
E-BOOK

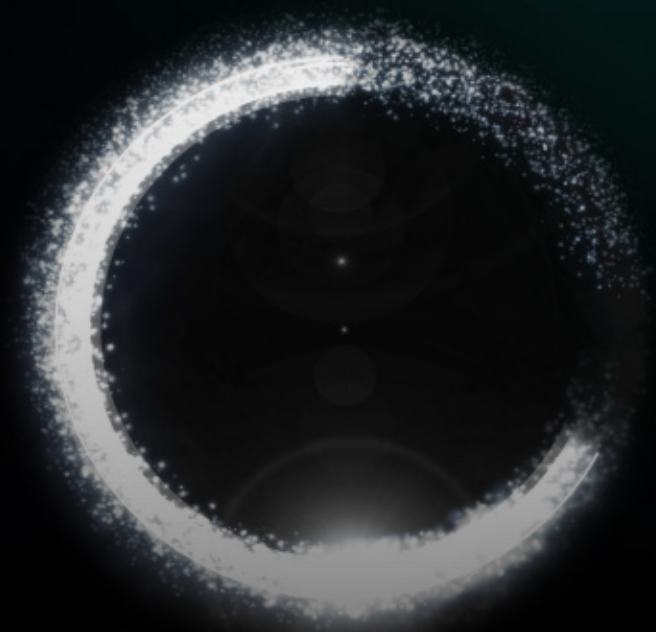
Les trois clés de la transformation Zero Trust : **plateforme, personnes et processus**

INTRODUCTION

Le parcours vers Zero Trust

La transformation digitale a fondamentalement changé le mode de fonctionnement des entreprises modernes. Vos **employés sont aujourd'hui plus souvent sur Internet que sur le réseau d'entreprise**, accédant de partout aux applications et aux données. Les données sensibles de l'entreprise sont devenues plus distribuées, résidant en dehors du périmètre de l'entreprise dans des applications SaaS, telles que Microsoft 365, et les applications privées dans AWS, Azure et Google Cloud Platform.

Le processus de transformation digitale améliore l'agilité de l'entreprise ainsi que la circulation d'informations, mais aussi étend considérablement la surface d'attaque et expose votre entreprise à de nouvelles menaces. Les architectures de sécurité traditionnelles, qui se focalisaient sur la protection du réseau, ne sont plus efficaces dans le contexte actuel. Pour protéger votre entreprise et conserver les avantages de **la transformation digitale, il faut migrer vers un modèle de sécurité Zero Trust fourni par le cloud**, plus à proximité de vos utilisateurs et de vos actifs commerciaux.



DÉFINITION

Zero Trust : Lumière sur le concept

Le concept de Zero Trust existe depuis plus d'une décennie, mais il y a eu tellement de confusion sur la signification réelle du terme. Il ne s'agit pas d'une simple technologie.

Zero Trust est une approche holistique de la sécurisation des entreprises modernes, avec pour assise l'accès basé sur le moindre privilège et le principe selon lequel **aucun utilisateur ou application ne devrait de but en blanc être considéré comme fiable**. Elle part de l'idée que tout est préjudiciable et **établit la confiance uniquement en fonction de l'identité de l'utilisateur et du contexte**, avec une politique servant de filtre à chaque étape du processus.

DÉFINITION

Zero Trust dans la pratique

Zero Trust s'attaque aux défis les plus colossaux de l'heure en matière de sécurité, de mise en réseau et de mise en œuvre de l'espace moderne de travail :

SÉCURITÉ

Contrecarrer les cybermenaces :

Zero Trust offre une protection contre les cybermenaces — non seulement pour les utilisateurs, mais aussi pour les charges de travail du cloud, les serveurs et même les applications SaaS.

Empêcher la perte de données :

Zero Trust fournit une approche holistique pour garantir que les données ne peuvent ni être divulguées ni égarées, que ce soit accidentellement ou intentionnellement par les utilisateurs, ou à partir des charges de travail du cloud.

RÉSEAU

Simplifier la connectivité des utilisateurs et des filiales :

Zero Trust permet aux entreprises de transformer les réseaux obsolètes en étoile, permettant ainsi aux filiales et aux utilisateurs à distance de se connecter en toute sécurité vers n'importe quelle destination directement sur Internet, peu importe le lieu de connexion de l'utilisateur.

Connectivité cloud sécurisée :

Plutôt que d'étendre les traditionnels VPN site à site au cloud, avec le risque de mouvements latéraux que cela comporte, Zero Trust permet aux charges de travail de se connecter en toute sécurité les unes aux autres.

MISE EN ŒUVRE D'UN WORKPLACE MODERNE

Sécuriser le télétravail :

Une solution Zero Trust digne de ce nom devrait permettre à vos employés de travailler en toute sécurité et en toute transparence de n'importe où, sans avoir à se soucier du réseau ou de savoir s'ils doivent activer ou non un VPN.

Optimiser l'expérience utilisateur :

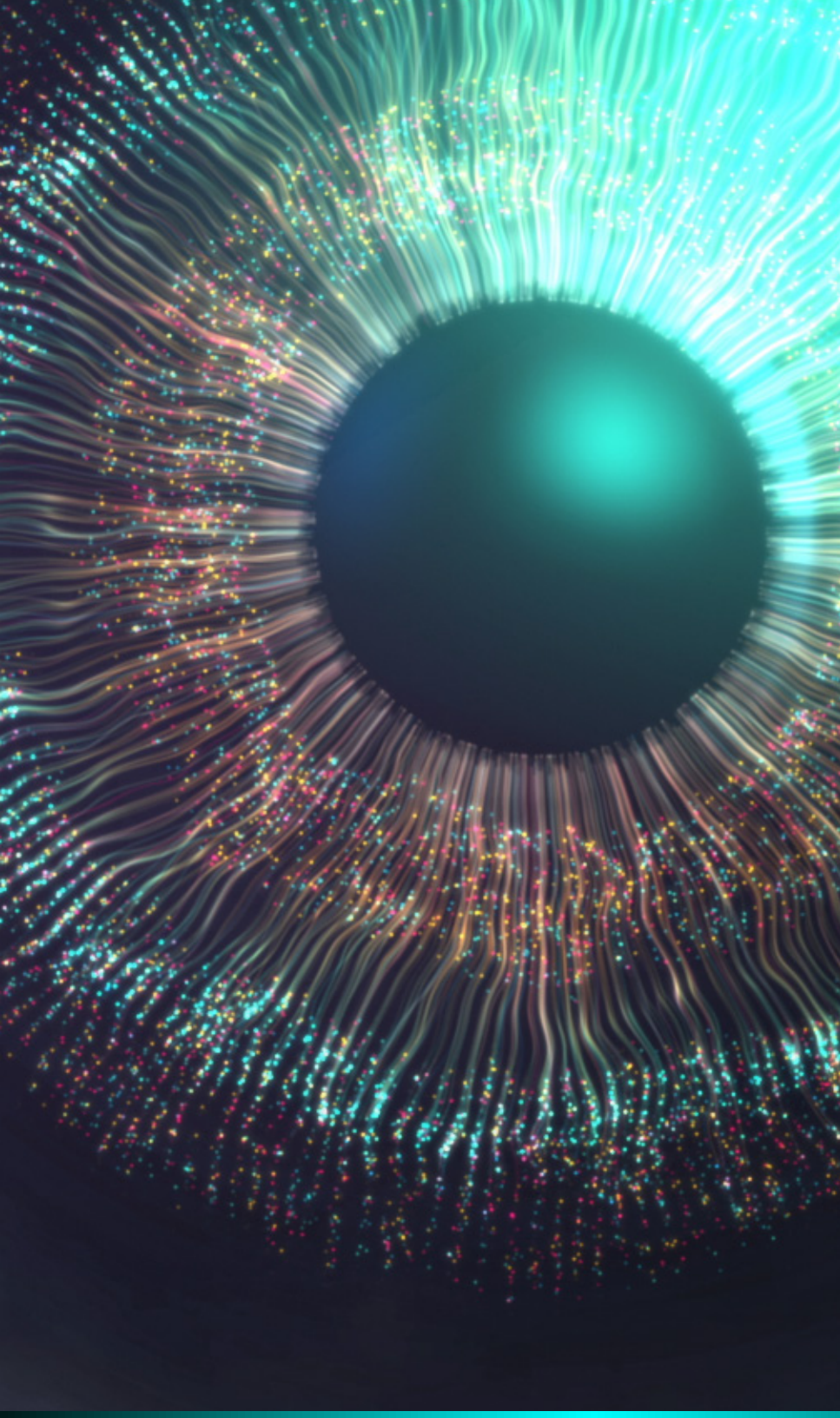
En s'assurant que vous maîtrisez l'expérience de chaque employé pour chaque application, Zero Trust permet aux entreprises d'offrir systématiquement une excellente expérience utilisateur.



Préparer une stratégie Zero Trust réussie

Alors qu'Internet devient votre nouveau réseau d'entreprise, Zero Trust vous permet d'accéder **rapidement, en toute transparence et en toute sécurité** à l'ensemble de votre écosystème d'entreprise.

Mais la mise en œuvre d'un modèle de sécurité Zero Trust n'est pas juste une fonction du service informatique — elle affecte tous les domaines de votre entreprise, et va au-delà des limites traditionnelles de celle-ci. Réussir la mise en œuvre de Zero Trust exige une stratégie détaillée qui aborde les défis et les opportunités relatives aux **personnes, aux processus et aux plateformes technologiques**. →



LES BASES DE ZERO TRUST

Plateforme

Zero Trust ne se résume pas à une simple technologie comme l'identité ou la segmentation d'application. Zero Trust est une stratégie, **une fondation sur laquelle vous pouvez construire votre écosystème de sécurité.** Elle connecte en toute sécurité les utilisateurs aux applications à l'aide de politiques commerciales sur Internet. L'essence du concept repose sur une plateforme technologique Zero Trust guidée par trois principes clés :

- ① Connectivité basée sur **l'identité et la politique d'accès**
- ② Rendre les **applications invisibles**
- ③ **Architecture basée sur le proxy** pour se connecter aux applications et inspecter le trafic

LES BASES DE ZERO TRUST

Plateforme

1 Connectivité basée sur l'identité et le contexte

Les VPN et pare-feux traditionnels mettent les utilisateurs sur le réseau pour qu'ils accèdent aux applications. Une fois sur celui-ci, la confiance étendue accordée à l'utilisateur augmente le risque de mouvement latéral par des menaces ou de potentiels hackers. À l'inverse, Zero Trust utilise l'identité et les politiques basées sur le contexte pour connecter à une application spécifique autorisée et en toute sécurité les utilisateurs authentifiés, sur la base de politiques d'accès et de sécurité granulaires, et ceci sans jamais placer les utilisateurs sur le réseau d'entreprise. Limiter les accès permet de contrer le mouvement latéral et réduit les risques. Et comme aucune ressource du réseau ne devrait être exposée à Internet, vous pouvez vous protéger contre les attaques DDoS et les attaques ciblées.

2 Rendre les applications invisibles

La migration des applications vers le cloud élargit considérablement la surface d'attaque. Les pare-feux traditionnels exposent vos applications sur Internet, ce qui les rend facilement accessibles aux utilisateurs ainsi qu'aux hackers. Une approche Zero Trust, en dissimulant les identités de source et en masquant les adresses IP, devrait éviter d'exposer sur Internet le réseau d'entreprise. En rendant les applications invisibles pour les adversaires et exclusivement accessibles aux utilisateurs autorisés, la surface d'attaque se trouve réduite, et l'accès aux applications — sur Internet, SaaS, ou dans des clouds publics ou privés — est en permanence sécurisé.

3 Architecture basée sur le proxy pour se connecter aux applications et inspecter le trafic

Les pare-feux de nouvelle génération ont du mal à inspecter le trafic chiffré. Par conséquent, les entreprises contournent souvent l'inspection du trafic chiffré, ce qui augmente le risque de cybermenaces et de perte de données. De plus, les pare-feux utilisent une approche de type « passthrough », qui permet au contenu inconnu d'atteindre sa destination avant toute analyse. Si une menace est détectée, une alerte est envoyée, mais elle peut arriver trop tard. Par contre, une protection efficace contre les menaces et une prévention complète des pertes de données nécessitent une architecture proxy conçue pour inspecter les sessions SSL, analyser le contenu des transactions et prendre en temps réel des décisions de politique et de sécurité avant de laisser le trafic atteindre sa destination. Tout cela doit en plus se faire à l'échelle — sans affecter les performances, quel que soit l'endroit où vos utilisateurs se connectent.



UN CHANGEMENT CULTUREL

Vos Équipes

La bonne plateforme est le point de départ de la réussite dans l'adoption de Zero Trust, mais ce succès dépend aussi **du développement de nouvelles compétences par l'entreprise ainsi que de l'adoption d'un nouvel état d'esprit culturel**. Responsables informatiques confrontés à la nécessité de transformer rapidement et en toute sécurité, praticiens sur le terrain qui mettent en oeuvre Zero Trust, utilisateurs finaux: tout l'écosystème doit être impliqué pour garantir le succès.

UN CHANGEMENT CULTUREL

Vos Équipes

Décideurs IT

En tant que décideur, vous devez être à la fois un innovateur et un stratège. Votre transition vers Zero Trust exige que vous aligniez les priorités commerciales et informatiques, que vous supprimiez les silos et que vous appliquiez les technologies et l'architecture appropriées pour piloter la transformation et obtenir les résultats souhaités pour votre entreprise. Pendant la transition vers Zero Trust, vous aurez besoin de :

- **Comprendre les meilleures pratiques et stratégies** de transformation de vos pairs et organiser l'entreprise pour mettre en œuvre ces changements
- **Aider vos professionnels de l'informatique à développer les compétences et les connaissances** nécessaires pour réussir la migration d'une architecture centrée sur le réseau vers une architecture Zero Trust
- Rendre Zero Trust **invisible pour vos utilisateurs finaux**



Action recommandée :

Contactez des innovateurs aux vues similaires quant aux meilleures pratiques concernant Zero Trust et la transformation digitale dans un forum tel que [Zero Trust REvolutionaries](#) 

UN CHANGEMENT CULTUREL

Vos Équipes

Experts IT

Vos équipes informatiques sont expertes en matière de mise en réseau et de sécurité, habituées à travailler sur du hardware et à définir des politiques basées sur 30 ans de principes de sécurité informatique et de mise en réseau. La migration vers Zero Trust **aura un impact direct sur vos équipes informatiques**. De nombreuses compétences sur lesquelles ils se sont appuyés par le passé devront être mises à jour, et ils devront développer de nouvelles aptitudes pour la transformation digitale ; mais comme résultat, ils auront un impact bien plus grand sur l'entreprise et un champ de connaissances plus précieux et futuriste.

Le succès repose sur la fourniture d'une **formation de pointe pour assurer la transition de vos équipes** en veillant à ce qu'elles adoptent les nouveaux processus commerciaux ainsi que les meilleures pratiques et procédures d'utilisation des services Zero Trust. En même temps, il vous sera facile de démontrer comment Zero Trust leur fera **gagner du temps** et leur permettra d'**apporter plus de valeur** à l'entreprise.



Action recommandée :

Aidez vos équipes à se familiariser avec Zero Trust grâce à un programme de formation certifié, la **Zscaler™ Zero Trust Academy** [🔗](#)

UN CHANGEMENT CULTUREL

Vos Équipes

Vos utilisateurs

S'il est appliqué correctement, le modèle Zero Trust est un catalyseur invisible pour vos utilisateurs finaux, permettant aux employés de travailler de n'importe où et sur n'importe quel appareil. Comme l'accès avec Zero Trust est toujours basé sur l'identité et les politiques d'entreprise et que le service cloud connecte automatiquement les utilisateurs aux applications via le chemin d'accès le plus rapide, l'emplacement géographique de l'utilisateur n'a plus d'importance.

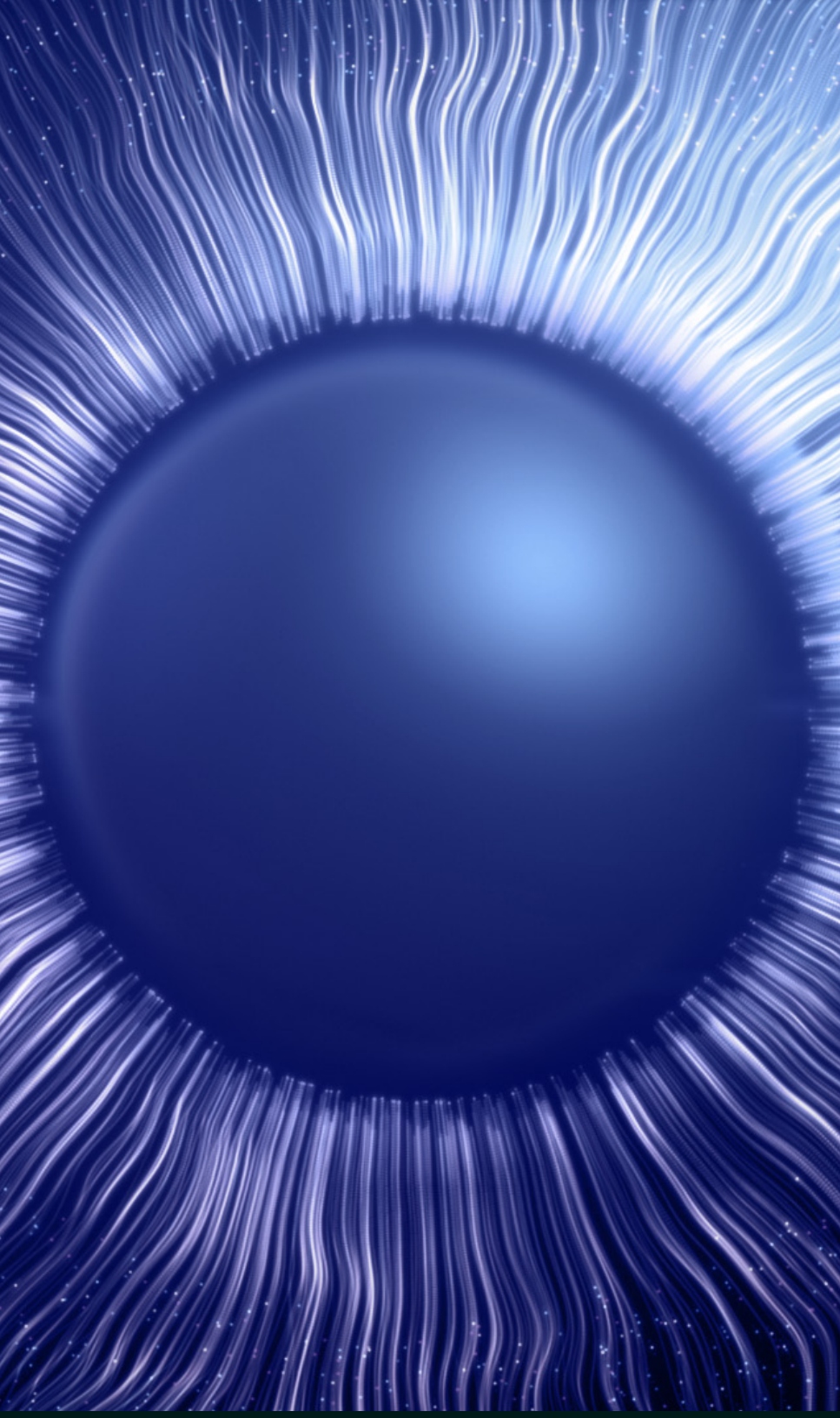
Un utilisateur travaillant au bureau bénéficie de la **même expérience d'accès rapide et cohérente** que lorsqu'il travaille à domicile, ou n'importe où d'ailleurs.

Dans le même temps, une robuste solution Zero Trust permet aux entreprises de **réduire considérablement les risques sans bloquer l'accès des utilisateurs** aux applications. Par exemple, la technologie d'isolation du navigateur dans le cloud peut fournir un accès sécurisé au contenu actif en fournissant des pages Web sous forme de pixels rendus dans un environnement isolé, sans impact sur l'expérience utilisateur. Elle peut également être exploitée pour limiter la possibilité de copier et de coller des données, empêcher le téléchargement de fichiers ou confiner les téléchargements au conteneur d'isolation afin de protéger les appareils endpoints contre les ransomwares et autres menaces sophistiquées. De cette façon, Zero Trust exploite la technologie pour limiter le risque en fonction du contexte.



Action recommandée :

Tirez profit des architectures Zero Trust qui comprennent des outils garantissant à vos utilisateurs une excellente expérience, tels que **Zscaler Digital Experience** 



UN PARCOURS PROGRAMMATIQUE

Processus

Quelles sont les étapes pour adopter Zero Trust et comment accélérer la transformation de votre entreprise ? Savoir par où commencer peut sembler l'aspect le plus compliqué de ce parcours, mais ce ne devrait pas être le cas. Zero Trust commence par une plateforme et doit s'étendre jusqu'à **inclure les données, les personnes, les appareils et les charges de travail.**

À ce titre, les intégrations de produits robustes avec votre fournisseur d'identité, votre solution de sécurité endpoints et votre solution SIEM sont des éléments essentiels du puzzle Zero Trust pour ajouter un contexte supplémentaire et simplifier l'adoption.

Processus

Compte tenu du besoin d'intégration, nous recommandons une **plateforme Zero Trust et un écosystème de partenaires technologiques** qui fournissent les outils suivants pour éclairer votre conception et vous permettre d'adopter Zero Trust :

- **Des plans de solutions** qui fournissent des architectures de référence de cas d'utilisation
- **Des guides de conception** qui partagent les principes de conception et les meilleures pratiques d'intégration
- **Des guides de déploiement** qui fournissent des conseils de configuration lorsque vous activez les intégrations pour le déploiement de démonstration de valeur (PoV) et de production

La mise en œuvre d'une solution holistique Zero Trust devient beaucoup plus facile avec les bons partenaires.

Recherchez des fournisseurs avec des architectures de référence validées conjointement et conçues pour répondre à un ensemble spécifique de cas d'utilisation, ainsi que des conseils de conception prescriptifs pour les architectes de sécurité sur l'utilisation de ces plateformes sur la base des meilleures pratiques.

Ces conseils fournissent un cadre plus structuré qui simplifie le déploiement, garantit des opérations efficaces et la meilleure expérience utilisateur, tout en favorisant l'application d'une sécurité optimale. Tout cela vous permettra d'accélérer l'adoption de Zero Trust au sein de votre entreprise.

Zero Trust commence maintenant

La transformation digitale rend les entreprises plus agiles et plus efficaces — mais elle vous oblige à repenser vos architectures réseau et de sécurité. Zero Trust fournit **aux entreprises axées sur le cloud le socle pour accélérer la transformation digitale** et permettre aux employés de travailler de manière productive, sécurisée et de n'importe où. Alors que vous envisagez votre transition, le développement d'une stratégie qui intègre la bonne plateforme, les bonnes personnes et les bons processus vous garantira à coup sûr le succès.

Sélectionnez une plateforme qui utilise l'identité et les politiques d'accès pour établir la confiance, et qui connecte les utilisateurs aux ressources sans les placer sur le réseau d'entreprise. Protégez les applications en les rendant invisibles aux adversaires, mais accessibles aux utilisateurs autorisés. Puis utilisez une architecture proxy et non un pare-feu de type passthrough pour sécuriser vos données et garantir une protection efficace contre la cybermenace.

Mettez à contribution vos pairs pour établir les meilleures pratiques et stratégies de transformation. Alignez votre entreprise sur l'adoption d'un nouveau schéma de pensée culturel et développez les compétences nécessaires à la mise en œuvre et à la gestion d'une architecture Zero Trust, tout en vous assurant que Zero Trust est invisible et transparent pour vos utilisateurs finaux. Le bon plan rend tout cela encore plus facile. Tirez profit d'**une plateforme Zero Trust avec de robustes intégrations de partenaires qui fournissent des architectures de référence validées conjointement et des conseils de conception prescriptifs** pour utiliser ces plateformes ensemble.

Ces éléments vous aideront à **embrasser Zero Trust, accélérer votre transformation digitale et faire du service informatique un véritable atout commercial.**

Découvrez les innombrables avantages d'**une véritable plateforme Zero Trust.**

Commencez votre transition 

