ScreenConnect: Remote-Support clever und sicher meistern

Category: Online-Marketing
geschrieben von Tobias Hager | 7. Februar 2026

ScreenConnect: Remote-Support clever und sicher meistern

Dein Kunde hat ein Problem. Du hast die Lösung. Aber dazwischen liegt ein Dschungel aus Firewalls, Sicherheitsbedenken und unzuverlässigen Tools. Willkommen in der Welt des Remote-Supports – wo jede Sekunde zählt und jedes Klick zu einem Sicherheitsrisiko werden kann. Wenn du denkst, TeamViewer sei die einzige Option, hast du ScreenConnect noch nicht kennengelernt. Zeit,

aufzuräumen – technisch, sicher und kompromisslos effizient.

- Was ScreenConnect ist – und warum es sich von klassischen Remote-Tools unterscheidet
- Warum Remote-Support 2025 neu gedacht werden muss – Stichwort: Sicherheit und Datenschutz
- Technische Architektur von ScreenConnect im Detail analysiert
- Wie du ScreenConnect sicher und DSGVO-konform einsetzt
- Welche Rollen Authentifizierung, Verschlüsselung und Netzwerkarchitektur spielen
- ScreenConnect vs. TeamViewer, AnyDesk & Co. – der brutale Vergleich
- Wie du ScreenConnect in deine IT- und Support-Prozesse integrierst
- Best Practices für IT-Dienstleister, Agenturen und Tech-Support-Teams
- Schritt-für-Schritt-Setup von ScreenConnect mit Sicherheitsfokus
- Warum ScreenConnect genau das Tool ist, das du schon gestern gebraucht hättest

Was ist ScreenConnect? Remote-Support mit Fokus auf Sicherheit und Kontrolle

ScreenConnect – inzwischen unter dem Branding ConnectWise Control bekannt – ist ein leistungsstarkes Remote-Support-Tool, das sich an professionelle IT-Abteilungen, Managed Service Provider (MSPs) und Unternehmen richtet, die Remote-Zugriffe nicht nur brauchen, sondern vollständig kontrollieren müssen. Anders als bei Mainstream-Lösungen wie TeamViewer oder AnyDesk steht bei ScreenConnect nicht der Komfort für Endnutzer im Vordergrund, sondern die technische und sicherheitsrelevante Integrität des gesamten Remote-Zugangsprozesses.

ScreenConnect ist kein „Install-and-forget“-Tool. Es ist eine eigenständig hostbare Lösung, die sowohl On-Premise als auch als Cloud-Service betrieben werden kann. Das macht es besonders interessant für Unternehmen mit strengen Compliance-Vorgaben oder einem hohen Sicherheitsanspruch. Du willst volle Kontrolle über Ports, Zertifikate, Authentifizierung und Logs? ScreenConnect liefert.

Remote-Support ist 2025 kein Add-on mehr, sondern ein essenzieller Bestandteil von IT-Service-Architekturen. Die Anforderungen steigen: DSGVO, ISO27001, NIS2 – wer Remote-Zugriffe nicht sauber absichert, riskiert mehr als nur schlechte Presse. ScreenConnect adressiert genau diese Schwachstellen mit granularen Berechtigungssystemen, Zwei-Faktor-Authentifizierung, rollenbasiertem Zugriff und vollständiger Protokollierung aller Sitzungen.

Ob du Support für Kunden leistest, Admin-Zugriffe auf Server brauchst oder Remote-Training durchführst: ScreenConnect bietet dir eine Plattform, die skalierbar, auditierbar und sicher ist. Und genau das unterscheidet es vom Rest. Willkommen im Remote-Support, wie er 2025 sein muss – nicht wie er 2015

war.

Remote-Support 2025: Warum Sicherheit das neue Killerfeature ist

Remote-Zugriffe galten jahrelang als notwendiges Übel – irgendwie notwendig, aber nie wirklich sicher. Doch spätestens seit der Pandemie und dem massiven Anstieg an Homeoffice-Arbeitsplätzen ist klar: Remote-Support ist keine Ausnahme mehr, sondern Alltag. Und dieser Alltag muss sicher sein. Denn mit jedem Zugriff, den du ermöglichst, öffnest du ein Tor in dein Netzwerk. Wer das nicht versteht, hat im Support nichts verloren.

Die Bedrohungslage hat sich verändert. Phishing, Credential Stuffing, Session Hijacking – die Angriffsvektoren sind vielfältig und entwickeln sich schneller als viele IT-Abteilungen reagieren können. Ein unsicherer Remote-Zugang ist heute keine Schwachstelle mehr, sondern ein Einfallstor mit Totalschaden-Potenzial. Und genau deshalb muss Remote-Support neu gedacht werden: nicht als Komfortfunktion, sondern als sicherheitskritische Infrastruktur.

ScreenConnect geht diesen Weg konsequent. Das beginnt bei der SSL-Verschlüsselung aller Datenströme, geht über granular konfigurierbare Rollen- und Rechtekonzepte bis hin zur vollständigen Audit-Fähigkeit jeder einzelnen Sitzung. Jeder Mausklick, jede Dateiübertragung, jede Authentifizierung – alles wird geloggt, versioniert und auf Wunsch in externe SIEM-Systeme integriert. Das ist kein Spielzeug. Das ist Enterprise-Grade Security.

Auch die DSGVO spielt eine zentrale Rolle. Wer personenbezogene Daten remote verarbeitet oder einsehen kann, muss Rechenschaft ablegen – und zwar technisch nachvollziehbar. ScreenConnect ermöglicht die Einrichtung von Zustimmungserklärungen vor Zugriff, Sitzungsaufzeichnungen und individuelle Zugriffsebenen. Damit ist die Einhaltung der Datenschutzrichtlinien nicht nur ein Versprechen, sondern ein Feature.

Fazit: Wer 2025 noch Support über Tools ohne Audit-Logging, ohne 2FA und ohne zentrale Rechteverwaltung anbietet, handelt fahrlässig – und zwar nicht nur gegenüber Kunden, sondern auch gegenüber dem eigenen Ruf.

ScreenConnect Architektur verstehen: On-Premise, Cloud

und Hybrid

Einer der größten Vorteile von ScreenConnect ist die Flexibilität in der technischen Bereitstellung. Du willst alles in der eigenen Infrastruktur betreiben? Kein Problem. Du bevorzugst die Cloud wegen Skalierbarkeit und Verfügbarkeit? Ebenfalls möglich. Oder du brauchst ein Hybrid-Modell mit eigener Authentifizierung und Cloud-Routing? Auch das lässt sich konfigurieren – und zwar bis in die tiefsten Layer.

Die On-Premise Variante von ScreenConnect ist besonders für Unternehmen interessant, die vollständige Kontrolle über ihre Infrastruktur benötigen. Du installierst die Server-Komponente auf einem eigenen Host, konfigurierst SSL/TLS-Zertifikate selbst, bestimmst Firewall-Regeln, Ports und Netzwerkzugriffe unabhängig. Das bedeutet: Kein externer Datenfluss, keine Abhängigkeit von Drittanbietern, volle Kontrolle über Logging und Compliance.

Die Cloud-Variante, betrieben von ConnectWise, bietet dagegen eine sofort einsatzfähige Lösung mit skalierbarer Infrastruktur. Ideal für kleinere Support-Teams oder Unternehmen, die nicht die Ressourcen für ein eigenes Hosting mitbringen. Auch hier sind alle Sicherheitsfeatures aktiv – aber du gibst einen Teil der Infrastrukturkontrolle ab. Dafür bekommst du automatische Updates, Redundanz und eine weltweit erreichbare Plattform.

Technisch basiert ScreenConnect auf einem WebSocket-basierten Kommunikationsprotokoll, das eine persistente Verbindung zwischen Host und Client ermöglicht. Das garantiert niedrige Latenzen, hohe Verbindungsstabilität und schnelle Reaktionszeiten. Die gesamte Kommunikation ist durch TLS verschlüsselt, die Authentifizierung erfolgt wahlweise über AD, LDAP, SAML oder lokale Benutzerkonten – inklusive 2FA mit TOTP oder Hardware-Token.

Die Clients (sowohl Host als auch Gast) sind für Windows, macOS und Linux verfügbar, ebenso wie Browser-basierte Clients. Mobile Apps existieren für iOS und Android. Und für Entwickler: Die API ist vollständig dokumentiert und erlaubt tiefe Integration in bestehende ITSM-, RMM- oder Monitoring-Systeme.

ScreenConnect sicher konfigurieren: Schritt-für-Schritt

Remote-Support ohne Sicherheitskonzept ist wie ein Haus ohne Türschloss. Deshalb hier die wichtigsten Schritte, wie du ScreenConnect sicher, DSGVO-konform und performant einrichtest:

- 1. Deployment wählen: Entscheide dich für On-Premise oder Cloud. Für maximale Kontrolle empfiehlt sich On-Premise – idealerweise hinter einem Reverse Proxy mit TLS-Termination.

- 2. SSL/TLS aktivieren: Nutze ein valides Zertifikat (z. B. via Let’s Encrypt oder eine interne CA). Kein Self-Signed-Zertifikat im Produktivbetrieb – das ist 2025 ein No-Go.
- 3. Benutzerverwaltung aufsetzen: Integriere AD/LDAP oder nutze SAML für zentrale Authentifizierung. Aktiviere Zwei-Faktor-Authentifizierung für alle Benutzer – Pflicht, kein Bonus.
- 4. Rollen und Rechte definieren: Erstelle granulare Rollen für Supporter, Admins, Auditoren etc. Vermeide globale Admin-Rechte für alle – das ist ein Einfallstor.
- 5. Logging und Auditing aktivieren: Aktiviere Sitzungstranskripte, Dateiübertragungsprotokolle und opt. Videoaufzeichnung. Exportiere Logs regelmäßig in zentrale SIEM-Systeme.
- 6. Datenschutzmaßnahmen implementieren: Zeige Nutzern vor Zugriff eine Einwilligungserklärung an. Dokumentiere Zustimmung und speichere sie revisionssicher.
- 7. Firewall-Regeln konfigurieren: Erlaube nur notwendige Ports. Nutze geo-basierte IP-Filter, wenn möglich. Keine offenen Ports ohne Monitoring.

ScreenConnect bietet für alle diese Schritte die notwendigen Konfigurationsmöglichkeiten – direkt im Admin-Backend oder über die Konfigurationsdateien. Wer hier schlampig arbeitet, verliert nicht nur Sicherheitslevel, sondern auch Vertrauen. Remote-Support ist Vertrauen – und das beginnt bei der Technik.

ScreenConnect im Vergleich: Warum TeamViewer alt aussieht

TeamViewer hat den Markt für Remote-Zugriffe geprägt – keine Frage. Aber was 2010 innovativ war, ist 2025 oft ein Sicherheitsrisiko. Die meisten “Klick-und-los”-Lösungen setzen auf Komfort statt Kontrolle. Und genau hier punktet ScreenConnect mit einer Architektur, die Sicherheit, Auditierbarkeit und Integration in Unternehmensprozesse in den Mittelpunkt stellt.

Im direkten Vergleich fällt auf: Während TeamViewer und AnyDesk primär für spontane Sessions zwischen zwei Endpunkten konzipiert sind, bietet ScreenConnect eine vollständige Plattform für dauerhafte Fernwartung, Asset-Management, rollenbasierten Zugriff und Integration in ITSM-Prozesse. Es ist nicht nur ein Tool, sondern ein System.

Auch in Sachen Sicherheit ist ScreenConnect weiter: Vollständiges Session-Logging, Unterstützung für Hardware-Token, detaillierte Rechtevergabe, vollständige On-Premise-Fähigkeit – das alles sucht man bei vielen Mitbewerbern vergeblich. Wer ein ISO-zertifiziertes Unternehmen betreut oder mit kritischen Infrastrukturen arbeitet, braucht genau das.

Klar, ScreenConnect ist kein Tool für Oma Erna, die Hilfe beim Router braucht. Es ist ein Enterprise-Werkzeug, das technisches Know-how voraussetzt – und genau deshalb in professionellem Umfeld überzeugt. Wer ernsthaft

Support betreibt, braucht mehr als eine schnelle Verbindung. Er braucht Kontrolle, Nachvollziehbarkeit und Sicherheit. Genau das liefert ScreenConnect – kompromisslos.

Fazit: ScreenConnect ist Remote-Support, wie er heute sein muss

Remote-Support ist keine Nebensache mehr, sondern Teil deiner technischen DNA. Und ScreenConnect ist das Tool, das diese DNA schützt, optimiert und skalierbar macht. Es ist technisch robust, sicherheitsfokussiert und voll integrierbar – genau das, was du brauchst, wenn du nicht nur Probleme lösen, sondern Vertrauen aufbauen willst.

TeamViewer war gestern. ScreenConnect ist heute – und morgen. Wer 2025 noch auf Tools setzt, die keine Audit-Trails, keine 2FA und keine On-Premise-Option bieten, spielt Support-Roulette. Und verliert. Du willst Remote-Support richtig machen? Dann hör auf zu improvisieren – und fang an, zu kontrollieren. Mit ScreenConnect.