AKAMAI SOLUTION BRIEF

Gain Visibility and Insight into Connected Devices with Armis and Akamai Guardicore Segmentation

As more kinds of devices are becoming connected and used in corporate networks, IT and security teams are facing a growing number of challenges. Some of those challenges are identifying and protecting the different kinds of devices, including OT, IoT, and IoMT.

Connected devices need to be monitored and controlled as a dynamic part of an organization's entire network, not within a silo. If left improperly governed, connected devices can become an entry point for attackers to move laterally inside the network, providing an open door for access to a growing amount of sensitive data.

Unmanaged device security: Challenges and risks

"Unmanaged devices" refers to assets that don't run a traditional security agent or aren't being directly managed by IT or security. These devices are everywhere — from OT and IoT devices such as cameras, HVAC systems, and medical equipment to bring your own devices (BYODs) and shadow IT.

The unique and dynamic nature of connected devices means that protecting them can pose several unique challenges for security teams:

Poor visibility
As many connected devices do not support installing agents directly, it can be difficult to gain contextual visibility into how many devices there are, what kinds of devices are present, and how they're communicating within your network. Without a clear understanding of the relationships between these devices and different workloads and applications, creating effective security policies becomes almost impossible.

Lack of access control
Traditional methods for controlling access are ineffective for unmanaged devices. Most of the security lifecycle happens after access is granted, and a compromised device might still be able to authenticate with the network.

Unpatchable devices
Some business-critical devices might simply be unpatchable because of a lack of support or specific technical considerations, and many of these devices are kept around long after their expiration dates. If a vulnerability is discovered in one of these devices, it can potentially be exploited by threat actors.

Benefits for your business

Asset inventory
Expand your visibility by discovering, tracking, and classifying all devices and assets on and off the network: managed, unmanaged, and IoT/OT/IoMT from a single view.

Enhanced segmentation
Leverage data pulled from Armis to create powerful segmentation rules based on attributes like risk scores, location, and much more.

Deep insight
Use this enhanced intelligence to detect threats, compromised or vulnerable devices, and any malicious or unintended behavior, down to a single device.

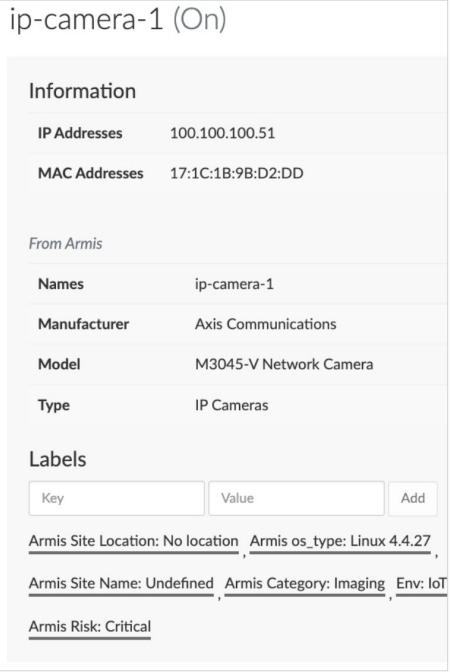
Comprehensive coverage
Enrich your data and understanding of assets that are running Akamai Guardicore agents, and obtain visibility into those assets that do not support agents.

Valuable mapping
Near–real time, continuous information on unmanaged devices added to your existing Reveal map of one hybrid, connected ecosystem.

Unmanaged does not equal uncontrollable

By integrating with Armis, Akamai Guardicore Segmentation adds device attributes and metadata, along with contextual information such as location and risk scores, into your single pane of glass view. This integration allows you to create asset labels in Akamai Guardicore Segmentation for unmanaged devices where agents cannot be directly installed. From one detailed map, you can now see what these devices are and where they meet the data center, including traffic origins and any application dependencies.

With this additional context gleaned from Armis, organizations can use Akamai Guardicore Segmentation to create tight segmentation policies that control communications from these devices into the data center.



Example: The metadata for the IoT asset "ip-camera-1" is pulled in from Armis. Labels can be applied to this asset for visualization and policy creation.

Key capabilities

- **Import asset types and rich metadata** from Armis into Akamai Guardicore Segmentation, enabling administrators to label their devices and visualize their communications using a near–real time interactive map of true network flows. Understand the application dependencies and gain a more complete picture of what is communicating within your environment.
- **Create targeted segmentation policy** by using metadata from Armis, such as OS, manufacturer, model, geographical location, and more, as attributes. Create one-rule policies that can control communications to your data center from all machines of a certain type, make, or location.
- **Leverage the risk scores** assigned by Armis to create and enforce policy for vulnerability management. Akamai Guardicore Segmentation supports the creation of labels based on these risk scores, which can be assigned to high-risk devices and used to build rules that control access from known vulnerable devices, thereby supporting a comprehensive vulnerability management strategy — especially for devices that cannot be patched.

For more information on protecting devices with Armis and Akamai Guardicore Segmentation, speak with sales.

| Published 12/24