WHY ARMIS

WHY ARMIS

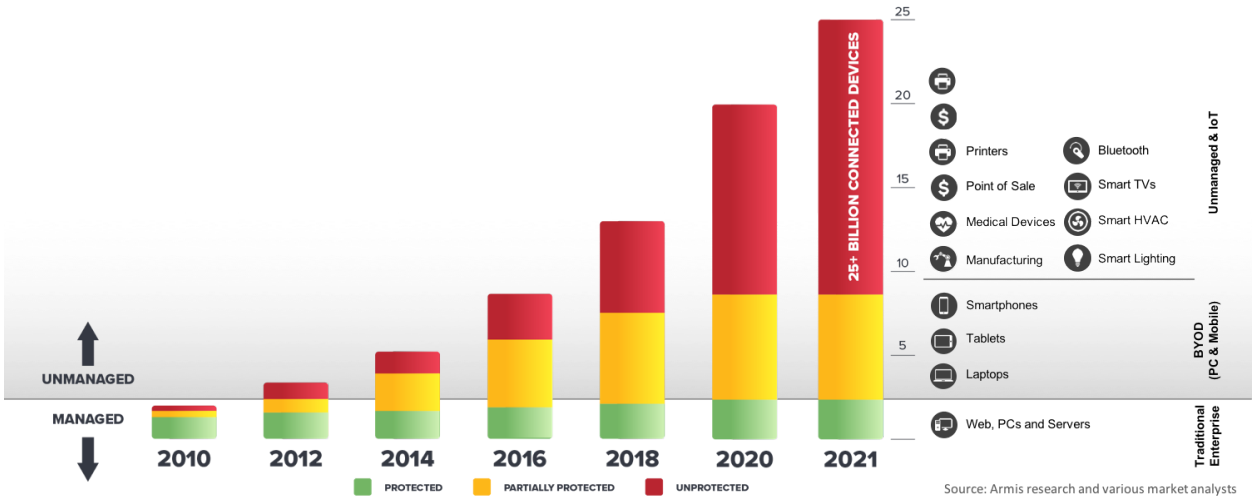
Top 10 Reasons To Consider Armis®

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.



Growth of unmanaged devices connected to enterprise networks which can't accommodate an agent

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 users.

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
- 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. This give us to ability to provide activity and behavior on devices like these:

Device	Key behavior traits detected
Samsung 60" Class J6200 Full LED Smart TV	• DNS queries followed by connection attempts to ypu.samsungelectronics.com - 10 consecutive attempts spaced 5 minutes apart, followed by a 45-minute gap before attempting again • Interfaces: BT, Wi-Fi • Stationary, does not connect to other devices on the network • Tizen OS • Several default applications such as Netflix and Amazon Instant Video
Nest Thermostat 3rd Gen	• DNS queries to transport.home.nest.com, transport.home.ft.nest.com in a periodic manner • Every night at 4AM, ~1GB of data transfer • Interfaces: Wi-Fi • Stationary, no other protocols, routing between Nests on the same network • No connection to other devices, no devices connecting to it
Nest Cam	• Periodic DNS queries and connections to: api.nest.com • Daily connections to: api.nest.com • IP video traffic (streaming data) to: oculus10-vir.nest.com • Interfaces: Wi-Fi • Stationary, no other protocols, no connection to other devices, no devices connecting to it.
Baxter Sigma Spectrum Infusion Pump	• OUI of Sigma • Outgoing periodic connections from device to a static server (Bayer pump server) on port 51244 • Incoming periodic connections from a static server (Baxter pump server) to device on port 51243 • Wi-Fi 2.4GHz only (12dBm-18dBm, dependent on bitrate) • Non-stationary • No other device connects to it (except for direct serial connections which are invisible to us).

Additional information on the device characteristics and behavior traits stored in the Armis Device Knowledgebase is at the end of this document.

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.

Each device identified by Armis is assigned a risk factor

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 Knowledgebase

Core to the Armis platform is our Device Knowledgebase. It is a giant, crowd-sourced, cloud-based device behavior knowledgebase—the largest in the world, tracking over 230 million devices—and growing. With our Device Knowledgebase, 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 Knowledgebase tracks all managed, unmanaged, and IoT devices Armis has seen across all our customers.

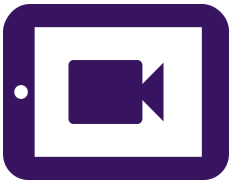
10. Real-Time and Continuous - Across Your Entire Environment

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.

Bonus - Zero Trust

In a world exploding in the number of devices around us, combined with the dissolution of the traditional network perimeter, Zero Trust is an architecture being employed to protect business and critical infrastructure. In a Zero Trust architecture, you cannot not trust any entity inside or outside of your perimeter at any time. Armis lets enterprises implement a strong Zero Trust security framework regardless of the type of device - providing support across the key Zero Trust pillars, including, Network, Users, Devices, Visibility & Analytics, and Automation & Orchestration. Armis generates information about all your devices and feeds that information into your overall security policy enforcement system.

Examples of Armis Threat Detection in Real World Environments



COMPROMISED TABLET

Unauthorized Video Streaming

- Every conference room had a tablet to control the video system on the guest network.
- The tablet in one conference room was streaming video and audio
- This represented a leakage of sensitive conversations.

Armis	NAC	Firewall	IPS/UEBA
✓	✗	✗	✗
• Gleaned WiFi traffic • Discovered and classified all devices and associated traffic volumes • Risk analysis engine identified anomalous traffic with the device	• Inventories devices and controls entry to the network. • Does not monitor traffic volumes • Not designed to detect anomalous devices. Video traffic seemed "normal"	• Designed to protect the perimeter. • Not designed to detect anomalous devices. • Data streaming from tablet seemed "normal" to firewall	• IPS looks for attacks, not for "normal" traffic such as video. • UEBA is not designed to detect anomalous devices. Video streaming from tablet seemed "normal" to UEBA

COMPROMISED SECURITY CAMERA (& ROUTERS)

Botnet Attack

- Security cameras on the network were compromised, part of a botnet, trying to propagate.

Armis	NAC	Firewall	IPS/UEBA
✓	✗	✗	?
• Discovered and classified all devices • Monitored traffic • Risk Analysis Engine saw cameras trying to connect to other cameras & routers via ports 23 and 80 • Triggered switches to quarantine the devices	• Inventories devices and controls entry to the network. • Does not monitor traffic over time. • Not designed to detect anomalous behavior.	• Not designed to monitor internal network traffic. • Firewalls have difficult time detecting botnet propagation or C&C because it is disguised as peer-to-peer	• IPS could have discovered cameras if IPS was in the right location and had a behavior signature • UEBA might have discovered the behavior anomaly, if it had the right data

ROGUE NETWORK STEALING CREDENTIALS

Theft of Network Credentials

- A corporate device is connecting to a pineapple that is collecting its Active Directory credentials or hashes

Armis	NAC	Firewall	IPS/UEBA
✓	✗	✗	✗
• Detects when a corporate device connects to an external network • Detects when credentials or hashes move over unencrypted wireless traffic	• Detects and controls entry to the corp network only • Would not “see” the external network, nor the connections to it	• Designed to protect the perimeter • Would not “see” the external network, nor the connections to it	• Neither IPS nor UEBA would “see” the external network and the connections to it

UNAUTHORIZED NETWORK BRIDGE

Printer Allowed Anyone to Connect

- A printer that is connected to the wired network has an open hotspot on it, providing access to unauthorized parties.

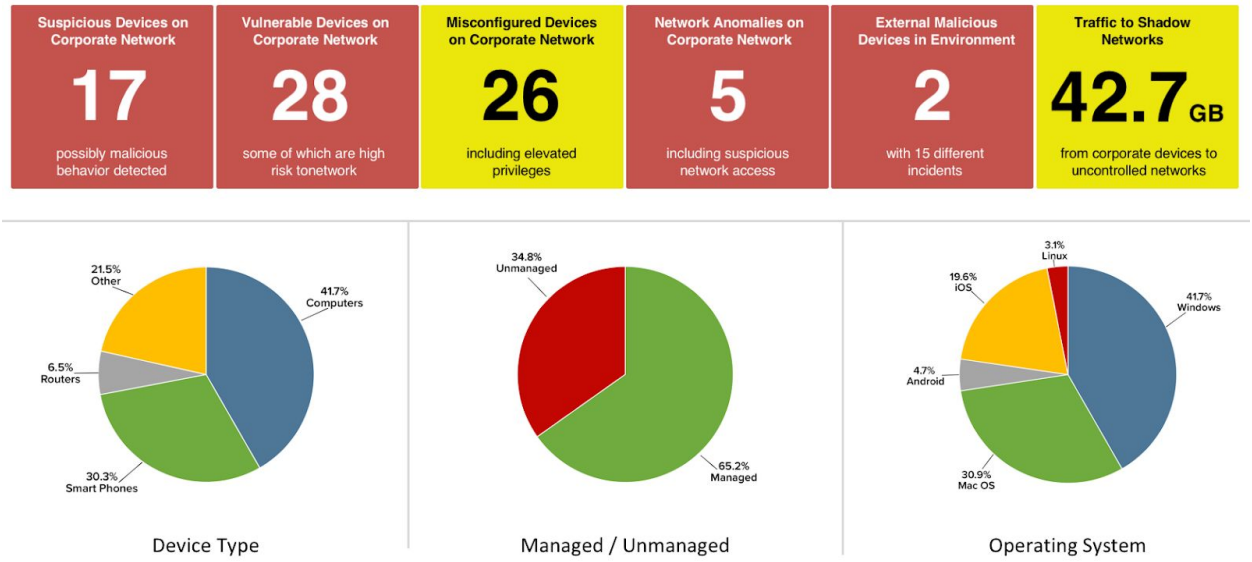
Armis	NAC	Firewall	IPS/UEBA
✓	✗	✗	✗
• Monitored the airspace • Discovered printer with open hot spot, provided an alert • If there were any actual connections to the printers, Armis would discover those, too	• Inventories devices and controls entry to the network • Does not monitor open hotspots or external connections to printers	• Designed to protect the perimeter • Does not monitor open hotspots or connections to those hotspots	• IPS looks for attack behavior, not for dormant open hotspots • UEBA would not see the hotspot or the external connections

COMPROMISED SMART TV

Smart Device Attempting to Infect Other Devices

- Boardroom was equipped with a Smart TV that had malware on it.
- Malware on the Smart TV was trying to infect nearby devices via Bluetooth

Armis	NAC	Firewall	IPS/UEBA
✓	✗	✗	✗
• Monitors Bluetooth & network traffic • Correlated traffic and activity to devices and locations. • Large amounts of WiFi & Bluetooth traffic detected. • TVs were beaconing to infect nearby devices	• The Smart TV was whitelisted on the NAC, so it let the TV onto the network. • Post-admission, NAC does not monitor behavior or external wireless connections	• The Smart TV was not sending out anything through the gateway. • The FW cannot see external wireless connections from devices	• The Smart TV was not sending out anything over the network. • The IPS cannot see external wireless connections from devices



Example of Armis Device Discovery and Security Assessment

Device Classification - Armis Device Knowledgebase Attributes

The following are a few representative examples of over 8,000 device characteristics and behavior traits stored in the Armis Device Knowledgebase. The total number of distinct device profiles currently exceeds 11 million.

Domains	• Which domains it accesses (if public)? • Are the DNS requests tunnel data? • How often it requests DNS servers? • How many different private DNS servers are requested? • How many DNS requests without accessing IP after? • How many public IPs accessed without DNS requests first? • How many different public IPs accessed? • How many different private IPs accessed? (What servers the device is contacting on the network?) • Are there external IPs used for internal purposes? • Which types of devices are called on private IPs?
Ports and protocols	• Which ports are used? • Which protocols are used per port? • How much data is used per port? • How many ephemeral ports are used? • Which ports seem to be open? • Existing / Used interfaces (Wi-Fi, Bluetooth, etc.) • How frequently is each port used? • How many different ports are used?
Time of activity	• Data histogram (average data sent per second/minute/hour/ • day/week/month) • Activity times by activity type • Data histogram per network

Headers	• User agents • Type of encryption • Cookies • Extension (X-*) headers • Method • Server • Path
Location or colocation	• Is the device stationary? • Is it moving at a specific speed? • Cross-reference of location/data usage • Location per time (same location at specific hours) • Co-location with other devices • Is the device behaving differently per location (DNS queries, traffic, etc.)
Device identity	• OUI • Device Name • OS / Version • Witnessed apps • User name
Other	• Fingerprints from DHCP • Fingerprints from SNMP • Fingerprints from other discovery protocols • Repetitiveness of data (same packets sent at different times) • Entropy of data measure (ArmisScore) • How is the device identified in the WLC? • Bluetooth services the device declares • SSID beaconing behavior (time, duration, SSID name, etc.) • Authentication and security of broadcasted network • TTL data per device • When the device downloads security updates • Duration of device connection to a specific network • How many different networks the device connected to • Frequency of network changing • Traffic between the device and other devices on the network • Cross-reference of all the above: For example, which ports/protocols are sending how much data per minute at which location?

About Armis

Armis is the leading agentless, enterprise-class device security platform, designed to protect organizations from cyberthreats created by the onslaught of unmanaged and IoT devices. Fortune 1000 companies trust our real-time and continuous protection to see and control all managed, unmanaged, un-agentable and IoT devices – from traditional devices like laptops and smartphones to new smart devices like smart TVs, webcams, printers, HVAC systems, industrial control systems and PLCs, medical devices and more. Armis provides passive and unparalleled asset inventory, risk management, and detection & response. Core to our platform is the Armis Device Knowledgebase. It is the world's largest cloud-based, crowd-source device behavior knowledgebase tracking 230 millions devices, and growing. Armis is headquartered in Palo Alto California.

armis.com

20200325-1