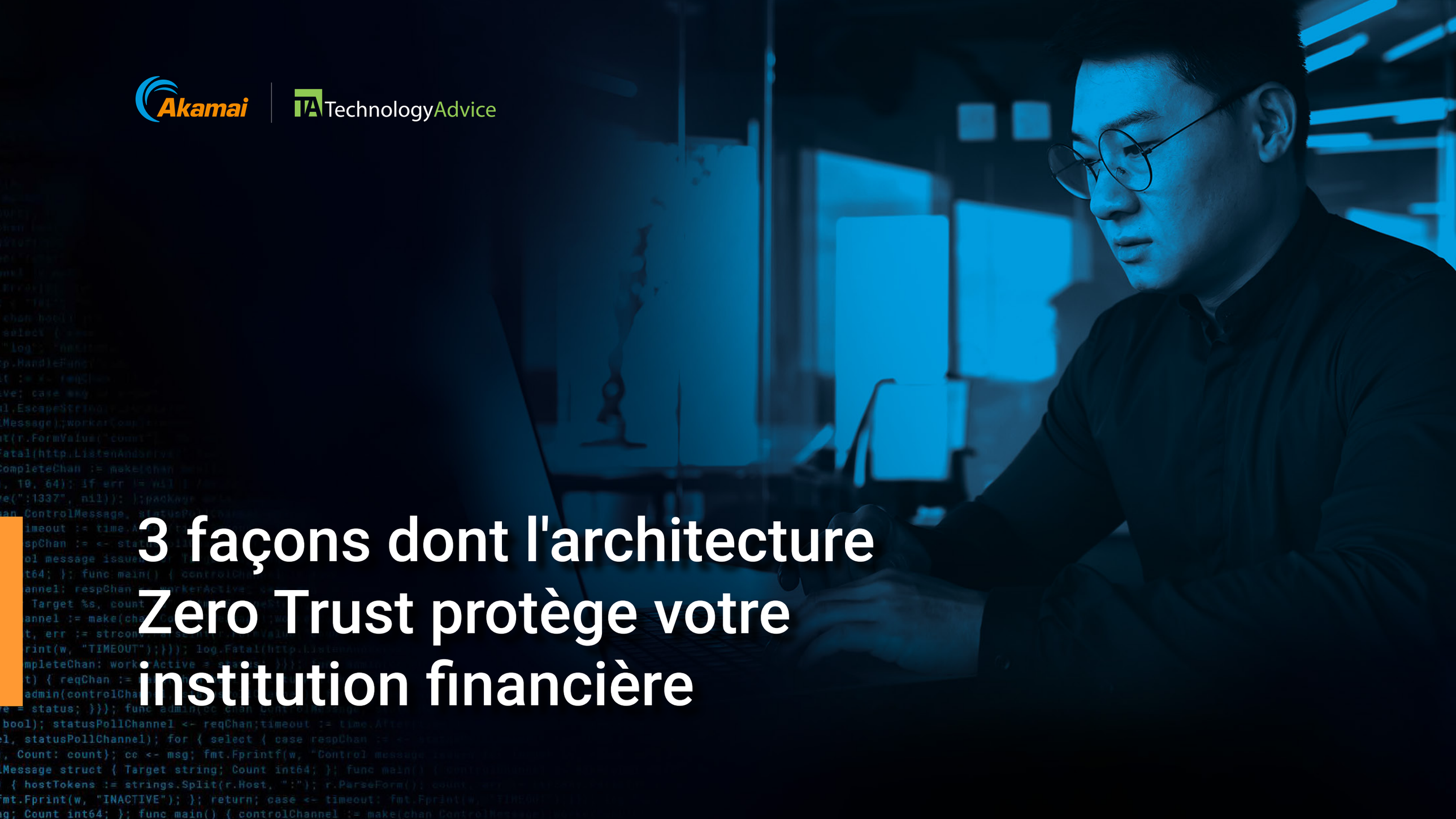
Akamai | TechnologyAdvice



3 façons dont l'architecture Zero Trust protège votre institution financière

Les institutions financières restent des cibles de choix pour les acteurs malveillants. Elles sont confrontées à une augmentation de 65 % des attaques ciblant les applications Web et les API si l'on compare le deuxième trimestre 2023 au deuxième trimestre 2022. Cet assaut incessant de cybermenaces en constante évolution non seulement épuise les ressources, mais détourne également l'attention des fonctions essentielles de l'entreprise.

Les solutions traditionnelles de pare-feux et de points de terminaison font implicitement confiance aux points de terminaison, aux terminaux et aux utilisateurs qui passent le filtre initial d'une combinaison de mot de passe et de nom d'utilisateur, parfois renforcé par l'authentification multifactorielle (MFA). Les applications, les API et les services système au sein du réseau fonctionnent souvent sans contrôle de sécurité au-delà de la surveillance de base des programmes malveillants au niveau des terminaux. Pour faire face aux menaces croissantes des ransomwares, aux réglementations strictes en matière de conformité et aux défis de la migration vers le cloud, les institutions financières adoptent désormais Zero Trust.

Zero Trust met fin à la confiance implicite et vérifie en permanence les autorisations d'accès pour toutes les applications, tous les utilisateurs et tous les terminaux en fonction du contexte de la demande et des autorisations. Même si un attaquant parvient à compromettre un terminal ou des informations d'identification pour accéder à un réseau, l'accès peut être strictement restreint et les dommages fortement réduits.

Mais de quelle manière exactement une structure Zero Trust protège-t-elle votre institution financière ?

Elle respecte les réglementations en constante évolution

Les institutions financières doivent consacrer des ressources importantes pour prouver qu'elles respectent différentes réglementations, telles que la norme de sécurité de l'industrie des cartes de paiement (PCI DSS) bien établie ou le règlement sur la résilience opérationnelle numérique du secteur financier (DORA), qui devrait être appliqué intégralement en janvier 2025. Les audits gagnent régulièrement en complexité, en coût et en temps, en raison d'exigences floues, contradictoires et changeantes. Pourtant, les institutions financières doivent réaliser l'investissement car un échec d'audit peut également entraîner des pertes de revenus, des sanctions réglementaires, des amendes ou des pénalités, ainsi qu'une atteinte à leur réputation et des responsabilités juridiques potentielles.

Les rapports de conformité exigent des comptes rendus clairs et précis des systèmes qui touchent aux données réglementées et exigent la preuve que ces systèmes sont correctement protégés. Cependant, l'environnement informatique des grandes institutions financières est trop vaste, trop détaillé et trop complexe pour permettre de suivre facilement les actifs et les accès.

Les pare-feux et systèmes de protection des terminaux existants permettent principalement d'assurer le suivi et la protection des utilisateurs et des actifs traditionnels. Le fait de s'appuyer sur cette approche conventionnelle de la segmentation du réseau pose des problèmes d'évolutivité des opérations, entrave la création et l'application de règles et limite l'agilité.

Pour surmonter les défis posés par les environnements existants avec une technologie alignée sur la stratégie future, les institutions financières ont besoin d'une visibilité granulaire sur le trafic Est-Ouest et de pouvoir appliquer des politiques de segmentation dans les environnements multicloud et de conteneurs. Face à la nécessité croissante de gérer plusieurs régions et types d'infrastructures informatiques, y compris la technologie des conteneurs, les institutions financières doivent disposer du chemin le plus simple et le plus direct vers la microsegmentation avec la flexibilité des règles, l'intégration DevOps et l'automatisation.

Sans identification, suivi et sécurisation réguliers de toutes les ressources, une institution financière ne peut garantir que l'accès aux données réglementées est entièrement contrôlé et protégé. Le fait d'ignorer ou de contrôler de manière inadéquate les données, les utilisateurs, les applications ou les terminaux augmente considérablement les risques de cyberattaque et l'échec potentiel d'un audit de conformité.

L'architecture Zero Trust refuse l'accès par défaut et toutes les connexions doivent être explicitement accordées en fonction d'un contexte : l'utilisateur autorisé, sur un terminal autorisé, avec accès autorisé aux données demandées. Zero Trust utilise par défaut l'accès de moindre privilège, ce qui entrave les anciennes connexions oubliées ou inconnues. La solution d'Akamai identifie rapidement les terminaux indésirables, les utilisateurs hérités (humains, API ou applications) et les sources de données oubliées qui infestent les anciennes succursales ou les environnements technologiques hérités des entreprises acquises.

L'architecture Zero Trust d'Akamai s'applique quel que soit l'emplacement de l'utilisateur, mais le contexte de l'emplacement peut être inclus dans le processus de décision d'accès. Les équipes de sécurité bénéficient du contrôle consolidé et des rapports nécessaires pour analyser rapidement et gérer entièrement l'accès aux ressources dans les réseaux locaux, les centres de données ou le cloud.

Face à la pression réglementaire accrue pour protéger les applications critiques et sécuriser le trafic Est-Ouest, les institutions financières se concentrent sur l'amélioration de la visibilité et la compréhension de leurs environnements. Grâce aux principes Zero Trust, elles peuvent désormais identifier et segmenter les actifs non conformes de façon fluide, ce qui permet aux équipes en charge des applications de gérer de manière autonome les règles de segmentation. Cela garantit un flux de travail efficace et simplifie le processus de création de rapports.

Le fait d'avoir une visibilité complète et contextuelle du trafic Est-Ouest facilite la cartographie et le cloisonnement des applications stratégiques, sans modification de l'infrastructure ni des applications. Cette fonctionnalité permet aux institutions de restreindre l'accès de tiers et de renforcer la sécurité globale.

L'acquisition de visibilité permet de rationaliser la migration sécurisée vers le cloud, tandis que l'intégration de la segmentation dans le cycle DevOps garantit des mises à jour immédiates des règles sans modifications substantielles de l'infrastructure, ce qui constitue une rupture par rapport aux pratiques antérieures en matière de VLAN. En outre, Akamai permet et simplifie la création, l'application et les rapports uniformes des règles de conformité sur plusieurs infrastructures. Cela est rendu possible grâce à une visibilité accrue, au mappage des dépendances des applications, aux règles de segmentation automatisées, à l'automatisation des stratégies DevOps et à une intégration fluide de la gestion des changements.

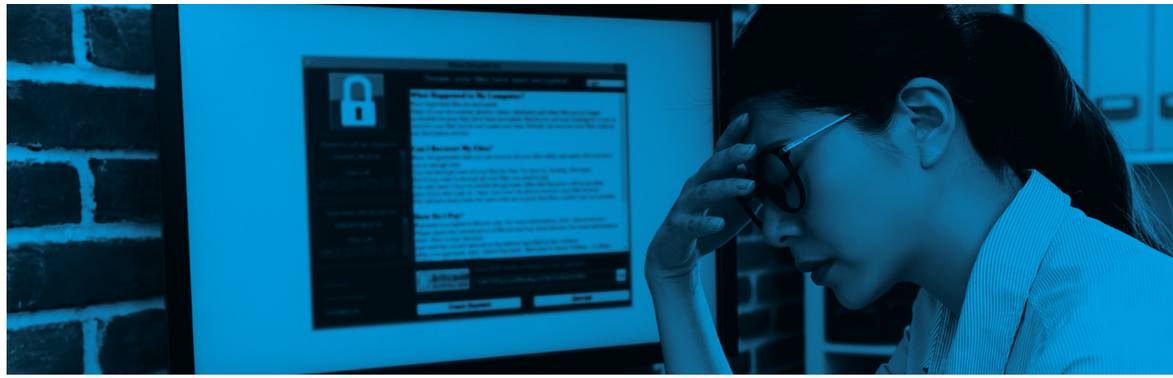
Elle empêche la propagation des ransomwares

Des succursales aux institutions financières internationales, les attaques de ransomwares font la une des journaux et sont un vrai casse-tête dans le monde entier. Selon le rapport 2022 sur le marché des ransomwares de Cybersecurity Ventures, « une entreprise, un internaute ou un terminal pourrait faire face à une attaque par ransomware toutes les deux secondes d'ici 2031 ».

Les institutions de services financiers se développant généralement par le biais de fusions et d'acquisitions, elles manquent souvent de visibilité sur l'ensemble de leur écosystème technologique, et laissent ainsi la porte ouverte aux attaquants. Les auteurs d'attaques par ransomware exploitent ces portes ouvertes ou recourent aux attaques par hameçonnage pour voler des informations d'identification ou déposer sur les terminaux des logiciels malveillants inconnus qui échappent aux systèmes de protection.

Les stratégies d'accès utilisateur excessivement permissives et l'authentification par mot de passe permettent aux attaquants de contourner les pare-feux, d'échapper à la détection au niveau des points de terminaison et d'obtenir un accès illimité aux réseaux qui font implicitement confiance au trafic, aux utilisateurs et aux terminaux connectés. Les auteurs d'attaques par ransomware, qui opèrent souvent en groupes organisés, tels que CL0P, exploitent les actifs compromis, puis se déplacent latéralement sur le réseau pour découvrir et exploiter d'autres actifs vulnérables. Les vulnérabilités Zero Day, comme la vulnérabilité d'injection SQL MOVEit, permettent aux attaquants d'accéder au réseau et de propager rapidement l'attaque en utilisant des scripts automatisés pour crypter les systèmes, voler des données et effectuer des demandes de rançon.

Les solutions Zero Trust d'Akamai permettent aux institutions financières d'identifier et d'isoler les systèmes critiques, et de restreindre l'accès au réseau vers et depuis ces systèmes. Cette approche atténue la probabilité et l'impact des attaques par ransomware et réduit le temps nécessaire pour y remédier. Dans un premier temps, Akamai suit et surveille les domaines et adresses IP malveillants, en mettant en place des mises en quarantaine appropriées pour empêcher le lancement de nombreuses attaques.



Par la suite, grâce à une visibilité du trafic réseau quasi en temps réel, Akamai observe et contrôle le trafic jusqu'aux niveaux du processus et du service. Cette connaissance approfondie permet aux équipes du centre d'opérations de sécurité et du centre d'opérations de réseau d'identifier et de cibler précisément les menaces spécifiques en cours.

Ensuite, même une attaque réussie sera étroitement limitée dans sa portée grâce à la microsegmentation inhérente à Akamai Guardicore Segmentation. Les informations d'identification et les autorisations seront vérifiées en permanence à chaque demande d'accès, et les connexions aux applications protégées par la solution Enterprise Application Access d'Akamai seront refusées.

En outre, les applications, serveurs et autres ressources dont les utilisateurs n'ont pas besoin sont automatiquement masqués, ce qui empêche les attaquants d'effectuer tout mouvement latéral ou toute extension d'accès. Enfin, la détection des anomalies offerte par Akamai Hunt signale les comportements inhabituels afin d'alerter les équipes de sécurité et les aider à identifier les attaques avant que les données ne puissent être exfiltrées ou chiffrées.

Elle rationalise la transformation digitale

Pour favoriser l'agilité, l'évolutivité et la modernisation, de nombreuses institutions financières déplacent leurs applications vers le cloud. Toutefois, ce déplacement donne lieu à un grand nombre de nouveaux problèmes.

Pour commencer, les institutions financières ne peuvent pas migrer des ressources et des connexions non détectées et inconnues. En outre, non seulement les migrations vers le cloud augmentent la surface d'attaque, mais les intégrations multicloud et cloud hybride local nuisent également souvent aux applications et introduisent des failles dans les couches de sécurité établies. De plus, les infrastructures logicielles déployables (conteneurs, machines virtuelles, etc.) se déploient automatiquement trop rapidement pour être sécurisées ou contrôlées efficacement à l'aide de solutions héritées.

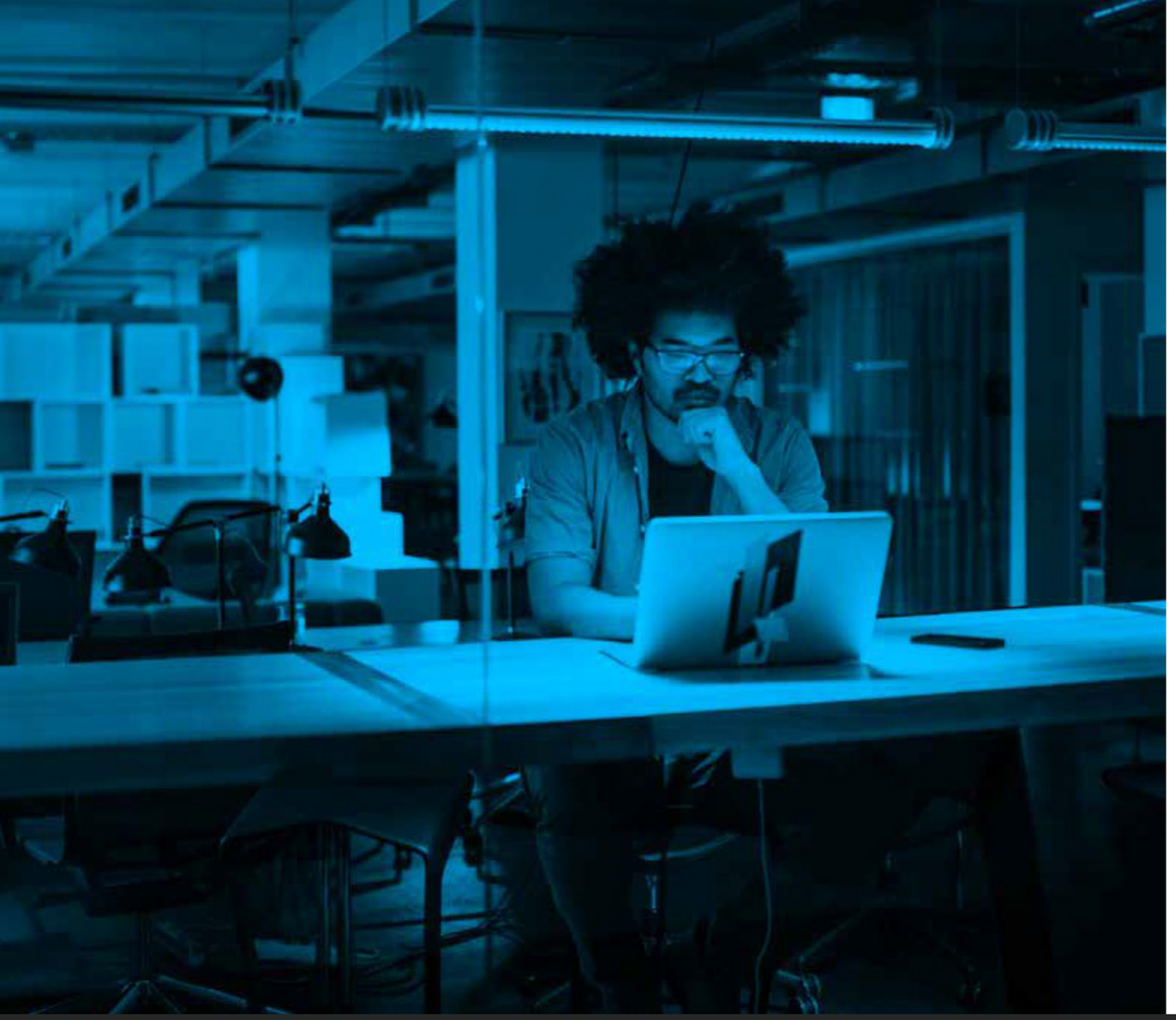
Les solutions Zero Trust permettent aux institutions financières de déployer plus facilement leurs applications basées sur le cloud, le tout en bénéficiant de meilleures protections et d'une charge opérationnelle réduite. Les solutions Zero Trust d'Akamai assurent le suivi de tous les flux de données afin d'identifier rapidement la surface d'attaque potentielle et d'appliquer les règles sans perturber l'activité.

Une fois la surface d'attaque identifiée, les équipes chargées de la sécurité et des opérations peuvent utiliser le système de contrôle centralisé d'Akamai pour segmenter et sécuriser les applications et surveiller les flux de données. Akamai permet un contrôle granulaire tout en réduisant les coûts opérationnels et la complexité. Pour les équipes chargées de la sécurité et des opérations au sein des institutions financières, l'application de règles universelles garantit une modernisation rapide et souple de l'infrastructure. Cela est rendu possible grâce à la sécurité robuste de la segmentation Zero Trust de moindre privilège, qui fournit un bouclier puissant contre les menaces en constante évolution.

Les institutions financières ne peuvent pas se permettre d’ignorer le Zero Trust

Les attaques contre les technologies héritées peuvent mener à des violations de données de grande envergure, coûter des millions en termes de dommages et détruire la confiance des clients et des partenaires. Les attaques deviennent de plus en plus sophistiquées et plus rapides, et, sans une visibilité complète sur l'écosystème technique, les institutions financières peuvent laisser la porte ouverte aux attaquants.

Akamai offre une meilleure visibilité sur le réseau, limite intelligemment l'accès des utilisateurs, détecte en permanence les menaces et signale toute anomalie pour vérification de la sécurité. Découvrez comment répondre aux besoins de votre institution financière grâce au portefeuille de solutions Zero Trust d'Akamai.



En savoir plus sur la sécurisation de vos finances digitales avec Akamai

En savoir plus

TechnologyAdvice | Akamai

Akamai protège votre expérience client, votre personnel, vos systèmes et vos données en vous aidant à intégrer la sécurité dans tout ce que vous créez, dans toutes vos conceptions et diffusions. La visibilité de notre plateforme sur les menaces mondiales nous aide à adapter et à faire évoluer votre posture de sécurité, pour activer le Zero Trust, arrêter les ransomwares, sécuriser les applications et les API, ou lutter contre les attaques DDoS, en vous donnant la confiance nécessaire pour innover, vous développer et ouvrir le champ des possibles. Pour en savoir plus sur les solutions de Cloud Computing, de sécurité et de diffusion de contenu, rendez-vous sur akamai.com et akamai.com/blog, ou abonnez-vous à Akamai Technologies sur X (anciennement Twitter) et LinkedIn.