

# Ein Single Sign-On, wie er sein sollte

Sechs Wege, wie Citrix Workspace einen nahtlosen Zugriff auf alle Anwendungen bereitstellt und gleichzeitig die Sicherheit und den Benutzerkomfort verbessert



## SSO (Single Sign-On) Lösungen wurden entwickelt, um das Leben von Mitarbeitern und IT zu vereinfachen.

SSO-Lösungen wurden entwickelt, um Managementkosten zu reduzieren und die Sicherheit zu erhöhen, während gleichzeitig der Benutzerkomfort verbessert wird. Viele Lösungen können diese Anforderungen jedoch nicht erfüllen und unterstützen nur einen bestimmten Anwendungstyp bzw. -untertyp. Dadurch sind Sie gezwungen, mehrere Zugangslösungen von verschiedenen Anbietern zu implementieren, um alle Anwendungen zu unterstützen. Dies macht jedoch alle Vorteile zunichte, die Sie sich in puncto Produktivität und Benutzerkomfort erhofft haben. Die Komplexität, die dadurch entsteht, läuft den Zero-Trust-Initiativen zuwider, die viele Organisationen eingeführt haben.

**Mit Citrix Workspace können Sie alle Anwendungen und Daten** in Ihrer dezentralen IT-Architektur konsolidieren, um einen Single Sign-On auf alle Anwendungen und Daten bereitzustellen, die Ihre Anwender für die Arbeit benötigen.

Citrix Secure Private Access arbeitet mit Ihrer vorhandenen Infrastruktur zusammen und konsolidiert mehrere Lösungen für den Remote-Zugriff wie z. B. traditionelle VPNs oder SSO-Lösungen. Dadurch wird das Management für die IT vereinfacht und Mitarbeitern ein zentraler Zugriff ermöglicht.

# Sechs Vorteile der SSO-Lösung von Citrix Workspace

1. Sicherer vertraulicher Zugriff auf Unternehmensressourcen ohne VPN
2. Eine granulare Kontrolle für SaaS-Anwendungen und das Internet
3. Kontrolle über Ihre Benutzeridentität
4. Besserer Schutz als nur Benutzernamen und Passwörter
5. Nahtlose Integration in Ihre bestehende Umgebung
6. Probleme schneller lösen mit End-to-End-Visibilität

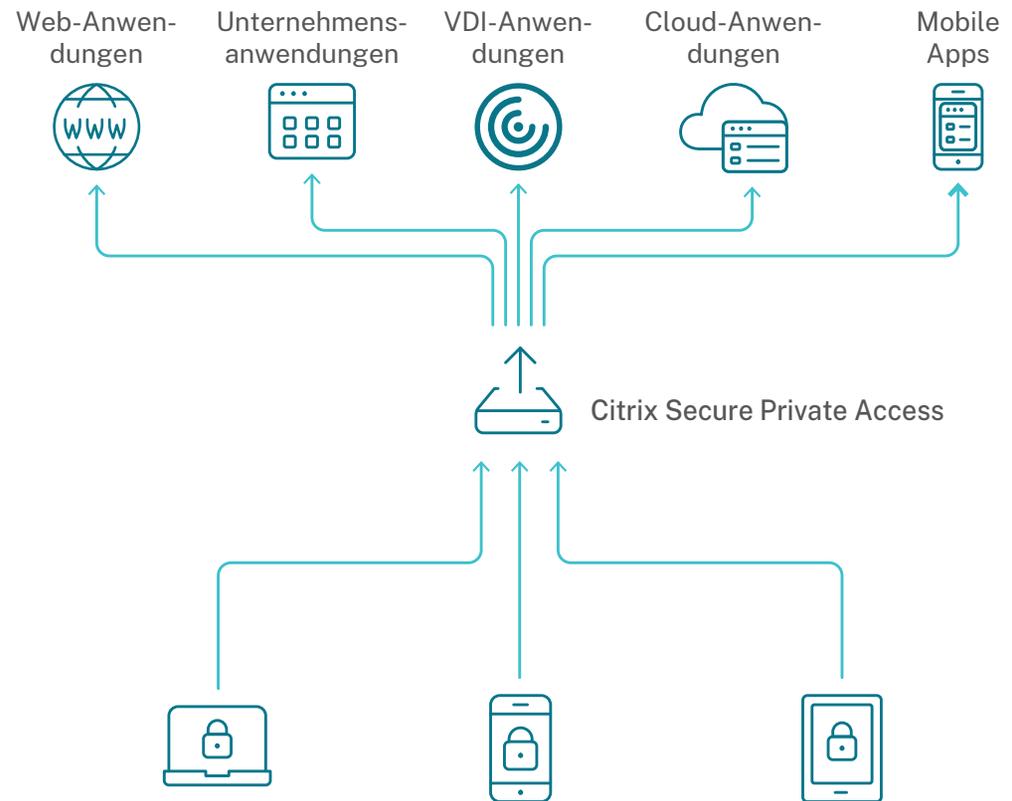
**Erfahren Sie auf den folgenden Seiten mehr zu jedem dieser Vorteile.**



# 1 Sicherer vertraulicher Zugriff auf Unternehmensressourcen ohne VPN

Viele Lösungen unterstützen nur bestimmte Anwendungstypen. Wenn Sie beispielsweise eine Lösung haben, die nur Ihre virtuellen und lokalen Unternehmens-Anwendungen unterstützt, benötigen Sie eine separate SSO-Lösung, um Zugriff auf Web- und SaaS-Anwendungen zu erhalten.

Citrix Workspace vereinfacht mit SSO den Zugriff auf virtuelle, SaaS- und Web-Anwendungen sowie Dateien-Repositorys in der Cloud und in Ihrem Rechenzentrum. Wenn Sie die Komplexität verringern, die durch das Vorhandensein mehrerer Zugangslösungen wie VPNs und SSO entsteht, kann die IT ihre Zero-Trust-Strategie besser umsetzen und gleichzeitig den Benutzerkomfort verbessern.



**Citrix Workspace mit Secure Private Access bietet Ihnen Zugriff auf alle Ihre Anwendungen und Daten**

## 2 Eine granulare Kontrolle für SaaS-Anwendungen und das Internet

Ihre SSO-Lösung sollte mehr bieten können als einen einfachen Zugriff. Sie benötigen zusätzlich granulare, kontextbasierte Kontrollen für SaaS- und Web-Anwendungen.

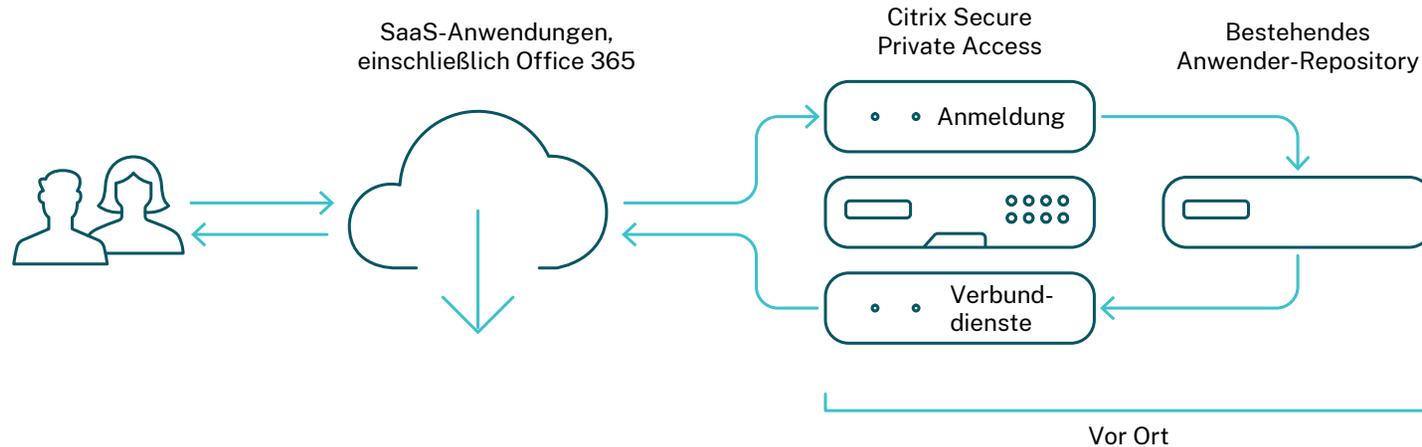
Außerdem stellt es ein Risiko für Ihre Organisation dar, wenn Mitarbeiter das Internet unüberwacht nutzen. Einige Organisationen schränken das Surfen im Internet ein, dies kann aber der Produktivität schaden.

Datenschutz ist für die meisten Organisationen eines der wichtigsten Ziele von Zero Trust. Citrix Secure Private Access unterstützt Sie beim Schutz von Daten durch fortschrittliche Sicherheitsrichtlinien für SaaS- und Web-Anwendungen. Über Kontrollfunktionen können Sie beispielsweise das Kopieren/Einfügen von Daten, das Drucken von Dokumenten oder das Herunterladen von Inhalten einschränken. Sie können zudem die Navigationsleiste, die Schaltflächen Zurück/Vorwärts oder den mobilen Zugriff kontrollieren und Wasserzeichen verwenden.

Administratoren können eine Blacklist oder Whitelist für URL-Kategorien erstellen, um den Zugriff auf Webseiten einzuschränken oder zu gewähren. Sie können auch URLs deaktivieren, die über SaaS-Anwendungen aufgerufen wurden. Zudem können Sie unbekannte SaaS-Anwendungen oder Links in einem sicheren Browser anzeigen, um sie vom Unternehmensnetzwerk und Ihren Unternehmensressourcen zu isolieren. So schützen Sie die Organisation, da Malware, die über schädliche Seiten verbreitet wird, niemals in Ihr Unternehmensnetzwerk gelangt.

Citrix Secure Private Access unterstützt standardmäßig einige der bekanntesten SaaS-Anwendungen, unter anderem Salesforce, G Suite, Office 365, Zoom, Workday und Expensify. Sie können vorkonfigurierte Anwendungsvorlagen verwenden, um auf einfache Weise Anwendungen zu veröffentlichen und Single Sign-On Richtlinien zu konfigurieren.

# 3 Kontrolle über Ihre Benutzeridentität



SaaS-Anwendungen wie Microsoft Office 365, Salesforce, Workday und ADP werden heutzutage immer wichtiger für die Arbeit. In der Tat nutzen große Unternehmen durchschnittlich 1.427 verschiedene Cloud-Services.<sup>1</sup>

Diese Anwendungen werden über eine Cloud bereitgestellt und befinden sich außerhalb des lokalen Netzwerks. Um einen SSO für sie zu ermöglichen, erfordern die meisten Lösungen eine Migration des gesamten Anwenderverzeichnisses in die Cloud. Dadurch werden Sie gezwungen, Ihre bestehende Identitätsinfrastruktur komplett zu ersetzen. Mit Citrix Secure Private Access haben Sie die Wahl und können Ihre eigene

Identitätsinfrastruktur für Citrix Workspace verwenden. Wir unterstützen zahlreiche Identitätsplattformen wie Microsoft, Google und Okta. Dies wird durch föderierte Identitäten ermöglicht. Hierbei werden interne SAML- oder ADFS-Verbunddienste genutzt, um einen sicheren, vertrauenswürdigen Token für den Cloud-Service bereitzustellen. Der Token enthält eine Reihe an Informationen zum authentifizierten Anwender, einschließlich seiner Identität. Diese Daten werden anschließend durch die eigenen Verbunddienste der Cloud validiert.

Mit Citrix haben Sie die Wahl und können Ihre bestehenden Investitionen in Identity Provider weiterhin ausschöpfen. Gleichzeitig erhalten Sie einen sicheren vertraulichen Zugriff auf Ihre Unternehmensressourcen.

# 4 Besserer Schutz als nur Benutzernamen und Passwörter

Die Authentifizierung von Anwendern wird immer wichtiger, besonders weil Organisationen jetzt Business Continuity Pläne implementieren und ein Großteil ihrer Mitarbeiter per Remote-Zugriff auf Unternehmensressourcen zugreift. Diese Mitarbeiter sowie Partner und Auftragnehmer, die nicht notwendigerweise Teil des Nutzerverzeichnisses des Unternehmens sind, nutzen private Endgeräte, um auf das Unternehmensnetzwerk zuzugreifen. Deswegen ist es besonders wichtig, Anwender schnell und zuverlässig zu identifizieren, sodass sie Zugriff auf Unternehmensressourcen haben.

Deswegen verlässt sich Citrix Secure Private Access nicht nur auf Benutzernamen und Passwörter. Die Lösung unterstützt Multi-Faktor-Authentifizierung, welche es der IT erlaubt, granular zu kontrollieren, wer auf das Unternehmensnetzwerk zugreift, worauf zugegriffen wird, zu welchem Zeitpunkt und mit welchem Endgerät.

Authentifizierungsmechanismen und -protokolle integrieren und unterstützt diese, darunter RADIUS, TACACS, NTLM, Diameter, SAML 2.0, OAuth 2.0 und OpenID 2.0. Die Lösung unterstützt auch Azure Active Directory für die Multi-Faktor-Authentifizierung mit Anmeldung ohne Passwort sowie ein lokales Active Directory für die Zwei-Faktor-Authentifizierung mithilfe eines nativen OTP.

Citrix Secure Private Access bietet Funktionen zum Scannen von Endbenutzergeräten vor und nach der Einrichtung einer Anwendersitzung. Anhand der Rolle, des Standorts und der Sicherheit des Endgeräts des Anwenders kann ein Administrator definieren, wie der Zugriff auf Anwendungen authentifiziert und autorisiert werden soll.



## 5 Nahtlose Integration in Ihre bestehende Umgebung

Eine Single Sign-On Lösung hat viele Berührungspunkte in Ihrer Umgebung: das Anwenderverzeichnis, die Authentifizierungsmechanismen, Anwendungen und selbst die Endgeräte

der Nutzer. Citrix Secure Private Access lässt sich einfach in Ihre bestehende Infrastruktur integrieren, damit Sie einen großartigen Benutzerkomfort bereitstellen und das IT-Management vereinfachen können.

Platzieren Sie Ihre Markenlogos auf dem individuell anpassbaren Anwendungsportal für Nutzer

Unterstützen Sie alle Authentifizierungsverfahren, einschließlich RADIUS, Diameter, Kerberos, Microsoft NTLM, TACACS und formularbasierte Authentifizierung

Unterstützen Sie alle Geräte von Endbenutzern, einschließlich Windows, Mac, Linux, iOS und Android

Unterstützen Sie alle SSO-Protokolle, einschließlich SAML, OAuth und OpenID

Bei der Wahl einer Authentifizierungslösung war für uns am wichtigsten, dass die Lösung sich einfach in unsere aktuellen Systeme integrieren lässt.<sup>2</sup>

## 6 Probleme schneller lösen mit End-to-End-Visibilität

Weil Citrix Secure Private Access Zugriff auf Ihre gesamte Anwendungsumgebung bereitstellt, kann die Lösung Ihnen einen umfassenden Einblick in diese gewähren. Dadurch können Sie die Anwendungsbereitstellung und die Performance überwachen und auftretende Mängel beheben.

Citrix Analytics, eine weitere Komponente von Citrix Workspace, bietet Ihnen einen durchgängigen Einblick in alle TCP- und HTTP-Sitzungen von Anwendern. Insight erfasst Authentifizierungsfehler, die durch ein abgelaufenes Passwort, ein gesperrtes Konto, einen fehlgeschlagenen Endgerätescan und andere SSO- oder Anwendungsstartfehler verursacht wurden, und ermöglicht dadurch eine schnellere Fehlerbehebung.

Citrix Analytics ermöglicht auch eine fortlaufende Authentifizierung und Autorisierung. Dies ist für viele Organisationen ein wichtiger Teil der Zero-Trust-Strategie. Bei Veränderungen des Benutzerkontexts, z. B. einem Login an einem anderen Standort oder mit einem neuen Endgerät, können zusätzliche Sicherheitskontrollen aktiviert werden, bevor der Zugriff auf die Unternehmensressource gewährt wird. Dabei kann es sich beispielsweise um einen zweiten Authentifizierungsfaktor handeln.

Mithilfe von Risikoindikatoren und Funktionen zur Erkennung von anomalem Nutzerverhalten können Sie Richtlinienkontrollen einrichten, die Sie frühzeitig vor schädlichem oder riskantem Nutzerverhalten warnen. Dazu gehören beispielsweise das Hoch- oder Herunterladen von Informationen an bzw. von schädlichen und riskanten Websites. Die automatischen Funktionen von Citrix Analytics können bestimmte Maßnahmen für Sie einleiten. Beispielsweise können Sitzungen aufgezeichnet, Links zu Dokumenten ungültig gemacht oder Anwenderkonten gesperrt werden.

Ermöglichen Sie Mitarbeitern, so zu arbeiten, wie sie es möchten. Mit Citrix Workspace können Sie einen tatsächlichen Single Sign-On für alle Anwendungen einrichten, indem Sie traditionelle VPNs oder SSO-Lösungen ersetzen. Vereinfachen Sie das IT-Management, stärken Sie die Sicherheit und verbessern Sie den Benutzerkomfort.

Weitere Informationen erhalten Sie auf [citrix.de/workspace](https://citrix.de/workspace).



Quellen:

1. 12 Must-Know Statistics on Cloud Usage in the Enterprise, Skyhigh Networks.
2. 2017 State of Authentication Report, Javelin.

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

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