Akamai

LIVRE BLANC

Surmonter les obstacles à la cybersécurité grâce à la segmentation logicielle

Akamai Guardicore Segmentation contribue à améliorer la sécurité des accès et à réduire les coûts liés aux cyberrisques dans le secteur financier européen

Présentation

Le secteur financier est un élément crucial de l'économie de l'Union européenne, et les systèmes financiers sont considérés comme des infrastructures critiques par certains gouvernements et régulateurs européens. Les produits et services fournis par les organisations de services financiers dépendent fortement de la haute disponibilité des systèmes informatiques et de l'accès en temps voulu aux informations fournies par de multiples canaux et parties.

Cependant, les attaques par ransomware et cryptomining ont montré la rapidité avec laquelle les acteurs malveillants peuvent perturber cette infrastructure critique pendant des jours, voire des semaines, et éventuellement s'étendre à des tiers connectés et à des homologues.

Les institutions financières européennes doivent impérativement se doter de capacités digitales de pointe pour être compétitives, acquérir des clients et les fidéliser. Pourtant, les exigences réglementaires croissantes en matière de contrôles de sécurité et de rapports ralentissent considérablement le rythme d'adoption du cloud. Le Règlement général sur la protection des données (RGPD) de l'Union européenne, par exemple, peut imposer des amendes allant jusqu'à 4 % du chiffre d'affaires mondial aux entreprises ne protégeant pas leurs clients.[1]

En outre, des réglementations récentes comme le programme de sécurité des clients de la Society for Worldwide Interbank Financial Telecommunication (SWIFT CSP) et les attentes de la Banque centrale européenne en matière de surveillance de la cyberrésilience (ECB CROE) appellent spécifiquement à une segmentation plus granulaire du réseau.

Les approches traditionnelles de segmentation et les procédures manuelles qui y sont associées ne permettent pas de suivre le rythme de l'innovation technologique, des risques de sécurité accrus et des réglementations de plus en plus strictes.

Les entreprises doivent non seulement adopter de nouveaux outils, mais aussi modifier fondamentalement leurs processus de sécurité et de segmentation pour adopter la simplicité, la transparence et l'automatisation.

Ce document aborde les points suivants :

- Les principaux défis en matière de cybersécurité auxquels le secteur financier européen est confronté aujourd'hui
- Les moyens dont disposent les banques et institutions financières pour faire face à ces risques grâce à une approche rentable et simple de la segmentation
- La manière dont l'approche d'Akamai Guardicore Segmentation aide les entreprises à simplifier leurs processus de sécurité, en réduisant considérablement les coûts et en accélérant la mise en conformité

De nos jours, la cybersécurité est complexe et coûteuse à gérer

Bien que les banques et institutions financières européennes se soient engagées à assurer la sécurité de leur organisation et à protéger les données de leurs clients, il n'est pas facile de renforcer la sécurité dans un monde où les risques évoluent, où l'accès par des tiers est nécessaire et où les exigences de conformité sont nombreuses.

L'augmentation des cyberrisques accroît les pertes monétaires

Les risques associés à la cybercriminalité sont particulièrement graves pour les institutions financières. Le secteur financier se classe déjà au deuxième rang des secteurs dépensant le plus pour lutter contre les attaques, avec un coût moyen de 5,72 millions de dollars par violation de données.[2]

Pourtant, la mise en place de mesures de sécurité rigoureuses est également coûteuse. La mise en œuvre de contrôles de sécurité pour protéger non seulement les plateformes multiples, mais aussi l'accès des tiers, essentiel à la prestation de services, est une tâche complexe. Elle s'accompagne d'une augmentation significative des coûts d'infrastructure et de main-d'œuvre.

La conformité coûte plus cher

Les organisations de services financiers européennes ont constaté une augmentation spectaculaire des coûts, du temps et des ressources globales nécessaires pour se préparer à la conformité et la valider. Tandis que les réglementations contribuent à assurer la stabilité du secteur financier, l'introduction continue de nouveaux mandats de cybersécurité a un impact sur la rentabilité et la croissance en ralentissant la transformation digitale et en exigeant des investissements substantiels.

La pression accrue pour renforcer les règles a commencé avec le RGPD et a été suivie par la directive sur la sécurité des réseaux et des systèmes d'information (NIS), les orientations CROE de la BCE et, plus récemment, la loi européenne sur la cybersécurité. Dans l'ensemble, avec l'ajout des mandats des fournisseurs tels que SWIFT CSP, la mise en conformité signifie aujourd'hui qu'il faut répondre à un grand nombre d'exigences techniques et de reporting.

Par conséquent, tout en modernisant leur technologie, les banques et institutions financières doivent également trouver des moyens de simplifier la gestion et réduire les coûts opérationnels liés à la cybersécurité et à la conformité.

Vulnérabilités en matière de sécurité des interactions entre les tiers et les marchés financiers

La directive révisée de l'UE sur les services de paiement (DSP2), qui vise à améliorer la commodité et la transparence pour les utilisateurs, a amplifié les risques d'accès par des tiers et de compromission des données personnelles. Les homologues des services financiers et les régulateurs exercent également une pression croissante en faveur de l'efficacité et de la transparence des processus commerciaux et technologiques.

Les exigences supplémentaires des clients en matière de sécurité, de mobilité et de nouveaux services ont entraîné une dépendance accrue à l'égard des infrastructures de technologies de l'information et de la communication de tiers, des fournisseurs d'externalisation et de leurs chaînes d'approvisionnement.

Les environnements étant de plus en plus connectés, la protection de tous les types de communications, y compris les transactions interbancaires et intrabancaires automatisées, est devenue une activité mobilisant beaucoup de ressources.

Aujourd'hui, une seule atteinte au centre de données d'une partie pourrait avoir un effet domino, car les attaquants n'auraient qu'à exploiter un seul actif pour se déplacer latéralement entre les parties interconnectées, y compris les institutions financières homologues et les marchés financiers, mettant ainsi en péril la sécurité et la continuité des activités de l'ensemble de l'écosystème européen des services financiers.

Le cloud hybride exige une nouvelle approche en matière de sécurité

Les mandats de conformité, ainsi que les directives de l'Autorité bancaire européenne[3], façonnent les tendances en matière d'adoption du cloud dans le secteur financier. Tandis que l'adoption du cloud est en hausse en Europe, les réglementations ont augmenté la complexité de la migration des systèmes sur site vers le cloud.

C'est pourquoi les entreprises européennes sont plus enclines à conserver leurs fonctions essentielles sur site et à adopter des environnements de cloud hybride plutôt que des environnements entièrement dans le cloud. De nombreuses banques ont également évolué vers l'utilisation de plusieurs fournisseurs de services cloud, ce qui se traduit par une infrastructure multicloud.

Cependant, les organisations ne recherchent généralement pas seulement une sécurité accrue. Elles cherchent aussi à réduire les coûts et à améliorer l'efficacité opérationnelle en modifiant les processus. L'automatisation et la modernisation des processus deviennent la clé du succès.

Relever les principaux défis en matière de cybersécurité grâce à la visibilité et à la segmentation du réseau

Le thème commun à tous ces défis est la nécessité d'isoler en toute sécurité les applications et charges de travail critiques, ce que l'on appelle communément la segmentation. Cela permet aux institutions financières d'assurer une sécurité à l'échelle en fonction des besoins de l'entreprise et de démontrer une approche basée sur le risque, conforme aux exigences réglementaires.

Les anciens pare-feu ne sont pas la solution

Plusieurs raisons expliquent pourquoi la segmentation n'a pas été plus largement adoptée et déployée dans les banques et institutions financières européennes.

Maintenance et intensité des ressources : de nombreux professionnels de la sécurité et de l'informatique hésitent à poursuivre les initiatives de segmentation, estimant qu'elles prennent trop de temps et mobilisent de nombreuses équipes et d'énormes quantités de ressources. Cette hésitation est compréhensible, car les méthodes traditionnelles ont tendance à être à la fois compliquées et chronophages. Prenons l'exemple de la configuration de réseaux VLAN, d'ACL (access control lists, ou listes de contrôle d'accès) et de pare-feu sur plusieurs sites et environnements. Le processus est souvent laborieux, lent et faillible. En outre, les méthodes traditionnelles s'appuient fortement sur des données d'identité peu fiables, comme les adresses IP, qui ont peu de sens et peuvent changer fréquemment.

Manque de visibilité : acculées par le manque de visibilité sur le trafic est-ouest, les entreprises ont du mal à identifier les dépendances intersectorielles et à créer des règles de segmentation qui n'endommagent pas les composants critiques. Même en utilisant des TAP de trafic ou des technologies similaires, la vue résultante manque souvent du contexte et des traductions sophistiquées nécessaires entre les IP et les ports. Dans un environnement dynamique tel qu'une plateforme en tant que service (PaaS), c'est pratiquement impossible.

Dépendance de l'infrastructure : si les charges de travail s'étendent dans le cloud, ce qui est de plus en plus fréquent, le processus devient encore plus compliqué. Placer un pare-feu matériel à chaque point de sortie des données représente un coût prohibitif. D'autres problèmes de gestion se posent en raison de la complexité des configurations de réseau. Ces configurations sont nécessaires pour répondre aux exigences d'environnements diversifiés avec des actifs virtualisés ou hérités en plus du cloud et des conteneurs.

> « Dans certains domaines, le régime réglementaire s'est efforcé de suivre le rythme de l'innovation technologique, mais il en va de même pour les cadres de gestion des risques et de contrôle des entreprises. »
>
> — Financial Markets Regulatory Outlook 2023, Deloitte's EMEA Centre for Regulatory Strategy

Introduire des changements fondamentaux dans les processus

Même les entreprises de services financiers de taille moyenne disposant de quelques centaines de serveurs peuvent générer des milliers d'éléments de règle de segmentation. La gestion manuelle de ces éléments est inefficace, notamment dans les environnements de diffusion automatisée d'applications, à l'aide d'outils comme Jenkins et de cycles CI/CD où le contexte est essentiel.

C'est pourquoi Akamai Guardicore Segmentation va plus loin, en aidant les entreprises à faire passer leurs cycles de création et de mise à jour de règle d'un processus fondamentalement manuel à un processus automatisé.

Avec Akamai Guardicore Segmentation, une fois que le profilage d'une application est automatisé et que toutes les dépendances sont cartographiées, la création et la mise à jour des règles peuvent être transformées en un processus reproductible, où les parties prenantes et les propriétaires d'applications n'ont plus qu'à approuver les règles générées automatiquement. Cela élimine presque totalement le besoin d'intervention manuelle, qui peut considérablement ralentir les projets, et réduit le risque de mauvaise configuration et d'erreur humaine.

La création automatisée de règles maintient leur cohérence structurelle et l'évolutivité de la règle elle-même, ce qui permet d'optimiser le pare-feu.

Accélérer la transformation informatique pour créer un véritable environnement Zero Trust

Les institutions financières ne doivent pas laisser les processus manuels et les ressources limitées les empêcher de réaliser une segmentation à grande échelle. Un véritable environnement Zero Trust nécessite non seulement la technologie adéquate, mais aussi la modernisation des processus de création, modification et maintenance des règles de sécurité.

Les pare-feu basés sur l'hôte ou le logiciel se sont imposés comme une approche simple et rentable de la sécurité au niveau des applications. Cette approche accélère considérablement la mise en œuvre, simplifie la maintenance courante et s'avère au final plus efficace pour atténuer les menaces. Akamai Guardicore Segmentation a été conçu dès le départ pour rendre la segmentation simple, rentable et plus rapide pour les entreprises de toutes tailles.

Il fournit une carte visuelle de toutes les applications du centre de données et de leurs dépendances. Ensuite, les opérateurs de sécurité sont en mesure de créer et déployer des règles de sécurité au niveau du réseau ou des processus individuels pour isoler et segmenter les applications et autres ressources stratégiques. En adoptant une solution logicielle superposée, la segmentation ne dépend plus de l'infrastructure sous-jacente. Elle protège les charges de travail des installations sur site, des systèmes hérités, des machines virtuelles, des conteneurs, des clouds, etc. Des règles peuvent être créées autour d'applications individuelles ou regroupées logiquement, quelle que soit leur localisation. Ces règles déterminent quels composants peuvent ou ne peuvent pas communiquer entre eux, jetant ainsi les bases d'une approche Zero Trust de la sécurité.

Réduire efficacement les cyberrisques et les coûts

Les institutions financières utilisant Akamai Guardicore Segmentation constatent qu'elles peuvent répondre à certaines de leurs préoccupations les plus pressantes en matière de sécurité tout en réduisant leurs coûts dans un court laps de temps :

Réduire les coûts liés aux cyberrisques en appliquant l'hygiène et les meilleures pratiques de sécurité du réseau dans des environnements de plus en plus complexes et interconnectés.

Simplifier la gestion de la conformité grâce à une visibilité contextuelle granulaire et à des règles de segmentation permettant de cartographier et d'isoler rapidement les actifs liés à la conformité et les applications stratégiques. En utilisant un environnement de surveillance unique, une institution financière peut raisonnablement démontrer qu'elle prend des mesures pour sécuriser les actifs critiques, atténuer le risque de fraude et protéger la vie privée des clients.

Protéger l'accès des tiers en imposant des itinéraires pour le trafic des tiers avec une segmentation basée sur l'identité, en isolant les utilisateurs et en les empêchant de se déplacer sur le réseau. Cela renforce la sécurité autour des interactions avec les tiers et les marchés financiers, en empêchant les attaquants de « se poser et de s'étendre » à partir d'un autre système compromis.

Isoler les systèmes de transfert de fonds et de paiement de l'informatique générale pour répondre aux exigences des systèmes de transfert de fonds et de paiement électroniques, notamment SWIFT, qui exigent une séparation stricte des services SWIFT de l'environnement informatique général d'une institution. La segmentation granulaire permet aux équipes informatiques des banques de définir des limites contextuelles (utilisateur, domaine) autour de la « zone » d'un fournisseur de services afin de restreindre davantage l'accès non autorisé.

Migrer vers le cloud rapidement et en toute sécurité en cartographiant les charges de travail et en faisant l'inventaire de toutes les applications stratégiques et de leurs dépendances avant la migration. Les règles de cloisonnement des applications peuvent utiliser ces cartes comme base d'une sécurité cohérente qui suit les charges de travail tout au long du processus de migration. Cette approche permet une migration dans le cloud plus rapide et plus sûre, en assurant les mêmes contrôles de sécurité, quels que soient les changements apportés aux applications ou à l'infrastructure.

Assurer la continuité de l'activité en limitant efficacement les violations grâce à une visibilité granulaire du trafic est-ouest et à des indicateurs de violation permettant d'alerter sur les mouvements anormaux afin d'arrêter les acteurs malveillants avant qu'ils n'exfiltrent des données financières et des données clients sensibles.

Limiter les mouvements latéraux pour réduire les risques. Aujourd'hui, la majorité du trafic des centres de données se déplace latéralement entre les applications (est-ouest), plutôt que d'entrer dans le centre de données depuis l'extérieur (nord-sud). L'établissement de limites internes en cloisonnant les applications et les systèmes stratégiques réduit efficacement la surface d'attaque, en protégeant contre la propagation latérale des attaques et en limitant les dommages en cas d'intrusion.

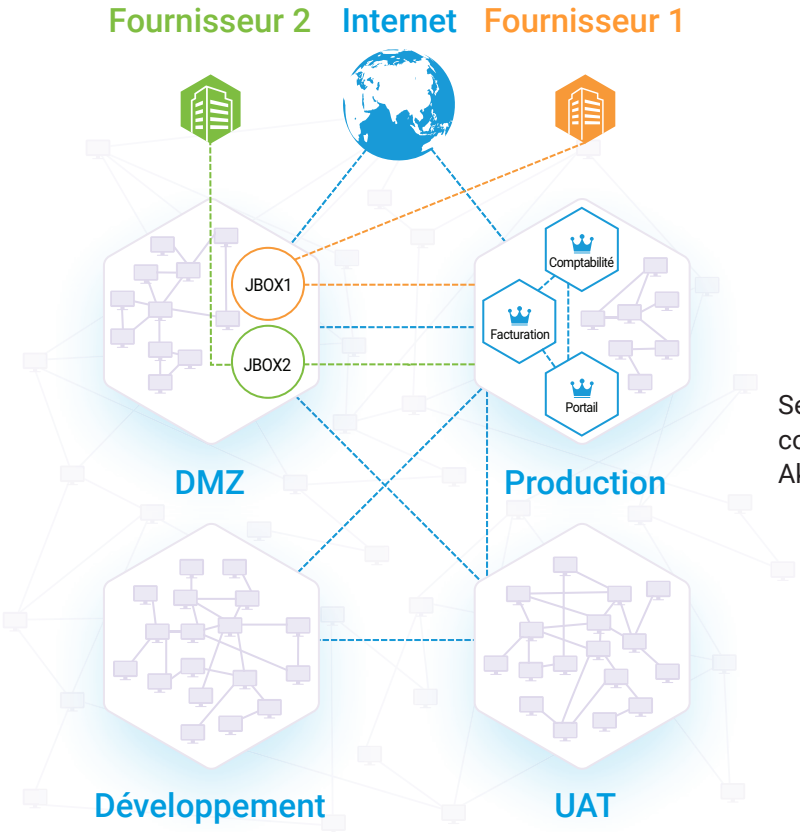
Étude de cas : réduction des coûts de mise en conformité dans une grande banque multinationale européenne

Une grande banque européenne était à la recherche d'une nouvelle approche efficace de segmentation du réseau, nécessaire pour se conformer aux exigences techniques de plusieurs organismes de réglementation, dont la Federal Reserve Bank of NY (FRBNY), la Monetary Authority of Singapore (MAS), la BCE et d'autres.

L'utilisation par la banque d'approches traditionnelles de segmentation, de règles de pare-feu et de VLAN s'est avérée inefficace, entraînant des coûts annuels élevés en termes de non-conformité. Elle avait également un impact sur les opérations informatiques, avec des temps d'arrêt de production importants et la mobilisation des ressources nécessaires à la création et à la mise à jour des règles.

Une approche plus rentable et plus facile à mettre en œuvre était nécessaire pour atteindre les objectifs de segmentation de la banque. La principale exigence de la nouvelle solution était de minimiser l'impact sur l'infrastructure et les ressources de la banque, tout en garantissant une conformité totale avec les réglementations en vigueur.

Après un processus d'évaluation rigoureuse de plusieurs fournisseurs, les décideurs des équipes de sécurité informatique et infrastructure de la banque sont parvenus à un consensus : Akamai Guardicore Segmentation permettait d'emprunter le chemin le plus rapide et le plus simple vers la microsegmentation.



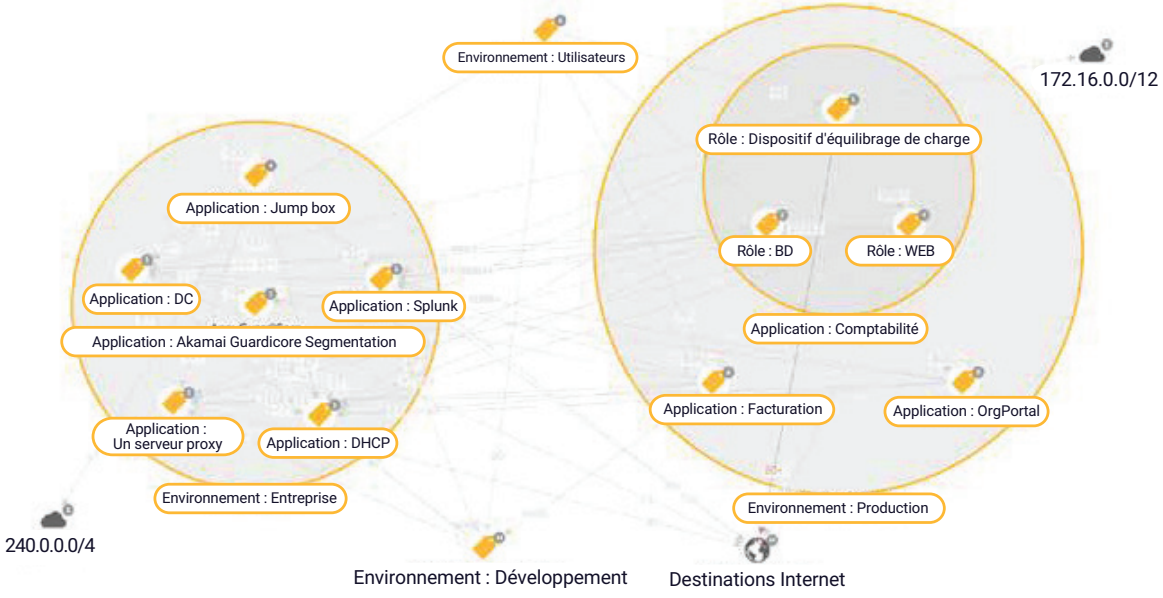
Segmentation de l'environnement et contrôle de l'accès des tiers avec Akamai Guardicore Segmentation

Simplifier et accélérer la segmentation

La banque a déployé Akamai Guardicore Segmentation dans plusieurs régions et types d'infrastructures informatiques, notamment les conteneurs. Comme il n'a pas été nécessaire de modifier les applications, l'environnement de production n'a subi aucune interruption de service. Elle a également permis à la banque d'obtenir rapidement une visibilité centralisée des charges de travail du centre de données et d'isoler les environnements de production, de test et de développement. Grâce à Akamai Guardicore Segmentation, le client a également pu restreindre l'accès aux serveurs des imprimantes, d'autres terminaux IoT et des utilisateurs non autorisés.

En moins de trois mois, le projet était achevé. Il s'est déroulé 10 fois plus rapidement que ce qui avait été initialement estimé avec les méthodes de segmentation traditionnelles. En cartographiant rapidement l'environnement et en créant des règles basées sur les informations collectées, la banque a amélioré sa posture de sécurité et répondu aux exigences de conformité pour plus de 10 000 actifs non conformes. La rapidité du déploiement a permis de réduire les risques et de réaliser d'importantes économies de coûts et de ressources.

L'équipe de services professionnels d'Akamai a aidé la banque à transformer complètement les processus de segmentation. Aujourd'hui, les règles d'étiquetage et de segmentation des actifs sont entièrement automatisées et intégrées aux processus de développement et de déploiement des applications. La création d'étiquettes, la gestion des changements, les incidents de sécurité et les demandes de service sont entièrement intégrés dans les flux de travail de Service Now. Le client a été extrêmement satisfait des résultats de la plateforme et de la valeur qu'elle a apportée, ainsi que des équipes de services techniques qualifiées et dévouées d'Akamai.



Pour en savoir plus sur Akamai Guardicore Segmentation, rendez-vous sur akamai.com/guardicore

1 « What are the GDPR Fines? » GDPR.eu, 13 février 2019.

2 « Cost of a data breach 2022 », IBM.

3 « A comprehensive guide to cloud adoption in Europe's banking sector », Techerati, 31 octobre 2019.

Akamai protège votre expérience client, votre personnel, vos systèmes et vos données en vous aidant à intégrer la sécurité dans tout ce que vous concevez, quel que soit l'endroit où vous le développez et où vous le diffusez. 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 sécurité, de traitement et de diffusion d'Akamai, consultez akamai.com et akamai.com/blog, ou suivez Akamai Technologies sur Twitter et LinkedIn. Publication : 06/23.