paloalto NETWORKS | PRISMA® ACCESS

Sécuriser les accès distants en toute simplicité

Prisma® Access unifie la sécurité des accès distants tout en boostant les performances pour les collaborateurs.

Aujourd'hui, le travail hybride est devenu la norme. Les collaborateurs et les infrastructures qui sous-tendent les opérations des entreprises se retrouvent dispersés dans le monde entier.

Ces nouveaux modes de travail et infrastructures décentralisés offrent une plus grande flexibilité. Ils permettent aux équipes de rester productives, où qu'elles soient : au bureau, en télétravail, en déplacement, sur le terrain… Quant aux entreprises elles-mêmes, elles peuvent exploiter l'agilité, la scalabilité et la résilience du cloud à leur propre rythme.

Mais pour profiter de tous ces avantages, elles doivent mettre en place une connectivité au moins aussi flexible que ces modèles émergents. Autre impératif : sécuriser ces connexions pour protéger les collaborateurs, les données et toutes les ressources qui interagissent dans ces environnements hautement distribués.

Seulement voilà, la plupart des approches de connectivité traditionnelles, y compris les VPN, sont incapables de fournir les performances, la sécurité et la simplicité de gestion à la hauteur des nouveaux enjeux. Un nouveau modèle s'impose.

Source : Gallup, « The Future of the Office Has Arrived: It's Hybrid », octobre 2023

Certaines entreprises prônent le retour au présentiel. Toutefois, le travail hybride n'est pas près de disparaître.

En 2023

5 collaborateurs sur 10
travaillaient en mode hybride

3 collaborateurs sur 10
étaient à 100 % en télétravail

2 collaborateurs sur 10
travaillaient à 100 % en présentiel

Le VPN, une solution de sécurité d'un autre temps

Les réseaux privés virtuels (VPN) font partie des meubles dans les entreprises qui, depuis des décennies, s'en servent pour sécuriser les accès distants de leurs collaborateurs à leurs données et ressources.

Mais depuis l'invention du VPN au milieu des années 90, leurs exigences en matière de connectivité ont bien changé. À l'époque, toutes les activités ou presque se déroulaient entre les quatre murs de l'entreprise. Seule une poignée de salariés nécessitaient un accès distant. La productivité des équipes dépendait avant tout des applications et des données hébergées dans des data centers on-prem, sur chaque site. C'est sur la base de ce modèle obsolète que les principes de sécurité VPN ont été élaborés. Le problème, c'est que ces principes sont toujours appliqués aujourd'hui.

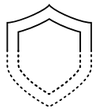
En précipitant le passage au télétravail, la pandémie a mis en lumière les nombreuses lacunes des VPN. Ces insuffisances ont fait peser une pression énorme sur les équipes IT et de sécurité chargées de déployer des accès sécurisés pour tous les collaborateurs, littéralement du jour au lendemain. Face au nouveau modèle que représente le travail hybride, les limites du VPN se révèlent une nouvelle fois source de stress pour ces équipes débordées.

Source : ESG, « Ten Considerations for Evaluating Zero Trust Network Access Solutions », septembre 2021

Les principales contraintes du VPN

Gestion complexe et manque de scalabilité

L'installation d'un nouveau VPN nécessite l'achat d'équipements et mobilise les équipes qui doivent gérer manuellement son déploiement, son utilisation et sa maintenance. Ainsi, lorsqu'une entreprise veut étendre la portée de son VPN, elle doit investir non seulement de l'argent pour acheter du matériel et recruter des talents, mais aussi du temps pour déployer et maintenir la solution.



Sécurité limitée

Les solutions VPN traditionnelles protègent les accès en périphérie du réseau. Une fois connectés à l'environnement, les utilisateurs peuvent accéder librement à toutes les applications et données qui y sont hébergées. Cette permissivité, associée à l'essor du télétravail et du travail hybride, explique la prolifération des attaques exploitant les vulnérabilités du VPN depuis la pandémie.

Expérience utilisateur médiocre

Les solutions VPN ne sont pas toujours aussi intuitives et simples d'utilisation qu'il y paraît. Les télétravailleurs ne maîtrisent pas tous les compétences techniques nécessaires pour résoudre leurs problèmes de connexion, ce qui engendre de la frustration. La façon dont les VPN acheminent et sécurisent le trafic crée également des ralentissements au niveau de la connectivité. Résultat, certains collaborateurs rechignent à utiliser le VPN, une aversion qui crée de grandes disparités dans les niveaux de sécurité au sein de l'entreprise.

Verdict

Les solutions VPN traditionnelles sont incapables de répondre aux exigences de connectivité du travail hybride. Pire encore, elles nuisent à la productivité des équipes, engendrent des risques et augmentent les coûts de gestion et de déploiement.

Source : TechTarget, « Hackers targeting VPN vulnerabilities in ongoing attacks », avril 2021

Le travail hybride complique la tâche des équipes de sécurité

59 % des personnes interrogées trouvent la cybersécurité et la gestion plus difficiles aujourd'hui

41 % estiment que l'essor du télétravail complique la cybersécurité

Source : ESG, « Ten Considerations for Evaluating Zero Trust Network Access Solutions », septembre 2021

Une approche plus sûre

La grogne que suscitent les VPN pousse les entreprises à envisager de nouvelles approches pour les connexions à distance, plus performantes et plus sûres, mais aussi plus simples à déployer et à gérer.

Parmi ces alternatives, le Zero Trust Network Access (ZTNA) fait figure de grand favori. Ces outils de pointe sécurisent la connexion des collaborateurs aux applications et données essentielles à leurs missions, quels que soient le lieu et l'appareil utilisés pour se connecter.

Le ZTNA permet aux entreprises de se départir des VPN et de leurs accès réseau trop permissifs. C'est même là l'un de ses principaux avantages. Comme son nom l'indique, le ZTNA applique les deux règles fondamentales du Zero Trust :

- **Principe du moindre privilège** – Les utilisateurs accèdent uniquement aux applications et données dont ils ont besoin, ni plus ni moins.
- **Ne jamais faire confiance, toujours vérifier** – L'identité et les droits d'accès de l'utilisateur sont vérifiés chaque fois que ce dernier veut accéder à une application, puis contrôlés en continu après cette validation initiale.

Grâce au ZTNA, les entreprises peuvent restreindre les accès en cas de compromission et éviter ainsi que la menace se propage à toute l'organisation.

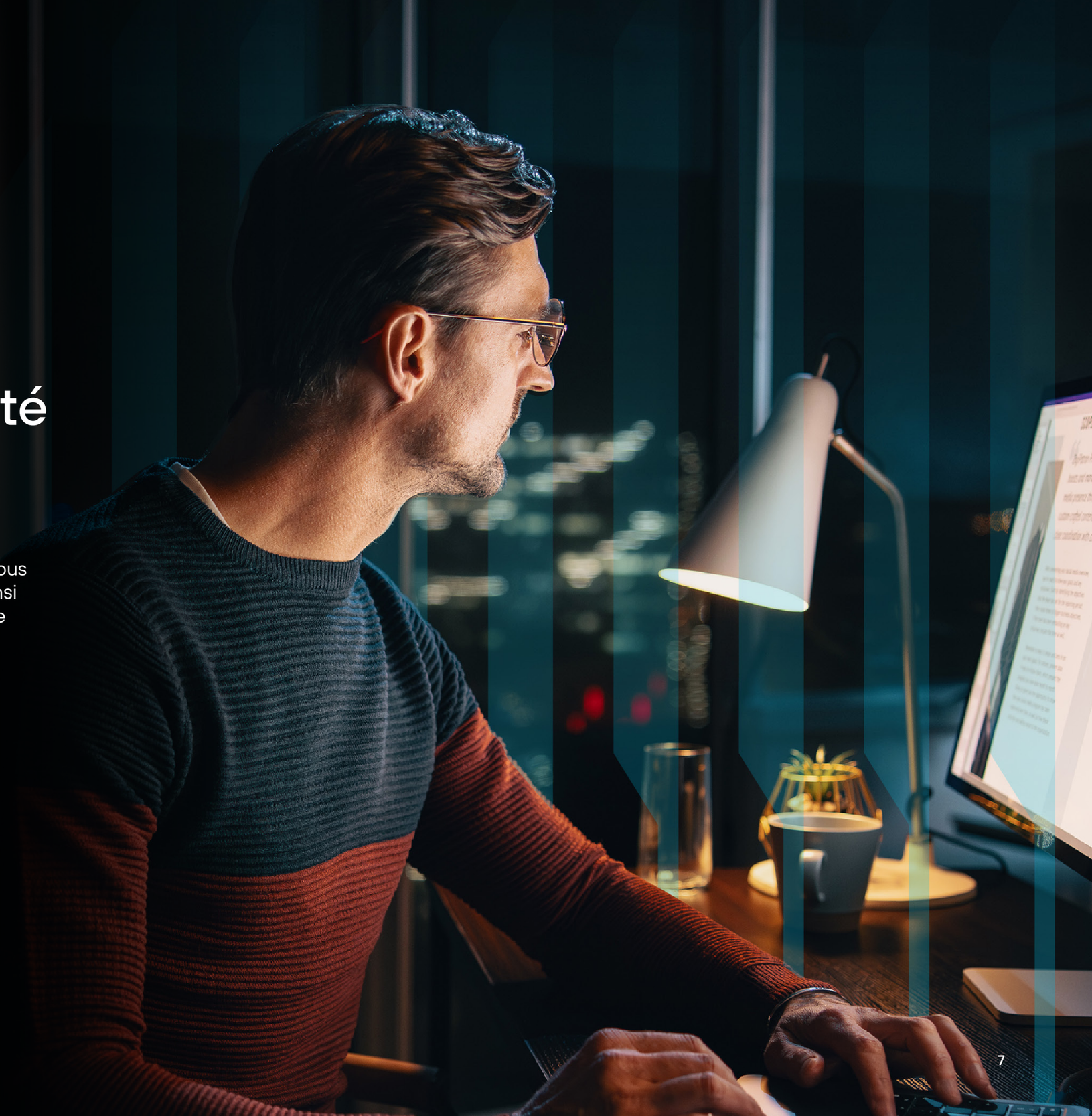
D'ici 2025, selon les prévisions Gartner,
70 % des nouveaux déploiements d'accès distants seront basés sur le ZTNA plutôt que sur des services VPN.

Source : Communiqué de presse Gartner, octobre 2022

Révolutionner la sécurité des accès distants

Prisma Access de Palo Alto Networks transforme vos accès distants pour pallier les lacunes des VPN. Cette solution cloud vous fournit une connectivité sécurisée et performante. Elle réduit ainsi votre exposition aux menaces tout en offrant aux utilisateurs une expérience applicative d'exception.

Prisma Access aide les équipes IT et de sécurité à protéger les utilisateurs, les applications et les données à l'échelle du cloud, facilitant et accélérant le déploiement de nouveaux accès pour tous vos collaborateurs.



Prisma Access : quand le travail hybride et le « full-remote » deviennent des leviers de compétitivité

- **Les accès sécurisés que vos collaborateurs hybrides exigent**
  Prisma Access fait rimer sécurité et productivité. Vos équipes bénéficient des mêmes performances pour les applications on-prem, cloud et SaaS, avec une connectivité « direct-to-app » sécurisée et une inspection continue du trafic.

- **Une protection granulaire qui réduit votre exposition au risque**
  Prisma Access exploite le Zero Trust pour individualiser la sécurité au niveau de chaque utilisateur et application. Elle réduit ainsi considérablement votre surface d'attaque.

- **Une gestion simplifiée des accès distants**
  Avec Prisma Access, la gestion manuelle des accès est de l'histoire ancienne. La solution Palo Alto Networks révolutionne la façon dont vous sécurisez et contrôlez les accès distants aux systèmes et données critiques en simplifiant et en unifiant la gestion et les opérations.

La différence **Prisma Access**

50 % de risque de compromission en moins

75 % d'efficacité en plus dans la gestion du SASE (Secure Access Service Edge) et la modification des politiques

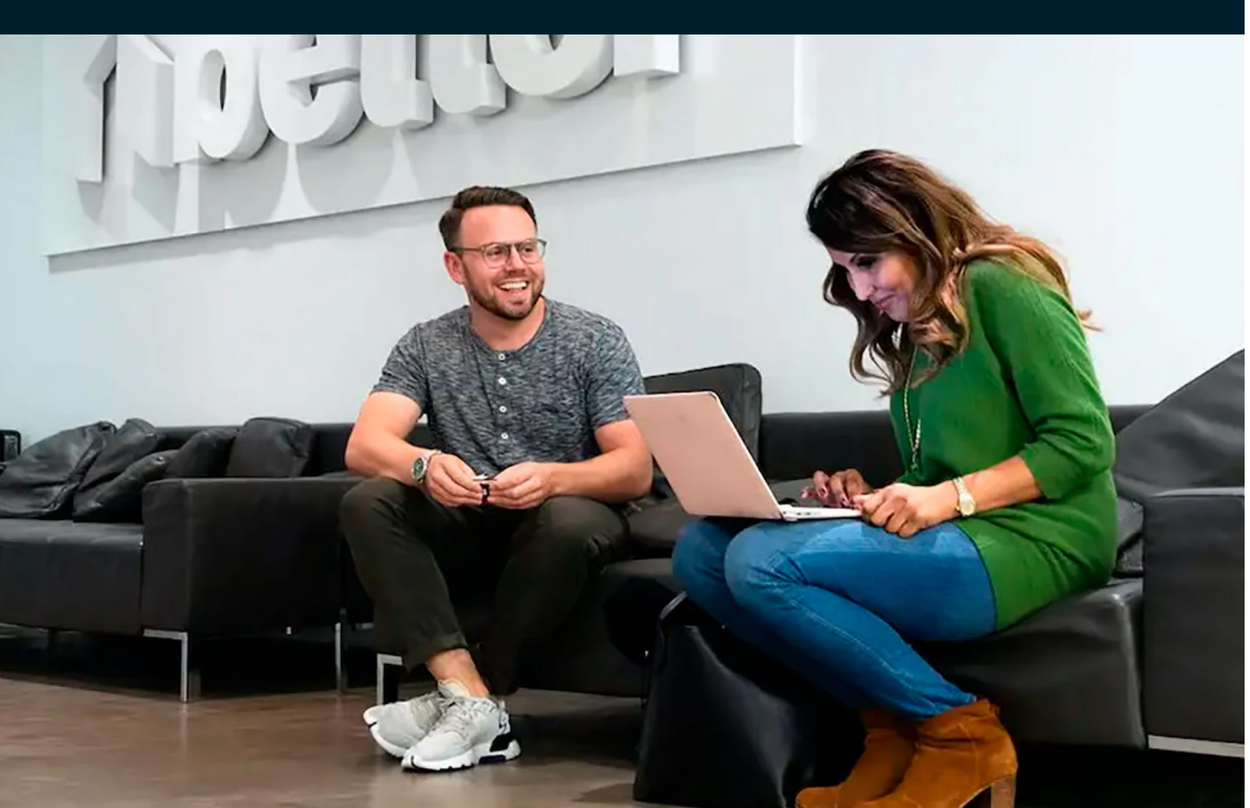
107 % de retour sur investissement (ROI)

Source : Forrester, « The Total Economic Impact™ Of Palo Alto Networks Prisma SASE », novembre 2023. Étude réalisée pour Palo Alto Networks.

SUCCESS STORIES

Better

Moderniser les accès distants rapidement et à grande échelle



Better a toujours fait de la sécurité une priorité. Pour préserver son image de marque de confiance et garantir le respect des règlementations, ce spécialiste du crédit immobilier sur Internet souhaitait moderniser son approche de la sécurité à tous les niveaux : réseau, terminaux et SecOps.

Sa stratégie impliquait également de sécuriser l'accès en ligne de ses clients et de ses collaborateurs. Bien que dotée d'un VPN, Better cherchait une solution cloud, par nature plus évolutive, plus simple à gérer et surtout plus facile d'accès pour les utilisateurs. Autre impératif : renforcer la sécurité des données.

Très intéressée par les fonctionnalités de Prisma Access, l'entreprise a lancé une preuve de concept (PoC) pour évaluer le potentiel de la solution Palo Alto Networks. À cette même période, la pandémie de Covid commençait à déferler sur toute la planète. Avec l'aide de Palo Alto Networks, Better a pu faire basculer ses effectifs en télétravail, en quelques jours et en toute sérénité.

Lisez l'étude de cas pour découvrir comment Better a modernisé son approche de la sécurité.

> « Prisma Access a permis à nos collaborateurs internes d'accéder à nos solutions logicielles à distance, en toute sécurité et partout dans le monde. C'était une véritable révolution. »
>
> **– Ali Khan**, Responsable de la sécurité des systèmes d'information, Better

SUCCESS STORIES

Beam SUNTORY

Améliorer la sécurité et la performance

Beam Suntory est le troisième plus grand producteur d'alcools distillés au monde. Il y a quelques années, un incident de sécurité majeur a incité l'entreprise à revoir sa copie en matière de cyberprotection.

Son réseau et son infrastructure de sécurité vieillissants causaient de nombreux problèmes : protection parcellaire, manque d'évolutivité, perte de connectivité et ralentissement de la productivité. Il était donc urgent de les remplacer.

L'entreprise considérait au départ sa transformation réseau et de sécurité comme deux projets distincts. Mais face aux réalités du terrain, elle a rapidement réalisé l'intérêt de fusionner ces deux aspects autour d'une architecture SASE.

Prisma SASE a permis à Beam Suntory de renforcer sa posture de sécurité, la fiabilité de son réseau ainsi que ses performances. Grâce à la simplification des opérations, l'équipe gère plus facilement les composants réseau et de sécurité.

Enfin, pendant la pandémie, Prisma SASE a grandement facilité le basculement des salariés en télétravail. Au lieu de passer par le data center, les utilisateurs ont pu accéder directement à leurs outils de productivité dans le cloud.

> « Prisma SASE nous a sauvé la mise tout en augmentant le niveau de performance et de sécurité. »
>
> – **Qun Wei**, Architecte réseau senior, Beam Suntory

Les trois prochaines étapes de votre migration

Avec Prisma Access, l'hybride et le distanciel deviennent des leviers de compétitivité. Offrez à vos collaborateurs des expériences d'exception, réduisez votre surface d'attaque et simplifiez la gestion des accès.

1

Découvrez comment Prisma Access sécurise les accès distants pour simplifier la vie de vos collaborateurs et de vos équipes IT.

2

Explorez les fonctionnalités ZTNA de Prisma Access.

3

Contactez-nous pour organiser une démo et transformer la sécurité des accès distants dans votre entreprise.

paloalto® NETWORKS | PRISMA® ACCESS