




Segmentation for IoT and OT

Extend your Zero Trust segmentation capabilities to all connected devices

Many enterprises are expanding their use of Internet of Things (IoT) devices and operational technology (OT) to drive growth, improve efficiency, and serve customers more effectively. While these technologies can unlock significant business value, they also represent a critical new attack vector that security teams must defend. IoT devices are particularly prone to hardware and software vulnerabilities, and many legacy OT systems were not designed with the security requirements of the connected world in mind. Akamai Guardicore Segmentation extends Zero Trust security to these devices, which reduces the risk that threat actors will exploit them to gain access to the broader enterprise IT infrastructure.

Benefits for your business

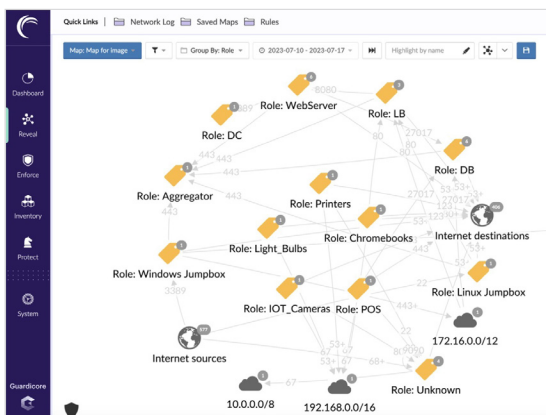
-  Discover, fingerprint, and classify all connected devices
-  Implement Zero Trust segmentation policies from a single interface, including for specialized IoT and OT systems
-  Combine agent-based and agentless policy enforcement to ensure full coverage

Discover new connected devices continuously

The deployment for IoT and OT devices is much different from endpoints and other traditional enterprise devices. Most notably, IoT and OT devices are deployed in much greater quantities, and the device footprint changes dynamically based on evolving operational needs. Akamai Guardicore Segmentation continuously monitors and discovers all connected IoT and OT devices. This ensures that unsanctioned devices are blocked from communicating and authorized devices are inventoried and protected.

Identify and categorize all connected devices

Akamai Guardicore Segmentation includes integrated device fingerprinting. Our sophisticated approach goes beyond easily spoofed device identifiers to analyze network behavior and other signals to develop a trustworthy fingerprint for every network-connected device. As devices are identified, they are also grouped into categories that can be used to create scalable, abstract security policies.



Visualize all of your enterprise assets together

IoT and OT devices discovered and categorized through Akamai Guardicore Segmentation appear alongside more traditional enterprise endpoints and application workloads in Akamai's Guardicore Reveal map – a single, highly interactive visual interface. This makes it easy for security teams to understand how all types of connected devices are interacting with one another and to develop effective Zero Trust segmentation strategies that combine host-based and agentless enforcement techniques.

Apply granular segmentation policies to all devices

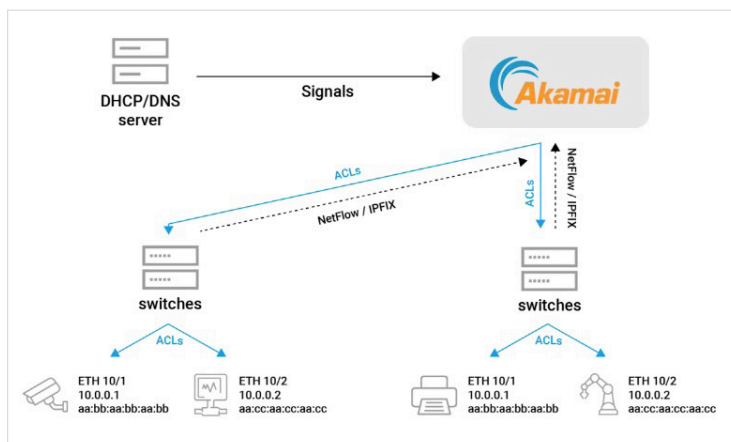
Akamai Guardicore Segmentation seamlessly extends its Zero Trust policy enforcement by offering network-based segmentation specifically designed for IoT devices and OT systems that cannot run host-based security software. This allows you to control and limit communication between OT and IoT devices, as well as other network resources. It enables you to establish secure boundaries while still allowing necessary connections to IT management systems, dedicated update servers, and logging servers.

Maintain visibility and control as devices roam

Akamai Guardicore Segmentation architecture maintains awareness and visibility even as devices roam to new network locations. These ensure that appropriate Zero Trust segmentation policies are always in place, including any required location-based adaptations.

How it works

Traffic generated by your network devices provides signals (e.g., DHCP, DNS, Netflow, TCP, etc.) that are used by Akamai Guardicore Segmentation to identify and classify all devices. Segmentation policies can then be created through a unified interface. For IoT and OT devices – and other devices that cannot run host-based agents – segmentation policies are enforced through automated implementation of access control rules at the network level.



Visit our [website](#) to learn more about extending Zero Trust to IoT and OT