Trend Micro

ZENTRALE ÜBERSICHT UND KONTROLLE

Bietet der Trend Micro™ Control Manager™ für On-Premise-Installationen und Trend Micro™ Apex Central™ für SaaS (Software-as-a-Service)

In der heutigen hochentwickelten Bedrohungslandschaft nutzen fortgeschrittene Angriffe mehrere Bedrohungsvektoren, die Benutzer-Endgeräte, Server, Netzwerke, Web und Email betreffen. Um den bestmöglichen Schutz für die eigene IT zu gewährleisten, benötigen Unternehmen eine Übersicht über mehrere Sicherheitsschichten hinweg. Und mit dem Wechsel zu Cloud-basierten Bereitstellungsmodellen müssen die Verantwortlichen darüber hinaus die Sicherheit überall in lokalen, Cloud- und hybriden Umgebungen verwalten.

Ein einheitliches Sicherheitsmanagement hilft dabei, die IT-Silos zu durchbrechen, die häufig verschiedene Schutzschichten und Bereitstellungsmodelle voneinander trennen. Diese Art des zentralen Ansatzes verbessert die Übersicht, verringert die Komplexität und eliminiert redundante und immer wiederkehrende Aufgaben der Sicherheitsadministration – all dies trägt zum besseren Schutz des Unternehmens bei, und macht das Leben leichter.

Die zentrale Übersichts- und Managementlösung liefert eine einzige, integrierte Schnittstelle für das Management, Monitoring und Reporting über mehrere Sicherheitsschichten hinweg – als SaaS-Lösung durch Apex Central™ als Service, als On-Premise-Lösung durch Trend Micro™ Control Manager™. Anpassbare Dashboards ermöglichen die Übersicht und situationsbezogene Aufmerksamkeit, sodass Verantwortliche den Status schnell bewerten, Bedrohungen identifizieren und auf Vorfälle reagieren können. Benutzerzentrierte Ansichten (basierend auf der Active Directory-Integration) erlauben es, das Geschehen an allen Endgeräten, den Nutzern gehörenden Geräten sowie deren Email- und Webverkehr zu analysieren und aufgrund dessen den Status der Richtlinien zu überprüfen und Änderungen an allen, die Nutzer betreffenden Bereichen vorzunehmen.

Und sollte es dennoch zu einem Vorfall kommen, so haben Unternehmen die komplette Übersicht über ihre Umgebung und können nachverfolgen, wie sich die Bedrohungen ausgebreitet haben. Je besser die Sicherheitsverantwortlichen einen Vorfall verstehen, desto wahrscheinlicher können sie verhindern, dass dies nochmals passiert. Direkte Links zur Trend Micro™ Threat Connect™-Datenbank bieten Zugang zu in der Praxis nutzbarem Wissen über Bedrohungen, aufgrund dessen die komplexen Beziehungen zwischen Malware-Instanzen, den Autoren und Verteilungsmethoden untersucht werden können.

TREND MICRO-PRODUKTE, DIE DER CONTROL MANAGER UNTERSTÜTZT

- **Hybrid Cloud Security**
- Deep Security
- **Network Defense**
- Deep Discovery Inspector
- Deep Discovery Director
- Deep Discovery Analyzer
- Deep Discovery Email Inspector
- **User Protection**
- ApexOne™
- Worry-Free™ Business Security
- Endpoint Encryption
- Endpoint Application Control
- Endpoint Sensor
- Security for Mac
- Vulnerability Protection
- Data Loss Prevention
- Mobile Security
- InterScan™ Messaging Security Virtual Appliance
- InterScan™ Messaging Security
- ScanMail™ for IBM Domino
- ScanMail™ forMicrosoft Exchange
- Hosted Email Security
- Trend Micro Email Security Advanced
- Portal Protect
- InterScan™ Web Security Suite
- InterScan™ Web Security Virtual Appliance
- InterScan Web Securtiy as a Service
- Cloud App Security
- OfficeScan
- Smart Protection Server
- Virtual Mobile Infrastructure

TREND MICRO™-PRODUKTE, DIE APEX CENTRAL™ AS A SERVICE UNTERSTÜTZT

- **Apex One™ as a Service als:**
  - *Apex One™ as a Service:* Application Control
  - *Apex One™ as a Service:* Vulnerability Protection
  - *Apex One™ as a Service:* DLP (data loss prevention)
- **Apex One™ as a Service**
- **Apex One™ (Mac) as a Service**
- **Apex One™ as a Service: Endpoint Sensor**
- **Apex One™ (Mac) as a Service: Endpoint Sensor**

HAUPTVORTEILE

Einfache, unternehmensweite Übersicht

- Gleiche Funktionalität bei SaaS (Apex Central™ as-a-Service) und On-Premise (Control Manager).
- Kontinuierliches Monitoring und schnelles Verstehen der Sicherheitslage im Unternehmen, Erkennen von Bedrohungen und Reaktion auf Vorfälle aufgrund einer sofortigen Einschätzung der Situation in der gesamten Umgebung. Gelingt es einem Angriff dennoch ins Unternehmen einzudringen, so lässt sich untersuchen, wohin er sich ausgebreitet hat.
- Eine intuitive, anpassbare Schnittstelle ermöglicht die Übersicht über alle Sicherheitsschichten sowie Nutzer und erlaubt es, über Drill-Down zu den gewünschten spezifischen Informationen weiter in die Tiefe zu navigieren.
- Sicherheits-Dashboards sind für sofortige Prüfungen ausgelegt, und Administratoren können kritische Bedrohungsarten, Benutzer oder Endpunkte priorisieren, damit die Maßnahmen zuerst die dringendsten Problemen in Angriff nehmen.
- Konfigurierbare Dashboards und Reports, Ad hoc-Abfragen und Benachrichtigungen liefern umsetzbare Informationen, die für die Gewährleistung des Schutzes und der Compliance erforderlich sind.
- Einfache Integration ins Security Operations Center (SOC) über die Einbindung in führende SIEM-Lösungen.
- Vordefinierte Reporting-Vorlagen und anpassbares SQL-Reporting vereinfachen die Compliance mit internen IT Audit-Anforderungen und Vorschriften.

CONNECTED THREAT DEFENSE FÜR HÖHEREN SCHUTZ

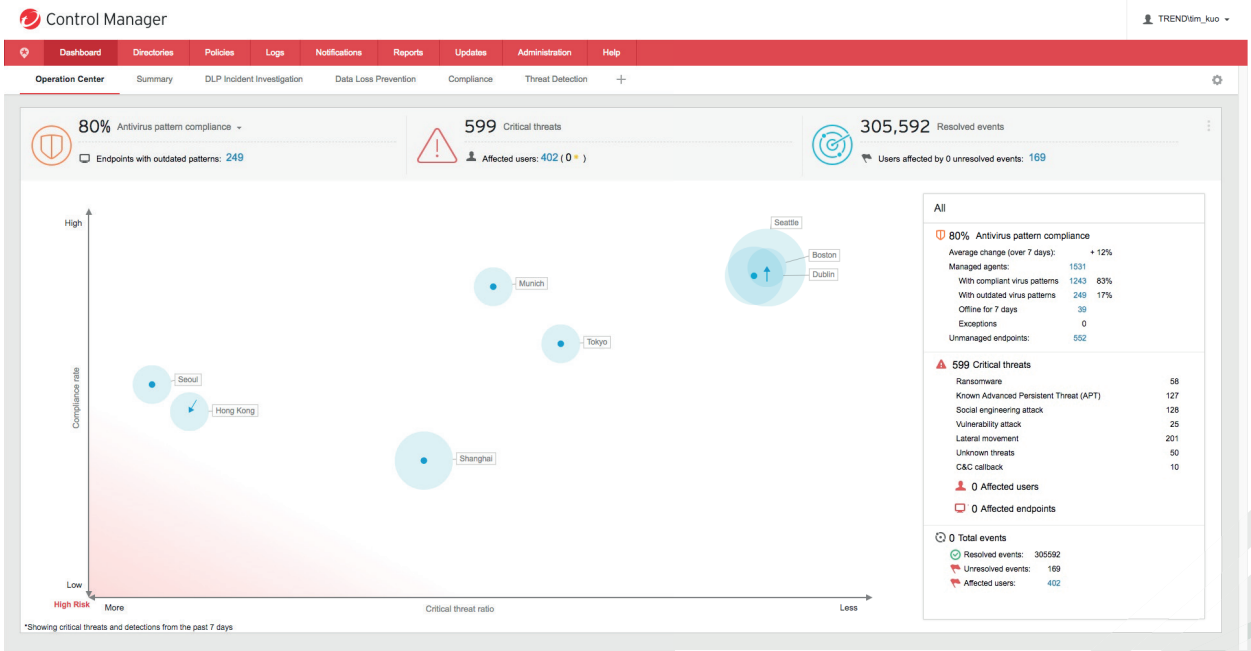
(nur für Trend Micro Control Manager verfügbar)

Überlegene Bedrohungsanalyse und -aufklärung

- Umfassende Reaktionen auf Bedrohungen und deren Untersuchung ermöglichen einen zeitlichen Rückblick, um festzustellen, wo sich eine Bedrohung in der Organisation ausgebreitet hat und um den vollständigen Kontext, die Zeitachse und das Ausmaß des Angriffs zu ermitteln, so dass eine schnelle Antwort auf eine Kompromittierung erfolgen kann.
- Direkte Verbindungen zur Trend Micro Threat Connect™-Datenbank bieten Zugang zu in der Praxis umsetzbarem Bedrohungswissen. Dazu gehören korrelierte Bedrohungsdaten, die charakteristische Verhaltensweisen, etwa Netzwerkaktivitäten und Systemänderungen, beschreiben sowie auch globale, System- und branchenspezifische Auswirkungen.
- Die Trend Micro-Wissensdatenbank liefert auch Vorschläge für Abhilfemaßnahmen und Prävention.

Nutzerbasierte Übersicht

- Mehrschichtige Übersicht, unabhängig davon, ob die Sicherheit On-Premise oder in der Cloud bereit gestellt wird, liefert eine zentrale Sicht auf nur einer Konsole.
- Eine straffere Sicherheitsadministration ermöglicht es, Bedrohungs- und Datenschutz für Endpoints, Server, Netzwerk, Mobilität, Messaging, Collaboration und Web über eine einzige konsolidierte Schnittstelle zu steuern.
- Die Integration mit Active Directory vereinfacht den Einsatz von Dashboards mit korrelierten Daten basierend auf der AD-Site oder -Abteilung.
- Nutzerzentrische Ansichten vereinfachen das Sicherheitsmanagement über alle Gerätearten hinweg, sodass Administratoren den Status der Richtlinien für alle Endpoints eines bestimmten Nutzers bereitstellen und überprüfen können, unabhängig davon, ob es sich um Desktop- oder mobile Endgeräte handelt.



Dashboards für den Sicherheitsbetrieb setzen auf innovative Heat Maps (auf Basis von Active Directory-Sites oder -Abteilungen), um Compliance- und kritische Bedrohungen anzuzeigen, die für IT- und Sicherheitsadministratoren am wichtigsten sind.

SYSTEMANFORDERUNGEN:

SERVER HARDWARE ANFORDERUNGEN
Ô Prozessor: Minimum 2.3 GHz Intel™ Core™ i5 oder kompatible CPU; AMD™ 64 Prozessor; Intel 64 Prozessor
Ô Memory: 8 GB RAM minimum
Ô Verfügbarer Festplattenspeicher: 80 GB minimum (SAS Festplatten-Typus)

SOFTWARE ANFORDERUNGEN
Betriebssystem
Ô Microsoft™ Windows™ Server 2008 Standard/Enterprise Edition mit SP2
Ô Windows Server 2008 (R2), Standard/Enterprise/Datacenter Edition mit SP1
Ô Windows Server 2012 Standard/Datacenter Edition (64-Bit)
Ô Windows Server 2012 (R2) Standard/Datacenter Edition (64-Bit)
Ô Windows Server 2016 Standard/Datacenter Edition (64-bit)
Webkonsole
Ô Prozessor: 300 Mhz Intel™ Pentium™ Prozessor oder äquivalent
Ô RAM: 128 MB minimum
Ô Verfügbarer Festplattenspeicher: 30 MB minimum
Ô Brower: Microsoft Internet Explorer™ 11, Microsoft Edge™, Google Chrome (Achtung: Bei der Nutzung des Internets)
Ô Weitere: Monitor mit 1366 x 768-Auflösung bei 256 Farben oder mehr | Adobe™ Flash™ 8 oder höher
Datenbanksoftware
Ô SQL Server 2008 Express mit SP4
Ô SQL Server 2008 (R2) Standard/Enterprise mit SP3
Ô SQL Server 2008 Standard/Enterprise mit SP4
Ô SQL Server 2012 Express mit SP3
Ô SQL Server 2012 Standard/Enterprise mit SP3
Ô SQL Server 2014 Express mit SP2
Ô SQL Server 2014 Standard/Enterprise mit SP2
Ô SQL Server 2016 Express mit/ohne SP1
Ô SQL Server 2016 Standard/Enterprise mit/ohne SP1
Virtualisierungsunterstützung
Control Manager liefert Unterstützung für virtuelle Plattformen, die von dem installierten Betriebssystem unterstützt werden.

Hauptvorteile

- Verbessert die Transparenz mit innovativen Heat Maps in Dashboards für den Sicherheitsbetrieb.
- Vereinfacht die Administration mit einer zentralen Konsole für Sicherheit und Datenrichtlinien.
- Erhöht den Schutz der Daten durch integriertes DLP mit wiederverwendbaren Richtlinienvorlagen über die gesamte IT-Infrastruktur hinweg.
- Reduziert das Risiko mit konsolidierten Updates und Sicherheitsbenachrichtigungen und Connected Threat Defense, um Informationen zwischen den Sicherheitsschichten auszutauschen.
- Senkt durch Zeitersparnis die Kosten für das Sicherheitsmanagement und reduziert die IT-Arbeitslast.

TREND MICRO™

Securing Your Connected World