La microsegmentation prend le virage du Zero Trust dans le secteur du commerce

Les entreprises commerciales des secteurs du commerce de détail, du voyage et de l'hôtellerie constituent des cibles attrayantes pour les cybercriminels, les gangs de ransomwares et les fraudeurs désireux de monétiser des données financières ou d'entreprise sensibles. Selon le rapport RH-ISAC Industry Insights, les types les plus courants d'informations ciblées pour le vol comprennent les informations de carte de crédit et de paiement, les informations personnelles identifiables (PII) provenant de programmes de récompense ou de fidélité, et la propriété intellectuelle.

Alors qu'elles sont déjà dans le viseur des attaquants, ces entreprises (et leurs équipes de sécurité) doivent faire face à de nombreux points d'intrusion potentiels dans leur réseau à travers lesquels les acteurs malveillants peuvent déployer des ransomwares et d'autres types de logiciels malveillants. Toutes les entreprises sont confrontées aux retombées des e-mails d'hameçonnage, des vols d'identifiants VPN et des attaques Zero Day, mais de nombreuses entreprises commerciales doivent gérer les risques supplémentaires introduits par les kiosques, les terminaux IoT, les tablettes en magasin, les terminaux de point de vente, le Wi-Fi pour invités, et bien plus encore ! Pour ajouter de la complexité, chaque point de vente, qui doit être ouvert au public pour mener à bien l'activité d'une entreprise, l'expose également à une surface d'attaque physique et à tout un éventail de menaces supplémentaires.

Les données lucratives et les nombreux vecteurs d'attaque augmentent pour les boucliers de protection de l'entreprise l'enjeu de pallier la principale cause d'accidents : l'erreur humaine, qui représente 82 % des incidents de sécurité. Le contrôle réglementaire accru du secteur des cartes de paiement (PCI) ou les réglementations gouvernementales (RGPD, SEC, etc.) ajoutent de la pression et consomment davantage les ressources et budgets de sécurité informatique déjà tendus.

Bien que l'élimination de tous les risques soit impossible, les entreprises commerciales d'aujourd'hui doivent adopter un état d'esprit de « violation présumée » pour détecter rapidement les infections inévitables et arrêter leur propagation ou leur contournement des défenses périmétriques. Les solutions de segmentation Zero Trust d'Akamai facilitent et accélèrent la sécurisation des applications, serveurs et environnements réseau des entreprises commerciales, et empêchent à la fois le chiffrement néfaste et l'exfiltration de données sensibles.

La microsegmentation, une fonctionnalité optimisée par une approche définie par logiciel, constitue la pierre angulaire des cadres de sécurité Zero Trust et propose trois fonctionnalités clés aux organisations commerciales. Tout d'abord, la microsegmentation limite naturellement les retombées potentielles d'une infection par ransomware en bloquant le mouvement latéral. Ensuite, elle peut contribuer à réduire les coûts liés à la mise en place et au maintien de la conformité PCI. Enfin, la microsegmentation offre la visibilité et la couverture granulaires nécessaires pour protéger les écosystèmes d'aujourd'hui, plus complexes, dans les environnements hybrides, multicloud et de microservices, ainsi que dans les infrastructures héritées.

Limitez les retombées potentielles des ransomwares

Un clic sur le lien d'un e-mail d'hameçonnage, des configurations de sécurité erronées, des ports RDP ouverts ou des informations d'identification compromises permettent régulièrement aux attaquants de commencer à explorer le réseau à la recherche des biens les plus précieux de votre entreprise lorsqu'ils se préparent à exécuter une attaque par ransomware. Les entreprises victimes d'un chiffrement massif réussi (et d'une double extorsion rendue possible par l'exfiltration de données) subissent plusieurs niveaux de pertes financières et de dégâts pour l'entreprise.

Si les commandes en ligne et les opérations en magasin sont ralenties ou interrompues, cela peut immédiatement entraîner **des pertes commerciales directes**, les clients ne pouvant pas acheter d'articles ou effectuer de réservations hôtelières ou aériennes. Les opérations de commerce électronique peuvent ne pas être en mesure de traiter, d'exécuter ou d'expédier des commandes existantes lorsque les systèmes et serveurs critiques deviennent inaccessibles ou sont mis hors ligne dans le but de limiter la propagation d'une attaque.

Les pertes commerciales indirectes commencent par l'embarras public et la détérioration de la réputation de la marque si des données sensibles de l'entreprise ou des clients sont compromises. Les gangs de ransomwares ont pour tactique privilégiée de publier les attaques et les fuites de données sur les sites de « name and shame », à la fois comme preuve et comme moyen d'extorquer davantage d'argent à leurs victimes en les pressionnant pour les pousser à payer. Les récentes exigences de la SEC obligent également les entreprises à notifier la SEC dans les quatre jours suivant un impact substantiel sur l'entreprise, ce qui alimente les gros titres et nuit à leur réputation.

Les coûts de récupération pour les frais juridiques, la réponse aux incidents, l'analyse des données et la résolution des violations directement liées à la récupération après attaque par ransomware sont élevés, car les consultants et les équipes informatiques s'emploient à récupérer les données, restaurer les sauvegardes et remettre les systèmes en ligne. Pourtant, même ces dépenses peuvent être dépassées par les frais de litige ou les pénalités et amendes réglementaires engendrées par la violation d'informations sensibles. Les primes de cyber-assurance peuvent augmenter considérablement et les compagnies d'assurance peuvent refuser de verser des remboursements pour les attaques par ransomware, ou ne plus les couvrir.

Les enjeux sont élevés, et il n'est pas surprenant que les attaques par ransomware aient été citées comme la principale préoccupation en matière de risque par les RSSI du secteur du commerce de détail et de l'hôtellerie pour 2024, et que les responsables de la sécurité soient prêts à investir dans des contrôles pouvant aider à réduire les risques une fois que les attaquants ont établi leur ancrage. Mais pour que les ransomwares se propagent, les attaquants doivent pouvoir pivoter et se déplacer latéralement une fois qu'ils ont obtenu un accès initial pour un impact maximal. Le rapport Microsoft Digital Defense 2022 note que 93 % des incidents de ransomware résultaient de contrôles inadéquats des mouvements latéraux qui ont permis aux acteurs malveillants de verrouiller les applications et infrastructures critiques, et que le temps médian pour qu'un attaquant commence à se déplacer latéralement à partir d'un point de terminaison du réseau de l'entreprise est de seulement une heure et 42 minutes.

Les récentes données d'Akamai sur l'état de la segmentation indiquent que les entreprises de commerce électronique ont signalé plus d'attaques par ransomware au cours des 12 derniers mois que les autres secteurs. C'est pourquoi les RSSI et les experts en sécurité se tournent vers des outils de sécurité Zero Trust tels que la microsegmentation pour réduire le risque d'infection par ransomware réussie, minimiser les surfaces d'attaque et « briser » la chaîne d'attaque des ransomwares.

La détection et le blocage de l'exploration par mouvement latéral limiteront la capacité des attaquants à accéder aux actifs informatiques nécessaires pour élever les privilèges, localiser les informations sensibles et propager les attaques par ransomware à grande échelle. En appliquant les principes de l'accès au moindre privilège aux charges de travail critiques sur l'ensemble de l'infrastructure commerciale, la solution de microsegmentation reconnue par les analystes d'Akamai offre une visibilité approfondie sur les flux de données est-ouest des applications et des charges de travail, et une protection granulaire via des règles définies par logiciel pour limiter les mouvements latéraux et empêcher les acteurs malveillants de se déplacer.

Même les grandes entreprises de cyber-assurance comprennent la valeur de la microsegmentation. Les ransomwares génèrent à la fois une hausse des achats et des réclamations ; de nombreux assureurs ont donc été contraints d'augmenter leurs exigences et leurs examens de contrôle de la sécurité, d'augmenter les primes (parfois jusqu'à 96 % d'une année à l'autre) et de réduire les limites de couverture des paiements de rançon pour tenir compte des pertes importantes. Certaines entreprises sont même exclues du marché de la cyber-assurance ou se voient tout simplement refuser une couverture. Bien que la cyber-assurance à elle seule n'empêche pas les intrusions dommageables et les retombées financières qui en découlent, il existe des contrôles de sécurité (comme la microsegmentation) qui permettent aux entreprises de répondre plus facilement aux exigences de souscription les plus récentes.

« Avec un seul agent sur une machine, nous avons résolu pour de bon le problème d'une attaque sur un point de terminaison par mouvement latéral ».

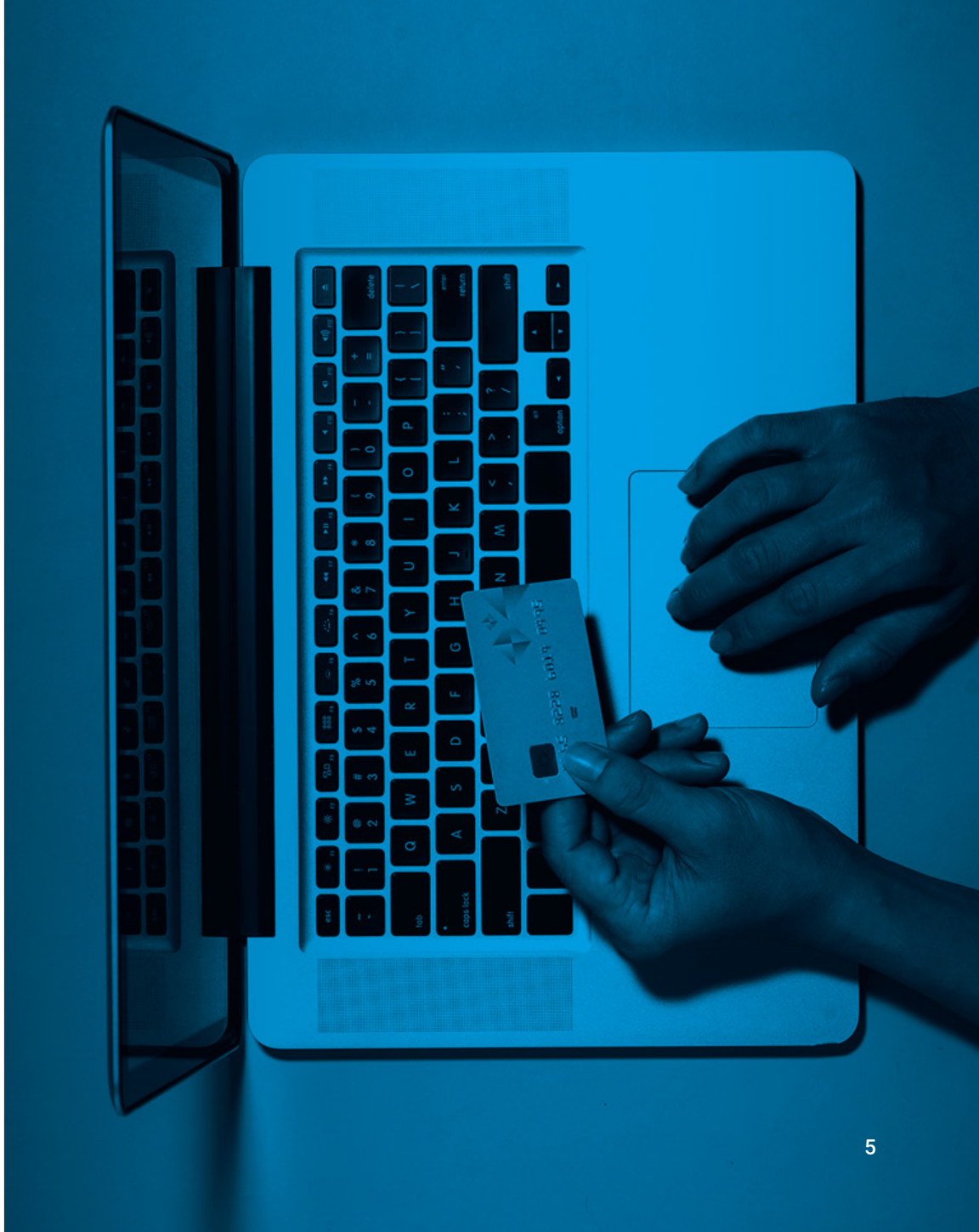
Architecte d'infrastructure,
Fabricant mondial de produits de détail et de biens de consommation

Réduisez la portée des audits de conformité PCI

Comme les entreprises de commerce électronique le savent bien, atteindre et maintenir la conformité PCI représente une part importante des budgets annuels de gouvernance, de risque et de conformité, et peut représenter une charge considérable pour les ETP et les ressources de sécurité. La norme de sécurité des données PCI (PCI DSS) exige des audits continus des politiques et des contrôles de sécurité afin de protéger l'environnement des données des titulaires de carte (EDTC). Le périmètre PCI, qui fait référence à l'identification des personnes, des processus et des technologies qui interagissent avec la sécurité des données des titulaires de carte (DTC) ou qui pourraient avoir un impact sur celle-ci, peut également augmenter considérablement les coûts associés à la réalisation d'un audit PCI.

Bien que la segmentation du réseau ne soit pas une exigence officielle de la norme PCI DSS, les entreprises commerciales utilisent depuis des années des méthodes de segmentation traditionnelles du réseau, telles que les VLAN, les ACL et les pare-feu internes, afin de réduire la portée, les coûts, les risques et les difficultés liés au maintien de la conformité. Cependant, à mesure que les environnements informatiques des entreprises de commerce de détail d'aujourd'hui deviennent plus dynamiques dans les architectures hybrides, multicloud et de microservices, les technologies et techniques de segmentation héritées ne peuvent pas suivre le rythme, entraînant des coûts opérationnels, de la complexité et des temps d'arrêt des applications, ainsi que des failles de sécurité.

En effet, les méthodes de segmentation héritées sont lourdes à gérer et à maintenir, consommant des ressources pour garantir que les systèmes, réseaux et applications situés dans les limites du CDE soient correctement sécurisés et contrôlés. Alors que les entreprises opèrent du centre de données et du cloud vers les ressources basées sur des conteneurs, nombre d'entre elles manquent de visibilité complète sur les flux de communication des applications et des systèmes, et peinent à maintenir les normes de configuration de pare-feu PCI requises.



Cela mène à de mauvaises pratiques de segmentation qui peuvent créer des failles de sécurité et entraîner l'échec d'un audit PCI. C'est pourquoi les entreprises commerciales se tournent vers la segmentation définie par logiciel pour appliquer plus facilement la séparation entre le CDE et les systèmes hors périmètre sur l'ensemble des infrastructures, réduire la portée d'un audit PCI et accélérer la conformité en permettant la segmentation et l'application jusqu'à la couche 7 du processus, ce qui va bien au-delà de ce que les outils hérités peuvent prendre en charge. L'agent léger d'Akamai ne nécessite pas de pare-feu, ni de modification du réseau ou de redémarrage des serveurs, et fonctionne indépendamment de l'infrastructure sous-jacente, ce qui signifie qu'il n'y a pas de temps d'arrêt des applications et qu'il est possible d'éviter les fenêtres de contrôle des modifications ou de maintenance.

La segmentation logicielle dissocie la sécurité de l'infrastructure et des systèmes d'exploitation sous-jacents, de sorte que la segmentation peut être effectuée indépendamment, sans toucher au réseau ou à l'application. En adoptant cette approche, les entreprises commerciales peuvent obtenir une visibilité granulaire sur le réseau et les actifs dans tous les environnements, avec une solution qui agit comme un pare-feu d'inspection dynamique distribué, pour obtenir une couverture complète. En réduisant la quantité d'efforts et de ressources nécessaires au déploiement et à la gestion, les entreprises peuvent améliorer d'environ 95 % la productivité SecOps et renforcer leur sécurité, tout en évitant les nombreux casse-tête liés à la conformité PCI. De plus, notre solution permet aux entreprises commerciales d'exploiter des vues historiques et en temps réel du réseau pour valider la conformité lors des audits.

> « La segmentation définie par logiciel nous a permis de créer et d'appliquer des règles de segmentation au niveau des processus, ce qui a considérablement amélioré notre posture de sécurité et notre capacité à répondre aux exigences techniques de la norme PCI-DSS. »
>
> Ingénieur principal en infrastructure, The Honey Baked Ham Company

Améliorez votre visibilité et votre couverture, de l'IoT à l'infrastructure héritée

De l'interruption de la propagation des ransomwares à la gestion des contrôles de sécurité de conformité PCI, les entreprises commerciales sont également confrontées à la complexité supplémentaire de la sécurisation des emplacements physiques tels que les magasins physiques, les installations de production et les entrepôts de distribution. Pour les compagnies aériennes, les capteurs et terminaux IoT peuvent permettre une surveillance en temps réel et une maintenance prédictive des systèmes aériens afin d'améliorer les performances et la sécurité. Les organisations hôtelières déploient des terminaux IoT pour créer des chambres d'hôtel intelligentes conçues pour améliorer l'expérience client et l'efficacité opérationnelle.

Bon nombre de ces emplacements et environnements contiennent une myriade d'actifs d'Internet des objets (IoT) ou de technologie opérationnelle (TO) qui ne peuvent pas exécuter d'agents de sécurité basés sur l'hôte, ce qui les rend encore plus sujets aux vulnérabilités matérielles et logicielles. Une étude de Forrester, The State of IoT Security, 2023, a noté que 33 % des leaders mondiaux de la sécurité citaient les terminaux IoT comme la cible numéro un des cyberattaques externes. Les entreprises doivent donc déployer une solution de segmentation avec une fonctionnalité sans agent capable de protéger les environnements IoT et TO, et de minimiser le risque qu'un acteur malveillant exploite la vulnérabilité d'un terminal pour tenter d'accéder à l'infrastructure informatique plus vaste.

Ce type de solution doit être en mesure de surveiller en permanence les nouveaux terminaux connectés et d'empêcher automatiquement les terminaux non approuvés de communiquer avec le réseau. Grâce à l'identification intégrée des terminaux, la solution d'Akamai détecte et classe automatiquement les terminaux connectés en groupes logiques qui forment la base de règles de sécurité abstraites et évolutives. Les politiques de segmentation peuvent être créées pour les terminaux IoT et TO via une interface unifiée, et, à l'image des autres politiques, elles suivront les empreintes digitales du terminal, quel que soit l'endroit où il se trouve (même si les terminaux sont déplacés vers de nouveaux emplacements réseau) ou le nombre de terminaux présents dans l'environnement.

Les règles basées sur le Zero Trust sont appliquées via des ACL de commutateurs réseau sans qu'un agent soit nécessaire, éliminant ainsi les lacunes en matière d'application qui peuvent créer des risques sur les déploiements IoT et TO. La définition de ces limites sécurisées permet toujours de disposer des connexions nécessaires aux systèmes de gestion informatique, aux serveurs de mise à jour dédiés et aux serveurs de journalisation afin de réduire les frictions en matière de sécurité. Notre solution vous permet de découvrir, visualiser et cartographier tous les systèmes IoT et TO ainsi que votre infrastructure informatique pour une vue unique sur les actifs de votre entreprise.

En plus de sécuriser les actifs IoT/TO et d'autres points de terminaison isolés (air gap), de nombreuses entreprises de commerce de détail s'appuient sur des systèmes, des serveurs et des applications qui s'exécutent sur des systèmes d'exploitation et une infrastructure hérités ou en fin de support qui ne peuvent pas être corrigés, ce qui crée un risque important. Bon nombre de ces serveurs hérités ne peuvent pas être supprimés car ils génèrent encore des revenus pour l'entreprise ou lui servent d'épine dorsale, en particulier pour les entreprises de commerce électronique qui n'ont pas été conçues pour le cloud. Avec la couverture et la compatibilité les plus vastes du secteur, les agents d'Akamai fonctionnent sur les systèmes d'exploitation récents et anciens, offrant une visibilité totale sur les flux réseau au niveau du processus et du service sous Windows et Linux, ainsi qu'une couverture des points de terminaison MacOS.

D'autres solutions ne fournissent qu'une visibilité partielle pour les systèmes d'exploitation hérités, sans visibilité aucune sur les systèmes Microsoft Windows antérieurs à Windows Server 2008 R2. Cela est dû au fait que l'agent des solutions de microsegmentation traditionnelles repose sur un pare-feu Windows pour appliquer des règles, ce qui n'était disponible qu'avec les systèmes postérieurs à 2002. Les agents pour systèmes Linux prennent en charge la visibilité au niveau de la couche 4 uniquement, sans règles au niveau du processus pour la couche 7 dans les environnements Linux, et dépendent d'iptables pour appliquer leurs règles. Akamai Guardicore Segmentation est pris en charge sur presque tous les systèmes d'exploitation Windows et Linux, nouveaux et anciens, car notre solution ne dépend pas de l'infrastructure sous-jacente pour fonctionner.

Simple, rapide, intuitif... et plus sécurisé

Du siège social au magasin de détail, du centre de données au cloud et au-delà, la microsegmentation est essentielle pour adopter le Zero Trust afin de sécuriser et de protéger les actifs informatiques critiques.

La simplicité d'Akamai Guardicore Segmentation réduit considérablement le temps et le niveau d'effort requis pour le déploiement, l'application, la surveillance et la réponse aux incidents par rapport aux méthodes de segmentation réseau traditionnelles plus lentes. Tout changement de règles peut être mis en œuvre rapidement et ne nécessite pas de modifications complexes du réseau, ce qui peut être critique pendant les périodes de pointe des ventes, les promotions, les lancements de produits ou d'autres événements importants.

Résultats : Tout comme vous ne demanderiez pas à vos clients, invités ou passagers de choisir entre qualité et sécurité, une bonne solution de microsegmentation ne vous demandera pas de choisir entre sécurité et agilité. Il est temps d'arrêter la segmentation à la dure.

Prêt à en apprendre davantage ?

Découvrez comment réduire votre surface d'attaque, sécuriser vos applications critiques et rationaliser la conformité avec Akamai Guardicore Segmentation, qui fait partie du portefeuille de solutions Zero Trust d'Akamai.

En savoir plus

TechnologyAdvice | Akamai

Akamai protège votre expérience client, votre personnel, vos systèmes et vos données en vous aidant à intégrer la sécurité dans tout ce que vous créez, dans toutes vos conceptions et diffusions. 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 de Cloud Computing, de sécurité et de diffusion de contenu d'Akamai, rendez-vous sur akamai.com et akamai.com/blog, ou abonnez-vous à Akamai Technologies sur X (anciennement Twitter) et LinkedIn.