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

Inhalte

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

Sie sollten Managementkosten reduzieren, die Sicherheit erhöhen und den Benutzerkomfort verbessern. Viele Lösungen können diese Anforderungen jedoch nicht erfüllen und unterstützen nur einen bestimmten Anwendungstyp bzw. -untertyp. Dadurch sind Sie gezwungen, mehrere SSO-Lösungen 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.

Mit Citrix Workspace **können Sie alle Anwendungen und Daten** in Ihrer dezentralen IT-Architektur **konsolidieren**, um einen Single Sign-On auf alle IT-Ressourcen bereitzustellen, die Ihre Anwender für die Arbeit benötigen. Citrix Access Control, eine Schlüsselkomponente von Citrix Workspace, konsolidiert mehrere Lösungen für den Remote-Zugriff in Ihrer bestehenden Infrastruktur. Dadurch wird das Management für die IT vereinfacht und Mitarbeitern ein benutzerfreundlicher Zugriff ermöglicht.

Sechs Vorteile der SSO-Lösung von Citrix Workspace

← Seite 3 | Seite 5 →

Zurück zum Inhaltsverzeichnis

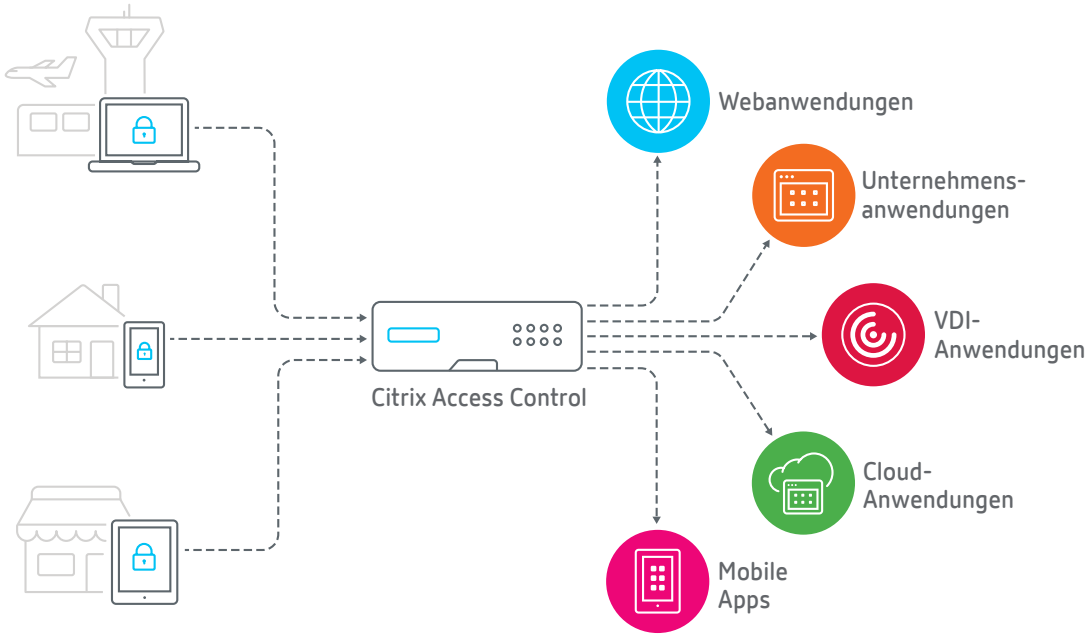
1. Sicherer Zugang zu allen IT-Ressourcen

Viele SSO-Lösungen unterstützen nur bestimmte Anwendungstypen. Wenn Sie beispielsweise eine Lösung haben, die nur virtuelle und lokale Unternehmens-Anwendungen unterstützt, benötigen Sie eine separate IDaaS (Identity as a service) Lösung, um Zugriff auf Web- und SaaS-Anwendungen zu ermöglichen.

Citrix Workspace mit Citrix Access Control ermöglicht Ihnen Zugriff auf alle Ihre Anwendungen

– sowie andere

Unternehmensressourcen, z. B. freigegebene Netzlaufwerke.



SSL VPN-basierter Remote-Zugriff ermöglicht den Anwendern, sich mit Netzwerk-Ressourcen von Remote-Standorten zu verbinden, damit sie standortunabhängig arbeiten können. Citrix Workspace nutzt zudem MicroVPN-Technologie, um mobile Endgeräte sicher mit diesen Ressourcen zu verbinden.

← Seite 4 | Seite 6 →

Zurück zum Inhaltsverzeichnis

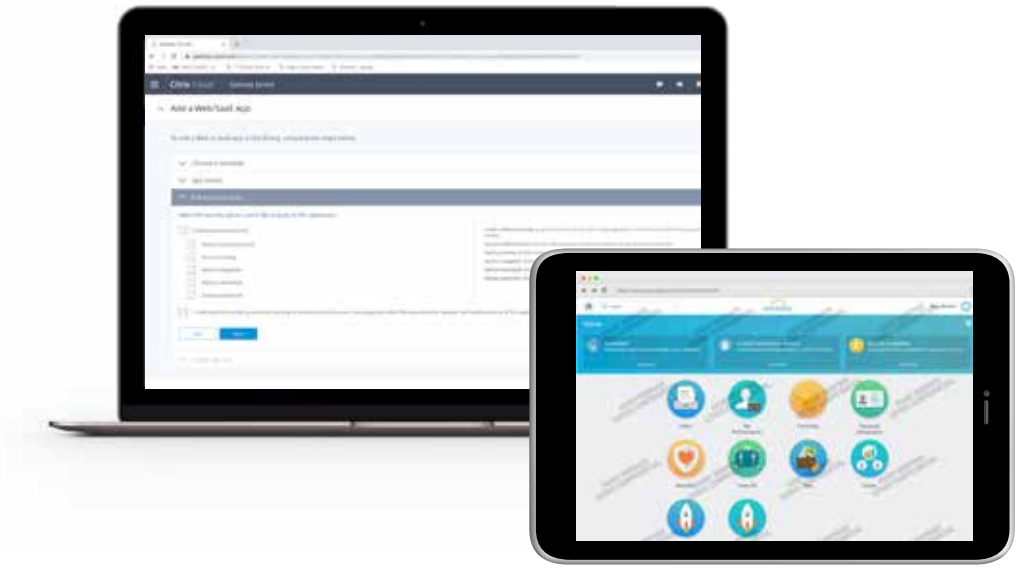
2. Eine granulare Kontrolle für SaaS-Anwendungen und das Internet

Ihre SSO-Lösung sollte mehr bieten können als einen einfachen Zugriff. Richten Sie granulare, kontextbasierte Kontrollen für SaaS-Anwendungen ein.

Es stellt ein Risiko für Ihre Organisation dar, wenn Mitarbeiter das Internet unüberwacht nutzen. Nicht selten verbieten Organisationen ihren Mitarbeitern das Surfen im Internet. Dies könnte jedoch die Produktivität negativ beeinträchtigen.

Citrix Workspace mit Citrix Access Control bietet verbesserte Sicherheitsrichtlinien für SaaS- und Web-Anwendungen. Schränken Sie bestimmte Aktionen wie Kopieren/Einfügen, Drucken und Herunterladen ein. Kontrollieren Sie die Navigationsleiste, die Schaltflächen Zurück/Vorwärts, den mobilen Zugriff und verwenden Sie Wasserzeichen. Sie 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.

Citrix Access Control unterstützt standardmäßig einige bekannte SaaS-Anwendungen, unter anderem SalesForce, G Suite, Office 365, Zoom, Workday, Expensify. Sie können vorkonfigurierte Anwendungs-Vorlagen verwenden, um auf einfache Weise Anwendungen zu veröffentlichen und Single Sign-On Richtlinien zu konfigurieren.



← Seite 5 | Seite 7 →

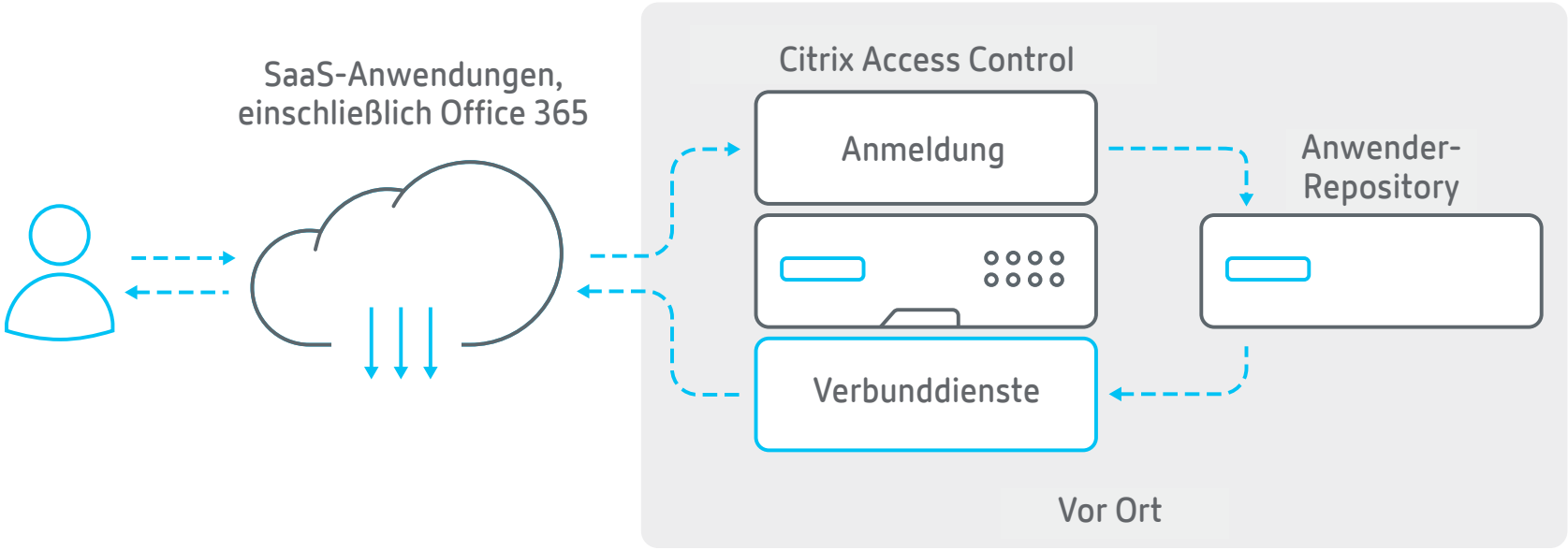
Zurück zum Inhaltsverzeichnis

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.[1]

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. Mit Citrix Access Control können Sie dieses auch weiterhin im Rechenzentrum speichern.

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.



← Seite 6 | Seite 8 →

Zurück zum Inhaltsverzeichnis

4. Besserer Schutz als nur Benutzernamen und Passwörter

Die Authentifizierung von Benutzern wird immer wichtiger, besonders weil Mitarbeiter immer mehr Endgeräte nutzen und von verschiedenen Standorten aus arbeiten. Viele Organisationen möchten auch ihren Partnern und Auftragnehmern, die nicht Teil des Anwenderverzeichnisses sind, einen Remote-Zugriff auf Unternehmensanwendungen und -daten bieten. Deswegen ist es besonders wichtig, Anwender schnell und zuverlässig zu identifizieren, sodass sie Zugriff auf Unternehmensressourcen haben.

Aus diesem Grund verlässt sich Citrix Access Control nicht ausschließlich 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.

Citrix Access Control lässt sich in alle Authentifizierungsmechanismen und -protokolle integrieren und unterstützt diese, darunter RADIUS, TACACS, NTLM, Diameter, SAML 2.0, OAuth 2.0 und OpenID 2.0. Citrix Access Control unterstützt auch Azure Active Directory für die Multi-Faktor-Authentifizierung sowie ein lokales Active Directory für die Zwei-Faktor-Authentifizierung mithilfe eines nativen OTP.

← Seite 7 | Seite 9 →

Zurück zum Inhaltsverzeichnis

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 Access Control 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.[2]

← Seite 8 | Seite 10 →

Zurück zum Inhaltsverzeichnis

6. Probleme schneller lösen mit durchgängiger Visibilität

Weil Citrix Access Control 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.

Gemeinsam mit Citrix Analytics, einer weiteren Schlüsselkomponente von Citrix Workspace, bietet Ihnen Citrix Access Control einen durchgängigen Einblick in alle TCP- und HTTP-Sitzungen von Anwendern. Insight erfasst neben SSO- oder Anwendungsstartfehlern auch Authentifizierungsfehler, die durch ein abgelaufenes Kennwort, ein gesperrtes Konto oder einen fehlgeschlagenen Endgerätescan verursacht wurden, und ermöglicht dadurch eine schnellere Fehlerbehebung.

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. Sie können zudem anzeigen, welche Webseiten von welchen Anwendern im Laufe der Zeit besucht wurden.

CITRIX®

Ermöglichen Sie Mitarbeitern, so zu arbeiten, wie sie es möchten. Mit Citrix Workspace können Sie einen umfassenden Single Sign-On für alle Anwendungen bereitstellen. Dadurch wird das IT-Management vereinfacht, die Sicherheit gestärkt und der Benutzerkomfort verbessert.

Mehr über Citrix Workspace erfahren

Quellen:

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

Zurück zum Inhaltsverzeichnis