LISTE DE CONTRÔLE D'AKAMAI

Fonctionnalités de la plateforme Zero Trust

Une plateforme Zero Trust efficace regroupe des solutions ponctuelles autrefois distinctes, notamment le ZTNA (Zero Trust Network Access), la microsegmentation, le pare-feu DNS et la recherche des menaces, dans une plateforme intégrée à console unique. Le déploiement rapide et efficace du Zero Trust permet de stopper les ransomwares, de répondre aux exigences de conformité et d'assurer la sécurité de vos équipes distribuées et de votre infrastructure de cloud hybride. Cette liste de contrôle peut être utilisée pour évaluer les capacités des fournisseurs ou comme liste d'exigences nécessaires pour mettre en œuvre le Zero Trust à partir d'une plateforme unique.

Catégorie 1 : exigences en matière de plateforme

Votre solution de plateforme Zero Trust doit être flexible, évolutive et facile à gérer.

- [ ] Une évolutivité répondant aux demandes de trafic et fournissant une protection continue sans perte de performances
- [ ] Possibilité d'intégration avec les outils de sécurité déjà en place chez les clients, tels que SIEM, SOAR, EDR, CMDB et bien plus encore
- [ ] Couverture des centres de données hétérogènes (environnements hybrides et multicloud, systèmes hérités, terminaux des utilisateurs finaux, clusters Kubernetes, machines virtuelles, environnements IoT/OT et bien plus encore)
- [ ] Modèles de déploiement flexibles prenant en charge diverses architectures hybrides : cloud, virtuel, sur site
- [ ] Capacité à prendre en charge les déploiements avec et sans agent (IoT/OT, PaaS)
- [ ] Prise en charge de Windows, Linux et macOS, et des systèmes d'exploitation hérités
- [ ] Fonctionnalités de journal d'audit pour garantir l'enregistrement de toutes les actions

Catégorie 2 : exigences en matière de visibilité

Une visibilité approfondie est essentielle pour comprendre l'environnement, identifier les connexions suspectes et réagir rapidement et précisément aux menaces.

- [ ] Visualisation sous forme de carte de toutes les applications et flux de charge de travail, ainsi que de l'accès d'un utilisateur à une application dans n'importe quel environnement (conteneurs, sans serveur, IaaS ou PaaS), le tout à partir d'une console unique
- [ ] Flux historiques et en temps réel pour l'investigation et l'analyse des événements
- [ ] Interopérabilité avec des pare-feux et du matériel tiers tels que des commutateurs
- [ ] Possibilité de collecter des données à partir de diverses sources tierces telles que CMDB, EDR et API cloud pour les étiquettes contextuelles et les règles
- [ ] Assistance à l'étiquetage, de préférence en exploitant l'IA pour plus de rapidité et de précision

Catégorie 3 : exigences en matière de règles

Les règles est-ouest (microsegmentation) et nord-sud (ZTNA) sont appliquées à partir d'un seul endroit, sur la base d'attributs qui peuvent être utilisés dans une série de cas d'utilisation, tels que la protection contre les ransomwares, la protection des télétravailleurs, la réponse Zero Day et la conformité.

- [ ] Règle définie par logiciel et distribuée dans toute l'entreprise sans nécessiter de pare-feux physiques internes qui créent des points d'étranglement
- [ ] Règles créées sur la base de divers attributs de charge de travail plutôt que sur la base des seuls adresses IP et ports
- [ ] Mise en œuvre de règles granulaires centrées sur les applications afin de protéger les charges de travail jusqu'au niveau du port, du processus et même du service
- [ ] Un moteur de recommandation de règles avec des modèles prêts à l'emploi et personnalisés, tirant de préférence parti de l'IA, qui accélère la création de règles
- [ ] Règles appliquées avec ou sans agent
- [ ] Contrôles des règles basés sur une cartographie complète des flux
- [ ] Règles préconfigurées de réduction des risques mondiaux basées sur les meilleures pratiques du secteur
- [ ] Règle pour le cloud hybride dans les environnements virtualisés, IaaS et PaaS
- [ ] Règles liées à la charge de travail avec possibilité de la suivre en cas de déplacement, de migration ou de modification
- [ ] Règle d'accès pour les utilisateurs sur site et à distance

Catégorie 4 : exigences relatives aux composants Zero Trust

Parmi les différentes fonctions intégrées dans une plateforme Zero Trust unifiée, le Zero Trust Network Access et la microsegmentation apparaissent comme les piliers fondamentaux. Ces technologies permettent aux entreprises de déployer des contrôles Zero Trust sans impacter négativement les équipes et la continuité des activités.

- ☐ Moteur unifié de règles d'accès et réseau (contrôle combiné est-ouest et nord-sud)
- ☐ Renforcement de l'identification avec l'authentification multifactorielle FIDO2 (MFA)
- ☐ Capacité à protéger les environnements informatiques et les utilisateurs contre un large éventail de menaces en surveillant et en filtrant le trafic DNS
- ☐ Détection continue des menaces évasives et surveillance de la stratégie de sécurité
- ☐ Partage de signaux entre les outils de la plateforme, pour s'assurer qu'un attaquant est arrêté même s'il parvient à passer à travers le mécanisme d'accès
- ☐ Adoption de systèmes de leurres dynamiques capables de traquer et de mettre en quarantaine les attaquants
- ☐ Possibilité d'interroger les points de terminaison ou les serveurs sur la présence de vulnérabilités, afin de permettre une atténuation et une détection rapides des ransomwares

Catégorie 5 : exigences en matière d'IA intégrée

De nombreux aspects d'une mise en œuvre efficace du Zero Trust peuvent être rationalisés avec l'utilisation de l'IA. Elle accélère et simplifie la création de règles, la conformité, la réponse aux incidents et l'évaluation des vulnérabilités.

- ☐ Communication avec les journaux réseau en langage naturel pour réduire le temps de réponse aux incidents, les efforts de portée de la conformité et plus encore
- ☐ Rationalisation de l'ensemble du processus d'élaboration des règles grâce à l'IA, qui suggère des étiquettes et des règles basées sur vos modèles de trafic uniques
- ☐ Traduction du langage naturel en syntaxe pour rechercher rapidement les vulnérabilités de votre réseau sans avoir à rechercher les IOC ou à écrire des requêtes personnalisées
- ☐ Mécanismes de recherche des menaces utilisant l'IA, permettant aux méthodes de détection avancées de détecter les anomalies et l'activité malveillante à côté desquelles passent les outils traditionnels

Pour en savoir plus, rendez-vous sur le site Sécurité Zero Trust d'Akamai.