Prisma Access Browser : l'allié de la protection SASE

Plus les collaborateurs travaillent dans le navigateur, plus l'entreprise est exposée

Le monde du travail a radicalement changé. C'est un fait. Dans ce nouveau paradigme, on accède aux ressources d'entreprise dans le cloud par un nombre croissant d'applications SaaS et web, on discute avec les collègues par messagerie instantanée, on utilise l'IA pour écrire des e-mails… Le travail ne se cantonne plus aux ordinateurs portables au bureau, mais s'étend aux smartphones en déplacement.

D'ailleurs, les collaborateurs ont changé, eux aussi. Entre les recrutements, les partenaires tiers, les consultants et les sous-traitants, le mot « collègue » désigne désormais une réalité complètement différente. Les nouveaux espaces de travail n'ont plus de frontières.

Dans ce paysage en pleine mutation, la transformation de la sécurité devient inévitable, elle aussi. Jadis simples à implémenter et à appliquer dans un environnement sur site centralisé, les politiques et les contrôles s'étendent désormais à l'échelle du monde entier. De nouveaux collaborateurs se connectent avec une variété d'appareils depuis différents emplacements, mais nécessitent le même niveau de protection et d'attention que leurs collègues du siège. En somme, il leur faut une sécurité standardisée et facile à configurer, qui n'entrave pas leur productivité. Faute de quoi, ils chercheront à contourner ces contrôles, qu'ils soient en télétravail ou non.

Dans ce contexte, l'adoption de modèles de travail hybride étendus et d'assistance pilotée par IA devient un impératif absolu. Pour conserver une productivité élevée, les travailleurs hybrides passent par un large éventail d'applications SaaS et d'appareils. L'outil de prédilection a, lui aussi, changé. Tout le travail, ou presque, s'effectue désormais dans un navigateur.

D'après une récente enquête de Palo Alto Networks, les collaborateurs passent plus de 85 % de leur journée sur les navigateurs web[1]. Le navigateur joue un rôle central dans les activités quotidiennes. Revers de la médaille, c'est précisément pour cette raison qu'il représente une cible de choix. Pour preuve : près de 95 % des entreprises interrogées ont décelé des menaces basées sur le navigateur dans l'ensemble du parc IT[2]. Pourquoi un chiffre aussi élevé ? Parce que le navigateur web tend à constituer un angle mort des solutions et des équipes de sécurité.

Difficile, en effet, de suivre le rythme de l'évolution fulgurante des menaces, d'un côté, et des nouveaux modes de travail, de l'autre.

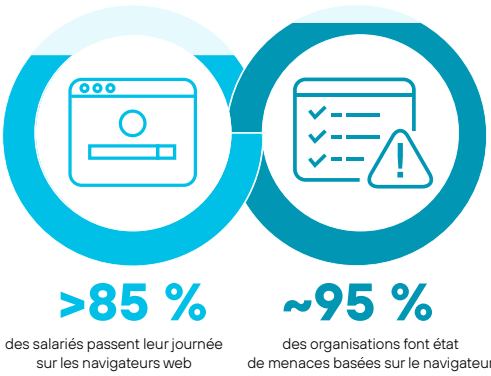

Figure 1. La grande majorité du temps de travail se passe dans un navigateur web exposé aux risques

Afin de lutter contre cette vulnérabilité croissante, Palo Alto Networks propose d'intégrer Prisma® Access Browser au socle du SASE. La solution libère tout le potentiel du SASE, pour une sécurité intégrale en quelques minutes sur l'ensemble des appareils. Premier et unique navigateur sécurisé intégré en natif dans le framework SASE, il protège les collaborateurs contre les menaces, tout en sécurisant l'accès aux applications web essentielles dans le respect des réglementations sur la confidentialité et les données. Avec en prime, une expérience utilisateur ultra fluide.

1. *Optimiser la sécurité des nouveaux environnements de travail,* Palo Alto Networks et Omdia, janvier 2025.
2. Ibid.

La nouvelle évolution des accès sécurisés

Les solutions de sécurité d'hier ont fait leur temps, mais ne suffisent plus à protéger les modes de travail d'aujourd'hui. Dépendance accrue aux appareils non gérés, infrastructures cloud, nouveaux protocoles réseau… Bref, les solutions traditionnelles sont dépassées. Elles n'assurent ni sur le plan de la sécurité ni de l'expérience utilisateur, laissant de fait les entreprises vulnérables aux menaces et en perte de productivité.

Plus précisément, les implémentations de sécurité d'ancienne génération n'offrent pas une couverture suffisante contre les menaces basées sur le navigateur. Résultat, les organisations se retrouvent à la merci des attaques passant par les applications et les extensions cloud-native. Or, le navigateur constitue désormais le premier espace de travail numérique. Cette évolution n'a, bien évidemment, pas échappé aux cyberattaquants, qui voient dans cet accès aux ressources d'entreprise sensibles un filon fort lucratif. Dès lors, une nouvelle approche s'impose : les principes du SASE doivent être directement intégrés dans l'environnement de navigation.

À l'heure où les collaborateurs travaillent de plus en plus sur les navigateurs web et les applications SaaS, il devient même urgent de combler les lacunes des anciens SASE. Pour une sécurité complète, les solutions SASE doivent s'étendre jusqu'au navigateur. Objectif : garantir un accès sécurisé basé sur des politiques, ainsi que des contrôles des données jusqu'au dernier kilomètre pour les applications SaaS et les appareils non gérés. Faute d'une visibilité à 360° et d'un contrôle total des interactions utilisateurs sur les applications web et cloud, les structures courent des risques accrus d'exposition des données et de problèmes de conformité. Avec la transition vers les environnements cloud et le travail hybride, l'extension du SASE à toutes les activités sur navigateur est la condition sine qua non d'une sécurité complète et d'une réduction des vulnérabilités liées aux actions des utilisateurs. Elle représente un puissant niveau de protection supplémentaire dans une stratégie de sécurité multidimensionnelle et multicouche, du réseau aux terminaux en passant par le navigateur.

Un nouveau SASE pour le travail hybride

Jamais le besoin d'une solution SASE complète n'a été aussi manifeste. Une solution globale, flexible et dispersée qui répond aux exigences d'aujourd'hui, et non pas d'hier, en plaçant l'environnement de travail au cœur de sa conception. Mais surtout, une solution capable d'assurer visibilité, sécurité et contrôle dans le principal outil de travail, le navigateur.

Palo Alto Networks fournit la seule solution SASE qui intègre un navigateur sécurisé en natif pour protéger le travail web-first sur les appareils gérés et non gérés. Pour la première fois, les utilisateurs disposent d'un accès Zero Trust continu, fluide et homogène aux applications SaaS et privées, depuis n'importe quel poste de travail. Les administrateurs contrôlent ainsi les points de rencontre entre utilisateurs et données. Désormais, les mêmes expériences et politiques de sécurité s'appliquent à tous les collaborateurs, où qu'ils soient.

La conception de la solution s'appuie sur le déploiement de politiques de sécurité granulaires, adaptées aux différents rôles et responsabilités de chaque collaborateur. Les collaborateurs n'ont accès qu'aux données et applications nécessaires à leur mission, les informations sensibles étant masquées et les applis ou sites web non essentiels bloqués. Cette politique du moindre privilège permet de renforcer la sécurité, sans affecter les performances des équipes.

Principales fonctionnalités de Prisma Access Browser

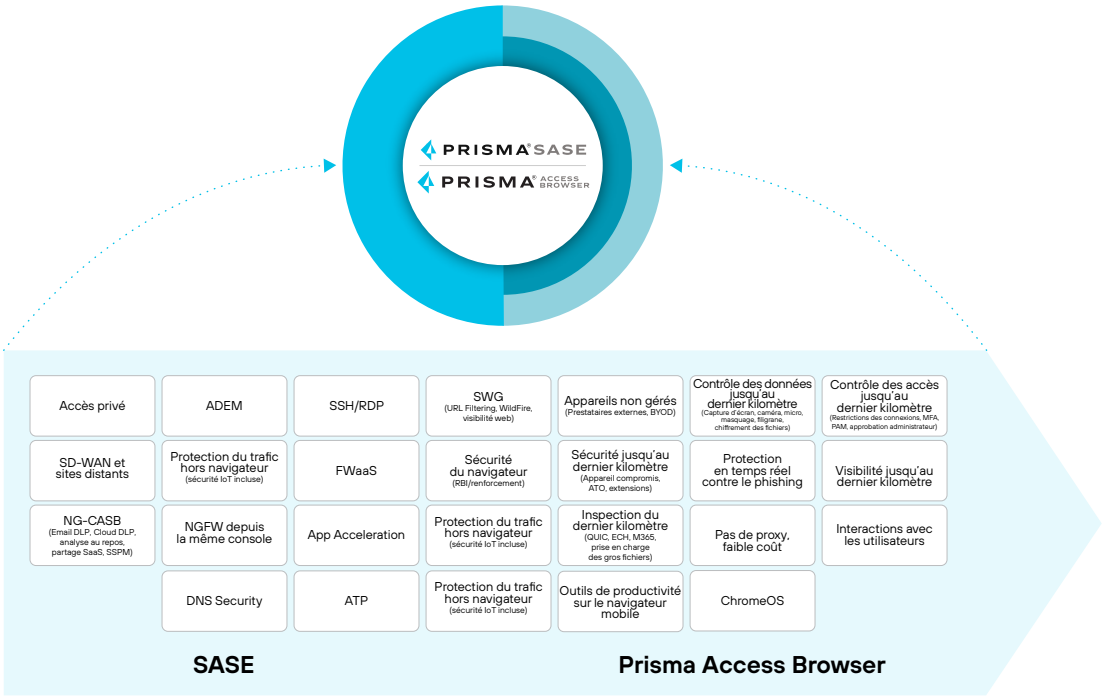

Figure 2. Prisma Access Browser étend le SASE et sécurise le navigateur pour une protection inégalée

Une sécurité multidirectionnelle sur tous les appareils

Protection contre les terminaux compromis

Prisma® Access Browser renforce la sécurité des appareils gérés et non gérés en créant un espace de travail sécurisé sur les équipements professionnels et personnels (ordinateurs portables, tablettes et smartphones inclus). Les collaborateurs travaillent ainsi en toute sécurité là où ils veulent, sans compromettre l'intégrité du réseau d'entreprise. Le navigateur isole les applications d'entreprise des menaces posées par les terminaux non approuvés, réduisant le risque de compromissions de données et d'infiltration de malware.

Les appareils gérés ne sont pas immunisés contre l'apparition de vulnérabilités : logiciels obsolètes, erreurs humaines ou attaques sophistiquées par phishing. Mais ce dernier type de menace demeure l'un des plus redoutables. Le phishing consiste à créer des e-mails ou des sites web assez convaincants pour duper les collaborateurs et les inciter à partager des informations sensibles ou à installer un malware. Les techniques étant de plus en plus sophistiquées, une protection complète s'avère absolument indispensable. Contre ces menaces, Prisma Access Browser intègre des fonctionnalités de sécurité avancées directement dans le navigateur. Avec le suivi web automatisé et la détection des menaces, il identifie et neutralise rapidement les tentatives de phishing, ainsi que bien d'autres menaces.

Protection contre les menaces

Prisma Access Browser offre une couche supplémentaire de chiffrement au niveau du navigateur pour protéger contre une multitude de dangers : enregistreurs de frappe, enregistreurs d'écran, certificats non fiables, réseaux publics non sécurisés… En désactivant les composants sensibles du navigateur et en les préservant des extensions malveillantes, il réduit non seulement la surface d'attaque, mais s'assure aussi que le travail des collaborateurs reste protégé à tout moment. En outre, les mesures proactives de Prisma Access Browser viennent compléter ce bouclier de sécurité. Au menu : vérification de la posture des appareils toutes les 90 secondes et collecte d'éclairages web pour le Threat Hunting et l'analyse forensique.

Pour une sécurité à toute épreuve, la solution s'intègre également à l'ensemble de la suite SASE. Piloté par Precision AI™ de Palo Alto Networks, Advanced WildFire®, le plus grand moteur de prévention des malwares en mode cloud, analyse plus de 77 millions de nouveaux fichiers et bloque au quotidien jusqu'à 450 000 fichiers malveillants uniques. À l'aide de la base de données CTI pure play optimisée par IA la plus vaste du marché, l'outil URL Filtering piloté par IA neutralise chaque jour 151 millions d'URL malveillantes. En parallèle, Advanced Threat Prevention défend en temps réel contre les attaques sophistiquées, grâce à des modèles de deep learning capables de stopper 90 % des attaques par injection.

Dans un tel environnement, la sécurisation de tous les appareils représente une priorité absolue pour les entreprises. À condition de pouvoir parer aux risques des terminaux non gérés, laisser aux collaborateurs la latitude de choisir leur équipement de travail, c'est la garantie d'une productivité et d'une satisfaction accrues. Avec une protection complète déployée sur tous les appareils, les organisations conservent une posture de sécurité solide, réduisent le risque de perte de données et garantissent leur conformité réglementaire.

Visibilité et contrôle renforcés sur les applications SaaS et web

Prisma Access Browser renforce la sécurité et le contrôle des activités utilisateurs dans les applications SaaS et web en étendant les politiques contextuelles Zero Trust à toutes les actions, quelle que soit l'application. Résultat, les contrôles sont appliqués de façon homogène dans l'ensemble de l'environnement, aussi bien pour les données et les identités que les accès privilégiés. En étendant le Zero Trust à tous les attributs d'appareils et d'utilisateurs, toutes les applications web et toutes les actions avec des contrôles au dernier kilomètre, les organisations gardent une maîtrise totale de leur infrastructure et se protègent contre les fuites de données accidentelles ou intentionnelles.

Moteurs de classification des données, authentification multifacteur (MFA), accès JIT… la solution réunit tous les atouts d'une couverture de sécurité infaillible. Qu'elles soient accidentelles ou intentionnelles, les fuites de données peuvent avoir de profondes répercussions. D'ailleurs, 55 % des entreprises ont subi une fuite accidentelle de données au cours des 12 derniers mois[3].

C'est là que le solide arsenal de fonctionnalités de Prisma Access Browser fait toute la différence pour réduire le risque de perte de données. En outre, les équipes de sécurité bénéficient d'éclairages granulaires sur les interactions des utilisateurs avec les ressources d'entreprise afin d'assurer la surveillance et la réponse en temps réel face aux menaces. Elles visualisent ainsi tous les attributs d'appareils et d'utilisateurs, y compris l'utilisateur/le groupe, la posture de sécurité de l'appareil, le réseau et l'emplacement. Fortes de cette visibilité accrue, les entreprises appliquent de strictes mesures de protection des données et de contrôle des accès aux informations sensibles en fonction du rôle utilisateur, du contexte et des comportements. Ce faisant, elles empêchent les accès non autorisés aux données et leur exfiltration et veillent à ce que seuls les administrateurs autorisés réalisent des actions à haut risque.

Or une meilleure visibilité et un contrôle renforcé sont essentiels pour garantir la sécurité et la conformité de l'environnement, en particulier lorsque des données sensibles et des applications critiques sont en jeu. Prisma Access Browser permet aux organisations de consigner dans des journaux, de surveiller et de contrôler tout le trafic web et SaaS, sans avoir à effectuer le moindre déchiffrement. Chargement/téléchargement de fichiers, copier/coller, saisie de texte, masquage de texte, impression, capture/partage d'écran, utilisation du micro/de la caméra… toutes ces actions peuvent également être soumises à des contrôles. Pour une solide protection des contenus, le navigateur s'intègre à Palo Alto Networks DLP, qui inclut plus de 1 000 classificateurs de données, ainsi que des fonctions ML/NLP avancées, OCR, EDM et IDM. Par ailleurs, il comporte 22 profils de conformité prédéfinis en fonction de diverses réglementations, notamment HIPAA, PII, RGPD et PCI.

3. *Sécurité des espaces de travail : état des lieux et éclairages pour les dirigeants IT et SecOps*, Palo Alto Networks et Omdia, février 2025.

Avec le contrôle des données, des identités et des accès jusqu'au dernier kilomètre, les entreprises appliquent leurs politiques de sécurité de façon homogène, indépendamment de l'emplacement ou de l'appareil de l'utilisateur. Le renforcement des autorisations MFA et JIT avec des mesures de sécurité supplémentaires (clés d'accès, processus d'autorisation administrateur, etc.) constitue une protection supplémentaire, en particulier pour les utilisateurs privilégiés.

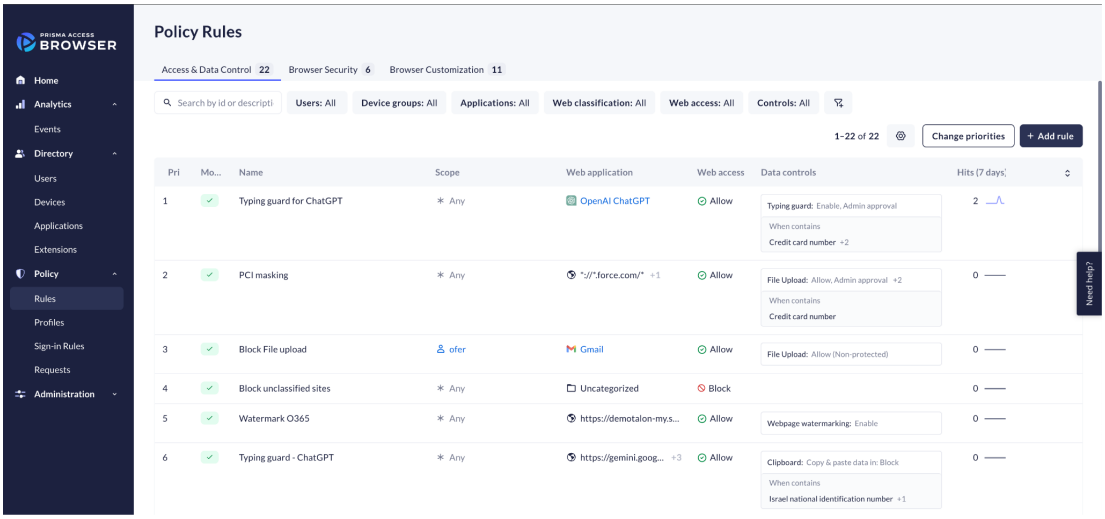

Figure 3. Les règles ultra-configurables couvrent tous les attributs d'appareils et d'utilisateurs, toutes applications confondues

Expérience utilisateur irréprochable

Prisma Access Browser est conçu pour offrir une expérience utilisateur d'exception, avec une disponibilité maximale et une nette amélioration des performances. Garante de fiabilité et de rapidité, son infrastructure entièrement distribuée assure une navigation fluide et productive. Applications publiques, SaaS, privées, SSH/RDP… toutes sont accessibles directement depuis le navigateur. Prisma Access Browser réduit au minimum les mesures de sécurité susceptibles d'entraver la productivité, afin que les utilisateurs ne soient pas tentés de contourner les protocoles et contribuent plutôt à maintenir la productivité. Pour répondre à la demande croissante d'applications GenAI, le navigateur fournit un accès sécurisé et optimisé à ces outils avancés, livrant une productivité accrue sans compromis sur la sécurité.

Le tout, avec des performances applicatives jusqu'à cinq fois supérieures aux solutions traditionnelles. Les collaborateurs pouvant ainsi accomplir leurs tâches plus rapidement et efficacement, l'entreprise tout entière gagne en productivité. Le navigateur récupère de manière proactive le contenu le plus pertinent, assurant ainsi des interactions rapides et fluides. Par ailleurs, les processus optimisés d'onboarding et d'offboarding se finalisent en quelques minutes, sans refonte de l'infrastructure. Une simplification des opérations IT qui réduit le coût total de possession (TCO) d'environ 80 % par rapport à la distribution d'ordinateurs portables.

La satisfaction des collaborateurs et l'adoption des technologies passent par une bonne expérience utilisateur. Lorsqu'ils naviguent avec rapidité et fiabilité, les salariés sont plus susceptibles de respecter les mesures de sécurité en place plutôt que de les contourner. Il en va non seulement de la productivité globale, mais surtout de la conformité aux politiques de sécurité. Prisma Access Browser assure une disponibilité maximale, sans aucun point de défaillance unique, ce qui renforce la confiance et la satisfaction des utilisateurs.

La réduction des coûts IT et la simplification de la gestion des appareils libèrent des ressources pour d'autres initiatives stratégiques, moteurs de croissance et d'efficacité pour l'entreprise. Le navigateur permet de définir facilement des politiques, puis de les déployer dans l'ensemble de l'entreprise. En outre, le module ADEM (Autonomous Digital Experience Management) prévient et résout les problèmes de performances applicatives, en fournissant des informations sur les performances des appareils et du réseau, l'état du Wi-Fi et bien plus encore.

Composante intégrale de l'ADEM, Real User Monitoring (RUM) garantit une productivité ininterrompue sur le navigateur avec des éclairages supplémentaires sur les performances, notamment les temps de rendu et de chargement des pages. L'intégration à la solution AI Access Security™ sécurise l'adoption de l'IA par les collaborateurs en deux volets : 1) par une visibilité totale en temps réel sur son utilisation (permettant d'identifier les applications d'IA et leurs utilisateurs) ; et 2) par une protection complète des données, qui passe par l'analyse des données, des secrets et de la propriété intellectuelle (PI) partagés. Disponibles à portée de clic, les contrôles d'accès bloquent les applications non approuvées, exécutent des politiques InfoSec et protègent les données. À la clé, une expérience utilisateur irréprochable et sécurisée.

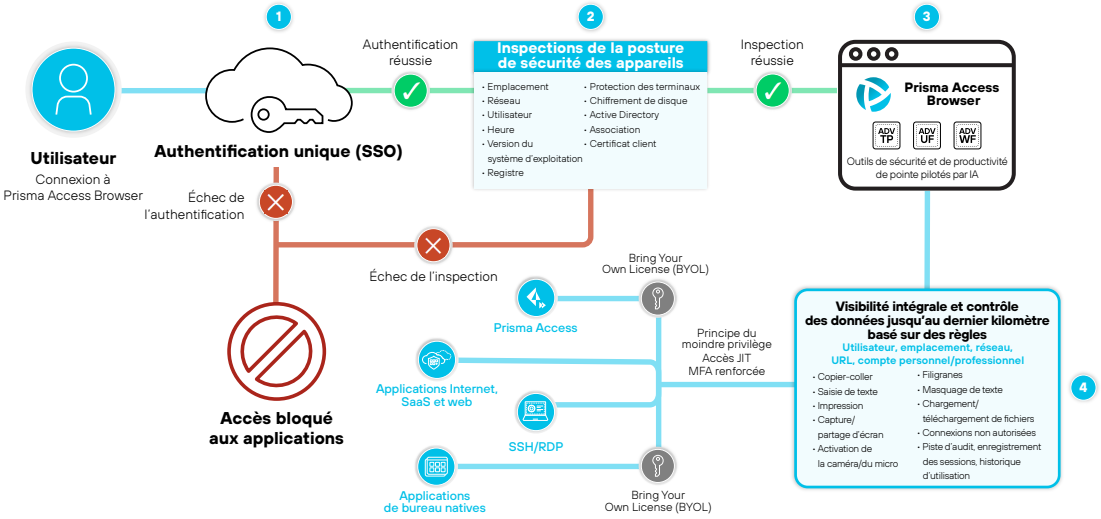

Figure 4. Exemple d'accès à un environnement de travail depuis Prisma Access Browser

Cas d'usage concrets de Prisma Access Browser

Travailleurs indépendants

Prisma Access Browser est conçu pour fournir aux collaborateurs externes un accès sécurisé et optimisé aux applications SaaS et privées en quelques minutes, quel que soit l'appareil. Une capacité qui s'avère cruciale dans de nombreux scénarios, notamment les fusions-acquisitions, les centres d'appel, ainsi que pour les équipes de terrain et de première ligne. Contrairement aux solutions traditionnelles basées sur les privilèges administrateur, Prisma Access Browser offre un accès fluide et sécurisé, sans intervention de l'utilisateur.

Fusions-acquisitions

L'intégration rapide et sécurisée d'un écosystème IT disparate fait partie des problématiques majeures d'une fusion-acquisition. À cela s'ajoute l'impératif de la productivité des collaborateurs pendant la transition afin d'accélérer la rentabilité, mesure clé de la réussite de l'initiative. Prisma Access Browser agit sur ces deux tableaux, en permettant aux nouvelles équipes d'accéder aux applications critiques en quelques minutes sur tous les appareils, gérés ou non, sans compromis sur la sécurité. Par cet accès rapide et protégé aux applications d'entreprise, SaaS et GenAI, Prisma Access Browser permet aux collaborateurs de rester productifs tout le long du processus de fusion-acquisition. Le tout, avec un coût financier moindre par rapport à la distribution d'ordinateurs portables et aux VDI. En conjuguant politiques de sécurité granulaires et protection avancée contre les menaces, les entreprises veillent à préserver les données sensibles pendant toute la durée de l'intégration.

Centres d'appel

Souvent, les centres d'appel combinent collaborateurs à plein temps, intervenants externes et prestataires tiers. Or, tous ces acteurs ont besoin d'accéder promptement et en toute sécurité aux données clients et aux applications d'entreprise. D'où l'intérêt de Prisma Access Browser pour sécuriser les accès en fonction du contexte sur tous les appareils. L'objectif : garantir à la fois l'efficacité des agents et la conformité aux réglementations sur la protection des données.

Équipes de terrain et de première ligne

Les équipes de terrain et de première ligne interviennent fréquemment dans des environnements où les mesures de sécurité traditionnelles s'avèrent souvent intenables. Avec Prisma Access Browser, ils accèdent en toute confiance aux applications et aux données d'entreprise depuis leurs appareils mobiles, disposant ainsi des outils nécessaires à l'exercice de leur mission.

En fournissant un accès sûr aux applications SaaS et privées pour tous les collaborateurs externes, Prisma Access Browser aide les structures à étendre leur périmètre de sécurité au-delà des frontières traditionnelles. De ce fait, la solution renforce non seulement leur agilité et leur flexibilité opérationnelles, mais sécurise et optimise aussi le travail de tous les utilisateurs, quel que soit leur appareil ou leur l'emplacement.

Bring Your Own Device (BYOD)

Avec Prisma Access Browser, les collaborateurs sont libres d'utiliser leur équipement personnel dans le cadre professionnel, accédant de façon sécurisée aux applications métiers, partout et à tout moment. Les avantages à la clé sont multiples : agilité des collaborateurs, choix des équipements, intégration des appareils mobiles, baisse des coûts et réduction de la dépendance aux VDI.

Agilité des collaborateurs

Dans un monde du travail en constante évolution, les collaborateurs doivent pouvoir accéder aux ressources d'entreprise en déplacement. Levier d'agilité, Prisma Access Browser sécurise les connexions aux applications SaaS et privées depuis des appareils personnels. En télétravail, en voyage ou au bureau, les collaborateurs continuent de travailler avec la même productivité, sans être rattachés à une machine ou à un emplacement spécifiques.

Choix des équipements utilisés

Avec Prisma Access Browser, le travail hybride ne se limite plus aux appareils fournis par l'entreprise. De fait, les collaborateurs peuvent accéder aux applications métiers depuis le smartphone, la tablette ou l'ordinateur portable de leur choix en toute simplicité, pour une expérience personnalisée.

Appareils mobiles

Pour les collaborateurs ayant besoin d'accéder aux applications métiers en dehors des bureaux traditionnels, l'intégration des appareils mobiles est absolument primordiale. C'est là que Prisma Access Browser entre en scène, embarquant en toute sécurité les appareils mobiles sur le réseau d'entreprise pour un accès fluide aux outils et aux informations essentiels. Concrètement, cette capacité sert surtout les équipes de terrain, les commerciaux et les télétravailleurs qui dépendent de leurs appareils mobiles pour rester connectés et productifs.

Coût inférieur à l'achat d'ordinateurs portables d'entreprise

Outre le défi logistique, la distribution d'ordinateurs portables d'entreprise représente un coût conséquent. La bonne nouvelle, c'est qu'elle n'est même plus nécessaire avec Prisma Access Browser : un nouveau collaborateur peut bénéficier d'un accès protégé depuis n'importe quel appareil personnel. L'organisation réalise ainsi d'importantes économies par rapport au coût d'achat et de provisionnement des équipements, en particulier pour les intérimaires ou les intégrations IT de grande envergure.

Les fonctions de BYOD offertes par Prisma Access Browser confèrent aux collaborateurs la liberté d'utiliser leurs propres appareils, clé d'une agilité et d'une productivité renforcées. En résumé, un accès sécurisé et flexible aux applications métiers réduit les coûts, rationalise les opérations IT et optimise le travail hybride.

GenAI sécurisée

Les outils d'IA générative révolutionnent certes les opérations en entreprise, mais introduisent également des risques pour la sécurité. Pour y parer, Prisma Access Browser fournit un environnement sécurisé afin d'exploiter les outils GenAI web. Avec les contrôles DLP jusqu'au dernier kilomètre du navigateur, les interactions entre les données et les plateformes d'IA au sein du navigateur sont protégées.

Interactions sécurisées avec les données

Sans le savoir, les collaborateurs peuvent charger des données sensibles dans les applications GenAI. Contre ce risque, la protection des données s'impose comme une nécessité. Blocage du copier-coller, désactivation du chargement de fichiers, prévention de la saisie d'informations sensibles dans l'appli… Prisma Access Browser protège les données en cours d'utilisation jusqu'au dernier kilomètre. Ces précautions sont d'autant plus vitales qu'elles empêchent la fuite accidentelle de données, lorsque les utilisateurs partagent des informations sensibles avec les systèmes d'IA.

Visibilité et contrôle des accès

Avec les outils de GenAI, deux problématiques majeures émergent : la visibilité sur e Shadow AI et le maintien du contrôle des accès utilisateur. Prisma Access Browser offre une vue à 360° sur l'adoption et l'utilisation de l'IA. Résultat, les équipes de sécurité IT sont à même de surveiller et de gérer les interactions avec des plateformes comme ChatGPT. La protection des informations sensibles et le respect des politiques d'usage acceptable passent par cette visibilité, d'autant plus utile dans les entreprises autorisant l'utilisation d'appareils non gérés.

Prisma Access Browser et AI Access Security

Conjugué à AI Access Security, une solution spécialement conçue pour la GenAI, le navigateur Prisma Access Browser sécurise l'adoption et l'utilisation de l'IA pour les appareils gérés et non gérés. En parallèle, il protège les données sensibles côté client et réseau. Quant à AI Access Security, elle contrôle les applications GenAI approuvées et fournit des protections supplémentaires pour la gestion de la posture GenAI, les marketplaces d'IA, les plug-ins et plus encore. Fonctionnant de concert au sein d'une solution SASE complète, tous deux fluidifient l'expérience des collaborateurs sur navigateur avec une liberté totale dans le choix des appareils, appuyée par une protection et des contrôles solides.

De son côté, Prisma Access Browser aide les entreprises à innover et à gagner en productivité, sans transiger sur la sécurité. À l'heure où l'IA occupe une place de plus en plus importante dans les opérations, cet équilibre entre sécurité et innovation est plus que jamais primordial.

Réduction des VDI

Bien souvent, l'entretien des solutions VDI s'avère aussi complexe que coûteux. Solution basée sur le navigateur, Prisma Access Browser réduit la dépendance vis-à-vis de l'infrastructure VDI et offre un environnement à la fois contrôlé et sécurisé pour les applications métiers. La diminution des déploiements VDI entraîne non seulement des économies opérationnelles, mais améliore aussi l'expérience utilisateur avec un accès plus rapide et plus fiable aux applications.

Optimisation des ressources

Les environnements VDI tendent à mobiliser d'importantes ressources tant pour la gestion que pour les opérations. En résulte une infrastructure complexe aux coûts élevés. La solution : migrer les activités de navigation de routine vers Prisma Access Browser pour alléger la pression sur les systèmes VDI. Une approche qui se traduit par une allocation des ressources plus efficace et une réduction des coûts d'infrastructure globaux.

Groupes d'utilisateurs segmentés

Tous les collaborateurs ne nécessitent pas un accès complet à l'infrastructure VDI. Pour beaucoup, une navigation sécurisée suffit. Avec Prisma Access Browser, il est possible de segmenter les utilisateurs en différents groupes, selon qu'ils travaillent depuis le navigateur seulement ou qu'ils requièrent un poste complet. Ce faisant, les entreprises optimisent les déploiements VDI avec le niveau d'accès adapté aux besoins des utilisateurs. Résultat : des économies pour l'entreprise et une amélioration des performances pour les utilisateurs sans poste de travail VDI complet.

Économies

Entre l'entretien des équipements et les coûts opérationnels, le maintien d'une infrastructure VDI finit par coûter cher. En sécurisant l'accès aux applications métiers via le navigateur, Prisma Access Browser propose une option plus économique. Avec un coût total de possession (TCO) moindre, les entreprises diminuent les déploiements VDI coûteux sans renoncer à un accès sécurisé aux ressources professionnelles dans un environnement contrôlé.

Réduction des coûts, simplification de l'infrastructure IT et amélioration de l'expérience utilisateur globale : telle est la triple promesse de Prisma Access Browser. Cette nouvelle approche de l'accès distant s'avère particulièrement stratégique à l'heure où les entreprises adoptent des solutions IT toujours plus flexibles et évolutives.

Continuité d'activité

Un accès transparent aux applications métiers critiques, même dans un contexte perturbé, constitue la clé de la continuité opérationnelle. À cet effet, Prisma Access Browser garantit une connexion sécurisée et ininterrompue aux ressources d'entreprise depuis tous les appareils, où qu'ils soient. Combinant protection des données intégrée et détection des menaces en temps réel, la solution préserve les informations sensibles et assure la bonne continuité des activités, même en cas d'incident ou de perturbation.

Sécurisation des accès sur tous les appareils

Avec un navigateur d'entreprise comme Prisma Access Browser, les collaborateurs ne sont pas interrompus dans leur travail, et ce, malgré d'éventuels problèmes techniques. Au contraire, ils continuent d'accéder en toute sécurité aux applications métiers partout dans le monde, depuis n'importe quel appareil, même non géré.

Activation en quelques minutes

En cas de perturbation, un clic suffit pour faire de Prisma Access Browser le nouvel espace de travail principal. Dans les paramètres, il est facile de définir quels utilisateurs ont le droit d'accéder à quelles applications, en imposant pour chaque activité des mesures de sécurité et une vérification de la posture des appareils. Ainsi, même en cas d'interruption de service, les collaborateurs disposent d'un accès rapide et sécurisé à leurs outils de travail.

Sécurité avancée

Les catastrophes comme les pandémies, les guerres et les pannes IT généralisées constituent une véritable aubaine pour les cybercriminels, qui profitent de la confusion des collaborateurs et des citoyens pour passer à l'attaque. Prisma Access Browser garantit la continuité des opérations dans un environnement sécurisé, avec une visibilité totale et un contrôle complet de toutes les activités dans le navigateur. Doté d'un haut niveau de granularité dans le contrôle des accès, des données et des identités, il permet une configuration parfaitement adaptée à vos activités et livre une vue à 360° sous-tendue par la journalisation des événements, l'enregistrement des sessions et bien plus.

Adoption fluide pour tous les collaborateurs

À l'heure où au moins 85 % du temps de travail d'un salarié s'effectue dans le navigateur, migrer vers Prisma Access Browser semblera parfaitement naturel. Exit l'achat d'équipements et la réinitialisation de systèmes. Les collaborateurs du monde entier n'ont qu'à ouvrir leur ordinateur portable pour réaliser en un rien de temps toutes les tâches indispensables au bon fonctionnement de l'entreprise : apporter les changements requis dans l'environnement de production, communiquer avec les clients et les collègues, accéder aux informations sensibles, utiliser les postes et les serveurs distants pour les processus métiers et bien plus encore.

Sécurisation des applications qui n'autorisent pas le déchiffrement

Aujourd'hui, les entreprises exploitent toute une panoplie d'applications SaaS et web, la plupart passant par des canaux chiffrés pour une meilleure efficacité opérationnelle. Malheureusement, cette dépendance n'a pas échappé aux cybercriminels. Ceux-ci s'engouffrent dans les canaux chiffrés d'applications très prisées, telles que Microsoft 365, Google Workspace et Slack, pour y cacher des malwares, établir des communications C2 et exfiltrer les données sensibles. Les chiffres parlent d'eux-mêmes : désormais, 86 % des cyberattaques sont lancées via de canaux chiffrés[4]. Par conséquent, un vrai framework de sécurité Zero Trust passe en premier lieu par une meilleure visibilité sur ces applications.

Déchiffrement hors pair avec les solutions de sécurité Palo Alto Networks

Avec son pare-feu nouvelle génération (NGFW) et ses solutions SASE, Palo Alto Networks offre les meilleures fonctions de déchiffrement du marché pour le trafic web et hors web. Pilotées par Precision AI, les solutions inspectent le trafic chiffré en profondeur afin de bloquer les menaces connues et inconnues, tout en mettant des capacités DLP avancées au service d'une solide protection des données. Néanmoins, certains types de trafic ne sont pas déchiffrés, du fait des fonctionnalités de l'application, des exigences réglementaires ou des besoins de l'expérience utilisateur. Conséquence : quelque 64 % du trafic web demeure chiffré et donc potentiellement vulnérable aux menaces furtives[5].

Visibilité sécurisée en complément du déchiffrement

Afin de remédier au chiffrement d'une part du trafic, Prisma Access Browser vient compléter nos fonctionnalités de déchiffrement réseau pour former une solution multicouche unifiée de sécurité Zero Trust. Seul navigateur sécurisé SASE-native du marché, il assure visibilité et contrôle sur toutes les applications ouvertes via le navigateur, sans nécessairement déchiffrer le trafic. En outre, il étend les politiques Zero Trust à l'ensemble des activités sur navigateur grâce aux mêmes capacités de détection des menaces avancées et de protection des données qui font l'excellence de nos solutions réseau. Par conséquent, l'ensemble du trafic, même non déchiffré, peut être surveillé et contrôlé pour une réduction des risques sans impact sur les performances.

Approche en double couche pour une protection complète

Prisma Access Browser s'intègre à la plateforme de sécurité réseau de Palo Alto Networks pour livrer une visibilité complète et un contrôle total sur le trafic chiffré dans l'ensemble des applications et des canaux de communication. Notre sécurité réseau assure un déchiffrement et une prévention des menaces inégalés, tandis que Prisma Access Browser sécurise les activités basées sur le navigateur incompatibles avec le déchiffrement. Leur puissance combinée garantit qu'aucun trafic, chiffré ou non, ne reste dans l'angle mort.

Ce modèle en double couche détecte les menaces furtives, préserve les données sensibles et protège en toute transparence les appareils gérés et non gérés. Face à la complexité des menaces actuelles, les entreprises adoptent avec Prisma Access Browser une véritable posture Zero Trust couvrant l'ensemble du trafic, sans compromis sur l'expérience utilisateur ni la productivité.

Cas d'usage innovants

Avec ses fonctionnalités de sécurité avancées directement intégrées au navigateur, Prisma Access Browser ouvre un tout nouveau champ de cas d'usage jusqu'alors impossibles à réaliser (ou du moins, difficilement) avec les solutions traditionnelles. Désormais, les entreprises peuvent réagir rapidement faux nouveaux modes d'attaque dynamiques grâce à des contrôles flexibles des données, accès et identités. Au menu : protection des données jusqu'au dernier kilomètre, sécurisation des utilisateurs privilégiés, prévention des menaces internes, continuité des opérations, adoption des outils GenAI et gestion du Shadow IT.

4. « 86 % des cyberattaques passent par des canaux chiffrés », Help Net Security, 21 décembre 2023.
5. *Sécurité des espaces de travail : état des lieux et éclairages pour les dirigeants IT et SecOps*, Palo Alto Networks et Omdia, janvier 2025.

Protection des données jusqu'au dernier kilomètre

C'est dans la dernière ligne droite de la transmission et de l'accès aux données que celles-ci sont le plus exposées aux compromissions. Les collaborateurs passant en moyenne 85 % de leur journée sur le navigateur, cette sécurisation « jusqu'au dernier kilomètre » est fondamentale. Chiffrement, contrôle des accès, surveillance en temps réel… Prisma Access Browser intègre en toute transparence un riche arsenal de mesures de sécurité directement dans le navigateur. Il propose ainsi des contrôles avancés tels que le masquage de données, l'obstruction des captures d'écran, la restriction des partages dans les outils de collaboration, le blocage des copier-coller, la prévention des impressions ainsi que l'application de filigranes sur les écrans sensibles.

Sécurité des utilisateurs privilégiés

Avec leurs droits d'accès supérieurs, les utilisateurs privilégiés constituent des cibles de choix. C'est là que Prisma Access Browser intervient pour renforcer leur sécurité : durcissement de l'authentification multifacteur pour les étapes critiques des workflows, protection des données jusqu'au dernier kilomètre, contrôles de sécurité pour veiller à l'intégrité des données, vérification de la posture des appareils, pistes d'audit détaillées de toutes les activités (y compris des enregistrements de sessions). Grâce à ces mesures de sécurité exhaustives, les utilisateurs privilégiés évoluent dans un environnement à la fois sécurisé et contrôlé.

Prévention des menaces internes

Qu'elles soient intentionnelles ou accidentelles, les menaces internes font peser un risque majeur sur la sécurité des données d'entreprise. C'est pourquoi Prisma Access Browser déploie tout un éventail de contrôles qui définissent notamment les applications à utiliser uniquement dans l'environnement sécurisé du navigateur. Ce faisant, les entreprises érigent des cloisons nettes entre espaces de travail numériques et comptes personnels, avec une maîtrise totale du type de fichiers pouvant être partagés ou accédés. À titre d'exemple, les fichiers téléchargés sur une application métier peuvent être chiffrés et interdits d'accès par des applications SaaS n'appartenant pas à l'entreprise. Ainsi, les données sensibles restent au sein du navigateur sécurisé, où elles sont protégées.

Accès aux comptes non gérés

Pour les salles de marché virtuelles ou les services financiers, les organisations ont souvent besoin d'accorder des accès à des comptes qu'elles ne gèrent pas ce qui présente un défi évident pour la sécurité. Prisma Access Browser sécurise ces applications en déployant une fonctionnalité de protection des comptes en attente de brevet. Le principe ? Cet outil innovant ajoute à chaque mot de passe utilisateur un élément secret, stocké dans Prisma Access Browser. En d'autres termes, aucun autre utilisateur ni aucun autre navigateur ne peuvent accéder au compte.

Shadow IT

L'utilisation d'applications et d'appareils non approuvés, ou Shadow IT, présente des risques importants en termes de sécurité. La bonne nouvelle, c'est que Prisma Access Browser offre aux entreprises une visibilité à 360° sur les activités web pour surveiller et gérer efficacement ce danger. En outre, la solution prévient les fuites des données et garantit la conformité aux politiques de sécurité de l'ensemble des applications et des appareils utilisés dans l'organisation.

Prisma Access Browser ouvre la voie à de nombreux cas d'usage innovants grâce à des contrôles flexibles des données, accès et identités directement dans le navigateur. À la clé, une sécurité et une productivité renforcées qui permettent aux entreprises de réagir face aux nouveaux modes d'attaque dynamiques avec sérénité et agilité. En éliminant l'angle mort que constitue le navigateur, Prisma Access Browser livre une puissante solution de sécurité complète, à la hauteur des défis complexes du monde du travail actuel.

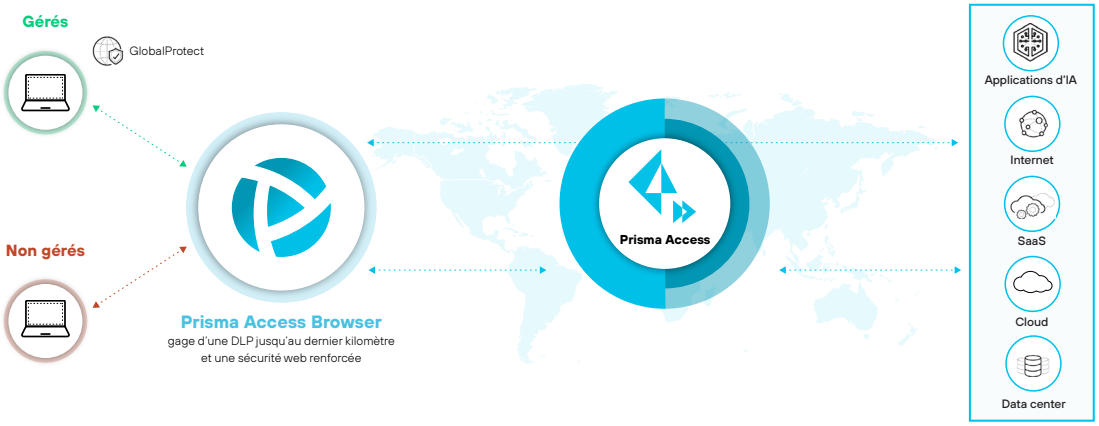

Figure 5. Prisma Access Browser libère la puissance du SASE

L'avenir de la sécurité web-first

Comme chacun sait, les menaces évoluent au rythme des avancées dans la sécurisation des collaborateurs. De l'exploitation des ressources cloud à l'adoption de l'IA au quotidien, nos modes de travail changent. Résultat, le maintien de la sécurité et de la productivité virent au casse-tête. Conçus pour des environnements plus statiques, les modèles de sécurité traditionnels ne suffisent plus. Le travail hybride requiert des solutions au diapason de sa propre flexibilité dynamique.

En ce sens, Prisma Access Browser représente un pas décisif dans la bonne direction. En étendant le SASE par le navigateur, cette solution garantit une expérience utilisateur fluide et sécurisée sur tous les appareils, gérés ou non, partout sur la planète.

Selon les prédictions, l'importance des navigateurs sécurisés ne devrait cesser de croître à l'avenir. Gartner estime en effet que « d'ici 2030, les navigateurs d'entreprise deviendront la principale plateforme de sécurité et d'accès aux outils de productivité des collaborateurs sur les appareils gérés et non gérés, assurant ainsi une expérience fluide dans une configuration de travail hybride »[6]. Cette tendance ne fait que souligner l'urgence d'une sécurité complète capable de répondre aux besoins actuels des entreprises en matière de flexibilité et d'agilité, à l'instar de la solution Prisma Access Browser.

Car le nouveau monde du travail est déjà là et il tourne autour du navigateur. Avec la généralisation du travail hybride, les outils sécurisés, efficaces et intuitifs prendront une importance plus cruciale encore. Non seulement Prisma Access Browser répond déjà à ce besoin, mais il anticipe aussi les problématiques futures d'un monde du travail en pleine mutation. Alliant sécurité hors pair et expérience utilisateur d'exception, le navigateur garantit la protection et la productivité des entreprises, quels que soient le lieu ou la façon dont les collaborateurs préfèrent travailler.

Il va de soi que les solutions de sécurité doivent évoluer au même rythme que les entreprises. Pour fluidifier cette transition, Prisma Access Browser propose une puissante approche intégrée de la sécurisation du navigateur, principale interface de travail aujourd'hui. Avec ses fonctionnalités avancées et son intégration fluide au framework SASE, il redéfinit les codes de la sécurité d'entreprise, ouvrant la voie à un avenir où productivité rime avec protection.

6. Dan Ayoub et al., *Emerging Tech: Security – The Future of Enterprise Browsers*, Gartner, 14 avril 2023.

paloalto NETWORKS

Oval Tower, De Entrée 99-197
1101HE Amsterdam, Pays-Bas

Téléphone :+31 20 888 1883
www.paloaltonetworks.fr

prisma_wp_pab-integral-part-of-sase_020425-fr