

Die Umstellung auf Remote-Zugriff erfordert die Modernisierung des Kontaktzentrums

Wenn Ihre Mitarbeiter in Kontaktzentren per Remote-Zugriff arbeiten, können Sie auch Fachkräfte von außerhalb Ihrer Region einstellen. Vielleicht denken Sie auch darüber nach, die genutzte Bürofläche zu reduzieren.

„Bis 2024 werden 30 % aller Organisationen ihre Kontaktzentren außerhalb der eigenen Niederlassungen betreiben. Die Anzahl der Vollzeit per Remote-Zugriff arbeitenden Mitarbeiter wird um 60 % steigen.“

Gartner: Overcome the Top 3 Challenges to Setting Up Contact Center Agents for Remote Working (Bewältigen Sie die drei größten Herausforderungen bei der Einrichtung von Remote-Zugriff für Mitarbeiter in Kontaktzentren) – Veröffentlicht am 26. Februar 2021

Mitarbeiter in Kontaktzentren sind die ersten Ansprechpartner für Ihre Kunden. Sie müssen in der Lage sein, klar über das Telefon zu kommunizieren und schnell auf Informationen zuzugreifen, um Kunden zeitnah zu helfen. Jede Störung der Anrufqualität oder der Anwendungsperformance kann die Länge der Anrufe erhöhen und die Kundenzufriedenheitswerte reduzieren. Wenn Sie die Performance Ihrer Mitarbeiter überwachen und managen können, stellen Sie sicher, dass Sie das beste Kundenerlebnis bieten.

Wir alle wissen, dass SLAs und Net Promoter Scores von entscheidender Bedeutung sind, aber das Onboarding neuer Mitarbeiter, die Bereitstellung von Online-Schulungen und die Möglichkeit, regelmäßig Team-Meetings abzuhalten, sind ebenfalls wichtig. Mit der Umstellung auf ein hybrides Belegschaftsmodell nimmt die IT-Komplexität zu. Dezentrale hardwarebasierte Legacy-Netzwerk- und -Sicherheitsinfrastrukturen sind schwierig zu managen und auf dem neuesten Stand zu halten.

Anwendungen aus dem Kontaktzentrum in die Cloud zu migrieren und den Betrieb des Kontaktzentrums zu dezentralisieren ist ein wichtiger Schritt, um das Kontaktzentrum langfristig weiterzuentwickeln. Ein paar Empfehlungen von Gartner sind:

- Migration zu Cloud-basierten Plattformen für Kontaktzentren, um Probleme mit der VPN-Skalierbarkeit zu vermeiden, da Cloud-Plattformen für die meisten Prozesse von Kontaktzentren keine VPNs benötigen. Organisationen, die planen, im eigenen Rechenzentrum zu bleiben, müssen ihre VPN-Infrastruktur neu aufbauen, um die Remote-Mitarbeiter zu unterstützen
- Einrichtung einer sicheren Arbeitsplatzumgebung für Remote-Mitarbeiter in Kontaktzentren durch die Ermöglichung von End-to-End-Sicherheit mithilfe einer Infrastruktur virtueller Desktops (Virtual Desktop Infrastructure, VDI) und WebRTC-Technologie, falls erforderlich

Dies kann auch dazu beitragen, die Infrastrukturkosten für Rechenzentren zu senken. Die häufige Verwendung von älteren VDI- und VPN-Technologien kann jedoch zu Schwierigkeiten bei der Aufrechterhaltung der Sicherheit führen und sie lassen sich für die größere Belegschaft nicht skalieren. Darüber hinaus wird die SaaS-Performance bei der Nutzung eines VPN leiden. Da viele Unternehmenskunden mindestens einen Teil der Infrastruktur im eigenen Rechenzentrum betreiben, benötigen sie eine bessere Alternative zu herkömmlichen VPNs und Legacy-Infrastrukturen. Darüber hinaus können bei Kunden von Legacy-VDIs Verbindungsprobleme am Endpunkt auftreten.

„Bis 2024 werden werden mehr Kontaktzentrums-Mitarbeiter in der Cloud als vor Ort arbeiten.“

Gartner: Overcome the Top 3 Challenges to Setting Up Contact Center Agents for Remote Working (Bewältigen Sie die drei größten Herausforderungen bei der Einrichtung von Remote-Zugriff für Mitarbeiter in Kontaktzentren) – Veröffentlicht am 26. Februar 2021

Einerseits bedeutet dies, dass Remote-Mitarbeiter nur einen Thin Client, eine Internetverbindung, einen

Browser für WebRTC und ein Softphone benötigen, um Contact Center Software as a Service (CCaaS) zu verwenden. Da Mitarbeiter jedoch auf das heimische WLAN (mit unbeständigen Internetgeschwindigkeiten) angewiesen sind, ist es für die IT schwierig, Probleme bei der Anwendungsperformance zu lösen, besonders da sie keinen Einblick in das Heimnetzwerk hat. Für das beste VoIP- und UCaaS-Anwendungserlebnis benötigen Mitarbeiter eine erstklassige Direktverbindung (lokale Internet-Breakouts) in ihrem Zuhause, da diese Anwendungen anfälliger für Verbindungsstörungen, Paketverluste und Latenz sind. Ohne professionelle Sicherheitsfunktionen im heimischen Netzwerk sollten Daten- und Anwendungsschutz als Service bereitgestellt werden, um Remote-Mitarbeiter vor Bedrohungen abzusichern.

Eine bessere Employee Experience fördert Produktivität und Kundenzufriedenheit

Tools für die Zusammenarbeit stellen in einer Remote-Umgebung sicher, dass Teams verbunden bleiben. Eine schnelle Einarbeitung und Schulung von Mitarbeitern ohne einen guten Plan, wie eine konsistente Performance aufrechterhalten werden kann, kann die IT und das Unternehmen zusätzlich belasten.



Citrix Workspace bietet sicheren Zugriff mit Citrix Virtual Apps and Desktops und Secure Workspace Access. Citrix Workspace bietet Mitarbeitern:

- eine zentrale Bereitstellung mit einem Benutzerkomfort wie bei Consumer-Lösungen. Mitarbeiter können jedes beliebige Endgerät nutzen – Desktop-PCs, Laptops, Mobilgeräte, geschäftliche sowie private Endgeräte und mehr. Mit diesem können sie sicher auf ALLE Ihre Anwendungen zugreifen
- einen sicheren und unkomplizierten Zugriff auf alle Anwendungen (Windows, SaaS, Web-Anwendungen). SSO bietet an jedem Ort einen sicheren Zugriff auf jede Anwendung und Datei, die Ihre Mitarbeiter benötigen, ohne dass mehrere Passwörter eingegeben werden müssen
- einen sicheren, Cloud-basierten Browser, der von Citrix gehostet wird und mit dem Mitarbeiter ohne Einschränkungen im Web surfen können

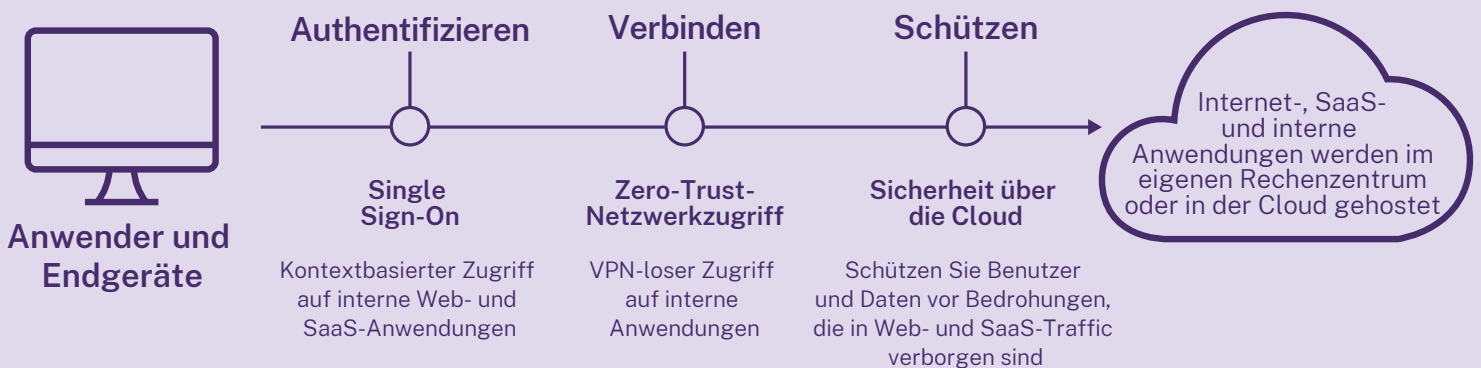
Je größer die Entfernung zwischen Mitarbeitern und den von ihnen verwendeten Anwendungen, desto schlechter ist die Qualität aufgrund von Latenz. Beim traditionellen Backhauling zu einem Rechenzentrum werden ineffiziente Routing-Praktiken genutzt, um ausgehende Internetverbindungen zur Cloud abzusichern. Um die Experience zu verbessern, optimiert Citrix SD-WAN den Datenverkehr intelligent und sendet ihn direkt an die von den Mitarbeitern benötigten Cloud-Anwendungen. Citrix SD-WAN kann Sprach- und anderen SaaS-Traffic erkennen und lokale Breakouts einrichten, um die Latenz zu reduzieren und gleichzeitig die Angriffsfläche gering zu halten. Durch die Nutzung drahtloser 4G-LTE-Verbindungen neben der Breitbandverbindung verfügen

Mitarbeiter über genügend Bandbreite und müssen sich keine Gedanken über Netzwerkstörungen machen. Die IT-Abteilung konfiguriert einfach die Citrix SD-WAN 110 Appliance und liefert sie in kurzer Zeit an alle Remote-Mitarbeiter.

Citrix SD-WAN lässt sich nahtlos in Citrix Virtual Apps and Desktops Service integrieren und bietet einen optimalen Benutzerkomfort für eine bis zu 5-fache Leistungsverbesserung. Die standardmäßige Integration mit dem Admin-Workflow des Citrix Virtual Apps and Desktops Service vereinfacht die Bereitstellung und Konfiguration, um die Migration zu beschleunigen und die Abhängigkeit von VPNs zu beseitigen. SD-WAN kann virtuellen Traffic von Citrix automatisch und in Echtzeit gegenüber anderem weniger wichtigen virtuellen Traffic priorisieren. Die Servicequalität wird an den Send- und Empfangspunkten gemessen, um eine verlustfreie Sprachübertragung zu gewährleisten.

Sicherheit und Datenschutz für Kundendaten

Mitarbeiter in Kontaktzentren beschäftigen sich Tag für Tag mit vertraulichen, personenbezogenen Informationen von Kunden, sodass Datenschutzverletzungen eine erhebliche Bedrohung für das Unternehmen darstellen. Infolgedessen ist die Gesetzgebung zum Datenschutz umfangreicher geworden. Wenn Sie in einer Welt, in der viele Mitarbeiter über ihren heimischen Breitband-Internetanschluss von zu Hause aus arbeiten, die Compliance aufrechterhalten wollen, müssen Sie auch diese Mitarbeiter und deren Endgeräte absichern.



Personenbezogene Informationen des Kunden sollten durch verschiedene Maßnahmen geschützt werden: eine integrierte Verschlüsselung von Daten über das WAN, zentralisierte Sicherheitsrichtlinien und eine nahtlose Integration in einen über die Cloud bereitgestellten Sicherheitsservice, der an ein SASE-Framework inklusive ZTNA ausgerichtet ist.

Der SASE-Ansatz von Citrix bietet ein integriertes, über die Cloud gemanagtes SD-WAN und einen Sicherheitsservice über die Cloud namens Secure Internet Access (SIA). Dieses einheitliche Framework basiert auf einer globalen Cloud-Architektur mit PoPs auf der ganzen Welt. Citrix kombiniert umfassende Cloud-basierte Sicherheit mit Zero Trust Network Access (ZTNA), SD-WAN, Analysen und sicherem Internetzugang. Citrix sichert den Zugriff auf Web-, SaaS/Cloud- und Legacy-Anwendungen ab und zwar mit Lösungen, die Benutzer und Daten authentifizieren, verbinden und vor Bedrohungen aus dem Netz schützen.

Benutzer profitieren von einer einheitlichen Oberfläche, über die sie auf alle Anwendungen zugreifen können, die sie benötigen, ohne dabei die Sicherheit oder Performance zu beeinträchtigen. Dadurch sollen Day 0- und Day 2-Operations vereinfacht und die Koordination von NetOps- und SecOps-Teams ermöglicht werden. Benutzer und Daten werden vor Bedrohungen geschützt, die in jeglichem Web- und SaaS-Traffic verborgen sind. Dies geschieht über einen Cloud Access Security Broker (CASB) und Data Leakage Prevention (DLP) sowie Web-Sicherheitsmaßnahmen, die vor böswilligen Websites, unbekanntem Betriebssystemen und Malware schützen.

Citrix Workspace mit Secure Workspace Access sichert Mitarbeiter ab und ermöglicht einen identitätsbasierten Zugriff, der auf einem globalen VPN-losen Netzwerk aus Points of Presence (POPs) besteht, die:

- beim Zugriff auf Anwendungen (Windows-, SaaS- und Web-Anwendungen) vor Bedrohungen schützen und über SSO, MFA und einen sicheren isolierten Browser gesetzliche Vorschriften zu personenbezogenen Daten einhalten
- Benutzern den Zugriff auf SaaS- und Web-Anwendungen mit weniger Passwörtern ermöglichen
- BYO-Geräte mit richtlinienbasierten Sicherheitskontrollen (Screenshot-Blockierung, Schutz vor Keyloggern, Wasserzeichen) und dem Citrix Secure Browser Service absichern, um Mitarbeiter daran zu hindern, Kundendaten, die in Web- und SaaS-Anwendungen gespeichert sind, zu gefährden

- automatisch skalieren, um das System an einen Zuwachs der Remote-Belegschaft anzupassen

Zudem verfügt die integrierte Firewall von Citrix SD-WAN über eine globale Richtlinienkontrolle, unterstützt zonenbasierte Richtlinien, sodass Sie eine granulare Mikrosegmentierung des Datenverkehrs vornehmen und einheitliche Richtlinien konsequent durchsetzen können. Citrix SD-WAN kann zudem auf intelligente Weise die sich schnell ändernden offenen Ports von SaaS- und IaaS-Anwendungen nachverfolgen und den Datenverkehr als vertrauenswürdig einstufen. Dieser Traffic kann anschließend direkt ins Internet geleitet werden, wodurch die Anwendungsperformance verbessert wird. Die Lösung verschlüsselt zudem den gesamten ausgehenden Datenverkehr von Zweigstellen, selbst wenn er über eine private MPLS-Leitung transportiert wird.

Werden Sie ausfallsicherer, um sich schneller anzupassen

Ihr Kontaktzentrum muss live mit Kunden kommunizieren können, um wettbewerbsfähig zu bleiben. Ausfallzeiten führen nicht nur zu verlorenen Umsätzen, sondern können auch die Wahrnehmung der Marke und die Net Promoter Scores verschlechtern sowie die Bindung von Mitarbeitern verringern. Ausfallsicherheit hilft Ihrem Unternehmen, Störungen mit weniger Aufwand zu überwinden und gleichzeitig sicherzustellen, dass die Interaktionen mit Kunden keinen Schaden nehmen. Wenn Sie sich auf Mitarbeiter- und Kundenengagement, Remote-Zugriff, Onboarding und Kommunikationsstrategien konzentrieren, wird Ihr Unternehmen in der Lage sein, sich schneller anzupassen und das Kundenerlebnis zu verbessern.

Citrix Workspace mit Citrix Virtual Apps and Desktops ermöglicht ein schnelleres Onboarding neuer Mitarbeiter. Citrix Workspace fördert das Engagement von Mitarbeitern in hybriden Umgebungen, indem es sie über Kommunikations- und Kollaborationstools miteinander verbindet, den Zugriff auf Anwendungen und Daten optimiert und Echtzeit-Schulungen ermöglicht.

Citrix Workspace ermöglicht Mitarbeitern sichere Verbindungen durch Microapps, die die Rückkehr ins Büro vereinfachen und sich auf das Wohlbefinden von Mitarbeitern konzentrieren. Citrix Secure Workspace Access kann automatisch skaliert werden, um jedem Anstieg der Remote-Mitarbeiterzahlen gerecht zu werden. Darüber hinaus bietet die Lösung einen sicheren

Zugriff auf alle Anwendungen und Dateien mit SSO- und MFA-Authentifizierung, um die Anzahl der Passwörter zu reduzieren, die Mitarbeiter verwalten müssen und die von Hackern missbraucht werden können.

Die Citrix SD-WAN 110 Plattform bietet Remote-Mitarbeitern eine zuverlässige Performance, indem sie mehrere Verbindungen miteinander kombiniert, darunter Breitband und 4G LTE. Dadurch können sie weiterarbeiten, selbst wenn ein Anbieter ausfällt oder eine Leitung überlastet ist. Failover auf Paketebene während Anrufen werden von Mitarbeitern gar nicht wahrgenommen.

Mehr Möglichkeiten für die IT dank umfassender Visibilität

Mangelnde Visibilität erschwert es der IT, Anwendungsprobleme von Mitarbeitern zu lösen, die die Produktivität senken können. Da Mitarbeiter und IT-Teams jetzt per Remote-Zugriff und mit privaten sowie unternehmenseigenen Endgeräten in ihren Heimnetzwerken arbeiten, wird die Situation noch komplizierter. Und wenn Sie unterschiedliche Anwendungen haben, wie Web-, SaaS- und traditionelle Unternehmensanwendungen, ist es ohne umfangreiche Visibilität schwieriger zu bestimmen, wo ein Problem liegt. Wie können Sie beispielsweise feststellen, ob ein Problem auf Netzwerkkonnektivität, Latenz oder ein Problem mit einem Server oder einer Cloud zurückzuführen ist?

Citrix Workspace lässt sich in Citrix Analytics integrieren, damit Sie einen Einblick in Echtzeit erhalten können. Dadurch können Sie Probleme einfacher überwachen und beheben. Citrix bietet die Möglichkeit, sowohl Sicherheit als auch Performance zu analysieren.

Citrix Analytics ist ein intuitiver Analysedienst, mit dem Sie unübliche oder verdächtige Aktivitäten in Ihren Netzwerken überwachen und identifizieren können. Durch Maschinenlernfunktionen und fortschrittliche Algorithmen können Sie das Verhalten Ihrer Anwender anhand von Risikoindikatoren überwachen. Dazu gehören Anwender, Endgeräte, Netzwerk-Traffic und Dateien. Citrix Security Analytics unterstützt Sie bei der Verhinderung von Zero-Day- und internen Angriffen durch:

- Überwachung von SSL-Zertifikaten
- Überwachung der Arbeitsumgebung und Erkennung von Angreifern, Verhaltensänderungen und Anomalien, um böswillige Aktivitäten zu stoppen und Datenverlust zu verhindern

Citrix Performance Analytics bietet fortschrittliche Maschinenlernfunktionen, um IT-Teams und Administratoren dabei zu helfen, die Ursache von Performanceproblemen in virtuellen Infrastrukturen zu bestimmen und die Auswirkungen auf Mitarbeiter zu verstehen. Performance Analytics:

- zeigt Metriken zur Standort-Performance in übersichtlichen Dashboards zum Benutzerkomfort und zur Infrastruktur an. Hier können Sie die Performance für Nutzer analysieren und die Auslastung Ihrer Citrix Virtual Apps and Desktops Standorte optimieren.
- sammelt Metriken zur Performance Ihrer Umgebungen in der Cloud und im Rechenzentrum.
- quantifiziert die Performance für Mitarbeiter und klassifiziert Benutzer anhand bestimmter Faktoren. Die Lösung liefert verwertbare Erkenntnisse zu fehlgeschlagenen Problembehebungsmaßnahmen, Bildschirmverzögerungen, verzögerten Sitzungsanmeldungen und anderen Leistungskennzahlen.

Da Verbindungs- und Performanceprobleme durch das Netzwerk entstehen können, können Sie mithilfe eines Tools für das zentrale Monitoring und Management einen Einblick in den Zustand, die Auslastung, die Qualität und die Performance des gesamten Netzwerks erhalten. Zudem können Sie detaillierte Informationen zu einzelnen Standorten und deren Verbindungen einsehen. Citrix SD-WAN Orchestrator ist ein in der Cloud gehosteter, mandantenfähiger Managementservice, der Unternehmen und Citrix Partnern zur Verfügung steht, die eigenständig handeln möchten. Die Lösung ermöglicht eine zentrale Überwachung von Zustand, Auslastung, Qualität und Performance des gesamten Netzwerks mit detaillierten Informationen zu einzelnen Standorten und deren Verbindungen. Die Fehlerbehebung wird durch Endgeräte- und Audit-Protokolle, Diagnosetools wie Ping, Traceroute und Packet Capture verbessert, um Probleme mit Netzwerkverbindungen zu beheben. Kunden von Citrix Virtual Apps and Desktops profitieren von einem umfassenden Einblick in HDX-Traffic von

einzelnen Standorten, Sitzungen und Anwendern – für eine schnellere Fehlerbehebung.

Machen Sie Ihr Remote-Kontaktzentrum zukunftssicher

Wenn Sie einen vertrauenswürdigen Partner haben, der die einzigartigen Bedürfnisse von Kontaktzentren versteht und weiß, wie man Herausforderungen bei der Remote-Arbeit löst, können Sie Ihre Transformation nahtlos durchführen. Das Letzte, was Sie brauchen können, ist eine Unterbrechung Ihres Unternehmensbetriebs, insbesondere mit einer hybriden Belegschaft oder bei einer Migration in die Cloud. Citrix unterstützt Sie dabei, die Tools sicher bereitzustellen, die Ihre Mitarbeiter brauchen (SaaS-Anwendungen, Web-Anwendungen, virtuelle Anwendungen und mehr), während Sie gleichzeitig das Management vereinfachen und die Bereitstellung beschleunigen.

[Gartner, Overcome the Top 3 Challenges to Setting Up Contact Center Agents for Remote Working \(Bewältigen Sie die drei größten Herausforderungen bei der Einrichtung von Remote-Zugriff für Mitarbeiter in Kontaktzentren\) – Pankil Sheth, Steve Blood, Stuart Downes, 26. Februar 2021](#)



Vertrieb
ce_info@citrix.com

Standort
Citrix Systems International GmbH, Rheinweg 9, 8200 Schaffhausen, Schweiz

©2021 Citrix Systems, Inc. Alle Rechte vorbehalten. Citrix, das Citrix-Logo und andere hierin aufgeführten Marken sind Eigentum von Citrix Systems, Inc. und/oder eines ihrer Tochterunternehmen und sind möglicherweise beim Patent- und Markenamt der Vereinigten Staaten und in anderen Ländern eingetragen. Alle anderen Marken sind Eigentum der jeweiligen Inhaber.