Prisma Access Browser

Contexte

Avec la généralisation des applications Web et SaaS, le navigateur devient le nouveau Workspace. Pourtant, les entreprises manquent de visibilité sur l'activité et le contrôle des users, ainsi que sur les équipements et les applications. L'utilisation des navigateurs traditionnels représente un risque important de compromission par exploitation de leurs nombreuses vulnérabilités et par une exposition accrue aux fuites de données (IA Gen, partage, upload/download). Enfin, par souci de flexibilité, dans le cadre d'une politique BYOD ou pour donner accès à des tierces parties (partenaires, indépendants, contractants…), ces applications sont ouvertes à des postes non managés, donc sans contrôle. Les solutions alternatives (VDI, postes dédiés, VPN, Proxy…) sont soit trop contraignantes pour la productivité et l'expérience utilisateur, soit trop élevées en TCO, soit trop complexes à gérer et à administrer.

Prisma Access Browser en 100 mots

Prisma Access Browser est **un navigateur d'entreprise** qui permet de créer **un espace de travail sécurisé pour tous les devices, managés ou non.** L'accès aux applications Web, SaaS ou privées est contrôlé de façon très **granulaire**, et **les endpoints comme les données sont protégés des menaces et des fuites**. Le ressenti utilisateur reste transparent et familier.

La **protection en continue** s'appuie sur les contrôles d'identité, de posture et la prévention en ligne **alimentée par l'IA de Palo Alto Networks**, qui bloque aujourd'hui plusieurs millions d'attaques quotidiennes. **Prisma Access Browser étend les fonctions SASE** à n'importe quel device, en quelques minutes.

Les 3 fonctions clés de Prisma Access Browser

Etendre le Zero Trust au navigateur

- Contrôle strict et continu de l'identité, du device, de la posture et de l'authentification
- Protection contre les menaces, filtrage Web, sandboxing, et protection DNS de Palo Alto Networks
- Masquage contextuel des données sensibles, contrôle/blocage des copies d'écran, du partage de documents
- MFA à la demande pour les actions sensibles

Créer un workspace sécurisé pour tout équipement

Protéger les données sensibles à la source

- Gestion des transferts de fichiers (restriction, chiffrement, blocage d'upload non autorisé, copier/coller externe au navigateur)
- Chiffrement renforcé du navigateur et contrôle/désactivation des composants sensibles
- Contrôle total des extensions installées et des permissions

Les interlocuteurs clés

- DSI/RSSI
- Responsable Architecture de sécurité
- Responsable Digital Workspace
- Responsable Sécurité réseau/SASE
- Responsable Sécurité Endpoint

Questions clés de découverte

- Quelle est votre proportion d'applications Web/SaaS critiques dans votre SI ?
- Comment gérez-vous la fuite de données dans votre navigateur aujourd'hui, comme le partage d'informations sensibles dans les apps d'IA générative ?
- Comment sécurisez-vous l'accès à vos applications Web/SaaS depuis un poste non managé ?
- Comment sécurisez-vous l'accès de tierces parties à vos applications Web/SaaS ?
- Envisagez-vous une réduction ou un remplacement de votre infrastructure VDI ?

Cas d'usage	Solution
Sécurisation des accès depuis des postes non managés (BYOD) ; Sécurisation des accès des partenaires/sous-traitant	PAB s'installe sans droit d'admin, sur n'importe quel poste et est compatible avec tous les OS. Pas de nécessité de dédier/livrer un PC.
Réduction des investissements VDI ou remplacement VDI	Remplacement du VDI en l'absence d'applis lourdes ; Suppression VDI pour les apps Web ; Intégration du client PAB au bureau VDI pour sécuriser les apps.
Protection contre la fuite de données, sécurisation des applis d'IA génératives	PAB permet une visibilité et un contrôle total à la source des actions de communication d'informations et de partage de fichiers, y compris les données échangées sur les applis d'IA gen.
Sécurisation du trafic chiffré (déchiffrement difficille/impossible)	Les règles d'inspection et de contrôle granulaires se font à la source, sans avoir à déchiffrer les flux.
Onboarding et offboarding rapides des utilisateurs (indépendants, fusion/acquisition)	PAB s'installe sur n'importe quel poste en une minute, sans droit d'admin et donne un accès immédiat à l'espace de travail.
Monitoring et logging complets des utilisateurs	Depuis une console unique, PAB permet le monitoring et la remontée d'informations granulaires de chaque action et pouvant aller jusqu'à l'enregistrement de session.

MIEL

Contactez-nous
01 60 19 02 30
reseausecu@miel.fr

Voir la démo →