TeamViewer | ivanti

Solution Brief

Mobile Device Management mit TeamViewer

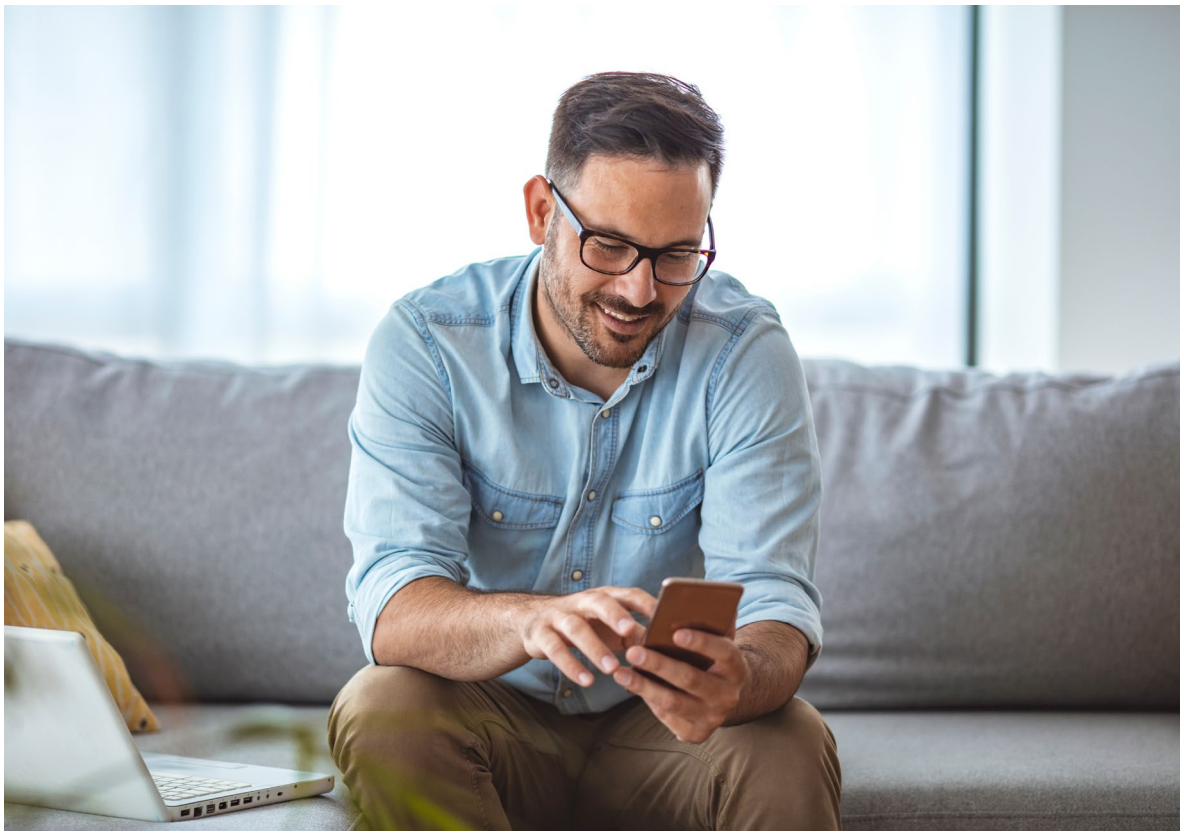
Sichern und verwalten Sie Ihr komplexes und ständig wachsendes Ökosystem aus mobilen Geräten mit TeamViewer.

Einleitung

Unternehmen ermöglichen flexibles Arbeiten, indem sie ihre Mitarbeitenden mehr und mehr mit mobilen Geräten ausstatten.

Durch die vermehrte Verwendung von Smartphones, Tablets und anderen mobilen Geräten ist es schwieriger geworden, diese Geräte zu tracken, zu verwalten, zu überwachen und zu warten, was das Risiko bei Verlust oder Diebstahl noch erhöht. Hinzu kommt, dass die weit verbreitete Nutzung unterschiedlicher mobiler Geräte für den Zugriff auf sensible Unternehmensdaten in unsicheren Netzwerken eine größere Angriffsfläche bietet.

Erfahren Sie, wie 360° Mobile Device Management (MDM) Ihnen hilft, rund um die Uhr den Überblick über Ihre mobilen Geräte zu behalten.



Herausforderungen für Unternehmen

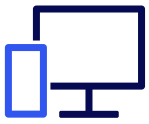
Eine dezentralisierte Belegschaft, die remote, von zu Hause aus oder unterwegs auf sensible Unternehmensdaten zugreift, stellt ein erhebliches Risiko für Unternehmen dar. Dies sind einige der häufigsten Gründe, warum der Einsatz einer MDM-Lösung für Unternehmen mit einer großen Anzahl an mobilen Geräten sinnvoll ist:

Datensicherheit
Mobile Geräte, die auf sensible Unternehmensdaten zugreifen, sollten durch Maßnahmen wie, durch Maßnahmen wie DatenVverschlüsselung, Mindestkennwortanforderungen für Passwörter und Anwendungsbeschränkungen ordnungsgemäß gesichert werdensind.

Compliance
Unternehmen in bestimmten , die in bestimmten Branchen tätig sind, sindmüssen an gesetzliche Vorschriften gebunden, die diefür die Nutzung von mobilern GGeräten einhaltenregeln.

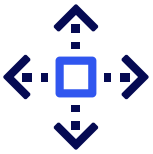
Produktivität der Nutzenden
Mobile Geräte sind zwar äußerst nützlich und helfen den MitarbeiternMitarbeitenden dabei, flexibel und reaktionsfähig schnell zu handelnbleiben, doch sie können jedoch auch eine Ablenkung darstellen. MDM-Lösungen bieten Funktionen wie App Management und das Filtern von Inhalten und können so Unternehmen bei der Verwaltung mobiler Geräte am am Arbeitsplatz unterstützen.

Steigende IT-Kosten
Die Verwaltung mobiler Geräte ist sowohl aufwändig als auch kostenintensiv. Darüber hinaus besteht ein hohes Risiko von Datenschutzverletzungen, die in bestimmten Branchen Bußgelder und Strafen nach sich ziehen können.



Diebstahl oder Verlust von Geräten
Eine mobile Belegschaft kann dazu führenzur Folge haben, dass Geräte unterwegs verloren gehen oder gestohlen werden. Diese Geräte können sensible Daten enthalten, die dann der Gefahr ausgesetzt sind von Dritten veröffentlichtoffengelegt oder weitergegeben zu werden könnten.

Personalfluktuation
Mobile Geräte von Mitarbeitenden zu sichern, die das Unternehmen verlassen, kann sowohl eine Herausforderung sein als auch ein erhöhtes Risiko darstellen. Insbesondere wenn die Geräte zur Wiederinbetriebnahme an die IT-Abteilung zurückgeschickt werden, sind sie Gefahren ausgesetzt.



Gerätevielfalt
Die Verwaltung eines stetig ständig wachsenden und diversenvielseitigen Ökosystems aus mobilen Geräten mit ihren jeweiligeneigenen Betriebssystemen, Konfigurationen und Richtlinien kann sehr komplex und zeitaufwäendig sein.

Highlights der Lösung

Mehr Sicherheit: MDM schützt sensible Unternehmensdaten, indem es Sicherheitsrichtlinien auf mobilen Geräten durchsetzt, um Datenschutzverletzungen und unbefugten Zugriff auf sensible Informationen zu verhindern.

Verbesserte Compliance: MDM kann dazu beitragen, dass mobile Unternehmensgeräte den branchenspezifischen Vorschriften entsprechen, z.B. SOC-2-Typ-II-Compliance, AES-256-Bit-Verschlüsselung und vieles mehr. Dazu gehören auch Funktionen zur Fernlöschung von Daten und zur Prävention von Datenverlusten. Beides kann Unternehmen vor Bußgeldern und Strafen schützen.

Steigerung der Produktivität: MDM kann die Produktivität von Nutzenden steigern, dazu beitragen, die Produktivität der Benutzer zu verbessern, indem es sicherstellt, dass diese nur auf Anwendungen und Inhalte zugegriffen werden kanngreifen können, die den Sicherheitsrichtlinien des Unternehmens entsprechen. Außerdem können IT-Abteilungen mit dem Einsatz von MDM Zeit und Kosten sparen, indem sie damit repetitive Aufgaben reduzieren.

Reduzierte IT-Kosten: MDM trägt zur Senkung der IT-Kosten bei, indem es viele der mit der Verwaltung mobiler Geräte verbundenen Aufgaben automatisiert. Dazu gehören beispielsweise die Bereitstellung von Geräten und Apps, die Implementierung von Anwendungen sowie die und Sicherheitskonfigurationen für Hunderte von Geräten im gesamten Unternehmen.

Verbesserte Übersicht und Kontrolle: MDM gibt Unternehmen einen besseren Überblick über ihre mobilen Geräte und dessen Nutzung, z.B. über die Betriebszeit, den Sicherheitsstatus und die Nutzung von Apps. Auf diese Weise können Unternehmen ihre Geräte optimiert verwalten und sicherstellen, dass sie sicher und vorschriftsmäßig genutzt werden.

Wichtige Features und Funktionen

Device management

User-Gruppen
Sparen Sie Zeit, indem Sie individuelle User-Gruppen erstellen und diese verwenden, um große Mengen an Inhalten und Apps auf einmal bereitzustellen.

Device Management Funktionen
Optimieren Sie Ihre Arbeitsabläufe mit Schnellfunktionen (Quick Action) wie „Sperren“,„Entsperren“,„Ausmustern“, „Zurücksetzen“,„Nachricht senden“ und „Einchecken erzwingen“.

Richtlinien
Erhöhen Sie Ihre Sicherheit, indem Sie wichtige, vordefinierte Sicherheitsrichtlinien für ausgewählte Geräte oder Apps konfigurieren und anwenden.

Einfaches Onboarding
Melden Sie Geräte automatisch mit dem Apple Business Manager und mit Google Zero-Touch Enrollment-Registrierung an.

Auslieferung und Konfiguration von Apps
Verteilen und konfigurieren Sie mobile Apps ganz unkompliziert.

Sicherheit und Verwaltung

Gerätesicherheit und -verwaltung
Sichern und verwalten Sie Endgeräte mit iOS- und Android-Betriebssystemen.

Verwaltung von mobilen Anwendungen
Übertragen Sie Anwendungen auf Geräte, verwalten Sie den AnwendungszZugriff und die Berechtigungen, und aktualisieren oder entfernen Sie Anwendungen per Remote-ZFernzugriff.

Sicheres E-Mail-Gateway
Verwalten, verschlüsseln und sichern Sie den Datenverkehr zwischen mobilen Endgeräten und Backend-Systemen im Unternehmen.

Sichere Produktivität

Eine sichere App für E-Mail und Personal Information Management (PIM)
Sichere E-Mail- und PIM- Anwendung für iOS und Android. Dazu gehören Verschlüsselung auf Regierungsniveau, zertifikatsbasierte Authentifizierung und die obligatorische Verwendung von Passcodes, um User-Daten vor unbefugtem Zugriff zu schützen.

Sicheres Surfen im Internet
Sorgen Sie für mehr Sicherheit beim Surfen im Internet, indem Sie sowohl Data-in-Motion als auch Data-at-Rest schützen. Individuelle Lesezeichen und sicheres Tunneling sorgen dafür, dass User schnell und sicher auf Unternehmensdaten zugreifen können.

Sichere Zusammenarbeit an Inhalten
Mitarbeitende, die remote arbeiten, können sicher auf wichtige Cloud-Datenbanken wie SharePoint, Box, Google Drive oder andere Dienste zugreifen und Inhalte gemeinsam bearbeiten.

Sichere Konnektivität

Per-App-VPN
Hierbei handelt es sich um eine Multi-OS-VPN-Lösung, die es Unternehmen ermöglicht, bestimmten mobilen Anwendungen den Zugriff auf Unternehmensressourcen hinter der Firewall zu gestatten, ohne dass User-Interaktionen erfordelich sind.

Conditional Access

Trust engine
Kombinieren Sie verschiedene Indikatoren wie User, Gerät, App, Netzwerk, Region und mehr, um eine adaptive Zugangskontrolle zu ermöglichen.

User-Authentifizierung ohne Passwort
Passwortlose Multi-Faktor-Authentifizierung mit Device-as-Identity (Gerät gibt die Identität vor) für eine Cloud- oder Vor-Ort-Anwendung.

Sicher entwickelt

BITSIGHT
The Standard in SECURITY RATINGS

BitSight Security stuft TeamViewer unter den Top 1% der Technologiebranche ein.
Menschen vertrauen darauf, dass Sie ihre IT-Probleme lösen. Sie benötigen also ein leistungsstarkes und sicheres Tool, um bestmöglich Support leisten zu können. – vor allem angesichts zunehmend komplexerer Technologien und sich ständig wandelnder Bedrohungen. Aus diesem Grund wird TeamViewer Remote Support bereits mit Sicherheit im Fokus entwickelt (Security by Design). Und genaus aus diesem Grund arbeiten wir auch kontinuierlich an Innovationen – damit Sie immer einen Schritt voraus sind.

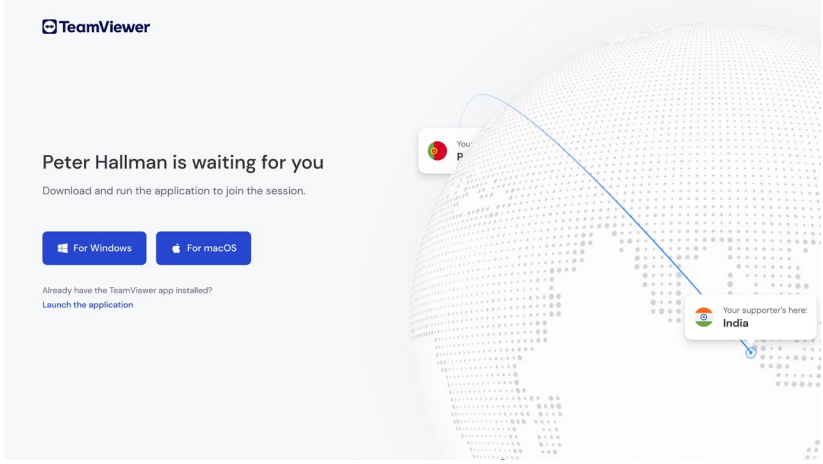
256-Bit-AES-Verschlüsselung

Zwei-Faktor-Authentifizierung

Brute-Force-Schutz

Schutz vor Betrug (Scam)

Allow- und Blocklist



TeamViewer zeigt Ihnen, wer von welchem Ort aus eine Verbindung herstellen möchte.

Zertifiziert und **vertrauenswürdig**

TeamViewer ist durch namhafte Standardisierungsbehörden zertifiziert und erfüllt sowohl die strengen europäischen Datenschutzbestimmungen als auch die HIPAA-Anforderungen Nordamerikas.

Interne IT-Teams und Serviceprovider auf der ganzen Welt vertrauen darauf, dass TeamViewer Remote Support ihre Effizienz steigern und ihren Support verbessern kann.

Möchten Sie mehr erfahren

Besuchen Sie unsere Website:
www.teamviewer.com

TeamViewer

Über TeamViewer

Als globales Technologieunternehmen und führender Anbieter einer Konnektivitätsplattform ermöglicht es TeamViewer, aus der Ferne auf Geräte aller Art zuzugreifen, sie zu steuern, zu verwalten, zu überwachen und zu reparieren. Ergänzend zur hohen Zahl an Privatnutzern, für die die Software kostenlos angeboten wird, hat TeamViewer mehr als 600.000 zahlende Kunden und unterstützt Unternehmen jeglicher Größe und aus allen Branchen dabei, geschäftskritische Prozesse durch die nahtlose Vernetzung von Geräten zu digitalisieren: zum Beispiel in den Bereichen Remote Connectivity, Augmented Reality, Internet of Things und Digital Customer Engagement.

Seit der Gründung im Jahr 2005 wurde die Software von TeamViewer global auf mehr als 2,5 Milliarden Geräten installiert. Das Unternehmen hat seinen Hauptsitz in Göppingen, Deutschland, und beschäftigt weltweit mehr als 1.400 Mitarbeiter. Die TeamViewer AG (TMV) ist als MDAX-Unternehmen an der Frankfurter Börse notiert.

www.teamviewer.com/kundenservice

TeamViewer Germany GmbH
Bahnhofsplatz 2 73033 Göppingen
Deutschland

+49 (0) 7161 60692 50

Stay Connected

www.teamviewer.com