

TeamViewer KI

Sicherheit, Kontrolle, Datenhandhabung

Bezieht sich auf: Tia, Session Insights und KI-gestützte Skripterstellung

Trust Center: compliance.teamviewer.com

Letzte Aktualisierung: 10. März 2026



Top issue types
Overview of top issue categories from support sessions.

Issue Category	Count
Application...	140
...	100
...	70
...	50
...	30
...	20
...	10

Top applications
top apps used during support sessions.

Application	Count
...	100
...	50
...	30
...	20
...	10

PowerShell

1. Opened Windows PowerShell (Admin) by right-clicking on the Start button and selecting **Windows PowerShell (Admin)** from the context menu.
2. Executed the following command in PowerShell:

```
reg add "HKEY_LOCAL_MACHINE\Software\Policies\VM  
/v RestrictDriverInstallationToAdmin  
/d 0  
/f
```

File Explorer

3. Opened File Explorer by clicking on the File Explorer icon in the taskbar.
4. Navigated to the following network path by typing it into the address bar:
`\\csdfkljdsd0010`
5. Double-clicked on the printer named PDZZSAI001 to connect it.
6. Closed File Explorer.

Zusammenfassung

Dieses Dokument bietet einen Überblick darüber, wie die Datenhandhabung der KI-Features von TeamViewer aussehen und wie wir sicherstellen, dass unsere Kundschaft jederzeit die Kontrolle behält. Es werden die für alle KI-Features geltenden Sicherheitsgrundlagen zusammengefasst, und beschrieben, wie die drei zentralen KI-Workflows – Dokumentation, Fehlerbehebung und Skripterstellung – Effizienz unterstützen und gleichzeitig die Sicherheits- und Datenschutzstandards von Unternehmen erfüllen können.

KI für effizienten Support mit integrierter Kontrolle

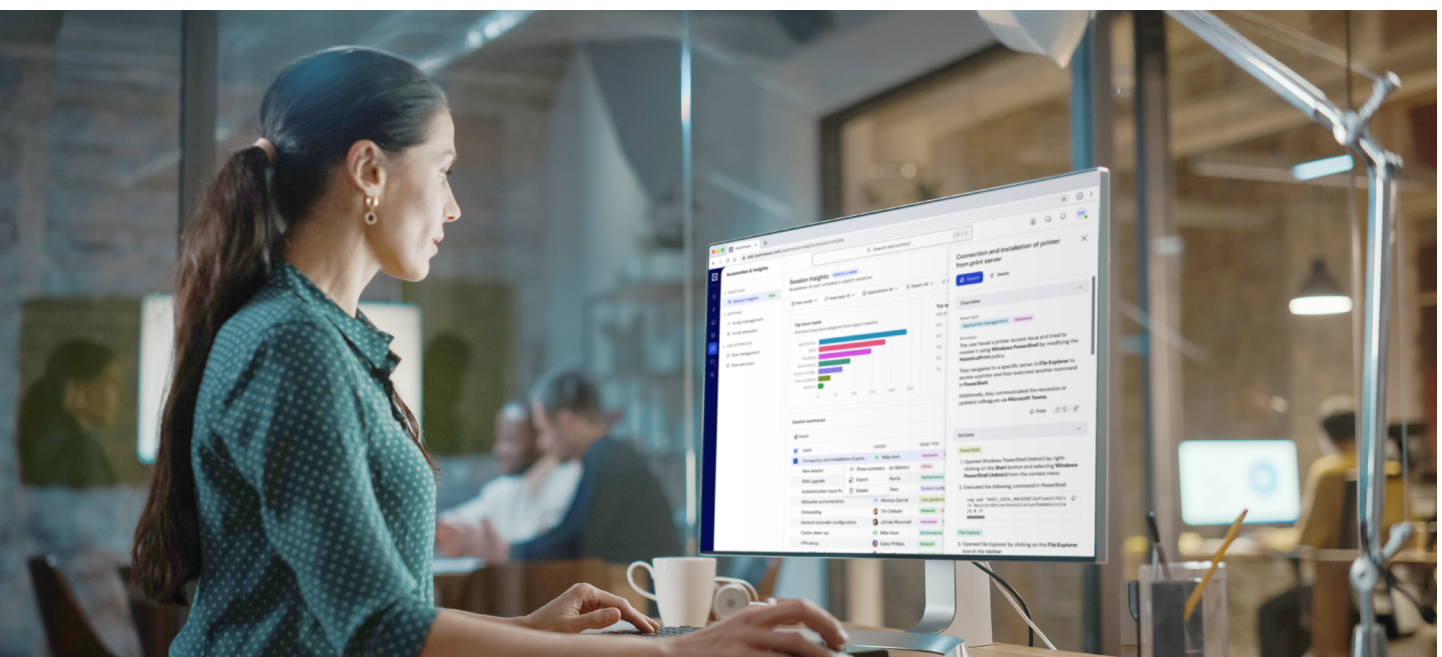
TeamViewer KI wurde dafür entwickelt, die Effizienz des IT-Supports bei der Dokumentation von Sessions, der Fehlerbehebung während Sessions und der KI-gestützten Erstellung von Skripten zu verbessern, und dabei stets sicherzustellen, dass Unternehmen die volle Kontrolle über ihre eigenen Prozesse behalten. Die Datenhandhabung basiert auf einem Security-by-Design-Ansatz: Richtlinienbasierte Kontrollmechanismen, Datenminimierung, Anonymisierung und starke Verschlüsselung für den gesamten KI-Workflow.

TeamViewer KI ermöglicht:

- **Die Dokumentation von Sessions:** Automatisierte, einheitliche Erfassung von Aktionen und Ergebnissen
- **Die Fehlerbehebung während Sessions:** Unterstützung, die auf kontrollierten Eingaben und Berechtigungen basiert
- **Die KI-gestützte Skripterstellung:** Schnellere Erstellung von Skripten mit Überprüfung und berechtigungsbasierter Ausführung

Zentrale Verpflichtungen auf einen Blick:

- **Admins kontrollieren Rollout und Zugriff** durch umfassende Einstellungen, Berechtigungen und Richtlinien.
- **Personenbezogene Daten werden minimiert und anonymisiert**, bevor sie weiterverarbeitet werden.
- **Daten sind sowohl während der Übertragung als auch im Ruhezustand durch Verschlüsselung geschützt**, unterstützt durch ein kontrolliertes Key Management.
- **Services von Drittanbietern werden nur unter vorab definierten Bedingungen genutzt** und im [Trust Center](#)



TeamViewer KI Plattform-Services

Alle Funktionen von TeamViewer KI basieren auf einer zentralen KI-Plattform. Diese schließt eine richtlinienbasierte Verwaltung, Technologie zur Datenminimierung, eine starke Verschlüsselung und klar definierte Grenzen für die Verarbeitung von Daten durch KI ein. In diesem Abschnitt werden die KI-Plattform-Services dargestellt, die allen KI-Workflows zugrunde liegen.

KI-Admin-Richtlinien und -Berechtigungen K

TeamViewer bietet Admins granulare Kontrollmöglichkeiten, mit denen sich einzelne KI-Funktionen aktivieren oder deaktivieren lassen, mit denen festgelegt werden kann, an welchen Stellen sie genau eingesetzt werden können, und Einstellungen vorgenommen werden können, welche User Zugriff auf KI-generierte Ergebnisse erhalten. Diese Kontrollmechanismen ermöglichen eine Softwareverteilung nach dem Least-Privilege-Prinzip und helfen Unternehmen dabei, die Nutzung von KI an interne Governance-Richtlinien anzupassen.

Unternehmensadmins können steuern, wie TeamViewer KI konfiguriert, genutzt und ausgerollt wird:

- **Admin-Einstellungen** —————> **KI-Admin-Einstellungen**
Konfiguration der KI-Funktionen, einschließlich der Aktivierung und Deaktivierung von einzelnen Features.
- **Admin-Einstellungen** —————> **User-Berechtigungen**
Berechtigungen, mit denen sich der Zugriff von Usern auf KI-generierte Inhalte festlegen lässt, darunter auch, welche User Session Insights ansehen oder bearbeiten dürfen, sowie wer Zugriff auf Remote Skripting erhält.
- **Admin-Einstellungen** —————> **Richtlinien**
Detaillierte Einstellungen für Rollouts und Einschränkungen für Endpunkte (z. B. lassen sich bestimmte Endpunkte von der Datenerfassung durch Session Insights ausschließen).

Anonymisierung und DSGVO A

Um personenbezogene Daten bestmöglich zu schützen, anonymisiert TeamViewer diese vor der Verarbeitung im Rahmen des Möglichen.

Anonymisierung auf Geräten (regelbasiert)

Bevor Daten vom TeamViewer Client an die TeamViewer Cloud-Umgebung eines Unternehmens gesendet werden, wird eine regelbasierte Anonymisierung angewendet. Beispiele hierfür sind:

E-Mail-Adressen	—————>	[EMAIL_ADDRESS]
Benutzernamen in URLs	—————>	[USERNAME]
Passwörter in URLs	—————>	[PASSWORD]
Kreditkartennummern	—————>	[NUMBER]
Sozialversicherungsnummern	—————>	[NUMMER]
IBAN	—————>	[IBAN]

Cloubasierte Anonymisierungsservices

Nach der clientseitigen Anonymisierung werden die Daten über zusätzliche Anonymisierungsservices in der TeamViewer Cloud geleitet, um verbleibende sensible Informationen (insbesondere personenbezogene Daten) zu identifizieren und zu entfernen, bevor die Daten in der TeamViewer Cloud gespeichert werden. Diese cloubasierte Anonymisierung nutzt algorithmusbasierte Methoden, einschließlich komplexer Regeln und maschinellen Lernens. Ergänzend zu diesen Maßnahmen kommt LLM-Technologie als abschließender Anonymisierungsschritt zum Einsatz.

Nicht-öffentliche Details: Die spezifischen Sub-Prozessoren, die für die cloubasierte Anonymisierung verwendet werden, sind in diesem Dokument nicht veröffentlicht und können im Rahmen einer Sicherheitsüberprüfung auf Anfrage und nach Unterzeichnung eines NDA bereitgestellt werden.

Verschlüsselung und Speicherung S

TeamViewer schützt Daten durch branchenübliche Verschlüsselung und kontrollierte Speicherorte.

Speicherorte für Daten

- Microsoft Azure (EU-27)

Verschlüsselung ruhender Daten

Für die Cloud-Speicher wird eine branchenübliche AES-256-Verschlüsselung genutzt, um Daten im Ruhezustand zu schützen. Weitere Informationen dazu: <https://www.teamviewer.com/de/resources/trust-center/industry-leading-security/>

Verschlüsselung während der Übertragung

Daten werden bei der Übertragung zwischen TeamViewer Clients, TeamViewer Cloud-Services, Cloud-Speichern und KI-Services mit HTTPS (TLS) verschlüsselt.

Kontrolliertes Key Management

Session Insights und Tia nutzen clientseitige Verschlüsselung mit HSM-geschützten Schlüsseln und dokumentierten Abläufen.

KI-Services (LLM-gestützt) V

Einige Funktionen von TeamViewer KI nutzen LLM-Services von Drittanbietern, um textbasierte Ausgaben wie Zusammenfassungen und Code bereitstellen zu können.

TeamViewer KI nutzt LLM-Services von Azure OpenAI und Google Gemini gemäß den veröffentlichten Nutzungsbedingungen dieser Provider.

Azure OpenAI

- Provider-Nutzungsbedingungen: [Microsoft Azure Legal Information](#)
- Referenz zu Datenverarbeitung und Datenschutz: [Daten, Datenschutz und Sicherheit für Azure OpenAI Service](#)
- Angegebener Hosting-Standort: EU-27

Google Gemini

- Provider-Nutzungsbedingungen: [Google-Nutzungsbedingungen](#)
- Referenz zu Datenverarbeitung und zum Datenschutz: [Datenschutzhinweis für Gemini Apps](#)
- Angegebener Hosting-Standort: EU-27

TeamViewer KI-Workflows

TeamViewer KI besteht aus drei praxisnahen Workflows, die entwickelt wurden, um sich der Arbeitsweise von Support-Teams anzupassen.

Session-Dokumentation (Session Insights)

Die Session-Dokumentation hilft dabei, IT-Support standardisiert zu dokumentieren, indem strukturierte Session-Zusammenfassungen und Überblicke der wichtigsten durchgeführten Aktionen erstellt werden. Dadurch wird Dokumentationsaufwand reduziert und die Zusammenarbeit zwischen Teams einheitlicher gestaltet. Ein häufiger Anwendungsfall ist die Übertragung von Zusammenfassungen aus Session Insights in ein ITSM-System, um Ticketdokumentation zu vereinfachen, Fallkontinuität zu ermöglichen und reibungslose Übergaben zu unterstützen. TeamViewer bietet sofort einsatzbereite Integrationen für führende ITSM-Plattformen.

Kontrolle durch Admins

Über die TeamViewer Admin-Einstellungen können Admins folgende Prozesse kontrollieren:

- Den Rollout von Session Insights für alle TeamViewer Verbindungen
- Die Berechtigungen für den Zugriff auf Session Insights und deren Bearbeitung

Weitere Informationen zur Feature-Konfiguration finden Sie hier:

<https://www.teamviewer.com/de/global/support/knowledge-base/teamviewer-remote-remote-control/generate-session-summaries-with-session-insights/>

Datenerfassung und erste Anonymisierung (Client)

Wenn Session Insights aktiv ist, werden Session-Daten auf dem Client erfasst. Interaktionen wie Klicks, Tastatur- und Terminaleingaben werden aufgezeichnet. Ein erster Anonymisierungsschritt wird direkt auf dem Client durchgeführt.

Clientseitige Verschlüsselung und HSM-geschütztes Key Management

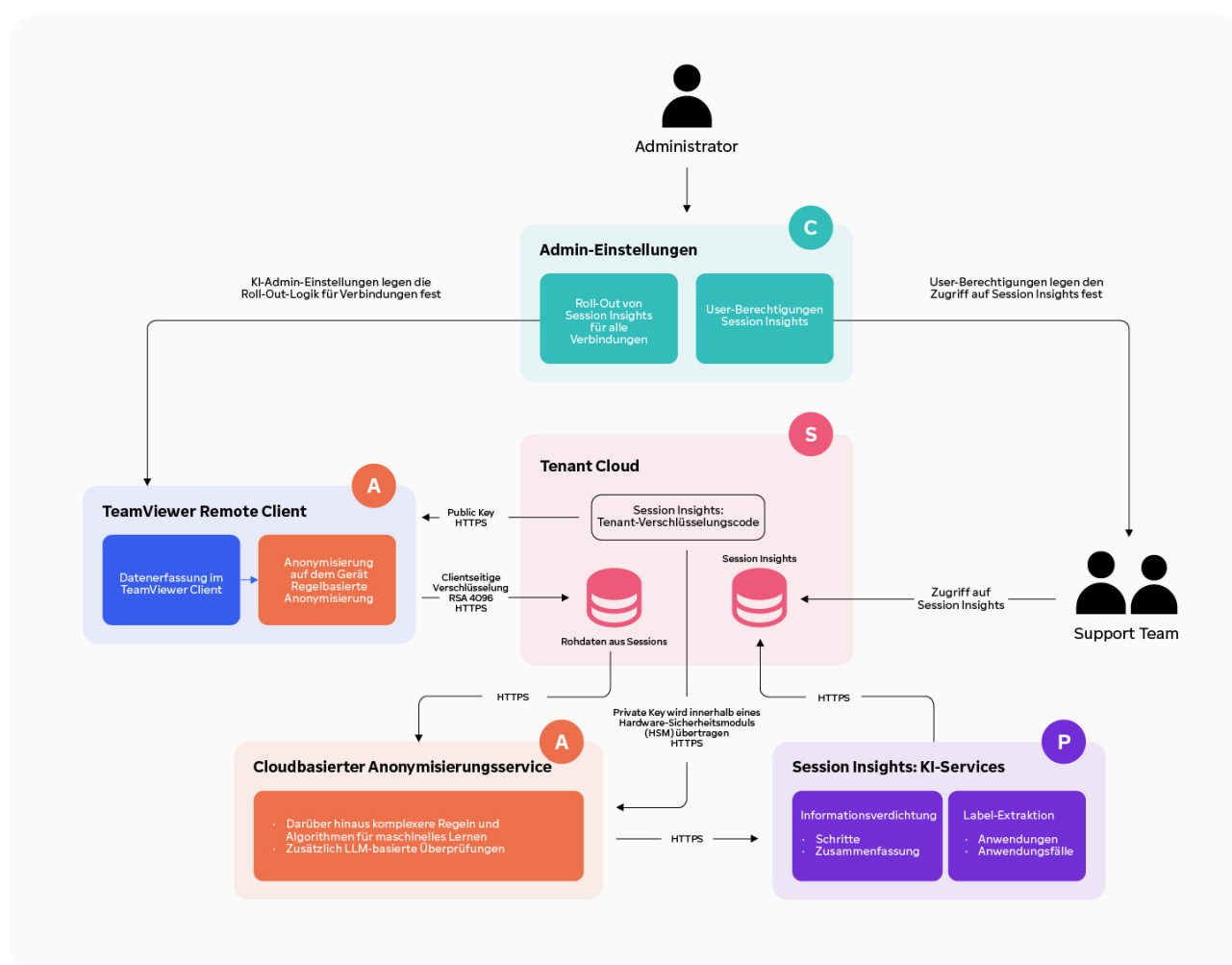
Session-Daten werden durch eine clientseitige Verschlüsselung (CSE) geschützt, um die Vertraulichkeit während der gesamten Übertragung und Verarbeitung sicherzustellen. Der Client ruft den Verschlüsselungscode sicher über HTTPS ab und verschlüsselt sämtliche Session-Inhalte, bevor diese das Gerät verlassen. Der zugehörige Entschlüsselungscode wird in einem hochsicheren, zertifizierten Hardware-Sicherheitsmodul (HSM) gespeichert, in dem alle schlüsselbezogenen Aktionen geschützt und vollständig aufgezeichnet werden. So kann gewährleistet werden, dass ausschließlich autorisierte Prozesse Zugriff auf die Daten erhalten und sämtliche Aktivitäten transparent protokolliert werden.

Anonymisierung in der Cloud und Erstellung von Zusammenfassungen

Nach der clientseitigen Anonymisierung werden in den Daten verbliebene personenbezogene Informationen mithilfe zusätzlicher cloudbasierter Anonymisierungsservices entfernt (Details auf Anfrage nach Unterzeichnung eines NDA). Die Informationen der anonymisierten Session-Daten werden anschließend von den Session Insights KI-Services komprimiert und Labels werden extrahiert. Die Ausgabe umfasst:

- Eine Auflistung durchgeführter Aktionen und eine kurze Zusammenfassung
- Anwendungszuweisungen pro Aktion
- Allgemeine Klassifizierung von Anwendungsfällen

Aufbau der Session-Dokumentation (Session Insights)



Das Diagramm zeigt, wie Admins Rollout- und Zugriffseinstellungen konfigurieren können (K), wie Session-Daten direkt auf dem Gerät anonymisiert und anschließend mithilfe cloudbasierter Algorithmen weiter bereinigt werden (A), und wie KI-Services zur Erstellung von Zusammenfassungen und Labels genutzt werden (V). Gespeicherte Daten werden in der Tenant-Cloud gespeichert, verschlüsselt und durch ein kontrolliertes Key Management geschützt (S). Sämtliche Datenübertragungen erfolgen über sicheres HTTPS/TLS. Durch die clientseitige Verschlüsselung wird sichergestellt, dass sensible Inhalte verschlüsselt werden, bevor sie die Geräte von Usern verlassen.

Legende (Buchstaben stehen für die jeweiligen Services der TeamViewer KI Plattform)

- | | |
|--|---|
| K Kontrollieren (Admin-Richtlinien & -Berechtigungen) | A Anonymisieren (Anonymisierung & DSGVO) |
| V Verarbeiten (LLM-Services) | S Schützen (Verschlüsselung & Speicherung) |

Verfügbarkeit von Features

- TeamViewer Remote: Business, Premium, Corporate, Tensor
- TeamViewer ONE: Standard, Advanced, Enterprise

Problembehebung während Sessions (Tia)

Tia bietet Unterstützung bei der Problembehebung während Sessions, basierend auf kontrollierten Eingaben und berechtigungsbasiertem Kontext. Tia arbeitet dabei ausschließlich schreibgeschützt und kann keine Aktionen auf dem Gerät durchführen. Tia kann keinen Code ausführen, keine Software installieren und keine Änderungen an Systemen durchführen. Ziel ist es, Support-Teams dabei zu unterstützen, Probleme innerhalb klar definierter Grenzen effizient zu diagnostizieren und zu lösen, während die Kontrolle in menschlicher Hand verbleibt.

Kontrolle durch Admins

- Tia steht Usern während Sessions zur Verfügung.
- Admins kontrollieren, wie viel Kontext Tia zur Verfügung steht, indem sie Tias Zugriff auf die Session Insights über die User-Berechtigungen verwalten.

Von Tia genutzte Daten

Tia nutzt innerhalb der TeamViewer-Umgebung eine kontrollierte Auswahl von Eingaben, darunter:

- Ein zu Beginn der Session automatisch vorgenommener Einblick in die technischen Daten des betreffenden Geräts
- Screenshots, wenn diese von Usern explizit ausgelöst werden
- Während der Session entstandener Gesprächskontext
- Vergangene Session Insights, sofern User über entsprechende Zugriffsrechte verfügen

Der Einblick in die Gerätedaten ist darauf ausgelegt, den für die Problembehebung minimal erforderlichen technischen Kontext bereitzustellen. Er enthält System- und Konfigurationsdaten, die Tia dabei helfen, die Geräteumgebung zu verstehen und eine grundlegende Diagnose zu stellen.



Gerätedaten-Einblick

Zu Beginn einer Session erhält Tia automatisch einen eingeschränkten Einblick in die technischen Informationen des Remote-Geräts. Dieser Einblick beinhaltet ausschließlich die Daten, die zum Verständnis der Systemkonfiguration und zur Unterstützung bei typischen Problembehebungen erforderlich sind.

Die Momentaufnahme kann folgende Elemente enthalten:

- **Hardwareinformationen**
Gerätemodell, Hersteller, Seriennummer, CPU, Arbeitsspeicher, Speicherkapazität und Zustand der Festplatte, Grafikkarteninformationen, Monitore, Netzwerkadapter, BIOS-Version und -Veröffentlichungsdatum
- **Informationen zum Betriebssystem**
Name, Version und Build des Betriebssystems, Installations- und Startinformationen, Sprache, Gebietsschema, Zeitzone, Speicher und Systemlaufzeit
- **Installierte Software und Treiber**
Die Namen, Versionen, Installationszeitpunkte und Hersteller von Anwendungen und Treibern, sowie Metadaten zu Anwendungsabstürzen und -problemen
- **Systemdienste**
Name, Typ und Status (zum Beispiel „läuft“ oder „angehalten“)
- **Informationen zu Netzwerkzustand und -sicherheit**
Adaptertyp/-modell, lokale IP-Adresse/lokales Subnetz und Firewallstatus
- **Informationen zu Akku- und Gerätestatus**
Akkuladestand und Gerätebetriebszeit
- **Nicht personenbezogene Geräteeinstellungen**
Z.b. ausgewählte Sprache und Zeitzone

Tia erfasst im Rahmen dieser Einblicke keine User-Inhalte, persönlichen Dokumente, Kommunikationsdaten, Tastenanschläge oder Aktivitätsdaten. Es werden ausschließlich technische Geräteinformationen erfasst, die ein Supporter auch im Rahmen einer regulären Support-Session einsehen könnte.

Einschränkungen für Tools, die auf Geräte zugreifen

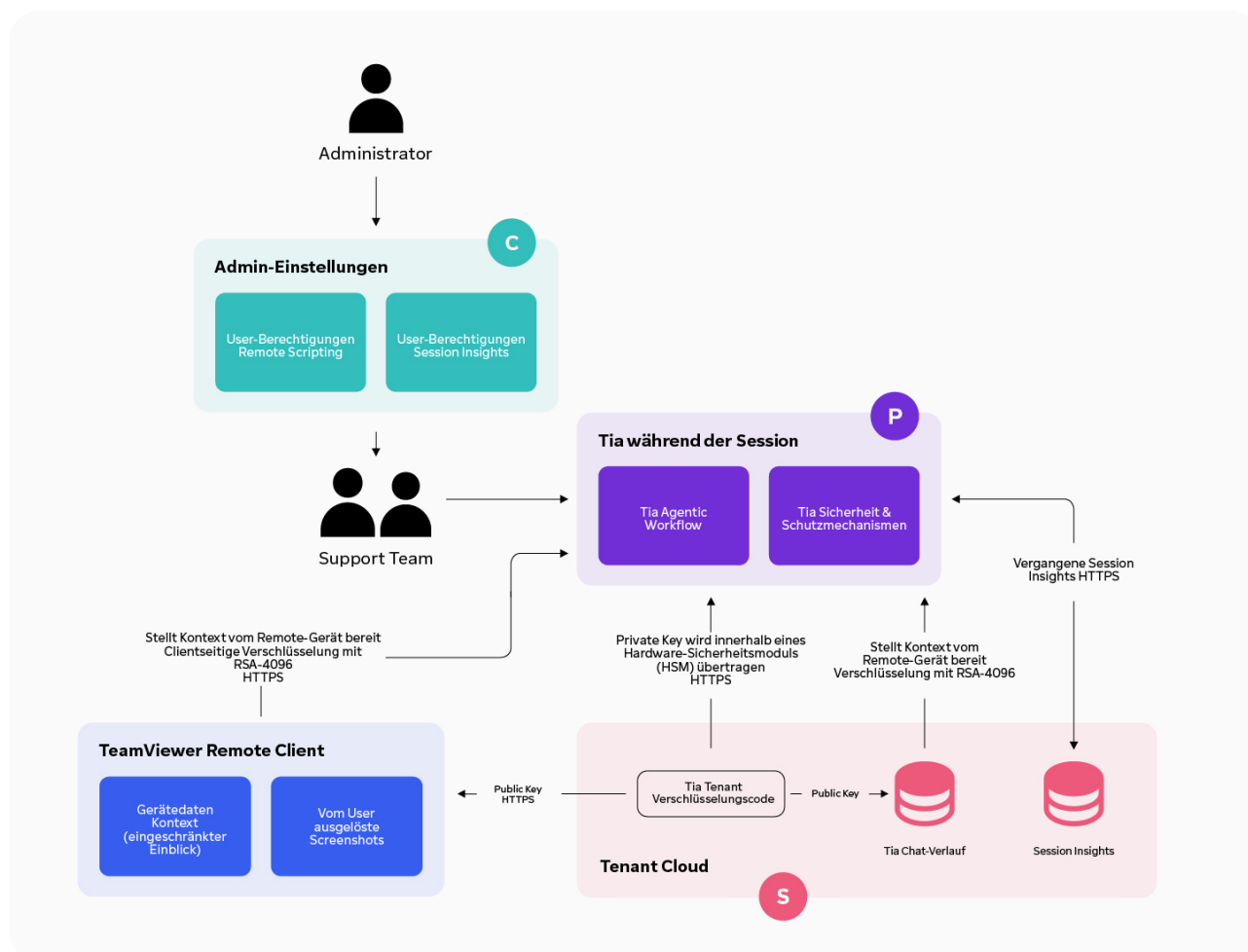
Tia basiert auf einer Multi-Agent-Architektur, mit der sich Informationen dynamisch bereitstellen lassen, die genau zur jeweiligen Anfrage passen. Es wird ausschließlich auf IT-bezogene Fragen geantwortet.



Tia nutzt kontrollierte, schreibgeschützte Tools zur Unterstützung bei der Problembehebung:

- Gezielte Einblicke in die Gerätedaten
- Screenshots (wenn von Usern ausgelöst)
- Zugang zu vergangenen Session Insights

Aufbau der Problembehebung während Sessions (Tia)



Dieses Diagramm zeigt, wie durch Admin-Einstellungen Zugriffsgrenzen (K) festgelegt werden können, wie Tia während der Session im Rahmen von Schutzmechanismen (V) arbeitet und wie relevante, mandantenspezifische Daten (z.B. Verschlüsselungscodes, Chatverläufe mit Tia und berechtigungsbasierte Session Insights) in der Tenant-Cloud (S) geschützt werden. Der Kontext des Remote-Geräts wird wie dargestellt über HTTPS/TLS mit clientseitiger Verschlüsselung (RSA 4096) bereitgestellt.

Legende (Buchstaben stehen für die jeweiligen Services der TeamViewer KI Plattform).

- K** Kontrollieren (Admin-Richtlinien & -Berechtigungen)
- V** Verarbeiten (LLM-Services)
- S** Schützen (Verschlüsselung & Speicherung)

Verfügbarkeit von Features

- TeamViewer Remote: Business, Premium, Corporate, Tensor
- TeamViewer ONE: Standard, Advanced, Enterprise

KI-gestützte Skripterstellung (Session Insights und Tia)

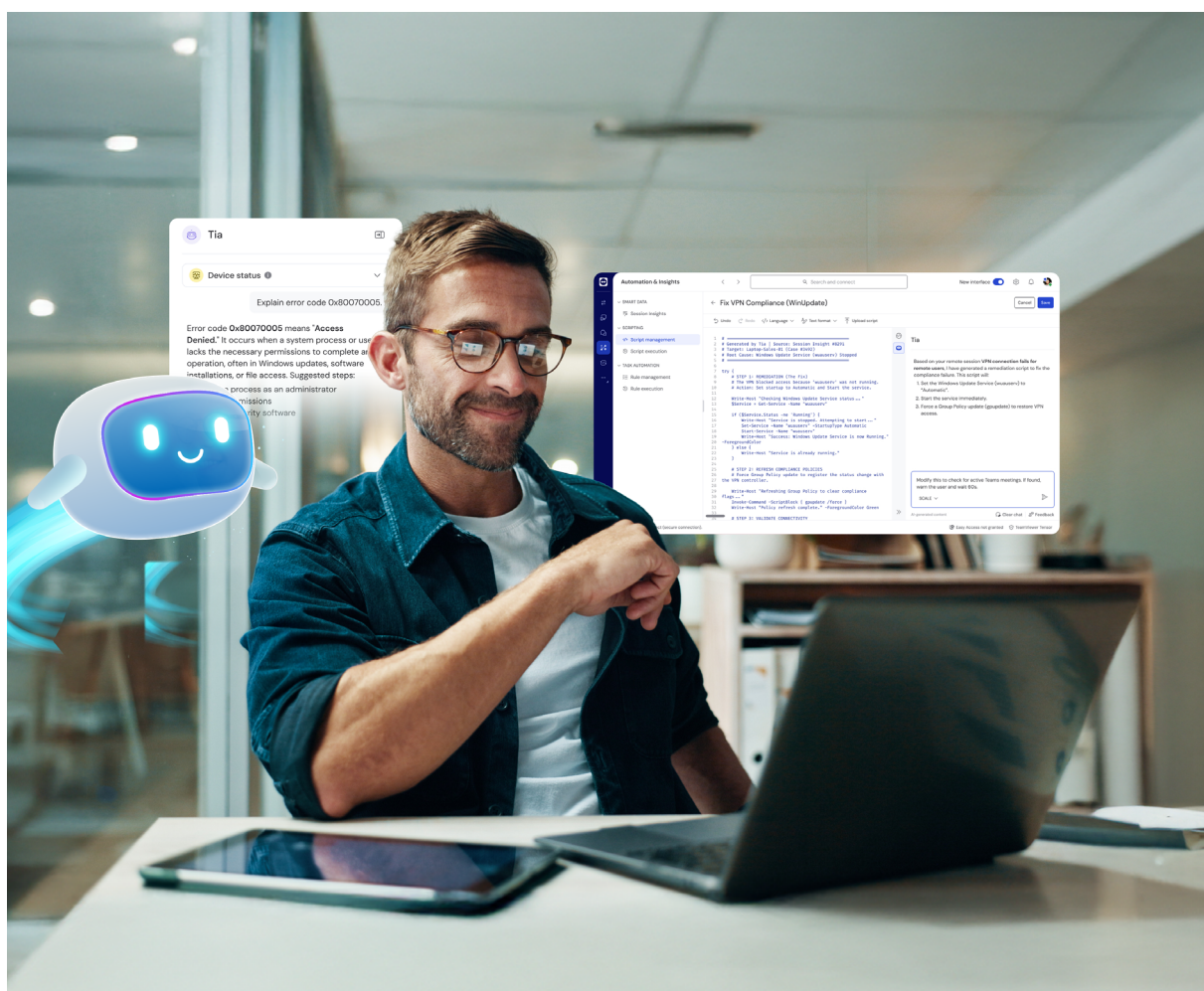
Die Unterstützung durch KI beschleunigt die Skripterstellung, indem die gewonnenen Erkenntnisse aus vorherigen Sessions für die Erstellung wiederverwendbarer Automatisierungen genutzt werden. Erstellung und Ausführung von Skripten lassen sich durchgängig durch Berechtigungen und etablierte Workflows kontrollieren.

Kontrolle durch Admins

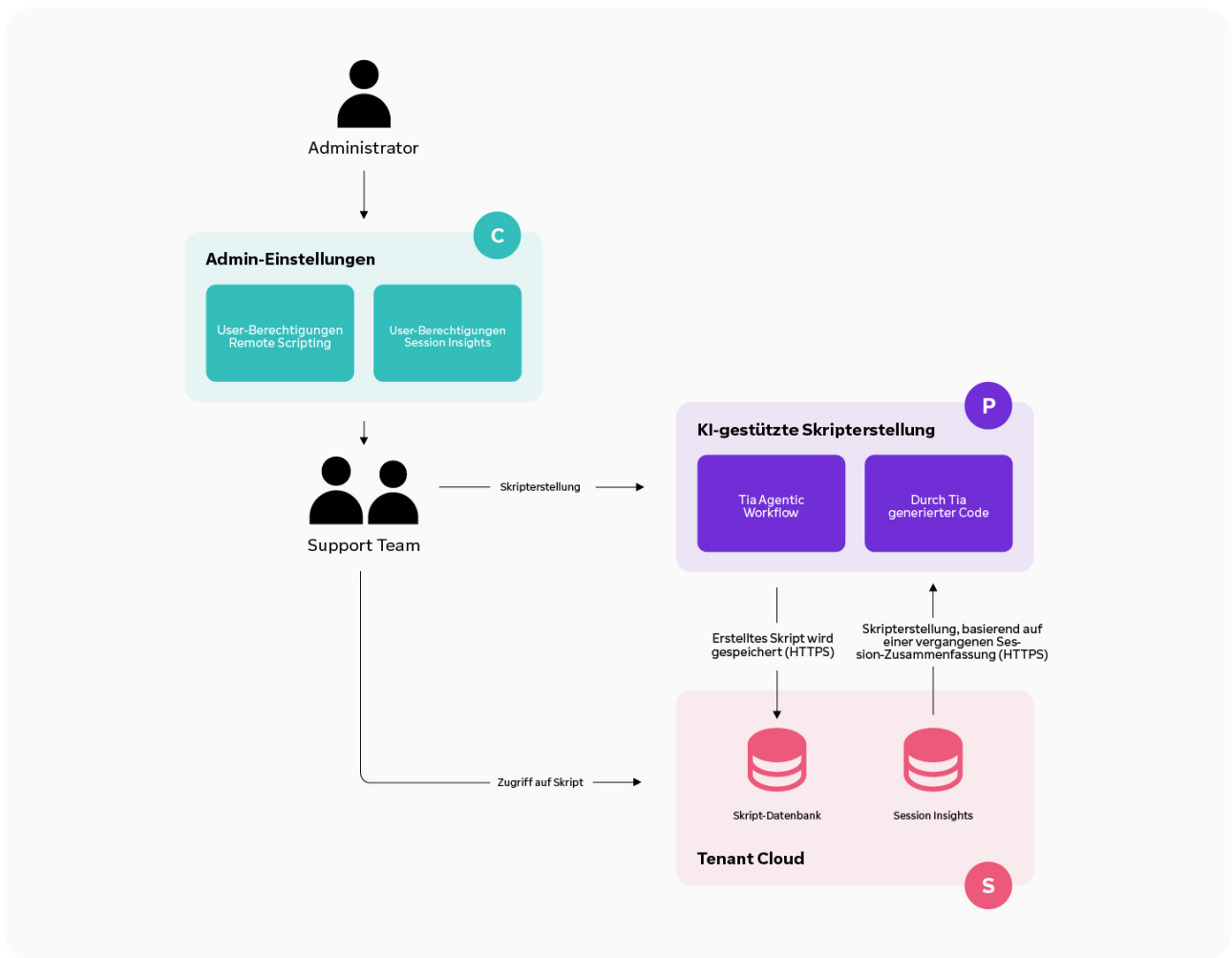
Admins steuern den Zugriff über die Auswahl von Berechtigungen für Remote Scripting und Sessions Insights und stellen sicher, dass Skripte ausschließlich von autorisierten Mitarbeitenden erstellt und verwendet werden können.

Erstellung, Speicherung und Ausführung von Skripten

- Support-Teams lösen die KI-gestützte Skripterstellung aus; Skripte können anhand von Eingabeaufforderungen (Prompts) und/oder vorherigen Session Insights erstellt werden.
- Erstellte Skripte werden für die Prüfung und Wiederverwendung in der Script Database der Tenant-Cloud gespeichert.
- Die Ausführung von Skripten ist nur mit entsprechenden Berechtigungen möglich und erfolgt über Workflows für Remote Scripting.



KI-gestützte Skripterstellung (Session Insights und Tia)



Dieses Diagramm zeigt, wie die Skripterstellung durch über die Admin-Einstellungen festlegbare Berechtigungen (K) kontrolliert wird, wie die KI-gestützte Skripterstellung den Workflow von Tia mit der Codegenerierung (V) verbindet und wie erstellte Skripte in der Skript-Datenbank der Tenant-Cloud gespeichert werden oder optional auf Grundlage vergangener Session Insights initiiert werden können. Beides wird als Tenant-Cloud-Ressource geschützt (S). Skripte bleiben zur Überprüfung verfügbar und werden über berechtigungsbasiertes Remote Scripting ausgeführt.

Legende (Buchstaben stehen für die jeweiligen Services der TeamViewer KI Plattform).



K Kontrollieren (Admin-Richtlinien & -Berechtigungen)



S Schützen (Verschlüsselung & Speicherung)



V Verarbeiten (LLM-Services)

Verfügbarkeit von Features

- TeamViewer ONE: Standard, Advanced, Enterprise

Häufig gestellte Fragen

Welche Daten sammelt und verarbeitet TeamViewer KI?

Ihre Admins können Rollout und Zugriff über Einstellungen, Berechtigungen und Richtlinien kontrollieren. Welche Daten genau gesammelt und verarbeitet werden, kommt auf den jeweiligen KI-Workflow an:

Session Insights (Dokumentation): Es werden Session-Interaktionen aufgezeichnet, die für die Erstellung von Zusammenfassungen und der Auflistung durchgeführter Aktionen benötigt werden. Diese Aufzeichnungen werden vor der weiteren Verarbeitung anonymisiert.

Tia (Problembehebung): Zu Beginn der Session wird ein eingeschränkter Einblick in die technischen Gerätedaten genutzt. Screenshots werden nur auf explizite Aufforderung der User aufgenommen. Zusätzlich werden vergangene Gespräche mit Tia sowie berechtigungsbasierte Session Insights verwendet. Es werden keinerlei User-Inhalte, persönliche Dokumente, Kommunikationsdaten, Tastaturanschläge oder Aktivitätsdaten aufgezeichnet.

KI-gestützte Skripterstellung: Zur Erstellung von Skriptentwürfen werden die Anweisungen (Prompts) des Users sowie optional Kontext aus früheren Session Insights verwendet.

Wo werden die KI-Daten verarbeitet?

Session-Daten werden direkt im TeamViewer Client aufgezeichnet und mithilfe eines regelbasierten Prozesses anonymisiert. Sensible Bestandteile (wie E-Mail-Adressen, Passwörter, Kreditkartennummern und IP-Adressen) werden entfernt, bevor die Daten das Endgerät verlassen. Die Daten werden in den cloudbasierten Services weiter anonymisiert.

Werden Session-Daten extern verarbeitet oder mit Drittunternehmen geteilt?

Ja. TeamViewer nutzt die LLM-Services von Dritten (Azure OpenAI und Google Gemini) unter vordefinierten Bedingungen, um die eigene KI bereitstellen zu können. Im Falle der Session Insights werden die Daten vor der weiteren Verarbeitung anonymisiert. Für den Workflow wird eine verschlüsselte Übertragung genutzt (HTTPS/TLS).

Welche Unterauftragsverarbeitenden nutzt TeamViewer für KI, und wo finde ich die offizielle Liste?

Eine Liste mit den Details und Bedingungen unserer Unterauftragsverarbeitenden finden Sie hier: <https://teamviewer.scene7.com/is/content/teamviewergmbh/teamviewer/central-image-hub/pdf/en/teamviewer-third-party-terms-en.pdf>.

Sind die Daten meiner Kundschaft während der Übertragung und im Ruhezustand verschlüsselt?

Ja.

- **Während der Übertragung:** Für die Übertragung zwischen TeamViewer Clients, Cloud-Services, Cloudspeicher und KI-Services werden die Daten mit HTTPS (TLS) verschlüsselt (wie in der Abbildung zur Session-Insights-Architektur gezeigt).
- **Im Ruhezustand:** Für den Cloudspeicher wird die branchenübliche AES-256-Verschlüsselung genutzt.
- **Zusätzlicher Schutz:** Die Daten der Session Insights und von Tia werden zusätzlich über clientseitige Verschlüsselung (CSE) geschützt.

Wie werden die Verschlüsselungscodes geschützt (kontrolliertes Key Management)?

Für Session Insights und Tia wird ein Public Key verwendet, den der Client per HTTPS abgerufen hat. Der zugehörige Private Key wird verschlüsselt gespeichert und zusätzlich durch einen Schlüssel gesichert. Dieser wird in einem zertifizierten Hardware-Sicherheitsmodul (HSM) aufbewahrt. Vor der Nutzung wird der Private Key innerhalb des HSM sicher entpackt. Alle HSM-Prozesse werden vollständig überwacht.

Wo werden meine Daten gespeichert?

Session Insights: Ergebnisse (Zusammenfassungen/durchgeführte Aktionen) werden in der Tenant-Cloud gespeichert, der Zugriff lässt sich über die User-Berechtigungen in den Admin-Einstellungen kontrollieren.

KI-gestützte Skripterstellung: Erstellte Skripte werden für die Prüfung, Wiederverwendung und kontrollierte Ausführung in der Script Database der Tenant-Cloud gespeichert.

Wie lange werden meine Daten gespeichert?

Wir speichern Ihre Daten für die Dauer Ihres Vertrages mit uns oder bis Sie sich entscheiden, diese bereits früher zu löschen. Gespeicherte, mit KI zusammenhängende Artefakte wie Session Insights und Skripte können jederzeit in den Admin-Einstellungen gelöscht werden.

Was geschieht nach Beendigung des Vertrags mit meinen Daten?

Wenn Sie Ihren Vertrag kündigen, können Sie Ihre Daten gemäß den geltenden Bestimmungen, darunter dem EU Data Act (EU-Datenverordnung), exportieren oder extrahieren. Nach Vertragsende behandelt TeamViewer die verbleibenden Daten gemäß dem vereinbarten Prozess zur Aufbewahrung und Löschung von Daten sowie den relevanten rechtlichen und vertraglichen Aufbewahrungsbestimmungen.

Was passiert mit entschlüsselten Daten während der Verarbeitung?

Die Daten werden auf dem Gerät anonymisiert, bevor sie zur Verarbeitung freigegeben werden. Eine zusätzliche Anonymisierung erfolgt in den cloudbasierten Systemen. Vor und nach der Nutzung der cloudbasierten Services verbleiben die Daten in verschlüsselter Form. Eine Entschlüsselung findet nur statt, wenn sie technisch notwendig ist, um die gewünschten Ergebnisse zu erzielen. Über die Service-Bereitstellung hinaus werden keine Daten in entschlüsselter Form aufbewahrt.

Werden unsere Daten für das Training von KI-Modellen genutzt?

Nein. TeamViewer nutzt keine User-Daten, um KI-Modelle zu trainieren. Sollte TeamViewer jemals in Betracht ziehen, die eigenen KI-Modelle mit anonymisierten Daten zu trainieren, würde das nur im Rahmen strenger Sicherheitsmaßnahmen, umfassender Transparenz für unsere Kundschaft und Aktualisierungen unserer Dokumentation und Nutzungsbedingungen geschehen.

Jede Veränderung in dieser Richtung würde sich in unserer Dokumentation sowie in unseren Nutzungsbedingungen widerspiegeln.

Können meine Prompts (Eingaben) / Outputs (Ergebnisse) von anderen verwendet oder dafür genutzt werden, externe Modelle zu verbessern?

Prompts und Outputs werden ausschließlich in der Service-Umgebung von TeamViewer verarbeitet und nicht mit anderen Usern geteilt. Sie werden auch nicht dafür genutzt, externe KI-Modelle zu trainieren oder zu verbessern. TeamViewer nutzt vollständig anonymisierte Daten, um die Leistung und Zuverlässigkeit der eigenen Services überwachen zu können, wobei zu jedem Zeitpunkt angemessene Sicherheitsmaßnahmen eingehalten werden.

Welche Informationsquellen nutzt Tia?

Tia nutzt Informationen aus der TeamViewer Umgebung. Unter anderem:

- Zu Beginn der Session wird automatisch ein Einblick in die technischen Daten des betreffenden Geräts vorgenommen
- Screenshots, wenn diese von Usern explizit ausgelöst werden
- Während der Session entstandener Gesprächskontext
- Vergangene Session Insights, sofern User über entsprechende Zugriffsrechte verfügen

Warum kann Tia Fragen zu CPU, Arbeitsspeicher und anderen Systemressourcen beantworten?

Diese Informationen sind Teil der Gerätedaten, die Tia während einer Session erhält.

Kann Tia installierte Anwendungen oder das Geräteinventar einsehen?

Um die Problembehebung unterstützen zu können, erhält Tia zu Beginn einer Session automatisch einen eingeschränkten Einblick in die technischen Daten des Geräts. Diese Daten können Folgendes beinhalten:

- **Informationen über Hardware:** Unter anderem Gerätemodell, Hersteller, Seriennummer, CPU, Arbeitsspeicher, Grafikkarteninformationen, Monitore, Netzwerkadapter und aktuelle BIOS-Version
- **Informationen zum Betriebssystem:** Unter anderem Name, Version, Build, Sprach- und Regionseinstellungen, Zeitzone und Systemverfügbarkeit
- **Installierte Software und Treiber:** Unter anderem die Namen von Anwendungen und Treibern, deren Versionen, Hersteller und Installationsdatum
- **Informationen zu Systemdiensten:** Unter anderem Name, Typ und Status
- **Informationen zum Zustand von Netzwerk und Sicherheit:** Unter anderem Adaptertyp/-modell, lokale IP-Adresse/lokales Subnetz und Firewallstatus
- **Informationen zu Akku- und Gerätestatus,** wie Akkuladestand und Gerätebetriebszeit
- **Nicht personenbezogene Geräteeinstellungen,** wie ausgewählte Sprache und Zeitzone
- Nicht enthalten sind User-Inhalte, persönliche Dokumente, Kommunikationsdaten, Tastenanschläge oder Aktivitätsdaten.

Sammelt Tia Informationen automatisch oder nur auf Anfrage?

Zu Beginn jeder Session erhält Tia einen eingeschränkten Einblick in die Gerätedaten, der technische Informationen zu Systemen und Einstellungen enthält. Diese Informationen werden für die Problembehebung benötigt. Zusätzliche Informationen, wie zum Beispiel Screenshots, werden nur abgerufen, wenn User dies explizit anfordern.

Führen die KI-Features Aktionen automatisch durch oder wird dafür menschliche Zustimmung benötigt?

Keines der KI-Features führt automatische Aktionen auf Geräten aus. Tia besitzt keinen Echtzeit-Zugriff auf Geräte, auch keinen Lesezugriff. Tia operiert nur auf Basis eines zu Beginn einer Session vorgenommenen, eingeschränkten Einblicks in die technischen Gerätedaten. Screenshots werden ausschließlich auf explizite Anforderung von Usern aufgenommen. Tia kann Anleitungen und Empfehlungen bereitstellen, aber keinen Code ausführen, keine Software installieren und keine Systemänderungen durchführen.

Im Rahmen des Workflows zur Skripterstellung kann die TeamViewer KI Skriptentwürfe bereitstellen. Die Ausführung der Skripte ist jedoch Usern vorbehalten und erfolgt innerhalb freigegebener Workflows. Skripte werden zur Überprüfung gespeichert und können ausschließlich über das berechtigungsbasierte Remote Scripting ausgeführt werden.

Lässt sich die KI vollständig deaktivieren?

Die KI-Funktionen lassen sich in den KI-Admin-Einstellungen aktivieren oder deaktivieren.

Kann die KI-Nutzung nach Usern, Geräten oder Gruppen eingeschränkt werden?

Ja. Admins können die KI-Nutzung in den Admin-Einstellungen durch Zugriffsbeschränkungen genau kontrollieren:

- **Nach User oder Rolle:** Über die User-Berechtigungen lässt sich einstellen, wer auf KI-Features und KI-produzierte Inhalte zugreifen kann.
- **Nach Gerät oder Gruppe:** Mithilfe von Richtlinien lässt sich einstellen, welche Features aktiviert oder deaktiviert sind (zum Beispiel können bestimmte Geräte oder Gerätegruppen von der Datenerhebung durch Session Insights ausgeschlossen werden).
- **Nach Feature:** In den Admin-Einstellungen lassen sich die einzelnen KI-Funktionen aktivieren oder deaktivieren.

Dies ermöglicht es unserer Kundschaft, TeamViewer KI gemäß dem Prinzip der geringsten Privilegien und in Übereinstimmung mit den internen Governance-Anforderungen zu nutzen.

Wie lässt sich die KI überprüfen?

Sie können die Ergebnisse mithilfe kontrollierter Artefakte validieren:

- Session Insights Zusammenfassungen/durchgeführte Aktionen (berechtigungs basiert).
- Generierte Skripte, die in der Skript-Datenbank gespeichert werden (überprüfbar/wiederverwendbar).
- Der Kontext von Tia ist auf die definierten Eingabequellen beschränkt (Gesprächskontext, Gerätedaten, von Usern angeforderte Screenshots, genehmigte Session Insights).

Kann Tia auf Daten zugreifen, die Supporter nicht sehen können?

Tia hat nur Zugriff auf eine klar definierte Zusammenstellung technischer Gerätedaten, sowie auf von Usern ausgelöste Screenshots und Gespräche, die während der Session stattgefunden haben. Der Zugriff auf Session Insights ist je nach Berechtigung ebenfalls möglich. Tia zeichnet keine User-Inhalte, persönlichen Dokumente, Kommunikationsdaten, Tastenanschläge oder Aktivitätsdaten auf. Die von Tia genutzten Gerätedaten entsprechen dem, worauf Supporter in einer standardmäßigen Support-Session ebenfalls zugreifen können.

Wie wird sichergestellt, dass die KI-Features der DSGVO entsprechen?

Dies wird durch eine mehrstufige Anonymisierung (sowohl auf dem Gerät als auch in der Cloud), Datenminimierung und Steuerungsmöglichkeiten für Admins erreicht. Mit diesen lassen sich das Rollout von und der Zugriff auf KI-Inhalte kontrollieren.

Gibt es eine Dokumentation im Sinne des EU-Gesetzes zur künstlichen Intelligenz (EU AI Act)?

Sie können die Dokumentationen über das TeamViewer Trust Center anfragen: compliance.teamviewer.com.

Wo finde ich Sicherheitsdokumentationen (AVV, ISO, SOC)?

Sie können die Dokumentationen über das TeamViewer Trust Center anfragen: compliance.teamviewer.com.

Nutzt TeamViewer ein Managementsystem für künstliche Intelligenz?

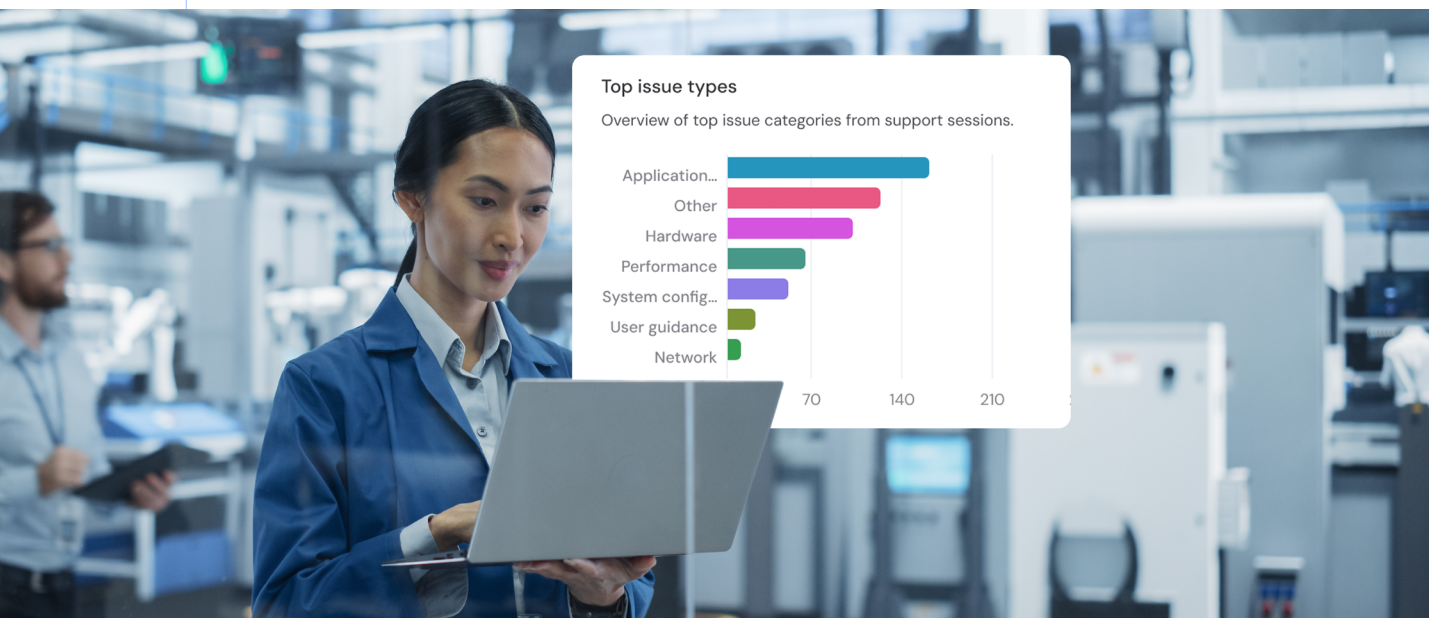
Ja, TeamViewer nutzt ein an der IEC 42001 ausgerichtetes Managementsystem für künstliche Intelligenz (AIMS). Die Zertifizierung wird derzeit durchgeführt (und ist zum jetzigen Zeitpunkt noch nicht abgeschlossen).

Als Teil des eigenen Softwareentwicklungslebenszyklus folgt TeamViewer zusätzlich anerkannten Best Practices für den sicheren Umgang mit KI. Das schließt Richtlinien von OWASP (einschließlich der relevanten Richtlinien für LLM-Sicherheit), NIST, CIS sowie Empfehlungen der Cloud Security Alliance (CSA) für KI-Sicherheit und -Governance mit ein.

Wie verhindert TeamViewer den Missbrauch seiner KI-Modelle oder Prompt-Injection-Angriffe?

TeamViewer nutzt einen mehrstufigen Sicherheitsansatz, um die Risiken von Zweckentfremdung und Missbrauch der eigenen KI-Funktionen zu reduzieren. Je nach Workflow können die folgenden Sicherheitsmaßnahmen zum Einsatz kommen:

- Schutzmaßnahmen gegen Prompt-Injection-Angriffe und Jailbreaks
- Maßnahmen zur Abschwächung von Halluzinationen (zum Beispiel Einschränkungen beim Tool-Zugriff)
- Durchsatzratenbegrenzung, Missbrauch-Erkennung und Monitoring
- Protokolle zur Unterstützung von Ermittlungen und Governance-Maßnahmen
- Mechanismen für menschlichen Eingriff und Zustimmung, zum Beispiel berechtigungsbasierte Ausführung von Skripten





Über TeamViewer

TeamViewers Digital-Workplace-Plattform ermöglicht effizientes, digitales Arbeiten durch die Optimierung und Automatisierung von Prozessen.

Was 2005 als Software für den Fernzugriff auf Computer begann, um Dienstreisen zu vermeiden und Produktivität zu steigern, entwickelte sich schnell zum branchenweiten Inbegriff von Fernwartung und IT-Support; und wird von hunderten Millionen Menschen weltweit zur Unterstützung bei IT-Problemen genutzt. Heute vertrauen mehr als 640.000 Personen und Unternehmen weltweit auf TeamViewer – von kleinen und mittelständischen Betrieben bis hin zu großen Konzernen – um digitale Arbeitsplätze für Büroangestellte und Industriefachkräfte effizienter zu gestalten.

Unternehmen aus allen Branchen nutzen die KI-gestützten Lösungen von TeamViewer, um Störungen an digitalen Endgeräten jeder Art zu verhindern und zu beheben, IT-Netzwerke und Industrieanlagen effizient zu verwalten und Prozesse mit Augmented-Reality-Funktionen zu optimieren. Auch dank der Integrationen mit führenden Technologielösungen hilft TeamViewer seiner Kundschaft dabei, Ausfallzeiten zu reduzieren, IT-Probleme schneller zu lösen und digitale Arbeitsabläufe zu verbessern. In einer Zeit des globalen Wandels – geprägt von hybriden Arbeitsmodellen, neuen Technologien und Fachkräftemangel – bietet TeamViewer einen klaren Mehrwert: höhere Produktivität, schnellere Einarbeitung neuer Talente und eine gesteigerte Zufriedenheit von Kundschaft und Mitarbeitenden.

TeamViewer hat seinen Hauptsitz in Göppingen, Deutschland, und beschäftigt weltweit über 1.800 Mitarbeitende. Im Jahr 2024 erzielte das Unternehmen einen Umsatz von rund 671 Millionen Euro. Die TeamViewer SE (TMV) ist an der Frankfurter Börse gelistet und gehört zum MDAX. Mehr Informationen unter www.teamviewer.com.

www.teamviewer.com/support

TeamViewer Germany GmbH
Bahnhofsplatz 2, 73033 Göppingen,
Deutschland
+49 (0) 7161 60692 50

TeamViewer US Inc.
5741 Rio Vista Dr Clearwater, FL 33760 USA
+1 800 638 0253

Stets sicher verbunden



www.teamviewer.com

Copyright © 2026 TeamViewer Germany GmbH und TeamViewer US. Alle Rechte vorbehalten.