armis

AGENTLESS DEVICE DISCOVERY & RISK ASSESSMENT

The Most Comprehensive Visibility for Managed and Unmanaged Devices

Visibility of all devices across an organization is fundamental to any security strategy. Today organizations must not only get an accurate inventory of all managed devices, but must address the exponential growth of unmanaged devices in the workplace. Armis provides the ability see them both.

Visibility. It is the critical need for every organization. All of the major security frameworks, such as the CIS Critical Security Controls and the NIST Framework for Improving Critical Infrastructure Cybersecurity, start with inventory. Easy to say, but much harder to do.

Which is why organizations still struggle to accurately identify all the devices in their environment. In fact, Armis research shows that on average companies are blind to 40% of the devices in their environment. This blind spot includes traditional devices like laptops, desktops, and smartphones, as well as new unmanaged smart devices like smart TVs, webcams, printers, HVAC systems, industrial robots, medical devices and more. As a result, businesses do not have a real-time, comprehensive view of all the assets in their environment—or know the risks associated with them.

The Visibility Problem

The typical large enterprise owns several kinds of visibility tools, each having a certain set of strengths and weaknesses. For example, agent-based tools can provide detailed information about the organization's **managed** computers—but only when the agents are working properly. Unfortunately, these systems are brittle (especially in large environments), the agents sometimes break or are disabled by the users, and of course the scope of agent-based systems does not extend to unmanaged or IoT devices.

Network scanners suffer from a different set of problems, as do network access control tools (see table). In all cases, these tools suffer from limited scope and/or inability to provide enough information to satisfy security use-cases.

THE ARMIS DIFFERENCE

Comprehensive
Managed or unmanaged, discovers & classifies all devices, on or off the network.

Agentless
Nothing to install on devices, no specific configuration or programming.

Passive
No negative impact on network performance.

Frictionless
Installs in minutes to hours. Leverages your existing infrastructure.

Visibility of **unmanaged devices** is critically important because of their exponential growth and sheer volume, as the number of unmanaged devices on most enterprise networks exceeds the number of managed endpoints. Moreover, these devices tend to be even more risky than managed endpoints, for the following reasons:

- Most of these types of devices cannot accommodate an agent, so they can't be secured.
- They are typically designed without much regard to security. For example, they often utilize unauthenticated management servers that can be remotely compromised via the DNS Rebinding exploit.
- Their embedded operating systems (Linux, Windows, Android) are not routinely updated, so over time they accumulate a large number of common software vulnerabilities.

- They are often installed without oversight by the security team, and without proper hardening and configuration. For example, they often are installed with default passwords.

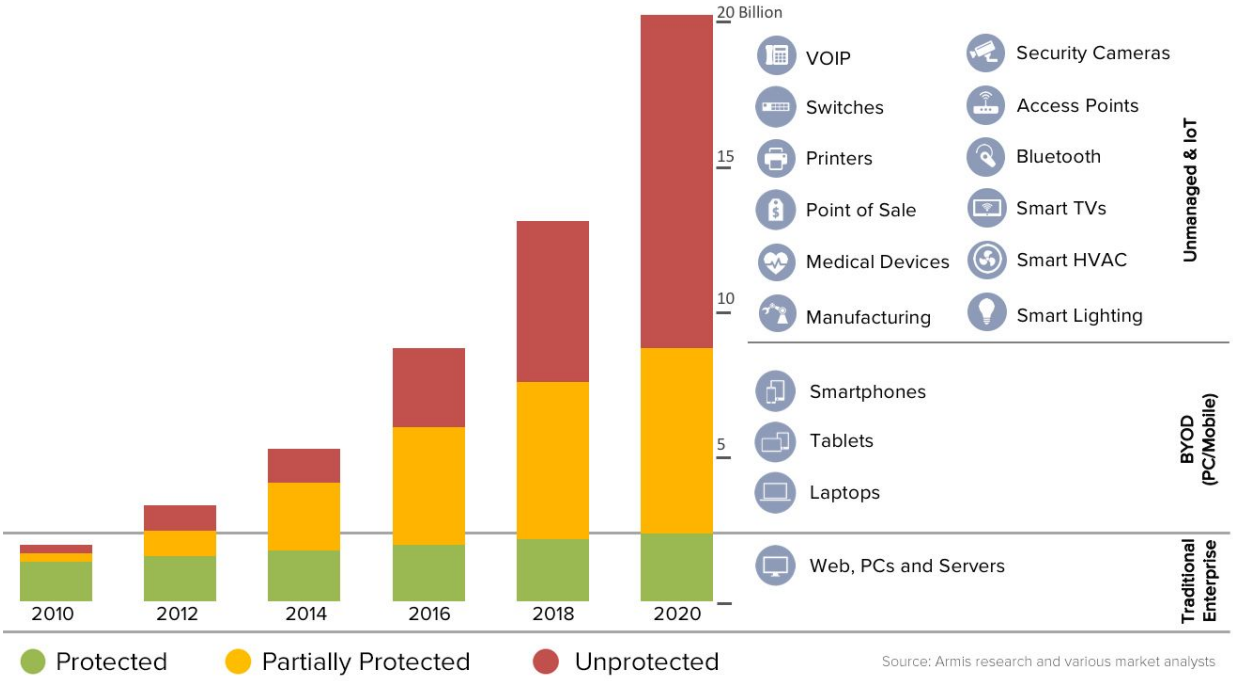

Figure 1: Visibility will only get harder with the growth of unmanaged devices in the enterprise

Security practitioners need a wide range of information about the devices in their environment, including visibility to the:

- "Things" themselves - What are they?
- Software running on the "things" - How vulnerable it is?
- Configuration of the device - Is it using default passwords, or sending sensitive data unencrypted?
- Activities of the device - Connections, traffic, relationships?
- Context of each device - Who owns it, where it is, and how it is supposed to be used?
- Risks and threats - Are they vulnerable? Are they at risk?

The answers to these questions will allow you to take proactive steps to protect your enterprise.

> Unmanaged and IoT devices are the new attack landscape.
> The FBI has issued recent alerts on attacks targeting these devices.
>
> *FBI, Alert I-080218-PSA, Aug 02, 2018*

Armis Eliminates the Visibility Blind Spot

Armis is the industry's most comprehensive device discovery platform. The Armis security platform is purpose-built to fill the gaps left by traditional visibility tools, discovery tools, and risk assessment programs. It requires no agents or additional hardware, making deployment fast and simple with very little impact to your existing IT infrastructure. Unlike tools that provide a limited amount of information about *some* of your connected devices, Armis provides a broad range of information about *every* device in your environment.

Discovery

Armis discovers and classifies every managed, unmanaged, and IoT device in your environment. The scope includes devices on your network (both wired and Wi-Fi) as well as off-network devices that are communicating via Wi-Fi, Bluetooth, and other peer-to-peer IoT protocols—a capability no other security product offers without requiring additional hardware sensors.

Unlike network scanners, Armis does not need specific configuration or programming. Instead, it's designed to analyze information from all parts of your network by default, providing coverage to all regions of your environment. It also builds a device inventory in real-time, ensuring that even transient devices are included.

COMPLETE DISCOVERY

Armis discovers all devices

- Managed and unmanaged
- Wired or wireless
- On or off the network

The scope of information that Armis provides for unmanaged devices is also the most comprehensive on the market. Unlike other "visibility" tools that simply tell you a device exists, the Armis platform tells you a wide range of information about each device, which is important for security use-cases. Below is a partial list of device characteristics we identify:

Device Information	Endpoint Behavior	Connection Information
• Device type • Manufacturer • IP address • MAC address • Computer name • User name	• Stationary vs. moving • Communication timing • Communication volumes • Cloud services accessed • Tunnels utilized • Encryption usage	• Connection type (wired, WiFi, Bluetooth, etc.) • Connection point (corp, guest, rogue, etc.) • Traffic volume and timing • Internet domains accessed
Software Information	**Wi-Fi Information**	**Switch Information**
• OS type and version • Applications	• AP name • AP CPU utilization • AP bandwidth utilization • AP OS version	• Switch name and location • Switch CPU utilization • Switch configuration • Internet domains accessed

Fig. 2: Sample of information Armis provides about devices

Figure 3 below shows the breadth of devices—both managed and unmanaged—that Armis is able to discover and identify. In addition, Armis can identify threats and risks associated with each device.

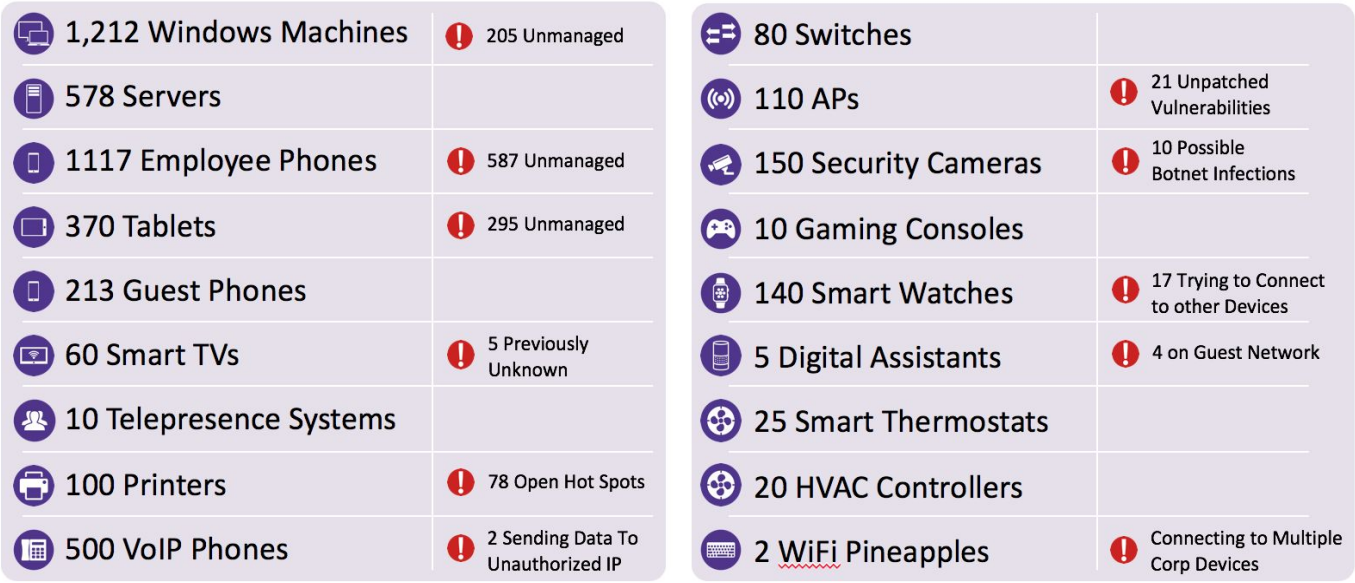

Figure 3: Sample list of discovered items, from a Fortune 1000 company.

Compare Armis to traditional solutions used for discovery

OTHER PRODUCTS	ARMIS
• Agent-based systems are designed to provide information about managed computers. They perform poorly or not at all with unmanaged devices.	• Armis is agentless, and provides a full asset inventory of everything in your environment, both managed and unmanaged assets.
• Network-based visibility tools, such as network access control (NAC), are blind to devices communicating in the airspace using Wi-Fi, Bluetooth, Zigbee, etc.	• Armis sees everything, including devices communicating in your airspace, to give you a more comprehensive inventory of devices and associated risks.
• Network access control (NAC) is not designed to assess the risk of unmanaged devices or monitor their behavior.	• Armis analyzes each device (managed and unmanaged) and calculates its risk score based on many factors including software vulnerabilities we detect, observed behavior, threat intelligence, and more.
• Scanner tools that run periodically, weekly or monthly, miss seeing transient devices.	• Armis discovers devices in real-time.

Risk Assessment

Being aware that devices exist isn't enough. You need to know whether or not they're at risk. Armis tells you, in simple terms.

After discovering and identifying each device, the Armis platform analyzes the device and calculates its risk score. The score is based on multiple risk factors. Armis' cloud-based risk analysis engine compares observed device characteristics and behavior against our Device Knowledgebase which contains 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 customers' environments.

This risk score helps your security team take proactive steps to reduce your attack surface. It also helps you comply with regulatory frameworks that require you to identify and prioritize all vulnerabilities.

Unlike other vendors, Armis provides risk scores for all devices automatically. There is nothing that you need to enter into the system—no policies or whitelists that you need to know in advance. Armis automatically generates a risk score based on the extensive knowledge that we have in our Device Knowledgebase combined with multiple threat intelligence feeds and machine learning.

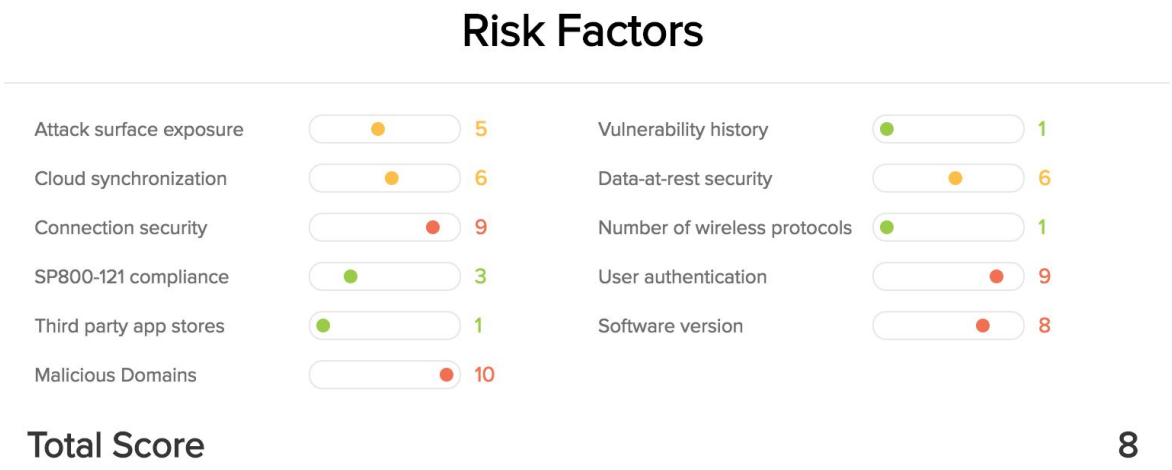

Figure 3: Sample risk score in the Armis console.

Frictionless Implementation

The benefits of the Armis platform are many, while the impact on your resources is low. The Armis security platform does not require agents or additional hardware. Instead, it works with your existing network infrastructure to collect the data it needs to discover, identify, and analyze the risk of all devices in your environment. The Armis platform collects data using a virtual appliance that sits out-of-band and passively monitors traffic. Since the platform is not in-line, it has no impact on network performance, other devices, or your users. It does not require any changes to your existing network, and it does not introduce any latency.

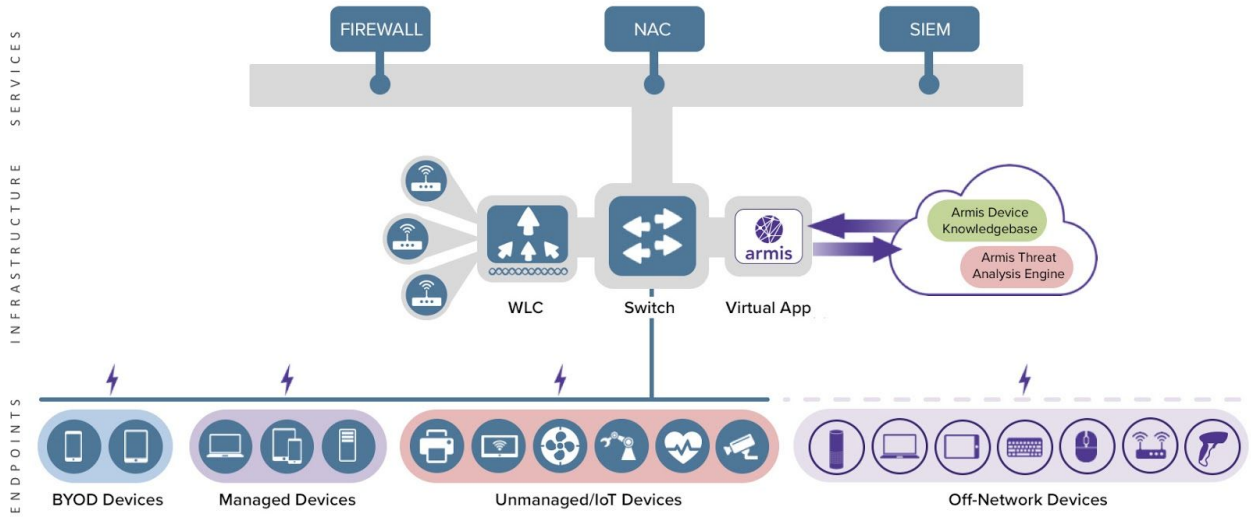

Figure 4: Armis agentless platform architecture

The Complete Picture

Once installed, Armis will begin discovering, classifying, and rating risk for all devices in your environment in real-time. Armis customers who have discovered and assessed the risks of previously unknown devices in their environment, are now able to prioritize their efforts and reduce their attack surface proactively.

On an ongoing basis, Armis helps identify attacks within your network involving unmanaged devices and can trigger automated actions to stop such attacks. Through its integration with your existing security enforcement points like Cisco and Palo Alto Networks firewalls, Network Access Control (NAC) products, and your wireless LAN controllers, Armis can automatically take action and restrict access of malicious devices immediately when they attack your network.

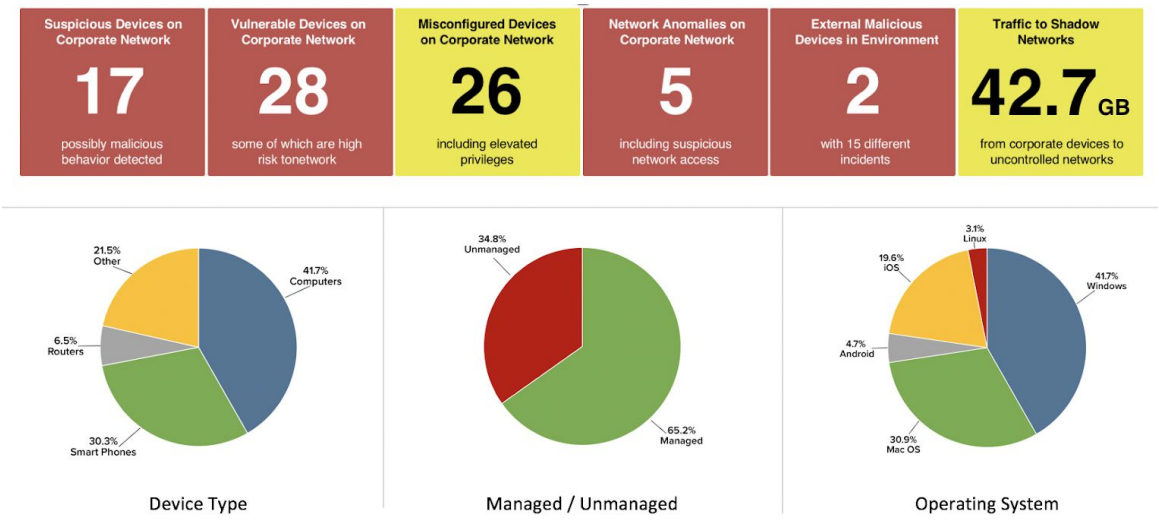

Figure 5: Sample top-line results from the Armis Device Security and Risk Assessment report.

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 laptop and smartphones to new unmanaged smart devices like smart TVs, webcams, printers, HVAC systems, industrial robots, medical devices and more. Armis discovers devices on & 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

20180924.1