RESUMO DO PRODUTO DA AKAMAI

Segmentação para Internet das coisas (IoT) e Tecnologia operacional (TO)

Estenda seus recursos de segmentação Zero Trust a todos os dispositivos conectados

Muitas empresas estão expandindo seu uso de dispositivos de Internet das coisas (IoT) e tecnologia operacional (TO) para impulsionar o crescimento, melhorar a eficiência e atender aos clientes de forma mais eficaz. Embora essas tecnologias possam oferecer um valor comercial significativo, elas também representam um novo vetor de ataque crítico que as equipes de segurança devem defender. Os dispositivos de IoT são particularmente propensos a vulnerabilidades de hardware e software, e muitos sistemas de TO legados não foram projetados tendo em mente os requisitos de segurança do mundo conectado. A Akamai Guardicore Segmentation estende a segurança Zero Trust a esses dispositivos, o que reduz o risco de que os agentes de ameaça os explorem para obter acesso à infraestrutura de TI corporativa mais ampla.

Benefícios para os seus negócios

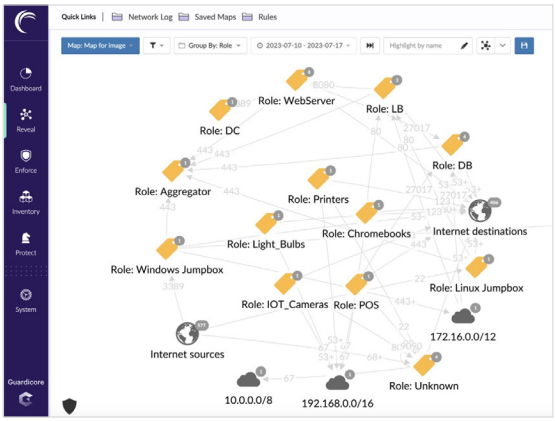
- Detecte, registre e classifique todos os dispositivos conectados
- Implemente políticas de segmentação Zero Trust a partir de uma única interface, inclusive para sistemas especializados de IoT e TO
- Combine a aplicação de políticas baseada em agente e sem agente para garantir cobertura total

Descubra novos dispositivos conectados continuamente

A implantação de dispositivos de IoT e TO é muito diferente de pontos de extremidade e de outros dispositivos empresariais tradicionais. Sobretudo, os dispositivos de IoT e TO são implantados em quantidades muito maiores, e a pegada digital muda dinamicamente com base nas crescentes necessidades operacionais. A Akamai Guardicore Segmentation monitora e descobre continuamente todos os dispositivos de IoT e TO conectados. Isso garante que aqueles não confirmados sejam impedidos de se comunicar e que os dispositivos autorizados sejam inventariados e protegidos.

Identifique e categorize todos os dispositivos conectados

A Akamai Guardicore Segmentation inclui o registro integrado de dispositivos. Nossa abordagem sofisticada vai além dos identificadores de dispositivos facilmente falsificados e analisa o comportamento da rede e outros sinais para desenvolver um registro confiável para cada dispositivo conectado à rede. À medida que os dispositivos são identificados, eles também são agrupados em categorias que podem ser usadas para criar políticas de segurança dimensionáveis e abstratas.



Visualize todos os ativos empresariais juntos

Dispositivos de IoT e TO descobertos e categorizados por meio da Akamai Guardicore Segmentation aparecem ao lado de pontos de extremidade e cargas de trabalho de aplicativos empresariais mais tradicionais no mapa Guardicore Reveal da Akamai, uma interface visual única e altamente interativa. Isso facilita para que as equipes de segurança entendam como todos os tipos de dispositivos conectados estão interagindo uns com os outros e possam desenvolver estratégias de segmentação Zero Trust eficazes que combinem técnicas de aplicação sem agente e baseadas em host.

Aplique políticas de segmentação granulares a todos os dispositivos

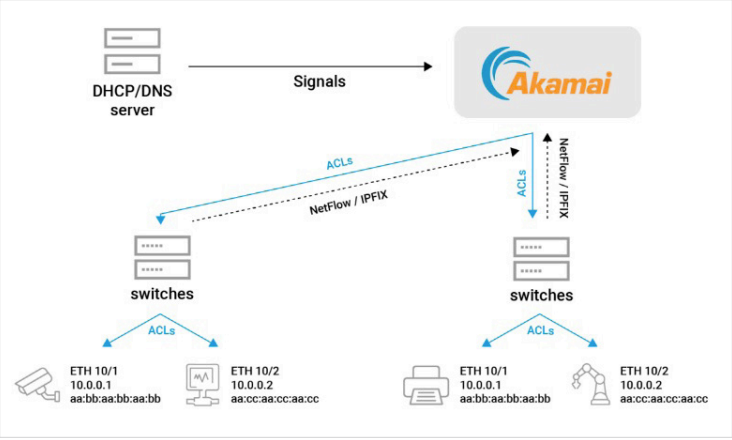
A Akamai Guardicore Segmentation estende perfeitamente sua aplicação de política Zero Trust oferecendo segmentação baseada em rede especificamente projetada para dispositivos de IoT e sistemas de TO que não podem executar software de segurança baseado em host. Isso permite que você controle e limite a comunicação entre dispositivos de TO e IoT, bem como outros recursos de rede. Ela permite estabelecer limites seguros e, ao mesmo tempo, possibilita as conexões necessárias aos sistemas de gerenciamento de TI, servidores de atualização dedicados e servidores de registro.

Mantenha a visibilidade e o controle à medida que os dispositivos se movimentam

A arquitetura da Akamai Guardicore Segmentation mantém o reconhecimento e a visibilidade, mesmo quando os dispositivos fazem roaming para novos locais de rede. Isso garante que as políticas de segmentação Zero Trust adequadas estejam sempre em vigor, incluindo quaisquer adaptações baseadas em localização que sejam necessárias.

Como funciona

O tráfego gerado pelos dispositivos de sua rede fornece sinais (por exemplo, DHCP, DNS, Netflow, TCP etc.) que são usados pela Akamai Guardicore Segmentation para identificar e classificar todos os dispositivos. As políticas de segmentação podem então ser criadas por meio de uma interface unificada. Para dispositivos de IoT e TO (e outros dispositivos que não podem executar agentes baseados em host), as políticas de segmentação são aplicadas por meio da implementação automatizada de regras de controle de acesso no nível da rede.



Visite nosso website para saber mais sobre como estender o Zero Trust à IoT e à TO