

Akamai Enterprise Application Access et Secure Enterprise Browser



Les solutions traditionnelles de SSE (Secure Service Edge) garantissent une sécurité complète, mais s'accompagnent souvent d'une protection fragmentée, d'une complexité opérationnelle et de perturbations pour les utilisateurs, ce qui nuit à la productivité. Les entreprises doivent alors gérer un grand nombre de structures de règles et de goulets d'étranglement en matière de performances des serveurs proxys, tout en peinant à se protéger efficacement contre les menaces Web sophistiquées.

Akamai Enterprise Application Access et Secure Enterprise Browser

Les solutions associées Akamai Enterprise Application Access et Secure Enterprise Browser, optimisé par Seraphic, répondent aux cas d'utilisation SSE les plus critiques (accès sécurisé aux applications, sécurité Web et protection des données) avec une approche ciblée hautes performances. Cette combinaison assure un accès ZTNA (Zero Trust Network Access) pour les applications d'entreprise privées, ainsi qu'une sécurité de navigation avancée pour les applications SaaS et l'accès Internet. Elle offre ainsi une protection robuste avec une couverture sans faille, contrairement aux plateformes traditionnelles.

En se concentrant sur les principales exigences de sécurité, plutôt que d'essayer de répondre à tous les besoins, cette solution promet des performances supérieures, une complexité réduite et une baisse du coût total de possession.

Principales fonctionnalités et capacités

Accès sécurisé (ZTNA pour les applications privées)

- **Contrôle d'accès aux applications privées**, qui remplace l'accès réseau étendu par des autorisations granulaires basées sur l'identité pour les applications d'entreprise.
- **Application dynamique des règles** fondée sur l'identité des utilisateurs, la position des terminaux et l'évaluation des risques en temps réel.
- **Intégration des fournisseurs d'identité**, qui prend en charge les infrastructures d'identité d'entreprise existantes pour un accès fluide aux applications privées.
- **Prévention de la perte de données** avec analyse du contenu en temps réel et application de règles pour les applications privées.
- **Prise en charge des applications privées multicloud**, pour un accès sécurisé aux applications internes dans les environnements hybrides et cloud natifs.

Avantages pour votre entreprise

- ✓ **Obtenez de meilleurs résultats SSE** grâce à des solutions ciblées qui excellent dans des cas d'utilisation spécifiques, sans avoir à faire de compromis entre plusieurs domaines de sécurité. Bénéficiez de performances supérieures pour l'accès aux applications, la sécurité des navigateurs et les défis actuels en matière de protection des données pour les terminaux gérés et non gérés.
- 📊 **Contrôlez le partage de données via des outils d'IA générative** avec une visibilité en temps réel et l'application de règles en matière de données pour ChatGPT, Copilot et les plateformes similaires. Vous gagnez ainsi en productivité tout en protégeant votre propriété intellectuelle et en respectant les exigences de conformité.
- 🕒 **Profitez d'une rentabilisation plus rapide** par rapport aux mises en œuvre de SSE complètes grâce à un déploiement et à une gestion simplifiés, tout en répondant aux principaux cas d'utilisation qui motivent la plupart des initiatives SSE (y compris les exigences de gouvernance émergentes).
- 👤 **Minimisez les perturbations pour les utilisateurs** avec la possibilité d'utiliser n'importe quel navigateur existant, plutôt que de forcer les utilisateurs à s'adapter à de nouvelles interfaces, à des navigateurs spécialisés ou à la dégradation des performances applicatives qui accompagne souvent les plateformes SSE traditionnelles.
- 📈 **Réduisez la complexité et les coûts liés au SSE** en fournissant des fonctionnalités de sécurité Web et d'accès sécurisé de base, via une architecture simplifiée qui élimine le besoin de licences de plateforme SSE complètes, de services professionnels étendus et de gestion continue complexe.

- **Accès avec et sans client**, qui s'adapte à divers scénarios utilisateur sans la complexité apportée par les VPN.
- **Performances optimisées** via l'infrastructure mondiale d'Akamai en bordure de l'Internet.

Sécurité Web et protection des données (accès Internet et aux applications SaaS)

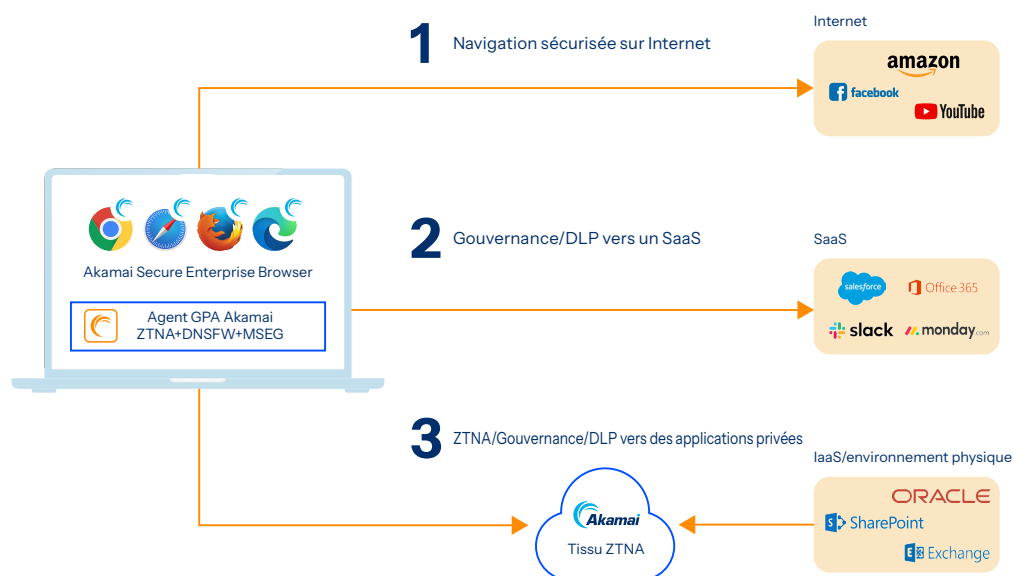
- **Contrôle d'accès aux applications SaaS** avec application de règles basée sur la posture des terminaux pour les applications cloud.
- **Prévention avancée des menaces**, avec le blocage des attaques « Zero Day » ainsi que des attaques sophistiquées basées sur le Web et axées sur l'identité, sans retard de détection.
- **Prévention complète des pertes de données** avec analyse du contenu en temps réel, masquage des données sensibles et application de règles sur les applications SaaS, la navigation Web et les grands modèles de langage basés sur l'IA.
- **Sécurité indépendante du navigateur**, qui transforme n'importe quel navigateur en un navigateur d'entreprise sécurisé pour l'accès Internet et aux applications SaaS.
- **Protection au niveau de la session**, qui comprend la sécurité des identités et la gestion des sessions chiffrées.
- **Sécurité des applications SaaS** qui étend la protection aux outils de collaboration actuels tels que Slack, Teams et autres applications cloud.

Capacités de remplacement des plateformes SSE

- **Protection SaaS et Web directe**, qui élimine le besoin d'adopter des solutions distinctes de courtier de sécurité d'accès au cloud (CASB).
- **Prévention des menaces intégrée**, qui remplace la fonctionnalité de passerelle Web sécurisée (SWG).
- **Sécurité intégrée au navigateur**, qui offre les avantages de l'isolation du navigateur à distance (RBI) sans impact sur les performances.

Architecture SSE simplifiée

Cette solution fournit des résultats dignes d'une plateforme SSE, mais avec davantage de flexibilité, grâce à deux composants optimisés qui fonctionnent parfaitement ensemble.



Sécurité réseau en bordure de l'Internet : l'accès Zero Trust aux applications d'entreprise privées à partir d'Akamai Connected Cloud élimine les failles de sécurité réseau auxquelles répondent les solutions SSE, tout en offrant des performances supérieures grâce à des points de présence dans le monde entier. Cette capacité remplace la passerelle Web sécurisée et les composants ZTNA de l'approche SSE traditionnelle pour l'accès aux applications internes.

Protection des données au niveau du navigateur : la sécurité avancée du navigateur offre une protection complète des applications SaaS et de l'accès Internet, garantissant ainsi une meilleure prévention des pertes de données et une sécurité Web directement au point d'interaction de l'utilisateur. En protégeant le navigateur, que les utilisateurs utilisent pour accéder à la fois aux applications SaaS approuvées et au contenu Internet en général, cette approche élimine le besoin d'adopter des solutions CASB, SWG et RBI traditionnelles, tout en offrant de meilleures performances et une meilleure expérience utilisateur.

Cette architecture conserve les valeurs fondamentales du SSE (accès sécurisé, protection Web et sécurité des données) tout en éliminant ses problèmes courants, tels que l'acheminement du trafic, la dégradation des performances et la gestion complexe des règles.

Pour en savoir plus sur Akamai Enterprise Application Access et Secure Enterprise Browser, optimisé par Seraphic, [contactez votre représentant Akamai ou contactez l'adresse \[sales@akamai.com\]\(mailto:sales@akamai.com\)](#).