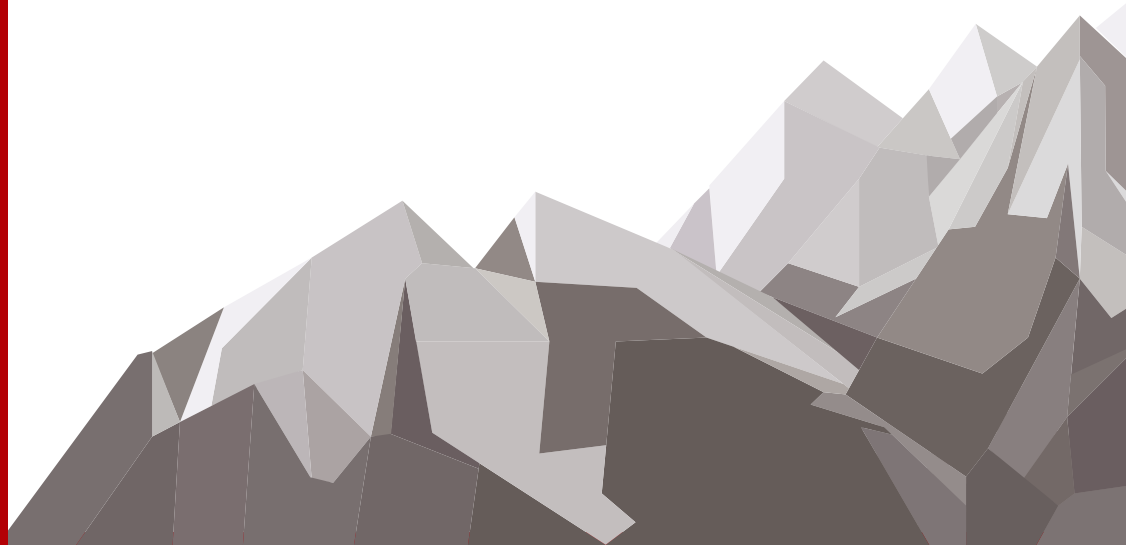
Trend Micro

APEX ONE™

Handbuch für Channel Partner

Inhalt



01 EINLEITUNG

01.1 Was ist Apex One™ ?

Trend Micro Apex One™ ist ein **Komplettpaket für moderne Endpunktsicherheit**. Mit einem **einzigen, schlanken Agenten** auf dem Endpunkt deckt Apex One™ die Funktionalität von Trend Micro OfficeScan, Vulnerability Protection, Application Control und Endpoint Sensor ab. Dies ermöglicht eine stark vereinfachte Implementierung und macht den Einsatz mehrerer Produkte unterschiedlicher Hersteller überflüssig.

Apex One™ schützt alle PCs, Macs und virtuelle Desktops innerhalb und außerhalb des Unternehmensnetzwerks. Die Lösung kann mit nahezu identischen Funktionen sowohl als Software-as-a-Service (SAAS) als auch On-Premise ausgerollt werden. Bestehende OfficeScan-Kunden erhalten Apex One™ als reguläres Update im Rahmen der eingesetzten Suite ohne zusätzliche Kosten. Für einige Funktionen wie zum Beispiel Endpoint Detection and Response (EDR)-Investigation können aber zusätzliche Lizenzierungen notwendig sein, abhängig von aktuellen Berechtigungen.

01.2 Warum Apex One™ ?

Die Liste der Bedrohungen für den Endpunkt wird immer länger und komplexer. Traditionelle, rein Signatur-basierte Sicherheitsprodukte bieten keinen ausreichenden Schutz mehr gegen Ransomware, Crypto-Malware, dateilose Angriffe & Co. Sogenannte Next-Generation-Technologien eignen sich zwar hervorragend zur Entdeckung und Abwehr einiger dieser Bedrohungen, sind bei anderen aber wiederum weniger wirksam. Um einen umfassenden Schutz zu gewährleisten, mussten IT-Sicherheitsteams daher bislang verschiedene Sicherheitsprodukte auf dem Endpunkt installieren und verwalten. Diese Herangehensweise führt zu einem erheblichen Aufwand für die Installation, Administration und Aktualisierung multipler Produkte sowie zu einer hohen Belastung der Endpunkt- und Netzwerkressourcen.

Durch den Einsatz isolierter Einzelprodukte entstehen zudem Informationssilos, die einen Gesamtüberblick zur Bedrohungslage unmöglich machen. Fehlende Kommunikation verhindert die richtige Einordnung von Alarmen und damit auch die Einleitung schneller, angepasster Reaktionen. Wenn Sicherheitsverantwortliche Informationen manuell aus verschiedenen Konsolen zusammentragen müssen, erschwert dies zudem Analysen zu Ursprung, Ausbreitung und zeitlichem Verlauf von Angriffen im Rahmen von Endpoint Detection and Response (EDR).

01.3 Was ist neu?

Apex One™ lernt kontinuierlich hinzu, passt sich an und teilt Bedrohungsinformationen automatisch mit der gesamten Umgebung. Dieser kombinierte Schutz wird über eine Architektur bereitgestellt, die Ressourcen effizienter einsetzt. Im Vergleich zu Mitbewerberprodukten werden daher sowohl CPU als auch Netzwerk weniger belastet.

01.4 Vorteile von Apex One™ im Überblick:

- Schützt vor bekannten und unbekannten Bedrohungen mit einem einzigen Agenten auf dem Endpunkt.
- Setzt immer die jeweils beste Technologie ein, inklusive Machine Learning, Verhaltensanalysen, Applikationskontrollen, Web- und File-Reputation etc.
- Gewährleistet die branchenweit schnellste Abschirmung von Schwachstellen, basierend auf führender Schwachstellenforschung.
- Integriert hochentwickelte Endpoint Detection and Response (EDR) Funktionen und den optionalen Managed Detection Response (MDR) Service, bei dem Trend Micro das Threat Hunting übernimmt.
- Kommuniziert mit anderen lokalen Sicherheitsprodukten und nutzt die aktuellen Informationen aus dem Trend Micro Smart Protection Network.
- Bietet zentralisierte Sichtbarkeit und Kontrolle der gesamten Funktionalität über eine einzige Konsole bei Bereitstellung über Apex Central.
- Integriert mobile Sicherheit über Apex Central, inklusive Schutz für Mobilgeräte, Mobile-App- und Mobile-Device-Management.
- Ermöglicht die Anpassung an individuelle Anforderungen durch optionale Module.
- Vereinfacht die Bereitstellung durch Software-as-Service- und On-Premise-Optionen.

02 VORTEILE VON APEX ONE™

02.1 Vorteile für unsere Partner

Mit Apex One™ bieten Sie Ihren Kunden modernen Endpunktschutz, der dem neuesten Stand der Technik entspricht und auch die Anforderungen der DSGVO an technologisch aktuelle Sicherheit erfüllt.

- Führender Hersteller: Trend Micro wird sowohl von Gartner als auch von Forrester Research als „Leader" im Bereich Endpunktsicherheit platziert*.
- Komplettschutz aus einer Hand: Ein Agent auf dem Endpunkt für umfassende Sicherheit und Endpoint Detection and Response (EDR) minimiert Ihren Aufwand. Einfache Aktivierung zusätzlicher Funktionen und Module.
- Erweitert Serviceangebot: Einhaltung der Compliance, forensische Endpoint Detection and Response (EDR)-Analysen – Apex One™ bietet vielfältige Optionen und integriert sich problemlos in Ihr Service-Angebot.
- Flexible Lizenzierung: Upselling-Optionen ermöglichen die Anpassung an die individuellen Bedürfnisse Ihrer Kunden.

* „Gartner Magic Quadrant for Endpoint Protection Plattforms 2018" und „The Forrester Wave™: Endpoint Security Suites, Q2 2018"

02.2 Vorteile für Ihre Kunden

Apex One™ bietet Ihren Kunden sowohl aus technischer als auch aus wirtschaftlicher Perspektive eine Reihe von Vorteilen:

- Alles in einem: Automatische Erkennung und Reaktion auf eine stetig wachsende Bedrohungsvielfalt, inklusive dateiloser Angriffe und Ransomware.
- Vollständige Sichtbarkeit: Aufschlussreiche Analysefunktionen und zentralisierte Sichtbarkeit des gesamten Netzwerks durch Verwendung fortschrittlicher Endpoint Detection and Response (EDR)- und Managed Detection and Response (MDR)-Werkzeuge, SIEM-Integration und offener APIs.
- Vereinfachte Compliance: Data Leak Prevention (DLP), Endpunktverschlüsselung und Gerätekontrolle schützen sensible Daten, wie von der DSGVO gefordert.
- Entlastung von Sicherheitsteams: Auslagerung des Threat Hunting durch optionalen Managed Detection and Response (MDR) Service.
- Schutz der Produktivität: Komplette Funktionalität wird über einen einzigen Agenten bereitgestellt. Geringere Belastung der Endpunktressourcen ermöglicht reibungsloses Arbeiten.
- Angepasste Bereitstellung: Nahezu identische Funktionalität für Software-as-a-Service (SaaS)- und On-Premise-Optionen. Zusatzmodule jederzeit über Lizenzschlüssel integrierbar.
- Verbesserte Kostentransparenz: Eliminiert die Notwendigkeit, Lizenzen für mehrere Produkte unterschiedlicher Hersteller zu verwalten.

03 Trend Micro Enterprise Suites und Apex One™

Der folgenden Tabelle können Sie entnehmen, wie sich Apex One™ in die Familie der Trend Micro Enterprise Suites einfügt:

* eingeschränkter Funktionsumfang
** dieser Service kann nur in Kombination mit Endpoint Detection and Response (EDR) erworben werden
● über Apex One Single Agent

	Smart Protection Complete	Smart Protection for Endpoints	Smart Protection for Office 365	Enterprise Security Suite	Enterprise Security for Endpoints and Mail Servers	Enterprise Security for Endpoints	Enterprise Security for Endpoints Light	Enterprise Security for Communi-cation & Collaboration	Enterprise Security for Gateways
Endpoint ● über Apex One Single Agent									
Security for Windows Desktop & Server ●	✔	✔		✔	✔	✔	✔		
Security for Linux Desktop & Server	✔	✔		✔	✔	✔	✔		
Security for Macintosh●	✔	✔		✔	✔	✔			
Security for Novell NetWare	✔	✔		✔	✔	✔	✔		
Virtual Desktop Integration●	✔	✔		✔	✔	✔			
Integrated for Data Loss Prevention●	✔	✔						✔	
Device Control ●	✔	✔		✔ *	✔ *	✔ *	✔ *		
Mobile Device Management	✔	✔		✔ *	✔ *	✔ *			
Vulnerability Protection ●	✔	✔		✔	✔	✔			
Endpoint Application Control ●	✔	✔							
Endpoint Encryption (File/Folder/Full Disk)	✔	✔							
Apex One as a Service	✔	✔							
Email & Collaboration									
Cloud App Security for Office365, Google Drive, Dropbox, Box	✔		✔						
Messaging Gateway	✔			✔					✔
Hosted Email Security	✔		✔						
Email Encryption	✔								
Security for Microsoft Exchange	✔			✔	✔			✔	
Security for IBM Lotus Domino	✔			✔	✔				
Security for Microsoft SharePoint	✔							✔	
Security for Microsoft Skype for Business	✔							✔	
Web									
Web Gateway	✔			✔					✔
InterScan Web Security as a Service	✔								
Management									
Central Management / Apex One Central	✔	✔		✔	✔	✔	✔	✔	✔
Control Manager as a Service / Apex One Central as a Service	✔	✔							
Optionale kostenpflichtige Erweiterungen									
Endpoint Detection & Response (EDR)●	✔	✔		✔	✔	✔	✔		
Managed Detection & Response Service **	✔	✔		✔	✔	✔	✔		
Cloud Sandboxing	✔	✔		✔	✔	✔	✔		

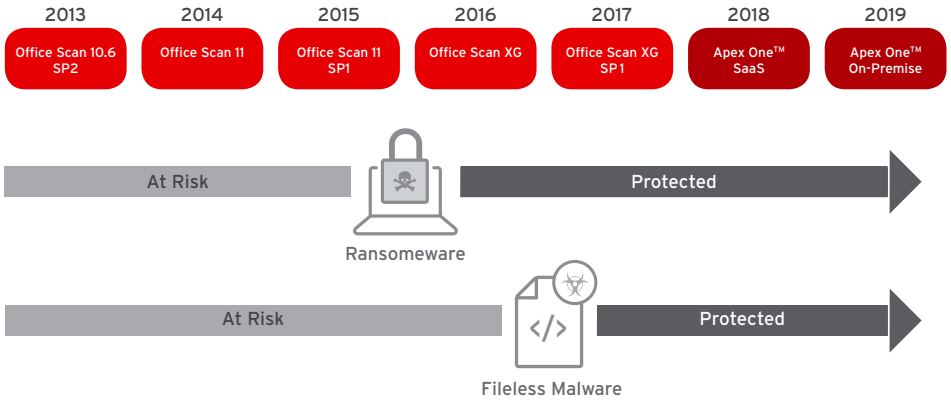
04 Vertriebsansätze - Upgrade und Add-on

04.1 Neukunden

ANFORDERUNG	LÖSUNG
• Umfassende Sicherheit für Endpunkte • Verfügbar als SaaS oder On-Premise	**Smart Protection for Endpoints** mit optionalen Add-ons für EDR (Endpoint Sensor) und MDR.
• Umfassende Sicherheit für Endpunkte, Mail und Web, inklusive Schutz für Office365, Dropbox, Box und Google Drive. • Verfügbar als SaaS oder On-Premise	**Smart Protection Complete** mit optionalen Add-ons für EDR (Endpoint Sensor) und MDR.

04.2 Upgrade für bestehende Kunden

Ganz wichtig! Jeder Ihrer Bestandskunden sollte schnellstmöglich kostenlos auf Apex One™ upgraden, um auch gegen Ransomware, Cryptomalware und dateilose Malware bestmögliche Schutzmechanismen ausgerollt zu haben. Einfach Version aktualisieren und alle Vorteile des Single Agent nutzen.



04.3.1 Upsell-Möglichkeiten für bestehende Kunden

Parallel oder nachgelagert zum kostenlosen Upgrade bietet sich das Upsell auf eine vom Funktionsumfang größere Enterprise Suite an! Denn hier bieten sich zahlreiche Mehrwerte für Ihre Kunden, insbesondere in punkto Datengrundschutzkonformität. Sie als Partner können im besten Fall 3 x mehr Marge generieren. Apex One™ macht es Ihnen leicht, Umsätze zu steigern und Marge zu optimieren. Ihr Kunde hat zum Beispiel Enterprise Security for Endpoints Light in Einsatz und Sie verkaufen ihm die Mehrwerte von Smart Protection for Endpoints.

Mehrwert für Sie als Partner

Renewal Enterprise Security for Endpoints Light

1.000 € Marge*

3x

Smart Protection for Endpoints Upsell

3.000 € Marge* im ersten Jahr
Je **3.000 € Marge*** in den Folgejahren

*Beispielrechung für bronze Partner

Nebenbei positionieren Sie Ihre Expertise, kommen nicht in die Situation gegen Microsoft „embedded" Security zu argumentieren und profitieren vom Service und höherer Kundenzufriedenheit.
In der Tabelle auf der nächsten Seite stellen wir Ihnen weitere Upgrade- und Upsell-Pfade im Überblick vor.

04.3.2 Weitere Upgrade- und Upsell-Pfade im Überblick:

IHR KUNDE HAT:	VORTEILE DES UPGRADES AUF APEX ONE™:	UPSELL UND ADD-ON MÖGLICHKEITEN:
Trend Micro™ Smart Protection Suites	• **Single-Agent-Architektur** ermöglicht die Bereitstellung der gesamten Funktionalität über einen einzigen schlanken Agenten • **Verbesserte Erkennungsfunktionen** inklusive Schutz vor dateiloser Malware • **Einfache Add-on-Funktionalität** eliminiert die Notwendigkeit komplexer Bereitstellungen • **Funktionsgleichheit** zwischen Hosted-SaaS- und On-Premise-Versionen	• **Zusätzliches EDR** mit Apex One™ Endpoint Sensor über dieselben Agenten, Management-Konsolen und Workflows • **Zusätzliches MDR** für Managed Detection and Response Services • **Zusätzliches cloudbasiertes Sandboxing**
Trend Micro™ Enterprise Security für Endpoints Trend Micro™ Enterprise Security Suite Enterprise Security for Endpoints Light Zusätzliche Trend Micro™ Suites	• **Single-Agent-Architektur** ermöglicht die Bereitstellung der gesamten Funktionalität über einen einzigen schlanken **Agenten** • **Verbesserte Erkennungsfunktionen** inklusive Schutz vor dateiloser Malware • **Einfache Add-on-Funktionalität** eliminiert die Notwendigkeit komplexer Bereitstellungen	• **Upgrade auf Smart Protection Suites** für erweiterten Schutz, inklusive Applikationskontrolle, DLP und Verschlüsselung. Bereitstellung von SPS als SaaS-, On-Premise- oder hybride Version • **Zusätzliches EDR** für Endpoint Detection and Response mit Apex One™ Endpoint Sensor über dieselben Agenten, Management-Konsolen und Workflows • **Zusätzliches MDR** für Managed Detection and Response Services • **Zusätzliches cloudbasiertes Sandboxing**
Trend Micro™ OfficeScan™ Standalone	• **Verbesserte Erkennungsfunktionen** inklusive Schutz vor dateiloser Malware • **Einfache Add-on-Funktionalität** eliminiert die Notwendigkeit komplexer Bereitstellungen	• **Zusätzliches EDR oder MDR** über einen einfachen **Lizenz-Code** • **Upgrade auf Smart Protection Suites** für erweiterten Schutz, inklusive Applikationskontrolle, DLP und Verschlüsselung. Bereitstellung von SPS als SaaS-, On-Premise- oder hybride Version

Upsell ist für Ihre Kunden relevant, denn nach der Datengrundschutzverordnung sind DLP und Encryption von der Kür zur Pflicht geworden. Wie lösen das Ihre Kunden, was können Sie anbieten? Zuerst Upgrade auf Apex One™ durchführen und im zweiten Schritt die Smart Protection Suite positionieren. Mit dieser Lizenz ist Ihr Kunde in punkto DLP und Encryption datengrundschutzkonform.

Virtual Patching ist für viele Kunden eine Herausforderung. Auch hier fordert die Datengrundschutzverordnung, stets und umgehend den aktuellen Patch auf allen Endpoints auszurollen. Und erneut gilt: Upgrade auf Apex One™ durchführen und die Lizenz für Vulnerability Protection aktivieren. Ihr Kunde profitiert von einer der besten Technologien am Markt.

04.4 Add-On

PRODUKTNAME	BESCHREIBUNG
Apex One™ Endpoint Sensor • On-Premise • Hosted/SaaS	Integrierte Endpoint Detection and Response (EDR) ermöglicht fortschrittliches Threat Hunting und die Untersuchung komplexer Bedrohungen.
Trend Micro Managed Detection and Response*	Managed Detection and Response (MDR) ist ein Service, bei dem Trend Micro das Threat Hunting und die 24x7 Alarmüberwachung für Kunden übernimmt.
Apex One™ Sandbox as a Service	Integrierter Sandbox-Service ermöglicht den Test von verdächtigen Dateien, Emails und URLs in einer sicheren virtuellen Umgebung.

* Erfordert Apex One™ und Apex One™ Endpoint Sensor

04.4.1 Endpoint Detection and Response (EDR)

Weshalb EDR?

Eine gute Endpoint Protection Lösung entdeckt effektiv und in Echtzeit bekannte und unbekannte Bredrohungen. Sie zeigt auf, was passiert ist, bietet jedoch keine Visibilität darüber, was die initiale Infektion verursacht hat und wer noch betroffen ist. Endpoint Detection and Response (EDR) ermöglicht die schnelle und fundierte Analyse komplexer Angriffe, zum Beispiel durch Root-Cause- oder Patient-Zero-Untersuchungen. Marktforscher wie Gartner prognostizieren für die nächsten Jahre zweistellige Wachstumsraten in diesem Bereich*. Dabei werden insbesondere Lösungen profitieren, die Endpunktschutz mit EDR kombinieren.

Apex One™ beinhaltet bereits eine Reihe fortschrittlicher EDR-Funktionen, die mit der kostenpflichtigen Lizenzierung von Trend Micro Endpoint Sensor zu einer vollständigen EDR-Lösung ausgebaut werden können. Endpoint Detection and Response (EDR) lohnt sich für Unternehmen, die die Notwendigkeit und den Bedarf für mehr Transparenz, Prävention und Analyse haben. EDR bedarf gleichfalls und fortlaufend Manpower und Know-how, um die Daten zu analysieren und zu interpretieren. Als Technologie ist EDR seit ungefähr 5 Jahren verfügbar, Analysten sprechen seit 2018 darüber, das bedeutet es gibt noch ausreichend Neukundenpotential für Sie und kaum Verdrängungswettbewerb.

* „Gartner 2018 Market Guide for Endpoint Detection and Response Solutions."

Endpoint Detection and Response (EDR) ermöglicht die schnelle und fundierte Analyse komplexer Angriffe, zum Beispiel durch Root-Cause- oder Patient-Zero-Untersuchungen. Marktforscher wie Gartner prognostizieren für die nächsten Jahre zweistellige Wachstumsraten in diesem Bereich*. Dabei werden insbesondere Lösungen profitieren, die Endpunktschutz mit EDR kombinieren. Apex One™ beinhaltet bereits eine Reihe fortschrittlicher EDR-Funktionen, die mit der kostenpflichtigen Lizenzierung von Trend Micro Endpoint Senor zu einer vollständigen EDR-Lösung ausgebaut werden können.

Vorteile von Endpoint Detection and Response (EDR) mit Apex One Endpoint Sensor:

- Wesentlich einfachere Handhabung durch Automation und Integration
- Kontextsensitive Überprüfungen und schnellere Reaktionen für Endpunkte.
- Aufzeichnung und detailliertes Reporting von Aktivitäten auf Systemebene.
- Erkennung und Analyse komplexer Bedrohungsindikatoren. z.B. bei dateilosen Angriffen.
- Scans auf mehreren Ebenen über Endpunkte hinweg, basierend auf Suchkriterien wie OpenIOC, Yara und verdächtigen Objekten.

Der ideale Kunde

- Unternehmen ab 500 Mitarbeitern
    - Finanzbranche, insbesondere Banken
    - Betreiber kritischer Infrastrukturen, wie zum Beispiel Energie, Lebensmittel- und Wasserversorger, Informationstechnik & Telekommunikation
    - Medienanstalten & Verlagshäuser
    - Firmen, die das geistige Eigentum besonders schützen müssen
- Noch kein EDR im Einsatz: Wunsch und Notwendigkeit für mehr Transparenz, Prävention und Analyse
- Bereits EDR im Einsatz: Unzufrieden mit der Komplexität und Ineffizienz multipler EDR Werkzeuge
- Unzufrieden mit der Komplexität und Ineffizienz multipler EDR Werkzeuge

* „Gartner 2018 Market Guide for Endpoint Detection and Response Solutions"

04.4.2 Managed Detection and Response (MDR)

Managed Detection and Response (MDR) ist ein optionaler Service, bei dem Trend Micro das Threat Hunting sowie die 24x7 Überwachung und Priorisierung von Alarmen übernimmt. Mithilfe von künstlicher Intelligenz werden Daten von Endpunkten, Netzwerken und Servern des Kunden analysiert, um auch Bedrohungen aus der Grauzone zu identifizieren. Darüber hinaus untersuchen Trend Micro Experten Ursache und Ausbreitung des Angriffs, um gemeinsam mit dem Kunden ein detaillierten Reaktionsplan zu entwickeln.

Vorteile von MDR:

- Kein Personalbedarf: Unternehmen mit 500 bis 10.000 Mitarbeitern verfügen in der Regel nicht über ausreichende Personalkapazität für dediziertes Threat Hunting.
- Verbesserte Alarm-Bewertung: Sicherheitsprodukte für Endpunkte und-Netzwerke generieren eine Vielzahl von Alarmen, die für sich genommen unwichtig erscheinen. Durch die intelligente Korrelation der Alarme werden Zusammenhänge sichtbar, die auf komplexe Angriffe hinweisen können.
- Expertise von Trend Micro: Mitarbeiter mit Security-Know-how sind teuer und schwer zu finden. Durch MDR profitieren Unternehmen von der Expertise weltweit führender Bedrohungsexperten.

Der ideale Kunde

- Unternehmen mit 500 bis 10.000 Mitarbeitern
- Verfügen zwar über Trend Micro EDR, aber nicht über Zeit und Know-how für effektive Nutzung

04.4.3 Cloud Sandboxing

Apex One™ bietet zusätzliche Sicherheit durch optionales Cloud Sandboxing für automatische, detaillierte Simulationen und Analysen potenziell gefährlicher Dateianhänge in einer sicheren virtuellen Umgebung, die von Trend Micro gehostet wird. Cloud Sandboxing erfordert eine eigene, kostenpflichtige Lizenz.

Der ideale Kunde

- Besonders gefährdete Unternehmen, wie Betreiber kritischer Infrastrukturen oder Inhaber geistigen Eigentums
- Bedarf an zusätzlichen Analysefähigkeiten

04.4.4 On-Premise oder SaaS-Lösung – es macht keinen Unterschied

Trend Micro Apex One™ kann sehr flexibel eingesetzt werden. Die meisten Funktionen können sowohl On-Premise als auch als SaaS-Version oder im Mischbetrieb ausgerollt werden. Sowohl Sie als Partner als auch Ihre Kunden erhalten somit größtmögliche Flexibilität.

	ON-PREMISE	SAAS
Schutz vor bekannten Bedrohungen (Dateien, Signaturen und Web Reputation)	✔	✔
Machine Learning, Erkennung von unbekannten Bedrohungen (vor der Ausführung und in Echtzeit)	✔	✔
IOA verhaltensbasierte Analyse zur Erkennung unbekannter Bedrohungen	✔	✔
Exploit Prevention	✔	✔
Virtual Patching	✔	✔
Applikationskontrolle	✔	✔
DLP integriert	✔	✔
Device Control	✔	✔
Zentrale Visibilität durch Apex Central	✔	✔
Analyse-Funktionen (EDR) mit Endpoint Sensor (Add-On/Option)	✔	✔
Managed Detection and Response (Add-On/Option)	✔	✔
Sandbox Analyse	✔	✔

Endpoint Encryption Funktionen (Full-Disk & Datei/Ordner) werden ausschließlich on-premise geliefert und benötigen einen speziellen Agent. Dieses grenzt klar von Endpoint Security und EDR-Funktionen ab.

05 Lizenzierung

Apex One™ ist immer Bestandteil einer Suite. Daher gelten die für die Suite zugrundeliegenden Lizenzierungsregeln.

Apex One™ als Bestandteil einer Enterprise Suite

- ab 26 Usern
- Kauf / Wartung

Apex One™ als Bestandteil einer Smart Protection Suite (for Endpoints oder Complete)

- ab 101 Usern
- Subscription-Modell

Endpoint Sensor as a Service und Sandbox as a Service

- ab 251 Usern
- Subscription-Modell
- Voraussetzung: gültige Apex One™ Lizenz
- Die User-Anzahl muss paritätisch zur Apex One™ -Lizenz sein

Endpoint Sensor on Premise für Endpoint Detection and Response (EDR)

- ab 26 Usern
- Subscription-Modell
- Voraussetzung: gültige Apex One™ Lizenz
- Die User-Anzahl muss paritätisch zur Apex One™ -Lizenz sein

Managed Detection and Response (MDR) for Endpoints

- ab 251 Usern
- Subscription-Modell
- Voraussetzung: gültige Apex One™ Lizenz und gültige EDR-Lizenz
- Die User-Anzahl muss paritätisch zur Apex One™- und EDR-Lizenz sein

Gibt es neue Artikelnummern für Apex One™ ?

Nein, es gelten weiterhin die bekannten Artikelnummern.

Bekommen OfficeScan-Kunden ein kostenfreies Upgrade auf Apex One™?

Ja! Allerdings nur in dem Funktionsumfang der vorher genutzten Lizenz.

Können nun alle OfficeScan Kunden die Apex One™ -Funktionalitäten wie Application Control und EDR nutzen?

Nein. Apex One™ bietet über den Single-Agent alle Funktionalitäten. Die Aktivierung und Nutzung dieser ist jedoch vom erworbenen Lizenzumfang/Upsell abhängig.

Wie können Kunden, die ältere Suites im Einsatz haben, die neuen Funktionalitäten nutzen?

Funktionalitäten wie Vulnerability Protection oder Application Control sind in den Smart Protection Suites enthalten. Durch ein Upgrade auf diese Suites können diese genutzt werden. EDR, MDR und Cloud Sandbox müssen in einer separaten Lizenz käuflich erworben werden.

Welche Lizenz-Voraussetzungen müssen erfüllt werden für die Nutzung von Managed Detection and Response (MDR)?

Für die Nutzung von MDR-Services müssen Kunden sowohl eine gültige Apex One™ Lizenz als auch eine Lizenz für den Apex One™ Endpoint Sensor haben.

Marketing-Materialien

Materialien zur Bewerbung von Upgrade, Upsell und Add-On Potentialen, haben wir für Sie unter http://www.trendmicro.com/apexoneforchannel zusammengestellt.

06 Fragen & Antworten

Ist Apex One™ ein neues Produkt oder eine neue Version von OfficeScan?
Lizenzrechtlich ist Apex One™ eine neue Version von OfficeScan. Jeder Kunde, der eine OfficeScan Lizenz im Rahmen einer Suite besitzt, kann künftig Apex One™ nutzen. Technisch gesehen ist Apex One™ die Kombination mehrerer Endpunktsicherheitslösungen, die als Bestandteil von Suiten lizenziert werden können.

Müssen Kunden auf Apex One™ upgraden?
Nein, das Upgrade ist optional. Im Rahmen eines effektiven Schutzes ist es allerdings dringend empfohlen, immer die aktuellste Version einer Sicherheitslösung einzusetzen.

Können Worry-Free Kunden Apex One™ nutzen?
Nein, Apex One™ ist ein Upgrade zu OfficeScan. Wenn Worry-Free Kunden Apex One™ nutzen wollen, ist ein CrossUpgrade auf die Smart Protection Suites erforderlich.

Gibt es Unterschiede zwischen SaaS- und On-Premise-Version?
Nein, Agent und Funktionalität sind identisch. Aufgrund der Eigenschaften von VDI-Umgebungen funktioniert das VDI-Plugin allerdings nur in On-Premise-Bereitstellungen.

Welche Kosten entstehen beim Upgrade auf Apex One™ ?
Beim Upgrade von einer Suite (z.B. Enterprise Security for Endpoints) auf Apex One™ entstehen keine zusätzlichen Kosten. Um den vollen Funktionsumfang bzw. bestimmte Optionen von Apex One™ zu nutzen, ist aber unter Umständen ein Upgrade auf eine höhere Suite (z.B. Smart Protection for Endpoints) oder die Lizenzierung der gewünschten Module erforderlich.

Was ist mit Kunden der NeatSuite oder ClientServer Messaging Suite?
Wenn ihr Kunde eine dieser beiden Suites einsetzt, kontaktieren Sie uns bitte unter salesinfo_de@trendmicro.com oder wenden Sie sich an Ihren Partner Business Manager.

Können alle Funktionen von Apex One™ einzeln lizenziert werden?
Nein, das bisherige Suiten-Modell bleibt bestehen. Manche Funktionen sind erst nach Upgrade der Suite verfügbar. Allerdings gibt es drei Optionen, die hinzugekauft werden können, wobei MDR nur mit EDR lizensiert werden kann:

- Endpoint Detection and Response (EDR)
- Managed Detection and Response Service (MDR)
- Cloud Sandboxing

EDR und MDR sind für alle Suiten verfügbar, die Apex One™ enthalten.

Wie können Kunden die SaaS-Version von Apex One™ testen?
- Kunden mit Smart Protection for Endpoints oder Smart Protection Complete Suite finden in ihrem Lizenzzertifikat einen Schlüssel für „OfficeScan as a Service“. Mit diesem Schlüssel kann die SaaS-Konsole von Apex One™ freigeschaltet werden.
- Kunden mit anderen Suites können einen Schlüssel für einen 30-tägigen Test beantragen. https://www.trendmicro.com/de_de/business/products/user-protection/sps/endpoint.html

Kann von einer On-Premise Smart Protection Suite zu SaaS migriert werden?
Ja, SaaS-Funktionen sind in den Lizenzen der Smart Protection Suites enthalten.

Kann von älteren Suiten zu SaaS migriert werden?
Ja, aber sie benötigen eine Lizenz für eine Smart Protection Suite.

Wie einfach ist die Migration von On-Premise zu SaaS?
Sehr einfach. Da der Agent baugleich ist, lässt sich über die Konsole eine SaaS-Server-Instanz anfordern, auf die Richtlinien und Konfigurationen kopiert werden. Die Agenten werden dann in die SaaS-Umgebung verlagert und angewiesen, auf die SaaS-Instanz zu verweisen. Damit ist die Migration abgeschlossen.

Ist Funktionalität von Application Control, Vulnerability Protection und Endpoint Sensor in der SaaS-Version verfügbar?
Ja.

Warum ist SaaS kein Add-on für alle Suiten?
Ältere Suiten verwenden unbefristete Lizenzen, was für SaaS-basierte Produkte aufgrund der kontinuierlich anfallenden Betriebskosten nicht passend ist. Nur unsere Smart Protection Suites verwenden ein Subscription-Modell.

Ist DLP Bestandteil von Apex One™ ?
Ja, DLP Funktionalität sowie Gerätekontrolle sind in Apex One™ integriert. Die Aktivierung ist abhängig von der Lizenz, denn einige ältere Suites umfassen kein DLP.

Ist Endpoint Encryption in den Apex One™ Agenten integriert?
Nein. Endpunktverschlüsselung, die zum Beispiel in Smart Protection Suites und einigen anderen älteren Suites enthalten ist, kann über einen separaten Agenten bereitgestellt werden.

Kann der MDR Service alleine erworben werden?
Nein, der MDR Service benötigt die Daten des EDR Moduls und kann nur mit diesem zusammen erworben werden. Er kann allerdings auch in Kombination mit anderen Trend Micro Lösungen wie Deep Discovery Inspector erworben werden.

07 Weitere Informationen

Auf dem Trend Micro Partner Portal unter https://community-trendmicro.force.com/Partner finden Sie die Sales Library, die eine Vielzahl von Präsentationen, Datenblättern, Solution Briefs, Whitepaper u.v.m. enthält. Diese Materialien sollten Ihnen helfen sollen, Trend Micro Lösungen bei Ihren Kunden zu positionieren. Viele Informationen sind auch in Deutsch verfügbar.

08 Ihr Kontakt zu Trend Micro

Telefon*:

Deutschland:	+49 (1805) 010873
Österreich:	+43 (820) 401147
Schweiz:	+41 (842) 010873

*DE: 14 Cent/Minute aus dem deutschen Festnetz. Bei Anrufen aus deutschen Mobilfunknetzen abweichende Preise von höchstens 42 Cent/Minute.
AT: 11,6 Cent/Minute aus dem österreichischen Festnetz. Abweichungen für Anrufe aus dem Mobilfunknetz möglich.
CH: 11 Rappen/Minute aus dem schweizer Festnetz. Abweichungen aus dem Mobilfunknetz möglich.

Email:
salesinfo_de@trendmicro.com

Renewals Deutschland:
bis 500 Mitarbeiter:
renewalsales@trendmicro.de

ab 501 Mitarbeiter:
renewalsales500@trendmicro.de

Renewals Österreich:
+43 (72) 08 82 401

Renewals Schweiz:
+41 (31) 52 80 515

Distribution Deutschland:

Arrow ECS AG
trendmicro.ecs.de@arrow.com

Ingram Micro Distribution GmbH
trendmicro@ingrammicro.de

Westcon Group Germany GmbH
trendmicro@westconsecurity.de

Distribution Österreich:

Arrow ECS Internet Security AG
sales@arrowecs.at

Westcon Group Austria GmbH
sales.at@westcon.com

Distribution Schweiz:

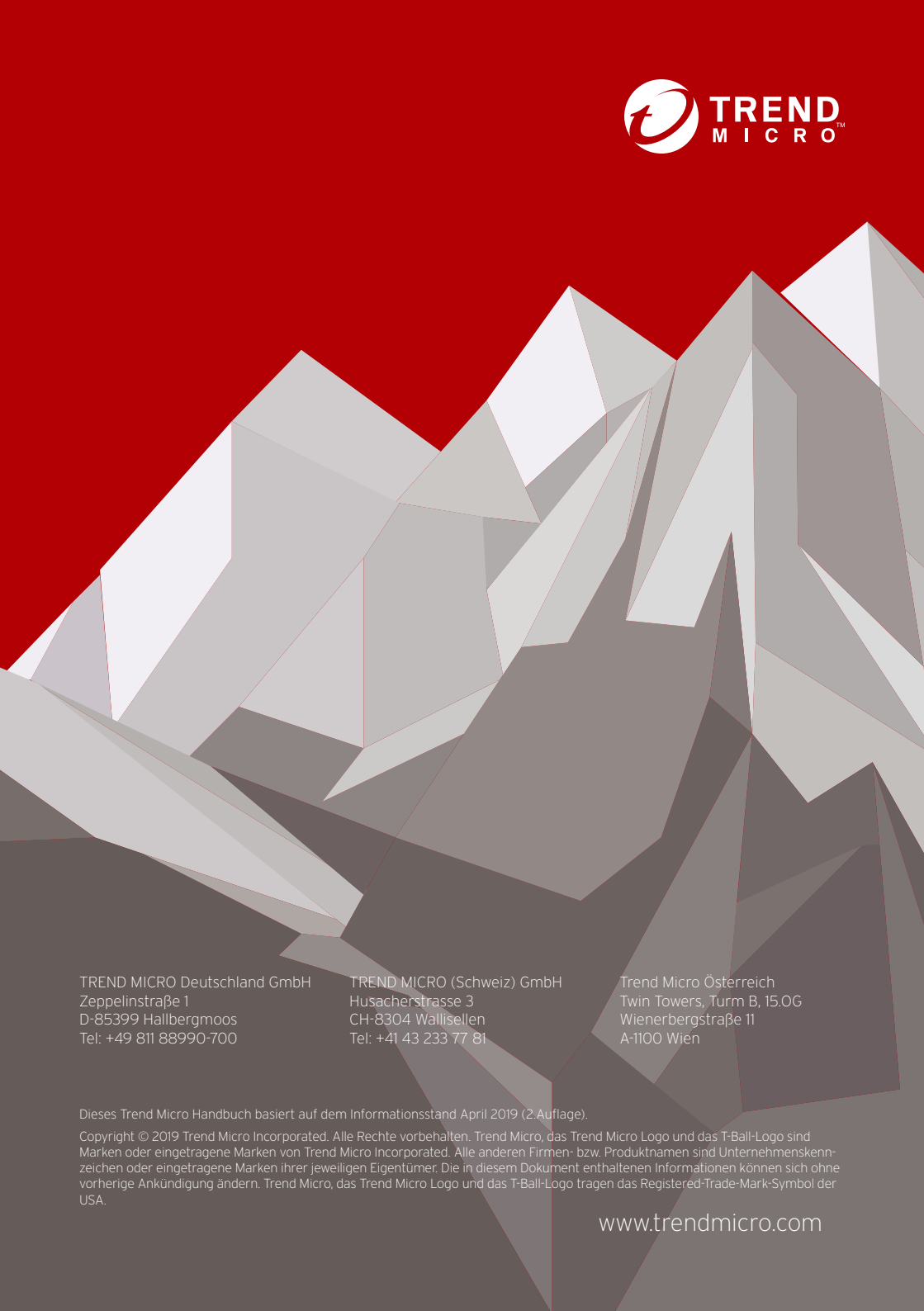
Arrow ECS Internet Security AG
sales@arrowecs.ch

Infinigate (Schweiz) AG
verkauf@infinigate.ch

Ingram Micro GmbH Schweiz
trendmicro@ingrammicro.ch

Dieses Trend Micro Handbuch basiert auf dem Informationsstand April 2019 (2.Auflage).

Notizen



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

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

Trend Micro Österreich
Twin Towers, Turm B, 15.OG
Wienerbergstraße 11
A-1100 Wien

Dieses Trend Micro Handbuch basiert auf dem Informationsstand April 2019 (2.Auflage).

www.trendmicro.com