

Prisma Access Browser

Le SEUL navigateur d'entreprise sécurisé pour tous les users, tous les appareils, toutes les applications

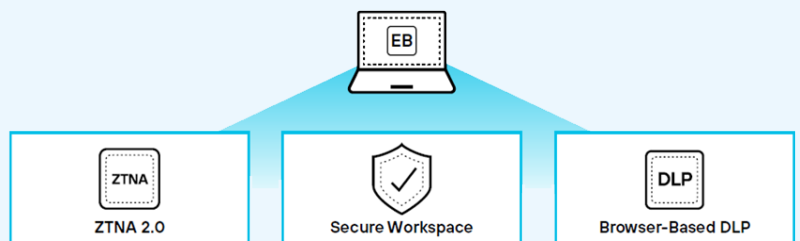


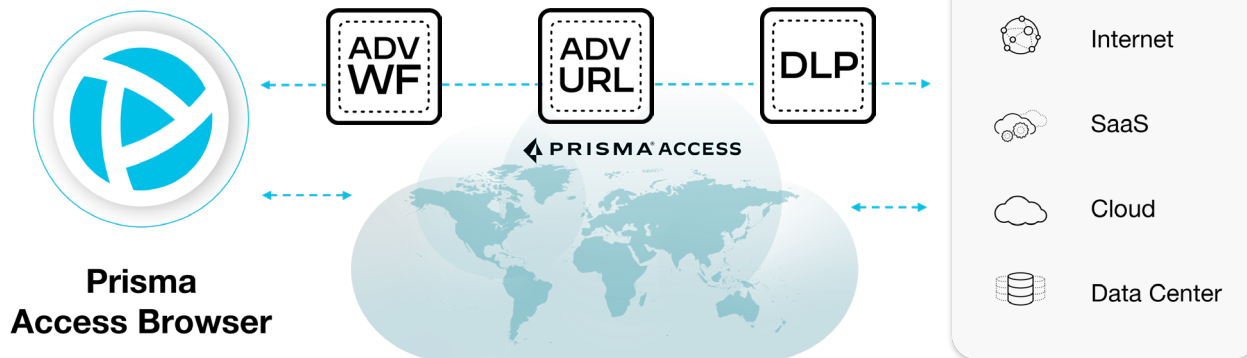
Avec la généralisation des applications Web et SaaS, le navigateur est devenu l'espace de travail principal. Cependant, la dépendance croissante au navigateur a également révélé une faille critique dans la sécurité des entreprises.

Le navigateur sécurisé Prisma Access Browser de Palo Alto Networks **étend la sécurité du SASE** à tous vos appareils gérés et non gérés, en toute transparence, sans problème de déchiffrement pour vous offrir contrôle, agilité et protection. Prisma Access Browser **disponible en stand alone**, s'installe sans droit d'admin sur n'importe quel poste, en quelques minutes et est compatible avec tous les OS.

Avantages de Prisma Access Browser

- **Sécurité SASE avancée** : Offrez une sécurité complète pour tous les appareils, qu'ils soient gérés ou non, contre les menaces internes et externes (y compris les attaques de phishing générées par l'IA, les malwares et les fuites de données).
- **Économie de coûts** : Bénéficiez d'une réduction significative du coût par rapport aux solutions VDI traditionnelles, grâce à l'architecture cloud-native efficace, à la simplicité opérationnelle de Prisma Access Browser et un déploiement simplifié sur les devices gérés et non gérés.
- **Accès sécurisé pour les tiers et le BYOD** : Permettez un accès sécurisé aux ressources de l'entreprise depuis des appareils personnels (BYOD) et pour les partenaires tiers, tout en maintenant la conformité et en protégeant les applications critiques.
- **Approche unifiée** : Intégrez des fonctionnalités de sécurité avancées telles que ZTNA 2.0, la prévention des menaces alimentée par l'IA et la prévention des fuites de données (DLP) basées sur le navigateur, pour une solution cohérente et facile à gérer.
- **Simplicité opérationnelle** : Centralisez le contrôle et la visibilité pour tous les appareils, depuis la plateforme unifiée de sécurité réseau de Palo Alto Networks (Strata Cloud Manager) simplifiant ainsi la gestion et améliorant l'efficacité IT.





Les cas d'usage de Prisma Access Browser

- **Tiers et collaborateurs externes** : Appliquez des politiques d'accès Zero Trust et des contrôles granulaires sur l'utilisation des données pour les partenaires tiers, en veillant à ce qu'ils disposent des outils nécessaires sans exposer votre réseau à des risques.
- **Applis d'IA génératives** : Protégez vos données d'entreprise sur les outils de GenAI et bloquez les applications GenAI non autorisées (Shadow AI). Enfin, contrôlez le type de données qui peuvent être utilisées sur ces applications.
- **BYOD** : Permettez un accès sécurisé aux ressources de l'entreprise depuis n'importe quel appareil personnel, tout en maintenant productivité, conformité et contrôle granulaire.
- **VDI** : Réduisez les déploiements complexes et coûteux, sans compromis sur la sécurité des applications avec un déploiement simplifié et instantané par email.
- **Onboarding et offboarding rapides des utilisateurs** : Installez PAB sur n'importe quel poste en une minute, sans droit d'admin et accédez immédiatement à l'espace de travail.
- **Logging complets des utilisateurs** : Permettez le monitoring et la remontée d'informations granulaires des logs de chaque action et allez jusqu'à l'enregistrement de sessions sur les applications sensibles définies.

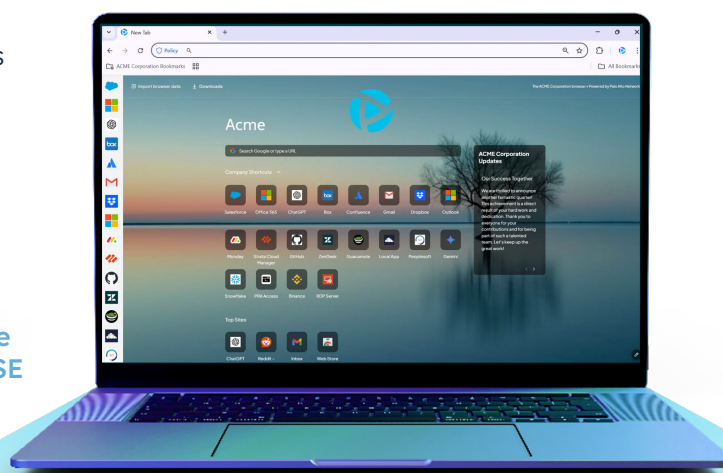
Prisma Access Browser : Le nouveau Workspace

Browse Bravely : Accès sécurisé à **toutes** les apps (SaaS, Web, privées, SSH, RDP...)

Performances 5 fois supérieures à un espace de travail classique

Disponible **en stand alone** ou **inclus dans l'offre SASE** selon la licence

Gestion autonome de l'expérience utilisateur. Anticipe et résout les problèmes de performance des apps



Contrôle total des extensions installées et des permissions

Onboarding/offboarding des collaborateurs en quelques minutes

Déploiement en quelques minutes, **sans refonte majeure** de votre infra, sur tous les OS

Disponibilité maximale **SANS spof (single point of failure)**

Accès rapide aux applications intégrées comme les apps d'IA génératives

Plus de problème de déchiffrement. Les flux sont traités à la source, avant chiffrement



Contactez-nous

01 60 19 02 30
reseausecu@miel.fr

PAB en vidéo →

