INFORMACIÓN SOBRE EL PRODUCTO DE AKAMAI

Segmentación para entornos IoT y OT

Amplíe sus capacidades de segmentación Zero Trust a todos los dispositivos conectados

Son muchas las empresas que usan cada vez más dispositivos del Internet de las cosas (IoT) y de tecnología operativa (OT) para impulsar el crecimiento, mejorar la eficiencia y atender a los clientes de forma más eficaz. Aunque estas tecnologías pueden generar un importante valor empresarial, también representan un nuevo vector de ataque fundamental que los equipos de seguridad deben defender. Los dispositivos del IoT son especialmente propensos a las vulnerabilidades de hardware y software. Por su parte, cuando se diseñaron muchos de los sistemas de OT heredados no se tuvieron en cuenta los requisitos de seguridad del mundo conectado. Akamai Guardicore Segmentation lleva la seguridad Zero Trust a estos dispositivos, con lo que se reduce el riesgo de que los atacantes los exploten para acceder a la infraestructura de TI empresarial más amplia.

Ventajas para su empresa

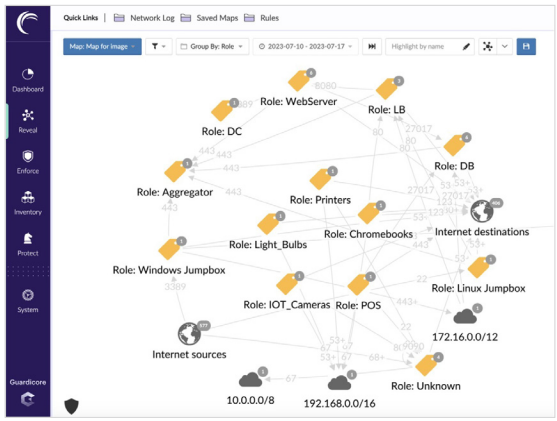
- Detecte, identifique con huella digital y clasifique todos los dispositivos conectados.
- Implemente políticas de segmentación Zero Trust desde una única interfaz, incluidos los sistemas especializados de IoT y OT.
- Combine la aplicación de políticas con o sin agentes para garantizar una cobertura completa.

Detecte en todo momento los nuevos dispositivos conectados

La implementación de dispositivos de IoT y OT es muy diferente a la de los terminales y otros dispositivos empresariales tradicionales. En concreto, los dispositivos de IoT y OT se implementan en cantidades mucho mayores y su cobertura cambia constantemente en función de las necesidades operativas. Akamai Guardicore Segmentation supervisa y detecta de forma constante todos los dispositivos de IoT y OT conectados. De esta forma, los dispositivos no autorizados no se pueden comunicar, mientras que se crea un inventario de los dispositivos autorizados para protegerlos.

Identifique y clasifique todos los dispositivos conectados

Akamai Guardicore Segmentation incluye la huella digital de dispositivos integrada. Nuestro sofisticado enfoque va más allá de los identificadores de dispositivos, que se pueden falsificar fácilmente, y permite analizar el comportamiento de la red y otras señales para desarrollar una huella digital fiable para cada dispositivo conectado a la red. Conforme los dispositivos se van identificando, se van agrupando en categorías que se pueden utilizar para crear políticas de seguridad abstractas y escalables.



Visualice todos los activos de su empresa en un mismo lugar

Los dispositivos de IoT y OT que Akamai Guardicore Segmentation detecta y clasifica aparecen junto con los terminales empresariales y las cargas de trabajo de aplicaciones más tradicionales en el mapa de Guardicore Reveal, una única interfaz visual muy interactiva. Esto permite a los equipos de seguridad entender cómo interactúan los distintos tipos de dispositivos conectados y desarrollar estrategias de segmentación Zero Trust eficaces, donde se combinan técnicas de aplicación basadas en host y sin agentes.

Aplique políticas de segmentación detalladas a todos los dispositivos

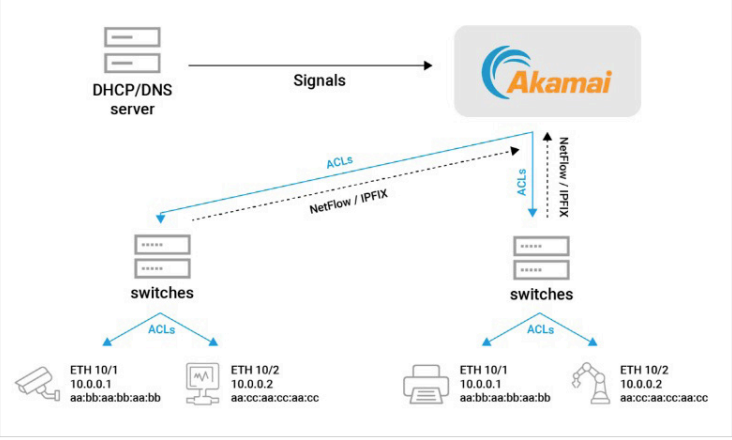
Akamai Guardicore Segmentation puede aplicar sin ningún problema sus políticas Zero Trust, al ofrecer segmentación basada en red diseñada específicamente para dispositivos de IoT y sistemas de OT que no pueden ejecutar software de seguridad basado en host. De esta forma, podrá controlar y limitar la comunicación entre los dispositivos de OT e IoT, así como otros recursos de red. También podrá establecer límites seguros y las conexiones necesarias a los sistemas de gestión de TI, servidores de actualización dedicados y servidores de registro.

Mantenga la visibilidad y el control aunque los dispositivos cambien de ubicación

La arquitectura Akamai Guardicore Segmentation seguirá reconociendo y mostrando los dispositivos, incluso cuando estos se trasladen a otras ubicaciones de red. Esto garantiza que siempre se apliquen las políticas de segmentación Zero Trust adecuadas, incluidas las adaptaciones basadas en la ubicación que sean necesarias.

Cómo funciona

El tráfico que generan los dispositivos de red emite señales (por ejemplo, DHCP, DNS, Netflow, TCP, etc.) que Akamai Guardicore Segmentation utiliza para identificar y clasificar todos los dispositivos. A continuación, se pueden crear políticas de segmentación con una interfaz unificada. En el caso de los dispositivos de IoT y OT, así como de otros dispositivos que no pueden ejecutar agentes basados en host, las políticas de segmentación se aplican mediante la implementación automatizada de reglas de control de acceso a nivel de red.



Visite nuestro sitio web para obtener más información sobre la aplicación de Zero Trust a IoT y OT.