LIVRE BLANC

Atténuation des risques, prévention et coupure de la chaîne d'attaque

Minimisez l'impact des ransomwares grâce à Guardicore Segmentation d'Akamai

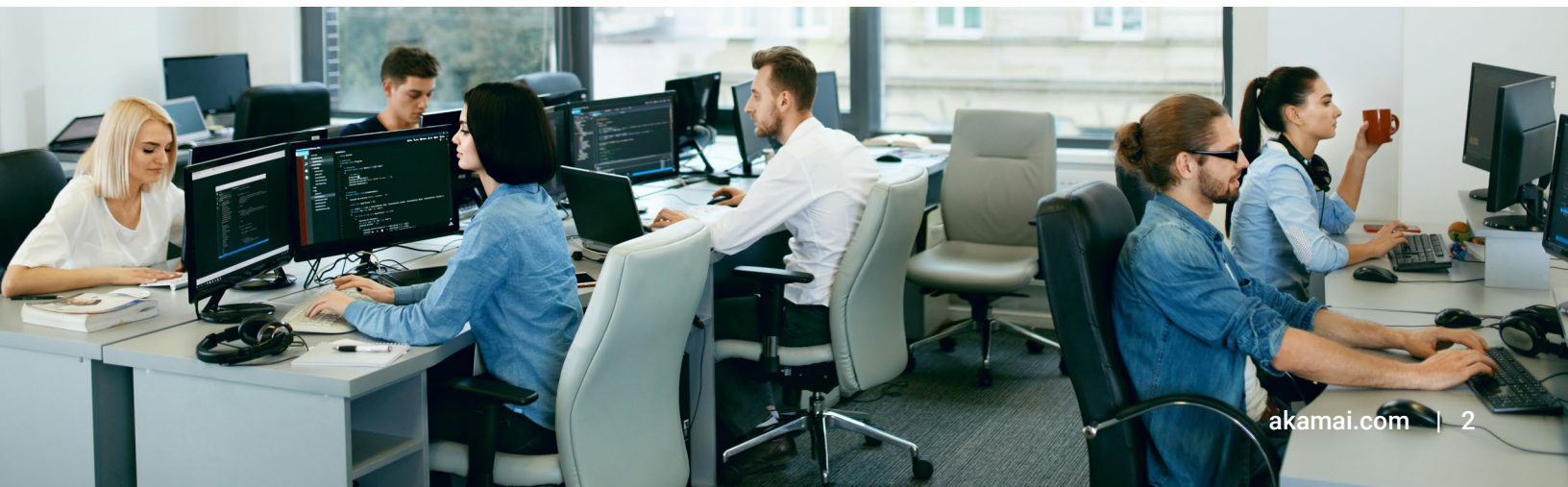
Présentation

Les ransomwares, à l'origine simple variété de programmes malveillants utilisés par les cybercriminels pour restreindre l'accès aux fichiers et aux données par le biais du cryptage, ont pris une ampleur particulièrement inquiétante. Alors que la menace de perte permanente de données est effrayante en soi, les cybercriminels et pirates informatiques ont désormais les moyens d'utiliser les ransomwares pour pénétrer et paralyser les grandes entreprises, les gouvernements fédéraux, les infrastructures mondiales et les organisations de santé.

Le cryptoworm WannaCry de 2017, qui a touché 230 000 ordinateurs dans le monde en exploitant une vulnérabilité de Microsoft Windows, constitue l'évènement marquant très médiatisé des menaces que représentent les ransomwares. Depuis, les pirates ont renforcé leurs outils et les attaques sont de plus en plus répandues. On a notamment pu voir l'émergence du ransomware en tant que service (RaaS), dans lequel les pirates vendent leur service. Le rapport mondial sur les menaces par ransomware d'Akamai au premier semestre 2022 a évalué les schémas d'attaque de Conti, un groupe RaaS bien connu qui a été détecté pour la première fois en 2020 et qui semble être basé en Russie. L'analyse met l'accent sur la nécessité de mettre en place des protections solides contre les mouvements latéraux et le rôle essentiel que ces protections peuvent jouer dans la défense contre les ransomwares. Elle a également constaté que l'écrasante majorité des victimes de Conti sont des entreprises dont le chiffre d'affaires se situe entre 10 et 250 millions de dollars américains.

> **La microsegmentation réduit la confiance tacite dans le réseau en n'autorisant que la connectivité explicitement définie par la règle, imposant ainsi un accès sur le principe du moindre privilège entre les applications pour le trafic de machine à machine.**
>
> **— Forrester, Best Practices For Zero Trust Microsegmentation, 27 juin 2022**

Cela indique clairement que les entreprises de toutes tailles sont menacées à cause de technologies obsolètes, de stratégies de défense considérées comme « suffisantes » axées uniquement sur les périmètres et les points de terminaison, d'un manque de formation (et d'un mauvais protocole en matière de sécurité) et de l'absence d'une solution miracle connue. En fait, le Rapport 2023 'Who's Who' dans les ransomwares de Cybersecurity Ventures prévoit que d'ici 2031, les ransomwares attaqueront une entreprise, un utilisateur ou un appareil toutes les deux secondes.



Tout dépend des mouvements latéraux

Les attaques par ransomware sont lancées à partir d'une brèche initiale, généralement obtenue via un e-mail de phishing, une vulnérabilité dans le périmètre du réseau ou une attaque de force brute créant des ouvertures en concentrant les défenses à distance du véritable point d'attaque de l'attaquant. Une fois que le logiciel malveillant a atteint un terminal ou une application, il poursuit son action par une escalade des privilèges et un mouvement latéral sur le réseau et plusieurs terminaux afin de multiplier les points d'infection et de chiffrement. Les attaquants mettent généralement la main sur un contrôleur de domaine, compromettent les informations d'identification, puis trouvent et chiffrent la sauvegarde pour empêcher l'opérateur de restaurer les services gelés.

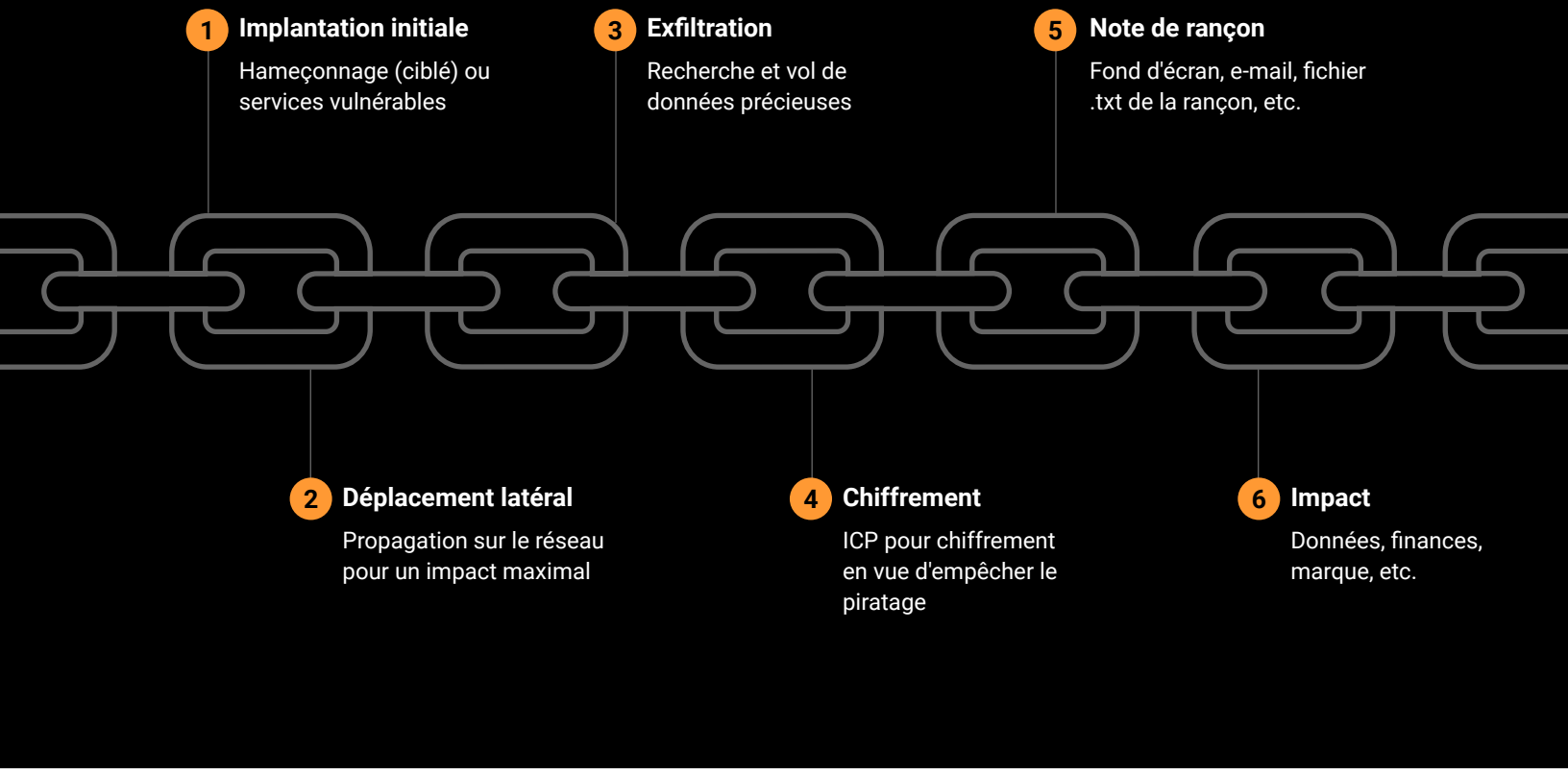
Le mouvement latéral est essentiel à la réussite d'une attaque. Si le logiciel malveillant ne peut pas se propager au-delà de son point d'entrée, il n'a aucun impact ; il est donc essentiel de prévenir les mouvements latéraux. Les fonctions de visibilité et de segmentation d'une solution telle que Guardicore Segmentation d'Akamai vous permettent de mettre rapidement en place des stratégies visant à prévenir et à contenir une violation initiale. Vous serez également alerté des mouvements latéraux et autres comportements suspects pour détecter rapidement les programmes malveillants afin d'être en mesure de réagir immédiatement.

Partie 1 : Stoppez la chaîne d'attaque des ransomwares — atténuation et prévention des risques

Les attaques par ransomware ne se propagent pas en infiltrant une seule machine ou un seul terminal. Les cybercriminels utilisent les ransomwares pour crypter le plus de systèmes possible d'un réseau afin de garantir le paiement d'une rançon.

Étant donné que le ransomware est une attaque à multiples facettes, la mise en œuvre de plusieurs couches de défense peut aider à prévenir les dommages étendus, la perte de données et les temps d'arrêt. La première couche de défense consiste à tenter de prévenir l'infection initiale par le ransomware.

La chaîne d'attaque des ransomwares



Prévention des infections initiales

Les points de contact avec Internet sont les plus vulnérables de tout réseau. Bien que de nombreuses attaques par ransomware reposent sur le harponnage ciblé, rien ne les empêche de compromettre vos services exposés à Internet.

Les fonctions de visibilité de Guardicore Segmentation d'Akamai vous permettent de surveiller les services exposés à Internet et de limiter leur exposition par le biais de stratégies pour :

- les services d'accès à distance (RDP, SSH, TeamViewer, AnyDesk, VPN) ;
- les services potentiellement vulnérables (Apache, IIS, Nginx) ;
- les machines potentiellement vulnérables (détecter les machines avec un système d'exploitation non mis à jour à l'aide de la fonction d'informations supplémentaire) ;
- les services exposés indésirables (bases de données, contrôleurs de domaine, serveurs Web internes ou serveurs de fichiers).

Coupure de la chaîne d'attaque avec la segmentation

Tout réseau sera forcément victime d'une faille de sécurité à un moment ou à un autre. Cela peut être dû, par exemple, au hameçonnage, à des erreurs humaines ou à l'exécution de services vulnérables dont les risques n'ont pas été correctement atténués. C'est pourquoi il est essentiel de mettre en place vos propres stratégies d'atténuation des risques.

Une fois qu'une machine est piratée, il faut limiter la propagation à l'intérieur de votre réseau. Pour ce faire, vous pouvez procéder de trois façons :

1. Segmentation par cloisonnement des applications

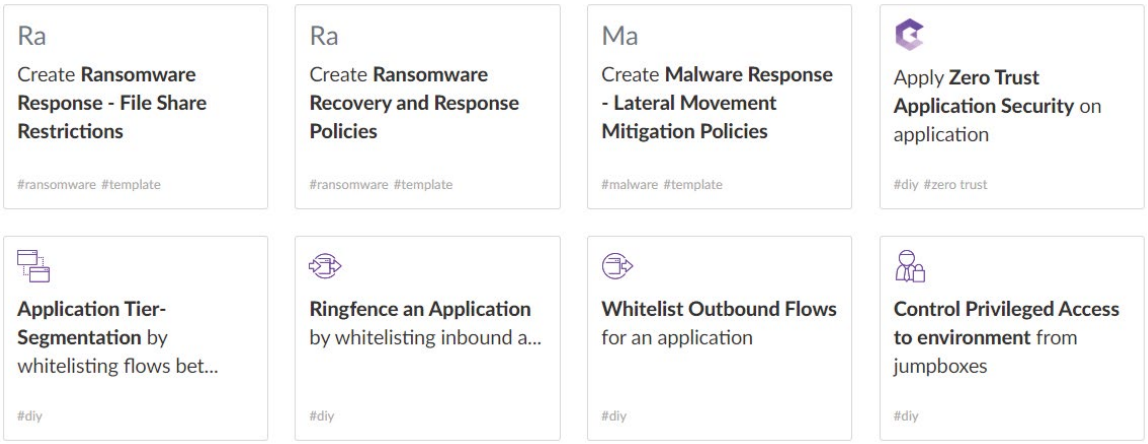
Il faut séparer le réseau en segments opérationnels (par application, utilisation ou environnement) et ne pas autoriser de connexions inutiles entre et au sein de ces segments.

Voici quatre directives de segmentation à prendre en compte :

- Bloquer toute communication entre les ordinateurs portables et les postes de travail.
- Bloquer la communication de processus qui s'exécutent avec des privilèges d'utilisateur de domaine « puissants », comme les administrateurs de domaine.
- Limiter les utilisateurs pouvant exécuter des processus sur vos serveurs.
- Limiter l'accès des ordinateurs portables/postes de travail aux serveurs de centres de données et aux instances sur le cloud.

Guardicore Segmentation d'Akamai vous permet de sécuriser facilement votre réseau contre les ransomwares. Grâce à des modèles prédéfinis, vous pouvez atténuer les attaques en définissant des règles en trois étapes simples :

1. **Sélectionnez votre objectif,** comme le cloisonnement d'une application critique, la création de stratégies d'atténuation des ransomwares ou la sécurisation d'un répertoire actif.
2. **Identifiez les ressources pertinentes à protéger,** comme les ressources d'application de commerce électronique que vous cherchez à cloisonner, toutes les charges de travail de répertoire actif dans le centre de données, ou les terminaux à protéger contre la propagation de ransomwares. Dans de nombreux cas, cette étape est réalisée automatiquement grâce à l'étiquetage IA d'Akamai.
3. **Protégez les ressources en créant des règles.** L'IA de Guardicore Segmentation d'Akamai suggère et recommande automatiquement des stratégies basées sur le trafic réel dans l'environnement, et apprend les schémas de communication des applications sur des centaines de réseaux.

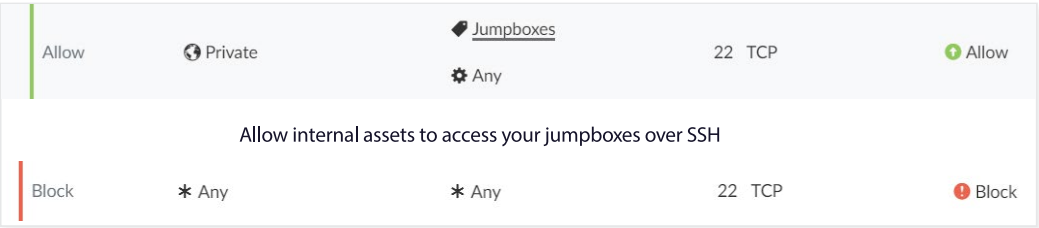


Exemple : Modèles Guardicore Segmentation d'Akamai

2. Prévention des mouvements latéraux avec des règles de restriction de protocole

Il existe des directives générales pour des protocoles et comportements spécifiques. Certains protocoles sont essentiels aux opérations quotidiennes et doivent donc être limités avec précaution. Guardicore Segmentation d'Akamai permet de visualiser tout le trafic afin de créer les règles les plus précises pour votre environnement autour de protocoles à haut risque tels que WinRM, SMB, RPC, RDP, SSH, parmi d'autres.

Par exemple, bien que SSH soit utile pour l'administration à distance et qu'il permette également de sécuriser d'autres protocoles (comme SFTP), il s'agit aussi d'un outil employé par les attaquants pour pirater les machines et propager l'attaque sur le réseau. Il faut limiter autant que possible SSH à l'échelle du réseau en créant des « jump box » pour les utilisateurs autorisés.



Règles créées dans Guardicore Segmentation d'Akamai

3. Protection des sauvegardes et des services de données critiques

Pour maximiser les dommages, les attaques par ransomware ciblent généralement les serveurs de sauvegarde de l'entreprise afin de chiffrer les données stockées. De même, les services de données et les serveurs de fichiers sont une cible privilégiée des ransomwares.

Utilisez Guardicore Segmentation d'Akamai pour limiter l'accès à vos serveurs de sauvegarde, bases de données et serveurs de fichiers, et pour restreindre l'accès depuis l'extérieur du réseau et depuis les parties de votre réseau qui n'ont pas besoin d'y accéder. Pour minimiser la communication entre les serveurs de sauvegarde critiques, vous pouvez utiliser Guardicore Segmentation d'Akamai afin de cloisonner les applications et de limiter la communication entrante et sortante d'une application aux processus et utilisateurs. Limiter l'exposition de vos services de données au minimum opérationnel réduira le facteur de risque de ces services et atténuera l'exposition aux ransomwares et les chemins de propagation.

Partie 2 : Détection des ransomwares et réponse

Face aux cybermenaces, telles que les ransomwares, la planification avancée et la vigilance sont essentielles. En réagissant rapidement aux brèches, vous pouvez minimiser les dommages causés à votre réseau. Guardicore Segmentation d'Akamai dispose de fonctionnalités qui peuvent vous aider à détecter les menaces et à y répondre.

Détection des menaces avec la technologie Guardicore Segmentation d'Akamai

Ces types d'incidents peuvent comprendre :

- **Tromperie** : détecte et intercepte les tentatives de mouvement latéral suspectes et les redirige vers des « pots de miel » dynamiques afin de surveiller et d'analyser leurs actions. Les rapports d'incidents de tromperie sont fiables et fournissent des données détaillées sur les activités malveillantes et la prochaine phase d'attaque du cybercriminel.
- **Analyses réseau** : les cybercriminels recueillent des renseignements une fois qu'ils sont rentrés dans un réseau. Ils utilisent les analyses réseau comme méthode de reconnaissance pour détecter les ports ouverts ou les services que les autres serveurs écoutent. Guardicore Segmentation d'Akamai détecte automatiquement les analyses réseau et alerte immédiatement les utilisateurs.
- **Détection basée sur des règles** : des règles de sécurité au niveau du réseau et des processus permettent la reconnaissance instantanée des communications non autorisées et du trafic non conforme.

Guardicore Segmentation d'Akamai présente la fonction d'informations

Guardicore Segmentation d'Akamai peut fournir une visibilité sur chaque actif en exploitant une fonctionnalité supplémentaire basée sur des requêtes osquery. Le cadre de requête fourni permet de détecter rapidement les activités anormales, telles que les clichés instantanés de volume, qui sont l'action de précryptage la plus courante des ransomwares. Akamai Guardicore Segmentation peut également détecter les chevaux de Troie utilisés pour acheminer des ransomwares, en recherchant une technique de processus creux commune masquant les programmes malveillants sous svchost.exe, un processus Windows légitime.

Recherche de menaces gérée

Le service de recherche des menaces Akamai Hunt avertit les utilisateurs de tout comportement anormal à l'intérieur de leur réseau. Il utilise de nombreuses techniques à ces fins, telles que l'analyse des connexions Internet entrantes et sortantes et de leur GeoIP associée, la recherche de nouveaux fichiers exécutables en nombre croissant sur le réseau, signe d'une possible propagation, ainsi que l'analyse des connexions des ressources pour détecter des signes de mouvements latéraux à travers des anomalies du nombre de voisins.

Réponse immédiate

Une fois que vous avez détecté une menace dans votre réseau, telle qu'un ransomware, vous pouvez déployer rapidement des mesures d'atténuation en appliquant des règles au niveau des processus et des utilisateurs afin de refuser et d'isoler activement les activités malveillantes.

Visibilité croissante sur les infections

Après un premier signe ou indicateur d'infection (IOC), vous pouvez rechercher des indicateurs supplémentaires, tels que des modèles de communication, des processus, des ports utilisés, des ressources infectées, etc. La solution Guardicore Segmentation d'Akamai contribue à identifier toutes les ressources concernées par cet indicateur (par exemple, toutes celles communiquant avec le C2, toutes celles communiquant avec un port unique ou encore toutes celles exécutant un processus malveillant). Vous pouvez ensuite rechercher sur la carte visuelle de votre environnement d'autres similitudes entre les machines infectées, ou des traces de propagation.

Partie 3 : Désinfection et récupération

Une fois que vous avez la liste de toutes les machines infectées et de tous les indicateurs d'infection, vous pouvez lancer le processus de désinfection. Répartissez vos machines entre trois groupes : **isolées**, **surveillées** et **propres**.

Isolées

- Ressources **infectées** par des programmes malveillants
- Mettez ces ressources **en quarantaine** jusqu'à la suppression du logiciel malveillant

Surveillées

- Ressources **susceptibles d'être infectées**
- **Surveillez-les** jusqu'à avoir la certitude que le programme malveillant a été **supprimé**

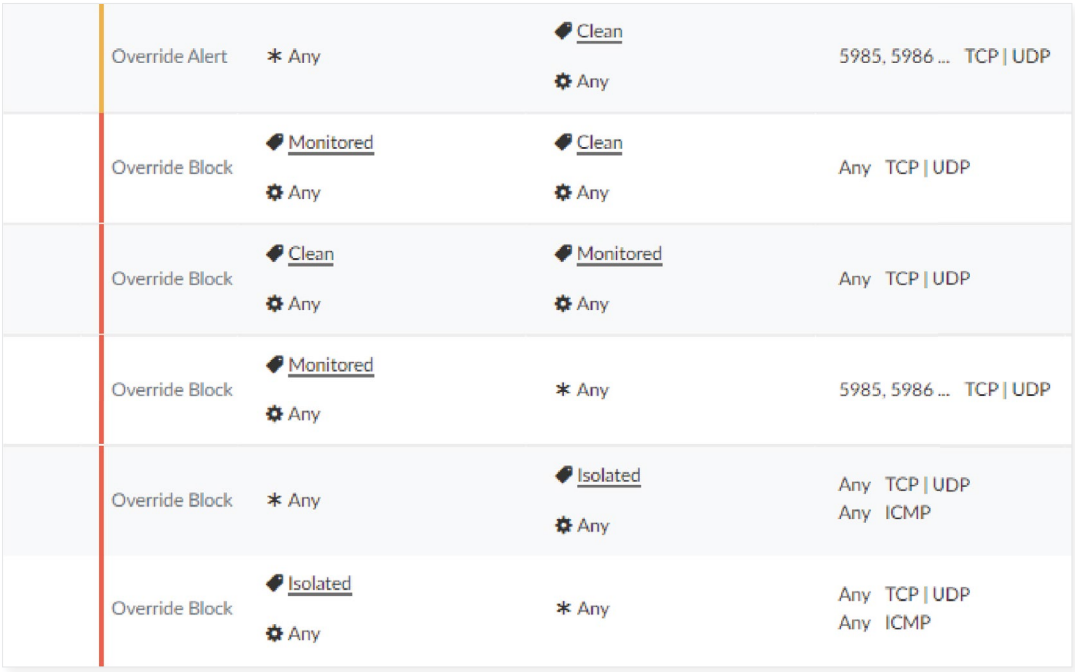
Propres

- Ressources **non infectées** qui peuvent **fonctionner normalement**

Instructions de segmentation pour la récupération

Après avoir défini les trois groupes, vous pouvez commencer à ajouter des règles pour segmenter votre réseau en créant quatre niveaux de communication :

- **Bloquez** toutes les communications entrantes et sortantes des machines **isolées**.
- **Bloquez** la communication du protocole de gestion à distance vers et depuis les machines **surveillées**.
- **Signalez** toute communication de protocole de gestion à distance sur les machines **propres**.
- **Bloquez** toutes les communications entre les trois groupes.



Règles de blocage et d'alerte dans Guardicore Segmentation d'Akamai

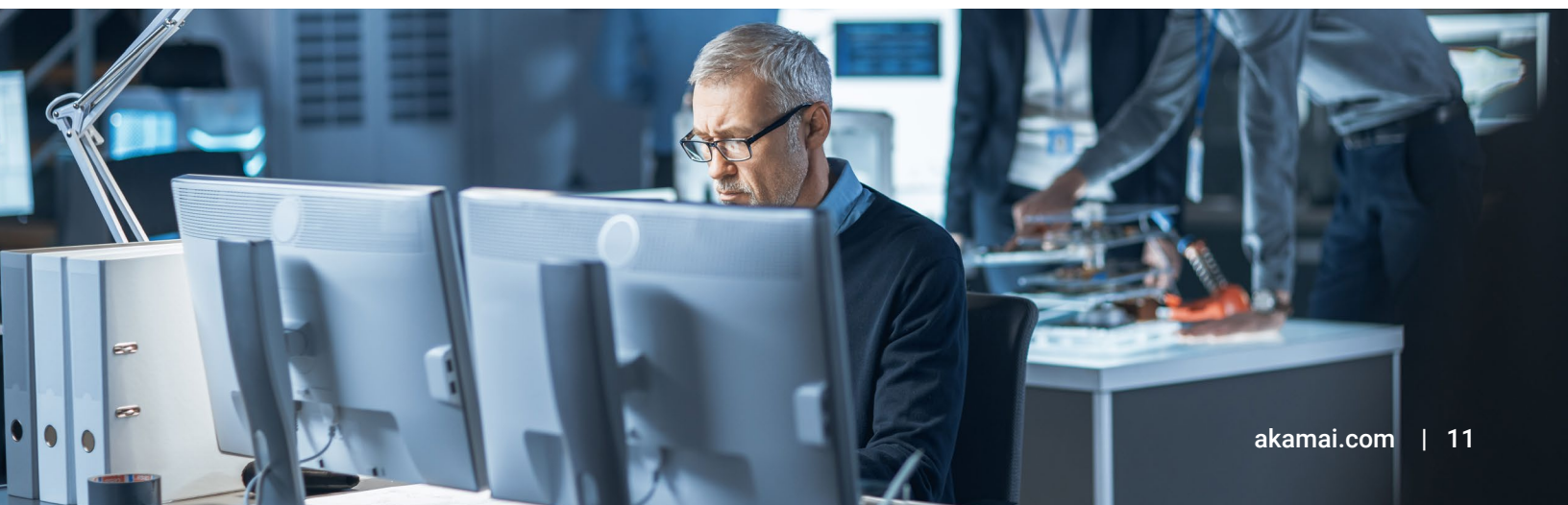
Modèle de récupération et de réponse aux ransomwares

Le modèle de règles de récupération et de réponse aux ransomwares inclus dans Guardicore Segmentation d'Akamai vous fournit une règle intégrée et facile à utiliser pour limiter l'accès aux groupes de ressources **isolées**, **surveillées** et **propres**.

Ce modèle vous permettra d'assurer facilement la continuité opérationnelle des machines **propres** sans craindre d'infection ou de réinfection des machines **isolées**.

Conclusion

Si vous utilisez toujours des anciens pare-feu ou une défense uniquement au niveau du périmètre, vous ne pouvez pas empêcher les ransomwares de se propager sur votre réseau et de verrouiller les applications et l'infrastructure critiques. C'est un fait : les violations sont inévitables et vous devez être prêt à les gérer. Guardicore Segmentation d'Akamai peut vous aider à détecter les menaces dans le trafic est-ouest des centres de données et à bloquer les mouvements latéraux dont dépendent les ransomwares pour chiffrer et demander des rançons sur vos actifs les plus critiques.



Cinq étapes pour atténuer l'impact d'une attaque par ransomware avec Guardicore Segmentation d'Akamai

Préparer en identifiant chaque application et chaque ressource en cours d'exécution dans votre environnement informatique.

Éviter en créant des règles pour bloquer les techniques de propagation de ransomwares courantes.

Détecter en recevant des alertes pour toute tentative d'accès aux applications segmentées et aux sauvegardes.

Corriger en lançant des mesures de confinement des menaces, et de quarantaine lorsqu'une attaque est détectée.

Récupérer avec des fonctionnalités de visualisation qui prennent en charge les stratégies de récupération par phases.

Stoppez les mouvements latéraux des ransomwares dans votre réseau. Vous ne nous croyez pas ? Jugez par vous-même. akamai.com/guardicore

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 sécurité, de traitement et de diffusion d'Akamai, consultez akamai.com et akamai.com/blog, ou suivez Akamai Technologies sur Twitter et LinkedIn. Publication : 05/23.