FICHE PRODUIT AKAMAI

Segmentation pour les terminaux IoT et OT

Étendez vos capacités de segmentation Zero Trust à tous les terminaux connectés

De nombreuses entreprises étendent leur utilisation de terminaux de l'Internet des objets (IoT) et de technologies opérationnelles (OT) pour stimuler leur croissance, améliorer leur efficacité et servir leurs clients de manière plus efficace. Bien que ces technologies puissent générer une valeur commerciale significative, elles représentent également un nouveau vecteur d'attaque critique que les équipes de sécurité doivent défendre. Les terminaux IoT sont particulièrement sujets aux vulnérabilités matérielles et logicielles, et de nombreux systèmes OT hérités ont été conçus sans que les exigences de sécurité du monde connecté soient prises en compte. Akamai Guardicore Segmentation étend la sécurité Zero Trust à ces terminaux, réduisant ainsi le risque d'exploitation par des acteurs malveillants cherchant à accéder à l'infrastructure informatique globale de l'entreprise.

Avantages pour votre entreprise

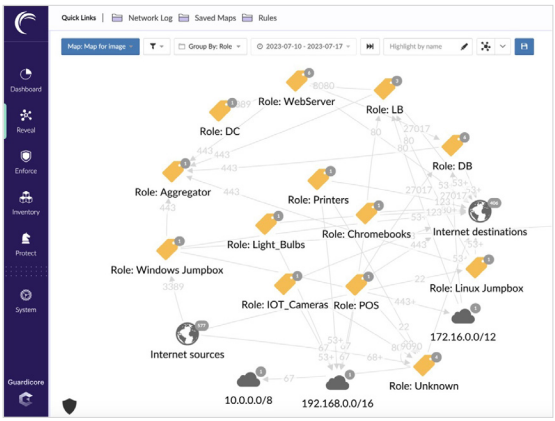
- Détectez, identifiez et classifiez tous les terminaux connectés
- Mettez en œuvre des stratégies de segmentation Zero Trust à partir d'une interface unique, y compris pour les systèmes IoT et OT spécialisés
- Combinez l'application de règles basées sur les agents et sans agent pour une protection complète

Découvrez de nouveaux terminaux connectés en continu

Le déploiement pour les terminaux IoT et OT est très différent de celui des points de terminaison et autres terminaux d'entreprise traditionnels. Plus particulièrement, les terminaux IoT et OT sont déployés en quantités beaucoup plus importantes, et l'empreinte du terminal change de manière dynamique en fonction de l'évolution des besoins opérationnels. Akamai Guardicore Segmentation assure une surveillance et une découverte en continu de tous les terminaux IoT et OT connectés. Cela permet d'empêcher les communications provenant de terminaux non approuvés et de répertorier et protéger les terminaux autorisés.

Identifiez et catégorisez tous les terminaux connectés

Akamai Guardicore Segmentation permet une identification intégrée des terminaux. Notre approche sophistiquée va au-delà des identifiants de terminaux pouvant être facilement usurpés ; elle analyse le comportement du réseau et d'autres signaux afin de mettre en place une identification fiable pour chaque terminal connecté au réseau. Les terminaux sont non seulement identifiés, mais également regroupés en catégories pouvant être utilisées pour créer des stratégies de sécurité abstraites et évolutives.



Visualisez l'ensemble des actifs de votre entreprise

Les terminaux IoT et OT découverts et catégorisés via Akamai Guardicore Segmentation apparaissent aux côtés des terminaux d'entreprise et des charges de travail applicatives plus traditionnels sur la carte Guardicore Reveal d'Akamai, une interface visuelle unique et hautement interactive. Cela permet aux équipes de sécurité de comprendre facilement comment tous les types de terminaux connectés interagissent les uns avec les autres et de mettre en place des stratégies de segmentation Zero Trust efficaces combinant des techniques d'application basées sur l'hôte et sans agent.

Appliquez des stratégies de segmentation granulaire à tous les terminaux

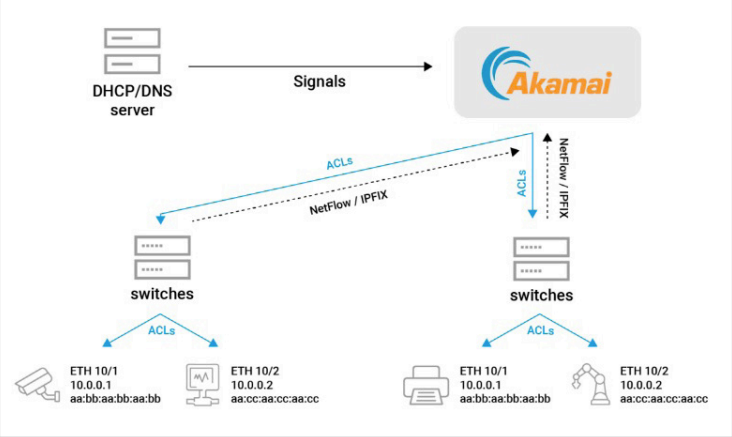
Akamai Guardicore Segmentation étend l'application de sa stratégie Zero Trust en toute simplicité, en proposant une segmentation basée sur le réseau spécialement conçue pour les terminaux IoT et les systèmes OT qui ne peuvent pas exécuter de logiciels de sécurité basés sur l'hôte. Vous pouvez ainsi contrôler et limiter la communication entre les terminaux OT et IoT, ainsi que d'autres ressources réseau, et définir des limites sécurisées, tout en autorisant les connexions nécessaires aux systèmes de gestion informatique, aux serveurs de mise à jour dédiés et aux serveurs de journalisation.

Conservez la visibilité et le contrôle lorsque les terminaux sont en itinérance

L'architecture d'Akamai Guardicore Segmentation assure vigilance et visibilité même lorsque les terminaux sont en itinérance vers de nouveaux emplacements réseau. Elle garantit le maintien des stratégies de segmentation Zero Trust adéquates, y compris toute adaptation basée sur l'emplacement requise.

Fonctionnement

Le trafic généré par vos terminaux réseau émet des signaux (par exemple, DHCP, DNS, Netflow, TCP, etc.) qui sont utilisés par Akamai Guardicore Segmentation pour identifier et classer tous les terminaux. Des stratégies de segmentation peuvent ensuite être créées via une interface unifiée. Pour les terminaux IoT et OT, ainsi que les autres terminaux qui ne peuvent pas exécuter d'agents basés sur l'hôte, les stratégies de segmentation sont appliquées au travers de la mise en œuvre automatisée de règles de contrôle d'accès au niveau du réseau.



Consultez notre site Web pour en savoir plus sur l'extension Zero Trust aux terminaux IoT et OT