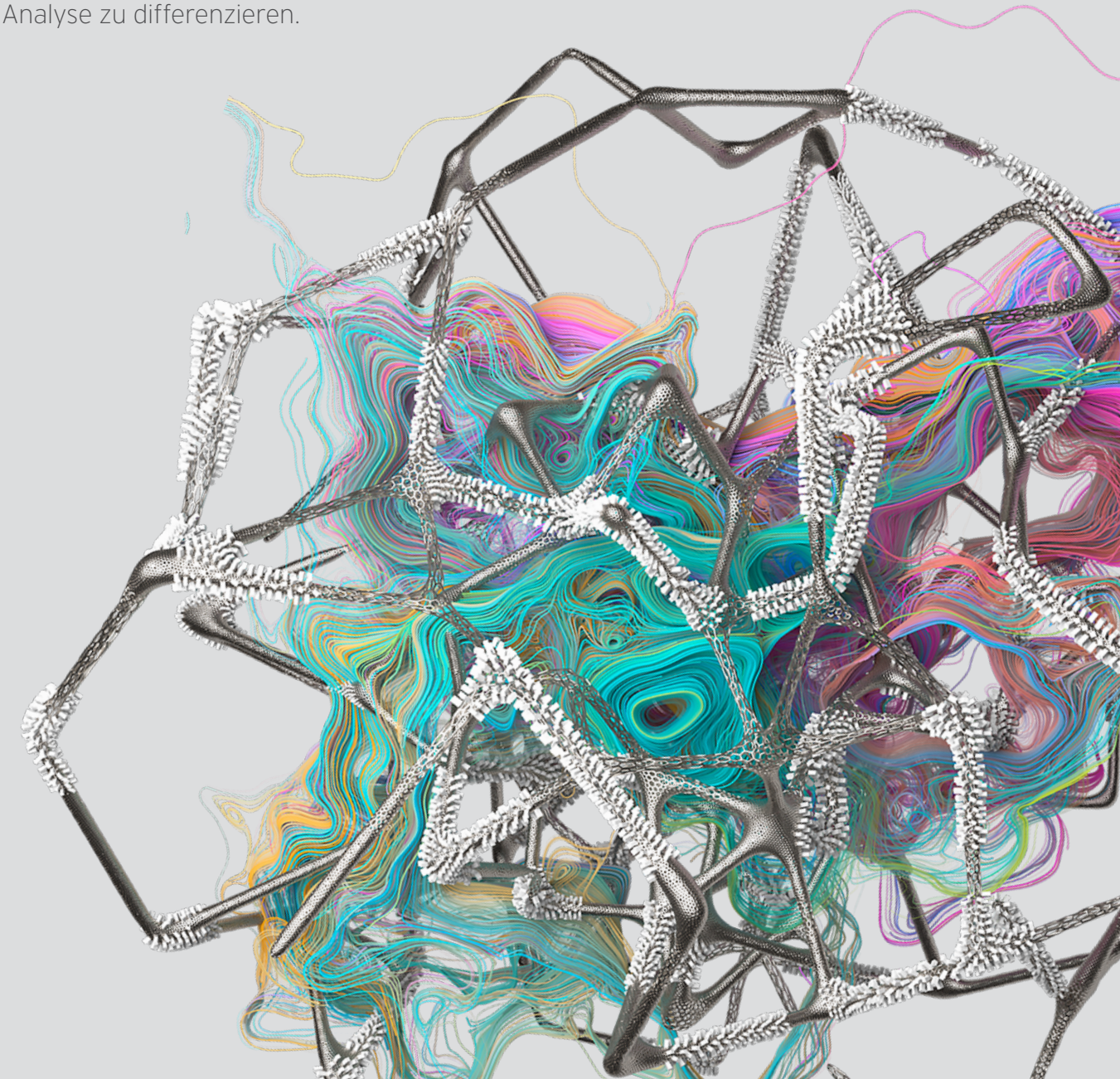
Trend Micro

BUYERS GUIDE FÜR ENDPUNKTSICHERHEIT

Beim Thema Endpunktsicherheit ist es sehr schwierig geworden, bloßen Hype von realen technischen Vorteilen zu unterscheiden. Gleichzeitig werden Sicherheitsbedrohungen immer komplexer und ausgefeilter. Deshalb ist es heute wichtiger als je zuvor, eine Lösung zu finden, die mit den Veränderungen der Bedrohungslandschaft auf Jahre hinaus Schritt halten kann.

Dieser Buyers Guide für Endpunktsicherheit definiert die zentralen Anforderungen an eine moderne Sicherheitslösung und unterstützt Unternehmen dabei, zwischen den vielen verschiedenen auf dem Markt angepriesenen Funktionen für Identifikation, Schutz und Analyse zu differenzieren.

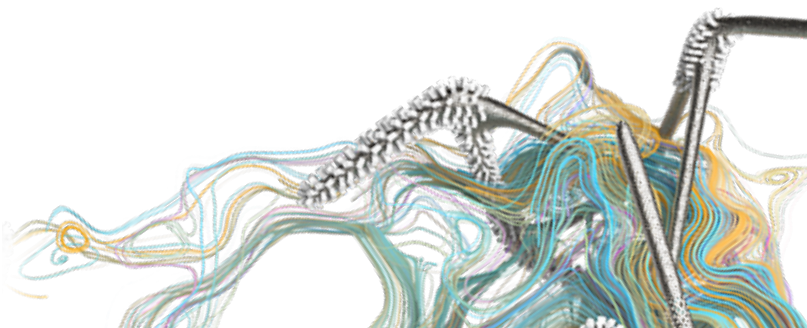


INHALT

>> KLICKEN SIE AUF EINEN EINTRAG, UM MEHR ÜBER DEN VORTEIL ZU ERFAHREN.

AUTOMATISIERTE ERKENNUNG UND REAKTION

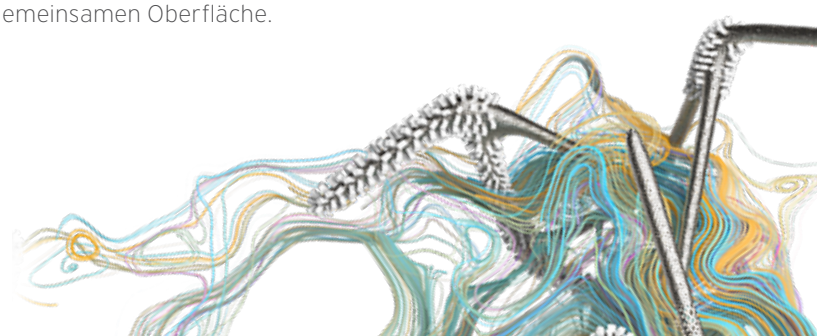
DATENSCHUTZ



INVESTIGATION UND ZENTRALISIERTE SICHTBARKEIT

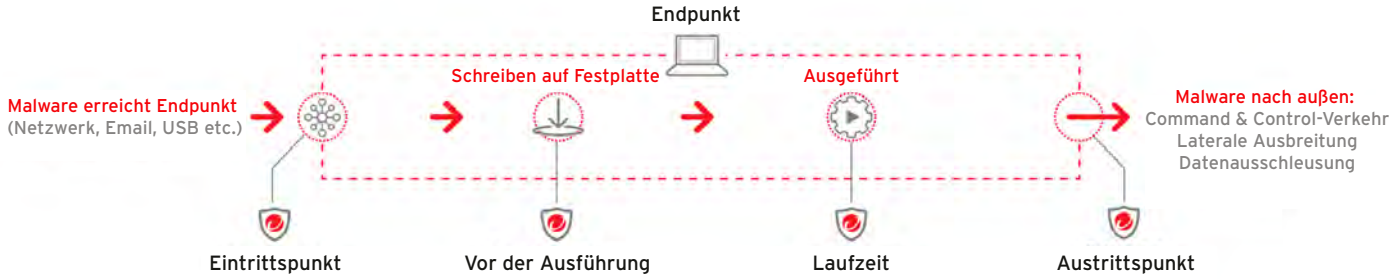
MANAGEMENT

ARCHITEKTUR



AUTOMATISIERTE ERKENNUNG UND REAKTION

Aufgrund der Komplexität moderner Sicherheitsumgebungen ist es wichtig für Unternehmen, alle Sicherheitslücken bei Anwenderaktivitäten und auf Endpunkten durch eine Kombination fortschrittlicher Techniken zu schließen. Eine einzelne Technik zur Bedrohungserkennung (z.B. Machine Learning oder KI) reicht nicht mehr aus, um alle Arten von Bedrohungen aufzuspüren. Benötigt wird stattdessen eine Mischung aus verschiedenen Techniken, darunter unter anderem Machine Learning vor der Ausführung und zur Laufzeit, Verhaltensanalyse, Applikationskontrolle und Schwachstellenschutz. Eine Endpunktsicherheitslösung muss außerdem fähig sein, immer weiter hinzuzulernen, sich anzupassen und Bedrohungsinformationen automatisch mit der gesamten Umgebung zu teilen.



Es ist wichtig den Endpunkt mit einem Rund-um-Schutz abzusichern: vom Eintrittspunkt für Malware bis zum Austrittspunkt

Machine Learning vor der Ausführung

Erkennt unbekannte Bedrohungen in ausführbaren Dateien.

Warum ist das wichtig?

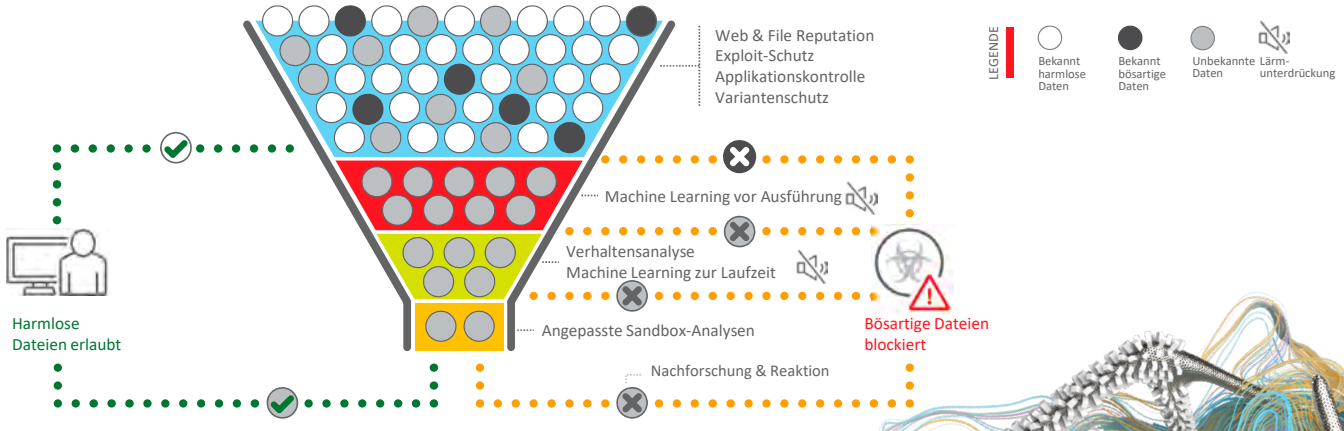
- Schutz vor neuen, gezielten Angriffen, die keinen bekannten Mustern folgen, aber Malware-Merkmale aufweisen.
- Machine Learning untersucht die Eigenschaften einer ausführbaren Datei, um festzustellen, ob Malware-Merkmale vorhanden sind.
- Entscheidungen basieren auf den entdeckten Merkmalen und nicht auf einem Muster, das die Engine vorher kennen muss.

Der Trend Micro Ansatz

- Das prognostische Machine Learning von Trend Micro Apex One™ bewertet Dateien im Vergleich zu einem cloudbasierten oder lokalen/offline Modell, um bislang noch unbekannte Bedrohungen aufzudecken.
- Unser generationsübergreifender Ansatz integriert weitere Erkennungsmethoden. Die Anzahl falscher Positivmeldungen, die das Machine Learning produziert, werden dadurch drastisch reduziert.
- Bereits bekannte Bedrohungen werden über signaturbasierte Techniken herausgefiltert. Es verbleibt lediglich eine kleine Zahl unbekannter Bedrohungen, die mittels ressourcenintensiveren Techniken wie Machine Learning untersucht werden. Diese Techniken können zudem eine gewisse Tendenz zu falschen Positivmeldungen aufweisen.
- Techniken zu Lärmunterdrückung reduzieren falsche Positivmeldungen. Dazu gehören unter anderem Census Checks (Untersuchung der Verbreitung und Reife von Dateien) und unsere globale Whitelist mit mehr als einer Milliarde als harmlos bekannter Dateien.

Worauf Käufer achten müssen

- Eine Lösung für Endpunktsicherheit darf sich nicht allein auf Machine Learning verlassen. Nur so kann der Einsatz ressourcenintensiver Erkennungsmethoden begrenzt werden, die außerdem eine erhöhte Zahl falscher Positivmeldungen produzieren.
- Mehrschichtiger Ansatz für Bedrohungserkennung
- Lärmunterdrückung (Census Checks)



Machine Learning zur Laufzeit

Verwendet Regel-Sets zur Analyse und Entdeckung von unbekannter Malware und dateiloser Bedrohungen, die erst während der Ausführung identifiziert werden können.

Warum ist das wichtig?

- Malware kann oftmals nicht über eine traditionelle Signatur identifiziert werden. Fortschrittliche Regeln untersuchen daher mögliche Malware-Merkmale.
- In Kombination mit anderen Erkennungstechniken wird so insgesamt eine fortschrittliche Erkennungsfunktionalität erzielt.
- Komplexe Malware kann bestimmte Arten von Machine Learning umgehen, da sie oftmals in Skripten versteckt oder an bestehende, harmlose Dateien angehängt wird. Diese werden vom Machine Learning vor der Ausführung unter Umständen nicht erfasst.
- Die Erkennung dateiloser Malware erfordert eine separate Machine-Learning-Laufzeit-Engine, um bösartige Prozesse zu identifizieren, die erst zur Laufzeit sichtbar werden.

Der Trend Micro Ansatz

- Verwendet fortschrittliche Funktionen für Machine Learning zur Laufzeit, um Dateien und ausgeführte Programme detailliert zu überwachen (z.B. Skripte oder Dokumente). Dazu wird das Verhalten mit einem Modell verglichen.
- Dieses Machine-Learning-Modell ist vollständig separat vom Machine-Learning-Modell für die Analyse vor der Ausführung. Unternehmen erhalten somit zwei getrennte und sehr effektive Methoden zur Bedrohungsüberwachung und können falsche Positivmeldungen reduzieren.
- Neue Regeln und Updates für das Machine-Learning-Modell werden im Vergleich zum Branchenstandard häufiger bereitgestellt, um die neueste Malware zu identifizieren.
- Die Machine Learning Engine wird kontinuierlich mit Bedrohungsinformationen aus verschiedenen Datenquellen (Sensoren) versorgt.
- Die umfangreiche Trend Micro Datenbank für Bedrohungsinformationen ermöglicht in Verbindung mit unserer Bedrohungsforschung einen herausragenden Überblick zu aktuellen, neuen Bedrohungen. Die gewonnenen Erkenntnisse werden von unseren Detection Engines verwendet (inklusive Machine-Learning-Modellen), um die Genauigkeit zu verbessern.

Worauf Käufer achten müssen

- Machine Learning zur Laufzeit identifiziert dateilose Malware während der Ausführung.
- Häufige Updates der Machine-Learning-Modelle unter Verwendung aktueller Bedrohungsinformationen.

Verhaltensanalysen zur Laufzeit

Erkennt unsichtbare Bedrohungen bei der Ausführung.

Warum ist das wichtig?

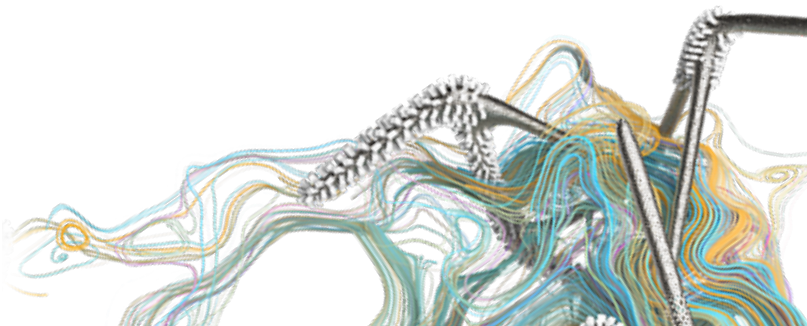
- Viele Bedrohungen werden schon vor der Ausführung erkannt, aber einige bleiben bis zur Ausführung unsichtbar. Dazu gehören zum Beispiel Malware, die in PowerShell-Skripten versteckt ist, und andere dateilose Angriffe.

Der Trend Micro Ansatz

- Verwendet Verhaltensanalysen zur Überwachung harmloser und verdächtiger Aktivitäten, wie zum Beispiel die schnelle Verschlüsselung vieler Dateien oder das Herausschleusen sensibler Informationen.
- Unsere Engine für Verhaltensanalysen bietet klare Indikatoren für laufende Angriffe (inklusive Ransomware und dateilose Malware). Basis hierfür sind spezifische Verhaltensweisen und verdächtige Indicators of Attack (IOA).
- Das permanente Hinzufügen neuer IOAs zur Engine verstärkt die Regel-Sets und ermöglicht die Erkennung neuer verdächtiger Verhaltensweisen.

Worauf Käufer achten müssen

- Kontinuierliche Aktualisierung der Engine für Verhaltensanalysen mit neuesten globalen Bedrohungsinformationen.
- Verhaltensmodelle, die permanent hinzulernen und sich anpassen.
- Fähigkeit zur Erkennung von Bedrohungen wie Ransomware und dateiloser Malware.



Laufzeit-Erkennung im Arbeitsspeicher

- Bietet Erkennungstechniken für spezialisierte speicherresidente Bedrohungen.

Warum ist das wichtig?

- Manche Endpunktbedrohungen werden niemals in Dateiform, sondern nur im Arbeitsspeicher ausgeführt. Diese Art von Bedrohungen kann von bestimmten traditionellen Sicherheitstechniken nicht erkannt werden.

Der Trend Micro Ansatz

- Apex One verwendet Laufzeit-Erkennung im Arbeitsspeicher, um bösartiges Skript-Verhalten und Code Injections zu identifizieren und zu stoppen.
- Blockiert Bedrohungen sogar nach dem Skript-Start und kann schädliche Aktionen rückgängig machen.

Worauf Käufer achten müssen

- Identifikation von bösartigem Skript-Verhalten im Arbeitsspeicher.

Applikationskontrolle (Whitelisting und Blacklisting)

Stellt fest, ob eine Applikation auf dem Endpunkt ausgeführt werden darf oder nicht.

Warum ist das wichtig?

- Um festzustellen, ob eine Applikationen ausgeführt werden darf, müssen Endpunktlösungen in der Lage sein, das voraussichtliche Verhalten der Applikation zu verstehen.
- Manche Organisationen definieren eine Liste erlaubter Applikationen (Whitelisting). Die Ausführung aller anderen Applikationen wird blockiert. Andere Organisationen wiederum bevorzugen die Definition von Listen unerwünschter Applikationen, die fortlaufend ergänzt werden (Blacklisting).

Der Trend Micro Ansatz

- Trend Micro Applikationskontrollen ermöglichen granulares und flexibles White- und Blacklisting. Organisationen können entweder nur ausdrücklich genehmigte Applikationen für eine Whitelist auswählen, oder die Ausführung aller Applikationen mit Ausnahme der Blacklist erlauben.
- Erstellt ein Inventar aller Applikationen auf dem Endpunkt. Diese Informationen können für Sperrregeln genutzt werden, die genau an die Organisation angepasst sind.
- Dynamische Regeln erlauben in Verbindung mit dem Trend Micro App Rating Service die automatische Freigabe harmloser Apps durch den Administrator.
- Reduzierter Administrationsaufwand durch flexible und granulare Freigabe bzw. Blockade von Applikationen mit Apex One.

Worauf Käufer achten müssen

- Blacklisting- und Whitelisting-Funktionalität gleichermaßen erforderlich.
- Flexible und granulare Kontrolle über Listen erlaubter/unerwünschter Applikationen.
- Offline-Modus mit der Möglichkeit für Programm-Updates bei Bedarf.

Virtual Patching (Intrusion Prevention)

Schützt Maschinen sogar ohne aktuelle Patches.

Warum ist das wichtig?

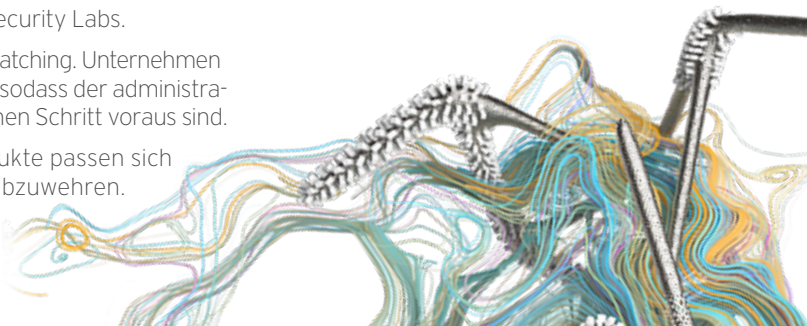
- Für viele Unternehmen ist es eine Herausforderung, die permanente Aktualität des Patch-Status ihrer Endpunkte zu gewährleisten.
- Schutz vor neuen Bedrohungen durch Bereitstellung aktueller Sicherheitspatches.
- Effektive Abwehr von Malware, die sich gezielt gegen Schwachstellen richtet.

Der Trend Micro Ansatz

- Bietet Organisationen das im Branchenvergleich aktuellste Virtual Patching.
- Trend Micro™ Vulnerability Protection™ ermöglicht sofortigen Schutz für bekannte und unbekannte Schwachstellen – schon bevor ein Patch verfügbar ist oder verteilt werden kann.
- Trend Micro Lösungen für Endpunkte, Netzwerke und die Cloud erhalten frühzeitigen Zugriff auf neue Schwachstelleninformationen. Basis hierfür ist unsere Zusammenarbeit mit der Zero Day Initiative (ZDI) und unsere Akquisition der Telus Security Labs.
- Schwachstellenschutz umfasst einen flexiblen Ansatz für das Virtual Patching. Unternehmen haben die volle Kontrolle über die eingesetzten Schwachstellenfilter, sodass der administrative Aufwand reduziert wird und Sicherheitsteams neuen Exploits einen Schritt voraus sind.
- Reagiert auf ansteigende und abnehmende Bedrohungen. Produkte passen sich dynamisch an, um Bedrohungen ohne Anwenderinteraktionen abzuwehren.

Worauf Käufer achten müssen

- Vulnerability Patching bietet im Gegensatz zu einfachem Vulnerability Assessment einen proaktiven Schutz.
- Datenfilterung über Schwachstellen hinweg.



URL- und Web-Reputation-Filter

Verhindert den Zugriff auf unsichere Webseiten, noch bevor es zu gefährlichen Aktivitäten kommen kann.

Warum ist das wichtig?

- Mitarbeiter können nicht beurteilen, ob eine Webseite unsicher ist, bevor sie geöffnet wurde. Eine gute Sicherheitslösung für Endpunkte sollte daher den Zugriff auf bestimmte Webseiten verhindern, bevor es zu gefährlichen Aktivitäten kommt.
- Die meiste Malware versucht innerhalb oder außerhalb des Browsers, Verbindungen zu bestimmten Web-Adressen herzustellen, die als bösartig bekannt sind.

Der Trend Micro Ansatz

- Apex One verwendet dynamisch aktualisierte Informationen zur Reputation von Webseiten, um bösartige URLs zu erkennen und zu blockieren. Basis hierfür ist die Integration mit dem Trend Micro™ Smart Protection Network™.
- Trend Micro Web-Reputation-Technologie ist nicht von einem Web-Browser-Plugin abhängig. HTTP-Kommunikation kann auf dem Kernel-Level geschützt werden. Dies ermöglicht sichere Applikationskommunikation, verbesserten Schutz und Eindämmung der von Malware verursachten Schäden.

Worauf Käufer achten müssen

- Kontinuierliche Aktualisierung der Informationen zur Webseiten-Reputation, unterstützt durch umfangreiche Threat Intelligence.
- Automatische Filterung bösartiger Sites.
- Kernel-Level-Erkennung und Blockade über alle Browser und Applikationen hinweg.

Sandbox-Überprüfung (On-Premises und in der Cloud)

Bietet eine sichere Umgebung für die Ausführung und Auslösung verdächtiger Dateien, um bösartige Aktivitäten zu identifizieren.

Warum ist das wichtig?

- Bedrohungen sind nicht immer eindeutig zu erkennen. Manchmal stößt die Endpunktlösung auf eine unbestimmte Datei, die näher untersucht werden muss. Dies erfordert eine sichere Umgebung, die von anderen Endpunkten getrennt ist.

Der Trend Micro Ansatz

- Bietet Cloud Sandboxing und angepasstes On-Premises Sandboxing. Die Simulation eines echten Endpunktes täuscht Malware, sodass bösartige Aktivitäten erkannt und blockiert werden können. Dies liefert Beweise für eine Bedrohung.
- Die Ergebnisse des Sandboxing können über APIs an andere Produkte verteilt werden, wodurch der Gesamtsicherheitsstatus verbessert wird.

Worauf Käufer achten müssen

- Anpassbare Sandbox simuliert echte Endpunkte.
- Dateien können sowohl in On-Premises- als auch in Cloud-Bereitstellungen zur Überprüfung an die Sandbox gesendet werden.
- Geteilte Nutzung von Bedrohungsinformationen durch verschiedene Sicherheitslösungen.

Packer-Erkennung

Erkennt Bedrohungen, wenn sie entpackt und ausgeführt werden.

Warum ist das wichtig?

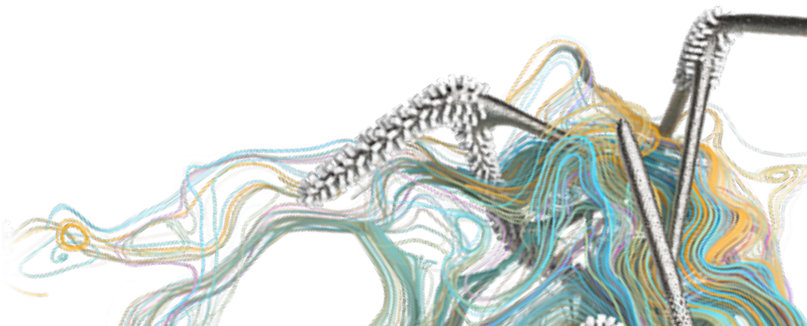
- Bestimmte Bedrohungen lassen sich erst identifizieren, sobald sie entpackt wurden und Aktionen ausführen.
- Vor der Ausführung können diese Bedrohungen von vielen Techniken nicht erkannt werden. Andere Laufzeit-Funktionen sind nicht mehr wirksam, wenn die Bedrohung bereits ausgeführt wird.

Der Trend Micro Ansatz

- Apex One identifiziert und blockiert Malware beim Entpacken – also vor der Ausführung.
- Zusätzlich werden weitere Techniken wie Verhaltensanalysen eingesetzt, um Angriffe zu blockieren.
- Viele Endpunktlösungen können diese Bedrohungen nur erkennen, aber nicht stoppen.

Worauf Käufer achten müssen

- Automatische Identifikation und Blockade von Bedrohungen während des Entpackens.



Laterale Ausbreitung (Ost-West-Datenverkehr)

Die Sichtbarkeit lateraler Dateibewegungen ist entscheidend für die Identifikation und Verfolgung von Datensicherheitsverstößen.

Warum ist das wichtig?

- Die frühzeitige Erkennung von Datensicherheitsverstößen reduziert den erforderlichen Bereinigungsaufwand und verhindert die Ausbreitung von Bedrohungen im Netzwerk.

Der Trend Micro Ansatz

- Apex One Endpoint Sensor bietet eine detaillierte Übersicht zu lateralen Bewegungen über Endpunkte hinweg. Trend Micro™ Deep Security™ erkennt zudem laterale Bewegungen im Netzwerk.
- Apex One mit Endpoint Detection and Response (EDR) und / oder Trend Micro Deep Discovery Inspector™ stellen ein vollständiges Bild aller Angriffsbewegungen im Netzwerk bereit.
- Der Trend Micro Managed Detection and Response (MDR) Service übernimmt auf Wunsch die Identifikation lateraler Bewegungen und nachfolgender Infektionen. Für die Eliminierung von Bedrohungen werden spezifische Anleitungen bereitgestellt.

Worauf Käufer achten müssen

- Detaillierte Übersicht zur Bedrohungsausbreitung zwischen Endpunkten sowie über Netzwerke und Server.

Varianten-Schutz

Erkennt Malware-Bedrohungen, bei denen es sich um Modifikationen bekannter Bedrohungen handelt.

Warum ist das wichtig?

- Viele neue Bedrohungen sind modifizierte Varianten bekannter Malware. Die Veränderungen sollen die Erkennung verhindern.

Der Trend Micro Ansatz

- Nutzt automatisierte Erkennungstechniken zum Varianten-Schutz, die kleine Mutationen bekannt bösartiger Dateien aufspüren.
- Identifiziert ganze Malware-Familien, auch wenn zentrale Bereiche der Malware-Datei verändert wurden, um der Erkennung zu entgehen.

Worauf Käufer achten müssen

- Automatische Entfernung bekannt bösartiger Dateien, inklusive Malware-Varianten.
- Erkennung von Malware-Familien und modifizierten Bedrohungen.

Anti-Malware / Malware-Scanning

Bildet einen ersten Schutzwall gegen bekannte Bedrohungen bei geringem Aufwand.

Warum ist das wichtig?

- Diese traditionelle Technik kann zwar nicht alle Bedrohungen aufspüren, bildet aber trotzdem ein wichtiges Element bei der effizienten und automatisierten Entfernung bekannter Malware von Endpunkten - bevor Schäden entstehen.

Der Trend Micro Ansatz

- Apex One verwendet eine Kombination von Malware-Erkennungstechniken, darunter statische Analysen, Signaturen sowie Datei- und Web-Datenbanken.
- Zusätzlich zu diesen Erkennungstechniken werden nicht-signaturbasierte Verfahren eingesetzt, um mehr komplexe und noch unbekannte Malware zu identifizieren.
- Durch den Einsatz von Anti-Malware im ersten Schritt werden ressourcenintensivere Techniken entlastet, die sich somit auf die Entdeckung unbekannter Bedrohungen fokussieren können.

Worauf Käufer achten müssen

- Der schnelle Einsatz von Malware-Scanning entfernt den Großteil bösartiger Dateien.

Endpunkt-Isolation und Quarantäne

Infizierte Endpunkte werden von anderen Systemen isoliert und in Quarantäne gestellt.

Warum ist das wichtig?

- Verhindert die Ausbreitung von Malware und Bedrohungen in der Organisation.

Der Trend Micro Ansatz

- Apex One kann Maschinen isolieren, ohne auf Netzwerk-Router oder andere Drittanbieter-Infrastrukturen zurückgreifen zu müssen.

Worauf Käufer achten müssen

- Eine Endpunktlösung muss fähig sein, ohne administrative Eingriffe eine Quarantäne durchzusetzen und bösartige Dateien vom Endpunkt zu löschen.

Beendigung von Prozessen

Beendet bösartige Prozesse automatisch.

Warum ist das wichtig?

- Gewährleistet die sofortige und automatische Entfernung von Bedrohungen, bevor sich diese auf andere Endpunkte ausbreiten können.

Der Trend Micro Ansatz

- Apex One beendet automatisch bösartige Prozesse. Infizierte Endpunkte werden isoliert und in Quarantäne gestellt.
- Prozesse können für einzelne oder mehrere Anwender beendet werden.

Worauf Käufer achten müssen

- Automatische Beendigung von Prozessen ohne Administratoreingriffe.
- Gleichzeitige Beendigung von Prozessen auf mehreren Endpunkten / für mehrere Anwender.

Rollback

Setzt Endpunkte auf den Stand vor der Infektion zurück.

Warum ist das wichtig?

- Ransomware kann immense finanzielle Folgen verursachen, zum Beispiel durch Umsatzeinbußen, Lösegeldforderungen und irreparable Schäden an Endpunkten und anderen Systemen.

Der Trend Micro Ansatz

- Apex One ermöglicht einen Rollback aller bereits entstandenen Schäden (im Fall von Ransomware). Maschinen werden in einen sauberen Stand zurückversetzt. Administratoren müssen nicht mehr jeden einzelnen infizierten Endpunkt neu aufsetzen, wodurch Zeit und Kosten gespart werden.

Worauf Käufer achten müssen

- Infizierte Dateien werden bereinigt und Maschinen auf den Stand vor der Infektion zurückgesetzt.
- Automatisierte Wiederherstellung ohne administrative Aufgaben.

Techniken für automatisierte Reaktionen

Sorgen für sofortige Entfernung von Bedrohungen, isolieren den Endpunkt und verhindern die weitere Ausbreitung.

Warum ist das wichtig?

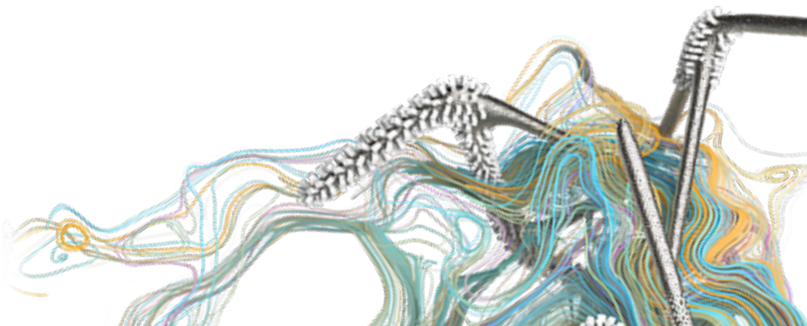
- Sicherheitsteams haben wichtigere Aufgaben, als sich um jede einzelne Endpunktbedrohung zu kümmern und manuelle Bereinigungen durchzuführen.

Der Trend Micro Ansatz

- Apex One ermöglicht Organisationen die automatisierte Reaktion auf Bedrohungen. Manuelle Eingriffe und spezialisierte Teams im Security Operations Center (SOC) sind hierfür nicht erforderlich.
- Apex One kann die von Malware verursachten Schäden eindämmen, Endpunkte bereinigen und auf den Stand vor der Infektion zurücksetzen. Damit lassen sich Datenverluste verhindern und Lösegeldzahlungen vermeiden.

Worauf Käufer achten müssen

- Automatische Quarantäne und Isolation von Endpunkten sowie Abbruch bösartiger Prozesse.
- Bereinigung infizierter Endpunkte und Wiederherstellung des Standes vor der Infektion.



DATENSCHUTZ

Der Schutz sensibler Daten ist eine der zentralen Anforderungen an Sicherheitslösungen für den Endpunkt – ganz unabhängig davon, ob es sich um Geschäftsgeheimnisse, vertrauliche Kundeninformationen oder auch Gesundheitsdaten handelt. Nachfolgend sind einige Schlüsselfunktionen aufgeführt, die Bestandteil einer umfassenden und effektiven Datenschutzstrategie sein müssen.

Data Loss Prevention (DLP)

Schützt sensible Daten wie Finanz- und Kundeninformationen oder geistiges Eigentum.

Warum ist das wichtig?

- Größere Mitarbeitermobilität, häufigere Verwendung privater Geräte und Applikationen für berufliche Zwecke und steigende Verbreitung von Advanced Persistent Threats (APTs) sind mitverantwortlich für eine wachsende Zahl von Datenschutzverstößen.
- Datenschutz auf dem Endpunkt hilft dabei, den Abfluss sensibler Daten vom Endpunkt zu verhindern.

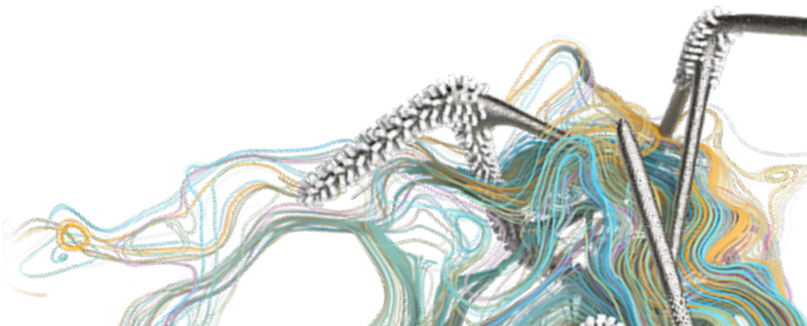
Der Trend Micro Ansatz

- Apex One verwendet einfach zu definierende bzw. zu modifizierende Regeln, um zu verhindern, dass bestimmte Arten von Daten das Unternehmen verlassen. Dazu gehören zum Beispiel Kreditkartendaten, Kundeninformationen und medizinische Aufzeichnungen.
- Apex One DLP kann verschiedene Aktionen durchführen: Reporting, Benachrichtigung, Logging, Bestätigungsabfrage und Blockade.
- DLP Templates unterstützen bei der Compliance mit DSGVO, PCI, HIPAA und anderen Regularien.
- Apex One DLP integriert die am häufigsten verwendeten DLP-Funktionen, um sensible Daten zu schützen – ohne Kosten und Mehraufwand für eine separate Lösung.

	Ansatz	Kanäle				
Data in Motion (DIM)	Netzwerk	Email	Web	IM	Filesharing	Cloud Apps
Data in Use (DIU)	Endpunkt	USB-Sticks	CDs & DVDs	Mobilgeräte	Externe Festplatten	Ausdrucke
Data at Rest (DAR)	Durchsuchung	Mobil-geräte	Datenbanken	Mail-Archive	Datei-freigaben	Content-Management

Worauf Käufer achten müssen

- Templates für häufige DLP-Regeln.
- Flexible und einfach zu definierende DLP-Regeln, die über Anwender, Gruppen und die ganze Organisation hinweg implementiert werden können.
- Erkennung sensibler Daten wie Kreditkarten-, Gesundheits- und Finanzinformationen.
- Mögliche Aktionen umfassen Reporting, Benachrichtigung, Logging und Blockade.
- Das Kopieren von Daten auf externe Speicher oder der Versand per Email kann verhindert werden.



Gerätekontrolle

Verhindert die Übertragung sensibler Daten zu Geräten wie USB-Sticks und externen Festplatten.

Warum ist das wichtig?

- Kontrolle und Überwachung der externen Geräte, die mit dem Endpunkt verwendet werden können, trägt entscheidend zum Schutz sensibler Daten bei.

Der Trend Micro Ansatz

- Die Gerätekontrolle von Apex One ermöglicht die Implementierung von Regeln, mit denen sich steuern lässt, welche Geräte mit dem Endpunkt verbunden werden dürfen.
- Trend Micro™ Data Loss Prevention™ (DLP) unterstützt die Spezifizierung bestimmter Hersteller oder Seriennummern von USB-Sticks, sodass Organisationen die granulare Kontrolle über Geräte erhalten.

Worauf Käufer achten müssen

- Granulare Kontrolle der mit dem Endpunkt verwendbaren Geräte.
- Kontrolle externer Geräte wie USB-Sticks und Festplatten.
- Regeln zur Kontrolle der erlaubten Datenspeicherungsoptionen.

Verschlüsselung

Schützt Daten, die auf einem verlorenen oder gestohlenen Gerät gespeichert sind.

Warum ist das wichtig?

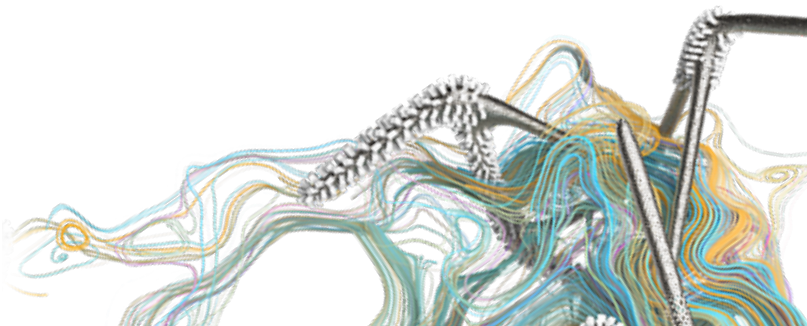
- Viele regulatorische und branchenspezifische Sicherheitsrahmenwerke schreiben Verschlüsselung für Organisationen vor, die sich im Falle eines Datenschutzverstoßes vor Strafzahlungen oder Meldepflichten schützen wollen.

Der Trend Micro Ansatz

- Apex One ermöglicht die Verschlüsselung ganzer Festplatten sowie von einzelnen Dateien, Ordnern und Wechselmedien.
- Apex One kann auch als Schlüsselmanager verwendet werden, wenn Organisationen Verschlüsselung über Microsoft® Windows® Bitlocker oder Mac File Vault einsetzen.
- Die Festplattenverschlüsselung von Apex One ist in die DLP-Regeln integriert und arbeitet mit diesen zusammen.

Worauf Käufer achten müssen

- Full-Disk-Verschlüsselung
- Verschlüsselung ausgewählter Dateien und Ordner.
- Schlüsselmanagement
- Integration mit anderen Schutzfunktionen ermöglicht die Definition individueller und effektiver Regeln.



INVESTIGATION UND ZENTRALISIERTE SICHTBARKEIT

Eine ideale Sicherheitslösung für den Endpunkt bietet Sichtbarkeit und Kontrolle aller geschützten Endpunkte. Dies ermöglicht Unternehmen ein vertieftes Verständnis der Komplexität der Sicherheitsumgebung.

Sichtbarkeit der Bedrohungsquellen und Bewegungen im Netzwerk ist der Schlüssel für mehr Endpunktsicherheit. Investigative Funktionalität wird immer wichtiger, daher erweitern viele Unternehmen ihre Sicherheitsplattformen durch Endpoint Detection and Response (EDR) Lösungen und Managed Detection and Response (MDR) Services.

Aufzeichnung von Endpunkt-Events (Telemetrie)

Zeichnet alle Aktionen und das Systemverhalten auf dem Endpunkt auf, um die rückblickende Untersuchung verdächtiger Aktivitäten zu ermöglichen.

Warum ist das wichtig?

- Die Aufzeichnung der Aktivitäten auf dem Endpunkt ist ein wichtiger Bestandteil aller EDR-Lösungen. Unternehmen können damit in der Zeit zurückblicken und Endpunkte vor oder nach einer Infektion untersuchen.
- Die Sichtweite hängt direkt von der Länge der aufgezeichneten Zeitspanne ab.

Der Trend Micro Ansatz

- Trend Micro Endpoint Sensor (EDR) zeichnet unterschiedlichste Daten auf, darunter Netzwerk-Events, Prozesse, System- und Anwender-Verhalten, Alarme und Kommandos. Endpoint Sensor ist als On-Premises-Lösung und als Service verfügbar.
- Informationen werden auf dem Endpunkt gespeichert. An den Trend Micro Apex One Central™ Server werden Metadaten gesendet, um Indicators of Compromise (IOC) zu identifizieren.
- Endpunkte mit einem IOC werden sodann isoliert und einer Root-Cause-Analyse (RCA) unterzogen, um Quelle und Ausbreitung eines Angriffs festzustellen. Danach stehen verschiedene Optionen für die Reaktion bereit.
- Trend Micro Endpoint Sensor als Service bietet eine kostenfreie 30-tägige Speicheroption als Standard bei Erwerb zusätzlicher 6 oder 12 Monate Datenaufbewahrung (länger als jeder andere EDR-Anbieter). Bei der On-Premises-Version von Endpoint Sensor ist die Datenaufbewahrung nur durch den verfügbaren Speicherplatz begrenzt.

Worauf Käufer achten müssen

- Optionen für On-Premises- und Security-as-a-Service (SaaS)-Bereitstellungen.
- Flexible Datenspeicheroptionen für SaaS.
- Effiziente Aufzeichnung von Anwendertelemetrie, Netzwerk-Events, Prozessen, System-Events und mehr.
- Integrierte Workflows mit einer einzigen Konsole für EDR und die Endpoint Protection Plattform (EPP).
- Flexible Suche über mehrere Parameter hinweg.
- Zusätzliche Bedrohungsinformationen und globale Threat Intelligence vom Hersteller.
- Optionen für sofortige Reaktionen.
- Fortschrittliches Threat Hunting mittels IOAs.

Metadaten-Sammlung (Server Side Sweep)

Bietet einen schnellen Schnappschuss der aufgezeichneten Telemetriedaten auf dem Endpunkt.

Warum ist das wichtig?

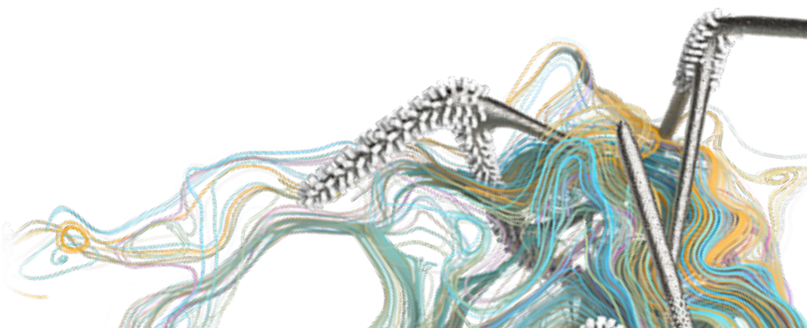
- Falls ein Endpunkt untersucht werden muss, können die Metadaten einfach nach speziellen Hashkeys oder bestimmten Verhaltensweisen durchsucht werden, um sofort Ergebnisse zu erhalten.

Der Trend Micro Ansatz

- Trend Micro Endpoint Sensor führt einen serverseitigen Metadaten-Sweep durch, um Indicators of Compromise (IOC) auf Online- oder Offline-Endpunkten zu finden.
- Deutlich weniger Daten müssen zentral gespeichert und verwaltet werden.

Worauf Käufer achten müssen

- Effiziente Sammlung von Endpunkt-Informationen.
- Serverseitige Metadaten-Sweeps



Root-Cause-Analyse (RCA)

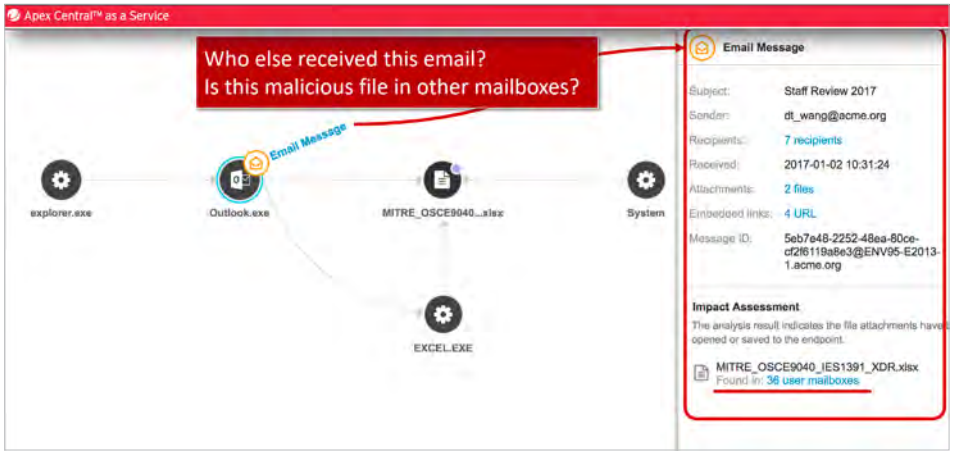
Zeigt alle Events auf einem infizierten Endpunkt bis zur Erkennung.

Warum ist das wichtig?

- Sicherheitsverantwortliche erhalten eine Übersicht zur Bedrohungsquelle, der Ausbreitung und erforderlichen Behebungsmaßnahmen.

Der Trend Micro Ansatz

- Apex One Endpoint Sensor bietet eine grafische und tabellarische Darstellung infizierter Endpunkte. So können der Eintrittspunkt und die Ausbreitung einer Bedrohung nachverfolgt werden.
- Root-Cause-Analysen zeigen laterale Bewegungen von Bedrohungen im Netzwerk sowie weitere möglicherweise infizierte Endpunkte.



Worauf Käufer achten müssen

- Grafische Darstellung von Malware-Infektionen auf Endpunkten.
- Sofortige Durchsetzung von Reaktionen auf dem Endpunkt.
- Detaillierte Untersuchung einer spezifischen Infektion.

Patient-Zero-Identifikation

Findet den Endpunkt oder Anwender, der als erster von einer Malware betroffen wurde.

Warum ist das wichtig?

- Der Patient Zero muss schnell und genau identifiziert werden, um eine weitere Ausbreitung von Bedrohungen zu verhindern.

Der Trend Micro Ansatz

- Durch die Suche nach IOCs einer Bedrohung können Endpunkte identifiziert werden, die bereits betroffen waren, bevor der jeweilige Vorfall als verdächtig oder bösartig erkannt wurde.

Worauf Käufer achten müssen

- Schnelle und akkurate Identifikation des Patient Zero.

IOC-Suchen und Sweeps in Echtzeit

Ermöglicht Echtzeit-Abfragen von Endpunkten zur Suche nach Indicators of Compromise (IOC).

Warum ist das wichtig?

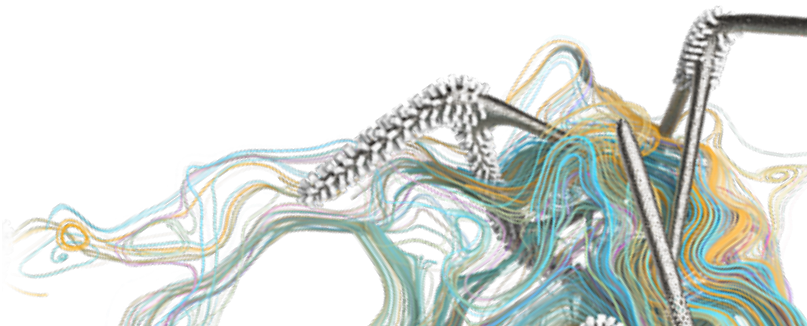
- Sicherheitsverantwortliche müssen feststellen können, ob ein IOC auf Endpunkten vorhanden ist, um so die Wahrscheinlichkeit eines Angriffs zu bestimmen.

Der Trend Micro Ansatz

- Endpoint Sensor kann Live-Untersuchungen durchführen und bietet die Möglichkeit, bei Endpunkt-Scans nach bestimmten IOCs oder verschiedenen anderen Kriterien zu suchen.

Worauf Käufer achten müssen

- Echtzeit-Scans nach IOCs.
- Suche über verschiedene Kriterien.



Unterstützung für Managed Detection and Response (MDR)

Bietet Kunden einen Managed Service für Threat Hunting und Reaktion.

Warum ist das wichtig?

- Viele Organisationen verfügen nicht über das erforderliche Know-how bzw. dedizierte Vollzeit-Teams für Threat Hunting und EDR Analysen.

Der Trend Micro Ansatz

- MDR Service einzeln oder in Kombination verfügbar für Endpunkte (Apex One), Server (Deep Security) und Netzwerke (Deep Discovery). Korrelation mehrerer Vektoren ermöglicht die verbesserte Erkennung komplexer Bedrohungen.
- Sammelt Telemetrie zu Anwendern, Netzwerken und Servern sowie Alarme. Informationen werden über fortschrittliche KI-Techniken miteinander korreliert, um Angriffe auf Kunden zu identifizieren.
- Bietet regelmäßige IOC Sweeps und IOA Hunting zur Identifikation von Angriffen. Durchführung vollständiger Root-Cause-Analysen und Zusammenarbeit mit dem Kunden, um wirksame Reaktionen auf Vorfälle bereitzustellen.
- Zugang zu Trend Micro Experten, die Root-Cause-Analysen erstellen und gemeinsam mit dem Unternehmen einen Reaktionsplan entwickeln.

Worauf Käufer achten müssen

- 24x7-Event-Monitoring und Alarmierung
- Fortschrittliche Korrelation von Daten aus verschiedenen Quellen, darunter Endpunkte, Netzwerke und Server.
- Detailliertes Reporting untersuchter Events, inklusive monatlicher Zusammenfassungen.
- Bereitstellung detaillierter Optionen zur Problembehebung, mit denen infizierte Endpunkte bereinigt und wiederhergestellt werden können.

Orientierungshilfe bei unbekannten Dateien

Bietet Anwendern eine geführte Übersicht zu Alarmen und priorisiert Bedrohungen, die eine sofortige Reaktion erfordern.

Warum ist das wichtig?

- Wenn Sicherheitsverantwortliche verdächtige unbekannte Objekte entdecken, müssen sie wissen, ob diese Objekte sicher signiert wurden, bereits an anderen Orten vorkommen oder riskante Eigenschaften aufweisen.

Der Trend Micro Ansatz

- Endpoint Sensor unterscheidet Bedrohungen, die eine sofortige Reaktion erfordern, von weniger gefährlichen Bedrohungen, bei denen eine spätere Behandlung ausreicht.
- Trend Micro integriert seine umfangreiche Bedrohungsforschung als weitere Informationsebene und bietet Zugang zu Threat Connect. Dieser Service korreliert entdeckte Objekte mit Daten aus dem Smart Protection Network.
- Endpoint Sensor stellt Informationen zu unbekannten Events bereit, damit Unternehmen eine Bedrohung besser verstehen können.

Worauf Käufer achten müssen

- Nach Prioritäten geordnete Liste der Bedrohungen.
- Orientierung für alle Dateitypen und Informationen über verdächtige und harmlose Objekte.

Alarme, Timelines und Sichtbarkeit der Bedrohungsinformationen

Bietet Unternehmen zentralisierte Sichtbarkeit für ihre gesamte Umgebung.

Warum ist das wichtig?

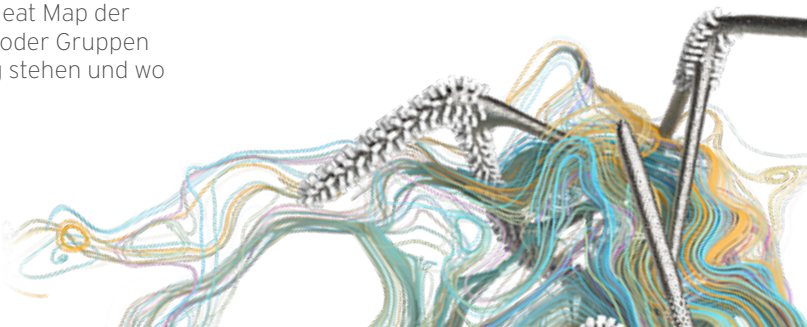
- Endpunkt-Sicherheitslösungen erfordern eine zentralisierte und detaillierte Übersicht zum Sicherheitsstatus einer Organisation. Dies beinhaltet Informationen zu Bedrohungen und Alarmen sowie zur Gesamtsicherheit.

Der Trend Micro Ansatz

- Apex One bietet Anwendern über Trend Micro Apex Central™ zentralisierte Sichtbarkeit über die gesamte Umgebung hinweg. Dazu gehören Endpunkt- und EDR-Alarme, Timelines, Bedrohungsinformationen und mehr. Die Sichtbarkeit erstreckt sich auf alle Trend Micro Produkte, inklusive Netzwerk-, Gateway- und Email-Sicherheit.
- Apex Central stellt außerdem eine detaillierte Active Directory Heat Map der Organisation bereit. So lässt sich erkennen, welche Abteilungen oder Gruppen im Unternehmen mit Bedrohungen oder Alarmen in Verbindung stehen und wo Sicherheitsrichtlinien nicht eingehalten werden.

Worauf Käufer achten müssen

- Zentralisierte Sichtbarkeit über alle Endpunkte und EDR-Sensoren hinweg.
- Detailliertes Mapping von Bedrohungen und Endpunkten zu Organisationseinheiten.



MANAGEMENT

Das Management komplexer Endpunktlösungen sollte eine entscheidende Rolle bei der Kaufentscheidung spielen. Der praktische Nutzen einer State-of-the-Art-Sicherheitsplattform ist eingeschränkt, wenn IT- und Sicherheitsteams tägliche Managementaufgaben nicht effizient durchführen können.

Eine Plattform, die fortschrittliche Erkennung und Reaktion, umfassende Sichtbarkeit, Kontrolle und Analysen integriert, kann den Verwaltungsaufwand für IT- und Sicherheitsteams deutlich senken und Betriebskosten reduzieren.

Rollenbasierter Zugriff auf Administrationsfunktionen

Bietet eine Reporting-Konsole, mit der sich Berichte und Alarme für verschiedene Funktionsgruppen anpassen lassen.

Warum ist das wichtig?

- Verschiedene Stakeholder im Unternehmen müssen die jeweils für sie relevanten Informationen und Daten erhalten.

Der Trend Micro Ansatz

- Anpassbare Dashboards bilden die unterschiedlichen Verantwortlichkeiten der Administration ab. Verschiedene Gruppen erhalten die für ihre Aufgaben wichtigen Informationen.
- Apex One bietet vollständige Active Directory Integration mit rollenbasierter Zugriffskontrolle. Administratoren können Sicherheitseinstellungen und Compliance über Anwendergruppen hinweg einsehen.
- Trend Micro bietet mehrere vorkonfigurierte Rollen mit verschiedenen Zugriffsebenen und Ansichten. Unternehmen können aber auch eigene Rollen erstellen.

Worauf Kunden achten müssen

- Active-Directory-Integration
- Dashboards können individualisiert werden.
- Granulare und rollenbasierte Zugriffskontrolle
- Anpassbare Rollen

API-Funktionen

Verbindet Drittanbieter-Plattformen für Management und Automation mit Sicherheitslösungen für Endpunkte.

Warum ist das wichtig?

- Endpunktlösungen funktionieren fast nie in vollständiger Isolation.
- Lösungen müssen über eingebaute APIs verfügen, um eine Verbindung zu externen Systemen herzustellen. Dies ist die Basis für Automation im Unternehmensnetzwerk.

Der Trend Micro Ansatz

- Apex One beinhaltet erweiterte API-Sets, über die Drittanbieter-Programme kommunizieren und Aktionen automatisieren können.
- Über APIs können Bedrohungsinformationen von Drittanbietern geteilt werden.

Worauf Kunden achten müssen

- Offene RESTful APIs
- Umfangreiche Drittanbieter-API-Sets
- Geteilte Nutzung von Bedrohungsinformationen durch mehrere Programme.

SIEM-Integration

Sendet sicherheitsrelevante Events an verschiedene Kontrollen.

Warum ist das wichtig?

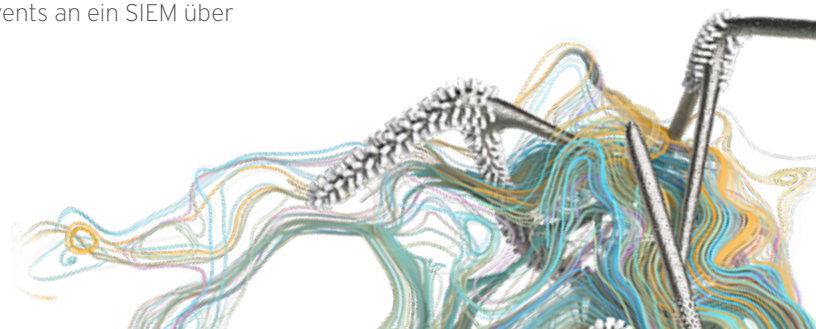
- Ein SIEM ist ein zentraler Ort, an dem Anwender eine Übersicht zu allen Events aus verschiedenen Sicherheitskontrollen innerhalb des Unternehmens erhalten.
- SIEMS integrieren mehrere Sicherheitslösungen, um einen umfassenden Überblick zur Organisation bereitzustellen.

Der Trend Micro Ansatz

- Apex One ermöglicht die Weiterleitung sicherheitsrelevanter Events an ein SIEM über Syslog oder andere Integrationen.

Worauf Kunden achten müssen

- SIEM-Integration über Syslog



Open-IOC-Integration

Ermöglicht die schnelle Identifikation und Merkmalserfassung von Angriffsindikatoren.

Warum ist das wichtig?

- Die Kommunikation von Produkten unterschiedlicher Hersteller über ein erweiterbares XML-Schema gewährleistet produktübergreifende Abdeckung und Schutz.

Der Trend Micro Ansatz

- Verwendet OpenIOC-Kommunikation für weitergehende Integration mit anderen Sicherheitsprodukten.
- Geteilte Bedrohungsinformationen verbessern den Sicherheitsstatus von Unternehmen deutlich.

Worauf Kunden achten müssen

- Integration mit Drittanbieter-Sicherheitssystemen.
- Geteilte Bedrohungsinformationen

Sprachunterstützung

Bietet mehrsprachige Unterstützung für Endanwender.

Warum ist das wichtig?

- Viele Unternehmen sind heute global aktiv, deshalb müssen Sicherheitslösungen mehrere Sprachen unterstützen.

Der Trend Micro Ansatz

- Trend Micro Produkte sind in mehr als einem Dutzend Sprachen verfügbar, um Kunden mit multinationalen Standorten bestmöglich zu unterstützen.

Worauf Käufer achten müssen

- Mehrsprachiger Support

Geteilte Nutzung und Verbreitung von Bedrohungsinformationen

Ermöglicht die Kommunikation zwischen Sicherheitsebenen und die gemeinsame Nutzung von Bedrohungsinformationen.

Warum ist das wichtig?

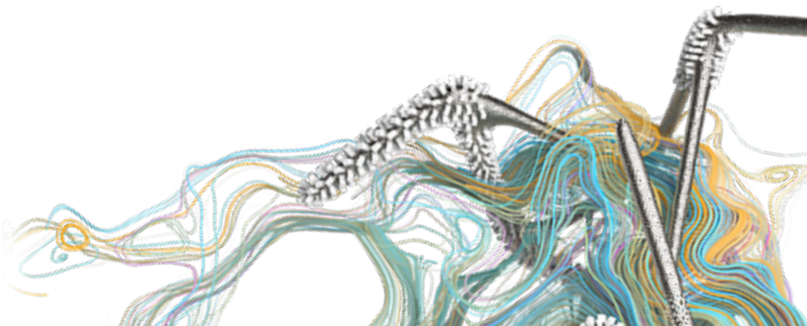
- Der Austausch und die gemeinsame Nutzung von Bedrohungsinformationen durch Endpunkte gewährleisten umfassenden Schutz für die gesamte Organisation.

Der Trend Micro Ansatz

- Informationen zu verdächtigen Netzwerkaktivitäten und Dateien können sofort zwischen Sicherheitsebenen ausgetauscht werden, um nachfolgende Angriffe in anderen Netzwerkbereichen zu stoppen.
- Unterstützung für STIX- und TAXII-Industriestandards gewährleistet verbesserte Bedrohungsabwehr.
- YARA-Integration ermöglicht die Suche nach komplexer Malware.
- Trend Micro™ Connected Threat Defense™ bietet verbesserte Sichtbarkeit, automatisierte Erkennung neuer Bedrohungen und schnelle Reaktionen auf mehreren Sicherheitsebenen.

Worauf Käufer achten müssen

- Automatische Verteilung von Bedrohungsinformationen und verdächtigen Daten über mehrere Sicherheitsebenen.
- Unterstützung für STIX, TAXII und YARA.



Unterstützung für PC- und Mac-Endpunkte

Schützt beide verbreiteten Endpunkt-Betriebssysteme.

Warum ist das wichtig?

- Viele Organisationen setzen heute eine Mischung aus Windows- und Mac-Endpunkten ein, die jeweils unterschiedliche Sicherheitsanforderungen haben.

Der Trend Micro Ansatz

- Apex One unterstützt Mac-Endpunkte mit einer Reihe effektiver Erkennungstechnologien, inklusive Gerätekontrolle, Machine Learning, Verschlüsselung und Bedrohungsuntersuchung.

Worauf Käufer achten müssen

- Unterstützung für Mac-Endpunkte und Betriebssysteme

Compliance

Gewährleistet die Einhaltung von Endpunkt-Sicherheitsrichtlinien durch Anwender.

Warum ist das wichtig?

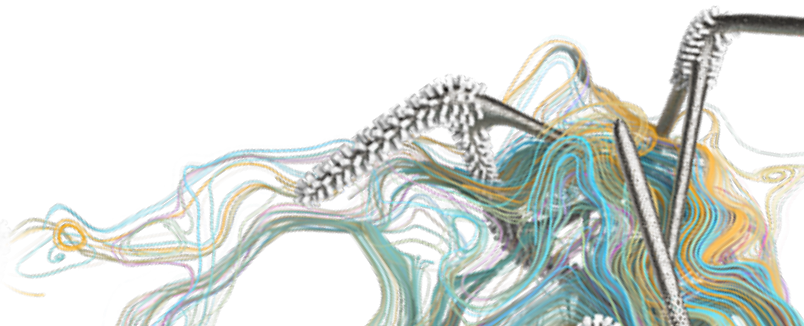
- Unternehmen müssen eine wachsende Zahl von Regularien und Vorschriften beachten, insbesondere hinsichtlich der Speicherung und Pflege sensibler Kunden-, Finanz- und Gesundheitsdaten.

Der Trend Micro Ansatz

- Apex One erleichtert die Compliance mit regulativen Rahmenwerken (DSGVO, PCI, HIPAA etc.) durch sofort einsatzbereite Richtlinien-Templates und Anleitungen für regionale Anforderungen.
- Einfach zu modifizierende Templates bilden individuelle Anforderungen ab.
- IT-Regeln bieten Administratoren einen Überblick zu Compliance-konformen und nicht mehr aktuellen Endpunkten.
- Anzeige der Compliance nach Abteilung. Mapping der Compliance zum Active Directory.

Worauf Käufer achten müssen

- Sofort einsatzbereite Richtlinien-Templates basierend auf branchenspezifischen Regularien.
- Flexible Richtlinien-Templates
- Compliance-Ansicht nach Organisationseinheiten.



ARCHITEKTUR

Architektur und Weiterentwicklung einer Endpunkt-Sicherheitslösung haben eine zentrale Bedeutung für die Effektivität und Skalierbarkeit sowie für den fortlaufenden Nutzwert.

Organisationen, die sich beständig verändern und wachsen, benötigen Endpunktsicherheit mit der Fähigkeit zur Anpassung. Nur so kann kontinuierlich die bestmögliche Sicherheit bereitgestellt werden, ohne negative Auswirkungen auf Performance, Handhabung und das tägliche Management.

Ein Interface für den Zugriff auf Funktionen der Endpoint Protection Platform (EPP)

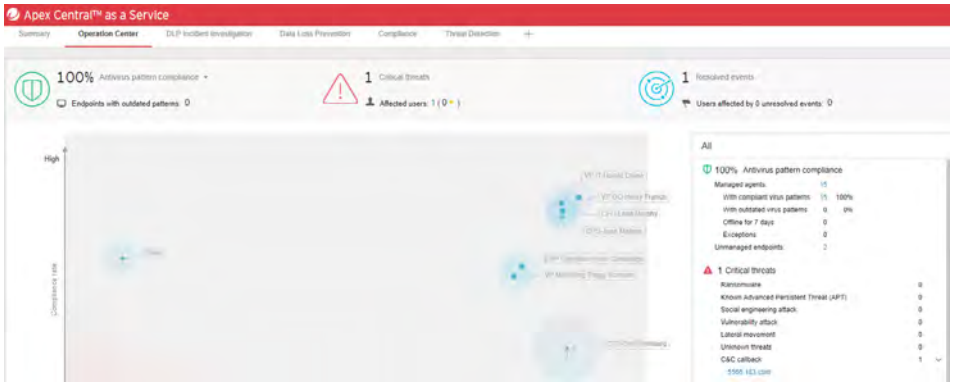
Visualisiert EPP- und EDR-Funktionalität sowie Alarme auf einer gemeinsamen Oberfläche.

Warum ist das wichtig?

- Ein einziges Interface reduziert die Zeit, die für die Suche nach Informationen in mehreren Konsolen benötigt wird, und bietet eine ganzheitliche Übersicht des Gesamtsicherheitsstatus.

Der Trend Micro Ansatz

- Apex Central bietet eine detaillierte Übersicht zu Alarmen, Richtlinieninformationen und Timelines für alle Endpunkte in der Umgebung.
- Anwenderzentrierte Darstellungen geben Administratoren einen Überblick zum Sicherheitsstatus eines bestimmten Anwenders, inklusive Email, Web, Verschlüsselung und Datenschutz.
- Administratoren verwalten und konfigurieren ihre EPP Richtlinien und Regeln, ohne die Managementkonsole verwenden zu müssen.



Worauf Käufer achten müssen

- Zentralisierte Konsole für Zugriff und Management Endpunkt- und EDR-Funktionen.

Skalierbarkeit

Ermöglicht Wachstum und Anpassung der Sicherheitsplattform ohne zusätzliche Komplexität.

Warum ist das wichtig?

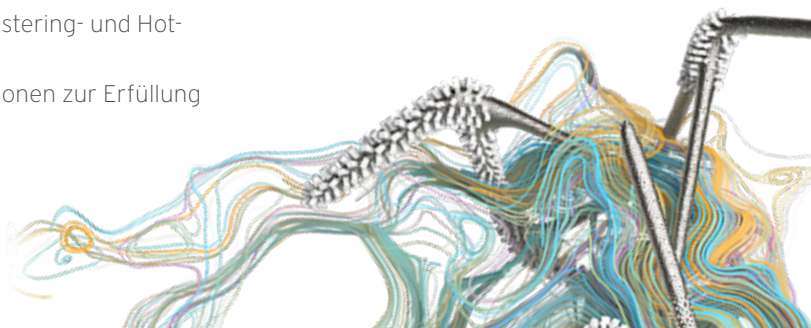
- Umfangreiche Änderungen bedeuten bei Sicherheitsprodukten meist einen erheblichen Aufwand. Deshalb ist Skalierbarkeit wichtig, denn sie ist die Voraussetzung für die Anpassung der Lösung an veränderte oder gewachsene Anforderungen.

Der Trend Micro Ansatz

- Apex One unterstützt Organisationen mit einer beliebigen Zahl von Anwendern. SaaS-Bereitstellungen mit Auto-Scaling passen sich an die Entwicklung von Unternehmen an.
- On-Premises-Bereitstellungen von Apex One profitieren von Clustering- und Hot-Backup-Funktionalität.
- Konsistente und zeitnahe Bereitstellung von Updates und Funktionen zur Erfüllung der Kundenanforderungen.

Worauf Kunden achten müssen

- Horizontaler Skalierungsansatz
- Dedizierte Ressourcen für Forschung und Entwicklung mit einer kontinuierlichen Feature Roadmap.



Einfache Prozesse für Bereitstellung und Updates

Bietet mehrere Bereitstellungsoptionen für die bestehende Organisationspraxis.

Warum ist das wichtig?

- Viele Anwender arbeiten heute remote und verwenden dabei mehr als ein Gerät (z.B. Desktop, Laptop, Tablet, Mobiltelefon). Wirksamer Endpunktschutz setzt voraus, dass diese Systeme effizient mit Updates und neuen Versionen der Sicherheitssoftware versorgt werden können.

Der Trend Micro Ansatz

- Die Bereitstellung von Trend Micro SaaS-Lösungen kann über einen Self-Service-Link oder den Download vorkonfigurierter Agenten erfolgen.
- On-Premises-Installationen sind über vorpaketierte Agenten, Self-Service-Links oder legitimierte Verteilung mittels Konsole möglich. Die Konfiguration kann die Entfernung bestehender Antivirus-Produkte vor der Installation einschließen.
- Apex One Agenten können mit der Managementinfrastruktur kommunizieren, zum Beispiel für Änderungen der Richtlinien-Konfiguration, Aktualisierung der Agenten mit neuesten Bedrohungsinformationen und / oder Updates der Agenten auf die neueste Softwareversion.
- Bietet flexible Bereitstellungsoptionen für Agenten, sodass Organisationen bestehende Prozesse und Werkzeuge zur Verteilung über MSI-Pakete, Web-Browser etc. verwenden können.

Worauf Käufer achten müssen

- SaaS- und On-Premises-Bereitstellungsoptionen.
- Automatische Deinstallation alter Versionen oder Austausch von Sicherheitsprodukten.
- Remote-Aktualisierung von Agenten und Endpunkten sowie Richtlinien-Konfigurationen.
- Flexible Bereitstellungsoptionen für Agenten.

Geografische Verfügbarkeit von SaaS und MDR

Globale Verfügbarkeit des Service für Bedrohungsanalyse und Reaktion.

Warum ist das wichtig?

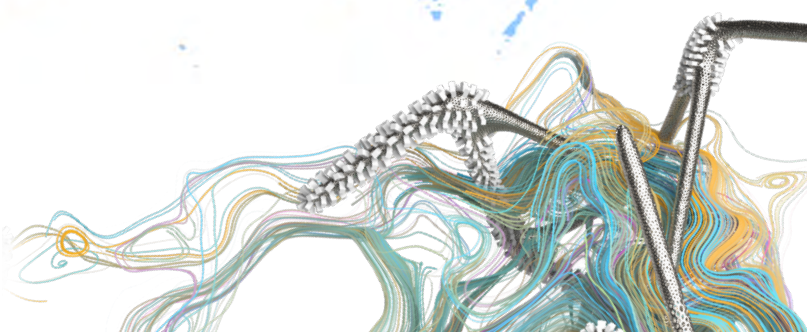
- Globale Abdeckung rund um die Uhr trägt zu kontinuierlichem Schutz und Compliance bei.

Der Trend Micro Ansatz

- Mehrere Rechenzentren und SOCs in verschiedenen Zeitzonen und auf verschiedenen Kontinenten.
- Strenge Sicherheitsregeln und dokumentierte Verfahren für die Datensammlung gewährleisten den höchsten Datenschutzstandard.

Worauf Kunden achten müssen

- Speicherung der Kundendaten in Übereinstimmung mit regionalen Vorschriften.
- SaaS-Zertifizierung nach ISO 27001:2013.
- DSGVO-Compliance



Effiziente Agenten-Architektur

Stellt angepasste Informationen zu aktiven Realworld-Bedrohungen bereit.

Warum ist das wichtig?

- Lösungen mit intensivem Ressourcenverbrauch und mehrere Agenten auf dem Endpunkt vergrößern das Risiko ungünstiger Auswirkungen auf die Performance und Software-Interaktionen.
- Wenn eine unzulänglich konzipierte Sicherheitslösung die Erledigung von Aufgaben erschwert, tendieren Anwender dazu, die Sicherheitsvorkehrungen zu umgehen.

Der Trend Micro Ansatz

- Setzt im ersten Schritt auf Threat Intelligence für Erkennung und Abwehr.
- Prüft Dateien und Prozesse anhand einer Liste bereits als harmlos / bösartig bekannter Dateien und Prozesse. Bedrohungen werden mit einem Listenvergleich nahezu in Echtzeit blockiert.
- Verwendet ein globales Cloud-Netzwerk für fortschrittliches Machine Learning vor und während der Ausführung sowie für vollständige Verhaltensüberwachung.

Worauf Käufer achten müssen

- Integration aktueller, globaler Bedrohungsinformationen in die Endpunktsicherheit.
- Kombinationen verschiedener Ansätze zur Bedrohungserkennung, mit denen als bösartig bekannte Dateien bereits gefiltert werden können, bevor ressourcenintensivere Verfahren zum Einsatz kommen.

Bereitstellungsoptionen für Security-as-a-Service (SaaS) und On-Premises

Bietet Flexibilität bei der Bereitstellung der Sicherheit und vollständige Produktparität beider Optionen.

Warum ist das wichtig?

- Viele Organisationen bevorzugen On-Premises-Bereitstellungen für Endpunkte, andere möchten einen Cloud-orientierten Software-as-a-Service-Ansatz verwirklichen. Wieder andere verfolgen einen hybriden Ansatz. Deshalb ist es wichtig, dass sich die Sicherheitslösung an den individuellen Mix der Bereitstellungsoptionen eines Unternehmens anpassen kann.

Der Trend Micro Ansatz

- Apex One bietet Kunden vollständige Kontrolle über die Bereitstellungsszenarien. Sowohl On-Premises- als auch SaaS-Optionen sind verfügbar.
- Unterstützt Kunden bei Ausbau und Anpassung ihrer individuellen Mischung aus SaaS- und On-Premises-Bereitstellung, um sich verändernde Anforderungen abzubilden.

Worauf Käufer achten müssen

- On-Premises- und SaaS-Bereitstellungsoptionen.
- Vollständige Produktparität zwischen SaaS und On-Premises
- Flexible Lizenzierung zwischen Bereitstellungsoptionen
- Option für Veränderungen der Bereitstellungsoptionen in der Zukunft

Globaler Support

Bietet Kunden-Support zu jeder Zeit und jedem Ort.

Warum ist das wichtig?

- Angriffe passieren weltweit rund um die Uhr. Eine Sicherheitslösung muss daher globalen Support bieten und verschiedene Zeitzonen abdecken.

Der Trend Micro Ansatz

- Bietet 24x7-Support als Standard für alle Lösungen.
- Support-Zentren rund um die Welt unterstützen Kunden bei Bedarf.
- Support erfolgt in den meisten Regionen in Landessprache.

Worauf Käufer achten müssen

- 24x7-Support
- Globale Support-Zentren mit Unterstützung rund die Uhr.
- Support in Landessprache.

TREND MICRO™

Securing Your Connected World