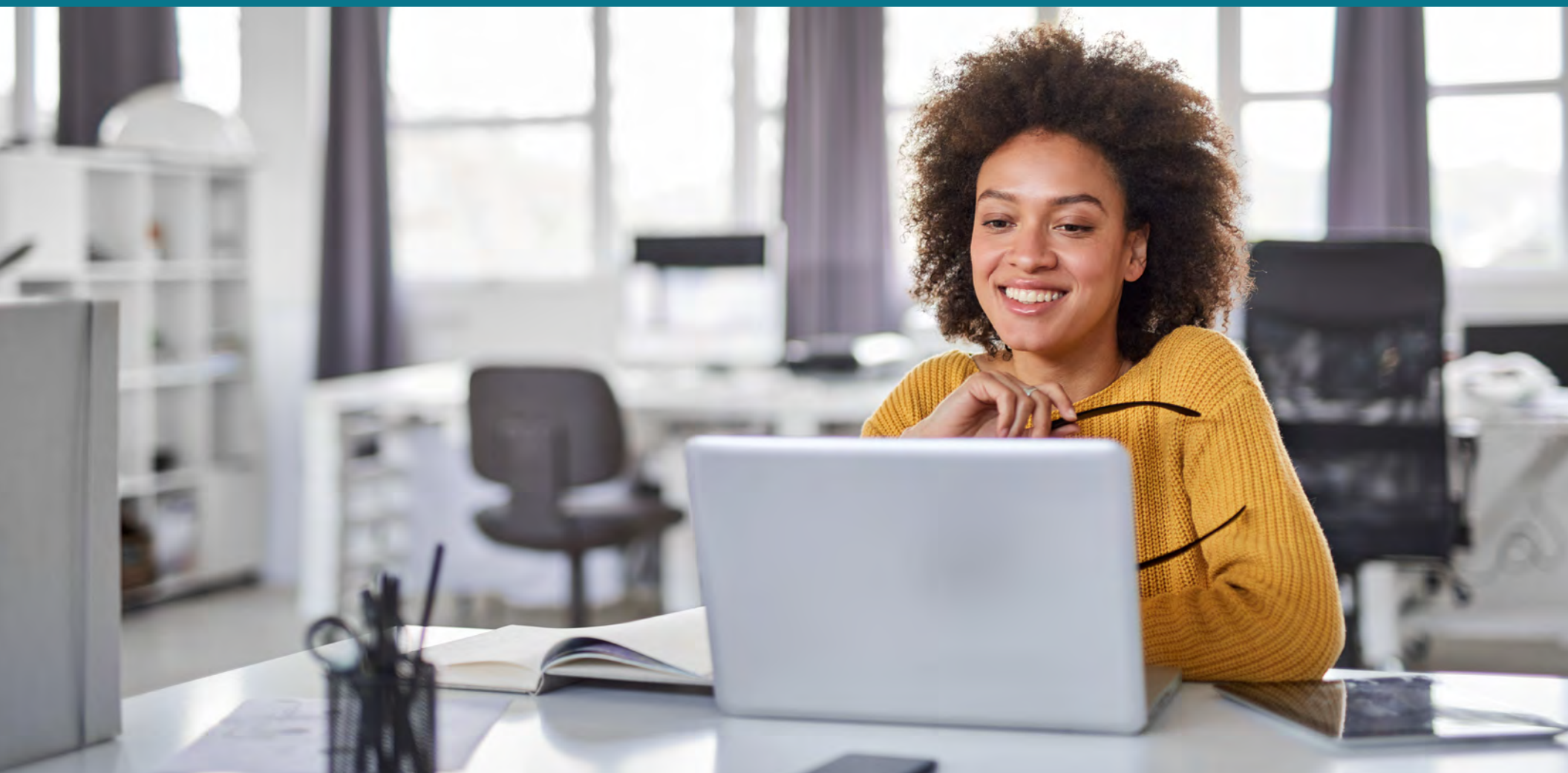


Le SSO (Single Sign-On) tel qu'il devrait être

6 façons pour Citrix Workspace de garantir un accès fluide à toutes les applications, tout en renforçant la sécurité et la qualité de l'expérience utilisateur



Les solutions d'authentification unique (SSO) ont été conçues pour faciliter la vie des collaborateurs et des équipes IT.

Les solutions SSO sont supposées réduire les coûts de management, renforcer la sécurité, tout en offrant une meilleure expérience utilisateur. Cependant, de nombreuses solutions ne sont pas à la hauteur, ne couvrant qu'un seul type ou un sous-ensemble de types d'applications. Vous êtes ainsi obligé de mettre en œuvre plusieurs solutions d'accès issues de différents fournisseurs afin de couvrir l'intégralité de votre paysage applicatif, renonçant aux avantages de productivité et d'expérience utilisateur auxquels vous aspiriez. La complexité générée par ce type de déploiement va également à l'encontre des initiatives de confiance zéro adoptées par de nombreuses entreprises.

Citrix Workspace vous aide à unifier toutes les applications et les données de votre architecture IT distribuée pour fournir un SSO (Single Sign-On) à toutes les applications et données dont vos collaborateurs ont besoin pour être productifs.

Fonctionnant avec votre infrastructure existante, Citrix Secure Private Access consolide plusieurs solutions d'accès distant, comme les VPN traditionnels ou les solutions d'authentification unique, simplifiant ainsi la gestion de l'informatique et offrant un accès unifié aux employés.

6 avantages de la solution d'authentification unique de Citrix Workspace

1. Accès privé sécurisé et sans VPN aux ressources de l'entreprise
2. Contrôle granulaire des applications SaaS et du web
3. Contrôle de votre identité d'utilisateur
4. Sécurité au-delà des noms d'utilisateur et des mots de passe
5. Intégration fluide avec votre environnement existant
6. Résolution plus rapide des problèmes avec une visibilité de bout en bout

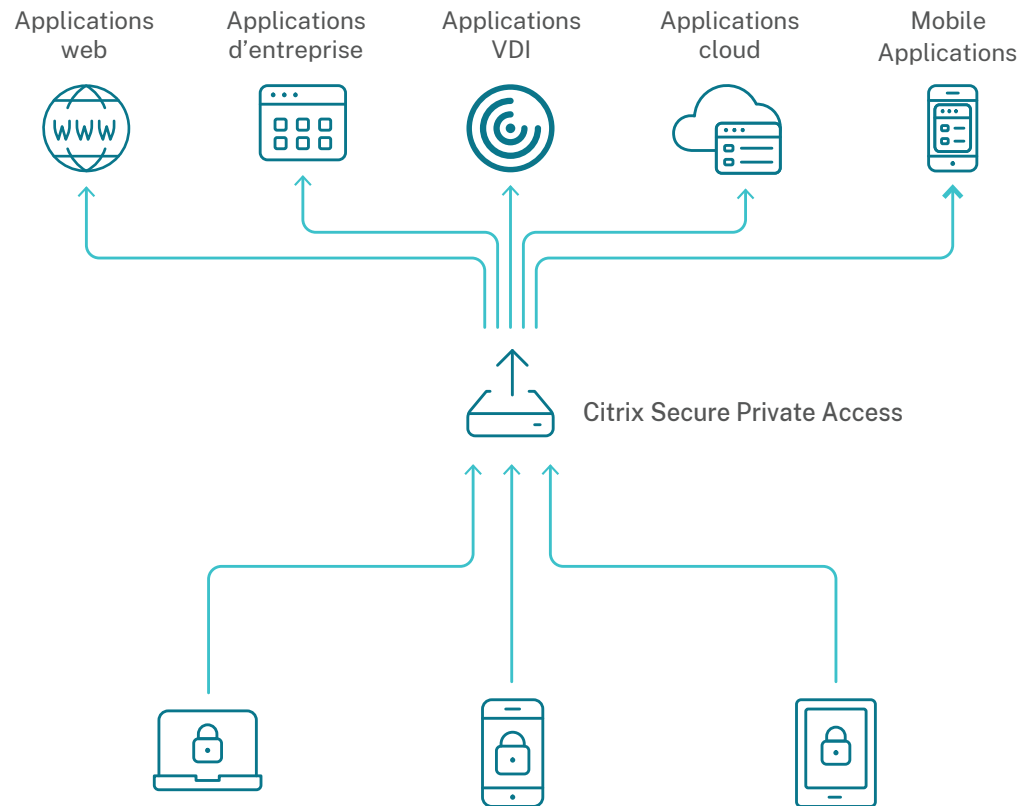
Découvrez les détails de chaque avantage dans les pages suivantes.



1 Accès privé sécurisé et sans VPN aux ressources de l'entreprise

De nombreuses solutions ne couvrent qu'une partie de vos applications. Si vous avez une solution qui couvre uniquement vos applications d'entreprise et virtuelles, par exemple, vous aurez besoin d'une solution SSO séparée pour fournir un accès à vos applications web et SaaS.

Citrix Workspace simplifie l'accès avec authentification unique aux applications virtuelles, SaaS et Web, ainsi qu'aux bibliothèques de fichiers dans le cloud et dans votre datacenter. En réduisant la complexité des solutions d'accès multiples comme les VPN et l'authentification unique, les équipes informatiques peuvent obtenir les résultats correspondant à leur stratégie Zero Trust tout en améliorant l'expérience de l'utilisateur final.



Citrix Workspace avec Secure Private Access vous donne accès à toutes vos applications et données

Contrôle granulaire des applications SaaS et du web

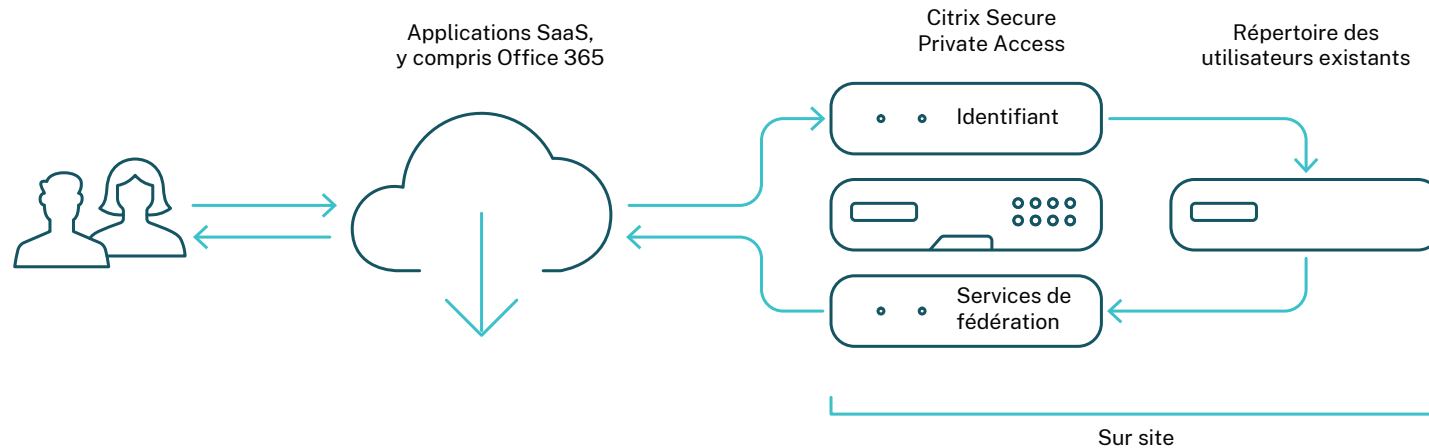
Votre solution SSO doit aller au-delà d'un accès basique et vous offrir un contrôle contextuel et granulaire sur les applications SaaS et web.

La navigation Internet non surveillée expose en outre votre entreprise à des risques. Certaines entreprises limitent la navigation sur Internet, mais cela peut entraver la productivité. La protection des données est l'un des principaux objectifs Zero Trust que la plupart des entreprises cherchent à atteindre. Citrix Secure Private Access aide à protéger les données grâce à des politiques de sécurité renforcées pour les applications SaaS et Web. Les contrôles comprennent notamment la restriction du copier/coller, de l'impression et de la possibilité de télécharger du contenu. Vous pouvez également contrôler la barre de navigation, les boutons suivant/précédent et l'accès mobile, ainsi qu'activer l'application d'images en filigrane.

Les administrateurs peuvent créer des listes noires et blanches de catégories d'URL pour autoriser ou refuser l'accès à certains sites web. Vous pouvez également désactiver les URL lancées depuis des applications SaaS ou présenter les applications SaaS ou les liens web inconnus dans un navigateur sécurisé pour les isoler des ressources ou du réseau d'entreprise. L'entreprise est protégée, les malwares introduits par des sites malveillants ne touchant jamais son infrastructure.

Citrix Secure Private Access prend en charge les applications SaaS les plus populaires, notamment Salesforce, G Suite, Office 365, Zoom, Workday et Expensify, dans son catalogue prêt à l'emploi. Vous pouvez utiliser des modèles d'application préconfigurés pour publier facilement des applications et configurer des stratégies d'authentification unique.

3 Contrôle de votre identité d'utilisateur



Les applications SaaS telles que Microsoft Office 365, Salesforce, Workday et ADP sont aujourd'hui essentielles à notre travail. En fait, l'entreprise moyenne utilise 1 427 services cloud distincts.¹

Pour fournir une solution d'authentification unique (SSO) à ces applications (qui sont mises à disposition à partir du cloud et se trouvent en dehors du réseau de datacenter), la plupart des solutions exigent que vous déplaciez votre annuaire d'utilisateurs vers le cloud, ce qui vous oblige à abandonner et à remplacer votre infrastructure d'identité existante. Citrix Secure Private Access vous donne le choix, en vous permettant d'apporter votre propre identité à

Citrix Workspace. Notre écosystème riche de plateformes d'identité prises en charge comprend notamment Microsoft, Google et Okta. Ceci est réalisé par la fédération d'identité, en utilisant les services internes de SAML ou ADFS pour fournir au service cloud un token fiable et sécurisé contenant une série de requêtes à propos de l'utilisateur authentifié, y compris son identité. Ces requêtes sont à leur tour validées par les propres services de fédération des services cloud.

En vous offrant ce choix, Citrix vous permet de transformer vos investissements existants en solutions d'identités, tout en offrant un accès privé sécurisé à vos ressources d'entreprise.

4 Sécurité au-delà des noms d'utilisateur et des mots de passe

L'authentification des utilisateurs devient de plus en plus importante, notamment à mesure que les entreprises mettent en œuvre des plans de continuité d'activité et qu'une grande partie de leur personnel accède à distance aux ressources de l'entreprise. Ces collaborateurs, ainsi que les partenaires ou les sous-traitants qui ne figurent pas dans l'annuaire de l'entreprise, travaillent hors du réseau d'entreprise et sur des appareils personnels. Il est donc indispensable d'identifier rapidement et correctement les utilisateurs et de les autoriser à accéder aux ressources de l'entreprise.

C'est pourquoi Citrix Secure Private Access ne s'appuie pas uniquement sur les noms d'utilisateurs et les mots de passe. Il a recours à une authentification multifacteur qui permet aux équipes IT d'avoir un contrôle granulaire sur les personnes qui accèdent au réseau d'entreprise, les éléments qui sont consultés, le moment où ils sont consultés et l'appareil utilisé pour y

accéder. en charge tous les mécanismes et protocoles d'authentification tels que RADIUS, TACACS, NTLM, Diameter, SAML 2.0, OAuth 2.0 et OpenID 2.0. Il prend également en charge Azure Active Directory pour l'authentification multifacteur et les connexions sans mot de passe, et Active Directory sur site pour l'authentification à deux facteurs utilisant l'OTP natif.

Citrix Secure Private Access offre la possibilité de scanner les appareils des utilisateurs finaux avant et après l'établissement d'une session utilisateur. En fonction des résultats relatifs au rôle et à l'emplacement de l'utilisateur, ainsi que de l'évaluation de la posture de sécurité de l'appareil, un administrateur peut déterminer s'il souhaite authentifier et autoriser l'accès à ses applications.



Intégration fluide avec votre environnement existant

Une solution SSO (authentification unique) dispose de nombreux points de contact dans votre environnement, que ce soit au niveau de l'annuaire des utilisateurs, des mécanismes d'authentification, des applications et même

des appareils des utilisateurs finaux. Citrix Secure Private Access intègre facilement votre infrastructure existante pour que vous puissiez garantir une expérience utilisateur exceptionnelle, tout en simplifiant la gestion informatique.

Personnalisez votre portail d'applications front-end avec le branding de votre entreprise

Prise en charge de tous les mécanismes d'authentification, notamment RADIUS, Diameter, Kerberos, Microsoft NTLM, TACACS et via formulaire

Prise en charge de tous les appareils utilisateurs sur les plateformes Windows, Mac, Linux, iOS et Android

Prise en charge de tous les protocoles SSO, y compris SAML, OAuth et OpenID

La facilité d'intégration aux systèmes existants était le facteur le plus important dans le choix d'une solution d'authentification d'entreprise.²

6 Résolution plus rapide des problèmes avec une visibilité de bout en bout

Citrix Secure Private Access vous donnant accès à l'ensemble de votre paysage applicatif, il vous apporte également la visibilité dont vous avez besoin pour surveiller et dépanner les problèmes de mise à disposition d'applications et d'expérience utilisateur.

Citrix Analytics, composant clé de Citrix Workspace, vous offre une visibilité de bout en bout complète pour toutes les sessions utilisateurs TCP et HTTP. Insight enregistre les erreurs d'authentification, qu'elles soient dues à un mot de passe expiré, un compte verrouillé ou un échec de vérification du point de terminaison, ainsi que tout échec de lancement d'une application ou du système d'authentification unique, afin que vous puissiez résoudre les problèmes plus rapidement.

Citrix Analytics fournit également une authentification et une autorisation continues, l'un des principaux objectifs de confiance zéro pour de nombreuses entreprises. La détection de facteurs contextuels tels que le changement de lieu ou d'appareil peut déclencher des contrôles de sécurité supplémentaires (par exemple, un second facteur d'authentification) avant d'accorder l'accès

à une ressource de l'entreprise. Grâce aux critères et indicateurs de risque qui vous aident à détecter les anomalies utilisateur, vous pouvez configurer les contrôles de stratégie afin d'identifier et d'être alerté rapidement en cas de comportements utilisateur inadaptés ou risqués, par exemple en cas d'accès ou de téléchargement/chargement d'informations depuis/vers des sites Web malveillants ou à risque. L'automatisation avec Citrix Analytics peut réagir à votre place, en effectuant des actions telles que l'enregistrement des sessions, l'expiration des liens de documents partagés ou le verrouillage du compte de l'utilisateur.

Donnez à vos collaborateurs la liberté de travailler à leur manière. Avec Citrix Workspace, vous pouvez fournir une véritable authentification unique pour toutes les applications, en remplaçant les solutions d'accès SSO et VPN traditionnels. Simplifier le management IT, renforcer la sécurité et améliorer l'expérience des utilisateurs.

Pour en savoir plus, consultez citrix.fr/workspace.



Sources :

1. 12 statistiques incontournables sur l'utilisation du cloud dans l'entreprise, Skyhigh Networks.
2. Version 2017 du rapport d'authentification, Javelin.

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

© 2021 Citrix Systems France. Tous droits réservés. Citrix, le logo Citrix et les autres marques citées dans le présent document appartiennent à Citrix Systems, Inc. et/ou à l'une ou plusieurs de ses filiales, et peuvent être déposés au USPTO (U.S. Patent and Trademark Office) aux États-Unis et dans d'autres pays. Toutes les autres marques appartiennent à leur(s) propriétaire(s) respectif(s).