TeamViewer Tensor

DATENBLATT

Skalieren, verwalten und sichern Sie Ihren Support mit TeamViewer Tensor

Unternehmen benötigen eine Lösung, die ihre Support-Erfahrungen standardisiert, harmonisiert und optimiert. Navigieren Sie durch komplexe IT-Prozesse, optimieren Sie Abläufe und bieten Sie Ihren Kunden, Mitarbeitern und Partnern schnelleren Support – nahtlos und sicher.

Einführung

TeamViewer Tensor ist eine für Großunternehmen geeignete Remote-Konnektivitätsplattform, die alle Geräteplattformen miteinander verbindet und es Support-Centern und Support-Center-Technikern ermöglicht, jeden Computer, jedes Mobilgerät, jede Mensch-Maschinen-Schnittstelle (HMI) und jede Industrieanlage zu verbinden, zu verwalten und zu steuern.

TeamViewer Tensor lässt sich entsprechend den Anforderungen Ihres Unternehmens linear skalieren und bietet branchenweit führende Konnektivitäts- und Echtzeit-Support-Tools in einer bequemen, einsatzbereiten, gesicherten SaaS-Umgebung.

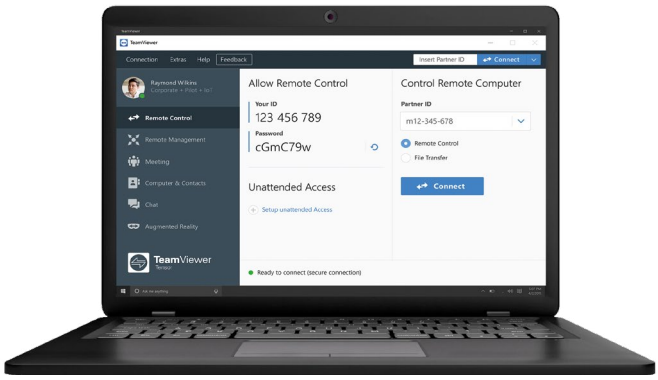
TeamViewer Tensor

Unterstützt von der weltweit größten Infrastruktur für Remote-Konnektivität – die 200 Länder umspannt und mehr als 2,5 Milliarden Geräte verbindet – skaliert TeamViewer Tensor linear, um die Anforderungen von Unternehmen zu erfüllen, und bietet schnelle, zuverlässige Konnektivität und Echtzeit-Support-Tools in einer sicheren, sofort einsetzbaren SaaS-Umgebung.

Maximieren Sie die IT- und Mitarbeiterproduktivität mit benutzerfreundlichem Remote-Zugriff und Support

Mit TeamViewer Tensor können Remote-Experten jeden Computer und jedes mobile Gerät supporten – von überall aus, zu jeder Zeit und auf jeder Plattform – und technische Probleme beheben. Dadurch werden Ausfallzeiten minimiert und gleichzeitig die Produktivität von IT und Mitarbeitern verbessert.

Bei der Arbeit von zu Hause aus oder unterwegs können IT-Teams und Mitarbeiter Ihres Unternehmens von überall aus produktiv bleiben und sicheren Remote-Zugriff auf Computer, mobile Geräte, Server, Maschinen und Betriebstechnologie (OT) erhalten. Mit dem Remote-Zugriff von TeamViewer Tensor sind Desktop-Dateien und Unternehmensanwendungen immer nur ein paar Klicks entfernt.



Ermöglichen Sie Ihrem Unternehmen, effizient und ortsungebunden zu arbeiten – alles ohne VPN.

- Bieten Sie Flexibilität bei der Remote-Arbeit, indem Sie Ihren Mitarbeitern von überall aus und jederzeit plattformübergreifend die Möglichkeit geben, eine Remote-Verbindung zu Unternehmenscomputern und Mobilgeräten herzustellen.
- Remote-Verwaltung, Überwachung und Steuerung von Industrieanlagen und -maschinen zur Verbesserung der Betriebseffizienz, Verkürzung der Problemlösungszeit und Maximierung der Verfügbarkeit.
- Warten und verwalten Sie Unternehmensserver und Android-basierte POS-Systeme (Point-of-Sale), und beheben Sie Probleme von überall aus in Echtzeit und minimieren Sie dadurch ungeplante Ausfallzeiten.

Sicherer Remote-Zugriff

1.400+ Enterprise Kunden

2,5+ Milliarden Installationen

600.000+ Abonnenten

TeamViewer Tensor Security Funktionen

Bei TeamViewer steht die Sicherheit immer an erster Stelle. Wir glauben, dass Sicherheit eine Kombination aus modernster Technologie, Best Practices und Disziplin ist.

Die TeamViewer ID

Die TeamViewer ID ist eine eindeutige Kennung für Ihr Gerät, die automatisch generiert und vor jeder Sitzung überprüft wird.

Höchste Sicherheitsstandards

Unsere Rechenzentren erfüllen die Sicherheitsstandards nach ISO 27001.

Schutz vor Brute-Force-Angriffen

Mit TeamViewer wird die Zeit zwischen fehlgeschlagenen Anmeldeversuchen exponentiell erhöht und erst bei Eingabe des richtigen Kennworts zurückgesetzt. Außerdem schützt es Geräte mit Remote-Zugriff und Verbindungspartner vor weiteren Angriffen.

Zwei-Faktor-Authentifizierung

Die Anmeldung erfolgt mit einem neuen, eindeutigen Code, der jedes Mal von einem Algorithmus generiert und von einem mobilen Gerät übermittelt wird.

Secure Remote Password Protocol (SRP)

TeamViewer verwendet das SRP-Protokoll zur Authentifizierung und Kennwortverschlüsselung. Das Kennwort wird also nie über das Internet gesendet, auch nicht verschlüsselt, und ist somit optimal vor fremdem Zugriff geschützt. Die Kennwörter werden auch im Backend verschlüsselt.

Verschlüsselung

Alle Interaktionen über TeamViewer, einschließlich Dateiübertragungen, VPN, Chat usw., sind durch eine 256-Bit-End-to-End-Sitzungsverschlüsselung mit einem Public-Private-Key-Austausch nach dem 4096-Bit-RSA-Verfahren geschützt.

Dynamisches TeamViewer Kennwort

Benutzer können eine Richtlinie erstellen, die nach jedem Neustart des TeamViewer Dienstes automatisch ein neues dynamisches Sitzungskennwort generiert. Es gibt aber auch eine optionale Einstellung, die es ermöglicht, nach jeder Sitzung ein dynamisches Kennwort festzulegen. Dieses Kennwort ist standardmäßig alphanumerisch und besteht aus sechs Zeichen, so dass es über 2,1 Milliarden mögliche Kombinationen gibt.

Sicherheitsfunktionen auf Unternehamensniveau

Mit TeamViewer Tensor können Unternehmen die branchenführende Remote-Konnektivität mit unternehmensgerechten Sicherheitsfunktionen und -fähigkeiten nutzen – alles ist darauf ausgelegt die Sicherheit Ihrer Daten, Verbindungen und Mitarbeiter zu gewährleisten.

Single Sign-On (SSO)

Mit Single Sign-On hat die IT-Abteilung mehr Kontrolle über die Bereitstellung und Deaktivierung von Unternehmenskonten für TeamViewer Tensor. Indem Sie den Zugriff auf Benutzer mit Unternehmens-E-Mails beschränken, können Sie mit TeamViewer Tensor mit SSO verhindern, dass nicht autorisierte Benutzer jemals Ihre Unternehmens-RAS-Plattform verwenden.

- Zentralisieren Sie die Kennwortkontrolle über Ihren SSO-Identitätsdienstanbieter. Das erspart der IT-Abteilung die Verwaltung von Kennwörtern und reduziert die Anzahl von Anfragen zur Kennwortzurücksetzung.
- Wenden Sie auf jeden autorisierten TeamViewer Tensor-Benutzer automatisch Unternehmens-Kennwortrichtlinien und Identitätsauthentifizierungsregeln an.
- Ermöglichen Sie Mitarbeitern, sich mit ihren SSO-Zugangsdaten bei TeamViewerTensor anzumelden.

Bedingter Zugriff

Behalten Sie den Überblick über alle TeamViewer-Verbindungen in Ihrem Unternehmen und steuern Sie diese zentral mithilfe eines speziellen, auf Conditional-Access-Richtlinien basierten Routers – von TeamViewer in einer privaten Cloud bereitgestellt.

- Erteilen Sie individuelle Benutzer- und Geräteberechtigungen für Fernzugriff, Fernsteuerung, Datenübertragung sowie TeamViewer Assist AR.
- Konfigurieren Sie Regeln auf Konto-, Gruppen- oder Geräteebene. Es werden Active Directory-Gruppen unterstützt (Active Directory und Azure Active Directory).
- Teilen Sie Drittanbietern, Auftragnehmern und Zeitarbeitskräften Fernzugriffsberechtigungen für einen klar begrenzten Zeitraum zu.
- Blockieren Sie alle ein- und ausgehenden Verbindungen von nicht autorisierten oder kostenlosen TeamViewer-Accounts.

Benutzergruppen und Rollen

Benutzergruppen und Rollen ermöglichen IT-Organisationen die Automatisierung der Verwaltung des Benutzerlebenszyklus hinsichtlich der Erstellung, Aktualisierung und Löschung von TeamViewer Tensor-Benutzern. Berechtigungsänderungen können so ganzen Benutzergruppen zugewiesen werden, wodurch mühsame, repetitive Verwaltungsaufgaben für einzelne Benutzer entfallen.

- Automatisieren Sie die Verwaltung des Benutzerlebenszyklus zum Erstellen, Aktualisieren und Löschen von Benutzern.
- Organisieren Sie Benutzer zur einfacheren Verwaltung in Gruppen.
- Verschieben Sie Benutzer bei Rollen- oder Abteilungswechseln in die entsprechende Gruppe.
- Führen Sie Berechtigungsänderungen für verschiedene Benutzer oder Benutzergruppen in einem Zug als Massenvorgang durch.
- Filtern Sie Benutzergruppen nach Rollen, um die Benutzerverwaltung zu erleichtern.

Überprüfbarkeit

Das integrierte Berichtsprotokoll erfasst alle Aktivitäten von Remote-Sitzungen und Aktionen der Management Console: Wer hat was, wann und wie lange für jede eingehende und ausgehende Verbindung getan. Ausgewiesene IT-Administratoren können diese Audit-Protokolle nur mit den entsprechenden Benutzerberechtigungen einsehen.

- Entscheiden Sie mit der Opt-In/Opt-Out-Funktion, ob ein Aktivitätsprotokoll für Remote-Sitzungen und Management Console benötigt wird oder nicht.
- Weisen Sie bestimmte Benutzerberechtigungen zu, die den Zugriff auf die Berichte ermöglichen.
- Behalten Sie die Rechenschaftspflicht bei und sorgen Sie für eine genaue Abrechnung der Dienste.
- Verfolgen Sie die Kundenzufriedenheit mit Sitzungskommentaren und Formularen für Kundenfeedback, um Ihre Dienstleistungen zu verbessern.
- Sparen Sie Kosten, indem Sie die Notwendigkeit von Protokollierungstools von Drittanbietern eliminieren.

Multitenancy

Multitenancy gewährt der zentralen IT einen besseren Überblick über vorhandene Lizenzen und bietet Funktionen zur weiteren Optimierung der Nutzung von TeamViewer Tensor, um Mitarbeitern und zugehörigen Geschäftsbereichen sicheren und skalierbaren Support zu bieten.

- Nachverfolgung, Überwachung und Steuerung der Nutzung von Tensor-Lizenzen in Ihren zentralen und dezentralen Organisationen.
- Mit Multitenancy skalieren Sie Ihre Support-Erfahrung kosteneffizient und optimal.
- Optimieren Sie die Lizenzverwaltung und verhindern Sie mit Multitenancy eine Über- und Unterauslastung Ihrer vorhandenen Tensor-Lizenzen.
- Unterstützen Sie zentrale IT-Administratoren bei der einfachen Verwaltung, Konsolidierung oder Trennung von Benutzern, Geräten und Gruppen basierend auf den Bedürfnissen und Anforderungen des Unternehmens.

Zertifizierung und Compliance

ISO 9001:2015

ISO 9001:2015 ist die weltweit anerkannte Norm, die die Anforderungen an ein Qualitätsmanagementsystem (QMS) festlegt. Organisationen nutzen die Norm, um ihre Fähigkeit zu demonstrieren, Produkte und Dienstleistungen zu liefern, die die Anforderungen von Kunden und Behörden erfüllen. Mit der Zertifizierung nach ISO 9001:2015 hat TeamViewer sein Engagement für ein umfassendes Qualitätsmanagement, Kundenorientierung und eine kontinuierliche Verbesserung der Prozesse zur Steigerung der Effizienz und zur Verbesserung der Qualität der angebotenen Produkte und Dienstleistungen unter Beweis gestellt.

Trusted Information Security Assessment Exchange bewertet die Informationssicherheit von Unternehmen und ermöglicht die Anerkennung der Bewertungsergebnisse unter den Teilnehmern, die in der Lieferkette der Automobilindustrie tätig sind.

Als zusätzliche Sicherheitsmaßnahme sichern wir alle unsere Programmdateien mit der DigiCert Codesignierungs-Technologie, so dass der tatsächliche Herausgeber der Software immer leicht identifizierbar ist. Wenn die Software nachträglich verändert wurde, wird die digitale Signatur automatisch ungültig.

HIPAA, HITECH, und SOC2

TeamViewer bietet Remote-Zugriff, Remote-Support und Online-Zusammenarbeit mit dem nötigen Maß an Sicherheit und Privatsphäre, damit Organisationen HIPAA-konform bleiben.

HIPAA-, HITECH- und SOC2-Zertifizierung
TeamViewer erhielt die HIPAA-, HITECH- und SOC2-Zertifizierung von A-LIGN, einem landesweiten Anbieter für Sicherheit und Compliance in den USA. Während HIPAA und HITECH für Organisationen im Gesundheitswesen von entscheidender Bedeutung sind, um die Vertraulichkeit und Sicherheit sensibler Daten und geschützter Gesundheitsinformationen (PHI) zu gewährleisten, ist SOC2 ein wesentlicher Berichtsrahmen für Dienstleistungsorganisationen, um ein Mittel zur Berichterstattung über nicht-finanzielle interne Kontrollen zu schaffen, damit ihre Kunden ein besseres Verständnis für die Durchsetzung der fünf Trusted Service Principles (TSP) erhalten.

Datenschutz-Grundverordnung (DSGVO)

Am 25. Mai 2018 trat die EU-Datenschutz-Grundverordnung (DSGVO) in Kraft. Die Verordnung zeigt die Bedeutung des Datenschutzes in unserer zunehmend digitalen Welt auf. TeamViewer ist ein weltweites Unternehmen, dem es wichtig ist, die persönlichen Kunden- und Mitarbeiterinformationen in Übereinstimmung mit der DSGVO zu verarbeiten.

Weitere Informationen über den Einsatz von TeamViewer für den Datenschutz und die Vorbereitungen auf die DSGVO finden Sie auf der Seite TeamViewer und DSGVO unserer Knowledge Base.

Weitere Informationen zum Thema TeamViewer Sicherheit finden Sie im TeamViewer Sicherheitshandbuch

California Consumer Protection Act (CCPA)

Am 28. Juni 2018 wurde das Kalifornische Verbraucherschutzgesetz (California Consumer Protection Act of 2018, CCPA) unterzeichnet und trat am 1. Januar 2020 in Kraft. TeamViewer verpflichtet sich zur Einhaltung des CCPA und des Datenschutzes. Weitere Informationen finden Sie auf der Seite TeamViewer und CCPA unserer Knowledge Base (Englisch).

Sie möchten mehr erfahren?

Scannen Sie den QR-Code, um mehr über TeamViewer Tensor™ zu erfahren, oder kontaktieren Sie uns

+49 7161 60692 50
tensor_emea@teamviewer.com

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.

Stay Connected

www.teamviewer.com