

Les enjeux des réseaux privés virtuels

Les réseaux privés virtuels (VPN, Virtual Private Network) permettent aux utilisateurs d'accéder à l'intranet d'une entreprise depuis l'extérieur en toute sécurité. Les VPN utilisent des connexions chiffrées pour accéder à des ressources internes sensibles via Internet. Ils visent à renforcer la connectivité et la protection de l'entreprise, mais les équipes IT et sécurité font désormais face à de nouveaux défis pour les sécuriser.

Les problèmes de cybersécurité actuels

Pour connecter leurs télétravailleurs, les entreprises utilisent depuis longtemps des réseaux privés virtuels afin de garantir connectivité et sécurité. Mais tout cela est en train de changer. Malgré les avantages du cloud en termes de collaboration et de facilité d'emploi, les organisations rencontrent de plus en plus de problèmes de sécurité. En transposant leur VPN dans le cloud, les entreprises exposent leurs données sensibles à un risque d'accès non autorisé.

Les informations d'identification en ligne de mire

Le vol d'identifiants par phishing est l'une des attaques les plus courantes. Le pirate incite un utilisateur à lui révéler sa combinaison nom d'utilisateur/mot de passe en se faisant passer pour un individu ou une organisation digne de confiance par le biais d'un e-mail, d'une messagerie instantanée ou de tout autre canal de communication. Fort des informations obtenues, il extrait les ressources visées ou il attaque d'autres personnes au sein de l'organisation. Les comptes professionnels sont souvent la cible de « spear phishing », une technique mêlant phishing et social engineering. Dans ce genre d'attaque, les criminels tentent de soutirer des informations confidentielles à leurs victimes en jouant sur les aspects émotionnels de la prise de décision.

L'authentification multifacteur (MFA) pour sécuriser les VPN

L'authentification multifacteur (MFA, Multi-Factor Authentication) ajoute au mode d'authentification principal (par exemple, un mot de passe) une couche de sécurité supplémentaire pour valider l'identité d'un utilisateur (par exemple, un jeton de sécurité). Elle repose généralement sur l'utilisation de facteurs d'au moins deux des catégories suivantes : connaissance (quelque chose que l'utilisateur connaît), possession (quelque chose que l'utilisateur possède) et biométrie (quelque chose qui constitue l'utilisateur).

L'objectif est de renforcer le niveau d'identification des utilisateurs souhaitant accéder à une ressource via un VPN. L'authentification MFA empêche les pirates d'accéder à votre compte même s'ils connaissent votre identifiant et votre mot de passe. Le principe des mécanismes multiniveaux est de décourager les cybercriminels en les obligeant à déjouer la protection de plusieurs couches d'authentification.

Mais toutes les solutions et approches MFA ne se valent pas. En général, les solutions MFA on-premise d'ancienne génération sont complexes à déployer, ne s'appliquent qu'à un nombre de cas d'usage limité et offrent une expérience utilisateur médiocre. Par conséquent, elles sont peu adoptées et coûtent cher aux équipes IT et sécurité.

Dans un contexte de sécurité en pleine mutation, Okta Adaptive MFA est une solution idéale, car elle peut s'intégrer avec les applications et ressources de l'entreprise tout en offrant une couche d'identification supplémentaire.

Sécuriser les VPN avec l'authentification multifacteur

okta

Okta Adaptive MFA pour les VPN

La solution Okta Adaptive MFA aide les entreprises à relever les défis de la cybersécurité et du VPN grâce à une couche de sécurité supplémentaire qui les préserve des failles de sécurité. Pour Okta, les trois bonnes pratiques suivantes sont les piliers d'une solution d'authentification multifacteur efficace.

1. Sécurité

Okta Adaptive MFA protège les identités et les accès aux données, où que l'utilisateur se trouve et tous environnements confondus. Un avantage non négligeable pour les entreprises qui utilisent des VPN et étendent leurs activités dans le cloud. De nos jours, les données ne sont plus seulement hébergées sur site : elles circulent et peuvent être stockées sur les terminaux mobiles et dans le cloud.

Okta Adaptive MFA vous aide à sécuriser votre VPN à l'aide de facteurs tels que les mots de passe à usage unique et les jetons de sécurité physiques. Chaque situation d'authentification nécessite une approche spécifique. Par exemple, le SMS ne constituera pas un second facteur idéal dans les zones où le signal mobile est faible. Dans ce cas, il faut envisager une solution MFA offrant un large choix de facteurs et de niveaux de sécurité, comme Okta Adaptive MFA.

Okta Adaptive MFA est compatible avec les principaux fournisseurs de VPN :



Okta Adaptive MFA aide les entreprises à renforcer la sécurité des applications stratégiques grâce à une authentification forte basée sur le contexte et sur l'emplacement de l'utilisateur ou du terminal. Pour les administrateurs IT et sécurité, cette solution permet d'appliquer une stratégie unifiée et d'obtenir une vue centralisée des données on-premise, cloud et mobiles, gage d'une visibilité et d'un contrôle accrus.

Sécuriser les VPN avec l'authentification multifacteur



2. Simplicité

Okta Adaptive MFA est aussi simple à utiliser qu'à administrer. Okta s'intègre à des milliers d'applications via des protocoles standard, reposant sur des normes établies, et peut appliquer l'authentification multifacteur à l'ensemble de ces applications de manière centralisée. Il est essentiel de choisir une solution MFA qui s'intègre aux applications et services que vous utilisez et qui soit suffisamment flexible pour prendre en charge les scénarios personnalisés.

Okta Adaptive MFA est facile à déployer et offre aux administrateurs un niveau de flexibilité, de visibilité et de contrôle accru. Si vous recherchez une solution MFA pour sécuriser votre VPN, il est important de choisir un produit convivial, capable de s'intégrer de manière simple et fluide avec vos solutions.

Okta Adaptive MFA permet de valider facilement l'identité des utilisateurs finaux lorsqu'ils accèdent au VPN et aux données. En dotant ces utilisateurs d'un moyen d'authentification simple et flexible (aligné sur les flux de connexion existants, par exemple), tout en exigeant des facteurs supplémentaires dans les scénarios à haut risque (hors du réseau de l'entreprise, par exemple), leur expérience s'en trouve améliorée. En effet, une solution MFA complexe et difficile à utiliser nuira à l'adoption de la technologie et aux objectifs de sécurité.

3. Évolutivité

Une solution MFA performante est capable de monter en charge et de s'adapter à l'ensemble de l'entreprise. Okta Adaptive MFA joue un rôle clé dans l'obtention d'une visibilité complète sur les zones à risque, depuis les réseaux on-premise jusqu'aux terminaux mobiles ou au cloud, etc. Ce niveau de visibilité permet, en cas d'incident, de réagir plus rapidement.

Comme nous l'avons mentionné précédemment, les approches fragmentées et les solutions disparates constituent un problème important pour les entreprises. Okta Adaptive MFA s'intègre facilement à vos outils de sécurité et fournit une authentification forte pour la quasi-totalité des applications.

Globalement, Okta Adaptive MFA offre un niveau de visibilité, de contrôle et de réaction accru à l'échelle de toute l'entreprise. Face à la multitude de plateformes et de modèles d'organisation, il est crucial que votre solution MFA puisse évoluer et s'adapter au rythme de vos besoins de sécurité.

Sécuriser les VPN avec l'authentification multifacteur



Conclusion

Les entreprises réalisent qu'elles ont besoin de solutions d'authentification multifacteur pour vérifier l'identité des utilisateurs qui se connectent à distance via un VPN. Mais toutes les solutions MFA ne se valent pas. Pour être performante, une solution MFA doit inclure une authentification forte, tenant compte du contexte. Son implémentation doit être rapide et non intrusive, et elle doit être simple d'utilisation tant pour les utilisateurs finaux que pour les administrateurs. De plus, elle doit pouvoir s'étendre à l'ensemble de l'entreprise et du dispositif de sécurité. Enfin, il convient de privilégier les éditeurs qui favorisent l'innovation et proposent des solutions capables d'évoluer au rythme de vos besoins de sécurité.

Okta Adaptive MFA remplit tous ces critères et offre la couche de sécurité supplémentaire dont vous avez besoin pour vous prémunir efficacement contre les brèches, tout en respectant les obligations réglementaires. Elle assure la sécurité de tous les groupes d'utilisateurs dans la quasi-totalité des cas d'usage et ce, que vos données soient dans le cloud ou on-premise. Avec un large choix de facteurs pour couvrir l'ensemble des scénarios d'identification, la solution Okta limite les risques de sécurité grâce à un contrôle accru des accès basé sur le contexte ou l'emplacement du terminal ou de l'utilisateur. Okta Adaptive MFA couvre toute l'entreprise grâce aux quelque 6 500 préintégrations d'Okta Integration Network et à la prise en charge des API pour les applications personnalisées. En connectant les applications métier entre elles et en assurant une intégration hors pair avec une multitude d'outils de sécurité, elle offre une visibilité de bout en bout et une protection renforcée.

Qui sommes-nous ?

Okta est un éditeur indépendant spécialisé dans la gestion et la protection des données d'identification, leader du secteur. La plateforme Okta Identity Cloud connecte et protège les collaborateurs des plus grandes entreprises au monde, en plus d'assurer une connexion sécurisée avec leurs partenaires, fournisseurs et clients. Grâce à son intégration avancée avec plus de 6 500 applications, Okta Identity Cloud permet à n'importe quel utilisateur de se connecter facilement et en toute sécurité, tous terminaux confondus.

Des milliers de clients, dont 20th Century Fox, Adobe, Dish Networks, Experian, Flex, LinkedIn et News Corp, font confiance à Okta pour améliorer leur productivité, doper leur chiffre d'affaires et préserver leur sécurité. Grâce à Okta, ils peuvent accéder facilement et sans risque aux technologies dont ils ont besoin pour accomplir leurs missions stratégiques.

Pour en savoir plus, rendez-vous sur www.okta.com/fr