Trend Micro™

MOBILE SECURITY FÜR UNTERNEHMEN

Transparenz und Kontrolle über mobile Geräte, Anwendungen und Daten gewinnen

Der Einsatz von Smartphones in Unternehmen hat massiv zugenommen, seit Mitarbeiter den Nutzen dieser Technologie auch für geschäftliche Zwecke erkannt haben. Nun fordern sie Unterstützung für eine Vielzahl an Einsatzmöglichkeiten. Unternehmen sehen sich angesichts der immer größer werdenden mobilen Belegschaft mit enormen Herausforderungen konfrontiert. Sie müssen ein Gleichgewicht zwischen der Förderung der Mitarbeiterproduktivität durch die Nutzung von Mobilgeräten und dem Schutz ihrer vertraulichen Unternehmensdaten finden. Im Idealfall soll beides gewährleistet werden, jedoch ohne dafür eine Vielzahl an neuen Anwendungen installieren und finanzieren zu müssen.

Trend Micro™ Mobile Security ist ein integraler Bestandteil der Trend Micro Complete User Protection Lösung. Über eine einzelne, integrierte Konsole erhalten Sie völlige Transparenz und Kontrolle über mobile Geräte, Apps und Daten. Die Lösung bringt Mitarbeiterproduktivität und Datenschutz in Einklang.

Mobile Security bietet:

1. Mobile Device Management (MDM)
2. Verwaltung mobiler Anwendungen
3. Reputationsprüfung mobiler Anwendungen
4. Virenschutz für Geräte (Android)

Als wichtiger Bestandteil einer umfassenden Sicherheitsstrategie sorgt Trend Micro Mobile Security in erheblichem Maß für eine Verringerung der Komplexität sowie eine Senkung der Kosten im Vergleich zu Standalone-Lösungen zur Sicherheit und Verwaltung mobiler Geräte, für die neue Verwaltungsinfrastrukturen erforderlich sind.

Im Gegensatz zu anderen Lösungen integriert Trend Micro Mobile Security verschiedene Ebenen des Datenschutzes zur Absicherung Ihrer Unternehmensdaten, ganz egal, wo sich diese gerade befinden. Verschlüsselung, Sperren und Löschen von Daten per Fernzugriff, Kennwortdurchsetzung und andere Tools greifen optimal mit Gerätesicherheit und App-Verwaltung ineinander, damit Ihre Daten stets sicher sind.

Geschützte Punkte

Unterstützt Smartphones und Tablets mit folgenden Betriebssystemen:

- iOS
- Android
- Windows Phone

Datensicherheit und Schutz vor Bedrohungen

- Virenschutz
- Durchsetzung von Datenverschlüsselung
- Kennwortdurchsetzung
- Sperren und Löschen von Daten per Fernzugriff
- Selektive Datenlöschung
- Mobile Device Management (MDM)
- Verwaltung mobiler Anwendungen (MAM)
- Reputationsprüfung mobiler Apps
- Web Reputation

VORTEILE

Weniger Kosten und Verwaltungsaufwand

- Vereinfachte Verwaltung von mobiler Sicherheit, MDM, Apps und Datenschutz in einer einzigen Lösung
- Einfachere Installation durch die mögliche Nutzung des Trend Micro Cloud Communication Servers, einem optionalen cloudbasierten Dienst, der Kommunikation automatisiert und die Komplexität der Umgebung reduziert
- Weniger Betriebskosten dank zentraler Transparenz und Kontrolle aller Endpunkt-Sicherheitslösungen
- Höhere Produktivität und Flexibilität, da eine Vielzahl von Plattformen unterstützt wird

Mehr Transparenz und Kontrolle

- IT-Abteilung kann mobile Geräte, Apps und Daten über eine einzelne Konsole nachverfolgen, überwachen und verwalten
- Liefert Daten zu Anzahl, Art und Konfiguration der Geräte, die auf Unternehmensressourcen zugreifen, auch wenn sie nicht am Netzwerk angemeldet sind
- Ermöglicht die zentrale Erstellung und Durchsetzung von Richtlinien auf einzelnen oder mehreren Servern
- Unterstützt das Konzept unserer Complete User Protection Strategie, da durch die Integration in die Trend Micro Control Manager Konsole zentrale Richtlinien und Verwaltungsfunktionen auch für weitere Trend Micro Lösungen wie den OfficeScan™ Endpunktschutz ermöglicht werden

Bringt Mitarbeiterproduktivität und Risiken in die Balance

- Bietet führenden Virenschutz und gewährleistet optimale Gerätekonfigurationen, um das Malwarerisiko zu senken
- Schützt Unternehmensdaten durch Sperren und Löschen von Daten per Fernzugriff, einschließlich der selektiven Löschung von Daten
- Schirmt persönliche Daten mittels Kennwort- und Richtliniendurchsetzung vor unbefugtem Zugriff und unangemessener Nutzung ab
- Erlaubt es der IT-Abteilung, die Nutzung riskanter Apps auf Basis minutengenauer Daten des cloudbasierten Trend Micro Mobile Application Reputation Service zu blockieren

WICHTIGE FUNKTIONEN

Zentrale Verwaltung

- Vereinfachte Administration mit dem Trend Micro Control Manager, der zentrale Richtlinienverwaltung zum Schutz vor Bedrohungen und Datenverlust auf mehreren Ebenen der IT-Infrastruktur bietet
- Bietet eine zentrale Übersicht über alle Anwender innerhalb des Unternehmen, ganz egal, ob Sie einen Desktop oder ein Mobilgerät nutzen, und zeigt Bedrohungen im zeitlichen Verlauf an, um komplexe Bedrohungen zu identifizieren, die Anwender möglicherweise über mehrere Angriffswege ins Visier nehmen
- Setzt Richtlinien konsequenter durch, da auf einen Klick die Datenschutzrichtlinien auf Endpunkt-, Messaging- und Gateway-Lösungen verteilt werden
- Vereinfachte Geräteanmeldung mittels Weblink, QR-Code oder iTunes Download
- Bietet sofortige Zusammenfassungen bezüglich Einhaltung von Compliance-Richtlinien, Bestand, Schutz und Sicherheitsstatus aller Geräte, auch wenn sie nicht am Netzwerk angemeldet sind
- Liefert transparente Angaben zu Anzahl, Art und Konfiguration der Geräte, die auf Unternehmensressourcen zugreifen

Sicherheit mobiler Geräte

- Profitiert vom führenden Malware-Schutz von Trend Micro basierend auf den cloudbasierten Informationen über Bedrohungen des Trend Micro Smart Protection Network™
- Erkennt und blockiert bösartige Anwendungen und Dateien
- Blockiert bösartige Internetinhalte und Webseiten mit Hilfe der Web Reputation Services
- Erkennt Angriffe über Netzwerkanwendungen, -ports und -dienste auf dem Gerät mittels Firewall und IDS
- Überwacht, blockiert und protokolliert ein- und ausgehende Anrufe und Textnachrichten (SMS/MMS) anhand von Benutzerrichtlinien

Datensicherheit

- Schützt Unternehmensdaten durch Sperren und Löschen per Fernzugriff, einschließlich der selektiven Löschung von Daten, bzw. durch Geräteortung bei Diebstahl oder Verlust des Mobiltelefons
- Setzt Datenverschlüsselung und Compliance durch
- Benachrichtigt die IT-Abteilung bei Jailbreaks oder unverschlüsselten Geräten
- Ermöglicht es dem IT-Administrator, verschiedene Mobilgerätefunktionen wie Kamera, Bluetooth®, 3G/4G und SD-Kartenleser zu sperren bzw. zuzulassen
- Zeigt der IT-Abteilung an, welche Geräte unangemeldet auf das Unternehmensnetzwerk zugreifen
- Ermöglicht der IT-Abteilung die Verteilung, Verwaltung und Konfiguration von KNOX-Containern auf Samsung KNOX-kompatiblen Geräten

Verwaltung mobiler Anwendungen

- Verhindert durch Blacklists und Whitelists, dass Geräte im Netzwerk unbefugte, riskante Anwendungen ausführen
- Verwaltet den Bestand und erstellt Reports, um die auf Geräten, von Gruppen und im Unternehmen verwendeten Apps transparenter darzustellen
- Ermöglicht dem IT-Administrator mit dem neuen Category App Management, bestimmte Arten von Apps je nach Kategorie zu verwalten und sogar zu sperren
- Installiert Anwendungen auf den Geräten von Endanwendern über die Corporate App Store Funktion, um so die Verwendung optionaler oder nutzungspflichtiger Apps zu beschleunigen. Volumenlizenzabonnements sind bereits in den App Store integriert.
- Ermittelt und blockiert Apps, die ein Sicherheits- oder Datenschutzrisiko bergen, und korreliert hierfür die Daten installierter Apps mit dem Trend Micro Mobile Application Reputation Service
- Ermöglicht die Nachverfolgung, Verwaltung und Installation von Volumenlizenzprogrammen auf iOS-Geräten

Mobile Device Management

- Ermöglicht der IT-Abteilung, Geräte mit Unternehmensnetzwerkfunktionen wie z. B. VPN, Exchange ActiveSync und Wi-Fi® per Fernzugriff anzumelden, bereitzustellen und zu deaktivieren
- Erleichtert die Verteilung von Apple TV und AirPrint Services für iOS-Anwender
- Unterstützt die Geräteortung und die Bestandsverwaltung, um private bzw. Firmengeräte zu schützen und nachzuverfolgen, auch wenn sie nicht am Netzwerk angemeldet sind
- Ermöglicht die konsequente Durchsetzung von geräteübergreifenden bzw. gruppenbezogenen Sicherheits- und Verwaltungsrichtlinien
- Bietet der IT-Abteilung die Möglichkeit, befugte Geräte mittels International Mobile Equipment Identity-Nummer (IMEI), WLAN- oder Mac-Adresse zu überwachen und relevante Richtlinien zu verteilen
- Ermöglicht der IT-Abteilung das Einschränken von Telefonfunktionen wie dem Bearbeiten von Konteninformationen, Roaming, AirDrop, mobile Datenkontrolle, Bildschirmsperre, Verbindungsherstellung, Find My Friends etc.

Entscheidende Vorteile

- Bringt neue Möglichkeiten für Mitarbeiter mit der Kontrolle durch die IT in Balance
- Senkt Installations-, IT- und Betriebskosten, da MDM, mobile Sicherheit, Anwendungsverwaltung und Datenschutz in einer einzigen Lösung kombiniert werden
- Bietet Absicherung durch Anti-Malware, Firewall und Schutz vor Eindringlingen (IDS) für eine Vielzahl von Geräten auf Basis der globalen Bedrohungsintelligenz von Trend Micro
- Schützt Daten beim Transfer durch Verschlüsselung, Sperren und Löschen per Fernzugriff und Funktionssperre
- Verbessert die Produktivität, da Mitarbeiter jederzeit und überall mit einem Gerät ihrer Wahl arbeiten können

Complete User Protection

Trend Micro Mobile Security ist eine Komponente der Trend Micro Complete User Protection, einer mehrschichtigen Lösung, welche die größte Bandbreite an miteinander kommunizierenden Schutzmechanismen vor Bedrohungen und Datenverlust für Endpunkte, E-Mail- und Kollaborationslösungen, Internetaktivitäten und mobile Geräte bietet.

BENUTZERLIZENZEN

Trend Micro Mobile Security wird pro Benutzer lizenziert. Ein Benutzer kann also mehrere Geräte haben, die aber nur als eine Lizenz gelten. Bei anderen Anbietern für Mobile Device Management erfolgt die Lizenzierung pro Gerät. Das belastet die IT-Abteilung, da sie den Bestand verwalten und voraussehen muss, welche weiteren Geräte der Mitarbeiter erwirbt.

SYSTEMVORAUSSETZUNGEN UND SUPPORT FÜR DIE VERSION 9.0 SP2

KOMPONENTE	VORAUSSETZUNGEN
iOS-MOBILGERÄTE	• iOS 4.3 oder höher • mindestens 3 MB Speicherplatz • 4 MB Arbeitsspeicher empfohlen
ANDROID-MOBILGERÄTE	• Android 2.1 oder höher • mindestens 8 MB Speicherplatz • 10 MB Arbeitsspeicher
WINDOWS PHONE-MOBILGERÄTE	• Windows Phone 8.0 • Windows Phone 8.1
MOBILE SECURITY MANAGEMENT SERVER	**Hardware** • 1 GHz Intel™ Pentium™ oder vergleichbarer Prozessor • mindestens 1 GB Arbeitsspeicher • mindestens 400 MB freier Festplattenspeicher • Bildschirm mit einer Auflösung von 800 x 600 und mindestens 256 Farben **Plattform** • Microsoft Windows Server 2003 Familie • Microsoft Windows Server 2003 R2 Familie • Microsoft Windows Server 2008 Familie • Microsoft Windows Server 2008 R2 Familie • Microsoft Windows Server 2012 Familie • Microsoft Windows Server 2012 R2 Familie **Empfohlene Plattform** • Windows Server 2003 R2 Enterprise Edition • Windows Server 2003 Enterprise Edition • Windows Server 2008 R2 Enterprise Edition • Windows Server 2008 Enterprise Edition SP1 • Windows Server 2008 Standard Edition • Windows Web Server 2008 Edition, SP
MOBILE SECURITY COMMUNICATION SERVER	**Hardware** • 1 GHz Intel™ Pentium™ oder vergleichbarer Prozessor • mindestens 1 GB Arbeitsspeicher • mindestens 40 MB freier Festplattenspeicher • Bildschirm mit einer Auflösung von 800 x 600 und mindestens 256 Farben **Plattform** • Microsoft Windows Server 2003 Familie • Microsoft Windows Server 2003 R2 Familie • Microsoft Windows Server 2008 Familie • Microsoft Windows Server 2008 R2 Familie • Microsoft Windows Server 2012 Familie • Microsoft Windows Server 2012 R2 Familie **Empfohlene Plattform** • Windows Server 2008 R2 Enterprise Edition • Windows Server 2008 Enterprise Edition SP1 • Windows Server 2003 R2 Enterprise Edition • Windows Server 2003 Enterprise Edition • Windows Server 2008 Standard Edition • Windows Web Server 2008 Edition, SP

SYSTEMVORAUSSETZUNGEN UND SUPPORT (Fortsetzung)

KOMPONENTE	VORAUSSETZUNGEN
MOBILE SECURITY EXCHANGE CONNECTOR	**Plattform** • Windows 2008 R2 (64 Bit) • Windows 2012 (64 Bit) • Windows Server 2012 R2 (64 Bit) **Hardware** • 1 GHz Intel™ Pentium™ oder vergleichbarer Prozessor • mindestens 1 GB Arbeitsspeicher • mindestens 200 MB freier Festplattenspeicher
SMS SENDER	• Android-Betriebssystem 2.1 oder höher
WEBSERVER FÜR COMMUNICATION SERVER	• Microsoft Internet Information Server (IIS) 6.0/7.0/7.5
SQL SERVER	• Microsoft SQL Server 2005/2008/2008 R2/2012/2005 Express/ 2008 Express/2008 R2 Express/2012 Express

> "Für unsere Kunden ist Mobile Device Management im Rahmen vieler größerer Geschäftschancen eine wesentliche Voraussetzung. Trend Micro Mobile Security bietet einen Gerätesicherheitsservice, der flexibel und stabil ist – genau wie der Kern unserer Firmenphilosophie. Außerdem ist die Lösung extrem benutzerfreundlich."

Timothy Maliyil
Gründer und CEO, AlertBoot

TREND MICRO™

Securing Your Journey to the Cloud