WHY ARMIS

WHY ARMIS

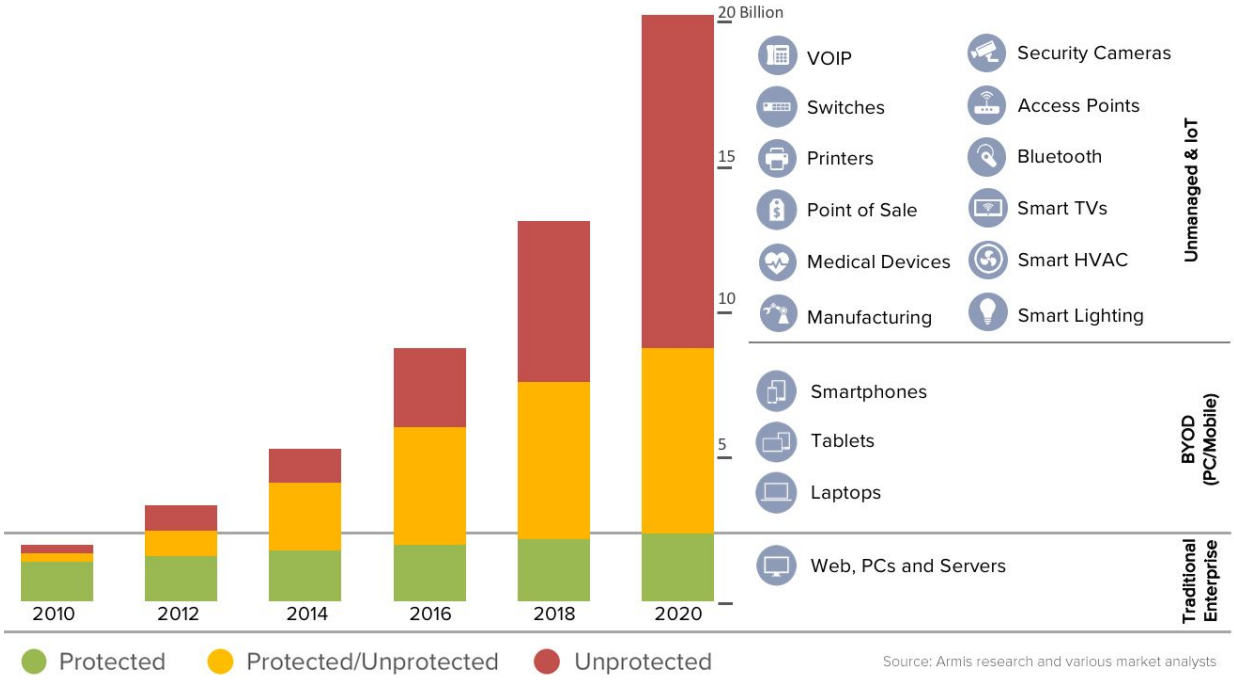
Top 10 Reasons To Consider Armis

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 inventory exceeds that of any other product on the market today.

2. Agentless

Armis is an agentless device security platform. We do not require agents or hardware, which makes Armis easy to deploy. It also means that Armis works with all types of devices, even those that can't accommodate agents. Typically, 40% of all devices in an enterprise cannot accommodate an agent, and that number is expected to grow to 60% by 2020 (see chart below). Unmanaged devices encompass a wide range of things — from printers, to VoIP phones, to security cameras, to the complete "Enterprise of Things."



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

3. Risks of Unmanaged Devices/IoT Are Increasing

Multiple sources—including the FBI, the US CERT, analysts such as Gartner, security vendors such as Symantec and Check Point and Verizon—confirm that attacks against unmanaged & IoT devices are increasing in number and sophistication. This reflects the new reality that unmanaged devices are now present in large numbers in enterprise environments, and these devices are typically *more* vulnerable than managed computers because they are not routinely patched.

Unmanaged devices can be easily reached by a remote attacker via a technique known as DNS rebinding, and the security vulnerabilities in unmanaged devices are too numerous to list. Once a device has been compromised, it can be used to launch an attack against the network infrastructure in order to break whatever network segmentation controls are in place.

Armis demonstrated this at the RSA security conference in May 2018, and the US CERT has warned that these attacks against enterprise network infrastructure are happening. In the face of this reality, traditional network segmentation controls—which are typically the only control that enterprises are using to "secure" unmanaged and IoT devices—are insufficient. 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. Entire Environment

Armis discovers and analyzes all endpoints no matter where they are or how they are connected to your network—wired, Wi-Fi, point-to-point technologies such as Bluetooth, and mesh technologies such as Zigbee. Armis even discovers and provides information about devices transmitting in your airspace such as rogue Wi-Fi access points and pineapples. The ability to capture this level of information without the need to deploy additional hardware is a unique Armis capability.

5. Passive Monitoring

Traditional network discovery tools probe your network intrusively. This approach can disrupt or even crash many kinds of devices, particularly operational technology. Armis takes a passive approach to monitoring devices. This means that Armis can't impacting network performance, other devices, or your users.

6. Device Classification

When the Armis platform detects a device either on or near your enterprise network, it uses the information it captures about the device's behavior and compares it with over 6 million known device profiles stored in the Armis Device Knowledgebase. This comparison allows the platform to identify devices with a high degree of accuracy including specific information like device make, model, location, and expected

behaviors. The following are actual examples of devices the Armis platform discovered in enterprise environments, as well as the device characteristics and behavior traits that were matched in the Armis Device Knowledgebase.

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. Real-Time Operation

Armis operates in real-time which means that transient devices are discovered, and short-lived events are processed by the Armis' cloud-based Risk Analysis Engine.

8. Proactive Risk Analysis

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

9. Threat Detection

The Armis Risk Analysis Engine compares observed device characteristics and behavior against a baseline of what we know to be normal behavior for each type of device. The Armis Device Knowledgebase includes both what we have observed in your environment and over six million unique device profiles that we have observed in other customer environments. See examples at the end of this document.

10. Automatic Protection

Armis doesn't just generate alerts—it triggers automated actions to stop an attack. Armis integrates 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.

Examples of Armis Threat Detection in Real World Environments

COMPROMISED TABLET

Unauthorized Video Streaming

- Every conference room had an 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.

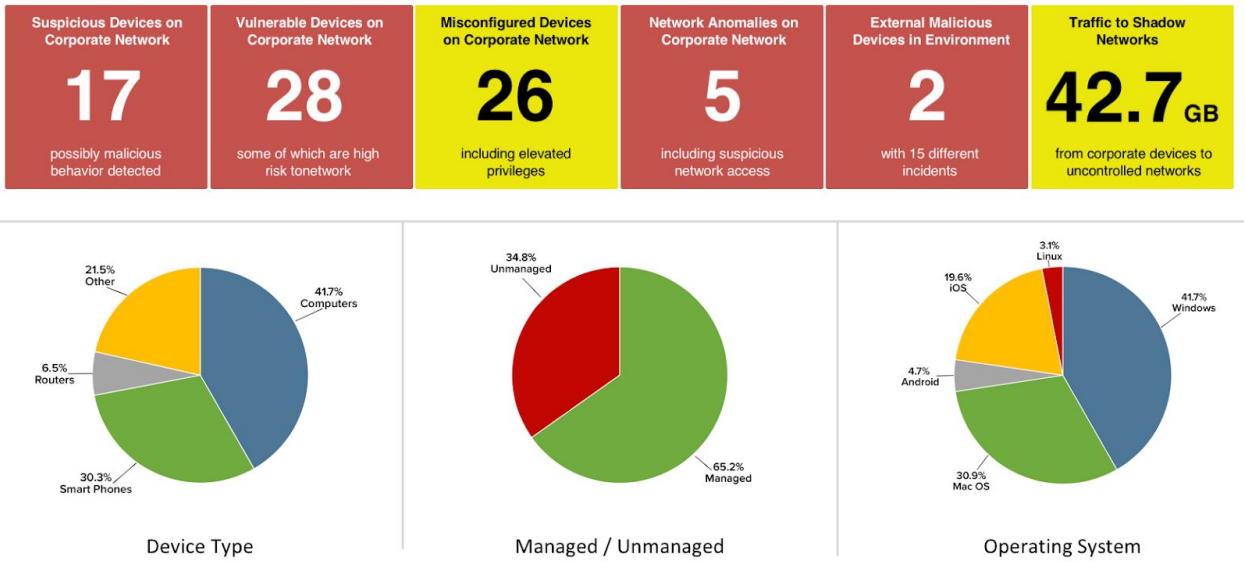
Armis	NAC	Firewall	IPS/UEBA
✓	✗	✗	✗
• Monitored the airspace • Discovered printer with open hot spot, provided an alert • If there were any actual connections to the printers, Armis would discover those, too	• Inventories devices and controls entry to the network • Does not monitor open hotspots or external 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 6 million.

Domains	• Which domains it accessing (if public)? • Are the DNS requests tunnel data? • How often requests DNS servers? • How many different private DNS servers 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 first agentless, enterprise-class security platform to address the new threat landscape of unmanaged and IoT devices. Fortune 1000 companies trust our unique out-of-band sensing technology to discover and analyze all managed, unmanaged, and IoT devices—from traditional devices like laptops and smartphones to new unmanaged smart devices like smart TVs, webcams, printers, HVAC systems, industrial robots, medical devices and more. Armis discovers devices on and off the network, continuously analyzes endpoint behavior to identify risks and attacks, and protects critical information and systems by identifying suspicious or malicious devices and quarantining them. Armis is a privately held company and headquartered in Palo Alto, California.

armis.com

20190527.1