenlegung.

DER GRAUE MARKT

Einige seriöse Unternehmen arbeiten in einer rechtlichen Grauzone innerhalb des Zero-Day-Marktes und verkaufen Exploits an Regierungen und Strafverfolgungsbehörden in Ländern auf der ganzen Welt.

DER SCHWARZMARKT

Sicherheitslücken werden an den höchsten Bieter verkauft. Nicht selten führt das zu Angriffen auf Privatpersonen, öffentliche Einrichtungen und Gruppen.

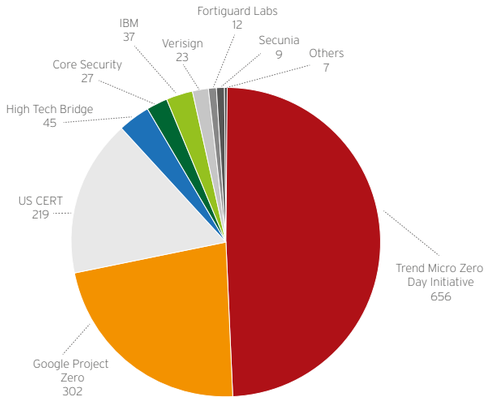
Fakten

- 2005 gegründet
- Weltweit über 3.000 Forscher
- Seit Gründung mehr als 3.500 Schwachstellen entdeckt und veröffentlicht
- Bis heute über 15 Mio. US-Dollar an Forscher gezahlt
- Seit 2007 die Nummer 1 bei der weltweiten Erforschung und Aufdeckung von Schwachstellen[2]

ZDI-Statistiken 2016

- Bei 22 % der öffentlich entdeckten Schwachstellen von Microsoft gewürdigt
- Führend bei der Meldung von Codefehlern an Microsoft
- Bei 28 % der öffentlich entdeckten Schwachstellen von Adobe gewürdigt
- Führend bei der Meldung von Codefehlern an Adobe
- 678 Schwachstellen veröffentlicht
- Mehr als 2 Mio. US-Dollar an Forscher gezahlt

Öffentlicher Markt für Schwachstellenforschung: Gemeldete Schwachstellen nach Institution, global 2015



Die Nummer 1 bei der weltweiten Erforschung und Aufdeckung von Schwachstellen

Seit dem Jahr 2007 stuft Frost & Sullivan die Zero Day Initiative von Trend Micro (damals noch TippingPoint) als die weltweit führende Organisation für die Erforschung von Schwachstellen ein. Frost & Sullivan erfasst jedes Jahr öffentliche Daten zu Schwachstellen, um die zuverlässigsten Anbieter im Bereich der Schwachstellenbekämpfung und die zuverlässigsten Forschungsorganisationen zu ermitteln. Der dabei erstellte Bericht enthält Informationen zu Softwareschwachstellen und den Organisationen, die sie offenlegen.

WIE FUNKTIONIERT DAS?

Die Zero Day Initiative führt intern eigene Forschungen durch, während die externe Forschungsgemeinschaft weiterhin eine wertvolle Bereicherung für das Programm darstellt.

Welchen Vorteil haben Trend Micro Kunden von der Zero Day Initiative?

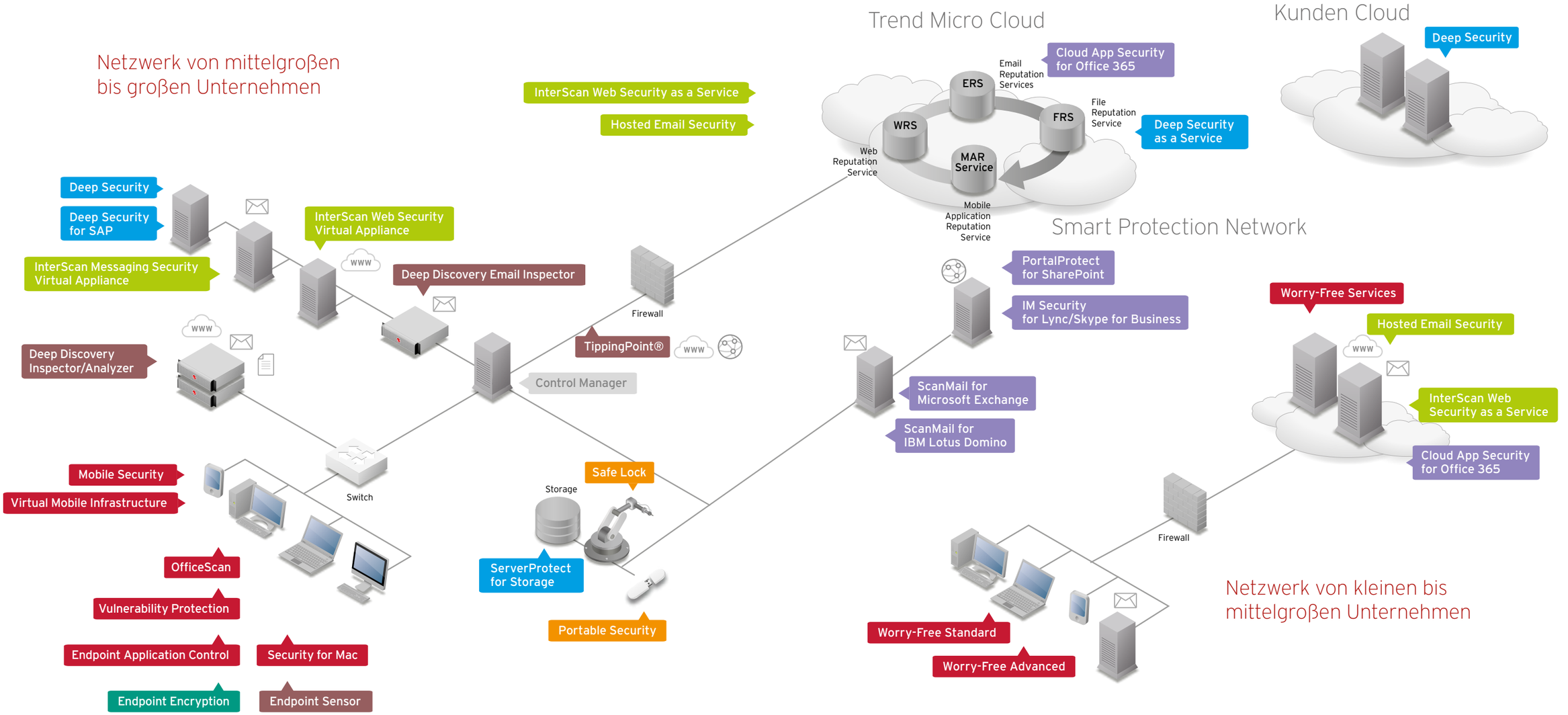
Das Schwachstellenerforschungs- und Bug-Bounty-Programm der Zero Day Initiative führt letztendlich zu sichereren Produkten und besser geschützten Kunden. Ohne die Zero Day Initiative würden viele Schwachstellen weiterhin unveröffentlicht bleiben oder auf dem Schwarzmarkt verkauft und für heimtückische Zwecke verwendet werden. Bevor der Anbieter einen Patch bereitstellt, verfügen Kunden bereits über einen präventiven Schutz, da sie exklusiven Zugang zu Schwachstelleninformationen haben, die an die Zero Day Initiative gemeldet wurden. Ferner erhalten sie einen Schutz für nicht mehr unterstützte ältere Software. Dank unserer langjährigen Beziehungen zu führenden Softwareanbietern und zur Forschungsgemeinschaft werden wir auch künftig auf die Sicherheit im Produktentwicklungszyklus Einfluss nehmen.

1 Gartner, Inc. „Defining Intrusion Detection and Prevention Systems.“ 20. September 2016.
2 Frost & Sullivan. „Analysis of the Global Public Vulnerability Research Market, 2015.“ Oktober 2016.
3 Uhley, Peleus. „Reflections on Pwn2Own.“ Security @ Adobe (Blog), 16. April 2016, http://blogs.adobe.com/security/2016/04/reflections-on-pwn2own.html.

04 LÖSUNGSÜBERSICHT

Positionierung im Netzwerk

Trend Micro fokussiert sich konsequent auf die Entwicklung von Sicherheitslösungen. Das umfangreiche Portfolio beinhaltet Lösungen zum Schutz des gesamten Unternehmens, von Mobilgeräten bis hin zu Rechenzentren und der Cloud. Als führender* Anbieter von Server- und Virtualisierungssicherheit unterstützt Trend Micro Ihre Kunden optimal bei der Umsetzung von Cloud- und Virtualisierungsprojekten. Darüber hinaus bieten wir Lösungen für die Herausforderungen, die durch zielgerichtete Angriffe, Compliance-Anforderungen und BYOD an Ihre Kunden gestellt werden. Zusätzlich profitieren Unternehmen von reduziertem Betriebs- und Managementaufwand der IT-Sicherheit.



* Quelle: Digital Transformation, Experton, 2016; Server Security, IDC, 2016; Security, Experton, 2016

Stand September 2017

04 LÖSUNGSÜBERSICHT

Leistungsumfang

Kategorie	Lösung	Erkennen von			Analyse
		Eintritts-punkten	C&C Verbindungen	internen Verbrei-tungen	bekannter Bedrohungen
Cyber Threat Security	Deep Discovery Inspector	●	●	●	●
	Deep Discovery Analyzer	●●	●		●
	Deep Discovery Email Inspector	●	●		●
	Endpoint Sensor	●	●	●	●
Schutz vor gezielten Angriffen/ATP	TippingPoint® Threat Protection System	●	●	●	●
	TippingPoint® Next-Generation Intrusion Prevention System NX Series	●	●	●	●

Kategorie	Lösung	Malware-schutz	Web Reputation	Firewall	IDS/IPS
Cloud & Data Center Security	Deep Security	●	●	●	●
	Deep Security as a Service	●	●	●	●
	Deep Security for SAP Systems	●	●	●	●
	ServerProtect for Linux	●			
	ServerProtect for NetApp/EMC Celerra/Hitachi/IBM/HP	●			

Kategorie	Lösung	Malware-schutz	Web Reputation	Spam-Schutz	Phishing-Schutz
Email & Collaboration	Cloud App Security for Office 365	●	●		●
	InterScan Messaging Security	●	●	●	●
	PortalProtect for Microsoft SharePoint	●	●		●
	IM Security for Lync and Skype for Business	●	●		●
	ScanMail for Microsoft Exchange	●	●	●	●
	ScanMail for IBM Lotus Domino	●	●	●	●
	Hosted Email Security	●	●	●	●
	Deep Discovery Email Inspector	●	●		●

Kategorie	Lösung	Malware-schutz	Web Reputation	URL Filter	Phishing-Schutz
Web Gateway	InterScan Web Security Virtual Appliance	●	●	●	●
	InterScan Web Security as a Service	●	●	●	●

Lösung	Analyse		Bereitstellung von		Reaktion
	unbekannter Bedrohungen	Sandbox Analyse	„Suspicious Objects“ (z.B. über Blacklist)	„Indicator of Compromise“ Informatonen	Blocken
Deep Discovery Inspector	●	●	●	●	●
Deep Discovery Analyzer	●	●	●	●	●●
Deep Discovery Email Inspector	●	●	●	●	●
Endpoint Sensor	●	●●	●●	●	
TippingPoint® Threat Protection System	●●	●●			●
TippingPoint® Next-Generation Intrusion Prevention System NX Series	●●	●●			●

Lösung	File Integrity Monitoring	Protokoll-überwachung	Virtual Desktop Infrastructure	agentenloser Schutz	Erhalten von Suspicious Objects / Connected Threat Defense	Sandbox Analyse
Deep Security	●	●	●	●	●●	●●
Deep Security as a Service	●	●	●			
Deep Security for SAP Systems	●	●				
ServerProtect for Linux						
ServerProtect for NetApp/EMC Celerra/Hitachi/IBM/HP						

Lösung	Data Loss Prevention	Social Enginee-ring Attack Protection	E-Mail-Verschlüsselung	Sandbox Analyse	Erhalten von Suspicious Objects / Connected Threat Defense	Business Email Compromise
Cloud App Security for Office 365	●			●		
InterScan Messaging Security	●	●	●	●●	●●	
PortalProtect for Microsoft SharePoint	●					
IM Security for Lync and Skype for Business	●					
ScanMail for Microsoft Exchange	●			●●	●●	
ScanMail for IBM Lotus Domino	●			●●	●●	
Hosted Email Security		●	●	●	●	●
Deep Discovery Email Inspector		●		●	●	

Lösung	Data Loss Prevention	Applikations-kontrolle	HTTPS/ SSL	Sandbox Analyse	Erhalten von Suspicious Objects / Connected Threat Defense	Machine Learning
InterScan Web Security Virtual Appliance	●	●	●	●●	●●	
InterScan Web Security as a Service		●	●	●		●

"●●" zusätzliches Produkt erforderlich | "○" eingeschränkter Funktionsumfang | Stand September 2017

04 LÖSUNGSÜBERSICHT

Leistungsumfang

Kategorie	Lösung	Malware-schutz	Web Reputation	Firewall	Machine Learning	IDS/IPS	Appli-kations-kontrolle
Endpoint Protection	OfficeScan	●	●	●	●	○	
	Endpoint Application Control						●
	Endpoint Encryption						
	Vulnerability Protection			●		●	
	Security for Mac	●	●				
	Portable Security	●					
	Safe Lock					○	●
	Integrated Data Loss Prevention						

Kategorie	Suite	Malware-schutz	Web Reputation	Firewall	Machine Learning	IDS/IPS	Appli-kations-kontrolle
Security Suites	Smart Protection Complete	●	●	●	●	●	●
	Smart Protection for Endpoints	●	●	●	●	●	●
	Enterprise Security Suite	●	●	●	●	●	
	Enterprise Security for Endpoints & Mail Servers	●	●	●	●	●	
	Enterprise Security for Endpoints	●	●	●	●	●	
	Enterprise Security for Endpoints Light	●	●	●	●		

Kategorie	Lösung	Malware-schutz	Web Reputation	Firewall	Machine Learning	URL Filter	Spam-Schutz
Small Business	Worry-Free Advanced	●	●	●	●	●	●
	Worry-Free Standard	●	●	●	●	●	
	Worry-Free Services	●	●	●	●	●	
	Worry-Free Services Advanced	●	●	●	●	●	●
	Cloud App Security for Office 365	●	●				

Kategorie	Lösung	Malware-schutz	Jail-break-Erkennung	Passwort-vorgabe	Selective Remote Wipe	Remote Locate/Lock	Appli-kations-kontrolle
Mobile Security	Mobile Security	●	●	●	●	●	●
	Virtual Mobile Infrastructure						●

Lösung	Data Loss Prevention	Sandbox Analyse	Geräte-steuerung	File/Folder/ Full-Disk-Ver-schlüsselung	System Lock-down	Erhalten von Suspicious Objects / Connec-ted Threat Defense	Integritäts-über-wachung
OfficeScan	○	●●	○			●●	
Endpoint Application Control					●	●●	
Endpoint Encryption				●			
Vulnerability Protection							
Security for Mac							
Portable Security							
Safe Lock			○		●		○
Integrated Data Loss Prevention	●		●				

Suite	Data Loss Prevention	Sandbox Analyse	Geräte-steuerung	Endpunkt-Verschlüsselung	Mobile Sicherheit	Optimierung VDI-Umgebungen	Mail-Filter	Web-Filter
Smart Protection Complete	●	●●	●	●	●	●	●	●
Smart Protection for Endpoints	●	●●	●	●	●	●		
Enterprise Security Suite		●●	○		○	●	●	●
Enterprise Security for Endpoints & Mail Servers		●●	○		○	●	●	
Enterprise Security for Endpoints		●●	○		○	●		
Enterprise Security for Endpoints Light		●●	○					

Lösung	Data Loss Prevention	Sandbox Analyse	Geräte-steuerung	Phishing-Schutz	Schutz für Mac	Mobile Sicherheit
Worry-Free Advanced	●		○		●	○
Worry-Free Standard			○		●	
Worry-Free Services			○		●	○
Worry-Free Services Advanced	●		○		●	○
Cloud App Security for Office 365	●	●				

Lösung	Virtual Mobile Infrastructure	Trennung von priv. u. geschäftl. Daten	3rd Party MDM Integ-ration	Verschlüsselung
Mobile Security			●	●
Virtual Mobile Infrastructure	●	●		

"●●" zusätzliches Produkt erforderlich | "○" eingeschränkter Funktionsumfang | Stand September 2017

Smart Protection for Endpoints

Trend Micro™ Smart Protection for Endpoints mit XGen™ Endpoint Security kombiniert ein äußerst zuverlässiges maschinelles Lernverfahren mit einer Reihe verschiedener Technologien zum Bedrohungsschutz, um Sicherheitslücken bei sämtlichen Anwenderaktivitäten und auf allen Endpunkten zu verhindern. Die Lösung lernt anhand von Bedrohungsdaten kontinuierlich hinzu, adaptiert diese Daten nach Bedarf und verbreitet sie automatisch über Ihre gesamte Umgebung hinweg. Darüber hinaus können Sie ganz flexibel zwischen einer lokal installierten oder cloudbasierten Lösung sowie einer Kombination beider Möglichkeiten wählen. Der wichtigste Vorteil liegt jedoch darin, dass Sie Anwenderaktionen unabhängig von Gerätetyp, Übertragungsweg der Bedrohungen und Installationsmodell von einer zentralen, transparenten Stelle aus verwalten können. So haben Sie die Sicherheit Ihrer Umgebung jederzeit vollständig im Blick. Mit über 25 Jahren Erfahrung im Bereich Sicherheitsinnovationen ist Trend Micro Ihr zuverlässiger Partner im Kampf gegen die Bedrohungen von heute und von morgen.

Vorteile

- Verhindert, dass Ransomware die Endpunkte verschlüsselt
- Schützt die IT vor Zero-Day Malware mithilfe signaturloser Technologien
- Gewinnt die Kontrolle über die IT-Umgebung Ihrer Endanwender zurück, indem Bedrohungsschutz und Datensicherheit zentralisiert wird
- Minimiert Risiken durch eine beliebige Kombination aus proaktivem, cloudbasiertem Schutz in Echtzeit.
- Zentrale, Nutzerzentrierte Verwaltung über SaaS- und On-Premise-Lösungen
  - Optimale Flexibilität bei Installationsmodellen bietet nahtlose Unterstützung der sich ständig ändernden Kombination aus lokal installierter und cloud-basierter Sicherheit.
- 24 / 7 Direkt-Support
  - Support rund um die Uhr stellt sicher, dass Trend Micro Ihnen bei Problemen unmittelbar mit der richtigen Lösung zur Seite steht.

Umfassender Schutz für Endpoints

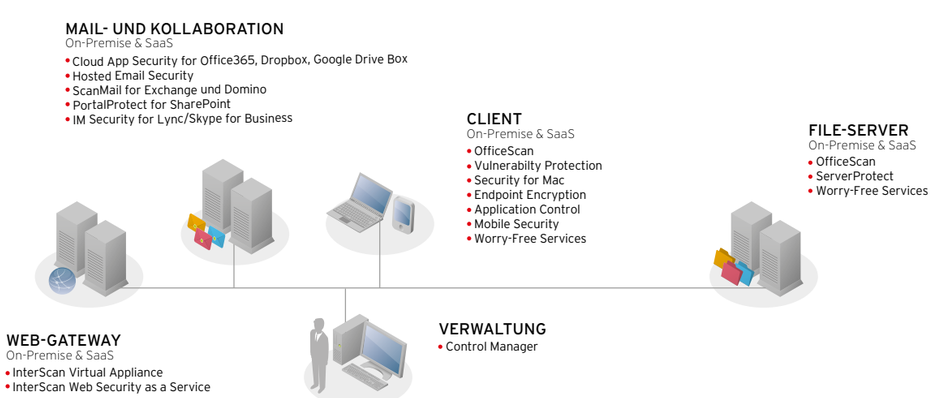
MEHRSCHICHTIGER SCHUTZ	PLATTFORMABDECKUNG	VORTEIL
ZENTRALE VERWALTUNG		
Control Manager	Software: Windows	Zentrale Sicherheitsverwaltung
ENDPUNKTSICHERHEIT		
OfficeScan	Software: Windows, Apple Macintosh	Schutz physischer und virtueller Windows- und Mac-Clients
Virtual Desktop Integration	VMware View, Citrix XenDesktop, Microsoft Hyper-V	Optimiert den Schutz von OfficeScan in virtuellen Desktop-Umgebungen
Worry-Free Services	Cloud-basierte Software as a Service	Schutz von Windows Server und Desktops, Mac-, iOS und Android Clients
Vulnerability Protection	Software: Windows Client Betriebssysteme	Proaktives HIPS und virtuelles Patching
Endpoint Application Control	Software: Windows	Whitelisting und Systemsperre
Endpoint Encryption	PCs, Laptops, CDs, DVDs und USB	Gerätesteuerung, Daten- und Schlüsselverwaltung
Server Protect	Software: Windows, Linux Server	Schutz physischer und virtueller Windows- und Linux-Server
MOBILE SICHERHEIT		
Mobile Security	iOS, Android, Windows Phone	MDM, Datensicherheit, mobile Sicherheit und Anwendungsverwaltung
INTEGRIERTE DATENSICHERHEIT		
Data Loss Prevention	Funktionserweiterung für OfficeScan	Unternehmensweite Durchsetzung von DLP-Richtlinien, sowie Erweiterung der Gerätesteuerung

Smart Protection Complete Suite

Trend Micro™ Smart Protection Complete ist eine Lösung aus ineinandergreifenden Sicherheitsfunktionen, die Anwender standortunabhängig bei allen Aktionen schützen. Diese moderne Sicherheitslösung liefert den besten mehrschichtigen Schutz auf Endpunkt-, Anwendungs- und Netzwerkebene und damit eine umfassende Bedrohungsabwehr im gesamten Unternehmen. Die zentrale Komponente der Suite ist XGen™ Endpoint Security, die ein äußerst zuverlässiges maschinelles Lernverfahren mit einer Reihe unterschiedlicher Technologien zum Bedrohungsschutz kombiniert, um Sicherheitsrisiken bei sämtlichen Anwenderaktivitäten zu minimieren. Weiterhin können Sie Ihren Schutz zusammen mit Ihrem Unternehmen ausbauen, indem Sie lokal installierte, cloudbasierte oder hybride Bereitstellungsmodelle flexibel anwenden, damit Ihre IT-Umgebung heute und in Zukunft sicher bleibt. Die Verwaltung erfolgt unabhängig vom Übertragungsweg der Bedrohungen über eine zentrale Stelle, die vollständige Transparenz bietet. Damit wird der administrative Aufwand minimiert und Sie haben die Sicherheit Ihrer Umgebung jederzeit vollständig im Blick. Diese umfassende Suite kombiniert Sicherheitsmodule auf verschiedenen Ebenen mit flexibler Cloud-Installation, vereinfachter Lizenzierung und zentraler Verwaltung zur netzwerkweiten Transparenz und Kontrolle über Bedrohungen und Daten.

Vorteile

- Verhindert, dass Ransomware die Endpunkte verschlüsselt.
- Schützt die IT vor Zero-Day Malware mithilfe signaturloser Technologien.
- Senkt den Verwaltungsaufwand und Gesamtbetriebskosten
- 24 / 7 Direkt-Support
- Umfassender Schutz für Office365, Dropbox, mobile Geräte, Desktops, Server, Mail-& Kollaborationsserver sowie Mail-& Web-Gateway
- Zentrale, Nutzerzentrierte Verwaltung über SaaS- und On-Premise-Lösungen



Umfassender Schutz für das gesamte Netzwerk

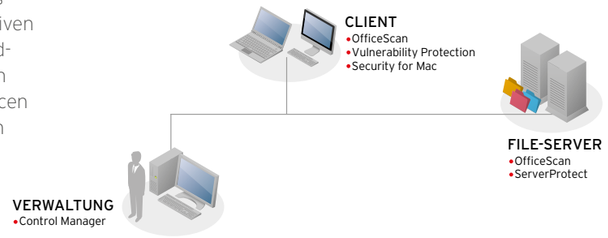
MEHRSCHICHTIGER SCHUTZ	PLATTFORMABDECKUNG	VORTEIL
ZENTRALE VERWALTUNG		
Control Manager	Software: Windows	Zentrale Sicherheitsverwaltung
ENDPUNKTSICHERHEIT		
OfficeScan	Software: Windows, Apple Macintosh	Schutz physischer und virtueller Windows- und Mac-Clients
Virtual Desktop Integration	VMware View, Citrix XenDesktop, Microsoft Hyper-V	Optimiert den Schutz von OfficeScan in virtuellen Desktop-Umgebungen
Vulnerability Protection	Software: Windows Client Betriebssysteme	Proaktives HIPS und virtuelles Patching
Endpoint Application Control	Software: Windows	Whitelisting und Systemsperre
Endpoint Encryption	PCs, Laptops, CDs, DVDs und USB	Gerätesteuerung, Daten- und Schlüsselverwaltung
Server Protect	Software: Windows, Linux Server	Schutz physischer und virtueller Windows- und Linux-Server
Worry-Free Services	Cloud-basierte Software as a Service	Schutz von Windows Server und Desktops, Mac-, iOS und Android Clients
MOBILE SICHERHEIT		
Mobile Security	iOS, Android, Windows Phone	MDM, Datensicherheit, mobile Sicherheit und Anwendungsverwaltung
EMAIL- UND KOLLABORATIONSSICHERHEIT		
Cloud App Security	Cloud-basierte SaaS	Schutz für Office365, Dropbox, Google Drive Box, u.a. mit Hilfe von Malware-Schutz, DLP, Sandbox-Analyse
InterScan Messaging Security	• Virtuelle Software-Appliance: VMware, Hyper-V, Software-Appliance • Software: Windows, Linux	Schutz des E-Mail-Gateways vor Spam und anderen E-Mail-Bedrohungen
ScanMail Suite for Microsoft Exchange	Software: Windows	Sperrung von Spam, Malware und anderen E-Mail-Bedrohungen am Mail-Server
ScanMail Suite for Lotus Domino	• Software: Windows, Linux für x86, IBM AIX, IBM i5 OS, Sun • Solaris™, Linux on IBM® zSeries, IBM z/OS	Sperrung von Spam, Malware und anderen E-Mail-Bedrohungen am Mail-Server
Hosted Email Security	Cloud-basierte SaaS	Permanent aktueller Schutz vor Spam und Malware, bevor sie Ihr Netzwerk erreichen
PortalProtect for Microsoft SharePoint	Software: Windows	Schutz Ihrer Zusammenarbeit in SharePoint
IM Security for Microsoft Lync/ Skype for Business	Software: Windows	Schutz von IM-Kommunikationen
SICHERES INTERNET-GATEWAY		
InterScan Web Security Virtual Appliance	• Virtuelle Software-Appliance: VMware, Hyper-V, Software-Appliance	Schutz des Internet-Gateways vor Internetbedrohungen/URL-Filter
InterScan Web Security as a Service	Cloud-basierte SaaS	Schutz des Internet-Gateways für Geräte außerhalb des Unternehmensnetzwerks
INTEGRIERTE DATENSICHERHEIT		
Data Loss Prevention	Funktionserweiterung für OfficeScan, InterScan Messaging, InterScan Web, ScanMail, PortalProtect, IM Security	Unternehmensweite Durchsetzung von DLP-Richtlinien

Enterprise Security for Endpoints / Enterprise Security for Endpoints Light

Trend Micro Enterprise Security for Endpoints kombiniert integrierte Komponenten für Bedrohungsschutz und Datensicherheit mit den Kostenvorteilen schnellerer Suchläufe und optimierter Leistung. Mit der ineinander greifenden Abwehr auf Desktops, Laptops und Servern können Sie den Endpunktschutz in einer zentral verwalteten Lösung konsolidieren und die Verwaltungskosten senken – mit dem branchenweit proaktivsten Schutz vor den Bedrohungen von heute. Schützen Sie Desktops, Laptops, Server und Smartphones innerhalb und außerhalb des Netzwerks mit einer innovativen Kombination aus erstklassigem Malware-Schutz und cloud-basiertem Schutz durch das Trend Micro Smart Protection Network. Neue File Reputation entlastet Endpunktressourcen durch cloud-basierte Pattern-Dateien und Web Reputation blockiert den Zugriff auf bösartige Websites.

Vorteile

- Sofortiger Schutz
- Niedrigere Geschäftsrisiken
- Umfassende Sicherheit
- Geringere IT-Kosten
- Erweiterbare Architektur



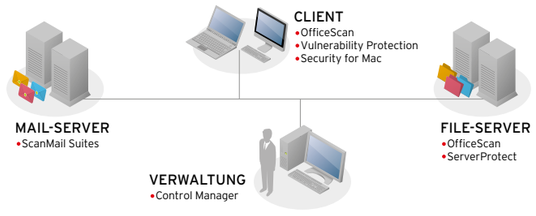
Übersicht	OfficeScan	OfficeScan Plug-ins: Vulnerability Protection	OfficeScan Plug-ins: Security for Mac	OfficeScan Plug-ins: VDI	OfficeScan Plug-ins: Mobile Sicherheit	ServerProtect for Windows, NetWare, Linux	Trend Micro Control Manager
Enterprise Security for Endpoints Light	●					●	Standard
Enterprise Security for Endpoints	●	●	●	●	●	●	Advanced

Enterprise Security for Endpoints and Mail Servers

Enterprise Security for Endpoints and Mail Servers schützt Ihr Unternehmen und Ihre Mitarbeiter durch integrierten, leistungsstarken Bedrohungsschutz und Datensicherheit, kombiniert mit den Kostenvorteilen einer optimierten Leistung und einheitlichen Verwaltung. Unterstützt durch die Cloud-Client-Architektur des Trend Micro™ Smart Protection Network™ bieten E-Mail-, File- und Web-Reputation-Technologien durch eine globale Bedrohungsabwehr sofortigen Schutz für Ihr Unternehmen. Die cloudbasierte Sicherheit von Trend Micro verlagert Pattern-Dateien von Ihren Endpunkten in die Cloud, um Computerressourcen zu entlasten und die Leistung zu verbessern. Maximaler Schutz und minimale Komplexität für Mail- und File-Server, Clients und mobile Endgeräte. Schützen Sie Ihre Mail-Server, File-Server, Desktop-PCs und Laptops mit einer einzigen integrierten Lösung vor Malware, Spyware, Spam, Phishing, unerwünschten Inhalten und komplexen Bedrohungen.

Vorteile

- Maximiert den Schutz
- Senkt Kosten
- Minimiert die Komplexität
- Zentralisiert die Richtlinienverwaltung von Sicherheitslösungen für Endpunkte und Mail-Server sowie anderen Trend Micro Sicherheitsprodukten
- Koordiniert Richtlinien für integrierten Schutz vor Datenverlust in Sicherheitslösungen für Endpunkte, Messaging-Gateways und Mail-Server
- Maximiert den Einblick durch konsolidierte Berichterstattung und fortschrittliche Bedrohungsstatistiken



Maximaler Schutz für Endpunkte und Mail-Server

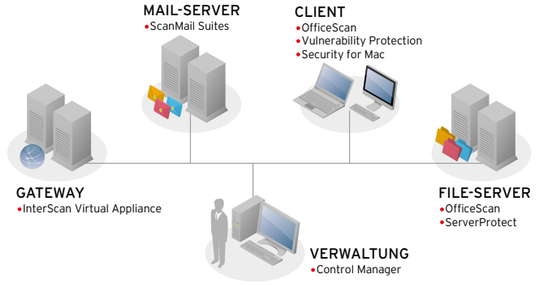
MEHRSCHICHTIGER SCHUTZ	PLATTFORMABDECKUNG	VORTEIL
MAIL-SERVER		
ScanMail Suite for Microsoft Exchange	Windows	Stoppt Spam und Spyware am Mail-Server
ScanMail Suite for IBM® Domino	Windows, Linux	Stoppt Spam und Spyware am Mail-Server
FILE-SERVER		
OfficeScan	Windows	Schützt Windows Server
ServerProtect for Windows / Novell NetWare	Windows, NetWare	Schützt Windows und NetWare File-Server
ServerProtect for Linux	Linux	Schützt Linux File-Server
CLIENT / MOBILES ENDGERÄT		
OfficeScan	Windows	Schützt Windows Clients
Vulnerability Protection	Windows	Proaktives HIPS und Abschirmung von Schwachstellen
Security for Mac	Apple Macintosh	Schützt Macintosh Clients vor Malware und blockiert bösartige Websites
Virtual Desktop Integration	VMware View, Citrix XenDesktop, Microsoft Hyper-V	Optimiert den Schutz von OfficeScan in virtuellen Desktop-Umgebungen
Mobile Sicherheit	Android, iOS, Windows Phone und andere	Schützt mobile Endgeräte wie Smartphones und Tablets
VERWALTUNG		
Control Manager Advanced	Windows	Zentrale Sicherheitsverwaltung

Enterprise Security Suite

Enterprise Security Suite bietet Ihnen hervorragend aufeinander abgestimmte Sicherheitsprodukte für Ihr gesamtes Netzwerk. Mit adaptivem Bedrohungsschutz und Datensicherheit behalten Sie den Überblick über den Transfer von Daten, ohne ausgebremst zu werden. Schützen Sie Ihr Internet-Gateway sowie Ihre Mail- und File- Server, Desktops, Laptops und mobilen Endgeräte mit dieser vollständig integrierten, zentral verwalteten Sicherheitslösung. Die Lösung bietet einen mehrschichtigen, bestmöglichen Schutz vor Malware, Spyware, Spam und komplexen Bedrohungen, einschließlich webbasierter Angriffe.
Durch den umfassenden Schutz, einschließlich Funktionen wie Virtualisierungsunterstützung, flexiblen Konfigurationsoptionen, hoher Skalierbarkeit und breiter Plattformunterstützung, minimiert die Enterprise Security Suite die Komplexität und senkt Kosten.

Vorteile

- Maximiert den Schutz
  - Reduziert das Risiko durch umfangreichen, mehrschichtigen Schutz vor vielfältigen Bedrohungen
  - Bietet sofortigen Schutz durch webbasierte Bedrohungsdaten
  - Erhöht die Produktivität durch branchenführende Spam-Abwehr und Web-Filter
- Senkt Kosten
  - Reduziert die Infektionsraten an Endpunkten
  - Senkt die Verwaltungskosten für die IT-Sicherheit
- Minimiert die Komplexität
  - Reduziert die Zeit für den Erwerb, die Installation und die Verwaltung durch eine integrierte Lösung
  - Vereinfacht die Administration durch eine webbasierte, zentrale Verwaltung



05 USER PROTECTION

05.1 Sicherheitssuiten

Maximaler Schutz und minimale Komplexität für alle geschützten Punkte und Plattformen

MEHRSCHICHTIGER SCHUTZ	PLATTFORMABDECKUNG	VORTEIL
GATEWAY		
InterScan Messaging Security Virtual Appliance	VMware oder Software Appliance	Virtualisierte E-Mail-Gateway-Sicherheit stoppt Spam und E-Mail-Bedrohungen
InterScan Web Security Virtual Appliance	VMWare, Hyper-V oder Software Appliance	Virtualisierte Internet-Gateway-Sicherheit stoppt Internetbedrohungen und filtert URLs
MAIL-SERVER		
ScanMail Suite for Microsoft Exchange	Windows	Stoppt Spam und Spyware am Mail-Server
ScanMail Suite for IBM® Domino	Windows, Linux	Stoppt Spam und Spyware am Mail-Server
FILE-SERVER		
OfficeScan	Windows	Schützt Windows Server
ServerProtect for Windows / Novell NetWare	Windows, NetWare	Schützt Windows und NetWare File-Server
ServerProtect for Linux	Linux	Schützt Linux File-Server
CLIENT / MOBILES ENDGERÄT		
OfficeScan	Windows	Schützt Windows Clients
Vulnerability Protection	Windows	Proaktives HIPS und Abschirmung von Schwachstellen
Security for Mac	Apple Macintosh	Schützt Macintosh Clients vor Malware und blockiert bösartige Websites
Virtual Desktop Integration	VMware View, Citrix XenDesktop, Microsoft Hyper-V	Optimiert den Schutz von OfficeScan in virtuellen Desktop-Umgebungen
Mobile Sicherheit	Android, iOS, Windows Phone und andere	Schützt mobile Endgeräte, wie Smartphones und Tablets
VERWALTUNG		
Control Manager Advanced	Windows	Zentrale Sicherheitsverwaltung

Enterprise Security for Gateways

Schützen Sie Ihre vertraulichen Daten sowie Ihre Mitarbeiter beim Umgang mit vielfältigen Internetinhalten. Trend Micro Enterprise Security for Gateways integriert eine virtualisierte Sicherheit für Internet- und Messaging Gateways. Die Lösung maximiert nachweislich den Schutz, minimiert den Aufwand und senkt die Gesamtkosten um bis zu 40 %.* Die cloud-basierte Web und E-Mail Reputation in Kombination mit branchenführendem Spam- und Antimalware sowie URL-Filter bieten eine mehrschichtige Multi-Threat-Abwehr, die Malware, Links zu bösartigen Websites und unerwünschte Inhalte blockiert, bevor diese in das Netzwerk eindringen können. Mit Reports in Echtzeit erhalten Sie einen beispiellosen Einblick in aktuelle Internetaktivitäten, um leichtsinniges Verhalten sofort zu unterbinden. Filter für ausgehende Inhalte sowie E-Mail-Verschlüsselung schützen vertrauliche Daten und unterstützen die Einhaltung von gesetzlichen Compliance-Richtlinien für eine umfassende Gateway-Sicherheit.

Vorteile

- Stoppt Spam, Phishing, Malware und unerwünschte E-Mail-Inhalte
- Nutzen der cloudbasierten E-Mail-, Web- und File-Bedrohungsdaten aus dem Smart Protection Network, um Bedrohungen zu stoppen, bevor sie das Netzwerk erreichen
- Verbessert die Auslastung vorhandener Server, verringert Wildwuchs und Energiekosten
- Optimiert die Leistung und vereinfacht die Verwaltung mit VMware Ready-zertifizierten Appliances
- Unterstützt die heterogene Verteilung auf die bevorzugte Hardware
- Zentralisiert die Protokollierung, Berichterstellung und Verwaltung für mehrere InterScan Web Security Server
- Verbessert den Schutz durch sofortiges Eingreifen bei riskanten Internetaktivitäten

* Osterman Research, Warum Sie Virtualisierung in Betracht ziehen sollten, Februar 2009

Maximaler Schutz und minimaler Aufwand am Gateway

MEHRSCHICHTIGER SCHUTZ	VORTEIL
GATEWAY	
InterScan Messaging Security Virtual Appliance	Virtualisierte E-Mail-Gateway-Sicherheit stoppt Spam, Phishing und E-Mail-Bedrohungen
InterScan Web Security Virtual Appliance	Virtualisierte Internet-Gateway-Sicherheit sperrt Internetbedrohungen und filtert URLs

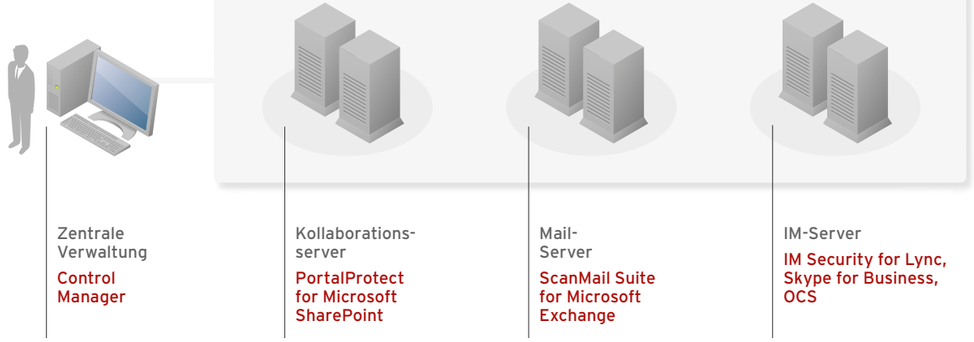
Enterprise Security for Communication and Collaboration

Als erster Anbieter von Sicherheitslösungen für Microsoft Exchange und SharePoint bietet Trend Micro einzigartigen Schutz für Ihre Microsoft Mailserver, Kollaborationssysteme und IM-Umgebungen. Die Enterprise Security for Communication and Collaboration Suite baut ein leistungsstarkes Schutzsystem auf und ermöglicht dabei eine erhebliche Verringerung des IT-Administrationsaufwands. Trend Micro Communication & Collaboration Security schützt Microsoft E-Mail-, Kollaborations- und IM-Systeme durch die Abwehr von Bedrohungen in Echtzeit, bevor diese angreifen können. Die einzigartige Cloud-Client-Architektur des Trend Micro Smart Protection Network bietet verschiedene Sicherheitsfunktionen (z. B. durch E-Mail und Web Reputation) zum Schutz vor Bedrohungen in Echtzeit, die mit führenden konventionellen Content-Sicherheitstechnologien zusammenarbeiten, damit Sie ohne ein erhöhtes Sicherheitsrisiko in Verbindung treten können.

Vorteile

- Reduziert das Risiko durch umfangreichen, mehrschichtigen Schutz vor vielfältigen Bedrohungen
- Die cloudbasierte Sicherheit des Smart Protection Network bietet sofortigen Schutz und unterstützt sowohl lokal installierte als auch gehostete Sicherheitslösungen, indem sie Bedrohungsdaten aus Internet, E-Mails und Dateien miteinander in Beziehung setzt
- Senkt Endpunktinfektionsraten
- Bietet unternehmensweite Transparenz im Bereich Bedrohungsschutz und Datensicherheit, um Ihr Unternehmen wirksam vor gezielten Angriffen und Datenverlust zu schützen

Communication & Collaboration Security



Enterprise Security for Communication and Collaboration bietet proaktiven Schutz für Microsoft E-Mail-, Instant-Messaging- und SharePoint-Systeme. Sie können Ihren Schutz einfach erweitern, indem Sie zusätzliche Datenschutzschichten in Form einer gehosteten oder Gateway-basierten Lösung für Messaging-Sicherheit, Datenschutz und E-Mail-Verschlüsselung hinzufügen.

- Data Privacy and Email Encryption Modul für InterScan Messaging Security
  Datenschutz und E-Mail-Verschlüsselung am E-Mail-Gateway verhindert den Verlust von Daten
- Hosted Email Security
  Stoppt Spam und E-Mail-basierte Malware mit kontinuierlich aktualisiertem Schutz in der Cloud
- Data Loss Prevention Modul für ScanMail for Microsoft Exchange
  Der Datenschutz für E-Mails verhindert Datenverlust am Mailserver
- Email Encryption
  Verschlüsselt E-Mails auf gehosteten, Gateway- und endpunktbasierten E-Mail-Lösungen

OfficeScan – Virtuelle Desktop Integration

Trend Micro Virtual Desktop Security eignet sich speziell für Umgebungen mit virtuellen Desktops. Die Lösung maximiert den Schutz für eine Vielzahl von Szenarien mit virtuellen Desktops.

Vorteile

- VDI-optimierte Agenten
- Verhindert Ressourcenkonflikte
- Bereinigt, scannt den Arbeitsspeicher und überwacht das Verhalten
- Erkennt automatisch, ob sich ein Agent auf einem physischen oder virtuellen Endpunkt befindet
- Verkürzt die Suchzeit auf virtuellen Desktops durch Whitelisting von Standard-Images und vorab durchsuchten Inhalten

Vulnerability Protection / Intrusion Defense Firewall

Trend Micro™ Vulnerability Protection bietet schnellere, leistungsstärkere Endpunktsicherheit, indem es den Schutz Ihrer Desktopgeräte vor Malware und Bedrohungen um proaktives virtuelles Patching ergänzt. Eine leistungsstarke Engine überwacht den Datenverkehr auf neue, spezifische Schwachstellen mithilfe hostbasierter Intrusion Prevention System (IPS)-Filter zur Abwehr von Eindringlingen sowie zum Schutz vor Zero-Day-Angriffen. So können Sie leicht Netzwerkprotokollabweichungen oder Richtlinienverstöße und verdächtige Inhalte erkennen, die auf einen Angriff hindeuten. Vulnerability Protection schirmt diese Schwachstellen gegen Angriffe ab, indem über einfache und schnell zu verteilende Filter umfassender Schutz bereitgestellt wird, bis Patches verfügbar sind und installiert werden können. In Kombination mit weiteren Endpunktlösungen von Trend Micro bietet Vulnerability Protection die branchenweit größte Bandbreite an Lösungen zum Schutz von Endpunkten, unabhängig davon, ob diese innerhalb des Netzwerks, mobil oder remote eingesetzt werden. Erweiterter Schutz von Schwachstellen auf Endpunkten. Sorgen Sie dafür, dass Ihre Endpunkte abgeschirmt bleiben, bis Patches verteilt werden können – oder bei nicht unterstützter Software bzw. nicht patchbaren Systemen gar auf unbestimmte Zeit. Wir helfen Ihnen dabei, Schwachstellen über einfache und schnell zu verteilende Filter vor Angriffen abzuschirmen. So bleiben Sie geschützt, bis Sie entsprechende Patches zu einem Zeitpunkt verteilen können, der für Ihr Unternehmen am sinnvollsten erscheint.

Vorteile

- Schützt Endpunkte bei minimaler Beeinträchtigung des Netzwerkverkehrs, der Systemleistung und der Produktivität von Anwendern
- Wehrt Angriffe ab, bevor sie Anwendungen am Endpunkt erreichen oder ausführen können
- Bietet Schutz, bevor Patches ausgerollt werden können
- Verringert das Risiko von Haftungsansprüchen durch Einhaltung von Compliance-Richtlinien zum Datenschutz
- Verlängert die Lebensdauer von veralteten und nicht mehr unterstützten Betriebssystemversionen (z. B. Windows XP)

Endpoint Application Control

Täglich werden Hunderttausende neuer, bösartiger Softwareanwendungen in Umlauf gebracht. Daher ist es mittlerweile sehr schwierig geworden, alle potenziellen Angriffswege abzusichern. Es besteht die Gefahr, dass vertrauliche Unternehmensdaten auf Computern von Anwendern verloren gehen, die möglicherweise unerwünschte Aktionen durchführen. Daten und Computer müssen somit mehr denn je vor unerwünschtem Anwenderverhalten und unbefugtem Zugriff geschützt werden. Herkömmlicher Antimalware kann dies leider nicht leisten. Sie benötigen daher einen mehrschichtigen Sicherheitsansatz, der Malware proaktiv stoppt, bevor sie auf dem Endpunkt ausgeführt wird. Zudem ist es wichtig, schnell auf Malware reagieren zu können, sobald sie den Endpunkt erreicht.

Mit Trend Micro Endpoint Application Control können Sie Ihren Schutz vor Malware und gezielten Angriffen erweitern, indem Sie die Installation und Ausführung unerwünschter und unbekannter Anwendungen auf Unternehmensendpunkten verhindern. Durch die Kombination aus flexiblen, einfach zu verwaltenden Richtlinien, Whitelisting-und Blacklisting-Funktionen und einer globalen, cloud-basierten Anwendungsdatenbank verringert diese einfach zu verwaltende Lösung ganz erheblich die Anfälligkeit für Angriffe an den Endpunkten. Endpoint Application Control integriert sich in die Trend Micro User Protection Lösungen und bietet dadurch einen weiteren Schutz vor Angriffen und Datenverlust.

Vorteile

- Schützt gegen unerwünschtes Ausführen bösartiger Software durch Benutzer oder Maschinen
- Einfache Verteilung der Agenten unter anderem mit Hilfe von OfficeScan
- Bietet erweiterte Funktionen, um Unternehmensrichtlinien durchzusetzen
- Verwendet korrelierte Bedrohungsdaten aus Milliarden von Datensätzen, die täglich korreliert werden
- Unterstützt die Einhaltung von Compliance-Vorgaben

Endpoint Encryption

Endpoint Encryption verschlüsselt Daten auf einer Vielzahl von Systemen wie Laptops, Desktops, Tablets, CDs, DVDs, USB-Laufwerken und andere Wechselmedien. Die Lösung umfasst die unternehmensweite Verschlüsselung von Festplatten, Dateien / Ordnern und Wechselmedien in Kombination mit gezielter Port- und Endgerätezugriffssteuerung, um den unberechtigten Zugriff auf vertrauliche Daten und deren Nutzung durch nicht autorisierte Benutzer zu verhindern. Über eine einzige Management-Konsole können Sie die Hardware- und Softwareverschlüsselung unternehmensweit für Festplatten, bestimmte Dateien, Ordner, Wechselmedien und Speichergeräte verwalten.

Funktionen

- Erweitertes Reporting und Auditing
  - Automatisierte Durchsetzung von gesetzlichen Compliance-Richtlinen mittels policy-basierter Verschlüsselung
  - Detaillierte Audits und Reports nach Anwender, Unternehmenseinheit und System
- Multi-Faktor-Authentifizierung vor dem Start
  - Flexible Authentifizierung, einschließlich festgelegter Kennwörter, CAC, PIV, Pin und ColorCode®
  - Führt bei falscher Authentifizierung Sperrfunktion aus
- Verwaltungstools und Integration von Active Directory
  - Nutzt Active Directory und die bestehende IT-Infrastruktur für die Installation und Verwaltung
  - Entlastet IT-Mitarbeiter, da Anwender ihre Kennwörter und Konten selbst ändern und zurücksetzen können

Vorteile

- Maximiert die Plattformabdeckung für die Verschlüsselung von Daten und Systemen
  - Verschlüsselt vertrauliche Daten durch vollständig integrierte Verschlüsselungsfunktion für Festplatten, Dateien / Ordner, USB-Laufwerke und Wechselmedien
- Senkt die Gesamtbetriebskosten durch zentrale Richtlinien- und Schlüsselverwaltung
  - Vereinfacht Abläufe mittels vereinheitlichter Datenspeicher durch einen zentralen Verwaltungsserver und eine Management-Konsole
- Vereinfacht die Endgeräteverwaltung per Fernzugriff
  - Wahrt die Einhaltung von gesetzlichen Richtlinien und schützt Daten im Falle eines verloren gegangenen Endgeräts oder vergessenen Kennworts, ohne die Anwender zu stören
  - Verwaltet Richtlinien und schützt Daten auf PCs, Laptops, Tablets, USB-Laufwerken, CDs und DVDs

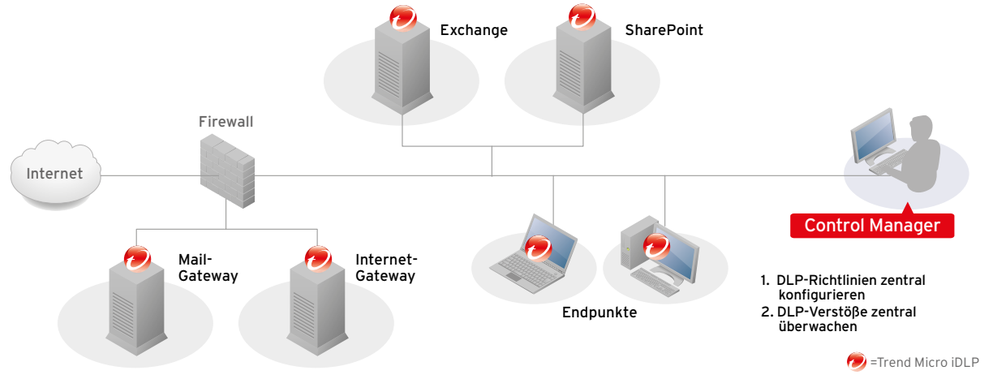
WICHTIGSTE FUNKTIONEN	ENDPOINT ENCRYPTION	DATEIVERSCHLÜSSELUNG
Zentrale Richtlinien- und Schlüsselverwaltung	●	●
FIPS 140-2 Verschlüsselungszertifizierung	Sicherheitsstufe 2	Sicherheitsstufe 2
AES-256-Bit-Verschlüsselung	●	●
Verschlüsselung von Dateien und Ordnern	●	●
Verschlüsselung von Wechselmedien (CD / DVD / USB)	●	●
Gezielte Port- und Gerätezugriffssteuerung	●	●
Verwaltung selbstverschlüsselnder Festplatten	●	
Festplattenverschlüsselung	●	
Netzwerkfähige Authentifizierung vor dem Starten	●	

Integrated Data Loss Prevention

Trend Micro Integrated Data Loss Prevention (iDLP) mit zentraler Richtlinienverwaltung vereinfacht die Datensicherheit auf mehreren Ebenen der bestehenden IT-Sicherheitsinfrastruktur. Es vereinfacht die Administration und sorgt für eine konsistente Durchsetzung, um die Sicherheit von Daten sowie die Einhaltung von Compliance-Richtlinien mit geringerem Aufwand und weniger Kosten zu erhöhen.

Vorteile

- Integrated Data Loss Prevention
  Die in herkömmliche Sicherheitslösungen (von Endpunkt über Messaging- bis hin zu Netzwerklösungen) integrierten Funktionen zur Datensicherheit vereinfachen die Implementierung, reduzieren die Kosten für die Infrastruktur und bieten Sorgenfreiheit in Bezug auf die Datensicherheit.
- Zentrale DLP-Richtlinienverwaltung
  Die zentrale Konfiguration und Anwendung vordefinierter Richtlinienvorlagen auf allen Schutzschichten reduziert den anfänglichen und zukünftigen Administrationsaufwand und sorgt für eine konsistente Durchsetzung der Richtlinien im gesamten Unternehmen.
- Anpassbare, konsolidierte Ansichten und Reports
  Zusammenfassende Protokolle, Reports und Dashboard-Ansichten bieten eine unternehmensweite Transparanz in Echtzeit und die Kontrolle über unrechtmäßigen Datenabfluss und Datenschutzverstöße.

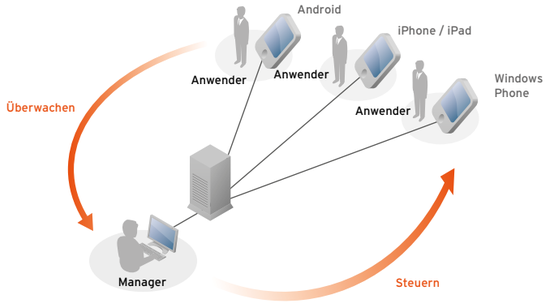


Mobile Security

Trend Micro Mobile Security ermöglicht Unternehmen, den bewährten Schutz von PCs auf mobile Endgeräte und Daten zu erweitern. Somit können jegliche, bei Mitarbeitern zunehmend beliebte Smartphone- und Tablet-Plattformen problemlos integriert werden. Durch eine zentrale Übersicht und Kontrolle für das Management und den Schutz von Endgeräten können Unternehmen ihre Kosten reduzieren. Die Lösung setzt die Verwendung von Kennwörtern durch, verschlüsselt Daten und löscht Daten von verloren gegangenen oder gestohlenen Endgeräten per Fernzugriff. Dadurch werden Daten zuverlässig geschützt und Datenverluste eingegrenzt.

Vorteile

- Schutz vor Bedrohungen
  - Malware
  - Spyware
  - Internetbedrohungen
- Zentrale Verwaltung aller mobilen Plattformen
- Mobile Device Management



Sicherheit für Macintosh-Geräte

Als Plug-in für OfficeScan setzt Trend Micro Security for Mac das Smart Protection Network™ wirksam ein, um das Gefahrenpotenzial durch Bedrohungen aktiv einzugrenzen. Die cloudbasierte Web-Reputation-Technologie verhindert in Echtzeit, dass Anwender und Applikationen auf bösartige Webinhalte zugreifen.

Vorteile

- Wehrt Angriffe durch Malware systemübergreifend ab, einschließlich Mac OS und Windows

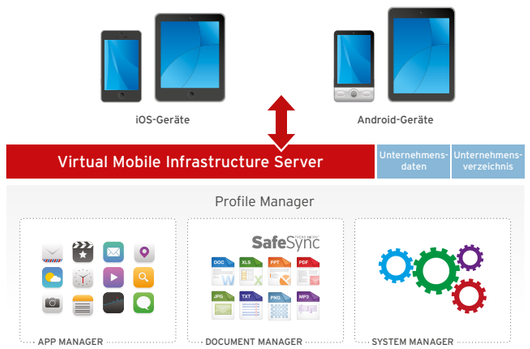
Virtual Mobile Infrastructure

Mobilgeräte, darunter auch Smartphones und Tablets von Mitarbeitern, sind heutzutage vollständig in den Alltag eines modernen Unternehmens integriert. Für die Wettbewerbsfähigkeit ist es unverzichtbar, dass Mitarbeiter auf Unternehmensdaten und -anwendungen zugreifen können, egal, wo sie sich gerade befinden und welches Gerät sie nutzen. Diese Entwicklung bringt jedoch erhebliche Sicherheitsrisiken mit sich.

Mit Trend Micro Virtual Mobile Infrastructure werden vertrauliche Daten nicht auf dem Mobilgerät gespeichert, da dies mit Sicherheitsmaßnahmen verbunden wäre, die den Datenzugriff, das Gerät und den Anwender erheblich einschränken. Anwender öffnen einfach eine iOS- oder Android-App und haben so über eine virtuelle mobile Infrastruktur (VMI) direkten Zugriff auf Unternehmensressourcen. Alle Daten und Anwendungen liegen dabei sicher und geschützt auf Unternehmensservern, während ein gehostetes Android-Betriebssystem ein gewohntes und intuitives, virtuelles Arbeitsumfeld bereitstellt.

Vorteile

- Optimiert die Sicherheit durch klare Trennung von privaten und geschäftlichen Daten, ohne die Nutzer einzuschränken
- Steigert die Zufriedenheit der Mitarbeiter und deren Produktivität
- Gewährleistet die Durchsetzung von Compliance-Richtlinien
- Mitarbeiter können gewohnte und weit verbreitete Apps für die Arbeit nutzen
- Der Diebstahl eines Geräts stellt kein Risiko dar, da Daten und Anwendungen nicht lokal auf dem Gerät gespeichert werden
- Senkt Kosten



ScanMail for Microsoft Exchange

ScanMail Suite for Microsoft Exchange bietet branchenführende, signaturbasierte Content Security sowie innovative E-Mail- und Web-Reputation-Technologien zum Schutz vor Datendiebstahl und versehentlichem Verlust. ScanMail for Microsoft Exchange identifiziert gezielte Angriffe mittels Erkennung von Exploits und Sandboxing als Teil von Network Defense – der Trend Micro Lösung für flexiblen Schutz vor individuellen Bedrohungen.

Vorteile

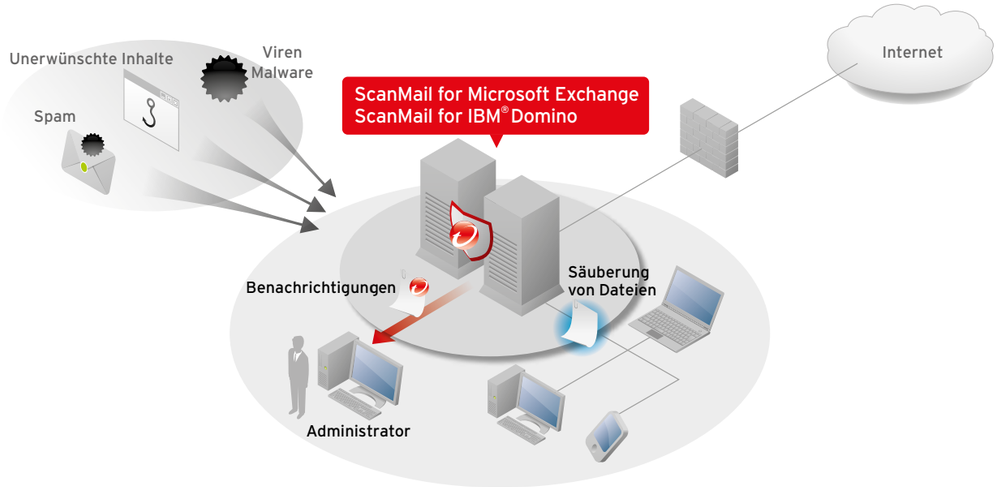
- Integration in und Optimierung der Microsoft Exchange Serverumgebung
- Schutz vor Spam, Malware und Zero-Day-Angriffen
- Flexible Content-Filter
- Einzigartige Web Reputation
- E-Mail Reputation (optional)
- Der integrierte Schutz vor Datenverlust schützt vertrauliche Daten
- Teil der Connected Threat Defense Strategie (Sandbox Integration, Suspiciouse Object Subscription)

ScanMail for IBM® Domino

Stoppt Malware, Spyware, Spam, Phishing und unangemessene Inhalte am Mail-Server – dem zentralen Sicherheitspunkt zur Überprüfung interner und eingehender Nachrichten – mit ScanMail Suite for IBM® Domino. Wird die Lösung in den Trend Micro Deep Discovery Advisor integriert, wehrt sie als Teil von Network Defense – der Trend Micro Lösung für flexiblen Schutz vor individuellen Bedrohungen – gezielte E-Mail-Angriffe ab.

Vorteile

- Führender Schutz vor Malware, Spyware, Spam, Phishing und Zero-Day-Angriffen
- Innovative Web-Reputation-Technologie
- Flexible Content-Filter



PortalProtect for Microsoft SharePoint

Trend Micro PortalProtect schützt Ihre Kollaborationssysteme mit einer dedizierten Schutzschicht vor Malware, Links zu bösartigen Websites und anderen Bedrohungen, die die meisten SharePoint Administratoren nicht kennen.
Die Web-Reputation-Technologie schützt Ihre Webportale vor Links zu bösartigen Websites, während leistungsstarke Content-Filter sowohl datei- als auch webbasierte Komponenten von SharePoint überprüfen.

Vorteile

- Schützt SharePoint Anwender und Daten
- Stoppt eine Vielzahl bösartiger Dateien und URLs
- Filtert unangemessene Inhalte aus den sozialen Komponenten von SharePoint
- Überprüft vertrauliche Daten im Hinblick auf Richtlinieneinhaltung und Risikomanagement
- Niedriger Administrationsaufwand
- Skalierbar auf jede Umgebungsgröße
- Der integrierte Schutz vor Datenverlust schützt vertrauliche Daten

IM Security for Microsoft Lync, Skype for Business und OCS

Schützen Sie Ihre Echtzeit-IM-Kommunikation durch die Abwehr schnelllebiger Angriffe, die dazu entwickelt wurden, Malware zu verbreiten, Opfer auf bösartige Websites zu locken und Daten zu stehlen. Unterstützt vom Trend Micro Smart Protection Network und der einzigartigen Cloud-Client-Architektur blockiert IM Security Links zu bösartigen Websites, bevor diese Links zugestellt werden. Signaturunabhängige Sicherheitstechnologie zum Schutz vor Zero-Day-Angriffen, führender Malware- und neuer Spyware-Schutz verhindern gemeinsam mögliche Schäden durch Malware. Zudem verhindern flexible Content-Filter die unangemessene Nutzung von IM-Diensten und schützen vor Datendiebstahl.

Funktionen und Vorteile

- Blockiert Links zu bösartigen Websites, bevor sie zugestellt werden – dank Web Reputation
- Erkennt und blockiert Zero-Day-Angriffe mittels proprietärer IntelliTrap Technologie
- Stoppt mithilfe einer dedizierten Überwachung noch mehr Spyware, bevor diese Endpunkte infiziert
- Filtert Inhalte zum Schutz vor Datenverlust und anstößiger Sprache
- Reduziert den Administrationsaufwand durch enge Integration in die Plattform und einer stabilen, zentralen Steuerung

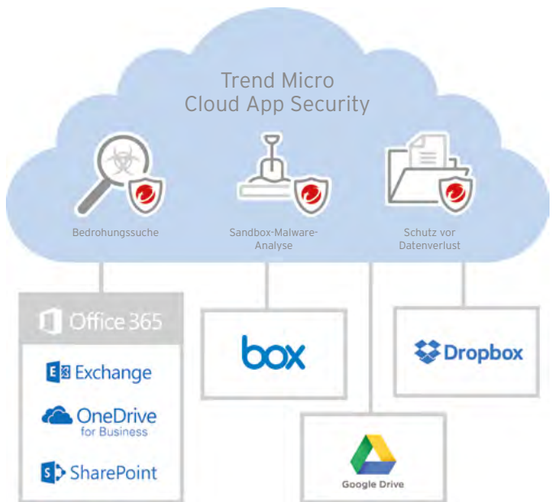
Cloud App Security

Cloud App Security erweitert den Schutz von Microsoft® Office 365™, Box, Dropbox und Google Drive um wichtige Kontrollmechanismen zur Entdeckung und Abwehr von Data Breaches und zielgerichteten Angriffen sowie zur Einhaltung von Compliance Anforderungen. Diese beinhalten unter anderem:

- Sandbox Malware Analyse: erkennt Zero-Day Malware und Malicious Code welcher u. a. in Office und PDF Dokumenten versteckt ist
- Data Loss Prevention: verbessert die Kontrolle und die Transparenz beim Austausch von sensiblen Daten

Vorteile

- Erweitert die integrierten Sicherheitsfunktionen um Sandbox-Malware-Analyse sowie DLP für Box, Dropbox, Google Drive, Exchange Online, SharePoint Online und OneDrive for Business
- Minimale Latenzzeiten anhand einer effektiven Risikobewertung der Dateien vor der Sandbox-Malware-Analyse
- Exploit-Erkennung in Dokumenten
- Keine Einrichtung eines Web-Proxys oder die Änderung des MX-Records zur Umleitung von E-Mails notwendig aufgrund der Verwendung von APIs (direkte Cloud-to-Cloud-Verbindung)

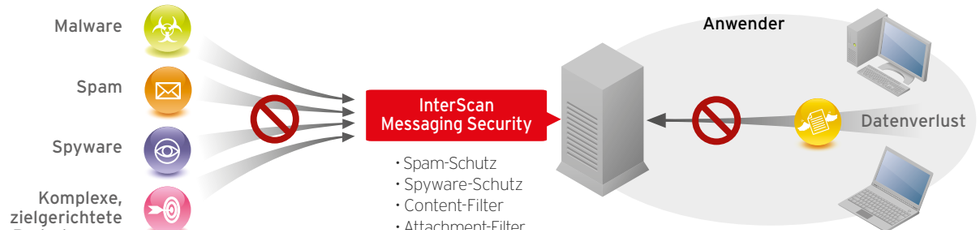


InterScan Messaging Security Virtual Appliance

Trend Micro InterScan Messaging Security stoppt herkömmliche Bedrohungen in der Cloud mithilfe globaler Bedrohungsdaten, schützt vertrauliche Daten mittels Funktionen zum Schutz vor Datenverlust und Verschlüsselung und erkennt als Teil einer individuellen APT-Abwehr (Advanced Persistent Threats) gezielte Angriffe. Die hybride SaaS-Installation vereint den Datenschutz und die Kontrolle einer lokalen virtuellen Appliance mit dem proaktiven Schutz eines cloud-basierten Vorfilter-Services.

Vorteile

- Erkennt und wehrt komplexe, zielgerichtete Bedrohungen (Advanced Persistent Threats, APTs) ab
- Vereitelt komplexe Malware und gezielte Phishing-Angriffe
- Vereinfacht Datensicherheit und Verschlüsselung
- Stoppt nachweislich mehr Spam – laut unabhängiger Tests die Nummer 1
- Teil der Connected Threat Defense Strategie (Sandbox Integration, Suspiciouse Objekt Subscription)

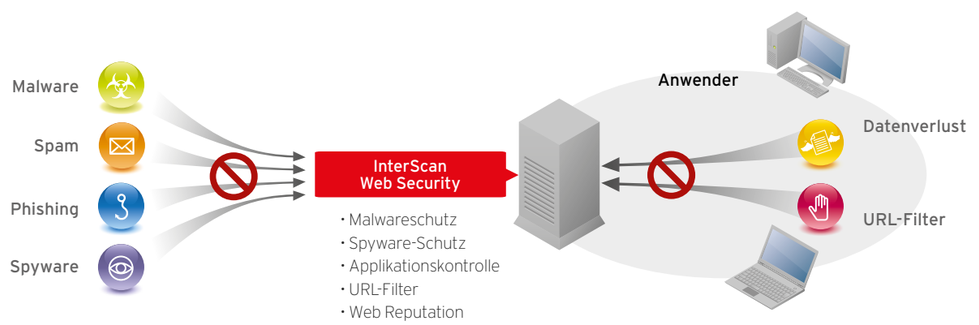


InterScan Web Security Virtual Appliance

InterScan Web Security Virtual Appliance ist eine virtuelle Software-Appliance, die Kontrolle über die Nutzung von webbasierten Anwendungen mit innovativer Malware-Suche, Web Reputation in Echtzeit und flexiblen URL-Filtern kombiniert, und so erstklassigen Schutz vor Internetbedrohungen bietet.

Vorteile

- Sofortige Transparenz und Kontrolle
- Stoppt Internetbedrohungen, bevor sie in das Unternehmensnetzwerk eindringen
- Senkt Ihre Gesamtkosten
- Der integrierte Schutz vor Datenverlust schützt vertrauliche Daten
- Teil der Connected Threat Defense Strategie (Sandbox Integration, Suspiciouse Objekt Subscription)

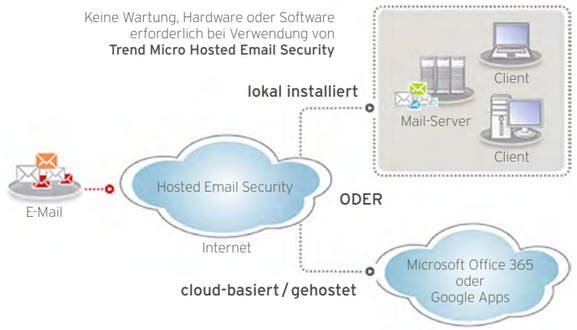


Hosted Email Security

Trend Micro Hosted Email Security ist ein cloud-basierter, wartungsfreier Service, welcher permanent aktuellen Schutz bietet und Spam und Malware stoppt, bevor sie das Netzwerk erreichen.

Vorteile

- Schutz vor zielgerichteten Angriffen sowie Social-Engineering Attacken
- Sandbox-Analyse in der Cloud
- E-Mail-Verschlüsselung durch Identity Based Encyrption Technologie
- Entlastet die Bandbreite und steigert die Produktivität

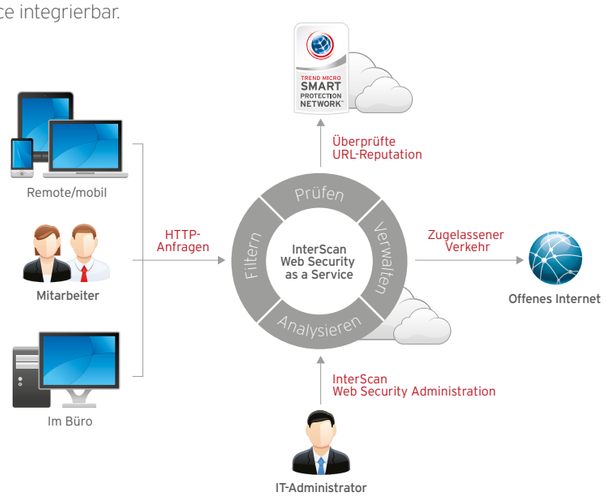


InterScan Web Security as a Service

Trend Micro InterScan Web Security as a Service (IWSaaS) bietet dynamischen Schutz vor Cyberbedrohungen in der Cloud, noch bevor sie Ihre Anwender bzw. Ihr Netzwerk erreichen. Sie erhalten Transparenz und Kontrolle über die Internetnutzung Ihrer Mitarbeiter in Echtzeit. Als cloud-basierte Lösung schützt IWSaaS jeden Anwender überall und auf jedem Gerät – basierend auf einer einzigen Richtlinie, unabhängig vom jeweiligen Standort des Anwenders. Damit entfallen ein kostenintensiver Rücklauf des Datenverkehrs oder die Verwaltung mehrerer geschützter Internet-Gateways an verschiedenen Standorten. Darüber hinaus lässt sich die Lösung flexibel je nach Wachstum Ihres Unternehmens erweitern, ohne in den Erwerb, die Verwaltung oder die Wartung von Software bzw. Hardware investieren zu müssen. Sollte eine hybride Installation sinnvoll sein, ist die lokale InterScan Web Security Virtual Appliance nahtlos mit den allgemeinen Verwaltungs-, Berichts- und Richtlinienfunktionen in InterScan Web Security als Service integrierbar.

Vorteile

- Bester Schutz – überall und auf jedem Gerät
- Bietet Anwendern mehr Freiheit und behält gleichzeitig die erforderliche Transparenz und Kontrolle
- Einfache aber leistungsstarke Verwaltung und Berichte
- Maximaler Cloud-Vorteil – Kosteneffizienz und Flexibilität



Worry-Free Advanced, Worry-Free Standard, Worry-Free Services

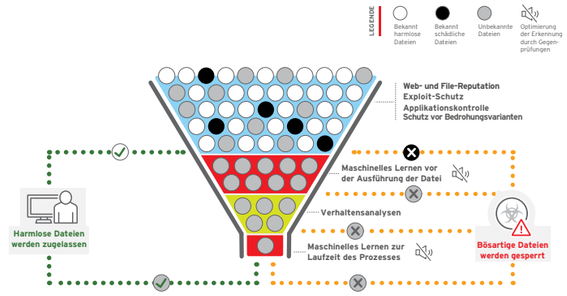
Trend Micro™ Worry-Free Services Advanced, unterstützt durch XGen™ Security, ist eine cloudbasierte Sicherheitslösung, die speziell für kleine Unternehmen konzipiert wurde und ausgezeichneten Schutz für Geräte und E-Mails bietet. Damit Sie Zeit und Ressourcen sparen, wird die Lösung von Trend Micro gehostet und verwaltet. Zudem kombiniert sie die Funktionen von Trend Micro™ Worry-Free Services zum Schutz Ihrer Geräte, Trend Micro™ Hosted Email Security zum Schutz Ihrer lokal gespeicherten E-Mails und Trend Micro™ Cloud App Security zum Schutz von Microsoft® Office 365™ E-Mail, OneDrive, SharePoint und Tools zur Zusammenarbeit wie Google Drive, Dropbox und Box.

Vorteile

- Schutz vor Ransomware
  - Worry-Free bietet Schutz vor komplexer Malware und Ransomware
  - Endpunkte inner- oder außerhalb des Unternehmensnetzwerks sind vor Malware, Trojanern, Würmern, Spyware, Ransomware und neuartigen Kombinationen geschützt.
- Wartungsfrei - Hosting und Verwaltung durch Trend Micro
  - Trend Micro Worry-Free™ Business Security Services ist eine gehostete Sicherheitssoftware. Die Kosten für die Verwaltung und den Unterhalt eines eigenen lokalen Servers brauchen nicht eingeplant zu werden, denn Hosting und Verwaltung wird in unserem unternehmensinternen Rechenzentrum in München sichergestellt. Das macht es besonders einfach: Trend Micro übernimmt die Wartung, der Kunde kann sich auf sein Kerngeschäft konzentrieren und spart IT-Kosten.

Vorteile Fortsetzung

  - Die Sicherheitssoftware wird automatisch aktualisiert. Es müssen keine Ressourcen oder weiteren Mittel für diesen Zweck eingeplant werden.
- Internetsicherheit der Spitzenklasse ohne Beeinträchtigung der Leistung
  - Trend Micro Worry-Free™ Services stoppt Bedrohungen in einer Cloud, bevor sie Ihr Firmennetzwerk oder Ihre Geräte erreichen. So ist das Unternehmen geschützt und die Leistung wird nicht beeinträchtigt. Dafür sorgt das Trend Micro Smart Protection Network. Dieses weltweite Frühwarnsystem sammelt täglich Millionen von Bedrohungsdaten, analysiert sie und verhindert, dass die Bedrohungen auf den Computer zugreifen und in das Unternehmen eindringen.



	Standard Edition	Advanced Edition	Services Edition	Services Advanced
ANTIMALWARE UND INTERNETSICHERHEIT				
Schutz vor Malware, Spyware und anderer Malware	•	•	•	•
DATENSICHERHEIT				
Gerätezugriffssteuerung: überwacht den Zugriff auf USB-Laufwerke und andere verbundene Geräte, um Datenverlust zu verhindern und Bedrohungen zu stoppen	•	•	•	•
EINZIGARTIG: Verhindert versehentlichen oder absichtlichen Versand kritischer Daten in geschäftlichen E-Mails		•		•
PLATTFORMEN				
PCs, Laptops, Windows Server, Mac Clients (iMac, MacBook und Server)	•	•	•	•
EINZIGARTIG: Android- und iOS-Geräte (jede Lizenz umfasst Schutz für zwei Geräte)			•	•
NEU und EINZIGARTIG: Schutz für mobile Geräte (nur für Microsoft Exchange ActiveSync Anwender)		•		•
MESSAGING-SICHERHEIT UND SPAM-SCHUTZ				
Echtzeitsuche in POP3-E-Mail-Konten	•	•	•	•
Stoppt Spam und E-Mail-basierte Malware, bevor sie die Mail-Server erreichen		•		•
Bedrohungsschutz und mehrschichtige Spam-Abwehr für Microsoft Exchange Server		•		•
ZENTRALE VERWALTUNG				
Webbasierte Management-Konsole	Über LAN oder VPN	Über LAN oder VPN	Zugriff an jedem beliebigen Ort über das Internet	Zugriff an jedem beliebigen Ort über das Internet
Standort des Verwaltungsservers	Lokal installiert	Lokal installiert	Kein Server erforderlich	Kein Server erforderlich
Verteilung von Updates und Patches an den Anwender	Manuell mit vollständiger Kontrolle	Manuell mit vollständiger Kontrolle	Automatisch	Automatisch
IT-Ressourcen erforderlich	IT-Ressourcen begrenzt erforderlich	IT-Ressourcen begrenzt erforderlich	Keine IT-Ressourcen erforderlich	Keine IT-Ressourcen erforderlich

05 USER PROTECTION

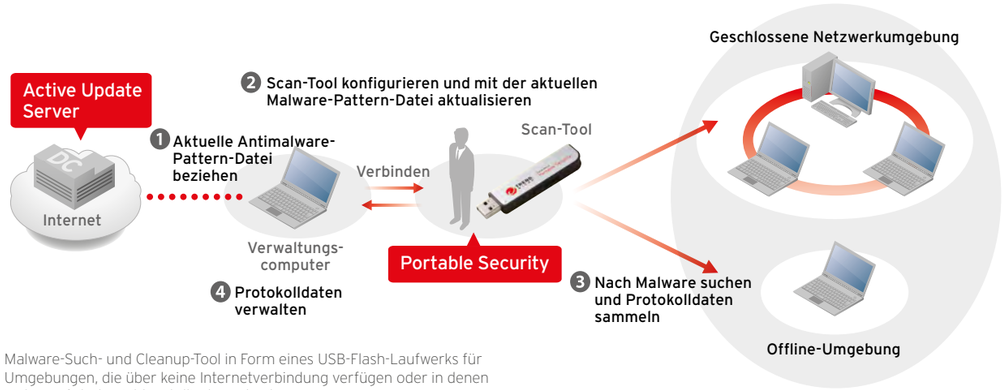
05.7 Security for Industry 4.0 und IoT

Portable Security

Trend Micro Portable Security ist ein neues Konzept im Bereich Antimalware speziell für Umgebungen, in denen sich die Installation einer Antimalware-Software oft als schwierig erweist, wie beispielsweise Produktionsumgebungen, Arztpraxen, öffentliche Einrichtungen oder Schulen. Portable Security verwendet einen USB-Stick, mit dem IT-Leiter Malware suchen und beseitigen können, unabhängig davon, ob eine Internetverbindung besteht oder nicht.

Vorteile

- Schnell einsetzbar und mit der Zeit skalierbar, keine Installation erforderlich
- Ausführung über USB-Stick, keine Installation erforderlich
- Sucht und entfernt Malware mithilfe der neuesten Pattern-Dateien
- Protokolliert Suchaktivitäten – einschließlich Verwaltung nativer Protokolldaten
- Aktualisierung über einen zentralen Verwaltungscomputer
- Reduziert Risiken
- Minimiert die Komplexität



Malware-Such- und Cleanup-Tool in Form eines USB-Flash-Laufwerks für Umgebungen, die über keine Internetverbindung verfügen oder in denen Malware-Schutz nicht installiert werden kann.

Safe Lock

Safe Lock wehrt Eindringlinge ab und verhindert das Ausführen von Malware, indem die Verfügbarkeit des Systems mittels Lockdown (Systemsperre) auf einen bestimmten Verwendungszweck beschränkt wird. Safe Lock schützt industrielle Kontrollsysteme und integrierte Geräte, die eine hohe Verfügbarkeit erfordern, sowie Geräte mit fest definierten Funktionen in geschlossenen Umgebungen. Dabei wird die Systemleistung durch das Produkt kaum beeinträchtigt und es müssen keine Pattern-Dateien aktualisiert werden. Dank der anwenderfreundlichen Benutzeroberfläche und der Kompatibilität mit Trend Micro Portable Security 2 lässt sich Safe Lock schnell und einfach installieren und bietet eine hohe Anwenderfreundlichkeit. Leitgedanke von Industrie 4.0 ist die intelligente Fabrik (Smart Factory). Dies beinhaltet, dass Kontrollsysteme untereinander und mit anderen Systemen auf höherer Ebene kommunizieren müssen. Die Systeme stellen damit ein potenzielles Angriffsziel für bösartige Aktivitäten wie z. B. Zeus dar.

Gewöhnlich ist die Installation von Sicherheitslösungen auf diesen Systemen nicht zulässig, da sie regelmäßige Änderungen und Updates erfordern. Safe Lock wurde speziell für die Sicherheitsanforderungen in Industrie 4.0-Umgebungen entwickelt, indem es Industrial Control Systems (ICS) mit einer einzigartigen Zusammenstellung aus Sicherheitstechnologien schützt, ohne dass regelmäßige Updates oder Änderungen anfallen.

Vorteile

- Whitelist für Anwendungen
- Verwaltung der Liste der zulässigen Anwendungen
- Schutz vor Schwachstellenausnutzung durch z.B. Injection
- Rollenbasierte Verwaltung
- Protokollierung ohne betriebsstörende Benachrichtigungen
- Native kompatibilität mit Trend Micro Portable Security
- Anwenderfreundliche und übersichtliche Benutzeroberfläche

06 HYBRID CLOUD SECURITY

06.1 Cloud- und Serversicherheit

Deep Security

Trend Micro Deep Security bietet eine umfassende Sicherheitsplattform für jede Art von Rechenzentrum unabhängig ob physikalisch, virtualisiert, cloudbasiert, virtuelle Desktopumgebungen oder dockerbasierter Anwendungsbereitstellung. Als Teil der Trend Micro XGen™ Familie bietet es einen vielschichtigen Sicherheitslösungsansatz. Es sorgt für Schutz vor Zero Day Angriffen, sichert Ihre Server vor Ransomware Angriffen und dient zur Erkennung von Datenmanipulation. Die Plattform kann mit hervorragend aufeinander abgestimmten Modulen erweitert werden, um Server-, Anwendungs- und Datensicherheit in Ihrem Rechenzentrum zu garantieren und somit zur Einhaltung von gesetzlichen Richtlinien (Compliance) beitragen.

Zukunftsweisende Technologien wie SAP und Docker können ebenfalls durch Deep Security geschützt werden, um Unterbrechungen im Betriebsablauf zu verhindern.
Durch die flexible Modulauswahl können Sie Ihre Sicherheitslösung ganz auf Ihre Anforderungen zuschneiden – mit einer beliebigen Kombination aus agentenbasiertem oder NSX-basiertem agentenlosem Schutz, einschließlich Malware-Schutz, Web Reputation, Firewall, Abwehr von Eindringlingen, Integritätsüberwachung, Applikationskontrolle und Protokollprüfung. Das Ergebnis: Eine anpassbare und effiziente Sicherheitsplattform für Server, die geschäftskritische Unternehmensanwendungen und -daten vor Angriffen und Unterbrechungen des Betriebsablaufs schützt und selbst die Problematik von Notfallpatchen eindämmt.

Funktionen

- Malware-Schutz
- Behaviour Monitoring gegen Ransomware
- Sandbox Analysis Integration
- Integritätsüberwachung
- Web Reputation
- Erkennung und Abwehr von Eindringlingen
- Bidirektionale Stateful-Firewall
- Protokollprüfung
- Applikationskontrolle
- Umfangreiche Betriebssystemunterstützung wie Windows, Linux und Unix
- Smart Folder für einfache Darstellung und Filterfunktionen
- Mandantenfähig
- Docker kompatible Integration
- Hypervisor-Integritätsüberwachung
- VMware NSX Support
- Integration in AWS und vCloud
- IPv6 Ready

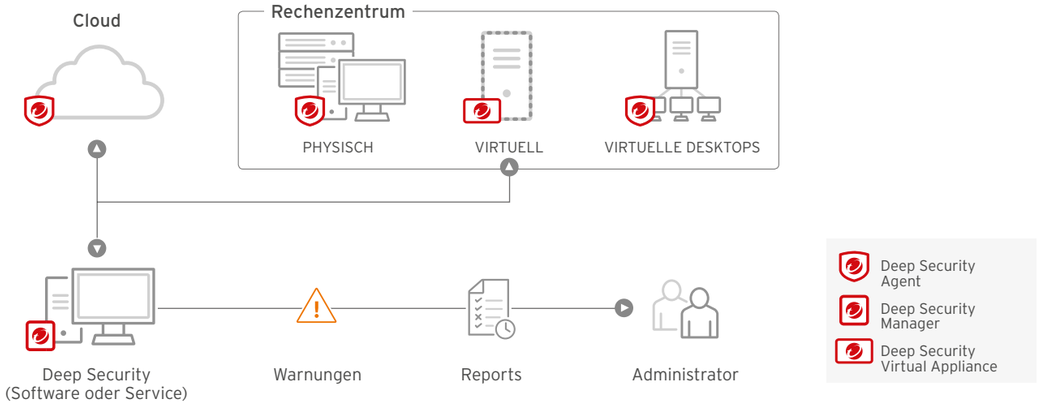
Vorteile

- Teil der XGen™ Familie: Mehrschichtiger Schutz gegen Ransomware und gezielte Angriffe
- Sandbox Analysis Integration zur Auswertung von unbekannten Schädlingen
- Teil der Connected Threat Defense Strategie zur einfachen Verteilung von Schadcodeinformationen innerhalb weiterer Trend Micro Produkten und 3rd Party Sicherheitsanbietern.
- Einfache und zentralgesteuerte Applikationskontrolle von Anwendungen und Skripten
- Schnellere Rendite bei Virtualisierung, VDI und Cloud-Computing
  - Bietet eine leichtere und einfacher zu verwaltende Methode, um VMs zu schützen
- Maximale Reduktion der Betriebskosten
- Verhindert Datenverlust und Unterbrechungen im Betriebsablauf
  - Erkennt und entfernt Malware in Echtzeit bei minimaler Leistungsbeeinträchtigung
- Kosteneffiziente Richtlinieneinhaltung
  - Erfüllt die wichtigsten Compliance-Anforderungen, u. a. für PCI DSS 2.0, HIPAA etc.
- Integration in vorhandene SIEM Lösungen

06 HYBRID CLOUD SECURITY

06.1 Cloud- und Serversicherheit

Hybrid Cloud Security

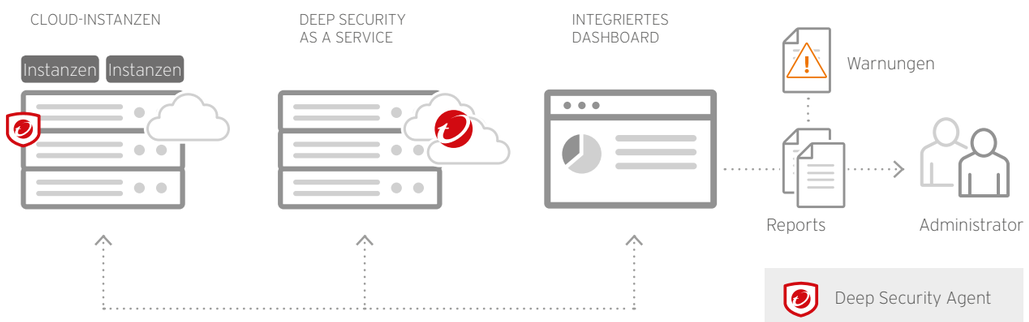


Deep Security as a Service

Trend Micro™ Deep Security as a Service bietet gehostete Sicherheitsoptionen für Cloud-Umgebungen, darunter Funktionen zur Erkennung und Abwehr von Eindringlingen (IDS / IPS), eine Firewall, Malware-Schutz, Web Reputation, Logüberprüfung und Integritätsüberwachung. Verwalten Sie alle Kontrollen über eine zentrale Konsole und mit einem einzigen leichten Agenten, nahtlos integriert bei führenden Cloud-Anbietern wie AWS, Microsoft Azure und VMware vCloud Air. Deep Security as a Service stellt alle Schutzfunktionen von Deep Security bereit – jedoch ohne den Aufwand der Bereitstellung und Wartung des Deep Security Managers. Wir kümmern uns um Produkt- und Kernel-Updates, konfigurieren und warten die Sicherheitsdatenbank und verwalten den Manager für Sie. So können Sie sich ganz auf Ihr Kerngeschäft konzentrieren.

Funktionen und Vorteile

- **Sichere DevOps:** Verteilungsskripte für Konfigurationsverwaltungstools wie Chef, Puppet und OpsWorks werden bereitgestellt, damit Sie Sicherheit in Ihre Betriebsabläufe einbinden können.
- **Hostbasierte Kontrollen:** Durch den hostbasierten Ansatz von Deep Security können Sie den Schutz für Workloads auf Grundlage von Tags individuell anpassen und Instanzen automatisch schützen, sobald sie online sind.
- **Proaktiver Schutz:** Mit den IPS-Funktionen werden Sie nicht einfach nur gewarnt, wenn Eindringversuche erkannt werden, sondern Sie können Angriffe auch abwehren.
- **Compliance:** Unterstützt bei wichtigen Compliance-Anforderungen für PCI DSS, HIPAA, NIST und SAS 70 und liefert detaillierte, prüffähige Reports, die verhinderte Angriffe dokumentieren und den Status der Compliance anzeigen.

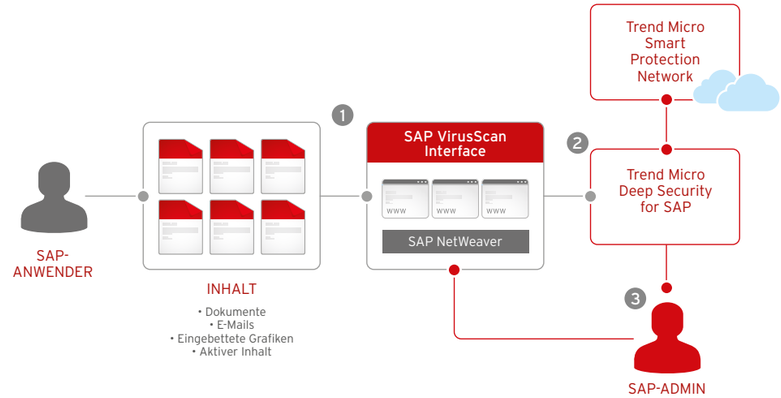


Deep Security for SAP®

Das Modul Trend Micro™ Deep Security™ für SAP führt Malware-Suchen durch und überprüft die gefundenen Informationen, um mögliche Bedrohungen in SAP-Systemen zu identifizieren. Diese erweiterte Erkennungsfunktion bietet zusätzlichen Schutz, der über die herkömmliche Malwareerkennung hinausgeht. Außerdem lässt sich diese Sicherheitslösung mit zusätzlichen Deep Security Modulen zum Schutz von SAP-Servern und sogar ganzer Rechenzentren erweitern – und das alles in einer einzigen Lösung.

Vorteile

- Für alle SAP-Plattformen mit SAP VSI 2.0-Unterstützungen optimiert, darunter SAP NetWeaver, SAP ERP, SAP HANA sowie für neue Produkte wie SAP Fiori
- Schutz vor Malware- und Cross-Site-Scripting (XSS)-Angriffen
- Deep Security Scanner for SAP kombiniert mit den Deep Security Modulen bieten umfassenden Schutz Ihrer SAP Umgebung
- Unterstütz Sie bei der Einhaltung diverser regulatorischen Compliance-Anforderungen wie PCI DSS 2.0, HIPAA, FISMA/NIST, NERC und SSAE-16

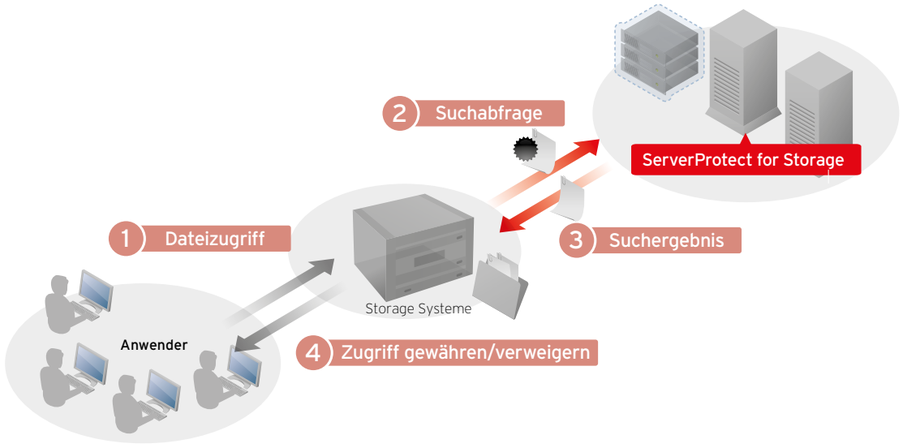


ServerProtect for Storage

Trend Micro ServerProtect for Storage ist die branchenweit zuverlässigste, leistungsstärkste Sicherheitslösung für Storage-Plattformen. Es schützt Dateispeichersysteme, indem Malware und Spyware in Echtzeit erkannt und entfernt werden.

Vorteile

- Enge Integration in EMC Celerra, NetApp, Hitachi Data Systems, IBM, HPE und weitere Storage Systeme
- Ermöglicht leistungsstarke Malwaresuche in Echtzeit bei minimaler Beeinträchtigung von Servern und ohne Auswirkungen für Endanwender
- Unterstützt auch Malwarescanning über iCAP-Protokoll



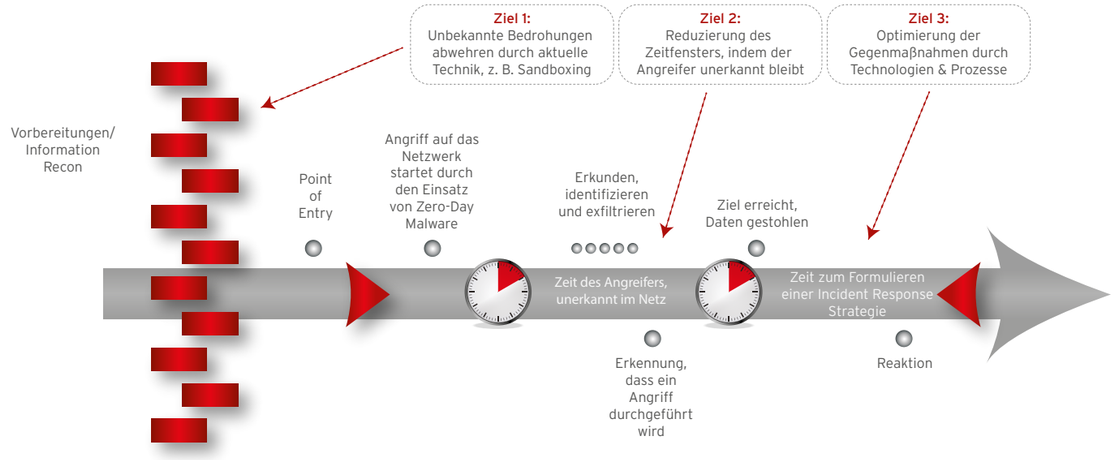
Deep Discovery

Trend Micro Deep Discovery ist eine Plattform zum Schutz vor komplexen Bedrohungen, mit der Sie die getarnten und gezielten Angriffe von heute erkennen, analysieren und flexibel abwehren können. Mit speziellen Erkennungs-Engines, benutzerdefiniertem Sandboxing und den globalen Bedrohungsdaten aus dem Trend Micro™ Smart Protection Network™ wehrt Deep Discovery Angriffe ab, die von Standardsicherheitslösungen nicht erkannt werden.
Als eigenständige Installation oder als integrierte Komponente sorgt Deep Discovery für Netzwerk-, Endpunkt- und E-Mail- Sicherheit und gewährleistet darüber hinaus einen integrierten Schutz Ihres Unternehmens vor komplexen Bedrohungen – genau dort, wo es besonders darauf ankommt.

Vorteile

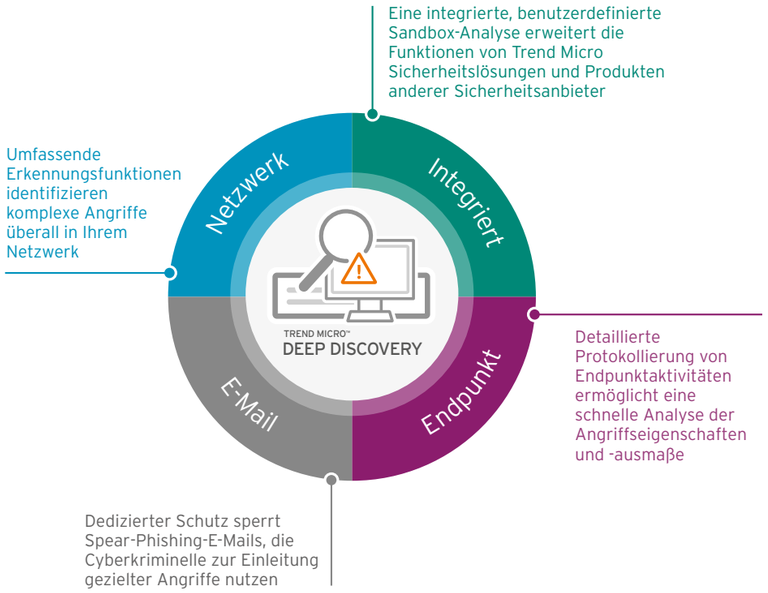
- Schutz vor Angriffen
  Einzigartige Technologien zur Bedrohungserkennung entdecken Angriffe, bevor sie Schaden anrichten können.
- Eine einzige Plattform mit einer Vielzahl von Lösungen
  Schützen Sie Ihr Unternehmen überall dort vor komplexen Bedrohungen, wo es besonders darauf ankommt.
- Schnelle Reaktion durch Bedrohungsdaten
  Deep Discovery und globale Bedrohungsdaten sorgen für eine schnelle und wirksame Reaktion auf Angriffe.

Sicherheit bei zielgerichteten Angriffen



Funktionen

- Erkennung komplexer Bedrohungen
  Erkennt Angriffe überall in Ihrem Netzwerk mit speziellen Erkennungs-Engines, Korrelationsregeln und benutzerdefiniertem Sandboxing.
- Anpassbares Sandboxing
  Nutzt virtuelle Umgebungen, die genau Ihren Systemkonfigurationen entsprechen, um die Angriffe zu entdecken, die sich gezielt gegen Ihr Unternehmen richten.
- Daten aus dem Smart Protection Network
  Verwendet cloudbasierte Sicherheitsdaten in Echtzeit zur Bedrohungserkennung und detaillierten Angriffsanalyse.
- Integration in Custom Defense
  Nutzt IOC-Erkennungsdaten gemeinsam mit anderen Sicherheitsprodukten von Trend Micro und Drittanbietern, um weitere Angriffe abzuwehren.



Deep Discovery™ Analyzer

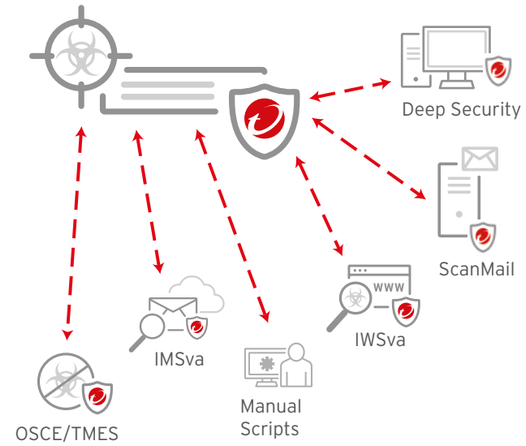
Der Deep Discovery Analyzer optimiert bestehende Sicherheitsinvestitionen von Trend Micro und anderen Anbietern (über eine Web-Services-API). Verdächtige Objekte können an die Deep Discovery Analyzer-Sandbox gesendet werden, um mithilfe verschiedener Erkennungsmethoden genauer untersucht zu werden. Wird eine Bedrohung entdeckt, können die Sicherheitslösungen automatisiert aktualisiert werden.

Funktionen

- Benutzerdefinierte Sandbox-Analysen
  nutzen Ihre Systemkonfigurationen, Treiber, installierte Anwendungen und Sprachversionen. Dieser Ansatz verbessert die Erkennungsrate komplexer Bedrohungen, die darauf abzielen, standardmäßige virtuelle Images zu umgehen. Die benutzerdefinierte Sandbox-Umgebung umfasst einen sicheren externen Zugriff, der mehrstufige Downloads, URLs, C&C-Kommunikation und mehr erkennt und analysiert. Darüber hinaus wird manuelles Einreichen von Dateien und URLs unterstützt.
- Flexible Installationsoptionen
  bieten die Möglichkeit, den Analyzer als Standalone-Sandbox oder im Rahmen einer größeren Deep Discovery-Installation als zusätzliche Sandbox-Funktion zu installieren. Die Lösung unterstützt bis zu 60 Sandbox-Instanzen pro Appliance. Darüber hinaus können mehrere Appliances zur Skalierung und Optimierung der Verfügbarkeit geclustert werden.
- Fortschrittliche Erkennungsmethoden
  wie statische und heuristische Analysen, Verhaltensanalysen, Web Reputation und File Reputation stellen sicher, dass Bedrohungen schnell erkannt werden.
  - Untersucht mithilfe mehrerer Erkennungsengines und Sandboxing ausführbare Windows-, Microsoft® Office- und PDF-Dateien sowie Internetinhalte und komprimierte Dateien.
  - Entdeckt Malware und Exploits in verbreiteten Office-Dokumenten durch spezielle Erkennungsmethoden und Sandboxing.
  - Führt Sandbox-Analysen von URLs durch, die in E-Mails enthalten sind oder manuell eingereicht wurden. Produkte und Sicherheitsforscher können verdächtige Bedrohungsexemplare einreichen. Die Lösung tauscht neue IOC-Erkenntnisse über Bedrohungen automatisch mit Trend Micro Lösungen und Produkten von Dritten aus. Unterstützung für Windows- und Mac-Betriebssysteme.
- Erkennung von Ransomware:
  Erkennt Skript-Emulation, Zero-Day-Exploits sowie zielgerichtete und kennwortgeschützte Malware, die gewöhnlich im Zusammenhang mit Ransomware steht. Darüber hinaus werden Informationen über bekannte Bedrohungen genutzt, um Ransomware mithilfe von Pattern- und Reputationbasierten Analysen zu erkennen.

Vorteile

- Bessere Erkennung
  - Höhere Erkennungsraten als in generischen virtuellen Umgebungen
  - Erstklassiger Schutz vor Umgehungsmethoden
- Sichtbare Rendite
  - Erweiterung bestehender Investitionen durch Integration in die Connected Threat Defense Strategie und gemeinsame Nutzung von Bedrohungsinformatione sowie zusätzliche Verarbeitungskapazität für Umgebungen mit hohem Datenverkehrsaufkommen
  - Keine zeitaufwändige manuelle Analyse verdächtiger Dateien
  - Vermeidung kostspieliger Beseitigung von Ransomware
  - Flexible Installationsoptionen für zentrale oder dezentrale Analysen



Deep Discovery™ Inspector

Deep Discovery Inspector bietet als physische oder virtuelle Netzwerk-Appliance ein netzwerkweites Monitoring des gesamten Datenverkehrs und ermöglicht damit umfassende Transparenz für sämtliche Aspekte von gezielten Angriffen, komplexen Bedrohungen und Ransomware. Mithilfe spezieller Engines zur Bedrohungserkennung und benutzerdefinierter Sandbox-Analysen identifiziert Deep Discovery Inspector komplexe und unbekannte Malware, Ransomware, Zero-Day-Exploits, C&C Kommunikation und versteckte Angreiferaktivitäten, die von Standard-Sicherheitsmechanismen unentdeckt bleiben.

Funktionen

- Überprüfung aller Netzwerkinhalte.
  Deep Discovery Inspector überwacht den gesamten Datenverkehr physischer und virtueller Netzwerksegmente, alle Netzwerk-Ports und über 100 Netzwerkprotokolle, um gezielte Angriffe, komplexe Bedrohungen und Ransomware zu erkennen. Dank unseres ortsunabhängigen Ansatzes zum Schutz des Netzwerkverkehrs kann Deep Discovery gezielte Angriffe, komplexe Bedrohungen und Ransomware im eingehenden und ausgehenden Netzwerkverkehr sowie laterale Ausbreitung, C&C-Kommunikation und anderes Angreiferverhalten in der gesamten Angriffsabwehrkette erkennen.
- Umfassende Erkennungsmethoden
  Deep Discovery Inspector erkennt Skript-Emulation, Zero-Day-Exploits sowie zielgerichtete und kennwortgeschützte Malware, die gewöhnlich im Zusammenhang mit Ransomware steht. Darüber hinaus werden Informationen über bekannte Bedrohungen genutzt, um Ransomware mithilfe von Pattern- und Reputation-basierten Analysen zu erkennen. Benutzerdefiniertes Sandboxing erkennt Verschlüsselungsverhalten, Änderungen an großen Mengen von Dateien sowie an Backup-Dateien für die Wiederherstellung.
- Benutzerdefinierte Sandbox-Analysen
  nutzen virtuelle Images, die genau den Systemkonfigurationen, Treibern, installierten Anwendungen und Sprachversionen eines Unternehmens entsprechen. Dieser Ansatz verbessert die Erkennungsrate von Ransomware und komplexen Bedrohungen, die darauf abzielen, standardmäßige virtuelle Images zu umgehen.
- Umfassende Bedrohungsinformationen
  stellen sicher, dass lokale Erkenntnisse zu Netzwerkbedrohungen mit globalen Bedrohungsinformationen aus dem Trend Micro™ Smart Protection Network™ korreliert werden.
- Beschleunigte und höhere Rendite
  durch eine flexible Architektur, die je nach Netzwerkdurchsatz eine Installation als Hardware oder als virtuelle Appliance ermöglicht. Bestehende Investitionen in NGFW/IPS, SIEM und Gateways werden durch den Austausch von Bedrohungsinformationen erweitert.
- Teil der Connected Threat Defense Strategie

Vorteile

- Bessere Erkennung
  - Mehrere Erkennungstechniken
  - Monitoring des gesamten Netzwerkverkehrs
  - Benutzerdefinierte Sandbox-Analysen
  - Umfassende Bedrohungsinformationen
- Sichtbare Rendite
  - Laut Forschungsergebnissen 145 % Rendite in 10 Monaten*
  - Erweiterung bestehender Investitionen
  - Flexible Installationsoptionen
  - Automatisierung zuvor manuell ausgeführter Aufgaben

* ESG, Validierung des ökonomischen Werts: Oktober 2015

Erkennen von

- Gezielten Angriffen und komplexen Bedrohungen
- Unbekannten und bekannten Ransomware-Angriffen
- Zero-Day-Malware und Exploits in Dokumenten
- Angreiferverhalten und anderen Netzwerkaktivitäten
- Internetbedrohungen, einschließlich Exploits und Drive-by-Downloads
- Phishing, Spear-Phishing und anderen E-Mail-Bedrohungen
- Herausschleusen von Daten
- Bots, Trojanern, Würmern, Keyloggern
- Zerstörerischen Anwendungen

Deep Discovery™ Email Inspector

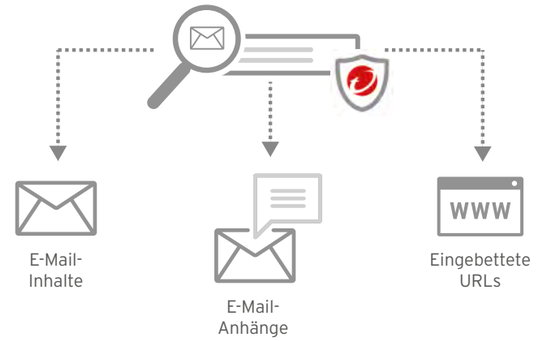
Deep Discovery Email Inspector nutzt innovative Techniken zur Erkennung und Abwehr von Spear-Phishing-E-Mails, über die ahnungslosen Mitarbeitern komplexe Malware und Ransomware zugestellt wird. Der Email Inspector wird hinter ihr bestehendes E-Mail-Gateway integriert und blockiert Spear-Phishing-E-Mails mit bösartigen Anhängen oder URLs, bevor diese in das Unternehmensnetzwerk gelangen.

Funktionen

- Analyse von E-Mail-Anhängen
  Untersucht E-Mail-Anhänge mithilfe mehrerer Erkennungsengines und Sandboxing. Analysiert werden zahlreiche ausführbare Windows-Dateien, dazu Microsoft Office- und PDF-Dateien, Webinhalte sowie Zip- und andere komprimierte Dateien.
- Erkennung von Exploits in Dokumenten
  Spezielle Erkennungs- und Sandboxing-Verfahren entdecken Malware und Exploits in gängigen Office-Dokumenten.
- Benutzerdefiniertes Sandboxing
  Sandbox-Simulation und -Analysen werden in Umgebungen durchgeführt, die genau Ihren Desktop-Softwarekonfigurationen entsprechen.
- Analyse von eingebetteten URLs
  URLs in E-Mails werden mithilfe von Reputationsprüfung, Inhaltsanalyse und Sandbox-Simulation analysiert.
- Kennwortinformationen
  Das Entsperren von kennwortgeschützten Dateien und Zip-Dateien wird mithilfe vom Kunden bereitgestellter Schlüsselwörter und einer Vielzahl von Heuristiken durchgeführt.
- Flexibilität bei Verwaltung und Installation
  Dank der gezielten Untersuchung von E-Mails und Richtlinien zu ihrer Handhabung kann praktisch jede Umgebung geschützt werden. Der Email Inspector kann zusammen mit jeder beliebigen E-Mail-Sicherheitslösung installiert und entweder im Modus MTA (Sperren) oder BCC (Überwachen) ausgeführt werden.
- Integration und gemeinsame Verwendung von Bedrohungsdaten
  Neue Erkennungsdaten (C&C, andere IOC-Daten) können mit anderen Sicherheitslösungen verwendet werden.

Vorteile

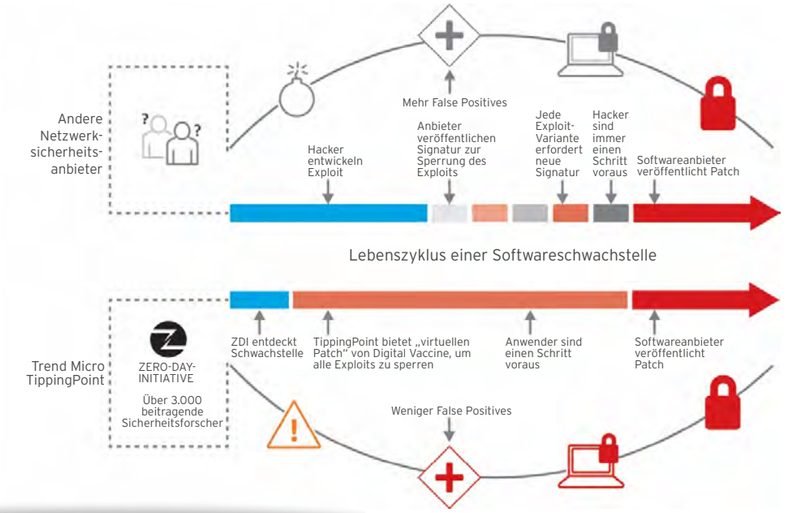
- Besserer Schutz
  - Stoppt Spear-Phishing-E-Mails, mit denen die meisten zielgerichteten Angriffe gestartet werden
  - Blockiert Ransomware, bevor Schaden entsteht
  - Findet mithilfe von benutzerdefiniertem Sandboxing Bedrohungen, die für Standard-E-Mail-Sicherheitslösungen nicht erkennbar sind
- Sichtbare Rendite
  - Stoppt zielgerichtete Spear-Phishing und Ransomware-Angriffe, wodurch die kostenintensive Behebung von durch Malware verursachten Problemen vermieden wird
  - Arbeitet reibungslos mit bestehenden E-Mail-Sicherheitslösungen zusammen
  - Tauscht IOCs mit Netzwerk- und Endpunktsicherheitsschichten aus



TippingPoint Next-Generation Intrusion Prevention System NX Series

Vor dem Hintergrund der sich verändernden Bedrohungslandschaft nimmt die Bedeutung der Netzwerksicherheit weiter zu und macht sie zu einer immer komplexeren Aufgabe. Die Trend Micro TippingPoint Next-Generation Intrusion Prevention System (NGIPS) unterstützt durch XGen™ Sicherheit eine neue Ebene linearen Echtzeit-Schutzes. Sie bietet proaktive Netzwerksicherheit für den heutigen und morgigen realen Netzwerkverkehr und für Rechenzentren. Die NX Serie nutzt eine Kombination von Technologien wie Deep Packet Inspection, Bedrohungsreputation und modernste Malware-Analyse auf einer nahtlosen Basis, um Angriffe auf das Netzwerk zu erkennen und zu verhindern. Sie ermöglicht es Unternehmen, einen proaktiven Ansatz für die Sicherheit umzusetzen und ein umfassendes Kontextbewusstsein sowie eine eingehendere Analyse des Netzwerkverkehrs zu ermöglichen. Dieses komplette Kontextbewusstsein, verbunden mit Informationen über Bedrohungen von Digital Vaccine® Labs (DVLabs) und der Zero Day Initiative (ZDI) bietet die nötige Sichtbarkeit und Flexibilität, um mit den heutigen, sich dynamisch entwickelnden Unternehmensnetzwerken Schritt zu halten.

Lebenszyklus einer Softwareschwachstelle



Lebenszyklus einer Softwareschwachstelle

Funktionen

- Höchste Portdichte
  NX Series unterstützt Konfigurationen mit bis zu 24 1GE-Segmenten, 16 10GE-Segmenten oder 4 40GE-Segmenten.
- Virtuelles Patching
  Ein leistungsfähiger und skalierbarer Abwehrmechanismus zum Schutz vor bekannten Bedrohungen, der sich auf die schwachstellenorientierten Filter stützt, um eine wirksame Barriere gegen Angriffe zu schaffen, die eine bestimmte Sicherheitsanfälligkeit ausnutzen möchten
- Schwachstellenschutz für Unternehmen
  Mit dieser Funktion können Kunden Informationen von verschiedenen Schwachstellenmanagement und Incident Response Anbietern nutzen, bekannte Schwachstellen (Common Vulnerabilities and Exposures, CVE) bestimmten Sicherheitsfiltern von TippingPoint Digital Vaccine zuordnen und entsprechende Maßnahmen ergreifen.
- Integrierter Schutz
  NX Series lässt sich in TippingPoint Advanced Threat Protection integrieren. Die Auszeichnung durch NSS Labs als effektivstes System zur Erkennung von Sicherheitsverletzungen mit der Bewertung „Empfehlenswert" demonstriert die hohe Wirksamkeit bei der Erkennung gezielter Angriffe und komplexer Bedrohungen.[1]

Vorteile

- Neutralisierung bekannter und unbekannter Malware:
  Erkennt und sperrt aktiv Angriffsversuche bekannter und unbekannter Malware
- Netzwerkverfügbarkeit:
  Inline-Installation auf einer speziell entwickelten Hardware mit Funktionen, die eine zuverlässige Leistung während eines Angriffs sicherstellen
- Branchenführende Bedrohungsinformationen:
  Nutzt Erkenntnisse der führenden Forschungsteams Zero Day Initiative (ZDI) und Digital Vaccine® Labs (DVLabs), um Unternehmenswerte durch aktuelle und umfassende Bedrohungsinformationen zu schützen
- Einfacher Betrieb:
  Zentrale Verwaltung von Richtlinien und Geräten mit TippingPoint Security Management System

1 -NSS Breach Detection System Test Report 2015

TippingPoint Threat Protection System (TPS)

Trend Micro TippingPoint Threat Protection System (TPS) ist eine Netzwerksicherheitsplattform unterstützt durch XGen™ Sicherheit. Sie bietet einen umfassenden Bedrohungsschutz gegen Schwachstellen, blockiert Exploits und bekämpft bekannte und Zero-Day-Angriffe mit hoher Genauigkeit. Es bietet branchenführende Abdeckung über die verschiedensten Bedrohungsvektoren von komplexen Bedrohungen, Malware und Phishing usw. hinweg, mit maximaler Flexibilität und hoher Leistung. TPS nutzt eine Kombination von Technologien wie Deep Packet Inspection, Bedrohungsreputation und modernste Malware-Analyse auf einer nahtlosen Basis, um Angriffe auf das Netzwerk zu erkennen und zu verhindern. Die Plattform ermöglicht es Unternehmen, einen proaktiven Ansatz für die Sicherheit umzusetzen und ein umfassendes Kontextbewusstsein sowie eine eingehendere Analyse des Netzwerkverkehrs zu ermöglichen. Dieses komplette Kontextbewusstsein, verbunden mit Informationen über Bedrohungen von Digital Vaccine Labs (DVLabs) bietet die nötige Sichtbarkeit und Flexibilität, um mit den heutigen, sich dynamisch entwickelnden Unternehmensnetzwerken Schritt zu halten.

Funktionen

- On-box-SSL
  Bietet Unternehmen die Möglichkeit, die Sicherheits-Blindspots zu reduzieren, die durch verschlüsselten Verkehr erzeugt werden
- Machine Learning zum Stopp von Exploit-Kits in Echtzeit
  Statistische Modelle, die mit Machine Learning entwickelt wurden, verfügen über die Fähigkeit, Exploit-Kits in Echtzeit auf dem TPS zu erkennen und abzuschwächen
- Enterprise Vulnerability Remediation (eVR)
  Ermöglicht es Kunden, Informationen von verschiedenen Anbietern für das Schwachstellen- und Vorfallmanagement zu sammeln, den TippingPoint Digital Vaccine-Filtern die Common Vulnerabilities and Exposures (CVEs) zuzuordnen und entsprechend zu handeln
- Hohe Verfügbarkeit
  TPS verfügt über mehrere fehlertolerante Funktionen, die es ideal für die „inline" Bereitstellung machen, einschließlich Hot-Swap-fähige Stromversorgungen, integrierte Inspection-Umgehung und Zero Power High Availability (ZPHA)
- Integrierter Schutz
  Die TPS Produktfamilie ist kompatibel mit Trend Micro Deep Discovery und TippingPoint Advanced Threat Protection; von NSS Labs als effektivstes Data Breach System empfohlen, um zielgerichtete Angriffe und komplexe Bedrohungen zu erkennen und zu blockieren
- Flexibilität
  TippingPoint TPS ist darauf ausgelegt, um Ihrem Netzwerk zu folgen, egal ob lokal oder online
- Einfache Verwaltung
  TippingPoint Security Management System bietet eine einzige Stelle zur Verwaltung von Richtlinien und Geräten
- Virtuelles Patching
  Ein leistungsfähiger und skalierbarer Abwehrmechanismus zum Schutz vor bekannten Bedrohungen, der sich auf die schwachstellenorientierten Filter stützt, um eine wirksame Barriere gegen Angriffe zu schaffen, die eine bestimmte Sicherheitsanfälligkeit ausnutzen möchten

Vorteile

- Macht bekannte und unbekannte Malware unschädlich
  Entdeckt und blockiert Angriffe durch bekannte und unbekannte Malware
- Unübertroffene Sichtbarkeit
  Überwacht alle Arten des Datenverkehrs einschließlich des verschlüsselten, um Angriffe zu erkennen und abzuschwächen
- Netzwerkzuverlässigkeit
  Enthält speziell entwickelte Hardware mit Funktionen, um bei einem Angriff höchste Leistung zu bieten
- Branchenweit führende Informationen über Bedrohungen
  Führende Forschungsteams für die aktuelle Bedrohungsabdeckung nutzen, um Ihre Vermögenswerte zu schützen
- Umfangreiche Sicherheitslösung
  Lösung eines einzigen Anbieters für Netzwerksicherheit, komplexe Bedrohungen und Endnutzerschutz

POWERED BY XGen™ SECURITY

Trend Micro TippingPoint Produkte und Lösungen unterstützt durch XGen™ Sicherheit – einem intelligenten, optimierten und vernetzten Sicherheitsansatz.

08 SICHERHEITSVERWALTUNG / OFFLINE-SICHERHEIT

Trend Micro Control Manager

Vereinfachen Sie die Administration der Trend Micro Sicherheitslösungen mit dem Control Manager. Diese webbasierte Management-Konsole überwacht die Sicherheitsleistung, berichtet über Malware-Vorfälle und Richtlinienverstöße und automatisiert Routineaufgaben. Die neuen Funktionen umfassen ein anpassbares Dashboard und einen schnellen Überblick über Bedrohungsstatistiken des Trend Micro Smart Protection Network, der cloud-basierten Sicherheitsinfrastruktur von Trend Micro.

Vorteile

- **Reduziert Risiken**
  Transparenz und Kontrolle der Sicherheit
- **Senkt Kosten**
  Vereinfacht die Sicherheitsverwaltung
- **Minimiert die Komplexität**
  Schafft ein integriertes, zentral verwaltbares Sicherheits system mit einheitlichen Abwehrfunktionen.

Control Manager ist in zwei Versionen erhältlich: Standard und Advanced

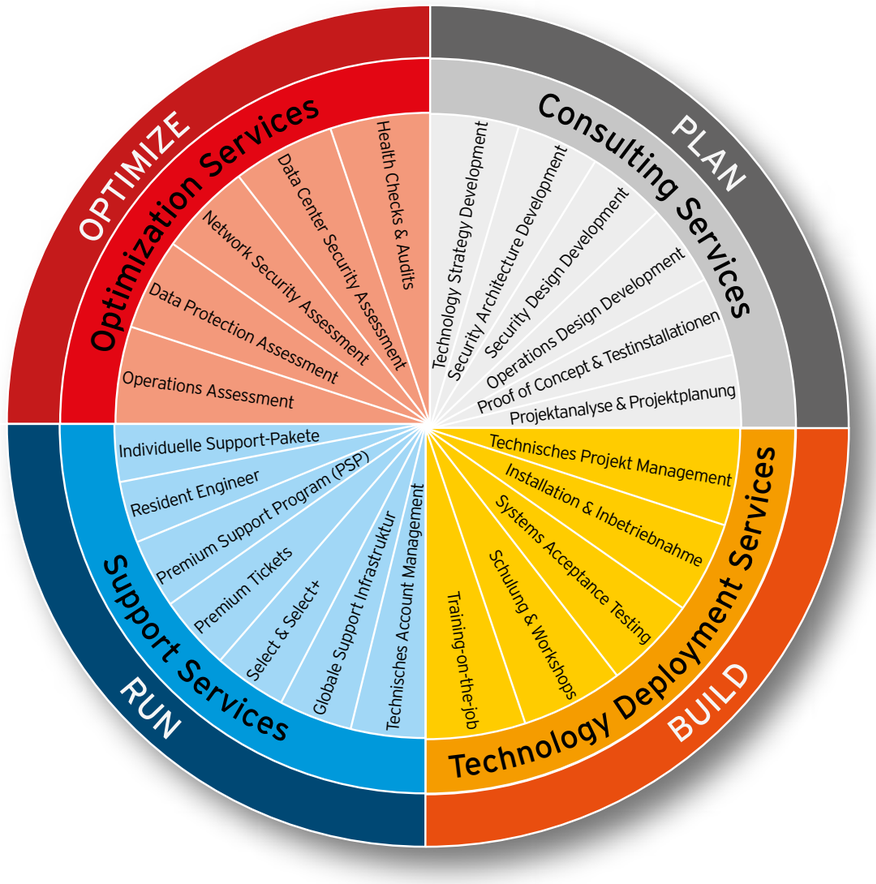
TREND MICRO CONTROL MANAGER	STANDARD	ADVANCED
Webbasierte, zentrale Sicherheitsverwaltung	●	●
Anpassbares Dashboard, bedarfsgesteuerte Abfrage, Warnhinweise	●	●
Bedrohungsstatistiken des Smart Protection Network	●	●
Transparenz in Clients		●
Mehrschichtige Verwaltung		●
Anpassbares Reporting		●
Lizenzverwaltung		●

09 SERVICE & SUPPORT

Services

Mit einer globalen Service & Support Organisation ist Trend Micro optimal aufgestellt, um nationale und internationale Kunden hinsichtlich der wachsenden Anforderungen im IT-Security Bereich zu unterstützen. Unsere Services basieren auf bewährten Methoden und ermöglichen es Ihnen, Produkte und Lösungen von Trend Micro in vollem Umfang zu nutzen und Ihre Investitionen langfristig zu schützen. Unsere Dienstleistungen decken den gesamten Lebenszyklus unserer Lösungen ab und reichen von Beratungsleistungen (PLAN) über die Unterstützung bei der Inbetriebnahme (BUILD) und dem Betrieb (RUN) bis hin zu Services, deren Ziel der optimierte Einsatz unserer Lösungen, die Erhöhung des Sicherheitsniveaus und Reduktion von administrativen Kosten ist (OPTIMIZE).

Das Trend Micro Service & Support-Netz spannt sich über den gesamten Globus – in jedem Kontinent der Erde ist Trend Micro mit Spezialisten für alle Produkte und Services vertreten. Basis für unsere Support-Leistungen sind vier global agierende Support Center (Center of Excellence, CoE), die einen hochwertigen Support für Ihre geschäftskritischen Umgebungen 24x7 bereitstellen. Ergänzend zu den technischen Spezialisten von Trend Micro stehen insbesondere zur Lieferung von Professional Services zertifizierte Servicepartner bereit.



09 SERVICE & SUPPORT

Consulting Services

Durch die kurzen Innovationszyklen der Technologien und die sich ständig ändernden Bedrohungslagen gibt es inzwischen verschiedene Lösungsansätze für die Bereiche der IT-Security. Investitionsentscheidungen müssen in diesem wettbewerbsintensiven Markt in immer kürzeren Zeiträumen vorbereitet, getroffen und realisiert werden. Mit unseren Consulting Services haben Sie Zugriff auf das Wissen und die Erfahrung unserer technischen Experten, die Sie beim Erreichen Ihrer Unternehmensziele unterstützen.

Unsere Consultants planen und designen in enger Zusammenarbeit mit Ihrem IT-Team Ihre Security Infrastruktur:

- Nach einer detaillierten Bestandsaufnahme liefern erfahrene Experten Unterstützung bei schwierigen technischen Herausforderungen und entwickeln zukunftssichere Lösungen für Ihre komplexen Anforderungen und die optimale, speziell auf Ihre Bedürfnisse zugeschnittene Architektur, um die Effektivität der Trend Micro Lösungen zu maximieren.
- Im Rahmen von Proof of Concepts (PoC) / Proof of Technologies (PoT) demonstrieren wir Ihnen die Vorteile der Trend Micro-Lösungen in einer Testumgebung. Unsere Experten zeigen und erläutern Ihnen die Funktionalität abgestimmt auf Ihre individuellen Anforderungen, so dass Sie bereits vor einer aufwendigen, vollständigen Implementierung konkrete Ergebnisse sehen.

Technology Deployment Services

Mit unseren Deployment Services unterstützen wir Sie bei der reibungslosen Implementierung neuer Produkte oder dem Upgrade bestehender Lösungen in Ihrer IT-Infrastruktur mit dem Ziel, einen maximalen Return on Investment zu gewährleisten. Unser Team analysiert Ihre Netzwerk- und Systemumgebung hinsichtlich der Leistungsanforderungen und Ihrer Sicherheitsstrategien. Auf Basis bewährter Vorgehensweisen entwickeln unsere Consultants gemeinsam mit Ihnen einen Umsetzungsplan. Im Fall von größeren Projekten wird die Umsetzung durch einen erfahrenen Projektmanager begleitet, der die notwendigen Ressourcen koordiniert und den Projektfortschritt kontinuierlich überwacht. Nach der Genehmigung des Umsetzungsplans wird die Lösung unter Berücksichtigung Ihrer Change-Management-Richtlinien implementiert. Die Implementierung endet in der Regel mit der Durchführung eines Abnahmetests, um die Funktionalität der Features der Lösung in Ihrer Umgebung nachzuweisen.

Schulungen

Unser umfassendes Schulungsprogramm hilft Ihnen dabei, Kenntnisse für die Installation, Konfiguration und Administration der bei Ihnen eingesetzten Trend Micro Lösungen zu erwerben und zu erweitern. Unsere Kurse werden in Trainingscentern bei Trend Micro oder bei unseren Trainings Partnern von erfahrenen Trainern durchgeführt und umfassen neben der Vermittlung von theoretischem Wissen Laborübungen, in denen Lerninhalte sofort praktisch umgesetzt werden. Das Kursangebot erstreckt sich über unser gesamtes Produktportfolio und reicht von Schulungen für Endpunkt und mobile Sicherheit, über Cloud- und Virtualisierungssicherheit bis hin zu Lösungen, die Schutz vor gezielten Angriffen bieten. Unsere Schulungen unterstützen Sie dabei, administrative Tätigkeiten zu reduzieren, das Schwachstellen-Management im Unternehmen zu verbessern, die Risiken zu minimieren und den allgemeinen Schutz des Unternehmens zu erhöhen.

Support

Trend Micro bietet Ihnen ein umfassndes Angebot an Supportleistungen, die entweder direkt oder von einem von Trend Micro beauftragten Unternehmen erbracht werden.

Standard Support

Für Business-Kunden steht der Trend Micro 24x7 Support bereits im Standard Support zur Verfügung welcher Bestandteil jedes aktiven Wartungsvertrages ist. Im Falle eines kritischen technischen Problems können Kunden, je nach Unternehmensgröße, direkt mit einem der vielen hochzertifizierten Trend Micro Support Mitarbeiter – den sogenannten Customer Service Engineers (CSE) – per Mail, Telefon, Chat oder über ein Webportal Kontakt aufnehmen. Die Customer Service Engineers helfen Ihnen bei dringlichen Angelegenheiten, zum Beispiel bei der Diagnose und Behebung von Problemen.

24x7 Support

Holen Sie sich die Expertise, die Sie brauchen – jederzeit. Der Trend Micro 24x7 Support umfasst die Inanspruchnahme von Customer Service Engineers, einem hochqualifizierten Team aus ehemaligen Systemadministratoren, Netzwerk- und Rechenzentrumstechnikern sowie Serviceberatern mit langjähriger Erfahrung, die sich täglich mit Sicherheitsherausforderungen auseinandersetzen. Unsere Spezialisten verfügen über umfangreiche Sicherheitsexpertise und Zugang zum globalen Technik-Ökosystem von Trend Micro und Tools zur Bewältigung einer Vielzahl von Sicherheitsherausforderungen, einschließlich Content-und Risikomanagement sowie der Verwaltung von Rechenzentren. Der Trend Micro 24x7 Support ist bei aktiven Wartungsverträgen für alle Business Produkte enthalten. Außerhalb der Bürozeiten gilt der 24x7 Support ausschließlich für „CRITICAL"-Cases (siehe www.trendmicro.com/severitydefinitions).

Customer Service Engineer

Die Trend Micro Customer Service Engineers sind der sich ständig wandelnden Bedrohungslandschaft immer einen Schritt voraus. Mindestens 25 % ihrer Zeit verbringen sie damit, sich weiterzubilden und ihr Wissen auszubauen. Dazu nehmen sie an internen und externen Schulungen teil, führen praktische Test zur Produktreife durch und erforschen neue Sicherheitsbedrohungen. Dank spezieller Schulungen sind unsere Customer Service Engineers in der Lage, die IT-Herausforderungen von heute fachkundig zu bewältigen – einschließlich Konsumerisierung, Cloud und Modernisierung von Rechenzentren sowie gezielte Angriffe, die eine Gefahr für Ihre wertvollen Daten sind.

Premium Support

Die Bewertung und Verwaltung Ihrer Unternehmenssicherheit ist eine echte Herausforderung – insbesondere angesichts gezielter Angriffe und anderer Bedrohungen, die sich über moderne Technologien wie Mobile und Cloud verbreiten. Wir wissen, wie schwer es ist, eine lückenlose Sicherheit und den permanenten Schutz Ihrer Daten und Infrastruktur vor neuen Bedrohungen zu gewährleisten. Der speziell für Großunternehmen und sehr große Organisationen konzipierte Trend Micro Premium Support stellt Ihnen fachkundige Ressourcen an die Seite, damit Sie die personalisierten Lösungen nutzen können, die Sie für einen lückenlosen Schutz brauchen. Ein persönlicher Customer Service Manager (CSM) hilft Ihnen bei der für Ihr Unternehmen effektivsten Sicherheitsimplementierung. Unsere Sicherheitsexperten sind umfassend geschult, um Sie bei der schnellen Reaktion auf Bedrohungen, Planung, Vorbereitung auf den Ernstfall und Lösungsoptimierung gezielt anzuleiten. Die Customer Service Manager konzentrieren sich auf Ihre Umgebung, Geschäftsprozesse und Ihren individuellen Sicherheitsansatz, damit Sie die maximale Rendite aus Ihren Sicherheitsinvestitionen erzielen. Die CSMs fungieren als Ihre persönlichen Vertreter bei Trend Micro: Sie schneiden unsere Lösungen auf Ihre spezifischen Unternehmens- und Sicherheitsbedürfnisse zu und ziehen bei Bedarf Spezialisten hinzu.

Der Trend Micro Premium Support beinhaltet:

- Optimierte Implementierung Ihrer Trend Micro Sicherheitslösung für den bestmöglichen Schutz Ihrer spezifischen Umgebung
- Echtzeitberatung zu aktuellen Sicherheitsbedrohungen und -risiken, mit der Sie Infektionen und gezielten Angriffen vorbeugen und den Verlust von geistigem Eigentum und anderen Daten verhindern können
- Regelmäßige Health Checks, die den permanenten Schutz vor Datenverlust und Geschäftsunterbrechungen sicherstellen
- Fachkundige Beratung zu Ihren ganz persönlichen Sicherheitsproblemen. Dadurch sparen Sie Zeit und Geld, denn Sie brauchen keine Sicherheitsoptionen zu untersuchen und implementieren keine suboptimalen Konfigurationen.
- Die jährlichen Meetings zur Sicherheitsplanung mit Ihren Management-Teams gewährleisten, dass Sie Ihre Sicherheitssysteme optimal nutzen und Sicherheitsinvestitionen nach den jeweiligen Bedürfnissen und Zielen priorisieren können. Ihr Customer Service Manager bietet Ihnen eine detaillierte Auswertung Ihres Sicherheitsprofils einschließlich möglicher Lücken und deren Behebung.

Customer Service Manager

Die Customer Service Manager arbeiten eng mit Ihrem Team zusammen, um einen reaktionsschnellen und persönlichen Service und Schutz zu bieten. Sie konzentrieren sich auf Ihr Unternehmen und entwickeln operative Strategien, die optimal auf Ihre Umgebung zugeschnitten sind. Durch die enge Zusammenarbeit kann Ihr Customer Service Manager Sie bei den komplexesten Sicherheitsaspekten unterstützen, Ihr Sicherheitsprofil technologie-, prozess- und mitarbeiterübergreifend optimieren und Ihre Trend Micro Sicherheitslösungen so konfigurieren, dass optimierte IT-Servicelevel erzielt werden.

Einzelheiten zum Support entnehmen Sie bitte dem Technical Support Guide unter https://esupport.trendmicro.com/media/13616460/Europe-Technical-Support-guide-2016.pdf

SUPPORT-ANGEBOTE

DAS KÖNNEN SIE VON DEN TREND MICRO SUPPORT SERVICES ERWARTEN	TREND MICRO 24X7 SUPPORT*	TREND MICRO PREMIUM SUPPORT
Telefonischer Support	Service rund um die Uhr	Service rund um die Uhr
Dedizierte Ansprechpartner	3	4
Produkt-Updates und -Upgrades	✓	✓
Support per Telefon, E-Mail und Internet	✓	✓
Inanspruchnahme von Customer Service Engineers	✓	✓
Zuweisung eines persönlichen Customer Service Managers		✓
Priorisierte Fallbearbeitung		✓
Analyse von verdächtigen Dateien (über Premium Support Connection)		✓
Unterstützung bei Installationen und Upgrades		✓
Laufende Sicherheitsbewertungen und -empfehlungen		✓
Monatliche Anrufe und jährliches Treffen vor Ort		✓
Anzahl der Regionen		1
Geeignet für globale und große Unternehmen		✓

* Der Trend Micro 24x7 Support ist bei aktiven Wartungsverträgen für alle Business Produkte enthalten (siehe www.trendmicro.com/severitydefinitions).

10 LIZENZIERUNGSLEITFADEN

Lizenzschritte

Lizenzen werden in folgenden Lizenzschritten vergeben:
5- 250 User: in 5er-Schritten
251 – 1.000 User: in 10er-Schritten
1.000 + User: in 25er-Schritten

Beispiel

Bei 573 E-Mail-Accounts wird auf die nächst höhere durch 10 teilbare Useranzahl (demnach auf 580 User) aufgerundet. Bitte beachten Sie: Die Staffelung für Enterprise Produkte beginnt ab 26 Usern.

Lizenzierung SMB Produkte

Trend Micro SMB Produkte sind ab einer Mindestanzahl von 5 Usern erhältlich.

Ausnahmen: Worry-Free Services ist ab 2 Usern verfügbar und kann in 1er-Schritten bezogen werden.

Trend Micro Worry-Free Produkte: Lizenziert wird die Summe der Anzahl aus Clients und Server. Jede virtuelle Maschine, auf der eine Worry-Free Lösung installiert ist, wird ebenfalls mitgezählt. Die Lizenzierung ist von 5 bis 250 Usern möglich.

Beispiel

Muster GmbH möchte mit Worry-Free Advanced ihr Netzwerk schützen. Die Firma hat 5 Server und 40 PC Arbeitsplätze, sowie 30 Mitarbeiter im Unternehmen. Lizenziert werden 45 User.

Lizenzierung Enterprise Produkte

Trend Micro Enterprise Produkte sind ab einer Anzahl von 26 Usern erhältlich. Nach oben ist die Anzahl unbegrenzt.

Lizenziert wird jeder User, der Zugang zu einem Endgerät hat, welches entweder direkt durch die darauf installierte Trend Micro Software geschützt wird oder über welches indirekt auf Server zugegriffen werden kann, welche den Netzwerkverkehr bzw. die auf den Servern hinterlegten Daten des entsprechenden Users durch die darauf installierte Trend Micro Software schützen. Dies gilt auch bei zeitversetzter Nutzung eines Endgerätes durch mehrere Mitarbeiter. Grundlage zur Ermittlung der benötigten Lizenzen kann z. B. die Anzahl der personalisierten E-Mail-Accounts sein. Die Anzahl der Endgeräte/Server, auf der das Produkt aufgesetzt wird, ist irrelevant.

Beispiel 1

Muster GmbH kauft eine Sicherheitslösung für den Mailserver Microsoft Exchange für 400 personalisierte E-Mail-Accounts. Erworben wird ScanMail for Exchange für 400 User. (Sammelaccounts wie info@muster.com, vertrieb@muster.com, etc. sind keine personalisierten Postfächer)

Beispiel 2

Muster GmbH erwirbt als Sicherheitslösung für seine Clients Trend Micro Enterprise Security for Endpoints. Ausschlaggebend ist die Anzahl der zu schützenden User, nicht die der Laptops, Workstations oder Server. Es sollen 100 Mitarbeiter geschützt werden, die insgesamt 120 PCs bzw. Laptops nutzen. Lizenziert werden 100 User.

Deep Security Lizenzierung: Lizenziert wird nach der Anzahl der installierten (virtuellen) Desktops / Server. Alternativ ist eine CPU-basierte Lizenzierung möglich. In public Cloud Umgebungen muss pro Desktop/Server lizenziert werden.

Beispiel

Muster GmbH möchte ihre 4 ESX Server mit je 2 CPUs durch Deep Security schützen. Je Server sind 5 virtuelle Maschinen im Einsatz. Lizenziert werden demnach 20 virtuelle Maschinen.

Lizenzierung Support-Leistungen

Für **Premium Support** Leistungen unterbreiten wir gerne ein individuelles Angebot auf Anfrage.

Neukauf

Unter Neukäufer fallen Kunden, die ihre erste Trend Micro Lizenz erwerben, beziehungsweise ein bestimmtes Produkt zum ersten Mal kaufen. Das Kaufdatum gilt als Anfangsdatum der Lizenz. Die Laufzeit einer Lizenz beträgt immer 1 Jahr. Wird ein mehrjähriger Lizenzvertrag geschlossen, gilt das erste Jahr als Neukauf. Die darüber hinausgehenden Jahre gelten als Verlängerung.

Lizenzerweiterung

Eine Lizenzerweiterung bezeichnet den Erwerb von zusätzlichen „Usern" durch Kunden, die bereits eine gültige Lizenz für das betreffende Produkt besitzen. Lizenzerweiterungen haben eine Laufzeit von 12 Monaten, die am Tag der Lieferung beginnt. Bei einer Lizenzerweiterung erreicht der Kunde unter Umständen eine höhere Lizenzstaffel und somit einen günstigeren Preis pro Lizenz. Die Berechnung der Lizenzerweiterung erfolgt stets in drei Schritten:

1. Schritt:
Die Anzahl der neuen User wird zur Anzahl der bestehenden hinzugefügt.
2. Schritt:
Für die Lizenzaufstockung wird der Stückpreis des Gesamtlizenzvolumens zugrunde gelegt.
3. Schritt:
Um ein einheitliches Ablaufdatum der alten und der neuen Lizenzen zu erreichen, muss bei den vorhandenen Lizenzen die Laufzeit entsprechend verlängert werden.

(Berechnung mit 2,5 % des Listenpreises je angefangenem Monat (30 % p.a.; bzw. 35 % p.a. für Worry-Free Lösungen) auf Basis des Stückpreises des Gesamtlizenzvolumens).

Wartungsverlängerung

Um die Nutzungsrechte eines Trend Micro Produkts zu behalten, muss vor Ablauf der Lizenzlaufzeit eine jährliche Wartungsverlängerung erworben werden. Für das erste Installationsjahr (Neukauf) ist die Wartung für 12 Monate im Kaufpreis enthalten. Der Wartungsanspruch umfasst Software Upgrades, Scan Engine- und Pattern File-Updates, sowie Zugang zu unserem 24x7 Standardsupport. Danach beträgt die Wartungsgebühr für 12 Monate 30 % (bzw. 35 % für Worry-Free Lösungen) vom jeweils aktuell gültigen Listpreis (Ausnahme siehe „Wartungsverlängerung von Services").

Bei der Verlängerung einer Lizenz beginnt die neue Laufzeit am Tag nach Ablaufdatum der vorhergehenden Lizenz. Dies gilt auch für den Fall, dass der Kunde seine Lizenz erst nach Ablaufdatum der vorhergehenden Lizenz verlängert.

Beispiel

Die Lizenz endet am 7. Juli:
- Die Laufzeit der Verlängerung beginnt am 8. Juli
- Sollte der Kunde die Lizenzverlängerung erst im August vornehmen, beginnt die Laufzeit der Verlängerung dennoch am 8. Juli

Wartungsverlängerung von Services

Trend Micro Services beruhen auf einer jährlich wiederkehrenden Nutzungsgebühr in Höhe von 100 % des jeweils aktuell gültigen Listpreises. Eine Wartungsverlängerung im klassischen Sinne gibt es daher nicht. Dies gilt z. B. für die Smart Protection Suites oder Worry-Free Services.

Cross-Upgrades

Ein Cross-Upgrade bezeichnet den Wechsel eines Kunden von einem Trend Micro Produkt oder einer Suite zu einer anderen Suite. Bereits im Einsatz und unter Wartung befindliche Trend Micro Produkte können mit ihrem Lizenzvolumen angerechnet werden. Die Wartung des bestehenden Produkts verfällt und beginnt mit dem Kauf des Produkt-Bundles aufs Neue für 12 Monate.

Cross-Grades

Bei einem Cross-Grade wechselt ein Kunde von einer bestehenden Plattform zu einer anderen; z. B. von Trend Micro ScanMail for Exchange zu Trend Micro ScanMail for IBM Domino. In diesem Fall bleiben Anfangs- und Ablaufdatum der ursprünglichen Lizenz bestehen. Es entfällt eine Wechselgebühr zum jeweiligen Listenpreis.

Discounts

Government Discount (eGovernment) bis zu 30%:
Gilt für nationale und kommunale Behörden, Städte, Landkreise, Ämter, Verwaltungen, städtische Krankenhäuser, Einrichtungen, die mindestens zu 50 % oben genannten Institutionen angehören, sowie Körperschaften des öffentlichen Rechts.

Academic Discount (NGO / NPO) bis zu 40%:
Gilt für alle Non-Government-/Non-Profit-Organisationen, staatliche oder staatlich anerkannte allgemein- und berufsbildende Schulen und Hochschulen, staatlich anerkannte Einrichtungen der Erwachsenenbildung; nicht-kommerzielle Einrichtungen, z. B. Kirchen und Glaubensgemeinschaften sowie Vereine, die ihre Gemeinnützigkeit belegen können, wie z. B. DRK, DFB, IOC, UNICEF.

Competitive Discount:
Bei Ablöse eines oder mehrerer kostenpflichtiger und vergleichbarer Mitbewerberprodukte gewährt Trend Micro einen Preisnachlass. Der Lizenznachweis über das bestehende Mitbewerberprodukt ist spätestens bei Bestellung vorzulegen.

Evaluierung von Lizenzen

Jede Trend Micro Lösung kann 30 Tage lang kostenlos getestet werden. Zum Download der Testlizenz gehen Sie bitte auf www.trendmicro.com. Benötigt Ihr Kunde einen Test-Key für einen längeren Zeitraum, richten Sie bitte eine Anfrage an sales@trendmicro.de unter Angabe folgender Informationen:

- Händlername
- Endkundenname
- Endkundenadresse
- Produktbezeichnung
- gewünschte Laufzeit
- Betriebssystem
- Sprache
- Produktversion
- Lizenzgröße

Lizenzzusammenführung innerhalb eines Konzerns

Lizenzen zweier Konzernunternehmen können im Zuge einer Wartungsanpassung (einheitliches Laufzeitende gleicher Produkte) innerhalb eines Konzerns zusammengefasst bzw. umgeschrieben werden. Hier ist eine Rücksprache mit einem Trend Micro Mitarbeiter erforderlich.

Das Konzernunternehmen, das die Lizenzen auf den Konzern umschreiben lässt und somit abtritt, muss sein Einverständnis darüber schriftlich erklären.

Sonstiges

Grundlage der Trend Micro Lizenzierung ist das „End User License Agreement" (EULA)
www.trendmicro.de/ueber-uns/rechtliche-hinweise/endbenutzer-lizenzvereinbarungen

Für Großkunden können abweichende individuelle Regelungen in Betracht kommen. Änderungen vorbehalten.

11 ANALYSTENMEINUNGEN, BRANCHENAUSZEICHNUNGEN & REFERENZEN

Trend Micro wurde mehrfach zum Marktführer im Bereich Endpunktsicherheit, Cloud-Sicherheit und Serversicherheit gekürt, und unsere Systeme zur Intrusion Prevention und Erkennung von Sicherheitsverstößen werden von Experten gerne empfohlen. Außerdem haben wir das weltweit umfassendste Netzwerk für Bedrohungsinformationen – unser Trend Micro™ Smart Protection Network™ wird laufend über Big Data-Analysen und maschinelles Lernen erweitert und durch Hunderte von Trend Micro Sicherheitsexperten und die Zero Day Initiative (ZDI) gestützt.

User Protection

Seit 2002 führend im Gartner Magic Quadrant for Endpoint Protection Platforms
Trend Micro erreicht im Leader-Quadrant des 2017 Gartner Magic Quadrant for Endpoint Protection Platforms die höchste Position für „Umsetzungskompetenz" und „Umfassende Vision". (Die Definition von Endpunkten beinhaltet bei Gartner auch Server). TippingPoint NGIPS wurde im Gartner Magic Quadrant 2017 for Intrusion Detection and Prevention Systems zur Nummer 1 gekürt.

[2] Gartner „Magic Quadrant for Endpoint Protection Platforms" von Eric Ouellet, Ian McShane, Januar 2017

Gartner spricht keine Empfehlungen für die in den Forschungspublikationen genannten Anbieter, Produkte oder Dienstleistungen aus und rät Technologie-Anwendern nicht, nur die Anbieter mit den besten Bewertungen zu wählen. Die Forschungspublikationen von Gartner geben die Meinung des Gartner Forschungsinstituts wieder und sind nicht als Tatsachen zu werten. Gartner lehnt jegliche Gewähr in Bezug auf diese Forschung ab, explizit oder implizit, einschließlich Garantien der Marktgängigkeit oder Eignung für einen bestimmten Zweck.

Forrester Wave™ platziert Trend Micro als führenden Anbieter von Suites für Endpunktsicheheit, 4. Quartal 2016

Trend Micro schneidet bei Langzeittests zur Bewertung von Endpunktsicherheit am besten ab

„Nachdem die Sicherheitslösung von Trend Micro in der Kategorie »Protection« hervorragend abschnitt und außerdem die geringste Auslastung der Clients erzielte, kam sie mit insgesamt 17,2 Punkten auf den ersten Platz."

AV-Test.org, Langzeittests zur Bewertung von Endpunktsicherheit, Februar 2014

Von der Info-Tech Research Group als beste Lösung im Bereich Endpunktsicherheit für 2014 gekürt
„Trend Micro wurde in der aktuellen Anbieterstudie der Info-Tech Research Group als »Champion« im Bereich Endpunktsicherheit ausgezeichnet."

Hybrid Cloud Security

Trend Micro ist weltweiter Marktführer im Bereich Serversicherheit

IDC, Worldwide Endpoint Security Market Shares, 2015: Currency Volatility Headwind, #US41867116, November 2016

Trend Micro als führender Anbieter von Cloud-Sicherheitslösungen gewählt
„Trend Micro ist zweifelsohne der führende Anbieter von Cloud-Sicherheitstechnologien und -Services und setzt damit die Maßstäbe für Marktbegleiter."

Experton Group, Cloud Vendor Benchmark 2014.

Network Defense

Trend Micro TippingPoint NGIPS wurde bei NGIPS-Tests als empfehlenswert eingestuft

NSS Labs, Breach Detection System Test Report 2016

Trend Micro Deep Discovery – das effektivste System zur Erkennung von Datensicherheitsverstößen mit der Bewertung „Empfehlenswert"
„Der Trend Micro Deep Discovery Inspector v3.7 Build 3.7.1096 erkannte HTTP-Malware, E-Mail-Malware und SMB-Malware in 100 % aller Fälle und Datensicherheitsverstöße in 96,6 % aller Fälle. Der Deep Discovery Inspector erkannte 98,3 % der getesteten Umgehungsmethoden gezielter Bedrohungen. Die Lösung bestand ferner darin alle Stabilitäts- und Zuverlässigkeitstests zu beauftragen."

NSS Labs, Breach Detection Systems Test Report – Trend Micro Deep Discovery Inspector v3.7 Build 3.7.1096, Juli 2016

11 ANALYSTEN-MEINUNGEN, BRANCHENAUSZEICHNUNGEN & REFERENZEN

Anwenderberichte

WPD AG
Lösung:
- Deep Discovery Inspector 500
- Deep Discovery Analyzer
- InterScan Messaging Security Virtual Appliance
- OfficeScan
- Endpoint Encryption
- Portal Protect for Sharepoint

GISA IT
Lösung:
- Deep Discovery Inspector
- Deep Discovery Analyzer

BARTSCHER GMBH
Lösung:
- Scanmail for Exchange
- InterScan Messaging Security Virtual Appliance
- Deep Discovery Mail Inspector
- Control Manager

KLINIKUM OLDENBURG
Lösung:
- Deep Discovery Inspector
- Control Manager
- OfficeScan
- Scanmail for Exchange
- Server Protect
- Portal Protect

LÜCK GMBH & CO KG
Lösung:
- Deep Security
- Smart Protection Complete
- Deep Discovery Inspector
- Deep Discovery Email Inspector
- Deep Discovery Endpoint Sensor

UPC CABLECOM
Lösung:
- Deep Security for SAP

Q-PARTNERS CONSULTING UND MANAGEMENT GMBH
Lösung:
- Deep Security for SAP

MAZDA
Lösung:
- Complete User Protection

Referenzen

HORN & COSIFAN COMPUTERSYSTEME GMBH

REICHHARDT GMBH

QL-IT LÖSUNGEN GMBH

STAUDINGER GMBH

BURKHARDT GMBH

Eine vollständige und stets aktuelle Übersicht der Trend Micro Anwenderberichte und Referenzen finden Sie unter: www.trendmicro.de

12 KONTAKTE | SONSTIGES

Online Registrierung (Customer Licensing Portal)

Trend Micro liefert Produktlizenzen mit einem Registrierungsschlüssel (RK), der zum Anlegen eines Kontos und zur Produktregistrierung verwendet wird. Nach der Registrierung müssen die Benutzer die Software mit einem Aktivierungscode (AC) aktivieren. Damit können sie auf den ActiveUpdate Server zugreifen und aktualisierte Pattern-Dateien herunterladen.

Die Trend Micro Produkt Registrierung obliegt Ihnen oder einem von Ihnen beauftragtem Fachhändler.

Die Online-Registrierung ermöglicht die Aktivierung eines neu erworbenen Produktes, die Verlängerung eines bestehenden Produktes oder auch die Zusammenführung von Box-Produkten. Folgender Link bringt Sie zur deutschsprachigen Online-Registrierung: https://tm.login.trendmicro.com

Testversionen – Beta-Programm – Download Center – Technische Unterlagen

Sie haben jederzeit die Möglichkeit die neuesten Trend Micro Software-Lösungen zu testen.
So besteht die Möglichkeit an Beta-Tests und Programmen teilzunehmen.
Mehr unter: http://beta.trendmicro.com

Des Weiteren können Sie das Trend Micro Update Center nutzen, um Test bzw. Demo-Software von der Trend Micro Website herunterzuladen. Sie haben dann in der Regel 30 Tage Zeit, die gewünschte Software zu testen. Nach der kostenfreien Testphase können Sie die Lizenz erwerben oder die Testphase beenden. Für individuelle Testanfragen wenden Sie sich bitte an Ihren Fachhändler.
Mehr unter: http://downloadcenter.trendmicro.com

Technische Unterlagen wie Administrator's Guide, Installation Guide, System Requirements, Readme, u. a. finden Sie unter:

http://docs.trendmicro.com

Trend Micro Kontakt

D: 0800 330 4533* oder sales_info@trendmicro.de
AT: 0800 880 903* oder sales_info@trendmicro.at
CH: 0800 330 453* oder sales_info@trendmicro.ch

* Kostenfrei aus dem Festnetz des jeweiligen Landes. Abweichende Gebühren aus dem Mobilfunknetz.

Technisches Support Team – Allgemeine Informationen zum Support, wie z. B. Download Center, Support-Datenbank, erhalten Sie unter www.trendmicro.com ››› „Support" im Hauptmenü.
Um einen Support Case zu eröffnen: http://esupport.trendmicro.com/srf/SRFMain.aspx

NOTIZEN

NOTIZEN

WHAT´S YOUR X?

Lösen Sie es mit Trend Micro

In der heutigen Welt ständiger Veränderungen suchen wir **„nach Lösungen für X“**, wobei **„X“** für die Probleme unserer Kunden steht.

Unsere Sicherheitslösungen sind generationsübergreifend und schützen daher unsere Kunden nicht nur jetzt, sondern auch in Zukunft.

TREND MICRO Deutschland GmbH • Zeppelinstraße 1 • D-85399 Hallbergmoos
Tel: +49 811 88990-700
Fax: +49 811 88990-799

TREND MICRO (Schweiz) GmbH • Husacherstrasse 3 • CH-8304 Wallisellen
Tel: +41 43 233 77 81

www.trendmicro.com

Dieser Trend Micro Product Guide basiert auf dem Informationsstand September 2017.