Armis is an agentless device security platform built to protect the world of unmanaged and IoT / OT devices, provide real-time and continuous cybersecurity asset management, risk management, and automated enforcement.

But, *why* Armis?

Below are the top ten reasons why Armis is necessary for your department and the best option for IoT management/security.

1.) **Comprehensive Asset Discovery and Inventory**

A complete inventory of hardware and software is critically important. This is why so many security frameworks, such as the CIS Critical Security Controls and the NIST Framework for Improving Critical Infrastructure Cybersecurity, start with inventory. Armis automatically generates a complete inventory of devices in your enterprise environment - on or off the network. The breadth, depth and accuracy of the Armis asset inventory and device discovery exceeds that of other products available today. Customers say they see 50% to 70% more devices using Armis

2.) **Agentless**

By 2021, up to 90% of these devices will be unmanaged and IoT devices. These new devices include everything from smart TVs, security cameras, digital assistants, printers, and HVAC systems, to industrial control systems and PLCs, to medical devices, and more. These devices can't take an agent. Armis is an agentless device security platform. This means that Armis works with all types of devices, even those that can't accommodate agents - while also working with traditional managed devices, such as desktops, laptops, and servers. Because we do not use an agent, Armis can be deployed in as little as minutes to hours, not weeks.

3.) **Unmanaged Devices/IoT Attacks Are Increasing**

If the rise in ransomware attacks was not bad enough, attacks against unmanaged and IoT devices are increasing as well.

- Attacks Up 300%. Last year it was reported that attacks against IoT devices were up 300%.
- Russia Targets IoT Devices. Microsoft reported that Russian hackers were targeting IoT devices to breach networks, and researchers identified a Russian group was developing a cyber weapons program leveraging IoT vulnerabilities.
- FBI Warns On Smart TVs. In late 2019, the FBI warned that hackers could take control of unsecured smart TVs - in the home and in the office.
- 100s of Millions of Unmanaged/IoT Devices Vulnerable. Armis disclosed URGENT/11, which identified that hundreds of millions of devices running real-time operating systems (RTOSs) were vulnerable to 11 critical zero-day vulnerabilities, including large numbers of manufacturing, OT, and medical devices

Beyond devices in the office, in hospitals and in manufacturing plants, the network infrastructure is also at risk. Unmanaged devices like switches, routers, and access points can be easily reached by a remote attacker via a technique known as DNS rebinding. Switches, routers, and IP phones and cameras using the Cisco Discovery Protocol were also found to be vulnerable to exploit, allowing an attack to compromise network traffic, even breaking network segmentation. The continuous behavioral monitoring of unmanaged devices, combined with automated threat response and establishment of data encryption tunnels whenever possible, are the new requirements for strong security

4.) **Visibility Across Your Entire Environment**

Armis discovers and analyzes all devices and endpoints across your entire environment. Those connected directly to your network or in your airspace. At corporate or remote offices. And even employees working from home. First, we integrate with your network, where we analyze all traffic and device behavior. This lets us not only see approved devices, but also unapproved or unmanaged devices, including device-to-device behavior, wired and wireless connections, and even point-to-point technologies such as Bluetooth, and mesh technologies such as Zigbee. Second, Armis integrates with the IT and security management tools you currently use to provide an additional layer of device identification, letting us identify gaps in security, and ensuring automated policy enforcement. All of this without the need for agents.

5.) **Passive Monitoring**

Traditional network discovery tools probe your network intrusively. This approach can disrupt or even crash many kinds of devices, particularly sensitive equipment such

as medical devices or operational technology. Armis takes a completely passive approach to monitoring devices. We won't crash or tip over devices; and we don't negatively impact network performance, or your user

6.) **Full Device Classification**

When the Armis platform detects a device either on or near your enterprise network, it can provide full identification and classification of a device including: Device name, device category, device type, device model, device brand, IP address, MAC address, location, user, operating system and version, applications (including name, version, date/time seen active), date and time first seen, date and time last seen, OUI, reputation, and behavior

We also track:

Connections including between the device and other devices including protocol used to connect, time of the connection, duration of the connection, amount of data transferred, physical layer information such as Wi-Fi channel used.

Alerts including information describing each alert such as date, time, type, activity that caused the alert, severity of the alert.

Services accessed by the device including related information such as the date and time, name of the service, amount of traffic, and transmission characteristics such as latency.

Traffic to and from the device including port, description.

Risks including details regarding each type of risk which include manufacturer reputation, cloud synchronization, connection security, data-at-rest security, malicious domains visited, number of wireless protocols used, malicious behavior, number of open ports, user authentication, threat detected, and vulnerability history.

Software vulnerabilities found on the device including related information such as CVE (with drill-down into details), description, publish date, attack vector, attack complexity, and whether user interaction is required. We track all this information "out of the box" for 90 days, with searchable history.

7.) **Proactive Risk Management**

Security professionals know that just being aware that devices exist isn't enough. You need to know whether or not they're risky. After discovering and classifying each device, Armis calculates its risk score. The score is based on multiple risk factors including software vulnerabilities, known attack patterns, connection security, and the observed behavior of each device (see image below). This risk score helps your security team take proactive steps to reduce your attack surface and meet compliance and regulatory frameworks that require you to identify and prioritize vulnerabilities

8.) **Automatic Threat Detection and Response**

Armis does not simply aggregate information of the devices you have or alert you that there is an issue. Armis triggers automated actions to stop an attack. We integrate with your existing security enforcement points like Cisco and Palo Alto Networks firewalls, Network Access Control (NAC) products, as well as directly with your switches and wireless LAN controllers, to restrict access or to quarantine suspicious or malicious devices. This automation gives you peace of mind that attacks on any devices will be stopped, even if your security team is busy with other priorities. Armis also integrates with your security management systems—your SIEM, ticketing systems, asset databases, etc.—to allow these systems and incident responders to leverage the rich information Armis provides. Armis can even inform your IT and security management tools of actions they need to take - supercharging them with greater information leading to enforcement actions.

9.) **World's Largest Device Knowledge base**

Core to the Armis platform is our Device Knowledge base. It is a giant, crowd-sourced, cloud-based device behavior knowledge base—the largest in the world, tracking over 230 million devices—and growing. With our Device Knowledge base, Armis understands not only what the device is and what it is doing, but what it should be doing. This is because we understand the context of each device in its use in each environment.

Context is critical to know the correct behavioral profile of a device. These device insights enable Armis to classify devices and detect threats with a high degree of accuracy. Armis compares real-time device state and behavior to "known-good" baselines for similar devices we have seen in other environments. When a device operates outside of its baseline, Armis issues an alert or can automatically disconnect or quarantine a device.

Alerts can be triggered by a policy violation, a misconfiguration, or abnormal behavior like inappropriate connection requests or unexpected software running on a device. The Device Knowledge base tracks all managed, unmanaged, and IoT devices Armis has seen across all our customers

10.) **Real-Time and Continuous - Across Your Entire Environment**

Armis' asset inventory, risk management, and detection & response all operate in a real-time and continuous manner. This means that every device, managed, unmanaged, or IoT, is always being tracked, including transient devices, with even short lived events identified and recorded to deliver a superior level of security

Armis is soon going to be the industry standard. If you're interested in learning more about Armis and how it can benefit your department, reach out to our small business at sales@acuitytechnical.com