computing research

FORSCHUNGSPAPIER

Remote Access und Support für Unternehmen: Ist es für Sie an der Zeit, eine moderne und sichere Konnektivitätslösung einzuführen?

Gefördert durch

TeamViewer

INHALTSVERZEICHNIS

Einführung

Unternehmen benötigen heutzutage Lösungen für Remote-Konnektivität, die skalierbar sind und mit denen sie gleichzeitig keine Abstriche bei ihrer Sicherheit machen müssen. Ob bei der Arbeit von zu Hause aus oder unterwegs, Mitarbeitende, Kunden und Kundinnen sowie geschäftliche Kontakte verlassen sich auf sicheren Remote Access, um Prozesse effektiv und effizient am Laufen zu halten.

Heutzutage haben Perimeter-basierte Sicherheitskonzepte ausgedient und Cybersicherheitsstrategien, denen das Zero-Trust-Modell zugrunde liegt, werden immer mehr zum Standard. Aufgrund dessen erfüllen VPNs nicht mehr die Anforderungen, die eine über den gesamten Globus verstreute Belegschaft an Unternehmen stellt. Angesichts eines zunehmend komplexer werdenden Umfelds, das von Cyberangriffen, Ausfällen sowie Ressourcen- und Fachkräftemangel geprägt ist, stehen Unternehmen unter dem Druck, produktive hybride Arbeitsumgebungen bereitstellen zu müssen. Wie begegnen IT-Entscheidungsträgerinnen und -Entscheidungsträger dieser Herausforderung?

Dieses Whitepaper untersucht die Herausforderungen, denen sich 125 IT-Führungskräfte stellen müssen, wenn es um aktuelle Trends wie hybride Arbeitsmodelle, die Reduzierung von CO2-Emissionen, globale Konnektivität sowie Robotik und Automatisierung geht. Unter den Befragten sind IT-Direktoren und -Direktorinnen, IT-Bereichsleitende, CIOs und CTOs aus verschiedenen Branchen wie dem Bankensektor, Fertigungsbereich, Gesundheitswesen und Behörden.

Wichtigste Erkenntnisse

Unternehmen setzen weiterhin unterschiedliche Arbeitsmodelle ein: Über 95 Prozent der Befragten arbeiten hybrid oder vollständig remote.

Rund 90 Prozent der Befragten stimmen zu, dass eine moderne Konnektivitätsplattform in der heutigen zunehmend hybriden digitalen Wirtschaftswelt unerlässlich ist.

Etwa ein Drittel der Unternehmen setzt eine moderne, sichere Konnektivitätslösung für Remote Access und Support ein.

Über 95 Prozent der Unternehmen sind zumindest daran interessiert, eine solche Lösung einzuführen.

Was sie dazu motiviert, sind Faktoren wie garantierte Flexibilität, Sicherheit und bessere Leistungen durch weniger Ausfälle.

Weniger als eines von vier Unternehmen gibt an, von ihrer aktuellen Konnektivitätslösung völlig überzeugt zu ein.

Die größten Herausforderungen, vor denen die Unternehmen stehen, sind die Sicherheit der Endgeräte zu gewährleisten, technische Probleme schnell zu lösen sowie ihrer Belegschaft das Arbeiten von zu Hause zu ermöglichen.

90 Prozent der Unternehmen, die eine moderne Konnektivitätslösung eingeführt haben, bewerten deren Erfolg mit mehr als 8 von 10 Punkten, wobei 10 für extrem erfolgreich steht.

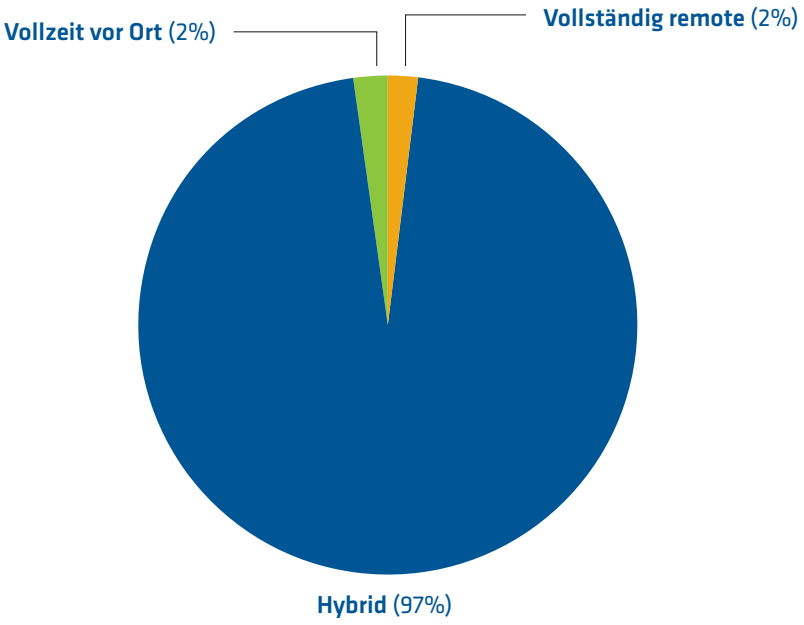
Die neue Arbeitswelt

Beschäftigte arbeiten immer dezentraler und oft von überall auf der Welt aus und sind dabei ständig in Bewegung. Deswegen ist es für Unternehmen heutzutage ein Muss, orts- und netzwerkunabhängig auf viele unterschiedliche Arten von Geräten remote zugreifen zu können, um sie zu verwalten, zu überwachen und zu patchen.

Die Pandemie hat zu einer starken Verlagerung hin zu hybriden Arbeitsmodellen und Remote Work geführt und dieser Trend wird anhalten. In den Unternehmen wächst die Zahl an Geräten wie Laptops, Tablets und Smartphones und damit auch der Bedarf daran, mit leistungsfähigen Lösungen Daten, Geräte sowie Mitarbeitende unterwegs und im Büro zu schützen.

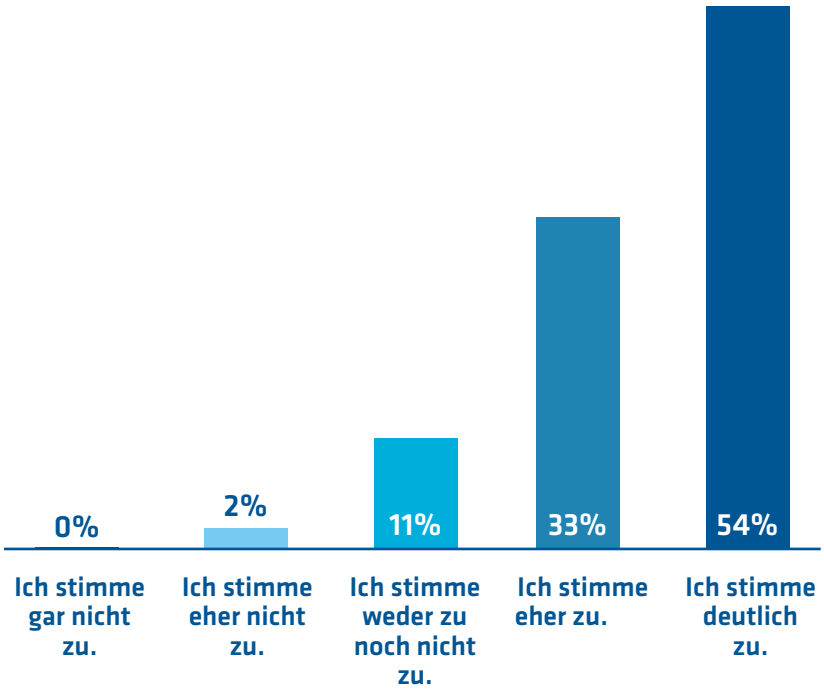
Dies zeigt sich in den Arbeitsmodellen, die Unternehmen aktuell umsetzen: 99 Prozent der Befragten geben an, dass ihre Beschäftigten entweder vollständig remote (zwei Prozent) oder hybrid (97 Prozent) arbeiten. Deshalb sind die Unternehmen darauf angewiesen, sich durch Remote Access und Support besser mit den Mitarbeitenden verbinden zu können und sie bestmöglich unterstützen zu können.

Abbildung 1: Arbeitsmodelle in Unternehmen



Neue Arbeitsmodelle und Verfahren sind das Rückgrat moderner Unternehmen. 90 Prozent der Befragten stimmen zu, dass eine fortschrittliche Konnektivitätsplattform in der zunehmend hybriden digitalen Geschäftswelt von heute unerlässlich ist. Lediglich ein Drittel der Unternehmen hat eine solche Lösung jedoch bereits vollständig umgesetzt.

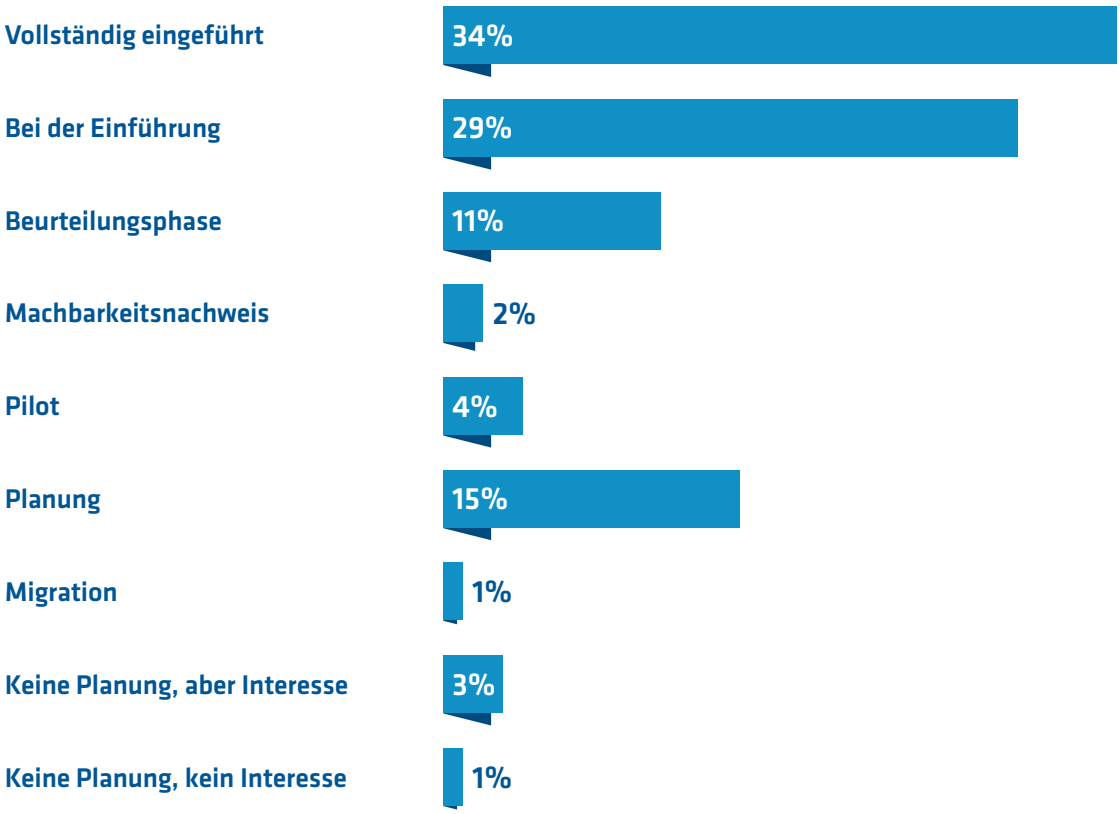
Abbildung 2: „Eine moderne Konnektivitätsplattform ist in der heutigen zunehmend hybriden digitalen Geschäftswelt unerlässlich“



Etwa 99 Prozent der Unternehmen sind allerdings zumindest daran interessiert, eine moderne Konnektivitätsplattform einzuführen, die ihnen dabei hilft, in diesem hart umkämpften Markt weiterhin agil zu bleiben und mit der die Beschäftigten produktiv arbeiten.

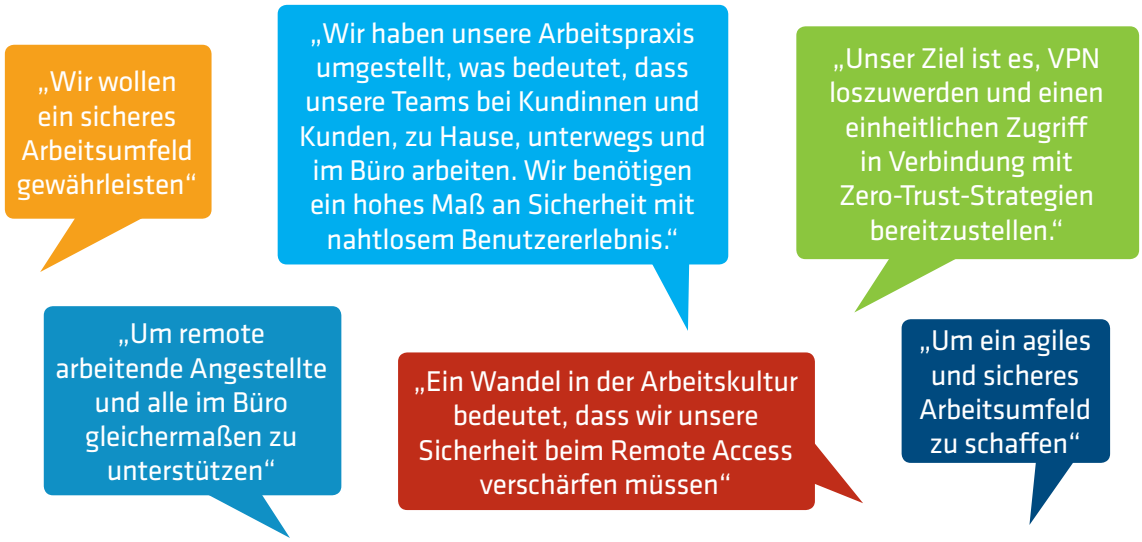
Während IT-Führungskräfte die Bedeutung von Remote Access und Support erkennen, wie Abbildung 2 verdeutlicht, ist ein großer Teil noch dabei, solche Lösungen zu begutachten, ihre Einführung zu planen oder steht erst ganz am Anfang der Umsetzung. Es liegt auf der Hand, dass bestehende und veraltete Systeme hier nicht mehr ausreichen. Der Bedarf an sicheren, fortschrittliche Konnektivitätslösungen für Remote Access und Support ist somit hoch.

Abbildung 3: Einsatz sicherer, moderner Konnektivitätslösungen für Remote Access und Support



Als Beweggründe, eine moderne Konnektivitätslösung einzuführen, hoben die Befragten Kosteneinsparungen, Sicherheit und Produktivität hervor.

BEWEGGRÜNDE

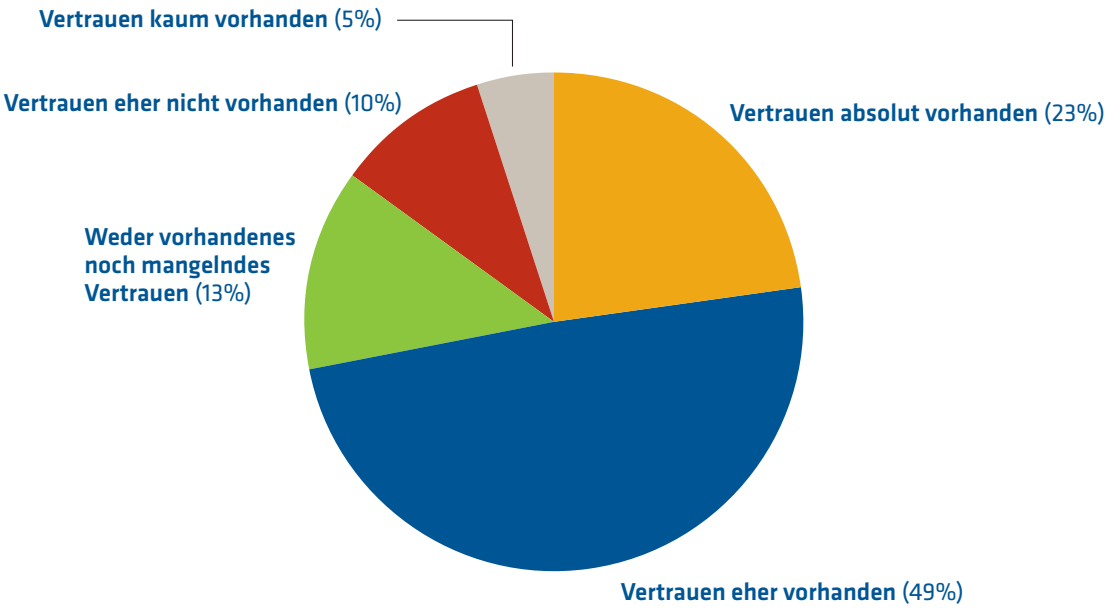


Moderne Lösungen für moderne Probleme

Versäumen es Unternehmen, eine sichere und einfach zu verwaltende Konnektivitätslösung bereitzustellen, die nicht nur am Firmenstandort zum Einsatz kommt, führt dies sehr wahrscheinlich dazu, dass die Mitarbeitenden weniger produktiv arbeiten können – und auch die Sicherheit eines Unternehmens kann durch Bedrohungen oder konzertierte Angriffe von außen leichter kompromittiert werden. Das schadet dem Ruf der Marke und das beeinflusst das Vertrauen der Verbraucherinnen und Verbraucher negativ.

Immer mehr Geräte und Personen, die sich außerhalb der Grenzen der abgesicherten Unternehmensnetzwerke befinden, bedeuten, dass sich Cyberkriminellen eine immer größere Angriffsfläche bietet, die diese gerne ausnutzen. Wie sollen Unternehmen hier ohne moderne Lösungen sichergehen, dass es zu keinen sicherheitsrelevanten Zwischenfällen kommt? Wie können sie Ausfälle auf ein Minimum reduzieren?

Abbildung 4: Vertrauen in bestehende Ansätze für Remote-Konnektivität



Die Antworten legen nahe, dass das Vertrauen in die momentan verwendeten Lösungen minimal ist: Nur 23 Prozent der IT-Entscheidungstragenden geben an, dass „Vertrauen absolut vorhanden“ ist. Der größte Teil, knapp die Hälfte, gab an, dass „Vertrauen eher vorhanden“ ist, während 15 Prozent entweder eher kein oder kaum Vertrauen in ihre bestehenden Praktiken haben.

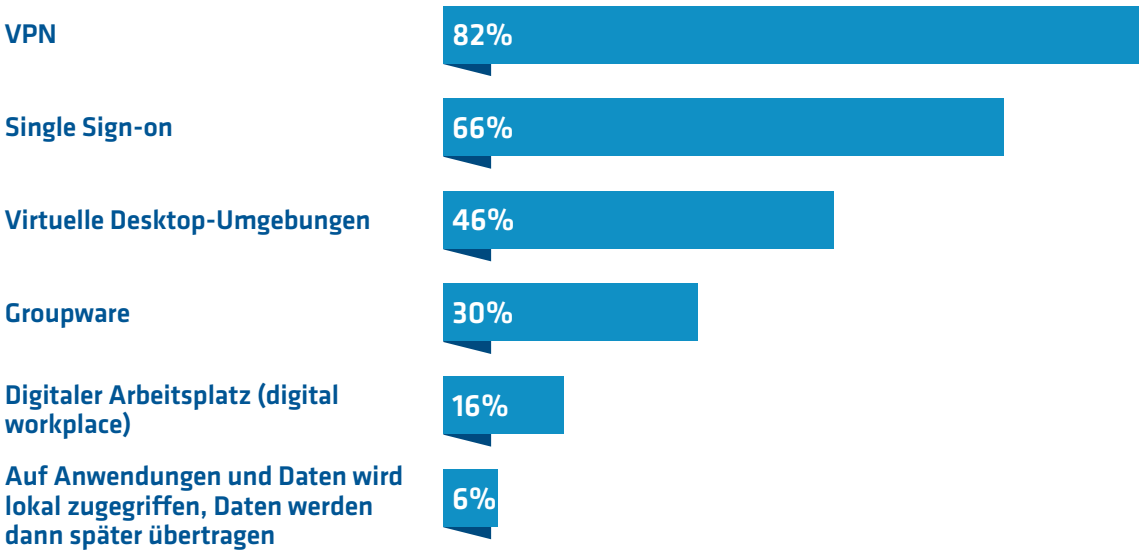
Dies deutet auch darauf hin, dass Unternehmen versuchen, eine moderne Belegschaft zu unterstützen, die Remote- und Hybridarbeit bevorzugt, ohne dabei die erforderlichen Schritte zu unternehmen, um solche Arbeitsumgebungen abzusichern. Das zeigt an, dass es Schwachstellen in der IT-Sicherheit gibt und technische Probleme nur verspätet gelöst werden, was sich kurzfristig negativ auf die Produktivität der Mitarbeitenden auswirkt.

VPN hinter sich lassen

Die gebräuchlichste und beliebteste Art, remote auf das Unternehmensnetzwerk zuzugreifen, sind VPNs. 82 Prozent der Unternehmen setzen sie ein. VPNs sind für Remote Work jedoch häufig unzureichend – was Unternehmen oft dazu zwingt, aus Bequemlichkeit Kompromisse bei der Sicherheit einzugehen.

VPNs sind nicht transparent, verursachen Reibungsverluste bei dauerhafter Nutzung und beschränkter Bandweite und sind für das Zeitalter des hybriden Arbeitens häufig nicht gewappnet. Dennoch wenden sich Unternehmen nur zögerlich von ihnen ab, was angesichts der weitverbreiteten Verwendung und Akzeptanz keine Überraschung ist.

Abbildung 5: Wie Benutzer normalerweise remote auf den Arbeitsplatz zugreifen



Die Pandemie führte zu verstärkter Nutzung von VPN, da in kurzer Zeit Rahmenbedingungen für die Arbeit von zu Hause geschaffen werden mussten. Vielen Unternehmen ermöglichte dies, Remote Work schnell einzuführen und den Geschäftsbetrieb aufrechtzuerhalten.

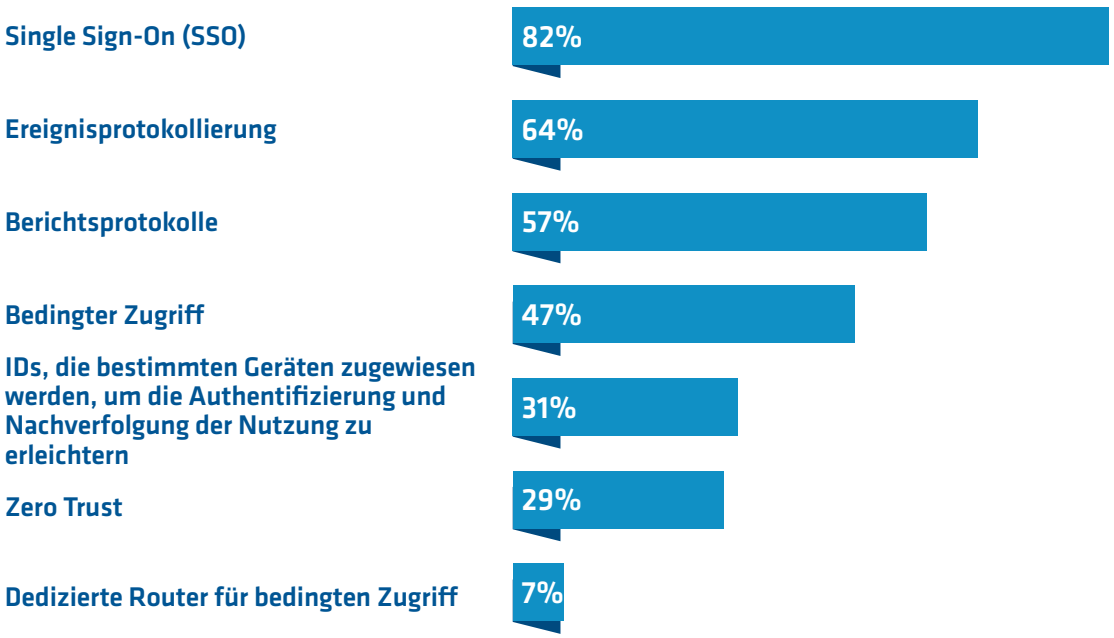
Ein Alternative zu VPN bietet Remote-Access-Software. Hier verbinden sich die Nutzenden direkt zu ihren Dateien und Programmen auf einem separaten Gerät. Im Gegensatz zu VPN ist dabei für einen dauerhaften optimalen Betrieb keine komplexe Konfiguration oder eine ständige Wartung notwendig. Die Installation ist einfach und kann mit nur wenigen Klicks auf vielen Geräten gleichzeitig erfolgen.

Das spart Kosten und Zeit, da keine Experten vor Ort nötig sind, die etwaige Fehler beheben müssen.

Mit Funktionen wie Single Sign-On, Ende-zu-Ende-Verschlüsselung, bedingtem Zugriff und der Möglichkeit, alle Aktivitäten innerhalb einer Sitzung zu protokollieren, verbinden Sie sich so remote, ohne Kompromisse bei der Sicherheit einzugehen. Die meisten Unternehmen nutzen diese Funktionen sowie weitere wie z. B. Berichtsprotokolle, um ihre Mitarbeitenden und Abläufe abzusichern.

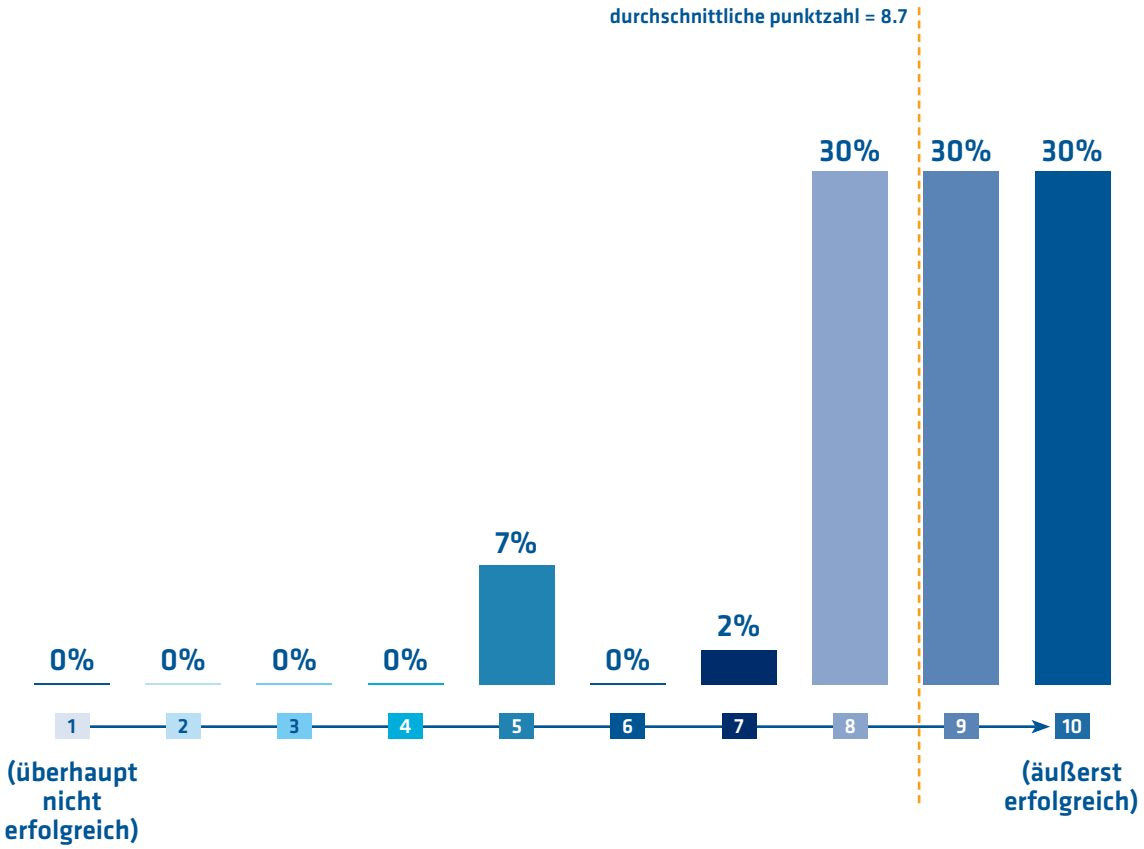
Zero Trust ist ein Modell und kein einzelnes Produkt. Das Konzept, das streng nach dem Prinzip „niemandem vertrauen, immer überprüfen“ vorgeht, wird in Unternehmen jedoch nur in geringem Umfang umgesetzt. Zero Trust ist ein ganzheitlicher Ansatz: Dabei werden Lösungen übernommen, die sich in bereits bestehende Systeme integrieren lassen und es erlauben, Vorgänge kontinuierlich zu überprüfen und nicht allen Nutzenden blind vertrauen zu müssen. Viele Unternehmen streben ein Zero-Trust-Modell zwar an, aber nur ein Drittel der Befragten berichtete, eine derartige Strategie bereits zu verfolgen. Sicherheitsrelevante Zwischenfälle häufen sich heutzutage allerdings und viele Belegschaften sind zunehmend über die ganze Welt verstreut. Deswegen können es sich Unternehmen nicht leisten, Kompromisse einzugehen, wenn es darum geht, ihre Endpunkte sicher zu verwalten.

Abbildung 6: Aktuelle Ansätze bei der Remote-Konnektivität



Wer bereits eine moderne Konnektivitätslösung implementiert hat, spürt die Vorteile deutlich: Einer von drei Befragten bewertet den Erfolg der eingeführten Lösung mit perfekten 10 von 10, wobei 10 „extrem erfolgreich“ bedeutet. Die restlichen Befragten, 60 Prozent, bewerten den Erfolg mit mindestens 8 von 10 Punkten. Die von den Befragten vergebene durchschnittliche Punktzahl betrug 8,5 von 10, was den umfassenden Erfolg klar belegt.

Abbildung 7: Erfolg vollständig eingeführter moderner Konnektivitätslösungen

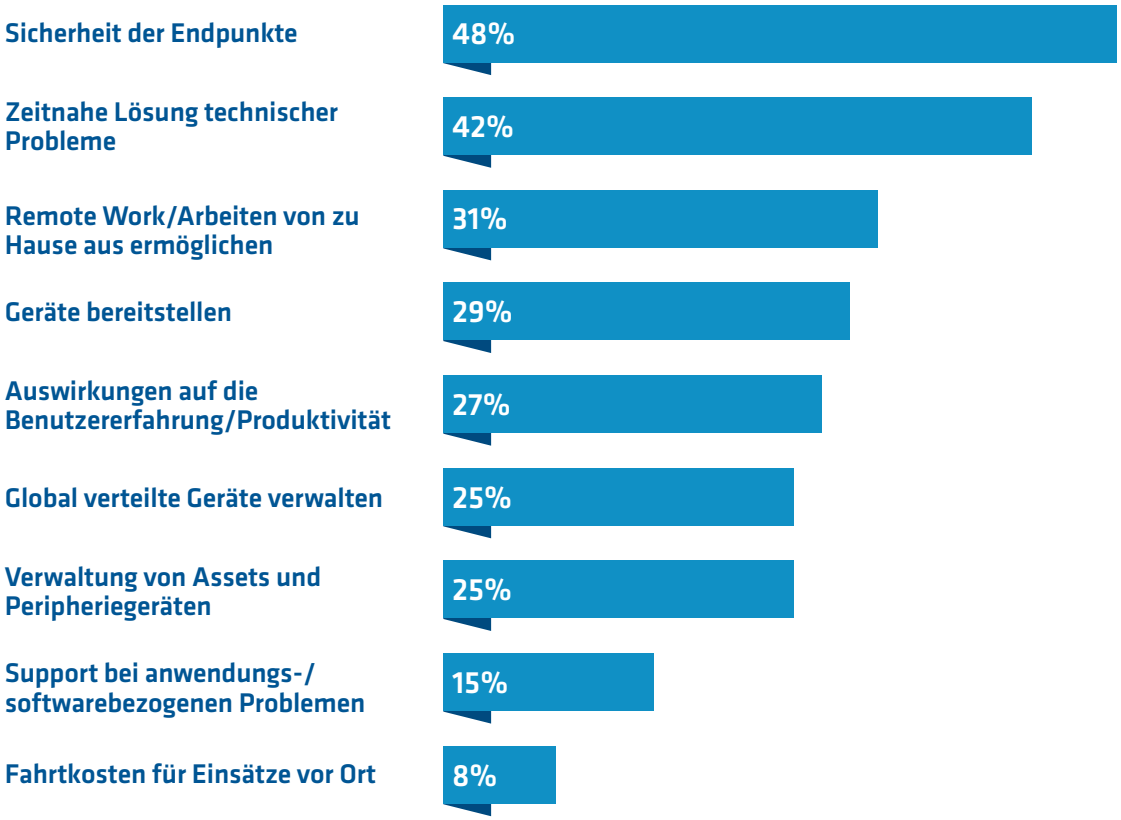


Hürden überwinden

Die größten Herausforderungen für Unternehmen in Bezug auf Remote Access und Support betreffen die Sicherheit sowie die Behebung technischer Probleme. Die Möglichkeit, Ihre Endgeräte aus der Ferne zu sichern und zu patchen, ist entscheidend. So bleibt Ihr Unternehmen geschützt und Ihre Mitarbeitenden arbeiten immer produktiv.

Angestellte erwarten, dass sie jederzeit nahtlos von jedem Gerät aus Zugriff haben. Das erweitert aber gleichzeitig die Angriffsfläche für Cyberkriminelle. Cyberangriffe werden immer häufiger und zunehmend raffinierter und Unternehmen müssen ihre Systeme schützen, indem sie aus der Ferne Schwachstellen patchen und Risiken minimieren.

Abbildung 8: Größte Herausforderungen bei Remote Access und Support
(3 maximal)



Informationen leichter auffinden zu können und weltweit verteilte Assets von idealerweise einem einzigen Dashboard aus verwalten zu können, sollte für Personen mit Entscheidungsbefugnissen in der IT oberste Priorität haben.

Endpunkte transparent zu überwachen und zu verwalten, hilft IT-Fachkräften dabei, Schwierigkeiten schneller zu erkennen. Bereits unter Zeitdruck stehendes Personal löst Probleme so rasch aus der Ferne. Das verringert den Druck auf die Teams und stellt gleichzeitig sicher, dass das benötigte Fachwissen zur richtigen Zeit zur Verfügung steht. Stressbelastete, schnelllebige Arbeitsumfelder machen einen effizienten und zuverlässigen technischen Support unbedingt notwendig.

User-First-Initiativen

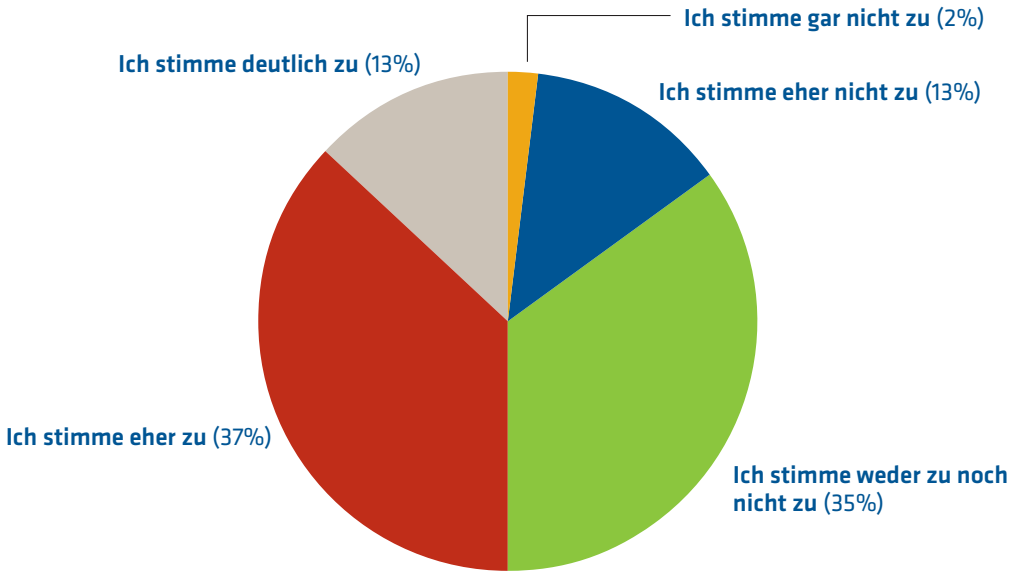
Teammitglieder, die unterwegs bzw. remote arbeiten, benötigen kontinuierlichen Support. Aus finanzieller Sicht oder unter dem Gesichtspunkt, dass Unternehmen die Produktivität aufrechterhalten wollen, ist es nicht mehr sinnvoll, dass Mitarbeitende anreisen, um Hilfe bei IT-Problemen zu bekommen, am Onboarding teilzunehmen oder auf Geräte zuzugreifen.

Wenn Unternehmen Probleme nicht vor Ort, sondern remote lösen, sparen sie enorm viel Zeit, Kosten und Arbeitsaufwand ein. Egal, ob es sich um IT-Kräfte handelt, die anreisen, um Fehler zu beheben, oder um Nutzende, die eine Lösung für ihr Problem benötigen.

Wenn IT-Fachleute akute Schwierigkeiten aus der Ferne beseitigen können, ermüden sie weniger, Ressourcen werden rechtzeitig umgeleitet und Anfahrtskosten reduzieren sich. Außerdem konzentrieren sich so die Fachleute innerhalb einer Firma an einem Ort und Unternehmen können Kundendienstleistungen problemlos skalieren.

Die Qualifikationslücke wächst, was Unternehmen deutlich spüren. Sie müssen internes Know-how nutzen, um einen Wettbewerbsvorteil auf ihrem Markt zu genießen und beizubehalten.

Abbildung 9: „Die IT-Qualifikationslücke in meinem Unternehmen wächst“



Darüber hinaus müssen Unternehmen die Fähigkeiten und die Entwicklung ihrer Beschäftigten fördern, um Mitarbeitende anzuziehen und zu halten: Die Hälfte der befragten Unternehmen stimmt eher oder deutlich zu, dass die Qualifikationslücken in ihren Teams wachsen. Nur zwei Prozent der Befragten konnten dieser Aussage überhaupt nicht zustimmen, was darauf hindeutet, dass Fachkräftemangel ein weitverbreitetes Phänomen ist.

Ebenso stimmen 73 Prozent zu, dass es heutzutage schwierig ist, IT-Fachleute zu gewinnen und im Unternehmen zu halten. Einen nutzerfreundlichen Arbeitsplatz zu stellen, an dem ein nahtloser Zugriff auf Ressourcen gegeben ist und Probleme zeitnah gelöst werden, ist für Unternehmen deswegen ausgesprochen wichtig.

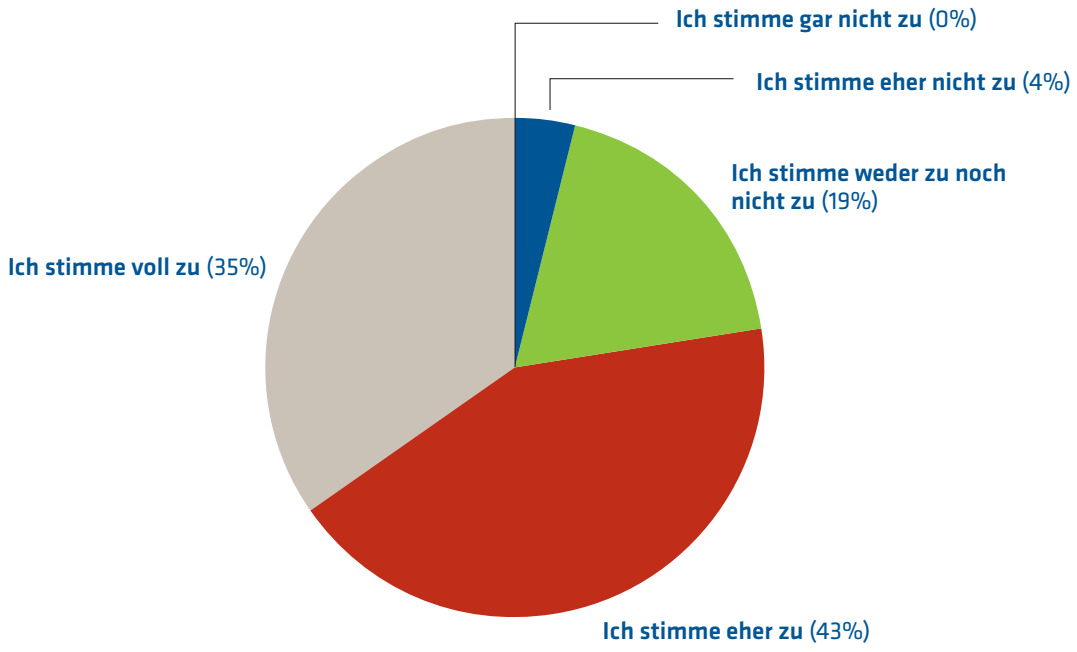
Die Auswirkung moderner Lösungen

Mit modernen Plattformen müssen Unternehmen keine Kompromisse eingehen, weder bei der Benutzererfahrung noch bei der Sicherheit. Prozesse wie Patch Management und Updates lassen sich automatisieren, was die Arbeitsbelastung von IT-Teams reduziert, die möglicherweise gleichzeitig mit einem Mangel an Mitarbeitenden oder begrenzten Budgets zu kämpfen haben. Damit gehen Unternehmen auch sicher, dass Updates und Analysen zeitnah und regelmäßig erfolgen. Dadurch reduzieren sie Ausfallzeiten und erhalten einen besseren Überblick, was dazu beiträgt, Probleme auf allen Geräten in einem Netzwerk besser zu identifizieren.

Mit Hilfe moderner Konnektivitätslösungen halten Unternehmen strenge Sicherheitsrichtlinien ein und stellen gleichzeitig sicher, dass Beschäftigte immer produktiv arbeiten und ohne Unterbrechungen kommunizieren können. Das Benutzererlebnis von Kundinnen und Kunden, Mitarbeitenden und Partnerinnen und Partnern wird intuitiver und nahtloser. Das wiederum führt zu einer schnelleren Wertschöpfung.

Remote Access hilft dabei, Qualifikationslücken zu überbrücken, indem Fachkräfte aus der Ferne Mitarbeitende vor Ort unterstützen. In Bereichen wie dem Einzelhandel, bei Point-of-Sale-Kiosken und in Lagerhäusern kommt es oft zu Verzögerungen. Wenn Support von Fachleuten nicht ohne Weiteres verfügbar ist, wirkt sich das nachteilig auf die dort Beschäftigten aus. Das kann schlussendlich auch zu einem negativen Erlebnis für Kundinnen und Kunden führen, sollte die Lieferkette engmaschig und digital sein, so wie es bei E-Commerce-Plattformen der Fall ist, die jeden Tag in großem Umfang Käufe abwickeln. Ein Drittel der Befragten stimmt voll und ganz zu, dass eine effektive Konnektivitätsplattform den Druck bezüglich des Supports der Mitarbeitenden verringern würde. 78 Prozent stimmen dieser Aussage zumindest teilweise zu.

Abbildung 10: „Eine effektive Remote-Konnektivitätsplattform würde den Druck bezüglich des Supports der Mitarbeitenden verringern“

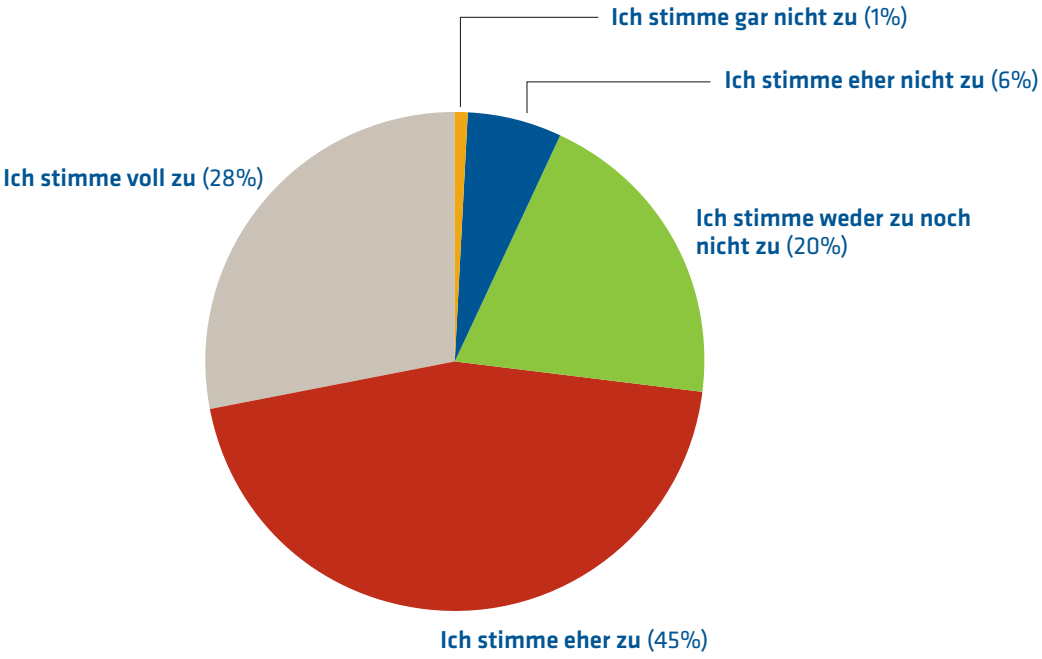


Die Arbeitswelt wird immer digitaler, da Unternehmen immer abhängiger von elektronischen Geräten und vernetzten Maschinen sind. Ein zuverlässiger Support ist deshalb von entscheidender Bedeutung. Moderne Remote-Konnektivitätsplattformen sind der Herausforderung gewachsen, da sie Unternehmen die Möglichkeit bieten, Geräte überall zu verwalten, ohne eine Fachkraft vor Ort zu Rate ziehen zu müssen.

Dies ist unabdingbar in Situationen, in denen Mitarbeitende möglicherweise nicht über die Fähigkeiten oder die Zeit verfügen, sich mit technischen Problemen zu befassen, wenn sie in anstrengenden und schnelllebigen Umfeldern agieren.

IT-Führungskräfte müssen eine Arbeitsumgebung schaffen, in der Beschäftigte ihr Bestes geben können. Ein zentraler Support hilft Unternehmen, in großem Umfang zu operieren und gleichzeitig eine vielfältige und geografisch verteilte Belegschaft zu unterstützen. Die richtige Technologie spielt dabei eine wichtige Rolle. Reibungslose, sichere Prozesse sind der beste Weg, um eine vernetzte, produktive und benutzerfreundliche Arbeitsumgebung zu ermöglichen, die es allen erlaubt, global miteinander verbunden zu bleiben.

Abbildung 11: „Es ist schwierig, IT-Talente zu gewinnen und zu halten“



Ein weiterer wichtiger Vorteil sind die Auswirkungen auf die CO2-Bilanz eines Unternehmens. Da Energieverbrauch und CO2-Emissionen zunehmend auf den Prüfstand gestellt werden, bemühen Unternehmen sich, ihren negativen Einfluss auf die Umwelt zu minimieren.

Mit einer Konnektivitätsplattform können Unternehmen auf Endpunkte zugreifen, sie warten und Support leisten sowie Netzwerke überwachen – alles aus der Ferne. Das bedeutet oft, dass Anfahrten überflüssig werden. Damit verringern Unternehmen ihren CO2-Fußabdruck erheblich. Emissionsarme digitalisierte Prozesse schaffen letztendlich eine nachhaltigere Zukunft für uns alle.

Fazit

Das Erlebnis, das Kundinnen und Kunden und Mitarbeitende haben, hängt von schneller, flexibler und benutzerfreundlicher Remote-Support-Technologie ab.

Technische Probleme so schnell und reibungslos wie möglich zu lösen, ohne die Sicherheit von Daten zu gefährden, ist ein Schlüsselfaktor für Erfolg und Produktivität aller Unternehmen in allen Branchen.

Nutzende müssen sich unabhängig von Geräteplattform, Endgerät, Standort oder Bandbreite verbinden können. Remote Access ermöglicht es, Probleme schneller zu lösen, die Zufriedenheit von Kundinnen und Kunden sowie Mitarbeitenden zu erhöhen und die Markentreue zu stärken. Die richtige Plattform ermöglicht es IT-Teams, technische Probleme der Beschäftigten rasch zu lösen, egal, wo sie sich aufhalten und welche Art von Gerät sie einsetzen.

Endpunkte aus der Ferne zu verwalten und zu warten, verringert Kosten erheblich. Statt sie routinemäßig vor Ort zu warten, sparen Unternehmen Geld und Zeit ein, indem Systeme remote überwacht und aktualisiert werden.

Die Ergebnisse zeigen, dass Unternehmen mit ihren aktuellen Lösungen nicht zufrieden sind. Es überrascht nicht, dass VPNs oft zum Einsatz kommen, wobei IT-Führungskräfte sich bemühen sollten, stattdessen leistungsfähigere, robustere und sicherere Plattformen einzuführen, die Remote Access und Support für eine Vielzahl von Geräten und Endpunkten erlauben.

Bei den Unternehmen, die eine moderne Konnektivitätslösung eingeführt haben, zeigen die Untersuchungsergebnisse von *Computing*, dass die Einführung ein ausdrücklicher Erfolg war.

Entscheidend ist, dass Remote-Access-Software kostspielige Besuche vor Ort überflüssig macht und es den Teams ermöglicht, Probleme schnell und zuverlässig ohne zusätzliche CO2-Emissionen zu lösen. Unternehmen, die in einem digital ausgereiften Markt wettbewerbsfähig bleiben wollen, müssen Tools bereitstellen, mit deren Hilfe sie problemlos in großem Maßstab und ohne Einbußen bei der Datensicherheit arbeiten können.

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 – von Laptops und Mobiltelefonen bis hin zu Industriemaschinen und Robotern.

TeamViewer wartet kontinuierlich mit Innovationen in Bereichen wie Augmented Reality auf und ermöglicht es Unternehmen aus allen Branchen, ihre Arbeitsprozesse zu digitalisieren.

Durch die Akquisition von Ubimax, Upskill und Viscopic hat TeamViewer eine vollumfängliche Augmented-Reality-Lösung auf dem Markt aufgebaut. TeamViewer Frontline optimiert Prozesse entlang der gesamten industriellen Wertschöpfungskette und ermöglicht einen vollständig digitalen industriellen Arbeitsplatz.

TeamViewer wurde 2005 gegründet, hat seinen Hauptsitz in Göppingen, Deutschland, und beschäftigt weltweit rund 1400 Mitarbeitende. Die TeamViewer AG (TMV) ist als MDAX-Unternehmen an der Frankfurter Börse notiert.

Oktober 2022