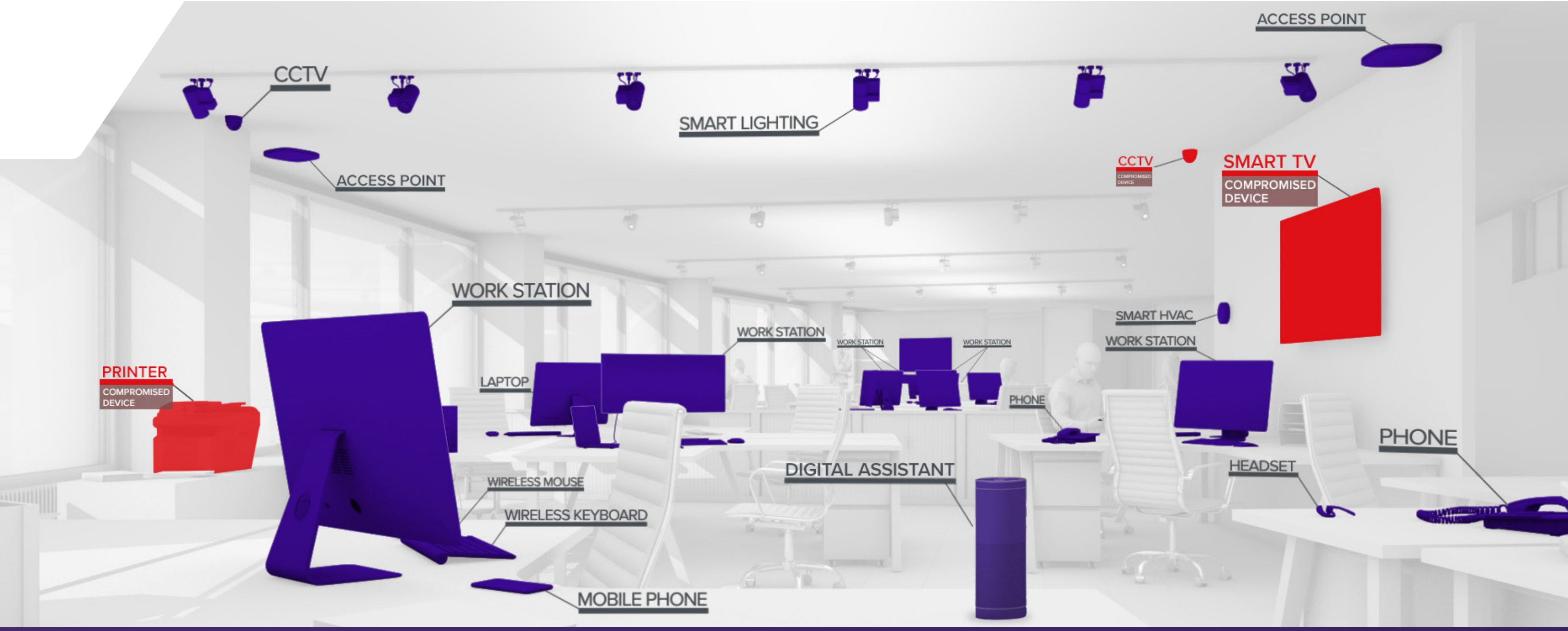


AGENTLESS DEVICE DISCOVERY AND RISK ASSESSMENT

The Most Comprehensive Cybersecurity Asset Management for Managed, Unmanaged & IoT 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 devices, managed, unmanaged, and IoT, but must also understand the risks associated with each device. Armis provides both types of information.

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. They need unified asset management of all devices - managed or unmangaged.

THE VISIBILITY PROBLEM

We have seen an explosion of all types of new devices and assets across the enterprise. At the same time, today we see 25 or so IT management and security solutions used across businesses that gather data about those devices and assets. With the increase in devices and tools comes a fragmentation in visibility, and gaps in security.

Agented solutions are valuable for traditional devices. But even they have issues of breaking or being 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 1). In all cases, these tools suffer from limited scope and/or inability to provide enough information to satisfy security use-cases.

THE ARMIS ADVANTAGE

COMPREHENSIVE
Discovers and classifies all assets in your environment, on or off your network.

AGENTLESS
Nothing to install on devices, no configuration, no device disruption.

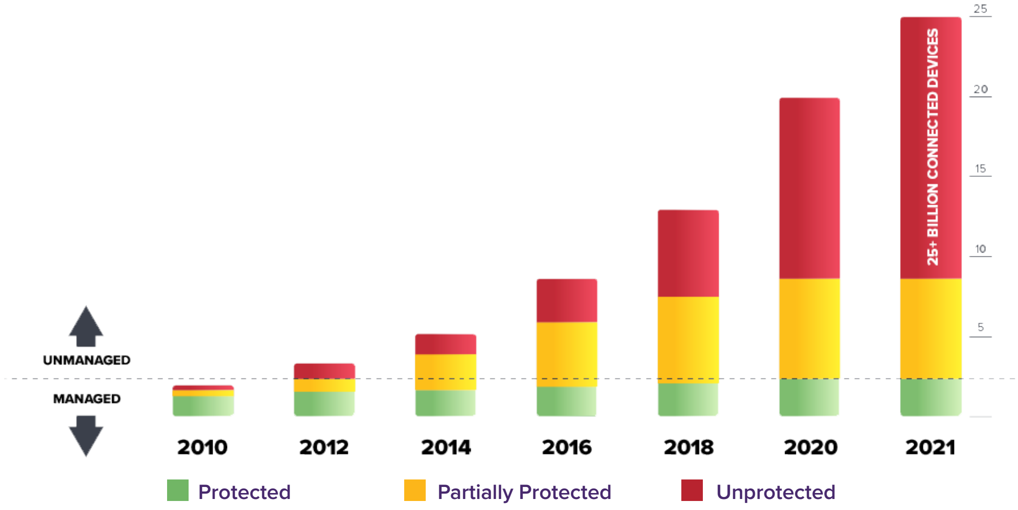
PASSIVE
No impact on your organization's network. No device scanning.

FRICTIONLESS
Deploys in minutes using the systems and infrastructure you already have.

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 riskier 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 as identified in the URGENT/11 or CDPwn vulnerabilities.
- Their embedded operating systems (Linux, Windows, Android, VxWorks, etc.) 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.

THE EXPLOSION OF “THINGS”



Cloud & Virtual Machines

- Amazon Web Services
- Microsoft Azure
- Google Cloud

Unmanaged & IoT

- VOIPs
- Switches
- Printers
- Point of Sale
- Medical Devices
- Manufacturing
- Smart TVs
- Smart HVAC
- Smart Lighting
- Security Cameras
- Access Points
- Badge Readers

BYOD (PC & Mobile)

- Smartphones
- Tablets
- Laptops

Traditional Enterprise

- Web
- PCs
- Servers

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?
- Gaps - How do I get a unified view of my asset inventory?
- 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.

FBI warns of security issues with smart TVs.
October 2019

Cyberattacks On IoT Devices Surge 300% In 2019
September 2019

Microsoft warns of hacker group targeting IoT devices.
August 2019

ARMIS ELIMINATES THE VISIBILITY BLIND SPOT

Armis provides the most comprehensive cybersecurity asset management for businesses. The Armis agentless device security platform is purpose-built to fill the gaps left by traditional visibility tools, discovery tools, asset management 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/security solutions and 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.

UNIFIED CYBERSECURITY ASSET MANAGEMENT

Armis discovers and classifies every managed, unmanaged, and IoT device in your environment. It aggregates device information across all your IT and security management solutions. Additionally, it identifies devices on your network (both wired and Wi-Fi) as well as off-network devices communicating via Wi-Fi, Bluetooth, and other peer-to-peer IoT protocols, as well as off prem devices.

By connecting all these sources of device and device data, Armis delivers a trusted, comprehensive, and unified asset management of the devices in your environment. It is completely passive, and builds a comprehensive device inventory in real-time, ensuring that every device, even transient devices, are included.

COMPLETE DISCOVERY

Armis discovers all devices

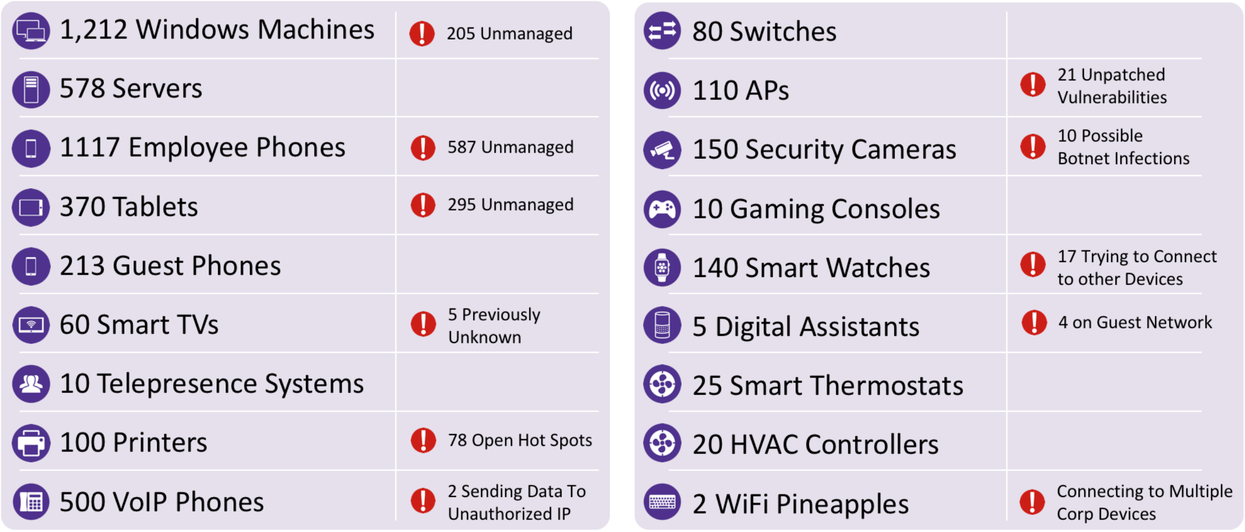
- Managed and unmanaged
- Wired or wireless
- On of off the network or premises

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, Wi-Fi, 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

Figure 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.



1,212 Windows Machines	205 Unmanaged
578 Servers	
1117 Employee Phones	587 Unmanaged
370 Tablets	295 Unmanaged
213 Guest Phones	
60 Smart TVs	5 Previously Unknown
10 Telepresence Systems	
100 Printers	78 Open Hot Spots
500 VoIP Phones	2 Sending Data To Unauthorized IP

80 Switches	
110 APs	21 Unpatched Vulnerabilities
150 Security Cameras	10 Possible Botnet Infections
10 Gaming Consoles	
140 Smart Watches	17 Trying to Connect to other Devices
5 Digital Assistants	4 on Guest Network
25 Smart Thermostats	
20 HVAC Controllers	
2 WiFi Pineapples	Connecting to Multiple Corp Devices

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 comprehensive 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 & associated risks.
Network access control (NAC) is not designed to assess the risk of unmanaged devices or monitor their behavior.	Armis analyzes devices (managed and unmanaged) and calculates a risk score based on factors like software vulnerabilities, behavior, threat intelligence & more.
Scanner tools that run periodically, weekly or monthly, miss seeing transient devices.	Armis discovers devices in real-time.
Legacy solutions bring a fragmented approach to even managed devices, siloed across disparate systems, and no tracking of unmanaged devices.	Armis brings visibility to every asset, across your IT and Security management solutions and your network - providing a unified view of all assets.

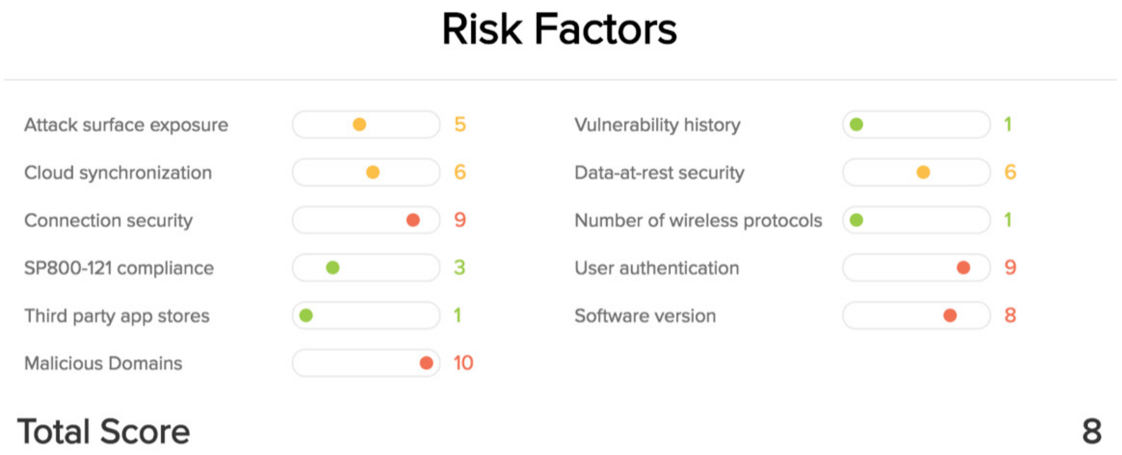
Table 1: Legacy solutions do not address the unmanaged devices challenge - nor do they provides a unified asset management.

RISK MANAGEMENT

Being aware that devices exist isn't enough. You need to know whether or not that device is at risk. 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 identifies this risk score based not just on the device, manufacturer, reputation, and known vulnerabilities - but by comparing the device to all similar devices in our Device Knowledgebase, where we track over 280 million devices each day. It is the largest cloud-based, crowd sourced device behavior knowledgebase where we compare that device and its behavior against "good known" profiles of devices to identify if there is an issue or threat.

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.



Risk Factors

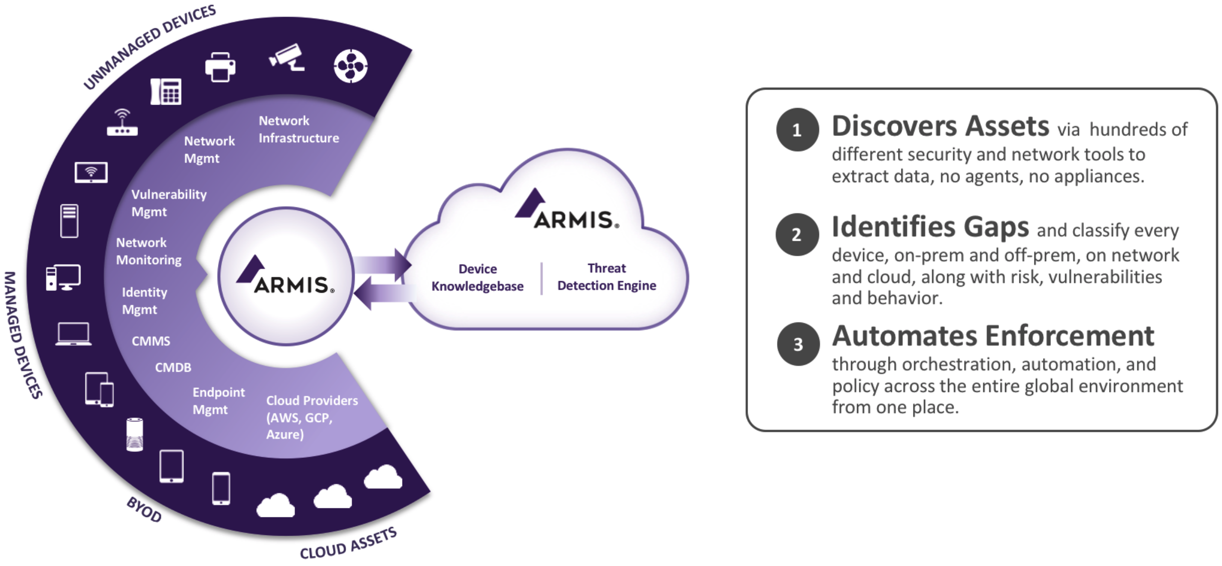
Attack surface exposure	5	Vulnerability history	1
Cloud synchronization	6	Data-at-rest security	6
Connection security	9	Number of wireless protocols	1
SP800-121 compliance	3	User authentication	9
Third party app stores	1	Software version	8
Malicious Domains	10		

Total Score 8

Figure 4: Sample list of discovered items, from a Fortune 1000 company.

FRICTIONLESS IMPLEMENTATION

Armis delivers these benefits with an extremely low impact on your resources. Our security platform does not require agents or additional hardware. It integrates easily with your existing IT and security management solutions and your network infrastructure to collect and aggregate the data it needs to discover and identify all the devices in your environment. We use a simple virtual machine that sits out-of-band and passively to collect data or monitor traffic. It does not disrupt your systems, network, or the devices it is tracking.



1 **Discovers Assets** via hundreds of different security and network tools to extract data, no agents, no appliances.

2 **Identifies Gaps** and classify every device, on-prem and off-prem, on network and cloud, along with risk, vulnerabilities and behavior.

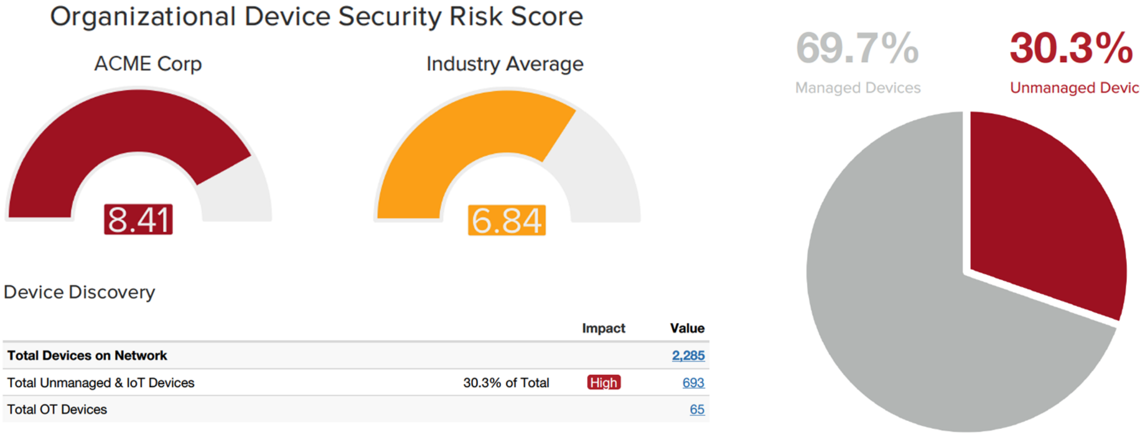
3 **Automates Enforcement** through orchestration, automation, and policy across the entire global environment from one place.

Figure 5: Armis agentless platform architecture

THE COMPLETE PICTURE

As mentioned, Armis begins discovering, classifying, and rating risk for all devices across your environment in real-time immediately upon installation. With this comprehensive inventory of devices and risks, IT and security professionals can more effectively prioritize their efforts to reduce their attack surface proactively, while improving their compliance and business continuity postures.

On an ongoing basis, Armis helps identify and stop attacks across your organizations. Armis can provide detection and response, orchestrating automatic security and policy enforcement. Through its integration with your existing security enforcement points like Cisco and Palo Alto Networks firewalls, Network Access Control (NAC) products, and network infrastructure, along with your other security solutions, Armis can automatically take action and restrict access of malicious devices immediately when devices are exposed, unsecured, or acting suspiciously or maliciously.



Device Discovery

		Impact	Value
Total Devices on Network			2,285
Total Unmanaged & IoT Devices	30.3% of Total	High	693
Total OT Devices			65

Figure 6: Sample top-line results from the Armis Device Security and Risk Assessment report.

ABOUT ARMIS

Armis® is the leading agentless, enterprise-class device security platform designed to address the new threat landscape of unmanaged and IoT devices. Fortune 1000 companies trust our real-time and continuous protection to see and control all managed, unmanaged, 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. Armis is a privately held company and headquartered in Palo Alto, California.

ARMIS

☎ 1.888.452.4011 armis.com