TeamViewer Tensor

DATENBLATT

TeamViewer Tensor™ Conditional Access

Verhindern Sie nicht autorisierte Remote-Verbindungen und machen Sie Ihre unternehmenseigenen Sicherheitsrichtlinien geltend – mit einem festgeschalteten, regelbasierten Router für bedingten Zugriff.

Zentrale Herausforderungen

Remote Access und Remote Support sind längst entscheidend für den Geschäftserfolg eines Unternehmens. Dennoch mühen sich IT-Abteilungen immer noch damit ab, die Kontrolle und den Überblick über Remote-Verbindungen und Nutzerberechtigungen zu behalten.

Organisationen, die Remote-Zugriffe unternehmensweit verwalten, benötigen vollständige Kontrolle über Berechtigungen auf Benutzer-, Geräte- und Gruppenebene. Nur so können sie Sicherheit und Compliance garantieren und nicht autorisierte Aktivitäten verhindern. Um ihre Netzwerkumgebung zu schützen und Risiken zu minimieren, benötigen IT-Administratoren darüber hinaus die Kontrolle über Berechtigungen für sensible Funktionen wie Skriptausführung und Dateitransfers.

Zusätzlich müssen sie nicht autorisierte Zugriffe von persönlichen oder kostenlosen TeamViewer Konten unterbinden, gleichzeitig aber Drittanbietern, Auftragnehmern und Zeitarbeitskräften solche Verbindungen erlauben, damit diese zeitlich befristet ihre Arbeit erledigen können.

Wie aber steuern Sie Remote-Zugriffe zwischen Ihrem Netzwerk, Ihren Geräten und der Außenwelt? Und wie stellen Sie sicher, dass nur die richtigen Personen zur rechten Zeit über den richtigen Zugriff auf die richtigen Systeme mit den richtigen Funktionen verfügen?

Genau hier setzt TeamViewer Tensor Conditional Access an. Es unterstützt Unternehmen bei der vollständigen Kontrolle aller ein- und ausgehenden Verbindungen, ermöglicht der IT jedoch die genaue Eingrenzung des Zugriffs für Benutzer, Geräte, Funktionen und Zeiten.

TeamViewer Tensor Conditional Access

TeamViewer Tensor Conditional Access ermöglicht Unternehmen die Kontrolle aller ein- und ausgehenden TeamViewer Verbindungen auf Benutzer-, Gruppen- und Geräteebene durch einen festgeschalteten Router mit regelbasierter Engine.

- Ermöglichen Sie der IT-Abteilung oder externen Anbietern durch zeitbasierte Optionen auch außerhalb der Geschäftszeiten unbeaufsichtigten Zugriff.
- Legen Sie für alle Remote-Access-Sitzungen Zugriffsrechte für Nutzer und Geräte fest.
- Schützen Sie Remote-Verbindungen zusätzlich durch Blockieren nicht autorisierter Zugriffe auf sensible Funktionen wie Skriptausführung und Dateitransfers.
- Erlauben Sie bestimmten Geräten den Zugriff nur mit eingeschränkter Funktionalität und zeitlich begrenzten Berechtigungen (z. B. Drittanbietern, Auftragnehmern oder Zeitarbeitskräften)

Technische Voraussetzungen

- Aktivierte TeamViewer Tensor Pro oder TeamViewer Tensor Unlimited Lizenz oder TeamViewer Tensor Conditional Access AddOn
- TeamViewer Client Version 15.5 oder höher
- TeamViewer Unternehmensprofil, erstellt in der TeamViewer Management Console
- DNS/IP-Adresse eines dedizierten Routers für bedingten Zugriff

Funktionshighlights

Router für bedingten Zugriff

Schützen Sie Ihre Netzwerkumgebung durch die vollständige Kontrolle aller Verbindungen mittels eines festgeschalteten regelbasierten Routers für bedingten Zugriff – einem „Gatekeeper", der von TeamViewer in Ihrer eigenen privaten Cloud bereitgestellt und verwaltet wird.

Granulare Steuerung von Berechtigungen

Legen Sie Regeln für den Remote Access fest und schränken Sie Funktionalitäten auf der Nutzer-, Gruppen- und Geräteebene ein. So verwalten Sie eingehende und ausgehende Verbindungen zentral und behalten die granulare Kontrolle.

Zeitlich begrenzter Zugriff

Erstellen und planen Sie mittels zeitlich begrenzter Zugriffsregeln individuelle temporäre Berechtigungen für externe Benutzer. So legen Sie fest, wer innerhalb eines klar begrenzten Zeitraums auf welche Geräte und Funktionen zugreifen kann.

Verwaltung von privilegierten Nutzern

Reduzieren Sie Risiken, indem Sie ausgewählten Nutzern privilegierte Zugriffsregeln zuweisen. Dadurch können diese sensible Funktionen verwenden, die Standardnutzer nicht benötigen.

Blockieren von Meetings

Entscheiden Sie selbst, ob Ihr Unternehmen für Videokonferenzen, VoIP-Anrufe und Chats Zugriff auf TeamViewer Meeting benötigt oder ob Sie diese Funktionen für alle Benutzer sperren.

Funktionsweise von TeamViewer Tensor Remote-Verbindungen

ohne Conditional Access VS. **mit Conditional Access**

Remote-Support für Mitarbeiter

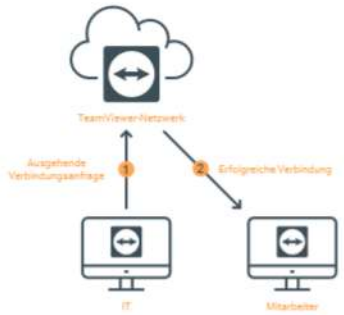

Abbildung 1a: Autorisierte Remote-Support-Verbindung für Mitarbeiter – IT-Administrator stellt erfolgreich eine Verbindung zum Mitarbeitergerät innerhalb des Unternehmensnetzwerks her.

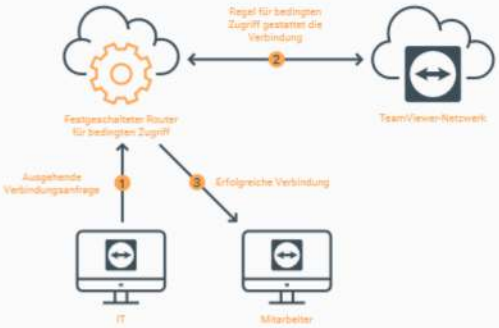

Abbildung 1b: Autorisierte Remote-Support-Verbindung für Mitarbeiter – IT-Administrator stellt eine Verbindung zum Router her, der den Zugriff auf das Mitarbeitergerät innerhalb des Unternehmensnetzwerks gestattet.

Kunden-Support

Abbildung 2a: Autorisierte Kundensupport-Verbindung – Support-Mitarbeiter stellt erfolgreich eine Verbindung zum Kundengerät außerhalb des Unternehmensnetzwerks her.

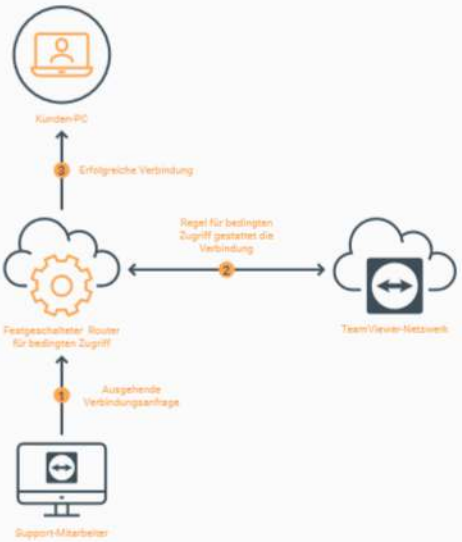

Abbildung 2b: Autorisierte Kundensupport-Verbindung – Support-Mitarbeiter stellt eine Verbindung zum Router her, der den Zugriff auf das Kundengerät außerhalb des Unternehmensnetzwerks gestattet.

Nicht autorisierte Remote-Verbindung

Abbildung 3a: Nicht autorisierte Verbindung aus dem Unternehmensnetzwerk zum Privatgerät – Mitarbeiter stellt erfolgreich eine Verbindung von seinem Arbeitsplatz zum Privatgerät im Homeoffice her.

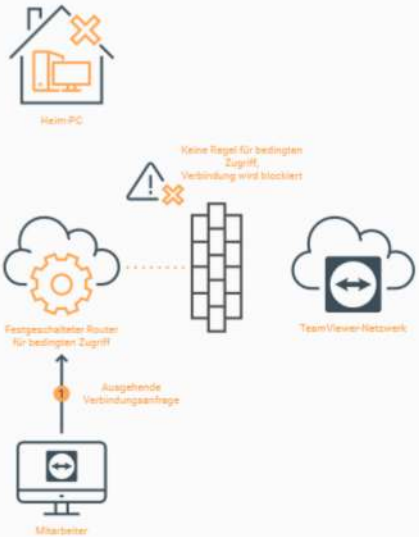

Abbildung 3b: Nicht autorisierte Verbindung aus dem Unternehmensnetzwerk zum Privatgerät – Mitarbeiter kann keine Verbindung von seinem Arbeitsplatz zum Privatgerät im Home-Office herstellen.

Funktionsweise

TeamViewer stellt den Router für den bedingten Zugriff in einer sicheren privaten Cloud bereit. Der Router wird durch eine regelbasierte Engine gesteuert, die einem „Gatekeeper" gleich Remote-Verbindungen zulässt oder blockiert.

Sobald die regelbasierte Engine konfiguriert ist, kann der IT-Administrator Conditional Access aktivieren, um Benutzern, Gruppen und Geräten den Zugriff zu erlauben. Sind die Regeln inaktiv – etwa während der ersten Einrichtung oder einer Wartung – ist Conditional Access standardmäßig deaktiviert. Dadurch werden alle Verbindungsversuche über TeamViewer blockiert.

IT-Administratoren können die Regeln für den bedingten Zugriff zentral in der TeamViewer Tensor Management Console festlegen, verwalten, filtern und bearbeiten. Die Regeln können individuell für Benutzer, Gruppen und autorisierte Computer oder Geräte festgelegt werden, inklusive granularer Berechtigungen für sensible Funktionen:

- ✓ Wählen Sie für einzelne Nutzer individuelle Optionen aus und definieren Sie Regeln für den noch sicheren Umgang mit Berechtigungen
- ✓ Legen Sie Bedingungen für die Zugriffe von Benutzern, Gruppen oder Geräten fest.
- ✓ Definieren und planen Sie zeitlich begrenzte Regeln und erhöhen Sie dadurch die Sicherheit externer Zugriffe.

** Unterstützte Plattformen: Windows und macOS*

ohne Conditional Access

Ohne Conditional Access kann Ihre IT lediglich eingehende Verbindungen zu den Geräten in Ihrem Netzwerk blockieren. Ausgehende Verbindungen sind zu jedem Gerät möglich, egal ob es von der IT autorisiert wurde oder nicht.

- ✓ Autorisiert, Verbindung möglich: Mitarbeitergeräte innerhalb des Netzwerks *(Abbildung 1a)*
- ✓ Autorisiert, Verbindung möglich: Kundengeräte außerhalb des Netzwerks *(Abbildung 2a)*
- ✓ Nicht autorisiert, Verbindung möglich: private Server und Geräte im Homeoffice *(Abbildung 3a)*

Alle verschlüsselten Daten werden über das TeamViewer Netzwerk übertragen.

mit Conditional Access

Mit Conditional Access kann Ihre IT **ein- und ausgehende Verbindungen blockieren**. Die Autorisierung von Verbindungen zu Geräten erfolgt nach vordefinierten Regeln.

- ✓ Nach Regeln autorisiert, Verbindung möglich: Mitarbeitergeräte innerhalb des Netzwerks *(Abbildung 2a)*
- ✓ Nach Regeln autorisiert, Verbindung möglich: Kundengeräte außerhalb des Netzwerks *(Abbildung 2b)*
- ✗ Nicht autorisiert, keine Regeln, Verbindung blockiert: private Server und Geräte im Homeoffice *(Abbildung 3b)*

Alle verschlüsselten Daten werden *ausschließlich* über den Router für bedingten Zugriff übertragen.

Hauptvorteile

Höhere IT-Sicherheit

Schützen Sie Ihre Netzwerkumgebung vor nicht autorisierten Remote-Zugriffen – einschließlich ein- und ausgehenden Verbindungsanfragen von persönlichen oder kostenlosen TeamViewer Konten.

Mehr Flexibilität

Erhalten Sie die vollständige Kontrolle über die Art und Weise, wie Benutzer Verbindungen zu Geräten herstellen. Vergeben Sie zeitlich begrenzte Berechtigungen an Externe, sodass diese ausschließlich Zugriff auf die von ihnen benötigten Geräte und Funktionen haben.

Weniger Risiken

Verbessern Sie die Compliance mit den Sicherheitsrichtlinien Ihres Unternehmens und minimieren Sie die Risiken nicht autorisierter Remote-Zugriffe durch privilegierte Zugriffsrechte und zeitlich begrenzte Regeln.

Höhere Effizienz

Steigern Sie die Produktivität und Effizienz der IT durch die zentrale Verwaltung und Steuerung aller ein- und ausgehenden Verbindungen sowie granulare Zugriffsrechte.

Mehr Benutzerfreundlichkeit

Ermöglichen Sie es Ihren Mitarbeitern mit intuitiven Funktionen ganz einfach remote zu arbeiten. Gewährleisten Sie auch ohne VPN einen sicheren Zugriff auf Systeme, Computer und Geräte.

Noch Fragen?

Sie wünschen eine kostenlose Beratung oder eine TeamViewer Tensor-Demo? Setzen Sie sich mit uns in Verbindung.

+49 7161 60692 50

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.Deutschland. Das Unternehmen ist börsennotiert und beschäftigt weltweit rund 1400 Mitarbeiter. Die TeamViewer AG (TMV) ist an der Frankfurter Wertpapierbörse notiert und gehört zum MDAX.

Bleiben Sie in Verbindung

www.teamviewer.com

TVT-DS-DE-CS-042022-1