Lösungsbeschreibung

Warum Citrix Workspace eine bessere Wahl für Remote-Mitarbeiter von heute ist als VPN

Mehr Menschen denn je arbeiten per Remote-Zugriff. Früher waren VPNs die bevorzugte Sicherheitslösung von Unternehmen, wenn es darum ging, einen sicheren Zugriff auf ihre Systeme und Dateien bereitzustellen. VPNs sind jedoch aufgrund ihrer Komplexität schwierig zu managen und verursachen Sicherheitsrisiken auf der Netzwerkebene. Zudem bieten sie einen schlechten Benutzerkomfort, einen unzureichenden Datenschutz und sind nicht skalierbar.

Das alte Sicherheitsmodell traditioneller VPNs, bei dem ein Schutzwall um das Unternehmensnetzwerk errichtet wird, wurde durch strenge Zero-Trust-Richtlinien ersetzt. Diese bieten einen kontextbasierten Zugriff auf Anfrage. Citrix Workspace bietet eine cloudbasierte Lösung ohne VPN. Mit dieser können Sie über jedes beliebige Netzwerk auf das gesamte Intranet sowie auf SaaS-, mobile und virtuelle Anwendungen zugreifen – und zwar über gemanagte, ungemanagte sowie Bring-Your-Own-Device (BYOD) Geräte. In dieser Lösungsbeschreibung erklären wir, warum Citrix Workspace eine bessere Wahl ist als VPNs, um die Anforderungen von Remote-Mitarbeitern in Sachen Sicherheit, Performance und Skalierbarkeit zu erfüllen.

VPNs sind komplex und schwierig zu managen

Remote-Mitarbeiter müssen oft verschiedene Zugriffsmethoden verwenden, je nach ihrer Rolle und der Ressource, auf die sie zugreifen möchten. Mitarbeiter, Administratoren, Partner oder Dienstleister nutzen verschiedene Anmeldepunkte innerhalb desselben VPNs. Üblicherweise sind mehrere VPNs erforderlich und auf SaaS-Anwendungen kann man nur mit einem anderen SSO-Portal zugreifen. Für Systemadministratoren ist das sehr zeitaufwändig und das Management kann zahlreiche Ressourcen erfordern. Um Kapazität für den Notfall hinzuzufügen, benötigt man häufig umfangreiche neue Hardware oder man muss in einem langwierigen Prozess neue Lizenzen beschaffen.

Bei VPNs ist es häufig so, dass Nutzer entweder einen vollständigen Zugriff erhalten oder gar keinen. Man muss komplexe VPN-Richtlinien konfigurieren, um zu verhindern, dass ein ungemanagtes Endgerät einen unbeschränkten Zugriff auf Netzwerk, Ressourcen und Daten erhält.

Wenn Sie Ihre traditionellen VPN-Appliances durch vollständig gemanagte, global verfügbare Cloud-basierte Services ersetzen, werden Sicherheitsrichtlinien im Netzwerk nicht mehr benötigt. Der Zugriff auf Anwendungen und Daten wird dann nämlich über kontextbasierte Sicherheitsmaßnahmen abgesichert.

VPNs sind nicht für die Nutzung bei hohem Datenvolumen gedacht

Egal, wo sich ihre Remote-Mitarbeiter befinden, sie erwarten einen nahtlosen Zugriff auf das Unternehmensnetzwerk – genau wie ihre Arbeitgeber. Mit einem VPN wird jedoch jeglicher Traffic von Nutzern durch das Unternehmensnetzwerk geleitet, was Ressourcen belastet und die Performance verschlechtert. VPNs werden zudem häufig an einem zentralen Standort implementiert. Wenn sich Anwender aus unterschiedlichen Regionen der Welt mit internen Web-Anwendungen verbinden, sorgt die zusätzliche Latenz für einen schlechteren Benutzerkomfort.

Remote-Mitarbeiter können es schwer haben, auf traditionelle Client-Server-Anwendungen zuzugreifen, wie z. B. Anwendungen für die Rechnungsstellung oder CRM-Anwendungen. Für diese Anwendungen wird ein Client auf dem Endgerät des Nutzers benötigt. Die Anwendungen nutzen zudem native Protokolle, die hohe Bandbreitenanforderungen haben und VPNs und Netzwerkeingänge schnell überlasten.

Wenn das Netzwerk immer stärker belastet wird und die Latenz steigt, reagieren Anwendungen langsamer. Dies führt zu einer uneinheitlichen und teilweise inakzeptablen Performance. Sie haben keinen Einfluss auf Performance und Benutzerkomfort, wenn am Standort des Nutzers suboptimale Netzwerkbedingungen herrschen.

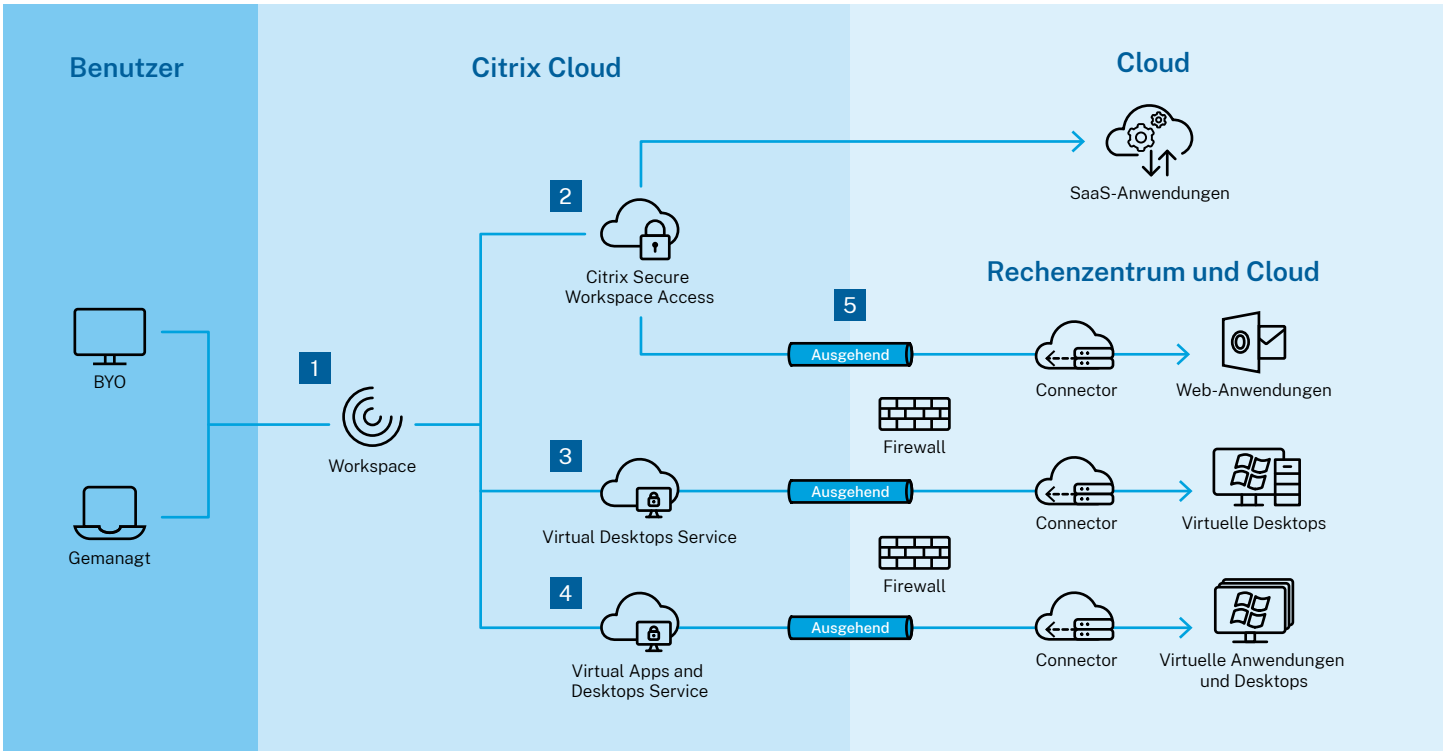
Citrix Workspace bietet Ihren Nutzern ohne VPN Zugriff auf Web-Anwendungen

Mit dem Citrix Secure Workspace Access Service, einem Teil von Citrix Workspace, können Nutzer ohne einen VPN über einen Browser auf Anwendungen zugreifen. Auf diese Art werden moderne Anwendungen nativ auf jedem Endgerät bereitgestellt. Alle kontextbasierten Sicherheitskontrollen sind bereits eingestellt und benötigen keinerlei Zugriff auf Netzwerkebene.

Da Citrix Secure Workspace Access global verfügbar ist, wird ein Nutzer automatisch zum nächstgelegenen Point of Presence (POP) geleitet. Somit profitiert er von der bestmöglichen Performance und Sicherheit bei der Nutzung von SaaS- und Web-Anwendungen.

Traditionelle Client-Server-Anwendungen können durch die Bandbreite beeinträchtigt werden. Ihre Performance leidet, wenn sie über ein Netzwerk mit einer hohen Latenz, wie z. B. ein privates WLAN, genutzt werden. Wenn diese Client-Server-Anwendungen jedoch über eine virtualisierte Plattform bereitgestellt werden, verbessert dies nicht nur den Benutzerkomfort, sondern ermöglicht auch granulare Sicherheitskontrollen auf der Anwendungsebene. Citrix Virtual Apps and Desktops, ein Teil von Citrix Workspace, bietet die beste Sicherheit und Performance für diese Anwendungen. Es werden nämlich Bandbreitenanforderungen minimiert und sowohl Performance als auch Sicherheitsmaßnahmen dynamisch angepasst.

Citrix Virtual Apps and Desktops bietet Remote-Mitarbeitern eine bessere Performance als native Anwendungen.



1. Freie Wahl des Identity Providers (AD, AAD, Okta, Google, Radius und weitere)
2. VPN-freier Zugriff auf SaaS- und Web-Anwendungen mit fortschrittlichen Sicherheitsfunktionen
3. VPN-freier Zugriff auf physische Windows 10-PCs
4. VPN-freier Zugriff mit verbesserter Sicherheit für Windows- und Linux-Anwendungen sowie -Desktops
5. Kontrollkanal für ausgehende Verbindungen bietet ressourcenspezifischen Zugriff

Ineffiziente Anwendungen, die entweder sehr rechenintensiv sind oder das Netzwerk stark belasten, werden im Rechenzentrum virtualisiert und optimiert. Auch der Anwendungs-Client wird virtualisiert und in der Nähe der Datenquelle ausgeführt. Der Remote-Mitarbeiter profitiert von einem für das Internet optimierten Protokoll, das selbst bei stark belasteten Netzwerken eine gute Performance bietet.

VPNs missachten die Privatsphäre von Mitarbeitern

Sicherheitsrichtlinien erfordern ein Monitoring des Netzwerks. Wenn in der VPN-Konfiguration das Split Tunneling deaktiviert wurde, wird jeglicher Datenverkehr, sogar von privaten Anwendungen, über das Unternehmensnetzwerk geleitet. Sie können privaten Datenverkehr überwachen, was eine deutliche Verletzung des Datenschutzes von Remote-Mitarbeitern darstellt, die das Endgerät für private Zwecke nutzen. Remote-Mitarbeiter haben berechtigte Bedenken, dass jemand ihre Internetverbindung abhören und Zugriff auf ihren Computer und ihr Heimnetzwerk erhalten könnte. Es könnten auch Daten über die von ihnen besuchten Webseiten gesammelt werden.

Wenn der Zugriff jedoch bei der Anwendungsebene endet, können Mitarbeiter beruhigt sein, dass ihre Privatsphäre geschützt ist. Der Endanwender wird nicht überwacht und privater Netzwerk-Traffic bleibt privat.

Durch VPNs können BYOD-Geräte IT-Teams und die Infrastruktur stärker belasten

Viele Organisationen erkennen die Vorteile, die Bring-Your-Own-Device Initiativen bieten. Hierbei wird Mitarbeitern genehmigt, ihre eigenen Endgeräte für die Arbeit zu nutzen. Wenn sich jedoch die Remote-Mitarbeiter einer Organisation per VPN mit dem Netzwerk verbinden und regelmäßige Sicherheitsupdates installiert werden, müssen IT-Ressourcen aufgewendet werden, um die Compliance und die Kompatibilität der Mitarbeitergeräte sicherzustellen. Ab diesem Punkt hören BYOD-Initiativen auf, Endgeräte- und Zugriffskosten zu verringern. Sie belasten stattdessen die IT-Infrastruktur stark.

Viele VPNs bieten keine kontextbasierten granularen Sicherheitsrichtlinien, um BYOD- und ungemanagte Endgeräte zu unterstützen. Remote-Mitarbeiter müssen ein vom Unternehmen ausgestelltes und genehmigtes Endgerät besitzen. Viele Organisationen nutzen auch Drittanbieter, die sich um Gehaltsabrechnungen, Zusatzleistungen und Help Desk Support kümmern. Da unabhängige Drittanbieter ihre

eigenen Endgeräte verwenden, ist es unmöglich, diese zu überwachen und abzusichern.

Im Gegensatz dazu bietet Citrix Workspace durch die Citrix Workspace-App oder einen Webbrowser einen erstklassigen Benutzerkomfort auf jedem Endgerät.

Remote-Mitarbeiter können über private oder BYOD-Geräte Zugriff auf physische Desktops anfordern. Mit Citrix Remote PC Access können sich Endanwender von überall per Remote-Zugriff mit ihrem physischen Windows-PC im Büro verbinden. Für mobile Endgeräte gibt es Micro-VPNs für einzelne Anwendungen, wodurch keine vollständigen VPNs benötigt werden, die dem gesamten Endgerät Zugriff gewähren. Der Benutzerkomfort wird verbessert, da kein VPN-Client mehr konfiguriert und gestartet werden muss. Dadurch wird ein nahtloser Zugriff auf geschützte Unternehmensdaten ermöglicht.

VPNs bieten einen umfassenden Zugriff auf Ihr gesamtes Netzwerk

VPNs basieren auf einem veralteten Sicherheitsmodell, das entweder einen vollständigen oder gar keinen Zugriff auf das Netzwerk gewährt. Zudem bieten Sie Ihnen keine Möglichkeit zu sehen, wer worauf zugreift. Dadurch ist es schwieriger, auf Bedrohungen innerhalb des Netzwerks einzugehen, z. B. aufgrund gestohlener Anmeldedaten.

VPNs erhöhen die Wahrscheinlichkeit von Angriffen auf das Netzwerk, auch wenn Nutzer nur Zugriff auf Anwendungen benötigen. Selbst infizierte Endgeräte können auf das Netzwerk zugreifen, wodurch Malware leicht verbreitet werden kann.

Citrix Workspace ist eine sichere Lösung für Remote-Mitarbeiter, die kein VPN verwendet

Citrix bietet eine zentrale, stressfreie Umgebung für die Remote-Arbeit, die alle Probleme Ihrer Organisation bezüglich Sicherheit, Management und Skalierbarkeit löst. Citrix Workspace macht alle Ressourcen über eine einzelne personalisierte Benutzeroberfläche verfügbar. Auf diese kann über jedes beliebige Endgerät zugegriffen werden.

Egal, welchen Ansatz und welches Endgerät Remote-Mitarbeiter wählen, sie können über einen SSO (Single Sign-On) auf ihre Anwendungen, Dateien und Daten zugreifen – ganz ohne VPN. Die Sicherheit wird durch den Citrix Secure Workspace Access verbessert. Dieser ersetzt traditionelle VPN-Appliances durch einen vollständig gemanagten, global verfügbaren Cloud-basierten Service. Komplexe Sicherheitsrichtlinien im Netzwerk werden durch einen geschützten Zugriff auf Anwendungen und Daten ersetzt.

Egal, ob Ihre Mitarbeiter virtuelle, Web- oder SaaS-Anwendungen nutzen: Citrix Workspace stellt anhand von konditionalen und kontextbasierten Informationen zu den Benutzern und ihren Endgeräten fest, ob sie dazu berechtigt sind. Mithilfe von kontextbasierten Sicherheitsrichtlinien können Sie nicht nur Benutzer identifizieren und authentifizieren, sondern auch kontrollieren, welche Aktionen sie innerhalb einer Anwendung ausführen können. Dies hängt von verschiedenen Faktoren ab, z. B. dem Nutzer, dem Endgerätezustand, dem Standort und der IP-Adresse. Mit Citrix Workspace können Organisationen zudem den Zugriff auf Anwendungen und Ressourcen einschränken. Nur vertraute Benutzer und Endgeräte dürfen bestimmte Funktionen ausführen, beispielsweise Ausschneiden und Einfügen, Drucken und das lokale Kopieren von Dateien.

Mit dem Citrix Secure Workspace Access Service können Sie sichere Zugriffskontrollen hinzufügen und SaaS- sowie Web-Anwendungen detailliert überwachen. Richtlinien zum Schutz von Anwendungen schützen vor Malware, die Tastenanschläge oder den Bildschirm aufzeichnen. Wasserzeichen sichern den Zugriff auf vertrauliche Anwendungen und Informationen ab. Statt einem Remote-Mitarbeiter, der sich über ein unbekanntes Endgerät verbindet, den Zugriff komplett zu verwehren, können Sie einschränken, auf welche Funktionen der Nutzer zugreifen kann.

Citrix Workspace ermöglicht es Administratoren, Nutzer konstant zu überwachen und Risikobewertungen zu erstellen. Nach der ersten Anmeldung kann der Zugriff eingeschränkt werden, um das Unternehmen zu schützen.

Vorteile von Citrix Secure Workspace Access:

- Einfache Implementierung und Konfiguration
- Einfaches Management und unkomplizierte Wartung
- Schützt das zugrundeliegende Netzwerk
- Datenschutz für Nutzer
- Nutzt kontextbasierte oder konditionale Zugriffskontrolle
- Bietet einen erstklassigen Benutzerkomfort
- Schnelle Skalierung und Provisioning
- Hohe Performance für Remote-Mitarbeiter
- Freie Wahl des Endgeräts (BYOD)
- Konstante Absicherung und Überwachung

Fazit

Für jede Organisation ist es wichtig, dass sich Remote-Mitarbeiter auf sichere Weise verbinden können, genauso sicher wie Mitarbeiter vor Ort. Dabei darf es keine Rolle spielen, wo sie sich befinden oder welches Endgerät sie verwenden. Anders als mit traditionellen VPNs behalten Sie mit Citrix Workspace den notwendigen Überblick und die Kontrolle über Ihre Infrastruktur.

Um mehr über die Funktionen und Vorteile von Citrix Workspace zu erfahren, wenden Sie sich an Ihren Vertriebsmitarbeiter oder gehen Sie auf citrix.de/workspace.

Enterprise Sales
Nordamerika | 800-424-8749
Weltweit | +1 408 790 8000

Standorte
Unternehmenszentrale | 851 Cypress Creek Road, Fort Lauderdale, FL 33309, USA
Silicon Valley | 4988 Great America Parkway, Santa Clara, CA 95054, USA