Trend Micro

CONTROL MANAGER™

Zentrale Transparenz und Richtlinienverwaltung für Datensicherheit und Schutz vor Bedrohungen

In der komplexen Bedrohungslandschaft von heute nutzen ausgeklügelte Angriffe mehrere Bedrohungsvektoren, die sich über Benutzerendpunkte, Server, Netzwerke, das Internet und E-Mail-Anwendungen hinweg erstrecken. Um Ihrer Organisation bestmöglichen Schutz zu bieten, benötigen Sie Transparenz auf mehreren Sicherheitsebenen. Mit dem Übergang zu cloudbasierten IT-Bereitstellungsmodellen muss Sicherheit auch für lokale, cloudbasierte und hybride Installationsumgebungen verwaltet werden.

Eine einheitliche Sicherheitsverwaltung hilft Ihnen, IT-Silos, in denen getrennte Schutzschichten und Bereitstellungsmodelle vorherrschen, miteinander zu verbinden. Dieser zentralisierte Ansatz verbessert die Transparenz, senkt den Verwaltungsaufwand und beseitigt unnötige, sich wiederholende Aufgaben in der Sicherheitsverwaltung. Ihr Unternehmen profitiert damit von mehr Sicherheit und einer erheblichen Erleichterung alltäglicher Aufgaben.

Trend Micro Control Manager™, die Lösung für zentralisierte Verwaltung und Transparenz, bietet eine einzige, integrierte Schnittstelle für Management, Überwachung und Berichterstattung über mehrere Sicherheitsebenen sowie für SaaS- und lokale Bereitstellungsmodelle. Anpassbare Dashboards bieten die erforderliche Transparenz und situationsbezogene Analyse, durch die Sie schnell einen Überblick über Ihre Sicherheitsprofile erhalten, Bedrohungen sofort identifizieren und direkt auf Vorfälle reagieren können. Benutzerbasierte Transparenz (basierend auf Active-Directory-Integration) ermöglicht es Ihnen zu sehen, was auf allen Endpunkten Ihrer Benutzer sowie bei deren E-Mail- und Web-Datenverkehr geschieht. So können Sie den Richtlinienstatus überprüfen und Anwenderaktionen gegebenenfalls korrigieren.

Falls Sie einen Bedrohungsausbruch erleben, haben Sie vollständige Transparenz in Ihrer Umgebung, um zu verfolgen, wie sich die Bedrohungen ausbreiten. Mit einem besseren Verständnis von Sicherheitsereignissen können Sie eher verhindern, dass diese erneut auftreten. Direkte Verknüpfungen zur Trend Micro Threat Connect Datenbank liefern praktisch nutzbare Erkenntnisse zu Bedrohungen, die Aufschluss über die komplexen Beziehungen zwischen Malware-Instanzen, -Entwicklern und -Verbreitungsmethoden geben.

Von Control Manager unterstützte Trend Micro Produkte

HYBRID CLOUD-SICHERHEIT

- Deep Security

NETWORK DEFENSE

- Deep Discovery Inspector
- Deep Discovery Analyzer
- Deep Discovery Email Inspector

BENUTZERSCHUTZ

- OfficeScan™
- Worry-Free™ Business Security
- Endpoint Encryption
- Endpoint Application Control
- Endpoint Sensor
- Security for Mac
- Vulnerability Protection
- Data Loss Prevention
- Mobile Security
- InterScan™ Messaging Security
- ScanMail™
- Hosted Email Security
- PortalProtect
- InterScan™ Web Security
- Cloud App Security

HAUPTVORTEILE

Einfache Transparenz auf Unternehmensebene

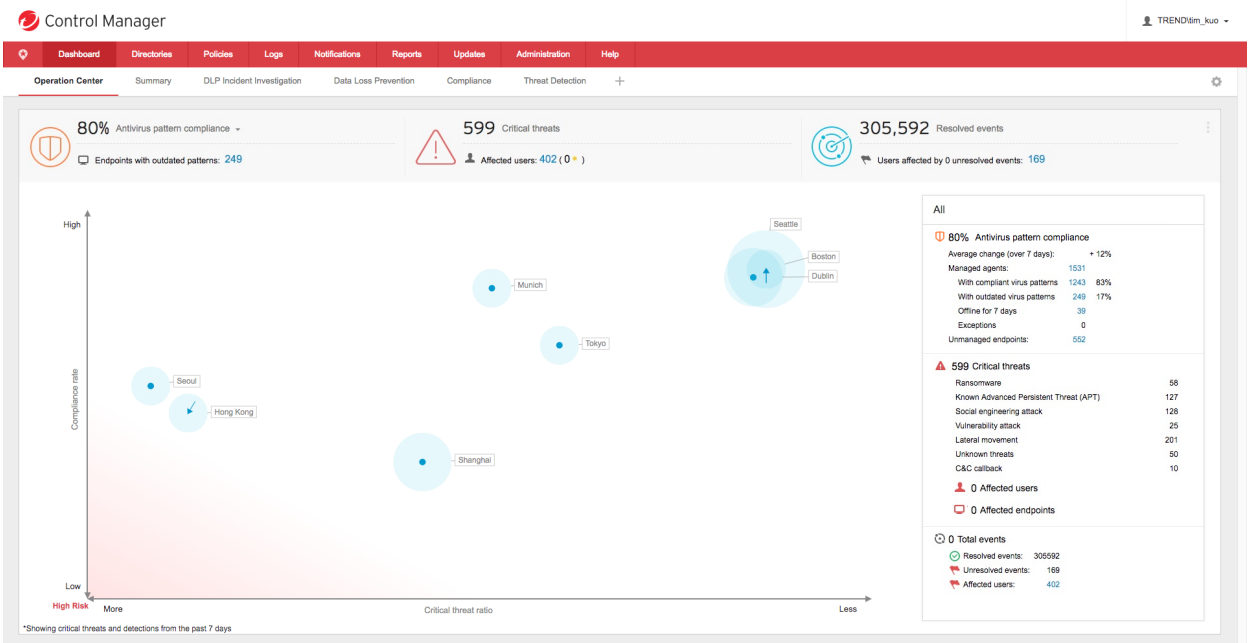
- Kontinuierliche Überwachung, schneller Überblick über Ihr Sicherheitsprofil, schnelle Identifikation von Bedrohungen sowie schnelle Reaktion auf Vorfälle dank minutengenauer, situationsbezogener Erkennung in Ihrer gesamten Umgebung. Sollte sich doch ein Angriff seinen Weg in Ihr System gebahnt haben, können Sie untersuchen, wohin er sich bereits ausgebreitet hat.
- Die intuitive, anpassbare Oberfläche sorgt für umfassende Transparenz aller Sicherheitsebenen und Anwender. Darüber hinaus ermöglicht sie Ihnen die detaillierte Anzeige relevanter Informationen.
- Sicherheits-Dashboards ermöglichen Administratoren eine sofortige Auswahl und Priorisierung kritischer Bedrohungsarten, kritischer Benutzer oder kritischer Endpunkte. So können sie die drängendsten Probleme zuerst behandeln.
- Konfigurierbare Dashboards und Berichte, Sofortabfragen und Warnmeldungen liefern Ihnen die erforderlichen Informationen, um umfassenden Schutz und die Einhaltung von Richtlinien sicherzustellen.
- Die Einbindung in Ihr Security Operations Center (SOC) ist dank Integration in führende SIEM-Lösungen ganz einfach erledigt.
- Vordefinierte Berichtsvorlagen und anpassbare SQL-Berichterstattung erleichtern die Compliance mit den Anforderungen interner IT-Audits und Regularien.

Connected Threat Defense für besseren Schutz

- Sicherheitsmanagement und -analyse auf mehreren Schutzebenen integrieren – kritisch für den Schutz vor komplexen Bedrohungen, die mehrere Bedrohungsvektoren ausnutzen
- Einheitliche Richtliniendurchsetzung über eine zentrale Konsole, um Bedrohungsschutz und Datensicherheit für verschiedene geschützte Punkte zu konfigurieren und zu verwalten: Endpunkte, mobile Geräte, Messaging, Kollaborationslösungen, das Internet, die Cloud und Rechenzentren; zusätzlich zu Breach Detection in Netzwerken
- Connected Threat Defense ermöglicht es Control Manager, verdächtige Objekte abzurufen, die möglicherweise über eine beliebige Anzahl lokaler Bedrohungsvektoren eingegangen sind, und bietet anderen lokalen Lösungen schnelle Reaktionsaktualisierungen. Dies ermöglicht schnelleren Schutz und verlangsamt die Ausbreitung von Malware/ Bedrohungen.
- Umfassende Reaktion auf Bedrohungen und Überprüfung ermöglichen eine frühzeitige Analyse der organisationsweiten Bedrohungsverbreitung und geben Aufschluss über den vollständigen Kontext, die Zeitspanne und das Ausmaß des Angriffs. So können Sie schnell auf Kompromittierungen reagieren.
- Direkte Verknüpfungen zu unserer Threat Connect Datenbank bieten Ihnen Zugriff auf praktisch nutzbare Erkenntnisse zu Bedrohungen. Dies umfasst wertvolle, korrelierte Bedrohungsdaten, die globale, system- und branchenspezifische Auswirkungen sowie charakteristisches Verhalten wie Netzwerkaktivitäten und Systemveränderungen beschreiben.
- In der Trend Micro Knowledge Base finden Sie Vorschläge zur Bedrohungsbeseitigung und -vermeidung.

Benutzerbasierte Transparenz

- Transparenz auf mehreren Ebenen, egal ob Sicherheit für lokale Installationen oder in der Cloud bereitgestellt wird. Mit einer zentralisierten Ansicht müssen Sie somit nicht von einer Konsole zur anderen wechseln.
- Eine vereinfachte Sicherheitsadministration ermöglicht die Verwaltung von Bedrohungsschutz und Datensicherheit für Endpunkte, Server, Netzwerke, mobile Geräte, Messaging, Kollaborationslösungen und das Internet über eine einzige konsolidierte Konsole.
- Dank Active-Directory-Integration werden Dashboards mit korrelierten Daten basierend auf der AD-Website oder der Abteilung vereinfacht.
- Über die anwenderzentrische Ansicht können Sie alle Gerätetypen einfach verwalten, sodass Sie Richtlinien für alle Endpunkte eines bestimmten Anwenders – egal ob Desktop oder Mobilgerät – verteilen und deren Status überprüfen können.



Dashboards für Sicherheitsfunktionen nutzen innovative Heatmaps (basierend auf Active-Directory-Websites oder Abteilungen), um Compliance und kritische Bedrohungen anzuzeigen, die für IT- und Sicherheitsadministratoren am wichtigsten sind.

SYSTEMVORAUSSETZUNGEN

SERVER-HARDWAREVORAUSSETZUNGEN
Ô Prozessor: Mindestens 2,3 GHz Intel™ Core™ i5 oder kompatible CPU; AMD™ 64-Prozessor; Intel 64-Prozessor
Ô Arbeitsspeicher: mindestens 8 GB RAM
Ô Festplattenspeicher: mindestens 80 GB (SAS-Festplattentyp)

SOFTWAREVORAUSSETZUNGEN
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)
Web-Konsole
Ô Prozessor: Intel™ Pentium™-Prozessor mit 300 MHz oder gleichwertig
Ô RAM: mindestens 128 MB
Ô Festplattenspeicher: mindestens 30 MB
Ô Browser: Microsoft Internet Explorer™ 11, Microsoft Edge™, Google Chrome (Hinweis: Bei Verwendung von Internet Explorer oder Edge deaktivieren Sie bitte die „Kompatibilitätsansicht".)
Ô Sonstige: Monitor mit mindestens 1366x768 Pixeln bei 256 oder mehr Farben | 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
Unterstützung von Virtualisierung
Control Manager unterstützt virtuelle Plattformen, die vom installierten Betriebssystem unterstützt werden.

Hauptvorteile

- Erhöht die Transparenz dank Dashboards für Sicherheitsfunktionen mit innovativen Heatmaps
- Vereinfacht die Administration mit zentraler Konsole für Sicherheits- und Datenrichtlinien
- Verbessert den Datenschutz durch Verwaltung von integriertem DLP in der gesamten IT-Infrastruktur mit wiederverwendbaren Richtlinienvorlagen
- Reduziert das Sicherheitsrisiko durch konsolidierte Updates und Warnmeldungen sowie durch eine verknüpfte Bedrohungsabwehr, um Informationen mit anderen Sicherheitsebenen zu teilen
- Senkt die Kosten für die Sicherheitsverwaltung durch Zeitersparnis und geringeren IT-Aufwand

TREND MICRO™

Securing Your Journey to the Cloud