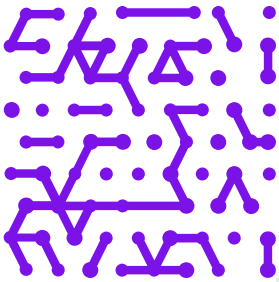
ARMIS® Guardicore

PARTNER BRIEF

Gain visibility and insight into connected devices with Armis and Guardicore

As more kinds of devices are becoming connected and utilized in corporate networks, IT and security teams are facing a growing number of challenges. One of those challenges is identifying and protecting all of the different kinds of devices — including IT, OT, IoT, and IoMT. Connected devices need to be monitored and controlled as a dynamic part of an organization's entire network, and not within a silo. If left improperly governed, these 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 those 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 such as cameras, HVAC systems and medical equipment, to BYOD (Bring Your Own Devices) and shadow IT.

According to the Verizon 2024 Data Breach Investigations Report, 14% of breaches involved the exploitation of vulnerabilities as the initial access step, which has almost tripled from 2023, and this trend seems to be continuing upward.

The unique and dynamic nature of connected devices means that it can be incredibly challenging for security teams to protect them, dealing with several unique challenges:

1 Poor visibility

As many of these devices do not support installing agents directly, it can be very 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 different workloads and applications with these devices, creating effective security policies becomes almost impossible.

2 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.

3 Unpatchable devices

Some business-critical devices might simply be unpatchable due to 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.

Unmanaged does not equal uncontrollable

By integrating with Armis, Guardicore 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 Guardicore for these unmanaged devices where Guardicore 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 Centrix™, organizations can use Akamai Guardicore Segmentation to create tight segmentation policies that control communications from these devices into the data center.

Key Capabilities

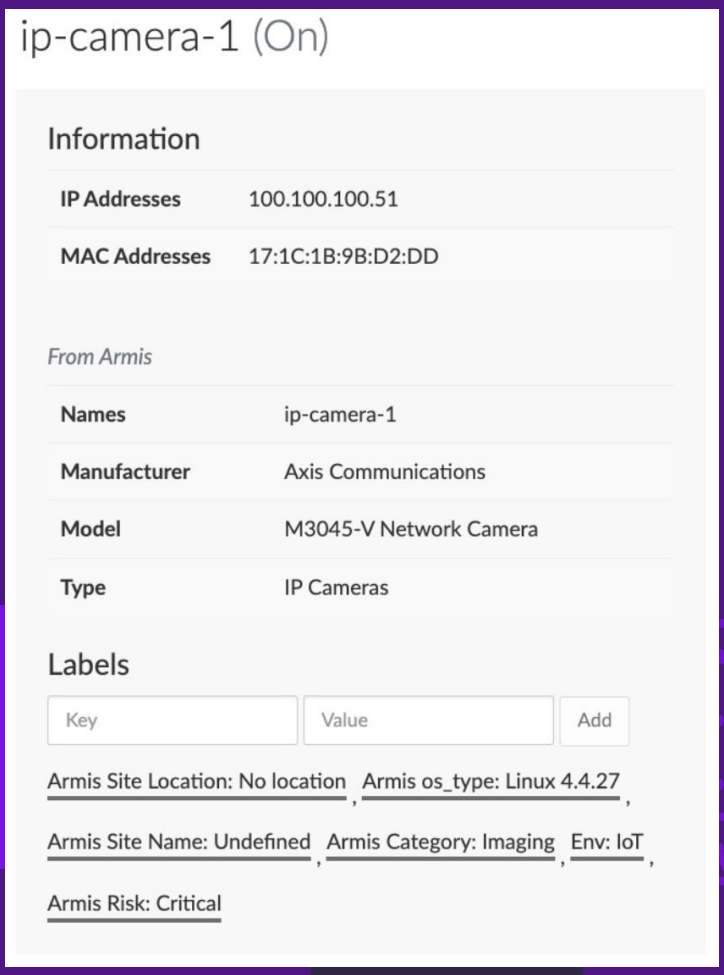
Import asset types and rich metadata from Armis Centrix™ into Guardicore, enabling administrators to label their devices and visualize their communications using a near-real-time interactive map of true network flows. Understand the application dependencies and gain a more complete picture of what is communicating within your environment.

Create targeted segmentation policy using metadata from Armis Centrix™ 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 a specific location.

Leverage the risk scores assigned by Armis as a way to create and enforce policy for vulnerability management. Guardicore 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 and support a comprehensive vulnerability management strategy — especially for devices that cannot be patched.

Example

> The metadata for the IoT asset “ip-camera-1” is pulled in from **Armis Centrix™**. Labels can be applied to this asset for visualization and policy creation.



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 IT/IoT/OT/IoMT from a single view.

Enhanced segmentation

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

Deep insight

Utilize 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 Guardicore agents, and obtain visibility into those assets that do not support agents.

Holistic mapping

Near-real-time, continuous information into unmanaged devices added to your existing Reveal map of one hybrid, connected ecosystem.

Armis, the cyber exposure management & security company, protects the entire attack surface and manages an organization's cyber risk exposure in real time.

In a rapidly evolving, perimeter-less world, Armis ensures that organizations continuously see, protect and manage all critical assets - from the ground to the cloud. Armis secures Fortune 100, 200 and 500 companies as well as national governments, state and local entities to help keep critical infrastructure, economies and society stay safe and secure 24/7.

Armis is a privately held company headquartered in California.

1.888.452.4011

Website

Platform
Industries
Solutions
Resources
Blog

Try Armis

Demo
Free Trial