Étude sur l'impact de la segmentation

Santé et sciences de la vie

La segmentation s'impose comme un moyen de défense puissant dans le monde de la cybersécurité. Découvrez comment les entreprises des secteurs de la santé et des sciences de la vie réduisent l'impact des ransomwares, améliorent leur visibilité, préviennent les attaques zero-day et assurent leur conformité.

Les organisations des secteurs de la santé et des sciences de la vie évoluent dans des environnements parmi les plus ciblés et réglementés au monde. Dans ce contexte, une défaillance en cybersécurité ne se limite pas à un problème informatique. Elle affecte la sécurité et la confidentialité de vos patients, votre conformité à la loi HIPAA (aux États-Unis) ou à d'autres réglementations nationales, ainsi que la réputation de votre organisation.

La menace est bien réelle. Selon l'**Étude 2025 d'Akamai sur l'impact de la segmentation**, menée par Phronesis Partners, 76 % des organisations de santé (assureurs, prestataires et domaine des technologies de la santé) ainsi que des sciences de la vie (pharmaceutique, équipements et terminaux médicaux) ont subi au moins une attaque au cours des deux dernières années. Au moins une fois par trimestre, 27 % des établissements de santé et 24 % des établissements de sciences de la vie ont signalé des violations.

L'étude d'Akamai s'appuie sur les réponses de 232 responsables des secteurs de la santé et des sciences de la vie aux États-Unis, en Europe, au Moyen-Orient et en Afrique (EMEA), en Amérique latine (LATAM) et en Asie-Pacifique (APAC). Dans l'ensemble, les résultats sont sans appel : les cybermenaces évoluent rapidement.

Pour renforcer leur résilience, de nombreuses organisations font de la segmentation un pilier central de leur stratégie de sécurité, et beaucoup d'autres prévoient de leur emboîter le pas.

Segmentation et confinement des ransomwares : un lien évident

Dans la quête visant à limiter les déplacements latéraux et à renforcer la sécurité Zero Trust, la segmentation joue un rôle majeur, comme en témoignent les tendances d'adoption. 45 % des organisations de santé et des sciences de la vie ont adopté une segmentation basée sur l'identité, tandis que la **microsegmentation** atteint 36 % dans la santé et 31 % dans les sciences de la vie.

Cette évolution s'explique par les limites des défenses périmétriques traditionnelles face aux ransomwares, aux risques liés aux accès tiers et aux environnements hybrides. Une fois à l'intérieur, les attaquants peuvent se déplacer librement. En liant les contrôles d'accès aux identités et aux charges de travail plutôt qu'à des réseaux statiques, la segmentation permet de contenir les violations, de réduire la surface d'attaque et de mieux protéger les données sensibles, telles que les dossiers patients et la propriété intellectuelle liée à la recherche, assurant ainsi une résilience opérationnelle dans des environnements hautement réglementés.

La plupart des entreprises déploient la segmentation pour isoler les actifs à haut risque (72 % dans les deux secteurs) et **contenir les ransomwares** (61 % dans le secteur de la santé et 65 % dans le secteur des sciences de la vie), ce qui reflète un passage de la simple prévention à la limitation du périmètre d'impact en cas de violation. Les ransomwares ciblant de plus en plus les systèmes sensibles tels que les dossiers des patients, les applications cliniques et les environnements de recherche, les entreprises privilégient des contrôles permettant de maintenir les actifs critiques segmentés du reste du réseau. Il en résulte un confinement plus rapide des attaques, une réduction des perturbations opérationnelles et une meilleure capacité à assurer la continuité des soins et de la recherche, même face à des menaces actives.

Informations stratégiques

45 % des organisations de santé et des sciences de la vie utilisent une segmentation basée sur l'identité

Confinement des ransomwares **31 %** plus rapide dans les sciences de la vie grâce à la microsegmentation

33 % des professionnels de santé déclarent que la segmentation réduit le coût de l'attestation et de la mise en conformité

Les trois principaux défis de la mise en œuvre :

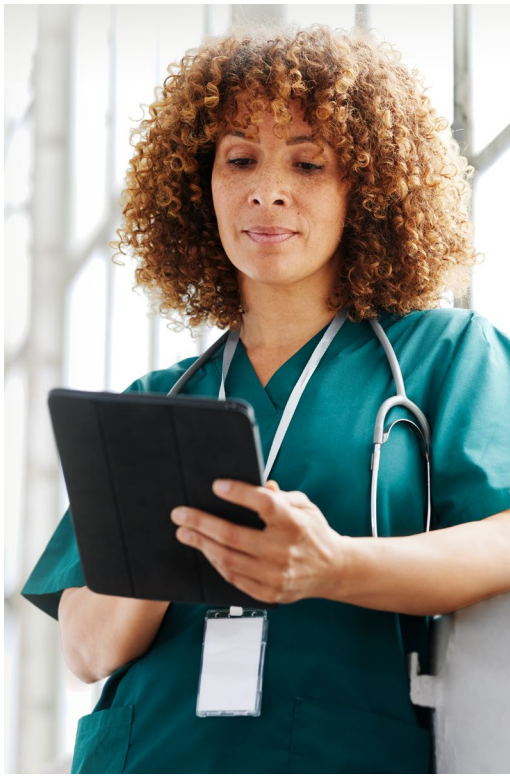
1. Complexité du réseau
2. Coût
3. Résistance organisationnelle

Akamai

La segmentation protège le plus souvent :

- Les points de terminaison (91 % dans la santé et 89 % dans les sciences de la vie)
- Les applications critiques pour l'activité (81 % dans le secteur de la santé et 82 % dans les sciences de la vie)
- Les serveurs (75 % dans le secteur de la santé et 61 % dans le secteur des sciences de la vie)
- Les contrôleurs de domaine et l'infrastructure d'identité (64 % dans la santé et 58 % dans les sciences de la vie)

La segmentation a un impact mesurable. Dans le domaine des sciences de la vie, les entreprises signalent une réduction de 31 % du temps nécessaire pour arrêter une attaque par ransomware. Les organisations du secteur de la santé font état d'une réduction de plus de 4 %. Si la durée varie, le constat est clair : la **segmentation** permet de contenir les menaces plus rapidement.



Comment les organisations mettent en œuvre la segmentation

La segmentation ne remplace pas les programmes de sécurité existants. Elle devient une couche critique au sein de ces dispositifs. Presque toutes les organisations de la santé et des sciences de la vie s'appuient déjà sur des pare-feux et des VPN, mais ces outils ne suffisent pas à empêcher les mouvements latéraux une fois qu'une menace a pénétré le système. Cette lacune alimente l'intérêt croissant pour la segmentation, malgré des freins persistants liés à la complexité, aux coûts et à la résistance organisationnelle.

La dynamique en faveur des approches de segmentation s'intensifie. Près de la moitié des organisations de santé (47 %) et plus de la moitié dans les sciences de la vie (53 %) prévoient de mettre en œuvre la microsegmentation dans les deux ans, et parmi les utilisateurs actuels, une large majorité augmente les budgets.

De toute évidence, les organisations reconnaissent que, sans segmentation, les violations sont plus difficiles à contenir et plus coûteuses à surmonter. L'impact se traduit par un passage d'une sécurité réactive à une approche axée sur la résilience : la segmentation limite le périmètre d'impact des attaques, protège les systèmes critiques et réduit les temps d'arrêt, ce qui en fait un investissement non seulement en sécurité, mais aussi en continuité d'activité.

Cyberassurance et conformité : un levier pour améliorer votre rentabilité

La segmentation influence également les coûts d'assurance et de conformité, des domaines qui ont un impact direct sur votre résultat net. Pour 35 % des organisations de santé et 28 % de celles des sciences de la vie, la segmentation est désormais obligatoire pour renouveler une cyberassurance.

Même lorsqu'elle n'est pas exigée, 57 % des répondants du secteur de la santé et 63 % de ceux des sciences de la vie indiquent que les assureurs la considèrent favorablement. 75 % des répondants du secteur de la santé et 77 % de ceux des sciences de la vie estiment que la segmentation améliore les chances d'acceptation des sinistres.

Elle présente également des avantages en matière de conformité. Elle apporte même des bénéfices financiers : 33 % des organisations de santé et 35 % de celles des sciences de la vie déclarent réduire les coûts de conformité grâce à la segmentation.

Faciliter la mise en œuvre de la segmentation

À mesure que les ransomwares évoluent et que la pression réglementaire s'intensifie, de plus en plus d'organisations de votre secteur adoptent la segmentation pour :

- Réduire les délais de confinement
- Renforcer la maîtrise des coûts de conformité
- Améliorer les résultats en matière de cyberassurance

Toutefois, **la mise en œuvre peut sembler complexe**, notamment lorsqu'il faut composer avec les coûts, la complexité et la résistance interne.

Un partenariat avec le bon fournisseur peut vous aider à simplifier le déploiement, à éviter les perturbations opérationnelles et à accélérer les résultats, sans surcharger vos équipes internes.

Méthodologie de recherche

Ce rapport repose sur les données d'une étude exclusive menée par Phronesis Partners pour Akamai en 2025. Il présente les informations recueillies auprès de 232 leaders mondiaux de la sécurité et de la technologie issus des secteurs de la santé et des sciences de la vie, offrant ainsi une vision rare de la façon dont les entreprises approchent la segmentation et évoluent vers la maturité en matière de microsegmentation. Cet échantillon couvre différentes régions et tailles d'organisation, offrant une vue haute résolution des pratiques actuelles, des défis et des priorités émergentes.

Pour consulter le rapport complet et en savoir plus sur les meilleures pratiques en matière de segmentation, téléchargez l'Étude 2025 sur l'impact de la segmentation.

Êtes-vous prêt à échanger sur vos défis en matière de segmentation et sur la manière dont Akamai peut vous aider ? **Demandez une démonstration** d'Akamai Guardicore Segmentation.

Pour en savoir plus sur le moyen d'éliminer les risques dans votre réseau grâce à une segmentation de pointe, rendez-vous sur **akamai.com/guardicore**.

Akamai est l'entreprise de cybersécurité et de cloud computing qui soutient et protège l'activité en ligne. Nos solutions de sécurité leaders du marché, nos informations avancées sur les menaces et notre équipe opérationnelle internationale assurent une défense en profondeur pour protéger les données et les applications des entreprises du monde entier. Les solutions de Cloud Computing complètes d'Akamai offrent des performances de pointe à un coût abordable sur la plateforme la plus distribuée au monde. Les grandes entreprises du monde entier font confiance à Akamai pour bénéficier de la fiabilité, de l'évolutivité et de l'expertise de pointe nécessaires pour développer leur activité en toute sécurité. Pour en savoir plus, rendez-vous sur akamai.com et akamai.com/blog, ou suivez Akamai Technologies sur X (anciennement Twitter) et LinkedIn. Publication : 04/26.