Akamai

LIVRE BLANC

Feuille de route vers une stratégie de sécurité de premier ordre

Obtenez un plan de transformation personnalisé avec le Zero Trust au cœur de votre projet

Pour garantir la protection d'Akamai dans un environnement de sécurité en constante évolution et éviter de nous reposer sur nos lauriers, nous avons récemment visualisé nos performances de sécurité à l'aide du modèle ZTMM (Zero Trust Maturity Model). Nous vous présentons ici comment cela peut mettre en évidence les domaines d'amélioration critiques pour votre organisation et créer une feuille de route claire pour atteindre une stratégie de sécurité de classe mondiale.

Simplifiez votre transition vers le Zero Trust

L'accès et la sécurité des entreprises sont complexes et évoluent en permanence. Dans ce contexte, il peut être difficile de savoir où concentrer les efforts lors de la transition vers une stratégie de sécurité Zero Trust.

C'est pourquoi nous vous recommandons d'utiliser le ZTMM comme outil pour évaluer et visualiser votre stratégie de sécurité actuelle. Nous l'avons utilisé pour évaluer notre propre stratégie de sécurité d'entreprise chez Akamai, ainsi que pour évaluer les stratégies de sécurité de plusieurs clients. À la fin du processus, vous disposerez d'une feuille de route d'actions pratiques pour vous rapprocher d'une architecture Zero Trust. (Consultez l'Annexe A pour plus d'informations sur le concept Zero Trust.)

Pourquoi le modèle de maturité Zero Trust est logique

Nous pensons que l'étape la plus importante sur la voie de la mise en œuvre d'une stratégie de sécurité renforcée est la première étape : la mise en route. Cependant, dans le sujet complexe et en constante évolution de la cybersécurité, débuter est plus facile à dire qu'à faire. Nous avons constaté que de nombreuses entreprises ont du mal à prendre des décisions concernant ce qu'il faut faire, dans quelle mesure et dans quel ordre elles doivent apporter des changements pour atteindre le Zero Trust.

C'est là que le ZTMM dévoile toute son efficacité. Il crée un cadre autour du Zero Trust, offrant un sentiment de linéarité, ce qui facilite sa mise en œuvre. Il aide les entreprises à créer un plan de changement et un budget pour les mises à jour. Il explique également les concepts de Zero Trust aux décideurs qui ne sont pas des spécialistes de l'informatique, ce qui aide les équipes informatiques à obtenir l'accord dont elles ont besoin.

Le ZTMM a été testé et éprouvé. Il a été développé par l'Agence américaine de cybersécurité et de sécurité de l'infrastructure (CISA, Cybersecurity and Infrastructure Security Agency) et a été largement adopté par les agences fédérales américaines.

Les cinq piliers et les trois capacités du modèle de maturité Zero Trust

Le ZTMM représente un gradient de mise en œuvre sur cinq piliers distincts, de sorte que des progrès mineurs peuvent être réalisés au fil du temps. Les piliers vous demandent de prendre en compte les identités, les appareils, les réseaux, les applications et les charges de travail, ainsi que les données (Figure 1). Le ZTMM nécessite également de réfléchir à trois capacités qui concernent les cinq piliers :

- Visibilité et analyses
- Automatisation et orchestration
- Gouvernance

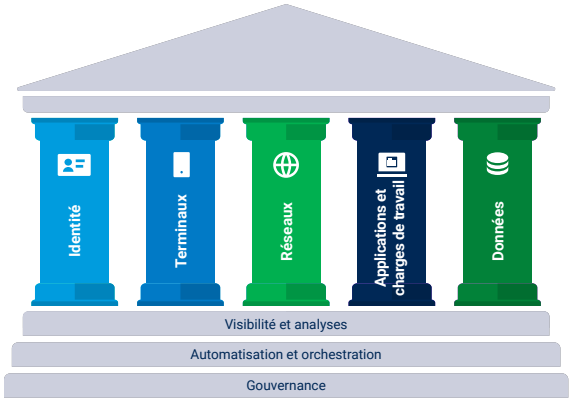


Fig. 1 : Le ZTMM de la CISA est l'un des nombreux moyens de soutenir la transition vers le Zero Trust (Source : CISA)

Un statut de maturité, qui décrit à quel point une organisation est proche d'atteindre une approche Zero Trust, est attribué à chacune de ces zones. Les quatre étapes de maturité (traditionnelle, initiale, avancée et optimale) décrivent le passage de la configuration manuelle et des VPN à la configuration idéale de « sécurité sans périmètre » (Figure 2). À l'étape de maturité optimale finale, les entreprises accordent des privilèges minimaux aux applications, refusent l'authentification et l'accès aux périphériques vulnérables, empêchent la propagation des menaces internes, détectent instantanément les incidents de sécurité et y répondent. (Consultez l'Annexe B pour obtenir une description plus détaillée du cadre ZTMM.)

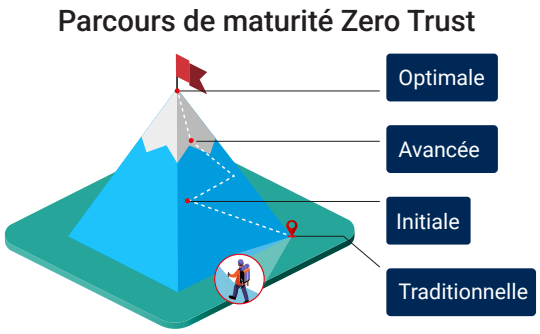


Fig. 2 : Le parcours de maturité Zero Trust (Source : CISA)

En mettant en évidence les domaines dans lesquels la maturité est la plus faible, le ZTMM aide les entreprises à développer un environnement de sécurité plus équilibré. Associée à notre expertise, la suite de solutions de sécurité d'Akamai, leader sur le marché, facilite plus que jamais la transition vers une stratégie de sécurité mature.

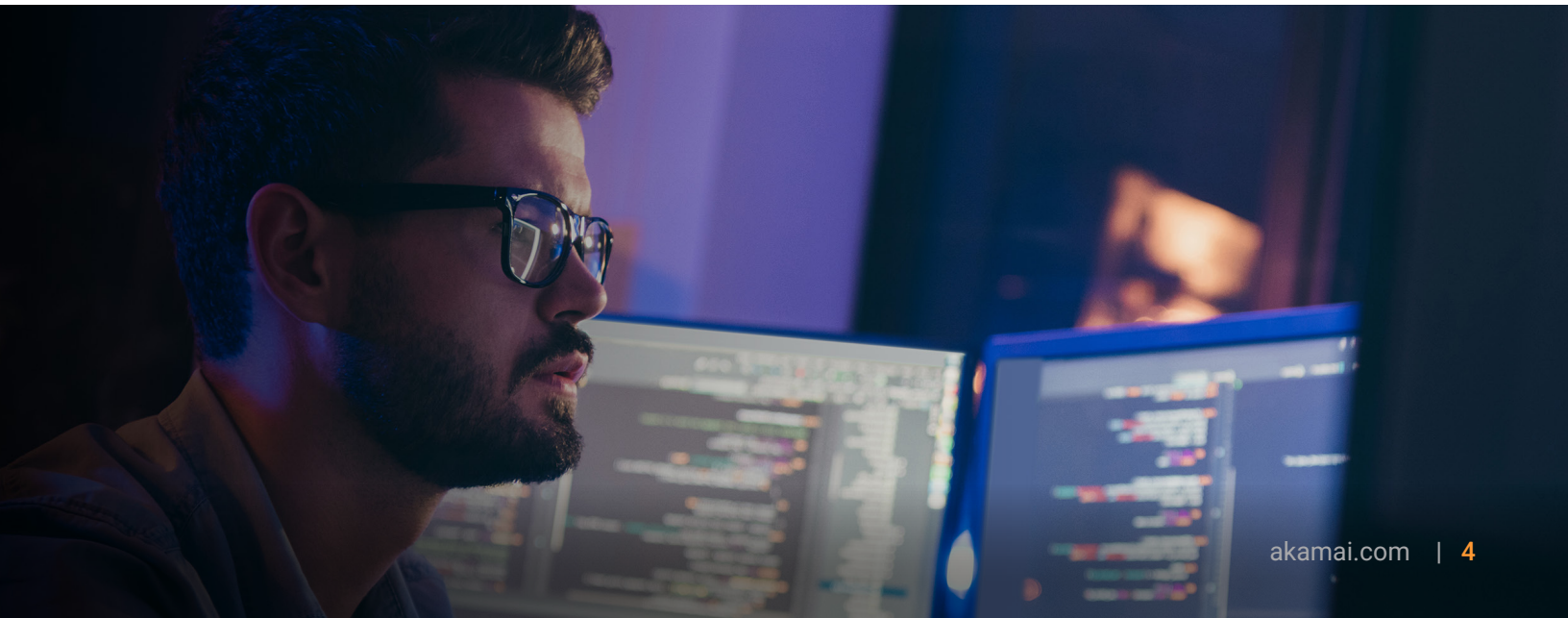
Vos équipes ont-elles du mal à mettre en œuvre le Zero Trust ? Elles ne sont pas les seules.

La création d'une architecture Zero Trust ne relève pas d'un seul service. Elle nécessite l'adhésion, la flexibilité et l'approbation de différentes parties prenantes à tous les niveaux de l'entreprise.

Akamai est l'entreprise de cybersécurité et de Cloud Computing qui soutient et protège la vie en ligne. Nos solutions de sécurité leaders sur le marché, nos informations de pointe sur les menaces et notre équipe des opérations mondiales protègent les données et les applications critiques à tous les points de contact, partout dans le monde. Cette vision d'ensemble signifie que nous comprenons les défis les plus courants lorsqu'il s'agit de passer à une stratégie de sécurité Zero Trust. Nous pouvons vous aider à trouver des solutions.

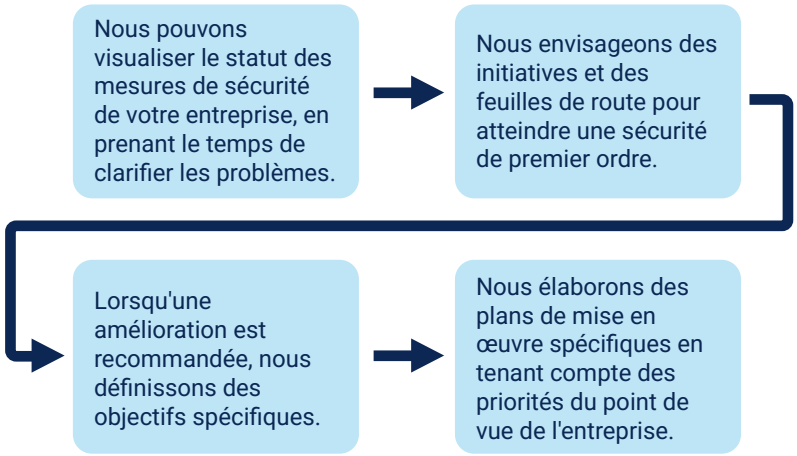
Trois défis Zero Trust courants

1. **Savoir par où commencer.** Nous recommandons généralement de commencer par la visibilité de la charge de travail et de réduire la surface d'attaque pour renforcer la cyber-résilience. Mais cela dépend, bien sûr, de la stratégie de sécurité actuelle de l'entreprise.
2. **Réussir rapidement et efficacement.** Atteindre le Zero Trust peut sembler si intimidant que les équipes ont des difficultés à se concentrer sur un seul élément ou à célébrer les petites réussites menant à cet objectif.
3. **Démontrer le retour sur investissement.** Les projets de Zero Trust ne sont pas bon marché et nécessitent généralement des changements culturels, ainsi que des changements technologiques, au sein d'une organisation. La capacité à démontrer le retour sur investissement, qu'il s'agisse d'une surface d'attaque réduite, d'une violation atténuée, d'une vulnérabilité sécurisée ou d'une victoire financière, est essentielle, en particulier pour les décideurs et les responsables de la sécurité.



Prêt à commencer votre transition vers le Zero Trust et à visualiser votre stratégie de sécurité ?

Vous pouvez utiliser le ZTMM pour visualiser l'état de maturité des mesures de sécurité actuelles de votre entreprise, comme nous l'avons fait chez Akamai. Cela vous aidera à mettre en évidence la manière dont vous pouvez équilibrer davantage votre processus et ce qui doit changer pour obtenir une architecture Zero Trust.



Comment Akamai peut vous aider à adopter une stratégie de sécurité Zero Trust

Une architecture Zero Trust réussie utilise différents contrôles et principes pour relever les défis de sécurité.

Nous examinerons les initiatives et les feuilles de route pour vous aider à créer un plan de mise en œuvre qui tient compte de l'ensemble de votre entreprise et de ses objectifs, afin d'atteindre une sécurité de premier ordre. Cette approche nous permet de travailler avec vous pour créer des systèmes et des processus de sécurité efficaces et durables sur le long terme.

Outre Akamai Cloud, notre suite de produits de sécurité comprend notamment une solution ZTNA distribuée avancée, une microsegmentation de pointe, une authentification multifactorielle (MFA) anti-hameçonnage et un pare-feu DNS proactif. Elle fera évoluer votre stratégie de sécurité vers l'étape optimale finale de l'échelle de maturité Zero Trust. De plus, l'ensemble du système peut être exécuté par un seul agent à l'aide d'une seule console (Figure 3).

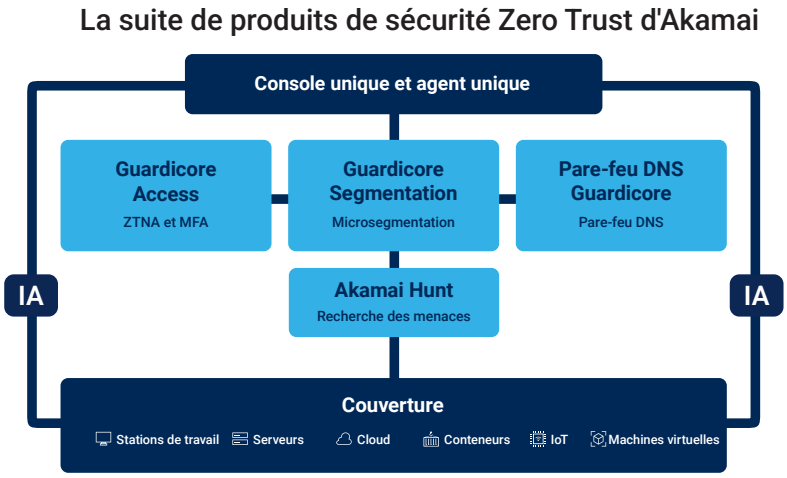


Fig. 3 : La suite de produits de sécurité d'Akamai peut être exécutée par un seul agent à l'aide d'une seule console

Étude de cas

Visualisez la stratégie de sécurité e-commerce d'un détaillant multinational avec le modèle de maturité Zero Trust

Nous avons récemment analysé la stratégie de sécurité e-commerce d'un détaillant multinational, en déterminant son état de sécurité et en fournissant une feuille de route correspondante pour l'amener à atteindre une stratégie de sécurité de classe mondiale. Notre équipe d'experts a identifié des domaines d'amélioration dans le ZTMM, que nous avons classés par ordre d'importance, du plus élevé au plus faible. Nous partageons ici les résultats.

Un système déséquilibré avec des variations dans la mise en œuvre

Dans chaque pilier, nous avons constaté que certaines fonctions ont été mises en œuvre au niveau de maturité le plus élevé (optimal), comme la gestion des périphériques mobiles et l'automatisation du déploiement d'applications. Cependant, certaines fonctions de chaque pilier sont restées au niveau traditionnel, ce qui présentait de graves risques.

En particulier, les fonctions importantes des piliers Identité et Réseau n'ont pas été renforcées. Ces piliers constituent la base d'une architecture Zero Trust. Ces fonctions comprenaient l'authentification multifactorielle, la gestion intégrée de l'infrastructure d'identités, le contrôle d'accès basé sur le contexte et la microsegmentation.

Infrastructure d'ID à risque

Nos analystes ont découvert que l'authentification par ID et mot de passe était la norme chez le détaillant ; l'utilisation de l'authentification multifactorielle était limitée à quelques systèmes. Cela a créé un risque élevé d'abus des informations d'authentification. En outre, il existait plusieurs infrastructures d'identification, telles que Microsoft Entra ID, Active Directory (AD) sur site et Lightweight Directory Access Protocol (LDAP). Étant donné que la gestion du détaillant n'était pas intégrée, il existait un risque de violation à partir d'une infrastructure d'identification avec des mesures de sécurité plus faibles, telles que LDAP.

Contrôles d'autorisation non intégrés

Les contrôles d'autorisation n'avaient pas été intégrés, chaque application était donc traitée individuellement. Il n'était pas possible de bloquer l'accès à partir d'appareils vulnérables ou un accès suspect. Si le PC d'un employé ou d'un partenaire ayant accès au réseau de l'entreprise était infecté par un logiciel malveillant, il existait un risque élevé d'accès non autorisé aux systèmes et aux ressources par des mouvements latéraux.

Segmentation inadéquate

Nous avons constaté que les mesures de sécurité du détaillant étaient principalement axées sur les menaces extérieures, en négligeant les risques posés par les attaquants qui avaient déjà pénétré dans le réseau. Sans une solide segmentation interne, une intrusion via le réseau Wi-Fi d'un entrepôt ou via des vulnérabilités dans le VPN aurait pu entraîner des mouvements latéraux incontrôlés. L'absence de barrières internes augmentait considérablement le risque de compromission généralisée du système, de fuite de données et de pannes opérationnelles, car l'attaque pouvait se déplacer librement sur le réseau sans que des mesures de confinement ne soient mises en place.

Gestion des failles de sécurité et réponse insuffisantes

Le détaillant ne disposait pas d'un système de gestion liant une nomenclature logicielle (SBOM) aux informations de vulnérabilité. Cela signifie qu'il ne pouvait pas identifier rapidement les vulnérabilités des applications et y répondre, ce qui représentait un risque élevé.

Nos recommandations

Nous avons conseillé au détaillant de prendre les cinq mesures suivantes pour renforcer sa stratégie de sécurité :

1. Prendre des mesures proactives pour réduire le risque d'intrusion non autorisée et de mouvement latéral existant avec la configuration actuelle
2. Continuer à intégrer l'infrastructure d'identité dans sa pile technologique existante
3. Développer un plan pour étendre les capacités d'authentification et d'autorisation, en association avec l'accès au réseau Zero Trust
4. Choisir la méthode la plus efficace pour mettre en œuvre une protection granulaire des charges de travail et des applications
5. Créer un système et un processus de réponse pour les menaces futures inconnues, développer un système et un processus pour renforcer la gestion des failles de sécurité et la réponse, et élaborer un plan

Si vous souhaitez débuter votre transition vers le Zero Trust, contactez-nous pour obtenir une évaluation gratuite de la sécurité.

Annexe A : Présentation du concept Zero Trust

La philosophie du Zero Trust est basée sur l'idée qu'aucun utilisateur, appareil ou système, à l'intérieur ou à l'extérieur du périmètre du réseau d'une organisation, ne devrait être considéré comme digne de confiance.

Au lieu de cela, des processus de vérification et de surveillance sont utilisés pour minimiser les risques. Cela inclut des approches telles que l'application de stratégies strictes de gestion des identités et des accès (IAM), l'utilisation de l'authentification multifactorielle (MFA) et la hiérarchisation du contrôle d'accès basé sur les rôles (RBAC).

Le concept de Zero Trust existe depuis 15 ans, mais il est devenu plus important au cours de la pandémie de COVID-19, lorsque les entreprises ont dû faire face à des exigences accrues en matière d'accès à distance. De nombreuses entreprises ont réalisé que leurs mesures de sécurité existantes ne tenaient pas la route lorsque les utilisateurs et les appareils étaient dispersés plutôt que centralisés.

Aujourd'hui, il existe de nombreuses applications de Zero Trust, notamment l'architecture Zero Trust, l'accès réseau Zero Trust (ZTNA), la passerelle Web sécurisée (SWG) Zero Trust et la microsegmentation.

En savoir plus sur le Zero Trust

Annexe B : Le cadre ZTMM 2.0

Les cinq piliers

Chaque pilier peut progresser à son propre rythme et plus rapidement que les autres, jusqu'à ce qu'une coordination entre les piliers soit nécessaire.

Pilier	Description
Identité	Attribut ou ensemble d'attributs qui décrit de manière unique un utilisateur ou une entité d'agence, y compris les entités non personnelles
Appareils	Tout actif pouvant se connecter à un réseau, y compris des serveurs, des ordinateurs de bureau et portables, des imprimantes, des téléphones portables, des appareils IoT (Internet des objets), des équipements réseau, etc.
Réseaux	Moyen de communication ouvert, y compris les canaux types, tels que les réseaux internes des agences, les réseaux sans fil et Internet, ainsi que d'autres canaux potentiels utilisés pour transporter des messages
Applications et charges de travail	Systèmes d'agences, programmes informatiques et services qui s'exécutent sur site, sur des appareils mobiles et dans des environnements cloud
Données	Fichiers et fragments structurés et non structurés résidant ou ayant résidé dans des systèmes, des appareils, des réseaux, des applications, des bases de données, des infrastructures et des sauvegardes, ainsi que les métadonnées associées

Capacités inter-piliers

Ces trois fonctionnalités prennent en charge l'ensemble de la structure Zero Trust, garantissant ainsi l'intégration, la réactivité et la cohérence des mesures de sécurité.

Capacités	Description
Visibilité et analyses	Les entreprises doivent disposer d'une vue claire et en temps réel de toutes les activités des utilisateurs, de l'état des appareils et des interactions réseau. Les menaces sont détectées et traitées rapidement, ce qui réduit les risques. Les entreprises prennent des décisions éclairées et proactives en matière de sécurité.
Automatisation et orchestration	L'erreur humaine est une cause courante de problèmes de sécurité. Lorsque l'automatisation et l'orchestration sont optimisées, les risques sont réduits. L'automatisation simplifie les tâches de routine et l'orchestration organise les actions de sécurité sur différents systèmes. Cela crée les conditions adéquates pour des réponses plus rapides et plus coordonnées aux menaces.
Gouvernance	Une bonne gouvernance de la sécurité crée une responsabilité, en veillant à ce que chacun suive les mêmes pratiques et réglementations en matière de sécurité. Cela permet de construire une base solide pour des opérations sûres. Cela définit également des directives Zero Trust claires et aide les entreprises à respecter les normes de conformité.

L'aspect maturité du modèle de maturité Zero Trust

ZTMM 2.0 définit quatre niveaux de maturité pour chaque fonction. L'objectif est de déterminer le niveau de maturité actuel des cinq piliers et des trois capacités, puis de créer un plan pour faire progresser chacun d'entre eux vers le niveau de maturité le plus élevé.

Niveau de maturité	Description
Traditionnel	Configuration, réponse et atténuation manuelles ; stratégies et solutions statiques et cloisonnées
Initial	Début de l'automatisation ; solutions transversales initiales ; quelques changements réactifs pour le moindre privilège ; visibilité agrégée pour les systèmes internes
Avancé	Contrôles automatisés, le cas échéant ; application des règles transversales ; changements de moindre privilège en fonction du risque/de la stratégie ; réponse aux mesures d'atténuation prédéfinies
Optimal	Contrôles automatisés, le cas échéant ; application des règles transversales ; changements de moindre privilège en fonction du risque/de la stratégie ; réponse aux mesures d'atténuation prédéfinies