Présentation du produit

Protéger votre personnel et votre entreprise avec SafeNet Trusted Access

cpl.thalesgroup.com

THALES
Building a future we can all trust

THALES
Building a future we can all trust

Parmi les entreprises les plus avancées sur le plan technique et les plus efficaces au monde, cellezs axées sur le cloud ont établi des nouvelles normes pour les employés modernes. Dans un contexte où les employés du monde entier ont besoin d'un accès en continu aux applications et aux services cloud, un nouveau défi se présente aux équipes en charge de la sécurité, qui doivent protéger leurs données et leurs applications les plus sensibles. En outre, avec l'idée préconçue selon laquelle un accès sécurisé rime avec une utilisation compliquée, les professionnels de la sécurité rencontrent des difficultés à obtenir le soutien nécessaire pour mettre en œuvre une nouvelle approche en matière d'authentification des employés.

Les entreprises axées sur le cloud ne devraient pas avoir à faire de compromis. Avec la solution adéquate, vous pouvez protéger l'accès aux applications et aux données sans interruptions, fournissant une expérience utilisateur optimale tout en maintenant les normes que vous avez établies dans votre organisation.

L'authentification et la gestion des accès traditionnels n'ont pas évolué pour s'adapter aux menaces actuelles

SafeNet Trusted Access protège l'accès à votre environnement d'applications de manière unique

L'authentification multifactorielle universelle ne couvre pas tous les cas de figure

Avec différents rôles, utilisateurs, sensibilités des applications, exigences de conformité, et bien plus encore, les stratégies d'AMF universelles impliquent une diminution de l'adoption par les utilisateurs, une trop grande complication dans certains cas de figure, ou encore des brèches.

Les employés hybrides et à distance introduisent des complexités d'accès

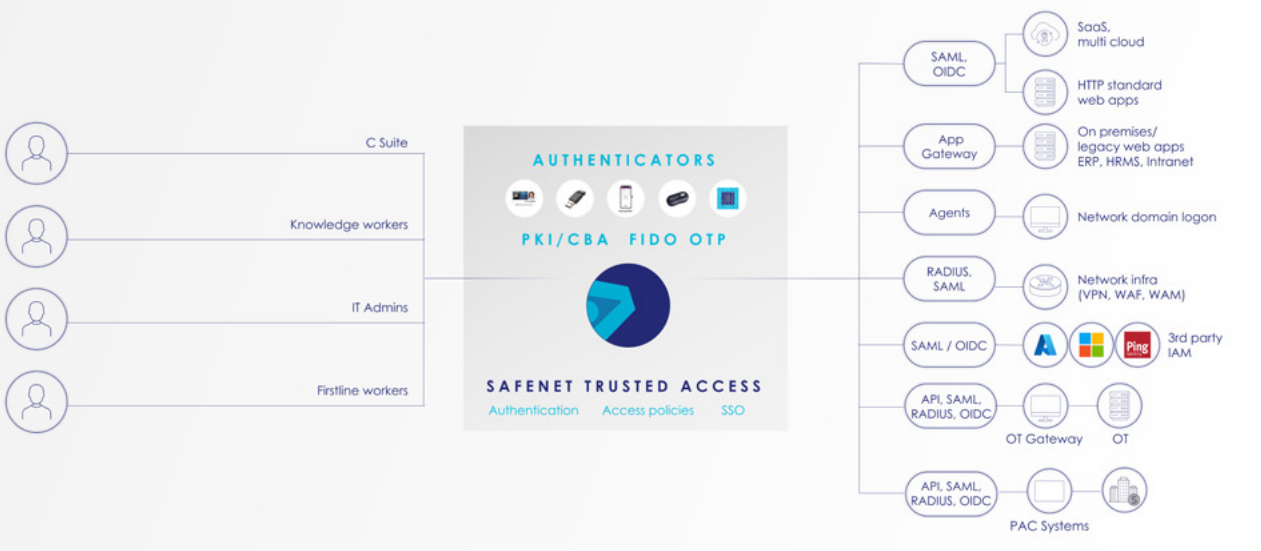
Beaucoup d'outils de gestion des accès sur site n'ont pas réussi à évoluer dans le sens des besoins modernes en matière d'autorisation des accès face à un nombre croissant d'employés hybrides et à distance.

Un contrôle accru exercé par les régulateurs chargés de la conformité

Les normes comme PCI DSS, NIS 2 et ISO 27001 nécessitent l'application de principes de moindre privilège et la mise en œuvre de stratégies d'AMF pour l'accès aux informations à caractère personnel et aux autres formes de données protégées, ce que les solutions obsolètes ne parviennent pas à faire efficacement, entraînant des amendes inévitables.

Les connexions axées sur les mots de passe sont hautement ciblées

Les pirates continuent d'utiliser leurs méthodes de vol d'identifiants de connexion ayant tant fait leurs preuves. Il leur suffit d'obtenir l'accès à un seul identifiant de connexion pour traverser plusieurs systèmes afin d'accéder à une véritable mine d'or de données inestimables.



SafeNet Trusted Access (STA) est une solution d'authentification unique (SSO), d'authentification multifactorielle (AFM) et de gestion des accès pour les applications cloud et sur site. Avec STA, vous pouvez :

Améliorer l'adoption de l'AMF avec une vaste gamme de tokens d'authentification en fonction de l'action des utilisateurs, de l'accès aux données, etc.

Automatiser les flux de travail adaptés aux besoins, comportements et caractéristiques spécifiques des différents utilisateurs

Maintenir un haut niveau de sécurité sans aucun compromis sur l'expérience utilisateur

Contrairement aux outils d'authentification et de gestion des accès basiques, STA permet aux organisations de sécuriser l'accès à leurs applications cloud et sur site en les protégeant contre les accès non autorisés, sans compromis sur l'expérience utilisateur. En tant que solution d'authentification moderne, STA favorise l'adoption de l'AMF pour tout utilisateur professionnel.

Profitez de l'avantage Thales

Une authentification unique (SSO) homogène pour l'intégralité de votre environnement d'applications

Éliminez les difficultés et la frustration associées à la gestion de plusieurs identifiants. Avec la SSO, les utilisateurs peuvent s'authentifier une fois et accéder de manière homogène à plusieurs applications, sans se soucier des mots de passe et des interruptions constantes. En outre, vous pouvez permettre une expérience d'authentification unifiée en intégrant STA au fournisseur d'identités (IdP) de votre choix.

Authentification sans mot de passe

En utilisant des méthodes avancées d'authentification résistantes à l'hameçonnage comme FIDO, Windows Hello, PKI, etc., votre organisation ne dépend plus des mots de passe extrêmement vulnérables.

Une gamme étendue de méthodes d'AMF modernes

- OTP Push sur mobiles et ordinateurs
- Appareils OTP
- Authentification basée sur un motif d'identification
- Authentification hors bande via e-mail et SMS
- Authentification contextuelle et adaptative
- FIDO 2
- Cartes à puces et identifiants PKI
- Google Authenticator
- Authentification sans mot de passe
- Biométrique
- Voix

Gradation des risques et accès conditionnel

Grâce à une configuration puissante des politiques, une gradation des risques et une évaluation des risques au niveau des points de terminaison, vous pouvez mettre en œuvre les bonnes politiques d'accès pour les bonnes applications et les bons utilisateurs, et maintenir l'intégrité de toutes les authentifications.

Rentabilité rapide et auto-inscription à l'initiative de l'utilisateur

Conçu pour fournir une utilisation optimale et fournie en tant que solution SaaS, STA permet aux organisations de configurer et déployer rapidement leurs stratégies d'accès. La fonctionnalité d'auto-inscription fournit un guide pas-à-pas pour permettre aux utilisateurs d'inscrire leurs tokens d'authentification, facilitant le travail du service informatique.

Analyses axées sur les données et intégration homogène des flux de travail

Avec des journaux d'évènements détaillés exportés automatiquement sur votre SIEM, vous pouvez bénéficier d'un contexte plus détaillé concernant les échecs de tentatives de connexion, vous permettant d'élaborer de futures politiques d'authentification.

Architecture de déploiement flexible et résiliente

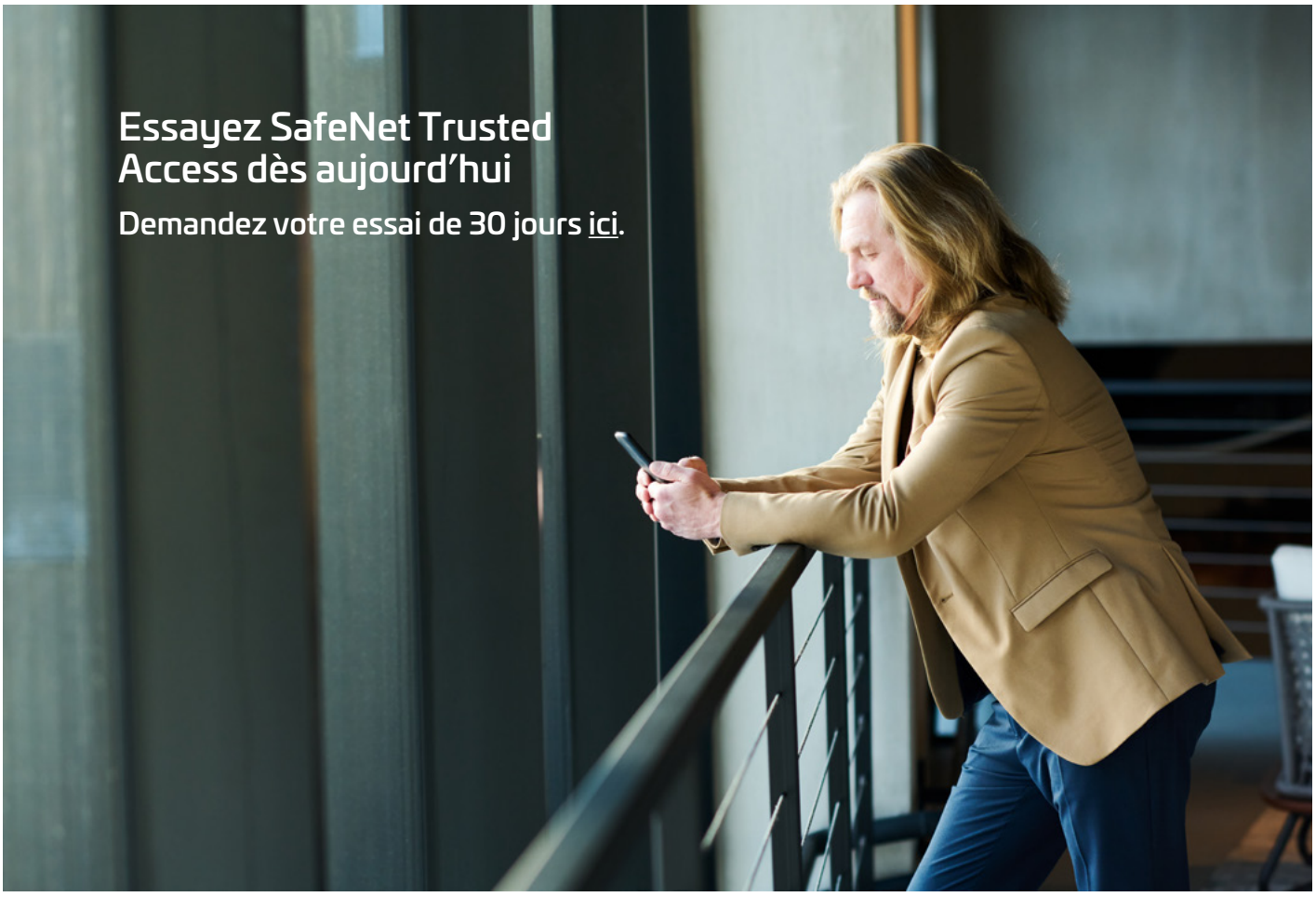
Garantissez un accès ininterrompu aux données et une continuité des activités avec Access Continuum, notre mécanisme de secours fiable, même pendant les interruptions et les pannes de service.

Prise en charge d'une vaste gamme de protocoles

- SAML
- OIDC
- WS
- Fed
- RADIUS cloud
- Agents
- API REST et SCIM
- Passerelles d'applications
- Applications héritées

À propos de Thales

En tant que leader de la cyber-sécurité, Thales sécurise les données sensibles, les identités, les applications et les logiciels pour les marques les plus dignes de confiance dans le monde entier. Grâce à un chiffrement, une gestion des accès aux identités, une sécurité des applications et des droits des logiciels avancés, Thales sécurise les environnements cloud, protège des cybermenaces, garantit la conformité et permet des expériences numériques fiables.



cpl.thalesgroup.com

Nous contacter – Pour consulter les emplacements de tous nos bureaux et nos coordonnées, veuillez vous rendre à la page cpl.thalesgroup.com/fr/contact-us