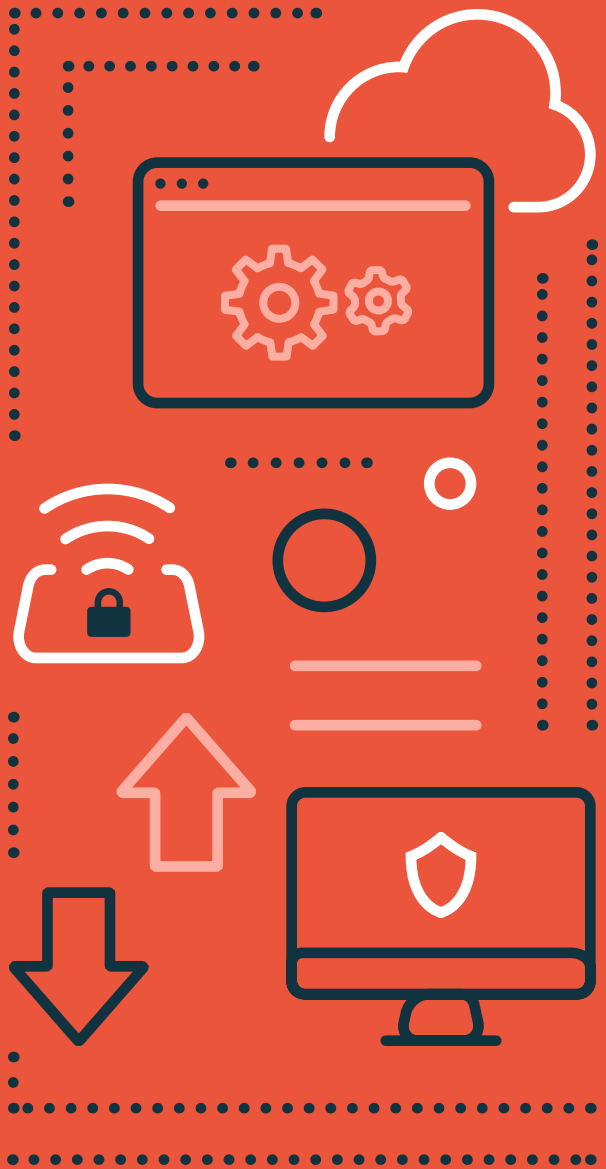


jamf

Accès réseau Zero Trust

Introduction

VOUS N'AVEZ AUCUNE IDÉE DE CE QU'EST L'ACCÈS RÉSEAU ZERO TRUST ? PAS DE SOUCI.

D'après **Gartner**, l'accès réseau Zero Trust (ou ZTNA, pour Zero Trust Network Access) est un **produit ou service qui crée une frontière d'accès logique, basée sur l'identité et le contexte, autour d'une application ou d'un ensemble d'applications**.

En termes simples, l'accès réseau Zero Trust est le successeur du réseau privé virtuel, ou VPN. Cependant, à l'inverse du VPN, qui date de 1996 et est basé sur le protocole PPTP (Peer-to-Peer Tunneling Protocol), **le ZTNA de Jamf Connect** est une solution moderne, conçue en incorporant un modèle de sécurité centré sur l'identité avec une gestion des règles en fonction du risque et des microtunnels spécifiques aux applications. Ces fonctionnalités limitent l'accès aux seules ressources que les utilisateurs sont autorisés à utiliser. Et tout cela est intégré dans une infrastructure Cloud qui simplifie la gestion, évolue d'un simple clic et ne nécessite pas de matériel propre.

DÉCOUVREZ DANS CET E-BOOK :

- Comment fonctionne Jamf
- Quelles fonctionnalités de sécurité sont intégrées
- Pourquoi vous devez reconsidérer votre approche de sécurité et votre authentification réseau

Et par où commencer.

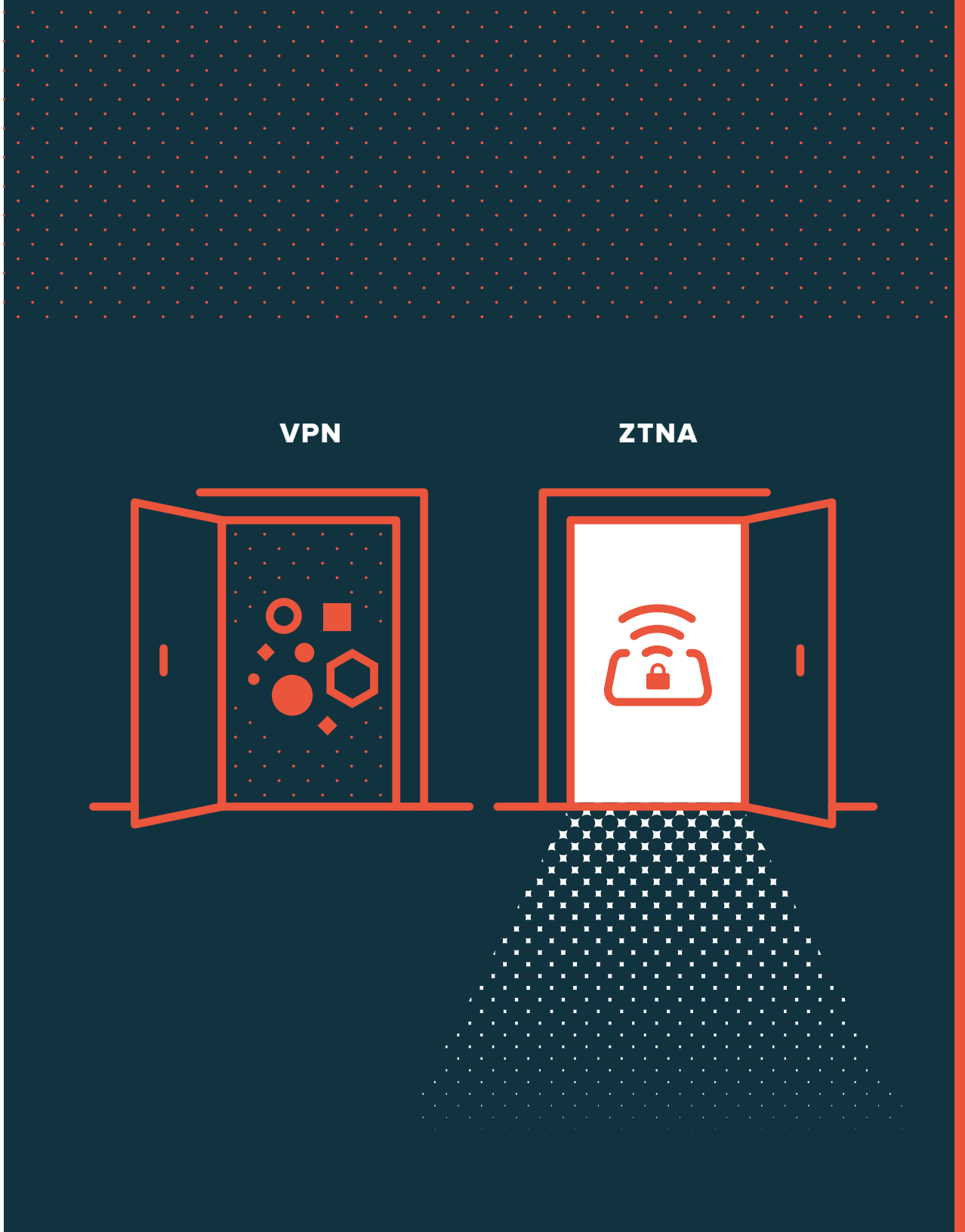
« PERSONNE NE FAIT CONFIANCE À PERSONNE. »

Dans le film « The Thing » de R.J. MacReady, le personnage de Kurt Russell perd progressivement toute confiance en ses compagnons à mesure que les problèmes s'accumulent. L'accès réseau Zero Trust partage cette vision des choses : cette technologie utilise des configurations de sécurité basées sur le principe du moindre privilège et centrées sur le principe « ne jamais faire confiance, toujours vérifier ».

Grâce à l'application du moindre privilège, associé aux contrôles de l'état des appareils en temps réel, **l'accès Cloud n'est accordé à chaque application que pour l'utilisateur autorisé demandant l'accès via ses identifiants uniques**.

Lorsqu'un utilisateur s'authentifie sur son appareil avec ses identifiants Cloud, les connexions professionnelles sont sécurisées et les applications non professionnelles sont acheminées directement vers Internet. Ce processus, appelé tunnelage partagé, permet de préserver la vie privée des utilisateurs finaux et d'optimiser l'infrastructure réseau. Cela permet d'optimiser encore davantage le réseau sous-jacent, en établissant la connexion ou le microtunnel de manière plus efficace. Grâce aux microtunnels, il est possible de sécuriser de bout en bout les utilisateurs, les appareils et les applications. Si l'un des éléments, par exemple un appareil personnel, n'est pas configuré pour avoir accès aux ressources de l'entreprise, l'accès sera interdit, même si des identifiants corrects ont été saisis.

Contrairement au VPN, qui accorde un accès global à l'ensemble du réseau de ressources pour les utilisateurs, l'approche granulaire de l'accès réseau Zero Trust renforce la sécurité en permettant aux utilisateurs d'accéder uniquement à ce dont ils ont besoin, au moment où ils en ont besoin. Ainsi, la sécurité de votre organisation est améliorée grâce à des règles personnalisées pour répondre aux exigences de conformité, et vous pouvez mieux protéger les utilisateurs finaux, les appareils de l'entreprise et les données.



« VOS RÈGLES COMMENCENT VRAIMENT À M'ÉNERVER »

Comme dans le film « New York 1997 », où l'infâme Snake Plissken prononce cette phrase alors qu'il est tiraillé entre les libertés offertes aux citoyens et les restrictions légales visant à maintenir la paix et la sécurité, les administrateurs informatiques peuvent se trouver confrontés à un dilemme :

Comment les organisations peuvent-elles assurer la sécurité tout en garantissant l'accès des utilisateurs finaux aux ressources et données nécessaires ?

Jamf est là pour ça.

Avec des règles centrées sur l'identité et les applications, qui permettent de gagner en productivité tout en éliminant la possibilité pour les utilisateurs de voir ou de trouver des données et des applications auxquelles ils ne devraient pas avoir accès, Jamf garantit que les règles d'accès unifiées s'appliquent de manière cohérente à tous les centres de données, infrastructures Cloud et applications SaaS, ainsi qu'à tous les systèmes d'exploitation modernes et paradigmes de gestion.

Les différentes règles en fonction du risque permettent d'améliorer la sécurité en empêchant l'accès aux ressources, en effectuant des contrôles réguliers sur les appareils afin d'évaluer leur état de santé, et en travaillant de manière proactive pour identifier les appareils qui sont susceptibles d'être compromis ou dont l'accès aux ressources semble risqué. La posture de sécurité globale du réseau est ainsi améliorée.

Relax,
tout est sous contrôle

Basée sur le Cloud, l'infrastructure utilisée par Jamf ne nécessite aucun matériel à entretenir, aucun contrat de prise en charge à gérer, ni aucun logiciel complexe à installer ou à configurer.

La nature centralisée, hautement évolutive et instantanément disponible du Cloud implique que les données sont protégées à la seconde même où vos appareils sont enrôlés dans le service, et ce quel que soit le nombre d'appareils de votre parc informatique ou l'endroit du monde où ils sont situés. Il suffit d'une connexion réseau.

Les fonctionnalités Cloud et les possibilités d'intégrations avec d'autres outils assurent une protection constante de vos terminaux. Les connexions sont chiffrées, l'état des appareils est surveillé et des workflows automatisés sont déployés pour remédier aux problèmes détectés, afin d'assurer le fonctionnement optimal des appareils et la sécurité des utilisateurs et des données.

COMMENT FONCTIONNE JAMF

Il ne travaille pas plus, mais mieux.

Un exemple d'intégration essentielle à l'architecture ZTNA est la capacité de permettre aux utilisateurs de s'authentifier par authentification unique (SSO) via votre **fournisseur d'identité Cloud habituel.** Cette fonctionnalité élimine les problèmes de gestion des certificats pour les utilisateurs ou les appareils, et élimine ainsi également la nécessité de maintenir votre propre autorité de certification (CA) dédiée, plus toutes les difficultés liées au réseau pour configurer la sécurité de ce type d'infrastructure dans des environnements de travail à distance ou hybrides.

Les administrateurs peuvent ainsi tirer parti de la connexion réseau de chaque appareil avec une connectivité Cloud pour travailler mieux, pas plus.

Moins de choses à faire, pour plus d'efficacité. Jamf est conçu non seulement pour protéger au mieux vos appareils, vos utilisateurs et vos données, mais aussi pour utiliser le moins de ressources possibles.

Jamf est nativement compatible avec Okta et Azure, et prend également en charge tous les grands fournisseurs d'identité, comme Google, Ping et d'autres encore, via la fédération avec Azure.

FONCTIONNALITÉS DE SÉCURITÉ

Modèle de sécurité centré sur l'identité

Seuls les utilisateurs autorisés peuvent se connecter aux applications d'entreprise, et la cohérence de l'application des règles est garantie dans les centres de données, le Cloud et les applications SaaS.

Microtunnels basés sur l'application

Ne connectez les utilisateurs qu'aux applications auxquelles ils sont autorisés à accéder : les microtunnels renforcent l'accès au moindre privilège et empêchent les déplacements latéraux du réseau (un vecteur courant de failles de sécurité).

Infrastructure moderne du Cloud

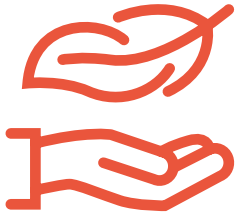
Aucun matériel à gérer, aucun contrat d'assistance à renouveler, ni aucun logiciel complexe à configurer ! Il n'est même plus nécessaire d'avoir le contrôle administratif d'un appareil pour permettre un accès sécurisé.

Intégration à vos fournisseurs d'identité

Permettez l'authentification des utilisateurs grâce à l'authentification unique (SSO) et éliminez la nécessité de gérer les certificats.

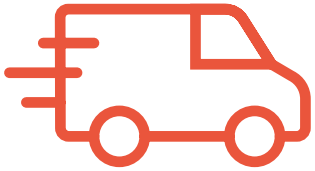
Règles d'accès en fonction du risque

Renforcez la sécurité en empêchant l'accès aux utilisateurs et appareils susceptibles d'être compromis.



Application légère

Établissez automatiquement des tunnels lorsque les applications doivent se connecter et se reconnecter de manière fluide en cas d'interruption.



Connectivité rapide et efficace

Accès sans restriction aux applications professionnelles (sans impact sur l'autonomie de la batterie) et fonctionnement silencieux en arrière-plan sans nuire à l'expérience utilisateur.

Tunnelage partagé intelligent

Assurez-vous de la sécurité des connexions professionnelles tout en permettant aux applications non professionnelles d'être acheminées directement vers Internet. Vous préservez ainsi la vie privée de l'utilisateur final tout en optimisant l'infrastructure du réseau.

Règle d'accès unifiée

Elle s'applique à tous les lieux d'hébergement (sur site, Cloud privés et publics, et applications SaaS), à tous les systèmes d'exploitation modernes et à tous les paradigmes de gestion.

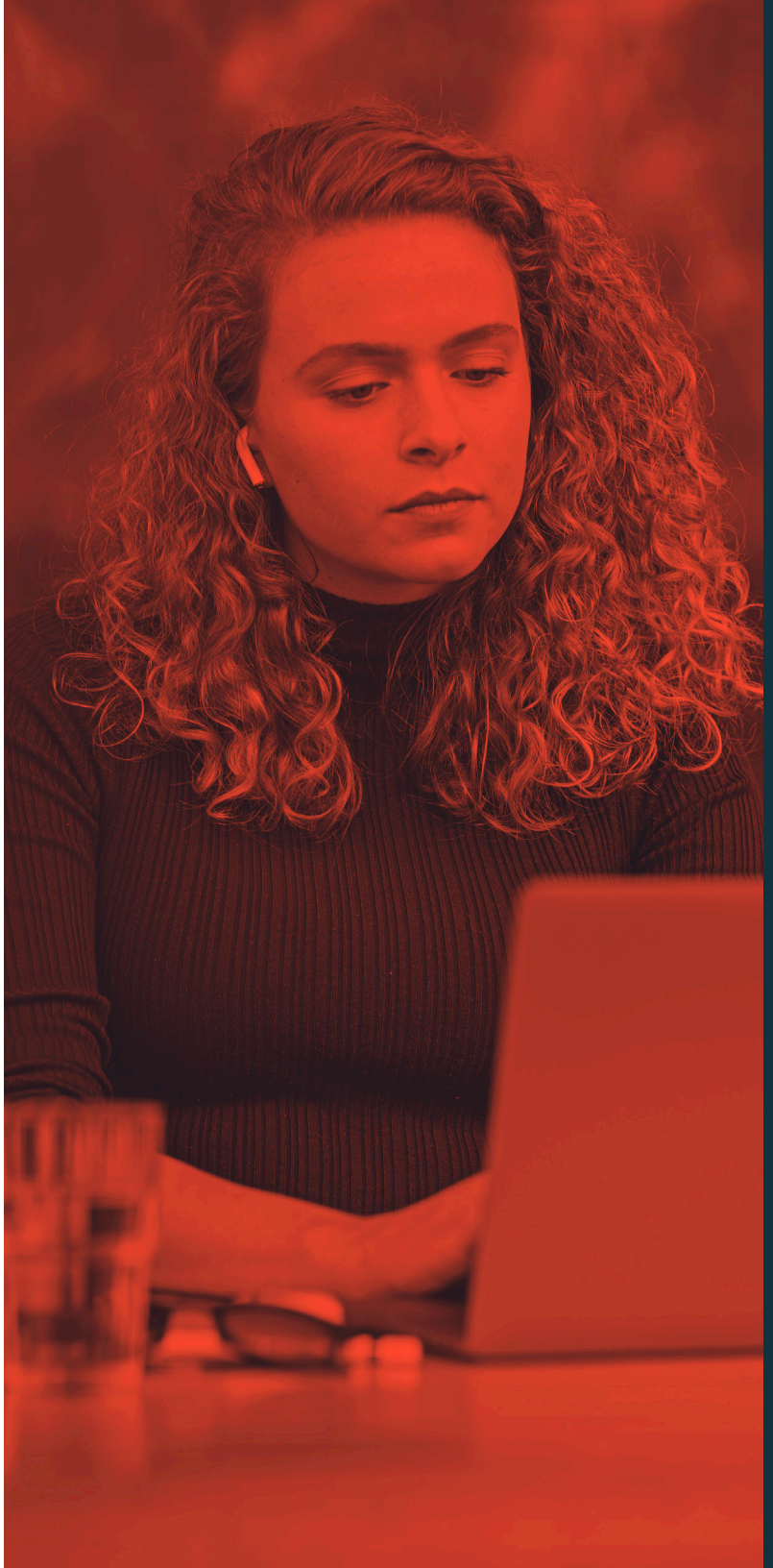
POURQUOI PASSER DU VPN À L'ACCÈS RÉSEAU ZERO TRUST

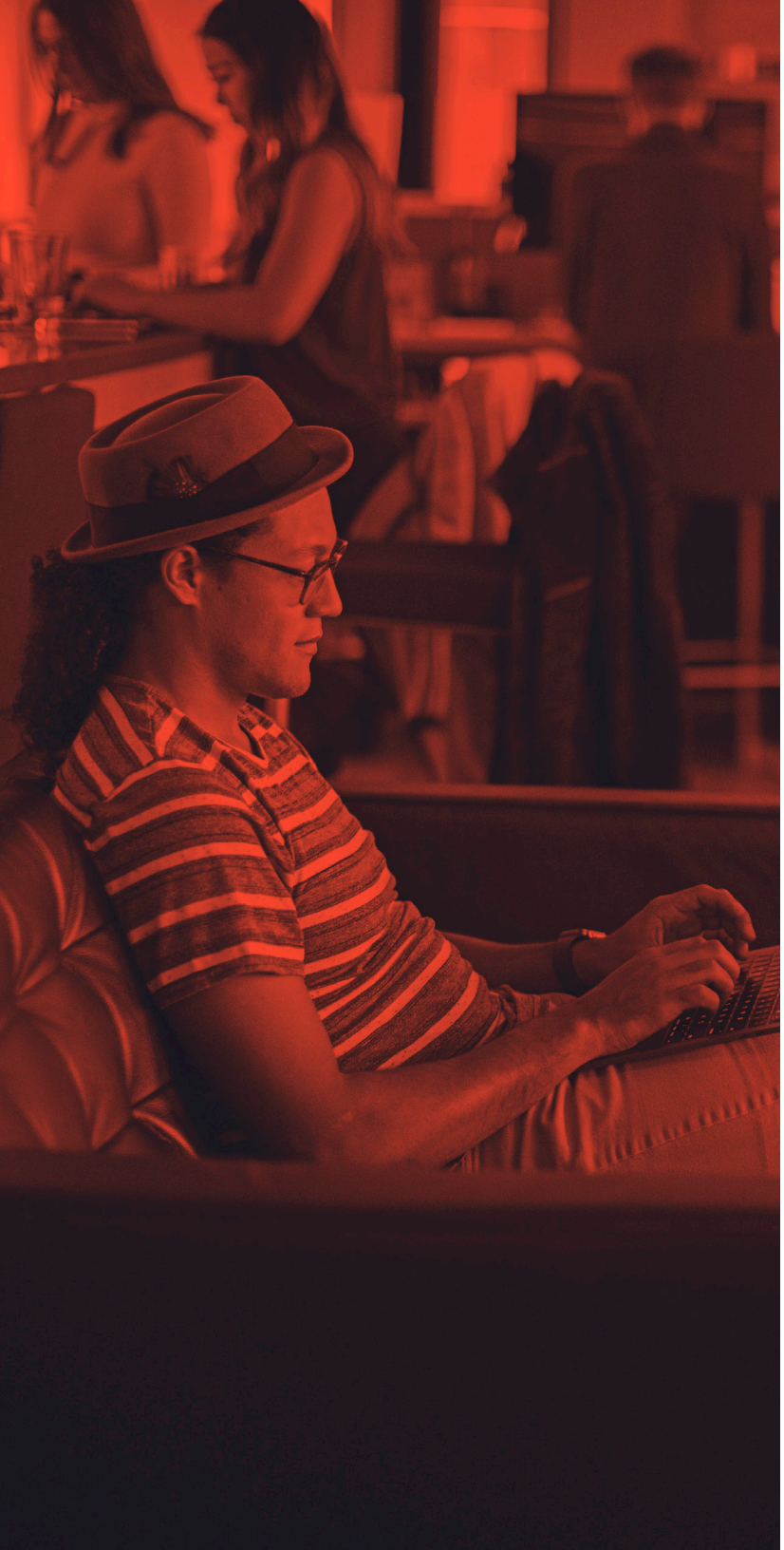
Même lorsqu'un VPN peut répondre à tous vos risques de sécurité, il reste un risque majeur : que l'utilisateur ne se connecte pas au VPN. Certains utilisateurs peuvent être réticents ou ne pas savoir comment se connecter au VPN. Dans ce cas, certaines organisations choisissent de ne pas placer leurs données à l'intérieur des frontières sécurisées du réseau, afin que les utilisateurs puissent tout de même y accéder. Ce faisant, elles mettent en danger leurs données.

Avec l'accès réseau Zero Trust, les utilisateurs n'ont pas à se soucier de savoir quand ou comment accéder aux sites sécurisés. Ils se connectent à leur appareil et, au moment opportun, ils peuvent accéder aux données sécurisées. En arrière-plan, l'accès réseau Zero Trust vérifie que l'utilisateur est authentifié et dispose des autorisations nécessaires, et que l'appareil est fiable. La fonctionnalité ZTNA permet aux organisations de sécuriser correctement leurs données tout en assurant un accès facile aux utilisateurs finaux.

L'époque où il fallait prendre des risques pour s'adapter aux utilisateurs qui avaient une nouvelle fois perdu leurs instructions VPN est révolue !

Quel que soit l'appareil ou le système d'exploitation de vos utilisateurs, l'accès réseau Zero Trust permet de créer automatiquement des microtunnels lorsque les applications doivent se connecter ou se reconnecter de manière fluide en cas d'interruption. Jamf ne réquisitionne aucune ressource matériel et ne sollicite pas la batterie lorsqu'il n'est pas utilisé.





Comme une sentinelle à son poste, il attend qu'une application, un utilisateur, une requête ou un service demande l'accès à des données protégées pour passer à l'action, préservant ainsi les ressources et assurant une expérience utilisateur fluide. Il empêche également les utilisateurs de voir ou de trouver des données ou des applications auxquelles ils ne devraient pas avoir accès. Enfin, il offre un périmètre défini par logiciel (SDP) basé sur le cloud afin de sécuriser les données en transit sur des connexions isolées pour chaque application.

Et lorsque Jamf est utilisé avec le Relais privé d'Apple (un nouveau service iCloud qui protège la confidentialité d'un individu en masquant son adresse IP et son emplacement sur les sites Web consultés), un accès sécurisé aux applications professionnelles est possible, sans les problèmes de performances, de confidentialité et de sécurité posés par les anciennes connexions VPN des entreprises.

L'utilisation conjointe de ces deux logiciels protège les utilisateurs lors de leurs navigations personnelles et professionnelles. Jamf peut être déployé sur des appareils personnels pour protéger et router le trafic professionnel. La navigation personnelle reste privée en étant acheminée via le Relais privé iCloud. L'approche combinant Jamf et le Relais privé iCloud+ est parfaite pour assurer la confidentialité et la sécurité sans compromettre les performances ni l'expérience de l'utilisateur final.

ET MAINTENANT ?

Commencez par sécuriser les appareils, les utilisateurs et les données dans votre environnement de travail à distance ou hybride à l'aide d'une approche de sécurité moderne : Jamf applique un accès au moindre privilège, basé sur le framework d'accès réseau Zero Trust et de sécurité centré sur l'identité.

Vérifiez l'état de vos appareils et automatisez les workflows de correction en fonction de règles basées sur les risques pour améliorer la posture de sécurité de votre parc réseau, tout cela à partir d'une console centralisée basée sur le Cloud, et sans nuire à l'expérience utilisateur intuitive.

Découvrez l'étendue des possibilités grâce à un essai gratuit, ou contactez votre revendeur Apple habituel pour vous lancer.

Demandez une version d'essai