Akamai

LIVRE NUMÉRIQUE

Surmonter les obstacles au déploiement pour protéger les systèmes critiques de santé et de sciences de la vie

Rapport global sur l'état de la segmentation

Table des matières

Introduction

Aujourd'hui plus que jamais, les technologies de l'information dans le secteur de la santé ont une incidence en coulisses, au niveau du conseil d'administration et de la salle d'examen. Les violations de données de haut niveau augmentent en termes de gravité et de fréquence, avec des conséquences massives sur la réputation et les opérations. Alors que les acteurs malveillants utilisent des tactiques de plus en plus sophistiquées et, dans de nombreux cas, unissent leurs forces, les dangers auxquels est confronté l'écosystème des soins de santé sont de plus en plus fréquents et de plus en plus graves. Compte tenu du volume important de technologies existantes, de la valeur financière des données des patients et des défis liés à la numérisation rapide et à l'expansion de l'Internet des objets médicaux (IoMT), cet environnement dynamique doit sécuriser son infrastructure, son organisation, ses applications et ses API d'une manière que personne n'aurait pu imaginer il y a seulement cinq ans.

Comme le montrent les conclusions du présent rapport, les cyberattaques accentuent la pression sur les leaders de la sécurité pour qu'ils choisissent les bonnes solutions dans un secteur où la disponibilité continue est une question de vie ou de mort.

Les personnes interrogées dans les organismes de soins de santé et de sciences de la vie aux États-Unis, en Amérique latine, en Europe, au Moyen-Orient, en Afrique et en Asie-Pacifique s'accordent en grande majorité sur l'efficacité de la segmentation pour assurer la protection des actifs. Mais elles indiquent également que les progrès réalisés dans le déploiement de la segmentation autour des applications et des actifs critiques de l'entreprise sont loin d'être parfaits. Les personnes interrogées (y compris les prestataires de soins de santé et les spécialistes des technologies de la santé, ainsi que d'autres entreprises spécialisées dans les services ou produits de santé) déclarent que le principal obstacle pour les organisations du secteur de la santé et des sciences de la vie a été le manque de compétences pour déployer la segmentation. La complexité historique du déploiement des méthodes de segmentation traditionnelles (qui ne couvrent pas les dispositifs médicaux) est aggravée par le fait que les équipes luttent toujours contre le manque de personnel qui a commencé avant la pandémie de COVID-19.

Une enquête de la Healthcare Information and Management Systems Society (HIMSS), organisation américaine à but non lucratif, a révélé que 84 % des experts américains en informatique de santé ont du mal à attirer du personnel et que 67 % d'entre eux estiment qu'il est difficile de le conserver. HIMSS a constaté que la majorité du personnel ne dispose pas d'une formation actualisée sur les menaces actuelles et émergentes.

Et en quoi consisterait cette formation actualisée ? Pour ceux qui avaient segmenté la plupart de leurs actifs critiques, la segmentation s'est avérée avoir un effet transformateur sur la défense, leur permettant d'atténuer et de contenir les ransomwares avec 11 heures d'avance par rapport à ceux qui n'avaient segmenté qu'un seul actif. Imaginez la différence que ces 11 heures représentent pour votre équipe, vos clients et la réputation de votre marque.

Dans l'ensemble, la segmentation a progressé lentement, mais ceux qui ont persévéré ont considérablement réduit leur risque

La segmentation, c'est bien. La microsegmentation, c'est encore mieux.

La segmentation est une approche architecturale qui divise un réseau en segments plus petits dans le but d'améliorer les performances et la sécurité.

La microsegmentation est une technique de sécurité qui permet de diviser de manière logique un réseau en segments de sécurité distincts, jusqu'au niveau de la charge de travail individuelle. Les contrôles de sécurité et la prestation de services peuvent alors être définis pour chaque segment unique.

Les attaques par ransomware et leurs conséquences prennent de l'ampleur

Une comparaison entre les données de 2021 et celles de 2023 montre que le nombre d'attaques par ransomware (réussies ou non) contre les organismes de santé sur une période de 12 mois a augmenté de 162 %. Les conséquences de ces attaques peuvent aller de l'arrêt des opérations, comme l'annulation ou la reprogrammation d'actes médicaux, à des problèmes d'interactions médicamenteuses dus à l'impossibilité d'accéder aux dossiers médicaux, en passant par des détournements d'ambulances vers d'autres établissements de soins de santé.

Augmentation en pourcentage du nombre d'attaques par ransomware au cours des 12 derniers mois, par secteur (données 2021 vs. données 2023)

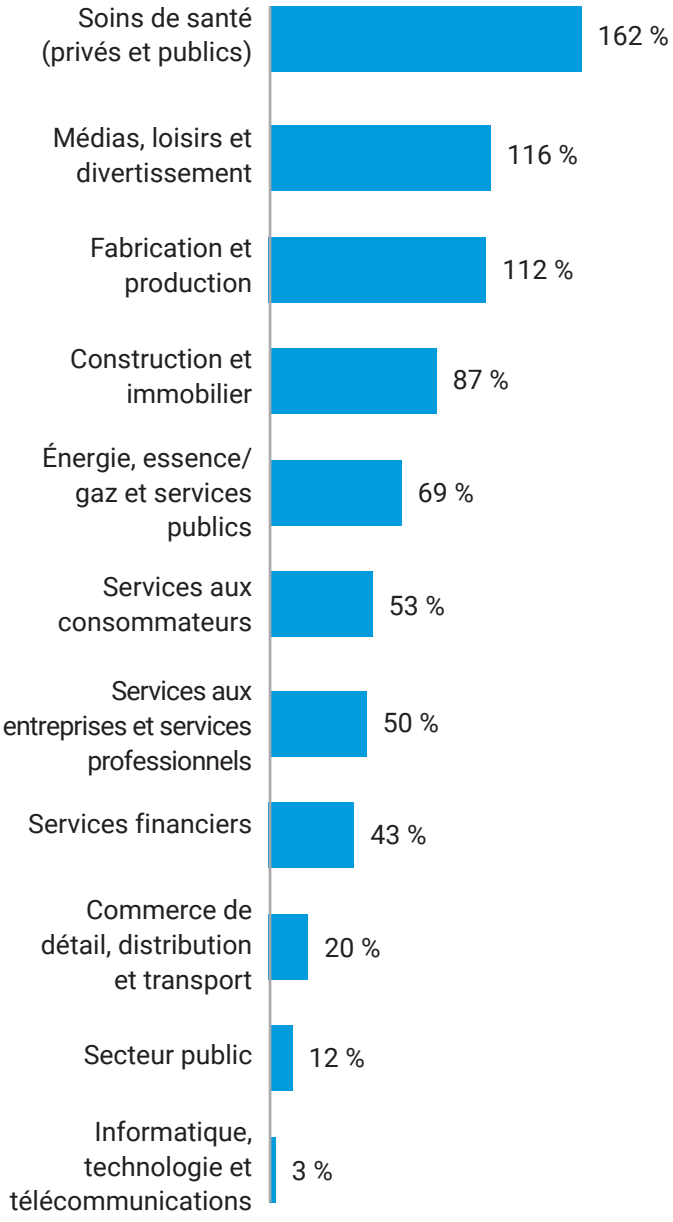

Figure 1 : Combien d'attaques par ransomware votre entreprise a-t-elle subi au cours des 12 derniers mois (qu'elles aient abouti ou non) ? Le graphique reflète la taille de la base constituée de 1 200 personnes interrogées et ne montre que le pourcentage moyen d'augmentation du nombre d'attaques au cours des 12 derniers mois, réparti par secteur.

En moyenne, le taux d'augmentation pour les soins de santé est le plus élevé de tous les secteurs. Cela pourrait indiquer que les organismes de soins de santé – y compris les hôpitaux pour enfants, qui sont également de plus en plus victimes d'attaques – sont moins susceptibles d'être considérés comme « hors limites » par les pirates informatiques.

Les attaques par ransomware contre les organismes de santé sont non seulement plus fréquentes en 2023 par rapport à 2021, mais leurs répercussions causent plus de dommages (figure 2). Les personnes interrogées indiquent en effet une augmentation des atteintes à la réputation, de la perte de fidélité des clients (patients) et des temps d'arrêt du réseau. Tous ces facteurs augmentent considérablement les enjeux pour les équipes de sécurité.

Cette pression a également affecté l'élaboration de stratégies agiles. Le nombre d'organismes de santé qui mettent à jour leurs stratégies ou politiques de cybersécurité au moins une fois par semaine est passé de 17 % en 2021 à 25 % en 2023, non seulement en réponse aux ransomwares mais aussi à une surface d'attaque en constante évolution.

En outre, les organismes de soins de santé sont parmi les plus susceptibles de subir des pertes financières à la suite d'une attaque de cybersécurité, par rapport aux autres secteurs (43 %, contre 36 % dans l'ensemble). Les organismes de santé sont également plus susceptibles de perdre la fidélité de leurs patients/membres à la suite d'une attaque de cybersécurité (48 %, contre 33 % dans l'ensemble). Cela montre qu'à bien des égards, les organismes de soins de santé sont plus exposés que d'autres types d'organismes.

Conséquences des ransomwares/ cyberattaques dans le secteur des soins de santé et des sciences de la vie

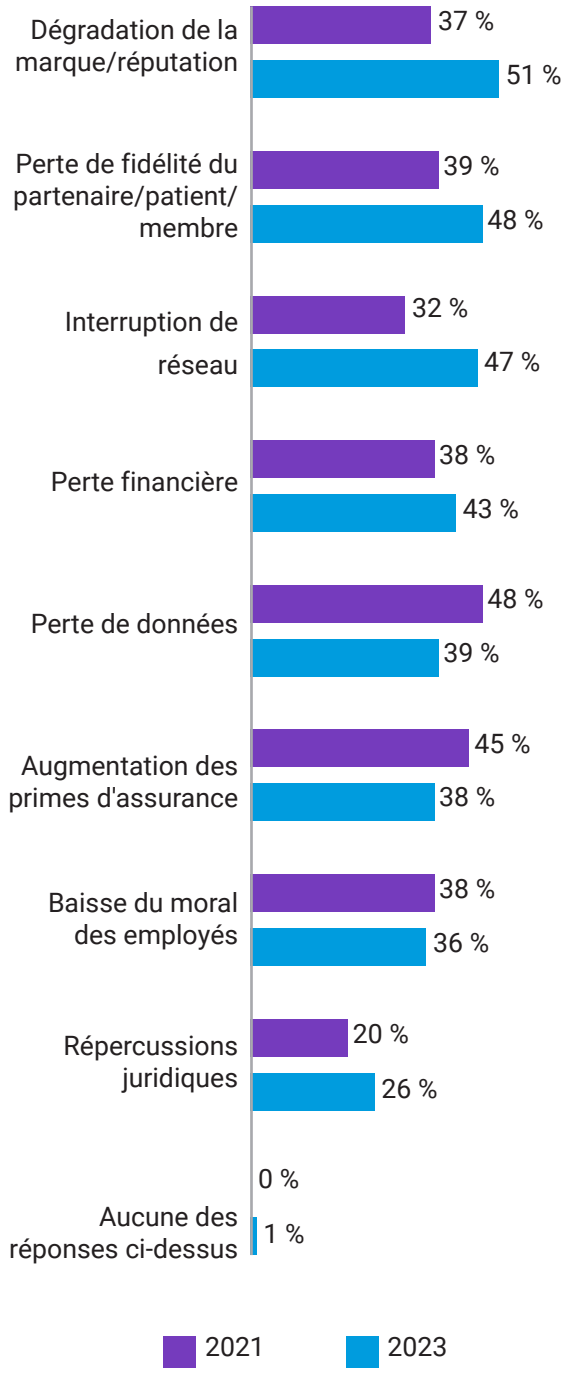

Figure 2 : Lorsque votre entreprise a déjà détecté un ransomware ou une autre cyberattaque, quelles conséquences cela a-t-il eu sur votre entreprise ? Le graphique montre les tailles de base par année, sans afficher toutes les options de réponse, divisé par des données historiques (2021=112, 2023=157), données du secteur de la santé uniquement.

La segmentation est admise comme étant la pierre angulaire de l'approche Zero Trust

Les personnes interrogées dans le secteur des soins de santé et des sciences de la vie s'accordent à dire que la segmentation est importante pour garantir la sécurité de leur entreprise, en particulier pour lutter contre les logiciels malveillants.

Zero Trust est une stratégie de sécurité de réseau en vertu de laquelle aucune personne ni aucun terminal à l'intérieur ou à l'extérieur du réseau d'une entreprise ne doit avoir accès à des systèmes ou à des charges de travail informatiques, sauf en cas de besoin explicite. En résumé, cela signifie aucune confiance implicite.

64 % des personnes interrogées déclarent que la segmentation est extrêmement importante et 94 % pensent qu'elle est essentielle pour déjouer les attaques préjudiciables.

L'adoption de l'approche Zero Trust est souvent motivée par des circonstances indépendantes de la volonté des responsables de l'informatique dans le secteur de la santé. Lorsqu'elles citent les raisons pour lesquelles leur entreprise a lancé un projet de segmentation, un tiers (33 %) des personnes interrogées du secteur de la santé déclarent que c'est parce que leur gouvernement met l'accent sur la cybersécurité et presque autant (29 %) indiquent que c'est parce qu'elles ont déjà été victimes d'une attaque par ransomware.

Cependant, seule une personne interrogée sur trois (34 %) dans le secteur de la santé indique que son cadre Zero Trust est entièrement complet et défini, et donc mature. Ce chiffre est l'un des plus bas de tous les secteurs, certains secteurs (tels que la construction et les services financiers) étant nettement plus susceptibles d'avoir mis en place un cadre Zero Trust mature (53 % et 47 %, respectivement). Aux États-Unis, la maturité du cadre Zero Trust devrait être menée par des organismes de santé (où 50 % déclarent disposer d'un cadre entièrement complet et défini), par rapport aux autres régions (seulement 23 % des autres pays et régions déclarent que leur cadre Zero Trust est entièrement complet et défini). Cela reflète la tendance générale, selon laquelle les entreprises américaines de tous les secteurs d'activité déclarent être victimes de cyberattaques, par rapport à d'autres régions (115 au cours des 12 derniers mois, contre une moyenne globale de 86).

Les organismes de soins de santé sont donc confrontés à des défis en ce qui concerne l'approche Zero Trust. Les personnes interrogées de ce secteur sont plus susceptibles d'avoir rencontré des problèmes liés à la technologie propriétaire lors de la segmentation de leur réseau (41 %, contre 32 % pour l'ensemble des secteurs), et sont également plus susceptibles de rencontrer des difficultés budgétaires lors de la mise en œuvre du cadre Zero Trust (47 %, contre une moyenne de 37 % pour l'ensemble des secteurs). Le soutien d'un partenaire expérimenté peut aider à surmonter certains défis : l'un des aspects les plus difficiles à mettre en œuvre dans un cadre Zero Trust pour les organismes de santé est la charge de travail liée aux applications (68 %, contre 60 % en général) ; un partenaire peut combler les lacunes en matière de compétences, qui ont été signalées par 45 % des organismes de santé.

La majorité des personnes interrogées dans les entreprises de soins de santé souhaite aller plus loin et mettre en œuvre la microsegmentation, qui protège les charges de travail des applications à un niveau granulaire :

92 % des personnes interrogées du secteur des soins de santé déclarent que la microsegmentation est au moins une priorité élevée, 43 % la désignant comme leur priorité absolue. Sur l'ensemble des secteurs d'activité concernés par l'étude, 34 % seulement considèrent la microsegmentation comme leur priorité absolue, ce qui montre que les organisations du secteur de la santé sont plus susceptibles, en moyenne, d'apprécier, et de préconiser, les cadres Zero Trust.

Les déploiements sont lents, mais la persévérance permet d'atteindre des résultats transformateurs

Même s'il est largement reconnu que la segmentation est essentielle pour prévenir les cyberattaques, le déploiement de la segmentation est lent.

Seuls 36 % des organismes du secteur de la santé ont segmenté plus de deux domaines d'activité critiques en 2023, et 43 % ont lancé un projet de segmentation du réseau il y a deux ans ou plus, ce qui laisse supposer que les efforts sont au point mort.

Les domaines critiques

- Applications critiques
- Applications destinées au public
- Contrôleurs de domaine
- Points de terminaison
- Serveurs
- Ressources/données commerciales critiques

Cette lenteur peut être attribuée à plusieurs des principaux obstacles rencontrés par les personnes interrogées dans le secteur des soins de santé : le manque de compétences/connaissances pour mettre en œuvre la segmentation (45 %), l'augmentation des goulots d'étranglement au niveau des performances (tels que ceux causés par la nécessité de résoudre manuellement les erreurs, 44 %) et l'utilisation de technologies propriétaires (41 %, figure 3). Le manque de compétences/connaissances en particulier est un problème pour les organisations du secteur de la santé, plus que pour les organisations de tout autre secteur (pour tous, inférieur aux 45 % du secteur de la santé, la moyenne intersectorielle étant de 39 %). Ces résultats s'alignent sur les conclusions récentes du Ponemon Institute, organisme de recherche de premier plan en sécurité informatique, concernant les menaces qui pèsent sur le secteur des soins de santé. Ces résultats comprennent principalement les ransomwares et les systèmes de compromission par e-mail d'entreprise (BEC). Si la compétitivité des salaires des professionnels des technologies de l'information dans le secteur de la santé est un défi, le volume croissant de besoins réglementaires complexes en est un autre.

Les organismes de santé du monde entier continuent de ressentir les effets de la pandémie de COVID-19 et de la pression qu'elle a exercée sur le capital humain et fiduciaire, ce qui ne fait qu'aggraver les difficultés.

Obstacles rencontrés lors de la segmentation du réseau dans le secteur des soins de santé et des sciences de la vie

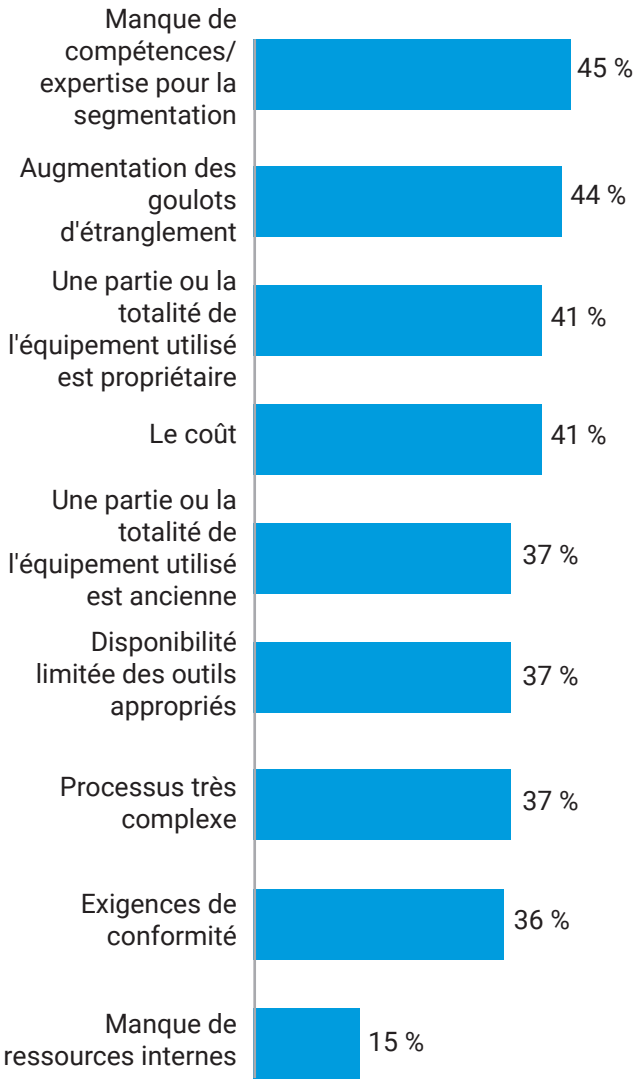

Figure 3 : Le cas échéant, quels problèmes votre entreprise a-t-elle rencontrés/prévoit-elle de rencontrer lors de la segmentation du réseau ? Le graphique montre une taille de base de 157 en 2023, et n'indique pas toutes les options de réponse. Cette question n'a été posée qu'aux personnes interrogées dans les entreprises qui ont segmenté leur réseau à un moment ou à un autre, uniquement dans le secteur des soins de santé.

Malgré la lenteur des progrès, les taux de segmentation augmentent progressivement sur tous les secteurs. Dans le secteur des soins de santé, le pourcentage d'entreprises ayant des applications/données critiques segmentées a augmenté de 20 % et les serveurs segmentés ont augmenté de 18 % entre 2021 et 2023. Bien que ces augmentations soient supérieures à la moyenne générale des augmentations observées dans tous les secteurs d'activité (12 % et 8 % respectivement), les principales vulnérabilités signifient que les taux de segmentation doivent s'accélérer. C'est dans le secteur de la santé qu'il est le plus probable qu'un employé ou un utilisateur basé au bureau soit la raison ou la source de l'accès au réseau par un pirate (47 %, contre 26 % dans l'ensemble), ce qui représente plus du double d'autres secteurs où la conformité est essentielle, comme les services financiers et l'énergie (19 % dans les deux cas). Les conséquences de ces attaques peuvent être limitées grâce à la segmentation, et compte tenu du caractère critique de nombreux systèmes au sein des organismes de soins de santé – des vies étant en jeu – cela démontre l'importance de la segmentation dès que possible.

Enseignements tirés de la segmentation de six secteurs d'activité essentiels

L'amélioration de la visibilité réduit les risques, ce qui est essentiel dans un secteur peu enclin à prendre des risques. La protection et la segmentation d'un plus grand nombre d'actifs rendent les organismes de santé plus sûrs, ce qui permet aux équipes de sécurité d'identifier plus rapidement les menaces et de réagir beaucoup plus efficacement.

Les conclusions de Vanson Bourne montrent qu'après une violation, la récupération s'effectue 11 heures plus rapidement avec la segmentation. Les chiffres : pour les entreprises du secteur des soins de santé qui ont mis en place une segmentation dans six secteurs critiques, il faut en moyenne trois heures pour stopper complètement une attaque par ransomware ; pour celles qui ont mis en place une segmentation sur un seul actif, il faut 14 heures.

De même, la segmentation permet de gagner 11 heures en limitant les mouvements latéraux. Pour les entreprises qui ont mis en place une segmentation dans les six secteurs critiques, il faut en moyenne trois heures pour limiter de manière significative le mouvement latéral d'une attaque par ransomware. Pour celles n'ayant segmenté qu'un seul actif, cela prend en moyenne 14 heures.

Pensez à la différence que cela représente pour votre équipe, les dommages causés à la marque et les coûts encourus pendant ces 11 heures dans l'un ou l'autre scénario.

Pour arrêter une attaque
3 heures

C'est le temps qu'il faut, en moyenne, pour arrêter complètement une attaque par ransomware, lorsque les six actifs de l'entreprise ont été segmentés. Lorsqu'un seul actif a été segmenté : **14 heures**

Pour limiter les mouvements
3 heures

C'est le temps qu'il faut, en moyenne, pour limiter de manière significative le mouvement latéral d'une attaque par ransomware, lorsque les six actifs de l'entreprise ont été segmentés. Lorsqu'un seul actif a été segmenté : **14 heures**

Comment une solution de microsegmentation logicielle aide à relever les défis

La microsegmentation permet non seulement une segmentation plus avancée et plus granulaire, mais elle est également devenue plus facile à mettre en œuvre.

Les solutions logicielles, comme Akamai Guardicore Segmentation, peuvent être déployées rapidement sans apporter de modifications physiques au réseau. Il n'est pas nécessaire d'attribuer une nouvelle plage IP aux nouveaux segments ou de se préoccuper de l'emplacement physique des serveurs et des terminaux. Cette solution est donc beaucoup plus rapide et facile à déployer que les approches basées sur l'infrastructure telles que les pare-feu et les VLAN. Et comme la solution ne repose pas sur le système d'exploitation sous-jacent pour l'application des règles, elle fonctionne de manière fluide sur toutes les machines et tous les systèmes d'exploitation : des serveurs dédiés physiques (bare-metal) aux déploiements multi-cloud, des technologies héritées comme Windows Server 2003 aux derniers appareils de l'Internet des objets médicaux (IoMT) et à la technologie conteneurisée. Cela signifie que vous ne gérez qu'une seule solution avec une seule interface pour visualiser et contrôler les connexions établies par différents systèmes d'exploitation et terminaux dans l'ensemble de votre environnement, quel que soit leur emplacement physique.

Comment elle facilite le déploiement

Akamai Guardicore Segmentation génère d'abord un visuel interactif de toutes les connexions établies dans votre environnement, ce qui est un composant essentiel pour surmonter les principaux obstacles au déploiement. En outre, Akamai a intégré dans sa solution des moyens actifs de remédier aux goulots d'étranglement des performances et de respecter les exigences de conformité.

Les goulots d'étranglement en matière de performances ne résultent pas nécessairement d'une contrainte technique exercée sur un système par une solution de segmentation, mais de goulots d'étranglement au niveau au niveau des équipes. Le temps et les efforts consacrés à la segmentation manuelle des domaines d'activité, puis au dépannage manuel de ces domaines en cas de panne, peuvent être considérables. Akamai s'efforce de résoudre ce problème, ainsi que le principal obstacle au déploiement, le manque d'expertise, en réduisant le temps passé à la segmentation manuelle et en offrant un support technique et des services professionnels de premier plan. Nos experts en segmentation vous accompagnent tout au long du processus de déploiement pour vous permettre d'atteindre vos objectifs de segmentation dans l'environnement informatique qui vous est propre.

La prise en charge du déploiement provient également de la solution elle-même : ses recommandations de règles et son étiquetage basées sur l'IA, ainsi que ses modèles de règle prêts à l'emploi pour les scénarios d'utilisation courants permettent d'économiser du temps et des clics, de simplifier le flux de travail, de réduire le temps global de mise en œuvre des règles et d'éviter les erreurs de configuration d'origine humaine. Pour un client, Akamai a livré en seulement six semaines un projet de segmentation granulaire qui devait prendre à deux ans et coûter plus d'un million de dollars, le tout en ne faisait intervenir qu'un seul ingénieur. Le coût global du projet a ainsi été réduit de 85 %, ce qui prouve que la segmentation granulaire peut être déployée rapidement et facilement, sans souffrir de goulots d'étranglement.

Comment la microsegmentation facilite la conformité

De nombreux organismes du secteur de la santé et des sciences de la vie déploient Akamai Guardicore Segmentation pour assurer leur conformité à un certain nombre de directives de conformité nationales et internationales, comme l'HIPAA, le RGPD, la norme PCI DSS et bien d'autres encore. Ces réglementations exigent généralement que les données du champ d'application soient séparées des autres systèmes de votre environnement.

Si l'utilisation de pare-feu et de VLAN peut s'avérer prohibitive, notre solution logicielle vous permet de créer des segments spécifiques pour les données du champ d'application et d'appliquer des règles de communication sur ce qui peut ou ne peut pas accéder à ces données. En utilisant notre carte visuelle avec des vues historiques et en temps quasi réel, vous pouvez attester de votre conformité à ces mandats en montrant physiquement que les données dans le champ d'application ne sont pas accessibles par des utilisateurs et des machines non autorisés.

Persévérez avec la bonne solution et le bon support pour transformer votre posture de sécurité

La segmentation peut être extrêmement difficile à mettre en œuvre. Mais comme le montre ce rapport, ceux qui parviennent à la mettre en œuvre efficacement constatent une réduction massive de leurs cyberrisques. La mise en place d'une segmentation adéquate limite le déplacement latéral des menaces et vous permet de réagir plus rapidement en cas de violation active. Et après une violation, les efforts de récupération sont sécurisés et prennent moins de temps.

Le choix d'une solution conçue pour surmonter les défis courants liés au déploiement de la segmentation, et le partenariat avec les experts qui vous accompagnent tout au long du parcours, vous place dans la meilleure position possible pour transformer votre posture de sécurité. En outre, plus vous segmentez de secteurs d'activité, plus vous faites progresser votre architecture Zero Trust, en réduisant les risques actuels et en assurant une défense de première ligne contre les futurs vecteurs de menace.

À retenir

Les cyberattaquants ciblent de plus en plus les organismes de soins de santé : les attaques par ransomware contre les organismes de soins de santé ont augmenté de 162 % entre 2021 et 2023. À titre de comparaison, le secteur de l'énergie a progressé de 69 % au cours de cette période, et les services financiers de 43 %.

Les personnes interrogées dans le secteur de la santé sont susceptibles de déclarer que leur entreprise a subi des pertes financières à la suite d'une attaque de cybersécurité : 43 % le signalent, alors que ce chiffre est de 36 % pour les personnes interrogées dans l'ensemble des secteurs d'activité.

La segmentation et la microsegmentation sont plus importantes dans le secteur des soins de santé que dans de nombreux autres secteurs : les décideurs en matière de sécurité informatique des organismes de soins de santé (64 %) sont plus susceptibles d'affirmer que la segmentation du réseau est extrêmement importante pour garantir la sécurité de leur entreprise que ceux de nombreux autres secteurs, tels que la construction (58 %), la fabrication (53 %) et le commerce électronique (48 %). Les sentiments des décideurs en matière de sécurité informatique dans le secteur de la santé rejoignent les chiffres des personnes interrogées dans les secteurs des services financiers et de l'énergie (66 % chacun).

Il est peu probable que les organismes de santé soient plus matures en ce qui concerne le déploiement de leur cadre de sécurité Zero Trust : les organismes du secteur de la santé sont peu enclins à dire que leur déploiement Zero Trust est totalement achevé et défini (34 %), contrairement à ceux des secteurs des services financiers (47 %), de l'énergie (46 %) et du commerce électronique (42 %).

Notre panel

Pour l'étude complète, nous avons interrogé 1 200 décideurs informatiques et de sécurité dans dix pays, afin de mesurer les progrès réalisés par les entreprises dans la sécurisation de leurs environnements, en mettant l'accent sur le rôle de la segmentation.

Ils ont été interrogés sur leurs approches de la sécurité informatique, leurs stratégies de segmentation et sur les menaces auxquelles leur entreprise sera confrontée en 2023. Ces informations et ces résultats nous donnent un aperçu de la manière dont les stratégies de sécurité ont évolué depuis 2021 et des domaines dans lesquels il reste des progrès à faire.

Les personnes interrogées viennent du monde entier, notamment des États-Unis, de l'Inde, du Mexique, du Brésil, du Royaume-Uni, de France, d'Allemagne, de Chine, du Japon et d'Australie. Elles provenaient d'organisations comptant plus de 1 000 employés, ainsi que d'un éventail de secteurs et de sous-segments de marché.

Remarque : cet échantillon différait légèrement de celui de 2021. Tailles des échantillons : 2023 : 1 200 personnes interrogées, 2021 : 1 000 personnes interrogées. En 2023, nous avons également interrogé des personnes en Australie, au Japon et en Chine. Les secteurs différaient légèrement de ceux de 2021. En 2023, nous nous sommes particulièrement concentrés sur le commerce digital comme secteur à part entière.

Pour les besoins de ce rapport sur les soins de santé et les sciences de la vie, nous avons analysé les réponses de 157 (2023) et 112 (2021) personnes travaillant dans le secteur. Ces personnes représentent les mêmes pays que ceux du rapport principal (États-Unis, Inde, Mexique, Brésil, Royaume-Uni, France, Allemagne, Chine, Japon et Australie).

L'étude complète comprenait les secteurs supplémentaires suivants : Commerce électronique (190), Services financiers (173), Informatique, technologie et télécommunications (125), Énergie, pétrole/gaz et services publics (94), Industrie manufacturière et production (91), Commerce de détail, distribution et transport (81), Médias, loisirs et divertissement (63), Construction et immobilier (60), Services aux entreprises et professionnels (58), Secteur public (46), Services aux consommateurs (33), Autres secteurs (29).

En savoir plus sur Akamai Guardicore Segmentation

Akamai soutient et protège la vie en ligne. Les entreprises leaders du monde entier choisissent Akamai pour concevoir, diffuser et sécuriser leurs expériences digitales, et aident des milliards de personnes à vivre, travailler et jouer chaque jour. La visibilité de notre plateforme sur les menaces mondiales nous aide à adapter et à faire évoluer votre stratégie de sécurité (activer Zero Trust, bloquer les ransomwares, sécuriser les applications et les API, ou lutter contre les attaques DDoS), vous donnant ainsi la confiance nécessaire pour innover, prospérer et ouvrir le champ des possibles. Pour en savoir plus sur les solutions d'Akamai pour les soins de santé et les sciences de la vie, rendez-vous sur akamai.com/healthcare et akamai.com/blog, ou abonnez-vous à Akamai Technologies sur X (anciennement Twitter) et LinkedIn. Publication : 05/24.

Vanson Bourne est un spécialiste indépendant des études de marché pour le secteur technologique. Sa réputation d'analyse rigoureuse et fiable est fondée sur des principes de recherche stricts et sur sa capacité à recueillir l'avis de cadres dirigeants dans toutes les fonctions techniques et commerciales, dans tous les secteurs d'activité et sur tous les grands marchés. Pour plus d'informations, rendez-vous sur www.vansonbourne.com.