Akamai

LIVRE BLANC

Atteindre la maturité Zero Trust avec Akamai

Prendre en charge les capacités transversales de la CISA pour les agences et services fédéraux

Introduction

La sécurité Zero Trust est devenue la référence absolue en matière de protection des données gouvernementales sensibles, des infrastructures critiques et des systèmes de sécurité nationaux. Les agences et services fédéraux ne peuvent plus se fier aux modèles de sécurité traditionnels basés sur le périmètre pour lutter contre les menaces actuelles. À mesure que les cybercriminels gagnent en sophistication et utilisent des tactiques avancées, telles que le vol d'identifiants, les ransomwares et les attaques internes, les organisations fédérales adoptent de plus en plus un cadre de sécurité Zero Trust. Cependant, ces initiatives restent parcellaires et il faut prendre davantage de mesures pour sécuriser les systèmes fédéraux.

Le modèle de maturité Zero Trust de la Cybersecurity and Infrastructure Security Agency (CISA) peut aider les agences et services fédéraux à mettre en œuvre des principes de sécurité qui éliminent la confiance implicite et appliquent des mécanismes de vérification stricts. Ce modèle repose sur cinq piliers fondamentaux : Identité, Terminaux, Réseaux, Applications et charges de travail, Données. En outre, trois capacités transversales garantissent une approche globale et cohérente en matière de cybersécurité : Visibilité et analyses, Automatisation et orchestration, Gouvernance.

Pour atteindre ces objectifs, la microsegmentation doit être considérée comme un élément essentiel de la sécurité Zero Trust, car elle joue un rôle fondamental dans la défense réseau interne (c'est-à-dire est-ouest). En segmentant les charges de travail et en limitant les mouvements latéraux, les organisations fédérales peuvent restreindre les violations potentielles et appliquer des stratégies Zero Trust. En outre, des solutions complètes de sécurité API (interface de programmation d'applications) doivent être mises en œuvre pour protéger les communications externes (c'est-à-dire nord-sud), en veillant à ce que seules les entités autorisées accèdent aux applications gouvernementales.

Ce livre blanc présente les étapes essentielles pour atteindre la maturité Zero Trust, en soulignant comment les solutions de sécurité avancées d'Akamai, notamment Akamai Guardicore Segmentation, Akamai API Security et Akamai Enterprise Application Access, permettent aux agences et services fédéraux de respecter les directives de la CISA et d'améliorer leur stratégie de cybersécurité.

De la sécurité basée sur le périmètre à la sécurité Zero Trust

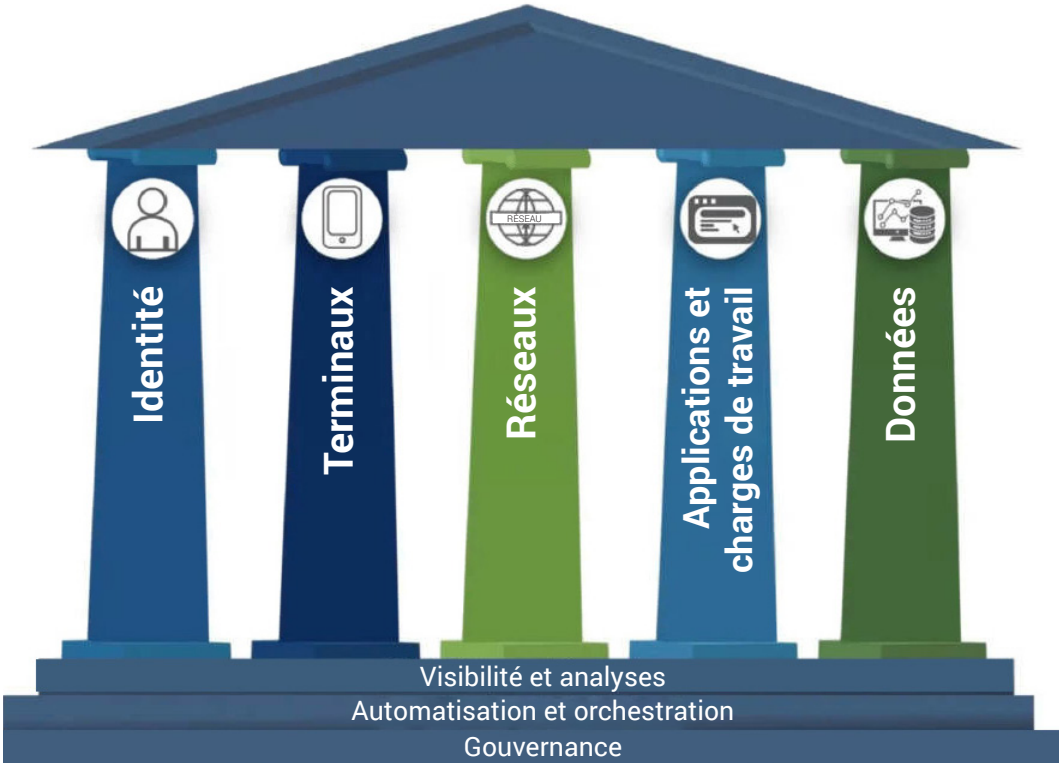
La cybersécurité traditionnelle reposait sur des défenses basées sur le périmètre, en partant du principe que toute entité à l'intérieur du réseau était fiable. Cependant, ce modèle a échoué à plusieurs reprises face aux nouvelles cybermenaces. Les pirates exploitent les identifiants faibles et les paramètres de sécurité mal configurés, et ils utilisent des techniques de mouvement latéral pour contourner les défenses traditionnelles et accéder aux informations sensibles.

La sécurité Zero Trust élimine la confiance implicite en exigeant une vérification continue des utilisateurs, des terminaux, des applications et du trafic réseau. Chaque demande d'accès est authentifiée, autorisée et surveillée en permanence en s'appuyant sur des évaluations des risques en temps réel. Cette approche réduit considérablement la surface d'attaque et empêche tout accès non autorisé, même si un cybercriminel parvient à accéder à une partie du réseau.

Le modèle de maturité Zero Trust de la CISA

Le modèle de maturité Zero Trust de la CISA fournit une feuille de route pour les agences et services fédéraux afin de renforcer progressivement leur cadre de sécurité (Figure). Ce modèle repose sur cinq piliers clés :

- **Identité :** appliquer des contrôles d'authentification, d'autorisation et d'accès renforcés pour garantir que seuls les utilisateurs légitimes peuvent interagir avec des ressources sensibles.
- **Terminaux :** surveiller, sécuriser et valider les terminaux pour s'assurer qu'ils sont conformes aux stratégies de sécurité avant d'accéder aux réseaux gouvernementaux.
- **Réseaux :** mettre en œuvre des stratégies avancées de microsegmentation et de contrôle d'accès pour empêcher les mouvements latéraux non autorisés.
- **Applications et charges de travail :** protéger les applications et les charges de travail avec des stratégies d'accès strictes basées sur les identités, des mesures de sécurité d'exécution et des contrôles de sécurité des API.
- **Données :** s'assurer que les données gouvernementales sensibles restent chiffrées, surveillées et protégées contre les accès et exfiltrations non autorisés.



Piliers du modèle de maturité Zero Trust de la CISA (source : CISA)

En plus de ces piliers, le modèle intègre trois capacités transversales essentielles qui s'appliquent à tous les composants Zero Trust :

- **Visibilité et analyses :** surveillance continue, journalisation et détection des anomalies pour identifier et atténuer les menaces en temps réel.
- **Automatisation et orchestration :** automatisation de la sécurité optimisée par l'IA pour appliquer des stratégies, répondre aux menaces et rationaliser le contrôle d'accès.
- **Gouvernance :** application centralisée des stratégies pour assurer la conformité aux réglementations fédérales, telles que la loi FISMA (Federal information Security Modernization Act) et la publication spéciale 800-207 du NIST (National Institute of Standards and Technology).

L'importance de la microsegmentation et de la sécurité des API

Dans les modèles traditionnels de sécurité réseau, les réseaux sont généralement divisés en larges segments, en utilisant des pare-feux basés sur le réseau. Bien que cette approche offre un certain niveau de sécurité, elle ne dispose pas de la granularité requise pour protéger pleinement les environnements distribués actuels. Dans les environnements fédéraux, la segmentation basée sur le réseau entraîne généralement un provisionnement excessif des ressources. Autrement dit, les utilisateurs et les applications ont accès à plus de ressources qu'ils n'en ont réellement besoin. Cela crée des opportunités involontaires de mouvement latéral. À mesure que les attaquants compromettent une partie du réseau, ils peuvent se déplacer vers des zones plus sensibles avec peu de résistance.

Le concept de microsegmentation permet de résoudre ce problème en offrant un contrôle précis du trafic est-ouest au sein du réseau. Dans un environnement microsegmenté, chaque application, charge de travail ou service est isolé des autres, et l'accès est restreint en fonction de stratégies de sécurité spécifiques. Ainsi, les utilisateurs, les terminaux et les applications ne peuvent communiquer qu'avec les ressources auxquelles ils sont explicitement autorisés à accéder. En mettant en œuvre une segmentation orientée applications basée sur les identités, la microsegmentation limite les dommages potentiels causés par les cyberattaques, réduit la surface d'attaque et applique le principe de Zero Trust.

En matière de trafic réseau nord-sud, les réseaux fédéraux s'appuient de plus en plus sur des API pour faciliter la communication entre les systèmes. Par conséquent, la protection des points de terminaison des API devient une priorité absolue. Les attaques d'API, y compris les attaques par injection, le « credential stuffing » et l'accès non autorisé aux données, ont fortement augmenté ces dernières années. Les agences et services fédéraux ont besoin de solutions complètes de sécurité des API afin de fournir une protection pendant tout le cycle de vie des API. Ainsi, le personnel de sécurité peut découvrir, surveiller et sécuriser le trafic des API en temps réel. La détection des API est particulièrement importante, car il n'est pas rare d'avoir des API dont personne n'a connaissance.

Les solutions Zero Trust d'Akamai en un coup d'œil

Identité

Akamai MFA est une solution d'identité FIDO2 sans clé qui protège les comptes des employés contre l'hameçonnage et d'autres attaques de type « machine-in-the-middle ». Elle garantit que seuls les employés fortement identifiés et authentifiés peuvent accéder aux comptes qui leur appartiennent. Les autres accès sont refusés et il est impossible de prendre le contrôle du compte de l'employé.

Terminaux

Akamai Guardicore Segmentation est une solution de microsegmentation leader du marché, conçue pour limiter la propagation est-ouest des ransomwares et autres logiciels malveillants. En surveillant et en appliquant en permanence des stratégies sur les terminaux, Akamai Guardicore Segmentation peut vérifier les configurations des terminaux, les installations logicielles et les vulnérabilités potentielles, garantissant ainsi que seuls les terminaux conformes peuvent accéder au réseau. En outre, la solution prend en charge une approche sans agent pour sécuriser les terminaux de l'Internet des objets (IoT).

Akamai Enterprise Application Access est une solution complète d'accès réseau Zero Trust qui garantit que seuls les utilisateurs et terminaux authentifiés peuvent accéder aux applications. En vérifiant l'identité et la stratégie de sécurité des terminaux, Enterprise Application Access complète les fonctionnalités d'Akamai Guardicore Segmentation. Si un terminal s'avère non conforme ou présente un risque de sécurité, Enterprise Application Access peut restreindre son accès aux applications sensibles.

Réseaux

Akamai API Security offre aux professionnels de la sécurité fédérale une visibilité complète sur l'ensemble des API grâce à la découverte continue et à l'analyse en temps réel du trafic nord-sud. La solution détecte les API inconnues, identifie les vulnérabilités et analyse le comportement des API, afin que les équipes de sécurité détectent les attaques et corrigent les risques dans cette surface d'attaque en croissance rapide.

Akamai App & API Protector réunit des technologies de pare-feu d'application Web, d'atténuation des bots, de sécurité d'API et de protection DDoS de couche 7 dans une seule solution. Cette solution identifie rapidement les vulnérabilités et atténue les menaces qui pèsent sur l'ensemble du réseau et des API.

Akamai Secure Internet Access Enterprise est un DNS (service de noms de domaine) basé dans le cloud. Il permet aux utilisateurs et aux terminaux de se connecter en toute sécurité à Internet, où qu'ils se trouvent, sans la complexité et les frais de gestion associés à d'autres solutions de sécurité.

Akamai Guardicore Segmentation offre un contrôle granulaire du trafic réseau, garantissant que seul le trafic légitime est autorisé.

Les solutions Zero Trust d'Akamai en un coup d'œil

Applications et charges de travail

Akamai Enterprise Application Access fournit un accès Zero Trust aux employés, aux sous-traitants tiers, aux partenaires et aux utilisateurs mobiles, où qu'ils se trouvent.

Akamai Guardicore Segmentation offre une visibilité et une compréhension des applications et des charges de travail.

Données

Akamai Secure Internet Access Enterprise fournit un accès sécurisé aux données grâce à des fonctionnalités telles que le filtrage de contenu, la protection avancée contre les menaces et la prévention des pertes de données. Il prend en charge la gestion de l'inventaire des données en empêchant les accès non autorisés et les fuites de données.

Akamai Guardicore Segmentation : la clé de la protection est-ouest

Akamai Guardicore Segmentation est une solution de microsegmentation de pointe, conçue pour aider les organisations, en particulier les agences et services fédéraux, à mettre en œuvre des contrôles de sécurité granulaires dans les environnements sur site et dans le cloud.

Segmentation granulaire des charges de travail et des applications

Contrairement à la segmentation traditionnelle, qui contrôle l'accès au niveau du réseau, Akamai Guardicore Segmentation applique des règles de sécurité au niveau des applications et des charges de travail. Cela garantit que l'accès est strictement limité. Par exemple, dans une agence fédérale, une application de ressources humaines (RH) peut se limiter à communiquer uniquement avec sa base de données RH désignée, empêchant ainsi les cybercriminels de se déplacer latéralement en cas de violation.

Microsegmentation basée sur l'identité

Akamai Guardicore Segmentation applique la segmentation en fonction de l'identité de l'utilisateur et du terminal, plutôt que simplement des adresses IP. Ainsi, l'accès est accordé de manière dynamique en fonction du rôle, du niveau de confiance et de la vérification en temps réel. Par exemple, les sous-traitants et les partenaires tiers peuvent être limités aux systèmes dont ils ont besoin, ce qui réduit les risques d'accès non autorisé.

Application dynamique des stratégies

Akamai Guardicore Segmentation ajuste en permanence les stratégies de sécurité en fonction de facteurs en temps réel, tels que le comportement des utilisateurs, l'intégrité des terminaux et l'activité du réseau. Si une activité suspecte est détectée, comme un volume anormal de transferts de données, Akamai Guardicore Segmentation peut automatiquement restreindre l'accès, bloquer le trafic ou alerter les équipes de sécurité. Cette approche proactive permet de faire évoluer les stratégies de sécurité pour contrer les menaces émergentes.

En intégrant la microsegmentation d'Akamai Guardicore Segmentation, les entreprises peuvent renforcer leur architecture Zero Trust, minimiser les risques et maintenir un contrôle strict des accès sur leurs réseaux.

ÉTUDE DE CAS

Akamai Guardicore Segmentation dans un environnement fédéral

Une agence fédérale a récemment mis en œuvre la solution de microsegmentation d'Akamai pour protéger ses systèmes internes contre les attaques de mouvement latéral. Avant d'adopter Akamai Guardicore Segmentation, l'agence s'appuyait sur une segmentation traditionnelle basée sur le réseau. Cette stratégie offrait une granularité limitée et permettait un accès étendu aux différents segments du réseau. Cela générait donc un risque important de mouvement latéral si une partie du réseau était compromise.

Grâce à Akamai Guardicore Segmentation, l'agence a été en mesure de :

- Mettre en œuvre une segmentation granulaire : en segmentant les charges de travail au niveau des applications, l'agence a réduit le risque de mouvement latéral et s'est assurée que chaque application ne pouvait communiquer qu'avec les ressources dont elle avait besoin.
- Améliorer la visibilité : les outils de visualisation de la solution ont fourni à l'agence une connaissance approfondie de son trafic interne, permettant ainsi aux équipes de sécurité d'identifier et de réduire les menaces potentielles en temps réel.
- Renforcer la sécurité: en intégrant Akamai Guardicore Segmentation à ses systèmes de gestion des identités et de contrôle des accès, l'agence a pu appliquer la stratégie Zero Trust sur l'ensemble du réseau. Elle a pu ainsi s'assurer que l'accès était surveillé en permanence et ajusté dynamiquement en fonction des évaluations des risques en temps réel.

Cet exemple illustre l'efficacité de la solution Akamai Guardicore Segmentation pour renforcer la sécurité du réseau, réduire le risque de mouvement latéral et limiter les autorisations au strict minimum, en toutes circonstances.

Sécurité des API : protection du trafic nord-sud

Akamai propose plusieurs solutions pour garantir la sécurité des API. La plateforme de sécurité des API d'Akamai garantit une visibilité complète sur les interactions des API, et elle détecte et atténue automatiquement les menaces nord-sud en temps réel. Grâce à l'analyse comportementale avancée, les agences et services fédéraux peuvent :

- **Identifier les API fantômes** qui pourraient être exploitées par les pirates.
- **Surveiller les modèles de trafic API** pour détecter les tentatives d'accès non autorisés.
- **Mettre en œuvre la limitation du débit des API** pour empêcher les attaques par abus et par déni de service.
- **Identifier les API oubliées, négligées ou inconnues** pour identifier les voies d'attaque potentielles.
- **Inventorier toutes les API**, indépendamment de leur configuration ou de leur type, y compris RESTful, GraphQL, SOAP, XML-RPC, JSON-RPC et gRPC.

Akamai Secure Internet Access Enterprise est un pare-feu DNS basé sur le cloud qui est conçu pour aider les équipes de sécurité à s'assurer que tous les utilisateurs et terminaux, du réseau et en dehors, peuvent se connecter à Internet en toute sécurité. Il bloque de manière proactive les requêtes DNS malveillantes, notamment les logiciels malveillants, les ransomwares, l'hameçonnage et l'exfiltration de données DNS à faible débit. Secure Internet Access Enterprise réduit la complexité de la sécurité, sans aucun équipement à déployer, gérer et mettre à niveau. La solution est simple et intuitive.

Akamai App & API Protector détecte et déjoue les menaces liées aux API pour les applications et les API exécutées dans Akamai Cloud, et peut bloquer en ligne tout trafic présentant une menace potentielle découverte par Akamai API Security. Lorsqu'elles sont déployées ensemble, les protections des API Akamai offrent une visibilité complète et continue des API et permettent au personnel de sécurité de découvrir, d'auditer, de détecter et de résoudre les problèmes de sécurité des API sur l'ensemble de vos applications.

Capacités transversales offertes par Zero Trust

L'un des principaux défis liés aux architectures Zero Trust est le risque de créer des silos technologiques. Chaque silo fonctionne souvent de manière indépendante, ce qui entraîne la fragmentation des contrôles de sécurité, de l'application des stratégies et de la détection des menaces. Par conséquent, l'intégration sur toutes les couches de sécurité est primordiale.

Pour les agences et services fédéraux qui gèrent des données très sensibles et des infrastructures complexes, cette approche fragmentée peut présenter des risques de sécurité importants. Les pirates peuvent exploiter le manque de visibilité entre les silos (ou piliers) ou tirer parti d'une application incohérente des stratégies sur différents systèmes. Pour atténuer ces risques, les organisations fédérales doivent adopter un modèle de sécurité unifié qui intègre la visibilité, la gouvernance et l'automatisation sur tous les piliers, garantissant ainsi une application cohérente des stratégies de sécurité et limitant les failles exploitables par les cybercriminels.

Pour parvenir à un modèle de sécurité unifié, l'intégration doit se concentrer sur les trois domaines transversaux du modèle de maturité Zero Trust de la CISA : Visibilité et analyses, Automatisation et orchestration, Gouvernance. Ces éléments sont essentiels à la mise en place d'une architecture Zero Trust, dans laquelle les accès et les autorisations sont ajustés dynamiquement sur tous les piliers, en fonction d'évaluations des risques en temps réel.

Visibilité et analyses

La visibilité est essentielle pour détecter les menaces, comprendre le comportement des utilisateurs et appliquer des stratégies de sécurité dynamiques sur tous les piliers. Sans une visibilité totale sur la façon dont les identités, les terminaux, les applications et les données interagissent, les équipes de sécurité sont laissées dans l'ignorance, ce qui rend difficile la détection des comportements anormaux ou des tentatives d'accès non autorisés. Les solutions Akamai offrent une visibilité complète et transversale, couvrant l'ensemble des piliers.

- Akamai Guardicore Segmentation surveille le trafic réseau parmi les charges de travail segmentées, offrant ainsi une visibilité sur le trafic est-ouest et détectant toute tentative de mouvement latéral au sein du réseau.
- Enterprise Application Access fournit des informations sur les modèles d'accès aux applications, en suivant la façon dont les utilisateurs interagissent avec les applications sensibles et en s'assurant que l'accès est ajusté dynamiquement en fonction des données contextuelles.

Grâce à l'intégration de ces fonctionnalités, les agences fédérales peuvent corréler les données sur tous les piliers, ce qui permet d'obtenir une vue unifiée des événements de sécurité. Lorsqu'un utilisateur demande l'accès à une application, les solutions d'Akamai peuvent vérifier non seulement l'identité de l'utilisateur, mais également la sécurité du terminal, le réseau qu'il utilise et le comportement en temps réel de l'application. Cela permet aux équipes de sécurité de détecter les menaces potentielles plus rapidement, de minimiser le risque d'élévation des privilèges et de s'assurer que les autorisations sont ajustées dynamiquement en réponse aux évaluations des risques en temps réel.

Automatisation et orchestration

La réponse aux incidents et l'application de stratégies sur plusieurs systèmes peuvent être des processus manuels, à la fois lents et fastidieux. Avec Zero Trust, les stratégies de sécurité doivent être appliquées de manière dynamique sur tous les piliers, ce qui nécessite un haut niveau d'automatisation et d'orchestration. Ainsi, à mesure que les niveaux de risque changent, les autorisations sont immédiatement ajustées au niveau minimum nécessaire, ce qui réduit le risque d'erreur humaine ou de délai de réponse. Les solutions d'Akamai offrent des flux de travail automatisés couvrant la sécurité des identités, du réseau et des applications.

- Akamai Guardicore Segmentation offre une microsegmentation automatisée, en ajustant de manière dynamique les stratégies de segmentation du réseau en fonction des modèles de trafic en temps réel et des anomalies détectées. Cela garantit que toute activité suspecte au sein du réseau est rapidement isolée, empêchant ainsi tout mouvement latéral.
- Enterprise Application Access automatise l'accès sécurisé aux applications, en s'assurant que les utilisateurs peuvent uniquement accéder aux applications via un proxy sécurisé et que les autorisations sont mises à jour en permanence, en fonction de l'évolution des facteurs de risque.

En automatisant ces processus, les agences et services fédéraux peuvent s'assurer que les stratégies de sécurité sont appliquées de manière cohérente et rapide, réduisant ainsi la fenêtre d'opportunités pour les pirates.

Gouvernance

La gouvernance est la base de toute stratégie de sécurité, en veillant à ce que les stratégies soient appliquées de manière cohérente et que les exigences de conformité soient respectées. Dans un modèle transversal, la gouvernance doit s'assurer que tous les contrôles de sécurité sont alignés sur les principes du Zero Trust. Grâce aux solutions d'Akamai, les agences peuvent mettre en œuvre des politiques de gouvernance couvrant tous les piliers.

- Gouvernance des identités : s'assurer que les contrôles d'accès basés sur les identités sont appliqués de manière cohérente sur les terminaux, les applications et les réseaux, et que les autorisations d'accès sont régulièrement examinées et mises à jour en fonction des évaluations des risques en temps réel.
- Gouvernance réseau : appliquer des stratégies de segmentation du réseau et de surveillance du trafic dans tous les environnements, y compris les infrastructures sur site, dans le cloud et hybrides ; Akamai Guardicore Segmentation permet aux agences de définir des stratégies de segmentation du réseau et de s'assurer qu'elles sont appliquées de manière cohérente dans l'ensemble de l'infrastructure.
- Gouvernance des données : protéger les données sensibles en s'assurant que l'accès est restreint sur la base du moindre privilège et que tous les transferts de données sont surveillés en permanence pour détecter tout accès non autorisé ou toute activité suspecte.

Les technologies d'Akamai sont conçues pour fonctionner ensemble de manière harmonieuse afin de fournir aux agences fédérales une architecture de sécurité entièrement intégrée et transversale, prenant en charge la stratégie Zero Trust.

ÉTUDE DE CAS

Intégration transversale dans une agence fédérale

Une grande agence fédérale était confrontée à des défis importants en matière de stratégies de sécurité fragmentées sur l'ensemble de ses couches d'identité, de réseau et d'application. Différents systèmes étaient chargés de gérer la vérification des identités, l'accès aux applications et la segmentation du réseau, ce qui entraînait une application incohérente des stratégies de sécurité et des failles en termes de visibilité.

En adoptant les solutions intégrées d'Akamai, l'agence a pu :

- **Unifier la sécurité des identités et des applications :** Enterprise Application Access, la solution ICAM (Identity, Credential, and Access Management) d'Akamai, a été intégrée pour garantir que l'accès aux applications était toujours authentifié en fonction des données d'identité en temps réel. Cela a permis à l'agence d'ajuster dynamiquement les autorisations d'accès aux applications en fonction du comportement de l'utilisateur et de l'intégrité du terminal.
- **Appliquer une segmentation dynamique du réseau :** la solution Akamai Guardicore Segmentation a été déployée pour segmenter le trafic réseau en fonction de l'identité et de l'accès aux applications, empêchant les mouvements latéraux entre les systèmes sensibles et garantissant la mise à jour continue des autorisations, en fonction des évaluations des risques en temps réel.
- **Améliorer la visibilité et l'automatisation :** l'agence a utilisé les outils intégrés d'analyse et d'automatisation d'Akamai pour obtenir une visibilité totale sur sa stratégie de sécurité et pour automatiser l'application des stratégies sur tous les piliers.

Suite à l'adoption de ces solutions, l'agence a réduit sa surface d'attaque, amélioré les temps de réponse aux incidents et a parfaitement répondu aux réglementations fédérales en matière de sécurité. Cet exemple illustre l'efficacité de l'intégration transversale pour transformer une architecture de sécurité fragmentée en un modèle de sécurité cohérent et dynamique, prenant en charge la stratégie Zero Trust.

Conclusion

Aujourd'hui, la sécurité Zero Trust n'est plus une option. Il s'agit d'une stratégie indispensable pour protéger les agences fédérales contre les cybermenaces sophistiquées. En mettant en œuvre la microsegmentation, la sécurité des API et de solides contrôles d'identité, les agences et services fédéraux peuvent réduire considérablement les risques tout en assurant la conformité avec les réglementations fédérales en matière de cybersécurité.

Akamai fournit une suite complète de solutions Zero Trust, notamment Akamai Guardicore Segmentation, Akamai API Security et Akamai Secure Internet Access Enterprise. Toutes ces solutions permettent aux agences d'adopter une stratégie de sécurité proactive et adaptative. En faisant appel à l'expertise d'Akamai, les organisations fédérales peuvent accélérer leur transition Zero Trust et garantir leur résilience à long terme en matière de sécurité.

Il est temps pour les agences fédérales d'agir. En intégrant les solutions de sécurité d'Akamai, les agences peuvent atteindre la maturité Zero Trust, atténuer les cyber-risques et protéger les actifs digitaux les plus critiques du pays.

Contactez Akamai dès aujourd'hui pour en savoir plus sur nos solutions de sécurité complètes.