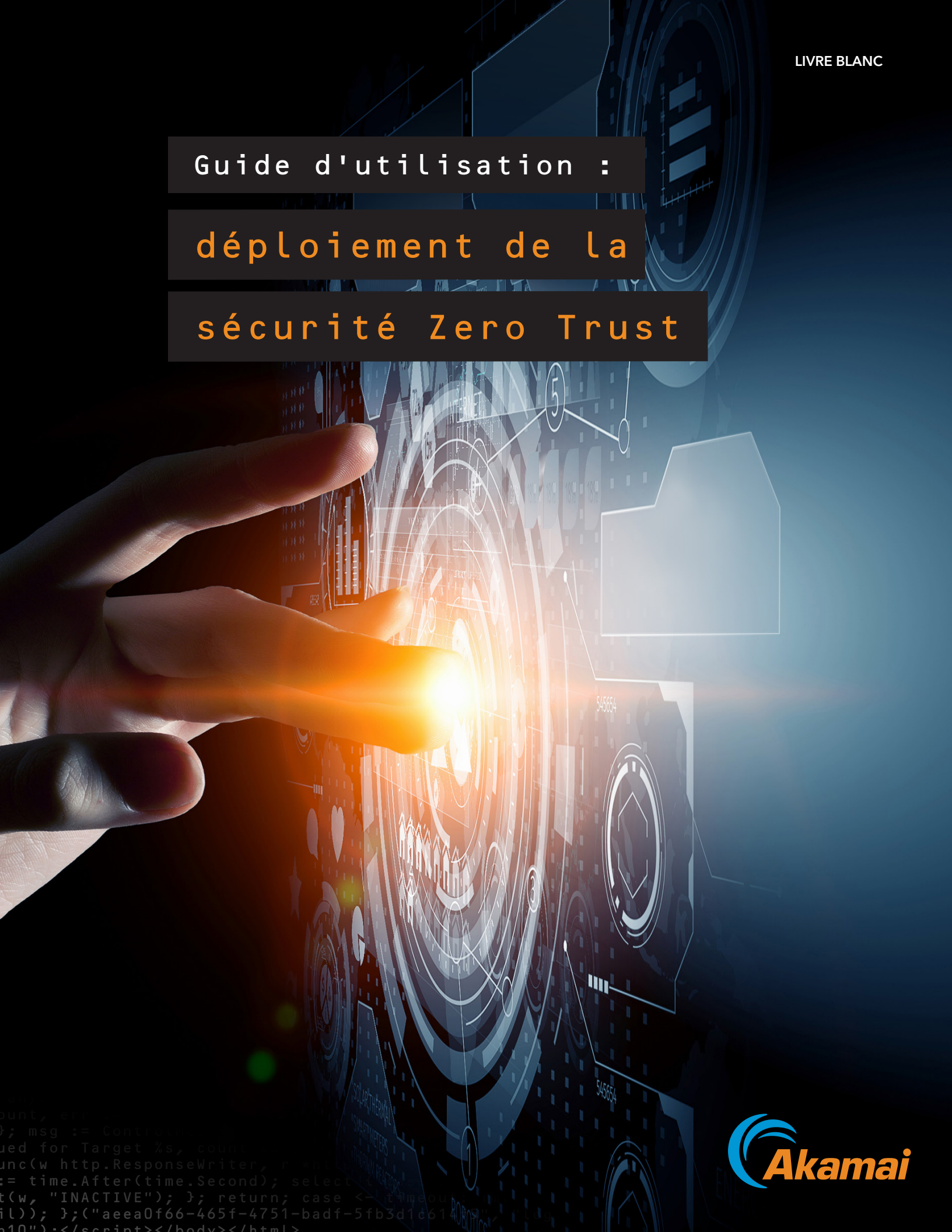
LIVRE BLANC

# Guide d'utilisation : déploiement de la sécurité Zero Trust



Akamai

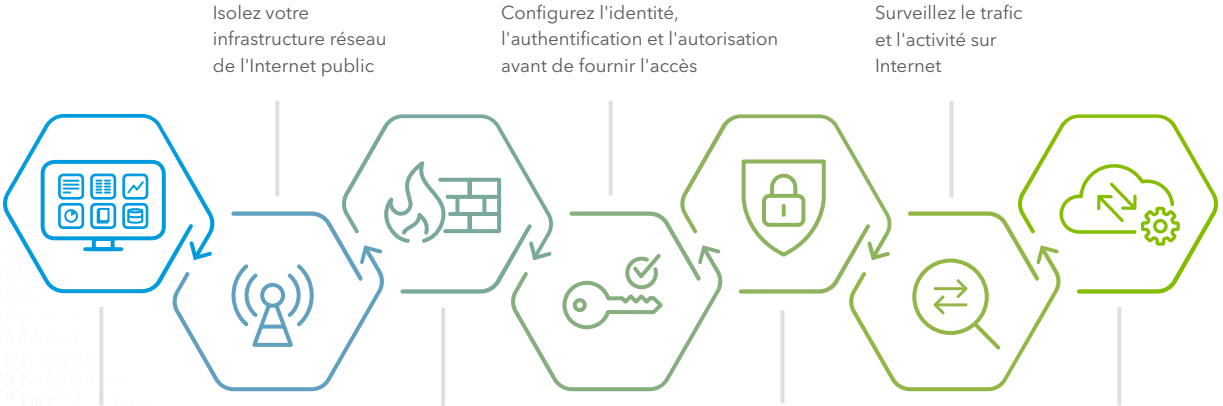
## Résumé

Dans le contexte actuel des entreprises, nous ne pouvons pas nous fier à la notion de périmètre réseau, où tout le monde en dehors de la sphère de contrôle de l'entreprise est malveillant et où tout le monde à l'intérieur est honnête et bien intentionné. L'adoption étendue des applications SaaS, la migration vers des architectures basées sur le cloud, un nombre croissant d'utilisateurs distants et l'afflux de terminaux BYOD rendent obsolète une sécurité basée sur le périmètre. De plus, une défense centrée sur le périmètre nécessite une gestion des stratégies de sécurité et des appliances, ainsi que des mises à niveau logicielles fréquentes, ce qui entraîne une complexité opérationnelle et accapare les équipes informatiques déjà débordées. Alors que la surface d'attaque s'étend et que les ressources informatiques limitées peinent à gérer une architecture réseau toujours plus complexe, les cybercriminels sont de plus en plus compétents, sophistiqués et motivés pour échapper aux mesures de sécurité. Il faut donc établir un cadre stratégique de sécurité qui réponde à ces défis spécifiques.

## Qu'est-ce que la sécurité Zero Trust et pourquoi est-ce important ?

Un modèle Zero Trust remplace l'architecture de sécurité axée sur le périmètre. Il garantit que les décisions relatives à la sécurité et aux accès sont appliquées de manière dynamique en fonction de l'identité, du terminal et du contexte utilisateur. Un cadre de sécurité Zero Trust impose également que seuls les utilisateurs et les terminaux authentifiés et autorisés puissent accéder aux applications et aux données. En même temps, il protège ces applications et ces utilisateurs contre les menaces avancées sur l'Internet.

Pour progresser dans votre parcours Zero Trust, et garantir ainsi la protection des utilisateurs, des applications et de l'avenir de votre entreprise, nous vous proposons des solutions :



# Fournissez aux utilisateurs un accès aux applications uniquement et non au réseau

Les technologies d'accès à distance existantes, telles que les réseaux privés virtuels (VPN), ne sont pas en mesure de répondre aux exigences croissantes des entreprises digitales sans périmètre d'aujourd'hui. Le VPN traditionnel représente une menace pour la sécurité de l'entreprise car il crée une brèche dans le pare-feu, offrant ainsi un accès au réseau sans entraves. Une fois qu'un pirate est entré, il peut se déplacer latéralement pour accéder à tout système ou application du réseau et l'exploiter. Non seulement les VPN traditionnels exposent l'entreprise à des risques de sécurité, mais ce sont aussi des solutions complexes qui nécessitent des ressources informatiques importantes pour la gestion du matériel et des logiciels, et dont la maintenance et la mise à jour sont coûteuses.

La segmentation du réseau, parfois considérée comme une contre-mesure à un accès généralisé des utilisateurs, s'est avérée coûteuse, compliquée à mettre en œuvre et difficile à gérer. En fin de compte, cela ne réduit pas les risques : autoriser n'importe quel accès permet toujours un mouvement latéral à l'intérieur du réseau. Bien que cette méthode cloisonne le trafic est-ouest au sein d'un sous-réseau, elle ne peut pas arrêter la propagation horizontale à l'intérieur du même sous-réseau.

Pour protéger votre entreprise et mettre en place une sécurité Zero Trust, accordez uniquement aux utilisateurs l'accès aux applications dont ils ont besoin pour leur rôle. Basez cet accès sur le droit, l'identité de l'utilisateur, le profil du terminal, l'authentification et l'autorisation. Ces meilleures pratiques réduiront les attaques latérales, limitant ainsi l'exposition du réseau. L'élimination des VPN traditionnels améliorera l'expérience utilisateur, augmentera la productivité du personnel et réduira les tickets d'assistance. En outre, s'affranchir des pare-feu, du matériel et des logiciels entraîne une réduction des coûts de maintenance informatique. Les autorisations réservées aux applications améliorent la gouvernance, offrant une visibilité et des informations sur les personnes qui accèdent aux applications, l'endroit où se trouvent les données et la manière dont elles sont accessibles.

Accordez uniquement aux utilisateurs l'accès aux applications dont ils ont besoin, et basez-les sur le droit, l'identité de l'utilisateur, le profil du terminal, l'authentification et l'autorisation.

## Isolez votre infrastructure réseau de l'Internet public

L'exposition des applications internes et de l'infrastructure d'accès à Internet les rend vulnérables aux attaques DDoS, par injection SQL et à d'autres attaques au niveau de la couche applicative. Les cybercriminels sont de plus en plus rusés. Ils utilisent des techniques en constante évolution pour analyser les configurations réseau de l'entreprise afin de détecter les applications vulnérables et les données importantes. Ainsi, les entreprises doivent isoler l'architecture d'accès et d'application de l'Internet public afin qu'elle ne puisse pas être ciblée par des acteurs malveillants utilisant des ports d'écoute ouverts. Si les cybercriminels ne parviennent pas à trouver le réseau ou déterminer quelles applications et quels services sont exécutés par le terminal cible, ils ne peuvent pas l'attaquer.

## Protégez les applications d'entreprise grâce au WAF

Les cyberattaques actuelles sont extrêmement ciblées. Les acteurs malveillants utilisent l'ingénierie sociale (e-mails, réseaux sociaux, messagerie instantanée, SMS, etc.) pour s'attaquer aux individus en utilisant des leures hautement personnalisés et pertinents. Les cybercriminels recherchent des utilisateurs spécifiques ayant une ancienneté, des compétences et des niveaux d'accès souhaitables, puis lancent des attaques d'applications ciblant les autorisations de ces utilisateurs.

Si l'ordinateur d'un utilisateur est compromis, il est souvent utilisé comme un terminal zombie. Celui-ci exécute des attaques à l'insu de son propriétaire sur des applications d'entreprise considérées pourtant comme sécurisées grâce à un pare-feu. Alors que la plupart des entreprises utilisent un Web Application Firewall (WAF) pour protéger leurs applications externes contre de telles attaques, nombre d'entre elles n'ont pas étendu cette protection aux applications d'entreprise situées à l'intérieur du réseau. Un WAF peut protéger les applications internes et les données qu'elles contiennent contre les attaques de couche applicative et d'injection, telles que l'injection SQL, l'exécution de fichiers malveillants, la falsification de requêtes intersite (CSRF) et les scripts intersite.

Les cybercriminels ciblent un terminal, le transforment en machine zombie et l'utilisent pour attaquer des applications considérées pourtant comme sécurisées grâce à un pare-feu.

## Configurez l'identité, l'authentification et l'autorisation avant de fournir l'accès

Les systèmes digitaux donnent accès à toute personne qui saisit le mot de passe correct, sans vérifier l'identité de la personne. Les identifiants faibles et les mots de passe réutilisés augmentent considérablement la surface et les risques d'attaque d'une entreprise. Étant donné l'écosystème des menaces actuel, il ne suffit plus de s'appuyer sur l'authentification à un seul facteur, comme le nom d'utilisateur et le mot de passe. L'authentification multifactorielle (MFA) fournit un niveau supplémentaire de vérification et de sécurité. Elle garantit que seuls les utilisateurs validés ont accès aux applications stratégiques de l'entreprise.

L'authentification multifactorielle est indispensable. Les identifiants faiblement sécurisés, ainsi que la réutilisation des noms d'utilisateur et des mots de passe entre les applications, augmentent considérablement la surface d'attaque d'une entreprise.

Une fois l'utilisateur authentifié et autorisé via MFA, l'authentification unique (SSO) permet aux utilisateurs de se connecter à toutes les applications à l'aide d'un seul ensemble d'identifiants. Cela améliore la productivité, car il n'est pas nécessaire de reconfirmer l'identité pour chaque application et il n'y a aucun problème de synchronisation entre les applications. La prise de décisions d'accès en continu sur une multitude de signaux, y compris MFA et SSO sur les applications IaaS, sur site et SaaS, confère à l'entreprise une meilleure protection tout en offrant aux utilisateurs finaux une plus grande commodité.

## Utilisez la protection avancée contre les menaces pour vous protéger contre l'hameçonnage, les programmes malveillants zero day et le vol de données via DNS

Malgré l'adoption généralisée de la sécurité à couches multiples par les entreprises, les acteurs malveillants continuent d'avoir accès aux entreprises en exploitant les failles de sécurité. Même avec des pare-feu, des passerelles Web sécurisées, des environnements de test, des systèmes de prévention des intrusions et des antivirus de terminaux déployés, les entreprises sont exposées et sont victimes de hameçonnage, de programmes malveillants zero day et de vol de données via DNS. Que manque-t-il donc aux entreprises ?

Le DNS est un vecteur souvent négligé. Les cybercriminels ont développé des programmes malveillants spécialement conçus pour exploiter cette faille de sécurité, en contournant les couches de sécurité existantes pour infiltrer le réseau et voler les données. L'ajout d'une couche de sécurité qui exploite le protocole DNS est essentiel : en utilisant cette étape de requête initiale comme point de contrôle de sécurité, une solution de sécurité DNS peut détecter et arrêter les cyberattaques dès le début de la chaîne de protection, protégeant ainsi l'entreprise de manière proactive.

Les entreprises doivent utiliser le protocole DNS comme point de contrôle de sécurité pour détecter et arrêter les cyberattaques dès le début de la chaîne de protection.

## Surveillez le trafic et l'activité sur Internet

Les entreprises doivent partir du principe que l'environnement est hostile. Il s'agit du principe fondamental de la sécurité Zero Trust. Ainsi, les entreprises doivent s'engager à vérifier et à confirmer toutes les activités, et non à les autoriser aveuglément. Pour ce faire, les entreprises ont besoin de visibilité sur ce qui se passe sur leurs réseaux, avec un trafic et des renseignements suffisants pour effectuer des comparaisons pertinentes.

Les entreprises doivent surveiller et vérifier toutes les demandes DNS émanant de terminaux aussi bien sur le réseau de l'entreprise qu'en dehors, qu'elles proviennent d'ordinateurs portables, de téléphones mobiles, d'ordinateurs de bureau, de tablettes, de réseaux Wi-Fi invités ou de terminaux IoT, afin de s'assurer que les requêtes ne sont pas dirigées vers des sites malveillants ou inappropriés. Les entreprises ont également besoin de pouvoir analyser le trafic pour déceler des signes d'activité suspecte, comme une communication avec un serveur de commande et de contrôle (CnC) ou un vol de données, et signaler immédiatement tout problème au service informatique. Une vue d'ensemble du volume du trafic mondial et de l'évolution des menaces permet aux services informatiques de repérer plus facilement les tendances irrégulières ou dangereuses.

## Prenez en charge l'intégration avec la gestion des événements et des informations de sécurité (SIEM) et l'orchestration via des API RESTful

Les entreprises peuvent avoir des centaines, voire des milliers, d'applications. Ces dernières nécessitent une configuration via API pour déployer rapidement des applications en masse tout en définissant des contrôles de règles d'accès. Il s'agit d'une fonctionnalité essentielle pour tout environnement d'application à grande échelle cherchant à migrer rapidement d'un accès VPN traditionnel vers un accès spécifique aux applications. L'adoption d'API continue d'augmenter à mesure que les entreprises adoptent le DevSecOps et recherchent les tâches de surveillance et de configuration disponibles via l'API RESTful. Elles ont également besoin de plug-ins pour intégrer les données relatives aux menaces et aux événements dans SIEM afin d'approfondir leurs recherches et de les mettre en corrélation. Un système évolutif doit également s'intégrer aux plateformes d'automatisation des flux de travail et à l'élimination des menaces par signalisation dans des solutions tierces de détection et de réponse des terminaux.

## Conclusion

La transformation digitale est une réalité et les entreprises doivent adopter un modèle de sécurité Zero Trust pour faire évoluer leur activité avec succès, en favorisant l'innovation et l'agilité sans compromettre la sécurité. La protection avancée contre les menaces, l'accélération des applications, l'authentification multifactorielle et l'authentification unique sur l'ensemble des applications (SaaS, sur site et IaaS) sont quelques-uns des principaux avantages qui accompagnent un environnement Zero Trust. De plus, un modèle de sécurité Zero Trust permet l'orchestration par API, ainsi que l'intégration avec les plateformes d'automatisation des flux de travail et SIEM, offrant une visibilité sur les utilisateurs et les applications tout en facilitant les déploiements à grande échelle en beaucoup moins de temps.

Akamai peut vous aider à orienter l'évolution de votre réseau et de votre sécurité. Effectuez une évaluation Zero Trust en sept questions pour comprendre dans quelle mesure votre entreprise est prête à adopter une infrastructure de sécurité Zero Trust. Vous recevrez les prochaines étapes personnalisées pour la transformation du réseau. Ou, pour obtenir les ressources qui vous aideront à amorcer votre transition, rendez-vous sur akamai.com/3waystozerotrust.

Akamai