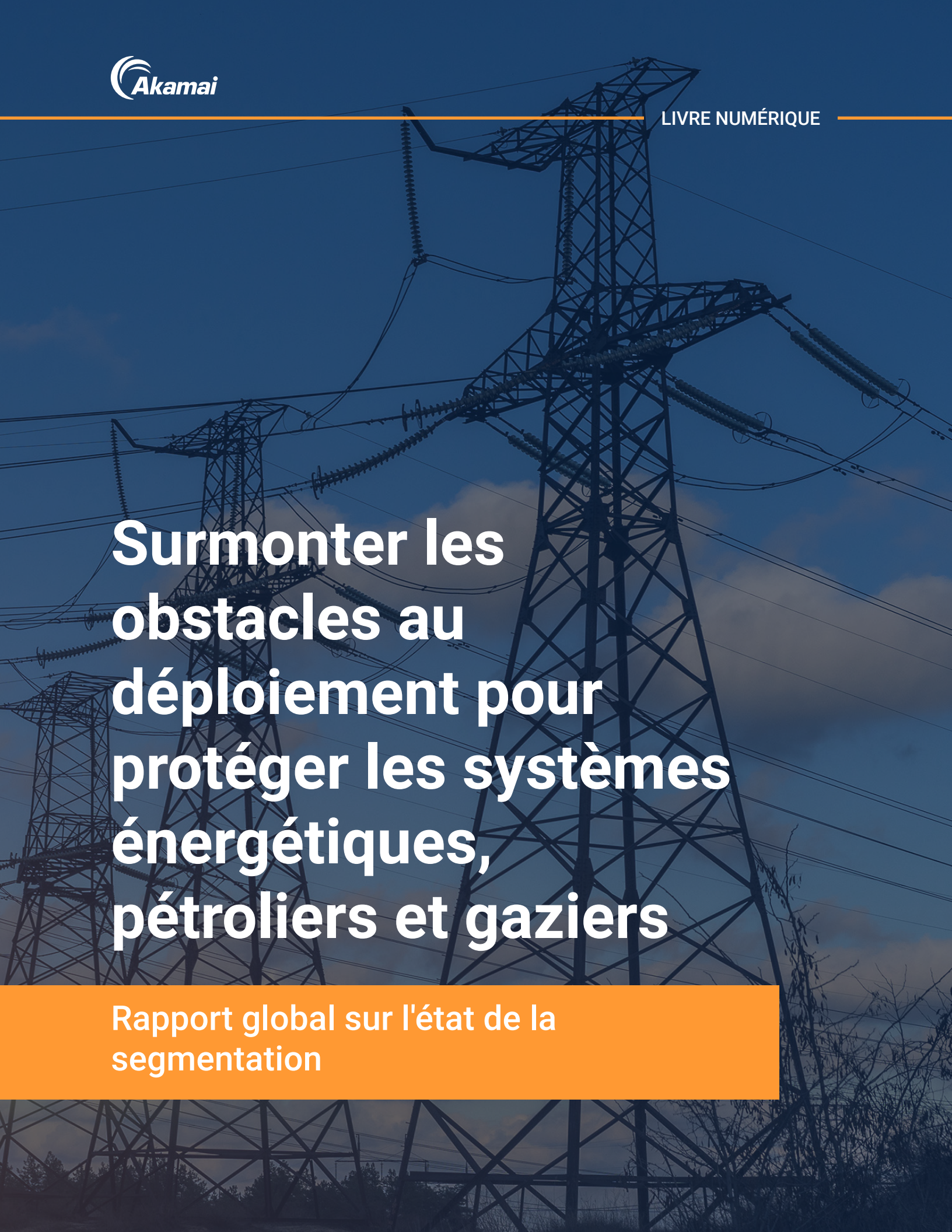
Akamai

LIVRE NUMÉRIQUE



Surmonter les obstacles au déploiement pour protéger les systèmes énergétiques, pétroliers et gaziers

Rapport global sur l'état de la segmentation

Table des matières

Introduction

Les services de sécurité informatique et technique ont toujours été confrontés à des défis importants, mais dans les secteurs de l'énergie, du pétrole et du gaz, et des services publics en général, la pression est encore plus forte en raison de la nature critique des services publics par rapport aux populations. Souvent, les conflits régionaux, les pressions politiques et les différends idéologiques exacerbent les difficultés et augmentent les dangers auxquels est confronté ce secteur. Cependant, comme les attaquants deviennent plus sophistiqués et combinent des techniques pour présenter des menaces plus importantes et plus fréquentes, les équipes de sécurité des entreprises du secteur de l'énergie sont soumises à une pression sans précédent. Sans systèmes connectés en ligne, ou sans systèmes connectés à ses réseaux privés de technologies opérationnelles, il est impossible pour un organisme œuvrant dans le domaine de l'énergie de fonctionner, et une seule violation réussie peut nuire considérablement à la réputation et à la performance financière de l'entreprise.

Les conclusions de ce rapport indiquent que les répercussions de ces attaques s'intensifient, augmentant ainsi la charge des responsables de la sécurité qui doivent choisir des solutions appropriées pour assurer la sécurité de l'ensemble de l'environnement tout en préservant les performances.

Dans le même temps, les agences de régulation et les gouvernements du monde entier sont en train de formuler des lignes directrices et des réglementations en matière de sécurité, en réponse à l'augmentation substantielle des menaces de cybersécurité rencontrées par ce secteur et à la nature critique des services qu'il fournit. Les entreprises du secteur de l'énergie sont tenues de respecter les normes réglementaires et de garantir l'entretien et la sécurité de leurs services.

Les personnes interrogées dans les entreprises du secteur de l'énergie (représentant toutes les régions, y compris les États-Unis, Amérique latine, EMEA et Asie-Pacifique) s'accordent en grande majorité sur l'efficacité de la segmentation pour assurer la protection des actifs, mais les progrès globaux dans le déploiement de la segmentation autour des applications et des actifs critiques de l'entreprise sont plus faibles que prévu. L'obstacle numéro un pour les entreprises du secteur de l'énergie a été l'augmentation des goulots d'étranglement au niveau des performances, ce qui suggère que les équipes pourraient hésiter à se lancer dans un projet qui pourrait perturber les performances. Il est essentiel de garder à l'esprit que, compte tenu de la nature vitale des services rendus au public par ces entreprises, des perturbations dans la fonctionnalité des solutions peuvent porter préjudice aux clients ou mettre en péril la sécurité de leur personnel de maintenance.

Inversement, il est attendu du secteur de l'énergie qu'il accorde plus d'importance à la segmentation que la majorité des autres industries, ce qui indique que sa valeur est incontestablement reconnue.

La segmentation a progressé lentement dans l'ensemble, 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 logiquement 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. Cette approche granulaire de la sécurité permet un contrôle plus précis de l'accès et de la protection des données sensibles. En mettant en œuvre la microsegmentation, les entreprises peuvent limiter l'impact d'une faille de sécurité et mieux protéger leur réseau contre les cybermenaces avancées. Globalement, la combinaison de la segmentation et de la microsegmentation fournit une stratégie de sécurité complète qui est essentielle pour protéger les actifs critiques dans le paysage des menaces complexe et dynamique d'aujourd'hui.

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

Le nombre d'attaques par ransomware (réussies ou non) dans les entreprises du secteur de l'énergie a considérablement augmenté au cours des deux dernières années, passant de 37 en moyenne en 2021 à 62 en 2023, et il n'y a aucune raison de penser que cette croissance ne se poursuivra pas à court terme. Les impacts peuvent avoir des effets néfastes sur la population et les économies, notamment des pannes d'électricité ou des dommages aux infrastructures, entraînant une perte de crédibilité de l'entreprise, le vol de données commerciales et personnelles, voire des risques pour la vie des personnes. Avec l'augmentation de la fréquence et de la gravité des attaques par ransomware, il est crucial pour les organisations du secteur de l'énergie de protéger leurs systèmes et leurs données. Le non-respect de cette règle met non seulement l'entreprise en danger, mais aussi la sécurité des personnes et des communautés qui dépendent de ces services. Les attaques par ransomware devenant de plus en plus sophistiquées, il est impératif que les entreprises restent vigilantes et proactives dans leurs stratégies de défense afin d'atténuer les dommages et les perturbations potentiels causés par ces menaces malveillantes.

Nombre moyen d'attaques par ransomware au cours des 12 derniers mois par secteur

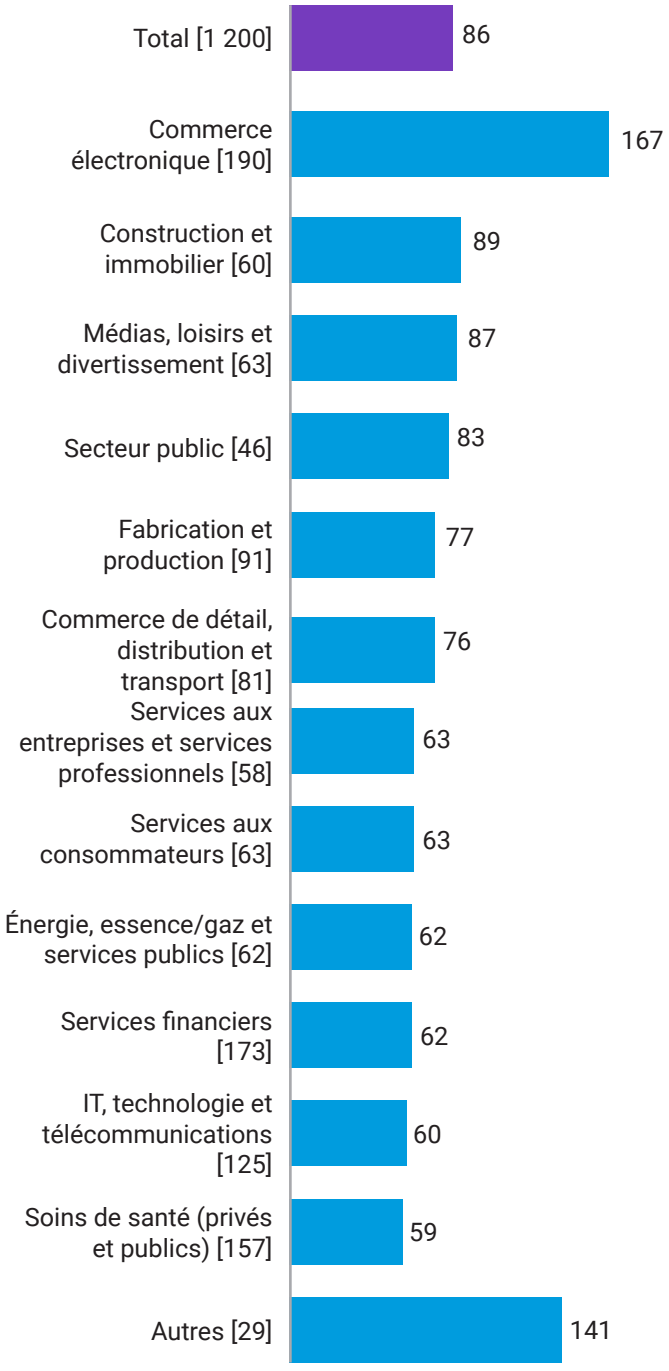


Figure 1 : Combien d'attaques par ransomware votre entreprise a-t-elle subi au cours des 12 derniers mois (qu'elles aient abouti ou non) ? Le graphique montre le nombre moyen d'attaques au cours des 12 derniers mois, les chiffres de base sont répartis par secteur.

L'une des raisons de ce nombre relativement faible d'attaques est que le principal actif d'une entreprise du secteur de l'énergie est généralement physique (pétrole, gaz, etc.) plutôt que numérique (argent ou données des clients). Ces entreprises ne sont pas non plus connues pour être des cibles « faciles », comme peuvent l'être d'autres entreprises relativement peu réglementées, comme dans le secteur des médias ou du commerce de détail. Cela signifie que les attaques sont plus susceptibles d'être motivées par des objectifs politiques que financiers. Ce constat peut être corroboré par le fait que, si seulement 5 % des personnes interrogées, tous secteurs confondus, déclarent que leur entreprise n'a jamais détecté de cyberattaque, ce chiffre passe à 24 % dans le secteur de l'énergie.

Les attaques par ransomware dans le secteur de l'énergie ont été plus fréquentes en 2023 qu'en 2021, mais la gravité de leurs impacts est plus mitigée (figure 2), nos répondants indiquant une augmentation notable des pertes de données, mais des baisses pour tous les autres problèmes. Cette tendance générale peut s'expliquer par la prise de conscience croissante de la valeur des données (qui sont donc considérées comme une cible prioritaire par les pirates informatiques), mais elle peut aussi être due à l'amélioration de l'approche dans le secteur de l'énergie. Le nombre d'entreprises du secteur de l'énergie qui mettent à jour leurs stratégies ou politiques de cybersécurité au moins une fois par semaine est passé de seulement 2 % en 2021 à 23 % en 2023. Les événements mondiaux (principalement liés aux conflits ou au changement climatique) amenant les pays à s'intéresser de plus près à leur sécurité énergétique, il n'est pas surprenant de voir les entreprises du secteur de l'énergie mettre davantage l'accent sur leurs stratégies en matière de cybersécurité.

Impact des ransomware/cyberattaques dans le secteur de l'énergie

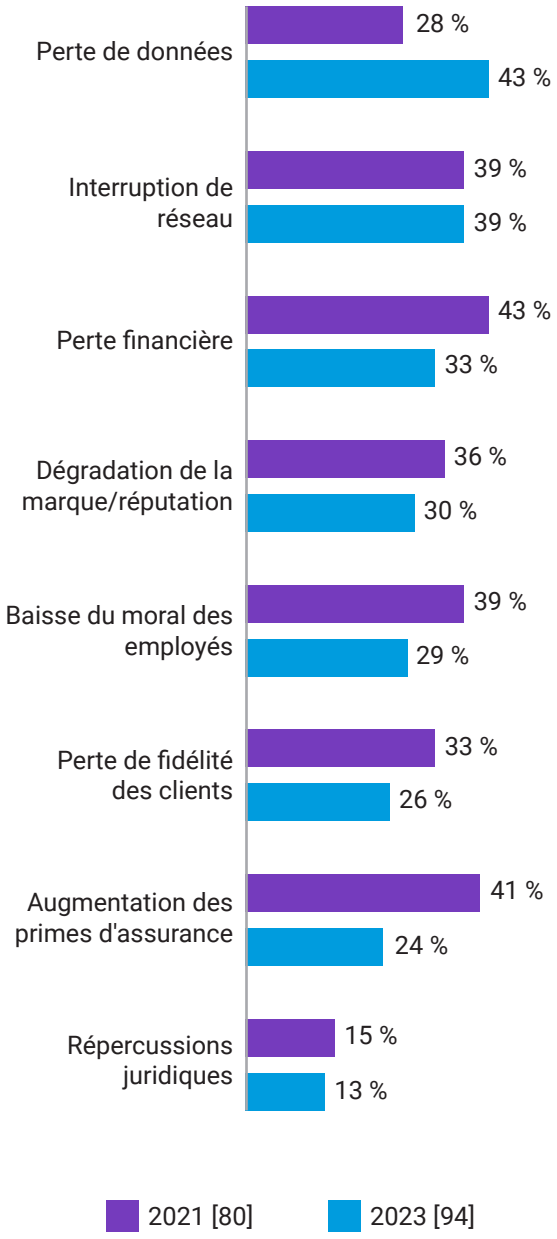


Figure 2 : Lorsque votre entreprise a détecté un ransomware ou une autre cyberattaque, quelles conséquences cela a-t-il eu sur votre entreprise ? Le graphique montre les tailles de base par année, sans afficher toutes les options de réponse, divisé par des données historiques, données du secteur de la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

La segmentation largement reconnue comme une partie importante du Zero Trust

Les personnes interrogées du secteur de l'énergie s'accordent à dire que la segmentation est importante pour garantir la sécurité de leur entreprise, en particulier pour lutter contre les logiciels malveillants. 60 % (un des scores les plus élevés de l'ensemble des secteurs) déclarent que c'est extrêmement important, et 95 % pensent que c'est essentiel pour aider à contrecarrer les attaques préjudiciables.

La segmentation contribue également de manière significative à un cadre Zero Trust, et la bonne nouvelle pour les entreprises du secteur de l'énergie est que des progrès ont déjà été réalisés dans ce domaine. Toutes (100 %) déploient ou ont déjà déployé un cadre de sécurité Zero Trust, bien que moins de la moitié (46 %) déclarent que leur cadre Zero Trust est totalement complet et défini, et donc mature. Il s'agit donc d'un domaine où la segmentation peut aider les entreprises du secteur de l'énergie dans leur adoption du cadre Zero Trust. C'est le résultat de l'enquête pour les environnements informatiques des entreprises, bien que l'environnement de technologie opérationnelle puisse être différent en raison des technologies utilisées.

La majorité des personnes interrogées dans les entreprises du secteur de l'énergie souhaite aller plus loin et mettre en œuvre la microsegmentation, qui protège les charges de travail des applications à un niveau granulaire : 88 % déclarent que la microsegmentation est au moins une priorité élevée, 47 % la désignant comme leur priorité absolue. Tous secteurs confondus, seuls 34 % considèrent la microsegmentation comme leur priorité absolue, ce qui montre que les entreprises du secteur de l'énergie sont plus susceptibles, en moyenne, d'insister pour que cette mesure soit mise en œuvre le plus rapidement possible. En outre, la quasi-totalité (98 %) des décideurs en matière d'informatique et de sécurité dans ce secteur indiquent qu'elle a été adoptée par au moins une minorité de leur secteur, ce qui montre bien qu'il s'agit d'une solution qui bénéficie d'une large notoriété.

Les déploiements sont lents, mais persévérer donne des résultats transformateurs

La dure réalité : même si l'on s'accorde largement à dire que la segmentation est la clé pour stopper les attaques, le déploiement de la segmentation a été plus lent que ce que l'on pouvait attendre. Seulement 38 % des entreprises du secteur de l'énergie ont segmenté plus de deux secteurs d'activité critiques en 2023 (contre 30 % en 2021), et 33 % ont lancé un projet de segmentation du réseau il y a deux ans ou plus, ce qui suggère que les efforts en la matière ont stagné.

La lenteur des déploiements s'explique le plus clairement par les principaux obstacles rencontrés par les personnes interrogées : goulots d'étranglement accrus au niveau des performances (49 %), exigences de conformité (43 %) et équipement propriétaire (41 %, figure 3).

Obstacles rencontrés lors de la segmentation du réseau dans le secteur de l'énergie

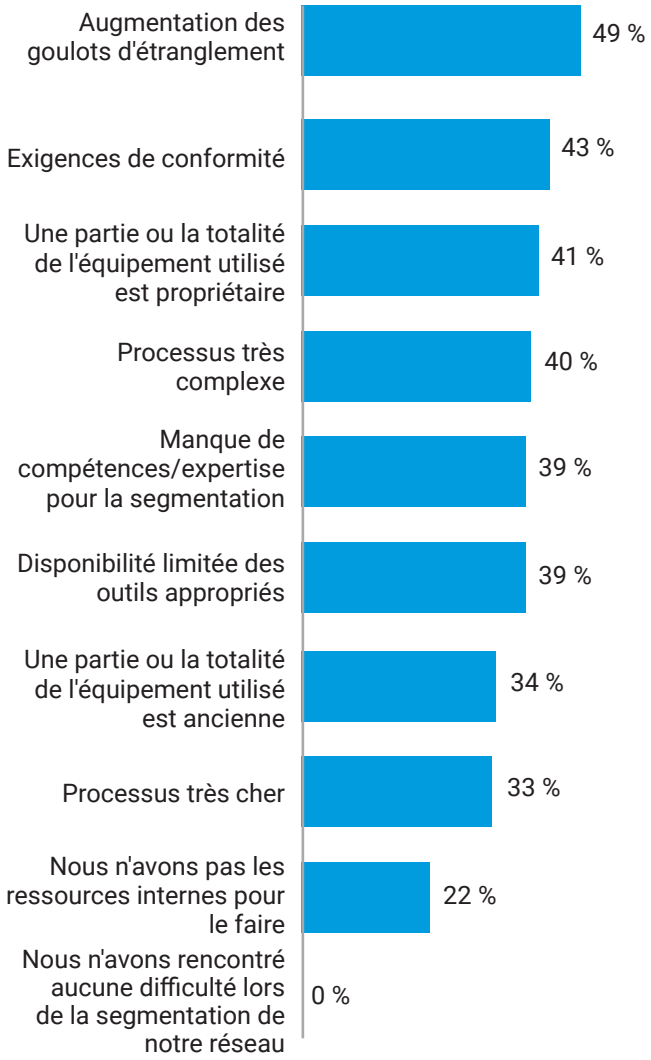


Figure 3 : Quels problèmes, le cas échéant, votre entreprise a-t-elle rencontrés/prévoit-elle lors de la segmentation du réseau ? Le graphique montre une taille de base de 94, et n'indique pas toutes les options de réponse. Cette question n'a été posée qu'aux personnes interrogées dans les entreprises qui ont segmenté leur réseauà un moment ou à un autre, uniquement dans le secteur de l'énergie.

Un fait encourageant pour le secteur de l'énergie, cependant, est que 42 % déclarent que leur projet de segmentation du réseau a commencé à la suite d'une recommandation de la direction ou du conseil d'administration. Ce chiffre est le plus élevé de tous les secteurs (la moyenne générale est de 28 %) et démontre que l'importance de la segmentation est clairement reconnue dans ce secteur.

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 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 à vos nouveaux segments ou de vous préoccuper de l'emplacement physique de vos serveurs et de vos terminaux. Cette solution est donc beaucoup plus rapide et facile à déployer que les approches basées sur l'infrastructure telles que les pare-feux et les VLAN. Et puisque la solution utilise son propre pilote propriétaire 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 multicloud, des technologies héritées comme Windows Server 2003 aux derniers terminaux IoT/OT et à la technologie conteneurisée. Cela signifie que vous ne gérez qu'une seule solution avec une interface unique pour visualiser et gérer les connexions établies par différents systèmes d'exploitation et appareils dans l'ensemble de votre environnement, quel que soit leur emplacement physique.

Il est important de noter que la solution Akamai Guardicore Segmentation peut également être utilisée dans des environnements de technologie opérationnelle ce qui permet d'appliquer la microsegmentation à des réseaux de contrôle privés, à des systèmes opérationnels hérités et à des dispositifs IoT sans agent.

Comment elle facilite le déploiement

La microsegmentation 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 des 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 des équipes, causés par la nécessité de segmenter manuellement les secteurs d'activité, puis de dépanner manuellement ces secteurs en cas de dysfonctionnement. Akamai s'efforce de résoudre ce problème, ainsi que le principal obstacle au déploiement, le manque d'expertise, en réduisant la nécessité de segmenter manuellement 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 ou de technologie opérationnelle qui vous est propre.

La prise en charge du déploiement provient également de la solution elle-même : ses recommandations de règles basées sur l'IA et 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 humaines de configuration. Pour l'un de nos clients, nous avons pu livrer un projet de segmentation granulaire estimé à deux ans et à plus d'un million de dollars de coûts totaux en seulement six semaines avec un seul ingénieur, réduisant ainsi le coût global du projet 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

Nombre de nos clients déploient notre solution pour garantir et attester la conformité à un certain nombre de mandats de conformité nationaux et internationaux, tels que la norme PCI-DSS, la SWIFT, la loi Sarbanes-Oxley, la norme HIPAA, le RGPD et bien plus encore. Ces mandats de conformité exigent généralement que les données du champ d'application soient séparées des autres systèmes de votre environnement. Si l'utilisation de pare-feux 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. En cas de violation, les efforts de récupération sont sûrs et prennent moins de temps, puisque l'impact devrait être limité au seul segment affecté.

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

La segmentation et la microsegmentation sont plus importantes dans le secteur de l'énergie que dans de nombreux autres secteurs : les décideurs en matière d'informatique, de sécurité informatique et de technologie opérationnelle du secteur de l'énergie (66 %) sont plus enclins à dire que la segmentation du réseau est extrêmement importante pour garantir la sécurité de leur entreprise que ceux des services aux consommateurs (36 %), mais moins que ceux du secteur de l'informatique et de la technologie (73 %).

Les décideurs du secteur de l'énergie sont beaucoup plus susceptibles d'affirmer que la microsegmentation est la première priorité (47 %) que leurs homologues des services aux consommateurs (12 %), et à peine moins que celles du secteur public (48 %).

Les entreprises du secteur de l'énergie sont parmi les moins susceptibles de n'avoir procédé à aucune segmentation : les personnes interrogées du secteur de l'énergie sont peu enclines à dire qu'aucun actif critique n'a été segmenté (4 %), bien qu'elles soient plus nombreuses que celles des secteurs de la construction, des services aux consommateurs et des médias (tous 0 %), mais moins nombreuses que celles du secteur public (15 %).

Les personnes interrogées du secteur de l'énergie sont parmi les plus susceptibles d'avoir fait le plus de progrès en matière de segmentation : les entreprises du secteur de l'énergie sont à peine moins susceptibles d'avoir segmenté plus de deux actifs critiques (38 %) que celles du secteur du commerce de détail (43 %) et beaucoup plus que celles du secteur des services aux consommateurs (3 %).

Notre panel

Pour l'étude totale, nous avons interrogé 1 200 décideurs informatiques et de sécurité dans 10 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 des progrès restent à faire.

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

Remarque : cet échantillon différait légèrement de celui de 2021. Tailles du modèle : 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.

Pour les besoins de ce rapport, nous avons analysé les réponses de 94 (2023) et 80 (2021) personnes travaillant dans le secteur de l'énergie.

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 le 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, rendez-vous sur akamai.com 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.