FICHE PRODUIT AKAMAI

Akamai Guardicore Access

Microsegmentation et ZTNA unifié

Une console unique pour la visibilité et le contrôle simplifie et accélère la sécurité Zero Trust

Les entreprises adoptent rapidement la sécurité Zero Trust pour arrêter les ransomwares, respecter les obligations de conformité et sécuriser leur personnel hybride et leur infrastructure cloud. Zero Trust Network Access (ZTNA) et la microsegmentation sont les deux solutions les plus essentielles pour les entreprises qui adoptent une architecture Zero Trust. Ensemble, elles contribuent à réduire la surface d'attaque, à contenir les violations et à fournir un meilleur contrôle d'accès avec une expérience utilisateur améliorée.

Le pouvoir de l'unification

Akamai Guardicore Access associe segmentation et ZTNA ; ils sont déployés avec un seul agent et gérés avec une seule console. Cette approche innovante garantit une visibilité complète de l'utilisateur à la charge de travail (nord-sud) et du point de terminaison au point de terminaison ou à la charge de travail (est-ouest), permettant ainsi un contrôle d'accès aux applications basé sur les identités et une segmentation des points de terminaison d'un seul coup. En combinant ces technologies, les entreprises bénéficient d'un cadre de sécurité robuste qui renforce les défenses du réseau, atténue les risques et favorise un environnement sécurisé et conforme.

La plateforme Akamai Guardicore est la première plateforme de sécurité à associer la microsegmentation de pointe et ZTNA, afin d'aider les équipes de sécurité à prévenir les ransomwares, à respecter les réglementations de conformité et à protéger à la fois les équipes hybrides et l'infrastructure cloud.

Pour la toute première fois, les entreprises peuvent mettre en œuvre la segmentation afin de minimiser leur surface d'attaque tout en gérant facilement l'accès à leurs équipes hybrides depuis n'importe quel endroit, le tout avec un seul agent utilisant une console unique sur tous les types de ressources et d'infrastructures.

Principales fonctionnalités

Visibilité de bout en bout
Obtenez une compréhension complète de votre réseau avec une visibilité de bout en bout, présentée à la fois sur la carte et les journaux, et donnant des informations sur les schémas d'accès des utilisateurs finaux. Ceci n'est possible qu'en combinant segmentation et ZTNA en un seul produit. Visualisez les chemins de connexion, des points de terminaison aux charges de travail, jusqu'au niveau du processus. La visibilité en temps quasi réel et historique facilite l'investigation et accélère l'atténuation.

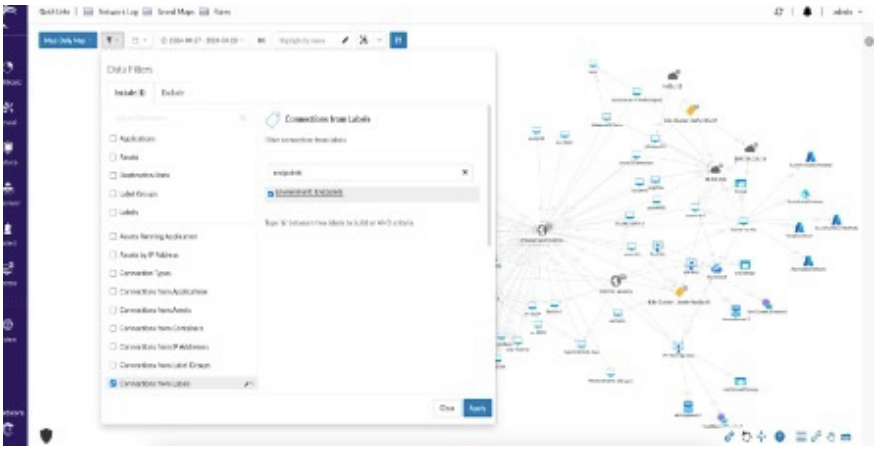
Avantages pour votre entreprise

Console unique, agent unique
Implémentez la segmentation pour minimiser la surface d'attaque tout en gérant facilement l'accès à des équipes hybrides où que vous soyez, avec un agent unique et une console unique

Couverture étendue
Appliquez des contrôles d'accès partout et sécurisez vos employés à distance et au bureau

Règle unifiée
Appliquez la règle pour le trafic est-ouest et l'accès nord-sud, sans changer de syntaxe ou de console, et bénéficiez du moyen le plus simple et le plus efficace d'agir sur la sécurité Zero Trust.

Découverte d'applications
Réduisez le délai de mise en place des stratégies en identifiant rapidement les applications nécessitant des autorisations d'accès. Découvrez facilement vos applications privées et obtenez des informations précieuses sur leurs habitudes d'utilisation, y compris l'accès utilisateur et la fréquence.



Découvrez facilement les applications pour lesquelles un accès est requis

Synchronisation des règles d'accès et de segmentation
Synchronisez automatiquement les contrôles d'accès et les règles de segmentation afin de réduire les dépendances entre les équipes et d'éliminer les risques d'erreur humaine.

Principaux cas d'utilisation

Protection complète contre les ransomwares : réduisez la probabilité et l'impact des attaques de ransomwares et d'autres programmes malveillants grâce à des règles basées sur l'identité et de machine à machine. Assurez-vous que les points de terminaison accèdent aux ressources sur la base du moindre privilège, tout en appliquant des contrôles d'accès granulaires.

- Protégez les ressources de grande valeur : autorisez les utilisateurs à accéder aux ressources critiques en fonction de contrôles d'accès sécurisés et bloquez le trafic VPN direct
- Limitez les utilisateurs privilégiés : bloquez le trafic VPN vers les ports d'administration exploitables pour fournir un accès sécurisé aux administrateurs

Équipes dispersées : prenez en charge le télétravail en appliquant des contrôles d'accès stricts, garantissant ainsi que chaque terminal se connecte uniquement aux ressources dont il a besoin. Cela minimise la surface d'attaque et réduit les mouvements latéraux au sein du réseau.

Conformité : mettez en œuvre des règles de segmentation des points de terminaison afin que les entreprises puissent s'assurer que les leurs sont conformes aux normes et réglementations de l'industrie en vigueur. Cela réduit le risque de sanctions pour non-conformité et renforce leur posture de sécurité globale.

Accès tiers : permettez aux sous-traitants et aux partenaires de se connecter à des applications spécifiques sans installer d'agent, en acheminant et en authentifiant leur accès via un portail Akamai dédié.

Rendez-vous sur le site Sécurité Zero Trust d'Akamai pour en savoir plus