cpl.thalesgroup.com

THALES

Respecter les directives du NIST en matière de sécurité Zero Trust

Livre blanc

Table des matières

Introduction

Avec la transformation numérique, la prolifération des technologies disruptives et l'émergence de tendances telles que le télétravail, les frontières numériques des entreprises ont disparu. La disparition de ces limites rend les solutions de sécurité périmétriques traditionnelles inadaptées pour répondre aux demandes croissantes d'accès à distance.

La combinaison de ces évolutions et de l'augmentation inquiétante d'incidents de sécurité et de fuites de données a complètement anéanti le concept de confiance. Ainsi, la sécurité Zero Trust repose sur le principe suivant : « ne jamais faire confiance, toujours vérifier » . La confiance est envisagée comme une vulnérabilité. La sécurité Zero Trust nécessite une vérification d'identité stricte et continue afin de réduire les zones de confiance implicites. Le NIST a récemment publié un schéma directeur pour une sécurité Zero Trust qui explique comment construire des architectures de sécurité Zero Trust efficaces.

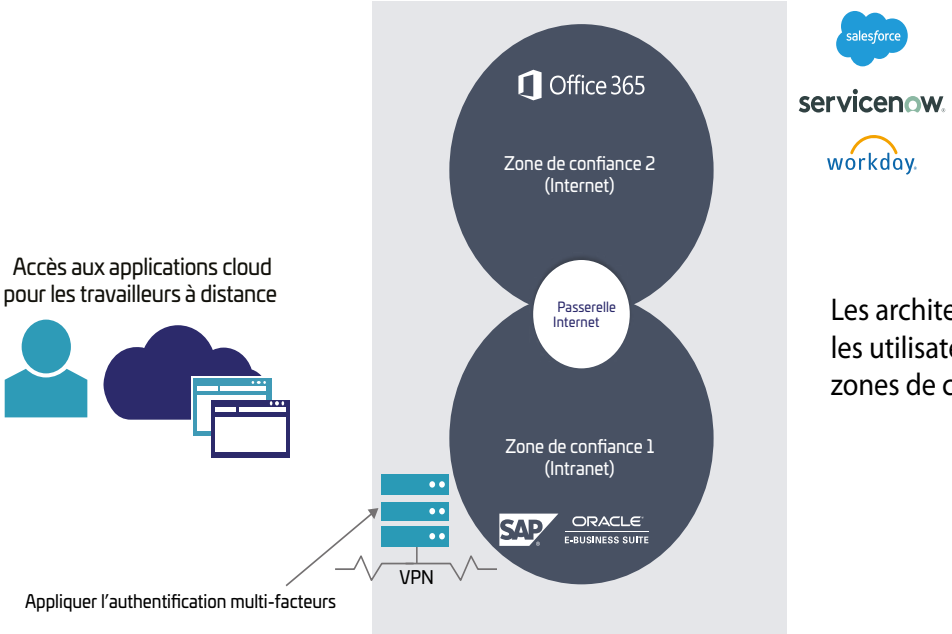
L'objectif de ce livre blanc est d'évaluer les directives du NIST en matière de sécurité Zero Trust et d'offrir des directives concrètes pour l'implémentation efficace d'une architecture Zero Trust axée sur l'identité. Le but est d'obtenir une sécurité optimale dans un environnement qui va au-delà des périmètres traditionnels.

Zero Trust : la protection au-delà du périmètre réseau

Dans les années 1980, le président américain Ronald Reagan utilisait cette formule pour décrire l'URSS : « faites confiance, mais vérifiez ». De retour dans les années 2020 avec la transformation numérique des entreprises par le biais de l'adoption et de la prolifération de technologies telles que l'IoT, l'approvisionnement de services cloud et l'utilisation de dispositifs mobiles ont entraîné la désintégration du périmètre de sécurité informatique traditionnel. Dans cet environnement où les applications sont fournies depuis le cloud vers le cloud, où les utilisateurs peuvent se trouver n'importe où, et où plusieurs appareils sont utilisés, il est impossible de reposer sur un seul point de confiance. Toutes les interactions sont intrinsèquement risquées, nécessitant une approche de vérification systématique.

Le principe et l'initiative stratégique Zero Trust aide les organisations à éviter les fuites de données et à protéger leurs actifs en refusant de faire confiance à quelque entité que ce soit. Le National Institute of Standards and Technology (NIST) définit la notion de Zero Trust comme une « collection de concepts et d'idées conçus pour réduire l'incertitude en mettant en place des décisions d'accès de moindre privilège à la demande précises dans des services et des systèmes d'informations face à un réseau considéré comme compromis. »

La notion de Zero Trust s'étend au-delà de la protection du périmètre informatique, un concept qui a dominé la sécurité traditionnelle, reconnaissant qu'en matière de sécurité, la confiance est une vulnérabilité. Les concepts de sécurité traditionnels considéraient qu'ils pouvaient faire confiance à tous les utilisateurs qui venaient d'entrer dans un réseau d'entreprise, y compris les acteurs malveillants et les hackers. La confiance leur permettait de se déplacer latéralement et d'accéder librement à ou d'exfiltrer toutes les données accessibles dans leur périmètre.



Les architectures héritées considèrent les utilisateurs comme fiables dans les zones de confiance implicites

Le Zero Trust est un modèle de sécurité qui nécessite une vérification stricte de l'identité et rapproche la décision d'authentification et d'autorisation de la ressource. La définition de la notion de Zero Trust indique qu'elle se focalise sur l'authentification, l'autorisation et la réduction des zones de confiance implicites, tout en conservant de la disponibilité et en offrant des mécanismes d'authentification transparents. Les règles d'accès sont aussi granulaires que possible pour mettre en place les accès de moindre privilège requis pour effectuer l'action nécessaire.

Pour atteindre cet objectif, la stratégie Zero Trust est gouvernée par les principes fondamentaux suivants :

- L'accès aux ressources d'entreprise est déterminé par une politique dynamique mise en place à chaque session et mise à jour en fonction des informations collectées sur l'état actuel de l'identité du client, de l'application/du service et de l'actif responsable de la demande, y compris d'autres attributs environnementaux et comportementaux.
- Toutes les communications vers les ressources doivent être authentifiées, autorisées et chiffrées
- L'authentification et l'autorisation sont indépendantes du réseau sous-jacent
- L'entreprise surveille et mesure l'intégrité et la posture de sécurité de tous les actifs détenus et associés.

Une nouvelle stratégie pour la sécurité Zero Trust ?

Dans le paysage numérique moderne où la mobilité des employés et les habitudes des clients en matière d'omniprésence nécessitent un accès à des ressources à tout moment et de n'importe où, la sécurité périmétrique traditionnelle semble inadaptée pour protéger contre les cyber-attaques sophistiquées.

L'utilisation de solutions de sécurité héritées qui reposent sur le routage sur site pour la mise en place d'une authentification et d'une autorisation sur le cloud entrave la productivité, l'évolutivité et l'expérience utilisateur, et augmente les coûts opérationnels. S'appuyer sur des solutions existantes ajoute en complexité, augmente les frais d'administration et créé de la confusion et de la frustration pour les utilisateurs.

La prolifération des technologies IoT, les plateformes de cloud multiple et les conteneurs nécessitent la création et la gestion d'un grand nombre d'identités pour leur authentification. Par conséquent, les entreprises se reposent de plus en plus sur l'utilisation d'identités et d'identifiants. Sans surprise, ces identifiants sont des cibles attrayantes pour les hackers. La corruption d'identifiants et le vol d'identité sont les causes principales des incidents de sécurité et des fuites de données.

En raison de l'augmentation de l'étendue des attaques, les réglementations telles que la RGPD, CCPA, PCI DSS et HIPAA reposent sur le principe de responsabilité et nécessitent une authentification et une autorisation robustes de toutes les communications de données et de tous les processus.

« L'utilisation de solutions de sécurité héritées qui reposent sur le routage sur site pour la mise en place d'une authentification et d'une autorisation sur le cloud entrave la productivité, l'évolutivité et l'expérience utilisateur. »

En outre, l'environnement de travail évolue à travers le monde. Les tendances de télétravail, alimentées par la pandémie de Covid-19, accélèrent l'adoption de plateformes cloud et augmentent la nécessité d'authentifier efficacement et d'octroyer l'accès aux ressources d'entreprises basé sur des décisions contextuelles, adaptatives et dynamiques, au point d'accès.

Ces développements ont conduit le NIST à normaliser les architectures Zero Trust. NIST SP 800-207, Zero Trust Architecture, sert de schéma directeur pour l'implémentation d'une architecture Zero Trust et « offre des modèles de déploiement et des cas d'utilisation généraux où la stratégie Zero Trust peut améliorer la posture de sécurité globale d'une entreprise en matière de technologie de l'information. » La sortie de cette publication contribuera à une adoption grandissante du modèle de sécurité Zero Trust.

Approches du NIST en matière d'architectures Zero Trust

Le NIST décrit trois approches de construction d'une architecture de sécurité Zero Trust efficace.

Axée sur l'identité

L'approche d'architecture Zero Trust axée sur l'identité positionne l'identité des utilisateurs, des services et des appareils au cœur de la création de politiques. Les politiques d'accès aux ressources de l'entreprise reposent sur l'identité et les attributs assignés. La première exigence pour accéder aux ressources d'entreprises est basée sur les privilèges d'accès octroyés à un utilisateur, un service ou un appareil donné. Afin d'accommoder une authentification plus adaptative, la mise en application de politique peut également prendre d'autres facteurs en considération, comme l'appareil utilisé, l'état de l'actif et les facteurs environnementaux.

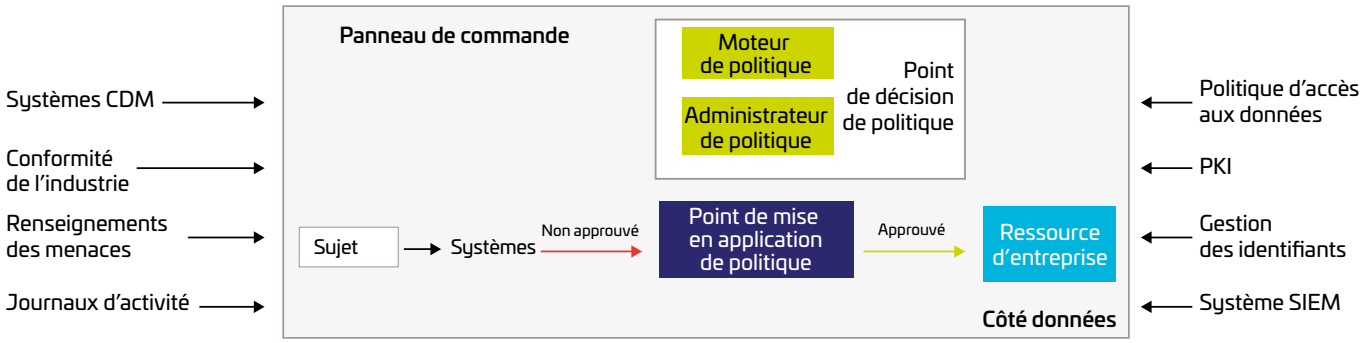


Figure 1 : Approche d'architecture Zero Trust axée sur l'identité du NIST. Source : NIST SP 800-207

Axée sur le réseau

L'approche d'architecture Zero Trust axée sur le réseau repose sur la micro-segmentation du réseau des ressources d'entreprises protégées par un composant de sécurité de passerelle. Pour mettre en place cette approche, l'entreprise doit utiliser des appareils d'infrastructure tels que les commutateurs intelligents (ou routeurs), des pare-feux nouvelle génération ou des réseaux SDN (Software-Defined Network) pour servir à la mise en place de politique de protection de chaque ressource ou groupe de ressources associées.

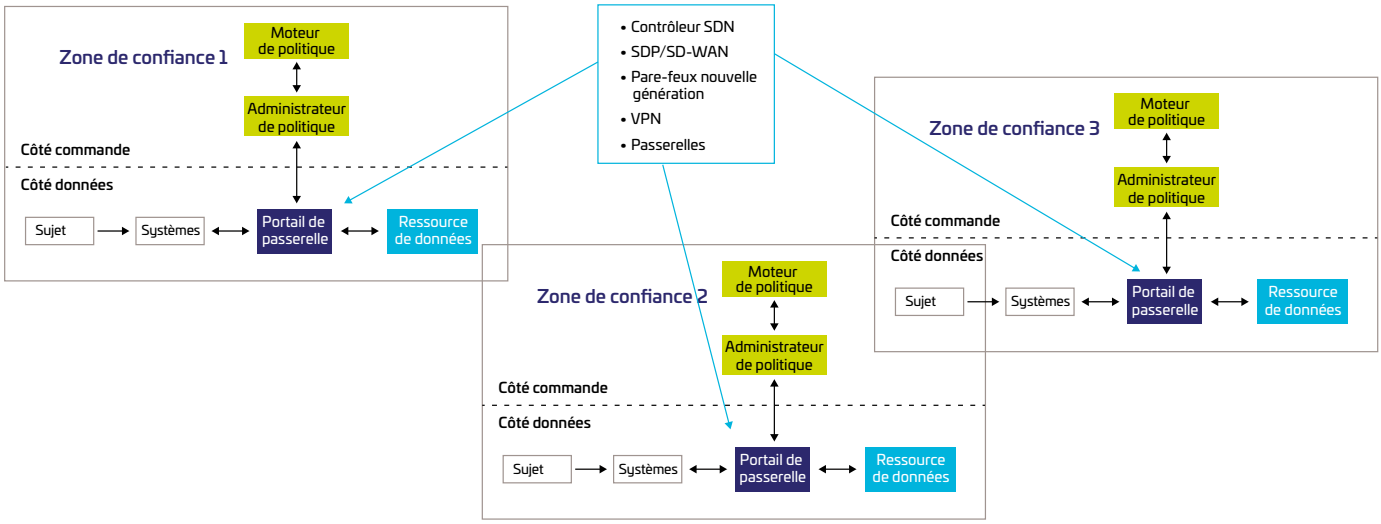


Figure 2 : Approche d'architecture Zero Trust axée sur le réseau du NIST. Adapté de NIST SP 800-207.

Une approche axée sur le réseau se focalise sur la segmentation du périmètre traditionnel en sous-zones. Les utilisateurs sont considérés comme fiables dès qu'ils accèdent à une zone. Tout en réduisant le risque jusqu'à un certain point, l'approche axée sur le réseau n'est pas entièrement sécurisée car elle considère qu'une entité est fiable dès qu'elle intègre la zone. Pour cette raison, cette approche nécessite des mesures de sécurité supplémentaires et une gouvernance des identités robuste.

Axée sur l'identité	Axée sur le réseau
Reposer sur un modèle de confiance d'identité robuste permet une adoption rapide des nouvelles technologies.	Difficile à configurer, à dépanner et à gérer en raison de sa multitude de zones de sécurité réseau.
La confiance d'identité est un modèle d'auto-renforcement : plus vous évaluez/contrôlez les identités sur les systèmes, plus vous gagnez en connaissances et plus la confiance se renforce.	Unique point de vulnérabilité : une fois que les utilisateurs sont dans la zone, ils peuvent naviguer librement avec un contrôle et une visibilité limités sur leurs actions.
L'évaluation de la confiance d'identité devient facilement omniprésente et peut être utilisée par les nouveaux services pour prendre des décisions de sécurité simples.	Peut ne pas être en mesure de prendre en charge les applications cloud dans une zone de confiance.
	Bien qu'il soit considéré comme mauvaise pratique de laisser des personnes externes entrer dans ces zones (des sous-traitants, par exemple), ce n'est pas facile à empêcher.

Tableau 1 : Comparaison des approches Zero Trust axées sur l'identité et sur le réseau

Combinaison basée sur le cloud

Une approche d'architecture Zero Trust combinée basée sur le cloud optimise la gestion des accès basée sur le cloud et le modèle SASE (Secure Access Service Edge). La solution de gestion des accès basée sur le cloud protège et exécute les identités des applications et des services cloud, tandis que les composants SASE, tels que les réseaux SDN ou les pare-feux nouvelle génération, protègent les ressources sur site et surveillent le trafic réseau.

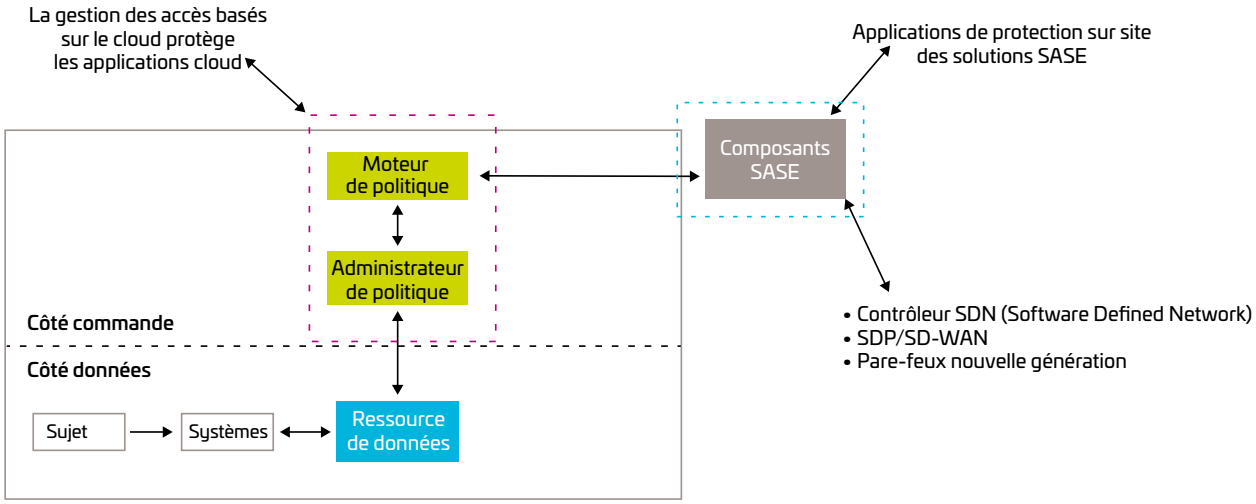


Figure 3 : Approche d'architecture Zero Trust combinée basée sur le cloud.

Implémentation d'une sécurité Zero Trust avec SafeNet Trusted Access de Thales

Le périmètre de sécurité d'entreprise moderne n'est plus constitué d'un emplacement physique ; il s'agit d'un ensemble de points d'accès séparés dans le cloud et fournis depuis le cloud. Les identités sont désormais le nouveau périmètre et doivent être au centre des décisions d'accès. L'identité de toute ressource, de tout utilisateur, de tout appareil ou de tout service fournit le contexte clé pour l'application des politiques d'accès.

L'identité est au centre de la sécurité Zero Trust pour les actifs de l'application et des données qu'une entreprise a pour but ultime de protéger. Le plus grand défi est d'employer une solution de sécurité Zero Trust complète qui couvre les identités et les données de bout en bout. Avec sa gestion des accès basée sur le cloud et ses solutions d'authentification, Thales répond aux besoins holistiques critiques des entreprises en matière de sécurité Zero Trust.

SafeNet Trusted Access est le point de départ pour des implémentations de sécurité Zero Trust efficaces, respectant les principes Zero Trust :

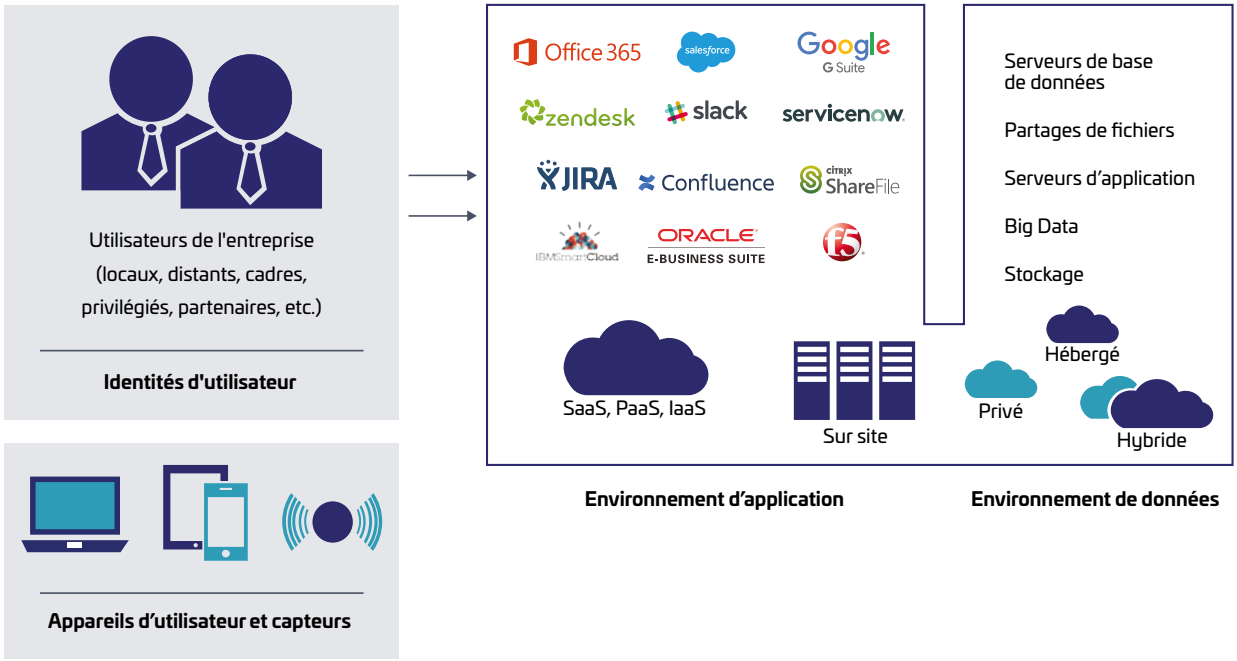
- Les décisions d'accès sont mises en application de manière dynamique au point d'accès de l'application, indépendamment de l'emplacement où l'application réside, de la localisation des utilisateurs, de l'appareil utilisé et du routage réseau
- Les décisions d'accès sont facilitées par les renseignements mis à jour des technologies de fournisseurs de sécurité de réseau tiers, notamment les VPN (Virtual Private Network), WAM (Web Access Management), WAF (Web Application Firewall), SASE (Secure Access Service Edge), etc.
- Les décisions d'accès suivant la logique de « refus automatique » sont réévaluées en permanence, même si les fonctionnalités SSO (Single Sign On) sont activées.

Avantages de l'utilisation de SafeNet Trusted Access de Thales pour l'implémentation d'une sécurité Zero Trust

Il existe plusieurs avantages à l'utilisation de SafeNet Trusted Access pour l'implémentation d'une architecture Zero Trust axée sur l'identité :

Approche logique sur le plan architectural

Les solutions périmétrique existantes contrôlent le trafic par le biais d'un hub central et sur site qui n'est pas efficace pour le trafic généré ou acheminé vers le cloud et est susceptible de créer un goulot d'étranglement et une défaillance d'un point d'accès unique. La solution SafeNet Trusted Access a été pensée pour le cloud et réside dans le cloud. Ainsi, elle ne dépend pas de l'infrastructure sur site et peut contrôler l'accès dans le cloud, évitant les goulots d'étranglement. En outre, puisque toutes les décisions d'authentification et d'accès sont mises en application continuellement à tous les points d'accès, SafeNet Trusted Access assure une sécurité sur tous les environnements réseaux dispersés, permettant l'implémentation des approches Zero Trust.



Flexible et agile

L'une des forces principales de SafeNet Trusted Access est son moteur de politique, qui permet la définition de politiques d'accès extrêmement flexibles. Les politiques de sécurité favorisent la création de règles à haut niveau de granularité et de spécificité afin de réévaluer les utilisateurs en permanence pendant une session ouverte, plutôt que pour certains événements uniquement, tels que les périodes d'indisponibilité de l'authentification. Si le niveau de risque change, SafeNet Trusted Access force l'utilisateur à s'authentifier à nouveau ou à établir une forme d'authentification plus robuste. Les politiques peuvent être définies à chaque application, s'appliquer à des plages réseau, des systèmes d'exploitation, ainsi que des collections utilisateur et des géolocalisations. Les règles d'authentification peuvent être établies comme dynamiques et adaptées au contexte en fonction du besoin, s'adaptant aux changements dans un environnement cloud dynamique.

Facilité de déploiement, de gestion et d'évolutivité

SafeNet Trusted Access offre une manière simple et évolutive de faciliter le télétravail ou le travail à distance, de n'importe où. Tandis que les solutions SASE évoluent en permanence et les solutions héritées ne sont pas adaptées pour répondre aux besoins modernes de sécurité Zero Trust, la plateforme SafeNet Trusted Access est facilement accessible, établie et certifiée. L'architecture Zero Trust axée sur l'identité étant utilisée par toutes les technologies et tous les services, SafeNet Trusted Access offre une solution évolutive et adaptative afin de protéger les ressources d'entreprises où qu'elles se trouvent.

Expérience utilisateur fluide et familière

La possibilité de s'intégrer avec fluidité à une vaste gamme d'applications et de services est essentielle pour garantir un cadre d'accès normalisé et unifié, ainsi qu'une expérience d'authentification cohérente pour les utilisateurs finaux. SafeNet Trusted Access offre un accès d'application cohérent sur tous les cas de figure de connexion et applique des routes réseau unifiées pour toutes les applications, qu'elles soient basées sur le cloud ou protégées derrière un VPN ou des proxys. Enfin, pour gérer les exigences en constante augmentation associées au télétravail, SafeNet Trusted Access peut activer des modèles BYOD sans compromis sur la sécurité.

Conclusion

Dans le concept de protection de périmètre réseau traditionnel, les acteurs malveillants étaient considérés comme fiables une fois qu'ils avaient pénétré les réseaux d'entreprise : ils étaient alors libres de naviguer sans encombre. Les concepts de sécurité Zero Trust permettent aux organisations de se développer dans le cloud en toute sécurité et de s'adapter aux environnements sans frontières et dispersés. SafeNet Trusted Access répond à ces besoins en garantissant de suivre la logique « ne jamais faire confiance, vérifier constamment » de par sa capacité à protéger les applications et les services en continu au point d'accès, indépendamment du réseau sous-jacent déployé, de l'emplacement de l'application ou de l'utilisateur, ou encore de l'appareil utilisé.

À propos de Thales

Les personnes à qui vous faites confiance pour protéger votre vie privée font confiance à Thales pour protéger leurs données. En matière de sécurité des données, les entreprises sont confrontées à un nombre croissant de moments décisifs. Qu'il s'agisse de mettre en place une stratégie de chiffrement, de passer au cloud ou de respecter les obligations de conformité, vous pouvez compter sur Thales pour sécuriser votre transformation numérique.

Une technologie décisive pour des moments décisifs.

THALES

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

> cpl.thalesgroup.com/fr <