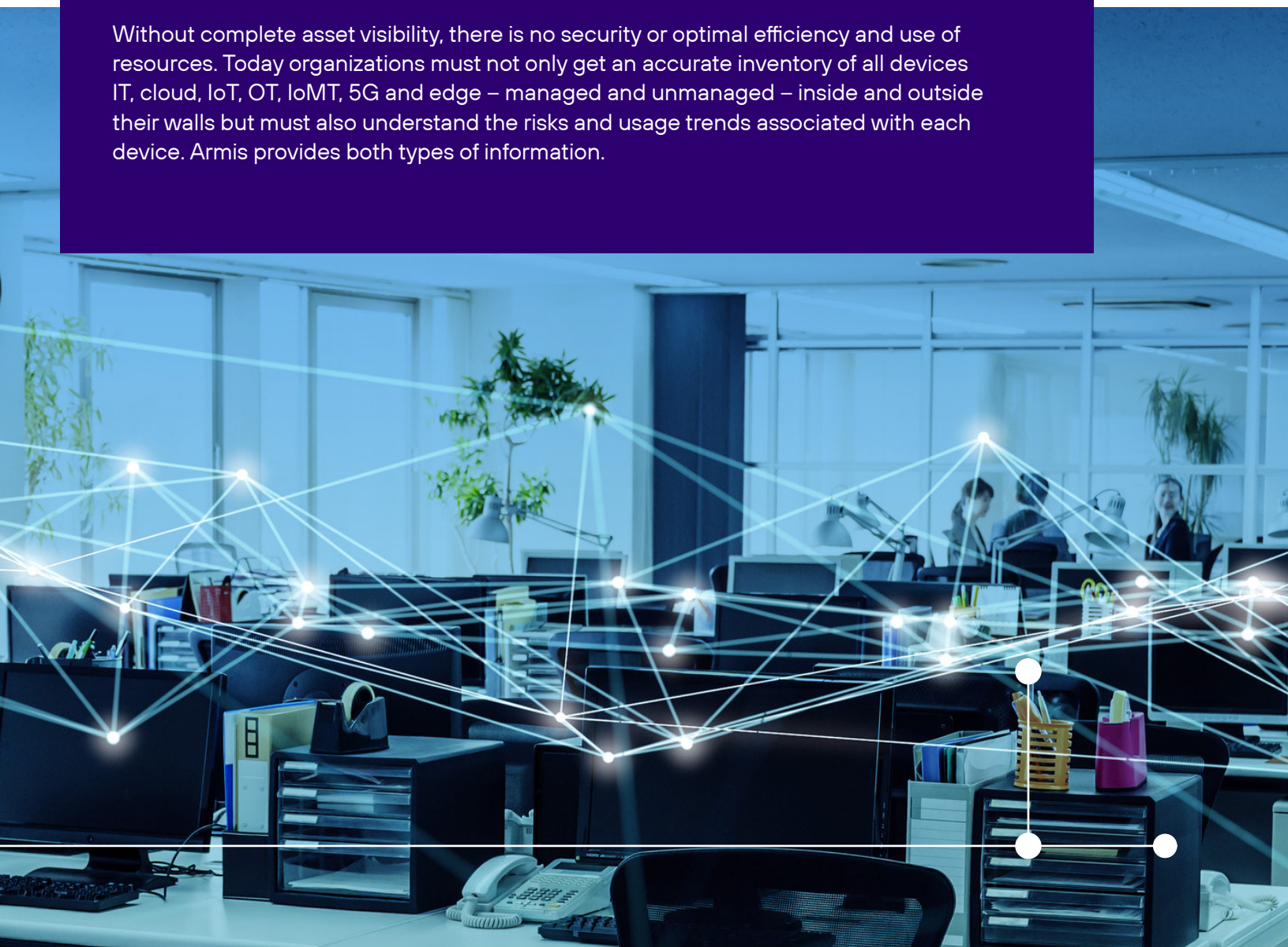
ARMIS®

White Paper

Agentless asset discovery, risk assessment, and intelligence.

The most comprehensive asset management for managed, unmanaged, and IoT devices.

Without complete asset visibility, there is no security or optimal efficiency and use of resources. Today organizations must not only get an accurate inventory of all devices IT, cloud, IoT, OT, IoMT, 5G and edge – managed and unmanaged – inside and outside their walls but must also understand the risks and usage trends associated with each device. Armis provides both types of information.



Asset visibility

It is the critical need for every organization. All the major security frameworks, such as the CIS Critical Security Controls and the NIST Framework for Improving Critical Infrastructure Cybersecurity, start with inventory. And in our perimeter-less world, that can be much easier said than done.

Today, most organizations struggle to accurately identify all the assets in their environment. In fact, Armis research shows that up to 90 percent of assets will be unmanaged and on average companies are blind to at least 40 percent of the assets in their environment. This huge blind spot includes traditional assets like laptops, desktops, and smartphones, as well as new unmanaged smart assets like smart TVs, webcams, printers, HVAC systems, security cameras, industrial robots, medical devices and more. Not only do businesses lack a real-time, comprehensive view of all the assets in their environment—they are in the dark about the associated risks and vulnerabilities these assets represent. But asset visibility is not just about threat mitigation. It also contributes to everything from efficient asset usage and SOC team workflows to the ability to innovate with confidence. That's why unified management of all assets managed or unmanaged has become so critical.

The Armis advantage

Complete visibility

- Powerful discovery
- Unified asset inventory

Contextual intelligence

- Multidimensional views
- Comprehensive analytics and intelligence

Continuous security

- Vulnerability assessment
- Policy enforcement

Rapid time to value

- Modern cloud architecture
- Industry leader, trusted partner

The visibility problem

We have seen an explosion of all types of new devices and assets across the enterprise. At the same time, most enterprises are using roughly 25 IT management and security solutions as part of their efforts to monitor, manage, and secure their assets. But asset and tools proliferation is contributing to fragmented visibility, critical gaps in security, and unnecessary spend.

Agented solutions are valuable for securing traditional assets. They are never deployed to 100 percent of target assets and can be unreliable, losing communication, becoming out of date, or being disabled by the users. And, of course, the scope of agent-based systems does not extend to unmanaged or IoT assets.

Network scanners and network access control tools also fall short when it comes to protecting against unseen and operational cyber risks, and optimizing resource usage. For example, network scanning tools that rely on point-in-time scans may miss transient assets. And they also can't scan employees' home networks. In all cases, these tools provide either limited scope and/or inability to provide enough asset behavior and context information to satisfy security and asset optimization use-cases (see table 1 on page 7 for more details).

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

- Most of these types of assets 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 (for example, Linux, Windows, Android and VxWorks) are not routinely updated, leading to an accumulation of a large number of common software vulnerabilities over time.
- 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'

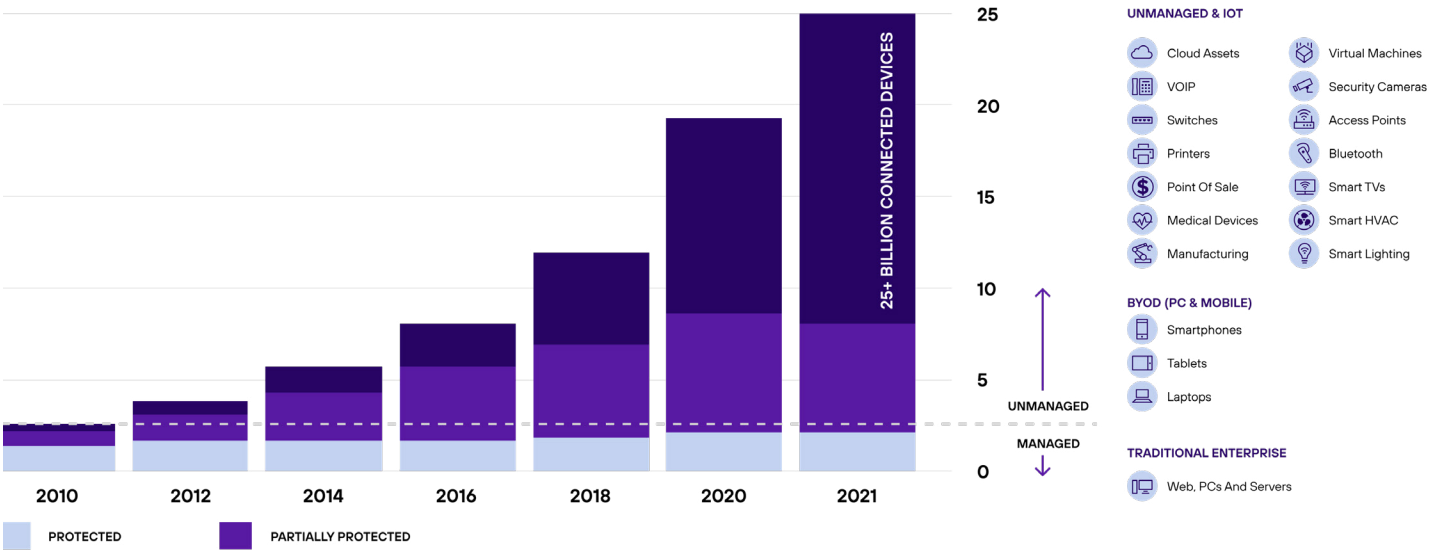


Figure 1: Visibility will only get harder with the growth of unmanaged devices in the enterprise.

Security and IT practitioners need a wide range of information about the assets in their environment, including visibility into:

- "Things" themselves, including unsanctioned and rogue assets: What are they?
- Gaps: How do I get a unified view of my asset inventory?
- Software running on the "things": How vulnerable is it?
- Configuration of the asset: Is it using default passwords, or sending sensitive data unencrypted?
- Activities of the asset: Connections, traffic, relationships?

- Context of each asset: Who owns it, where it is, and how it is supposed to be used?
- Asset utilization: is the user utilizing the asset or simply storing it?
- 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 while optimizing efficiency, and supporting innovation with confidence.

The headlines speak volumes

IoT Attacks Skyrocket, Doubling in 6 months.
ThreatPost, September 2021

TLStorm exploits expose more than 20 million UPS units to takeover. Was yours one of them?
TechRepublic, March 2022

Log4j could be the most serious security threat ever seen, CISA head warns
TechRadar, December 2021

Armis eliminates visibility blind spots

Armis provides the most comprehensive asset intelligence platform for businesses, providing unified visibility, asset intelligence, and superior security. The Armis unified asset intelligence 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 assets, the Armis platform aggregates asset information across all your IT and security management solutions and provides a broad range of information about every managed, unmanaged, and IoT asset in your environment. It also identifies assets on your network (both wired and Wi-Fi), including off-network assets communicating via Wi-Fi and other peer-to-peer IoT protocols, and off-prem assets.

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

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

Visibility and control

The Armis unified asset intelligence delivers:

- **Complete** visibility to see every asset
- **Contextual** intelligence to know your asset truth
- **Continuous** security to protect the business

Device Information

- Device type
- Manufacturer
- IP address
- MAC address
- Computer name
- User name

Endpoint Behavior

- Stationary vs. moving
- Communication timing
- Communication volumes
- Cloud services accessed
- Tunnels utilized
- Encryption usage

Connection Information

- Connection type (e.g., wired, Wi-Fi)
- Connection point (e.g., corporate, guest, rogue)
- Traffic volume and timing
- Internet domains accessed

Software Information

- OS type and version
- Applications

Wi-Fi Information

- Access point (AP) name AP CPU utilization
- AP bandwidth utilization
- AP OS version

Switch Information

- Switch name and location
- Switch CPU utilization
- Switch configuration
- Internet domains accessed

Figure 2 below shows the breadth of assets—both managed and unmanaged—that Armis can discover and identify. In addition, Armis can identify threats and risks associated with each asset.

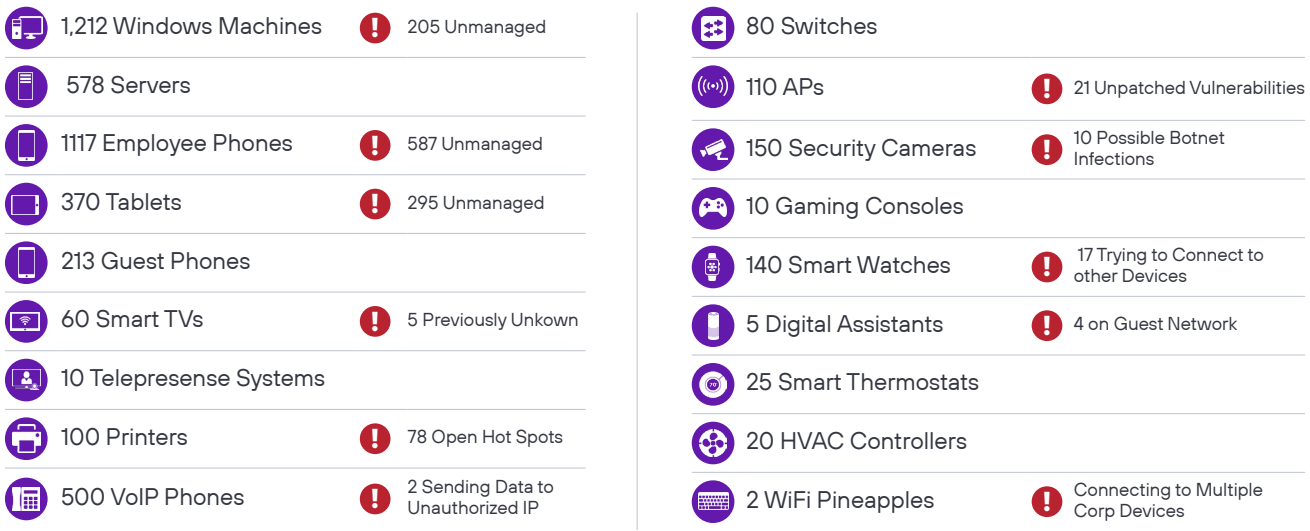


Figure 2: Sample list of discovered items, from a Fortune 1000 company.

Compare Armis to traditional solutions used for discovery

Other Products	ARMIS.
Agent-based systems are designed to provide information about managed computers. They typically don't work with unmanaged assets, and usually perform poorly when they do.	Armis discovers every connected asset across IT, IoT, OT, IoMT, 5G, virtual, and cloud including managed, unmanaged, and unmanageable assets, with the industry's most powerful agentless asset discovery and connection mapping.
Network-based visibility tools, such as network access control (NAC), are blind to assets communicating in the airspace using Wi-Fi.	Armis sees everything, including assets communicating in your airspace, to give you a more comprehensive inventory of assets and associated risks.
Network access control (NAC) is not designed to assess the risk of unmanaged assets or monitor their behavior.	Armis delivers deep context to fingerprint unknown assets, enrich asset data, assess asset behavior anomalies, and resolve asset conflicts through the industry's only global asset knowledgebase and multi-dimensional views of all assets.
Scanner tools that run weekly or monthly miss transient assets.	Armis discovers all connected assets in real-time.
Even for managed assets, legacy solutions only provide fragmented views that are siloed across disparate systems with no unmanaged asset tracking.	Armis provides real time cyber threat intelligence and enrichment to orchestrate effective response through trusted security partners and adaptive trust policies. Actively secures every asset, reduces threat response time. Monitors asset utilization to improve efficiency help optimize resource usage. Underpins innovation initiatives with in-depth visibility and robust protections.

Table 1: Legacy solutions do not address the unmanaged devices challenge - nor do they provide contextual intelligence and continuous security.

Risk management

Being aware that assets exist isn't enough. You need to know whether that asset is at risk. After discovering and identifying each asset, the Armis platform analyzes the asset and calculates its risk score. The score is based on multiple risk factors. Armis identifies this risk score based not just on the asset, manufacturer, reputation, and known vulnerabilities—but by comparing the asset to all similar assets in the Armis Intelligence Engine, where we track over two billion assets—and growing—each day. It is the largest cloud-based, crowd-sourced asset behavior knowledgebase where we compare the behavior of each asset against "known-good" baselines for similar assets we have seen in other environments 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 assets 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 the Armis Intelligence Engine combined with multiple threat intelligence feeds and machine learning.

Risk Factors

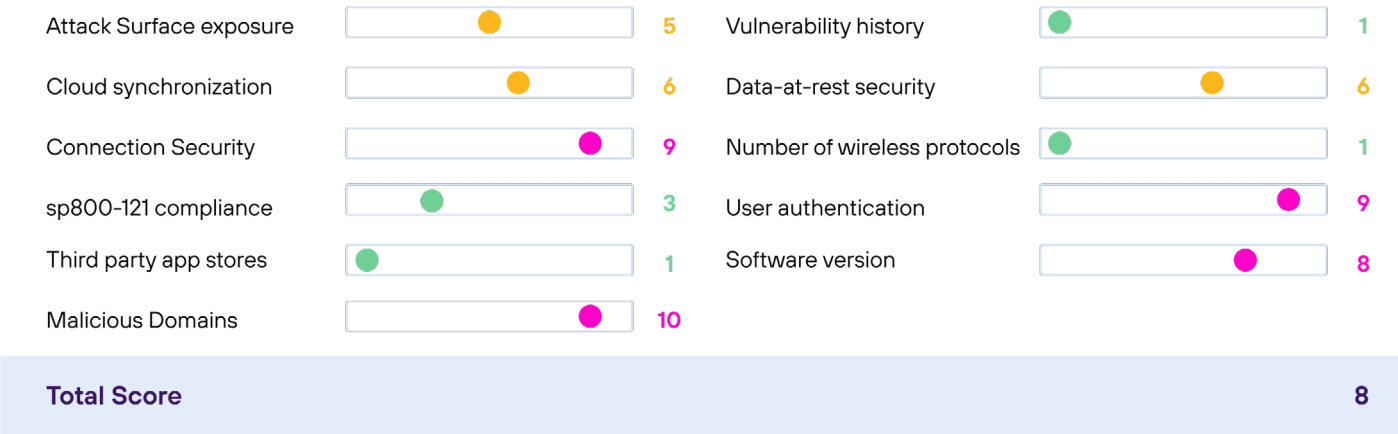


Figure 3: Sample list of discovered items, from a Fortune 1000 company.

With this comprehensive inventory of assets 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 assets immediately when they are exposed, unsecured, or acting suspiciously or maliciously.

Organizational Device Security Risk Score

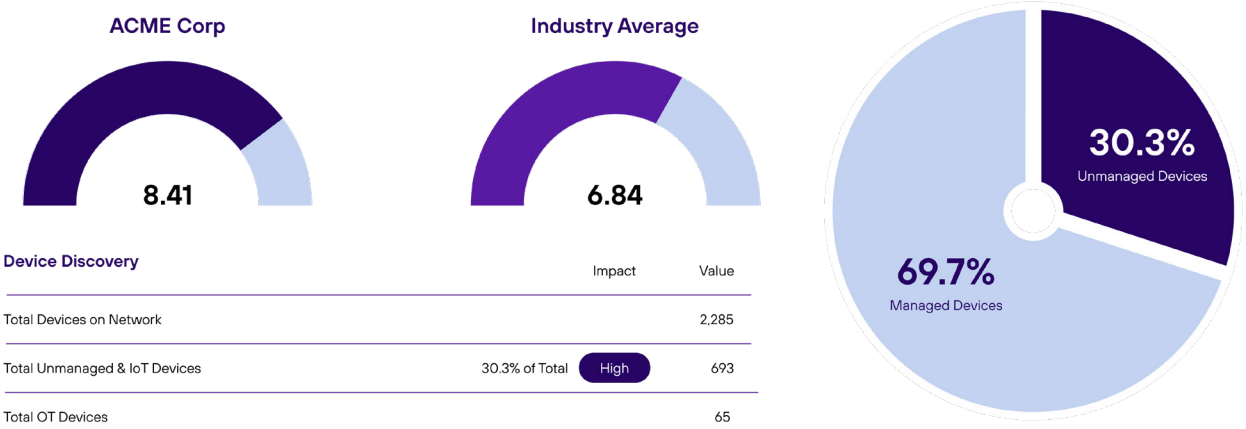


Figure 4: Sample top-line results from the Armis Device Security and Risk Assessment report.

Asset optimization

The need for complete asset visibility in today's environments is about more than risk management. You also need centralized, easy, and clear insights into assets to optimize their usage and your team's productivity.

Through integrations with most major cybersecurity tools and automations, the Armis unified asset intelligence platform helps your teams streamline asset management workflows. Armis consolidates data from key security tools and databases, including IT asset management and configuration management databases, to provide clean, accurate, and up-to-date information. Rationalized data and multidimensional views of every connected asset from across disparate environments empowers teams on numerous levels, including prioritizing updates based on potential impact to the business, quickly finding the location, user, and owner of specific assets, and more. It all adds up to improved asset utilization and faster mean time to resolution while increasing the number of assets each team member can realistically manage.

Confident innovation

In many enterprises, security concerns around assets can be a barrier to innovation. The attributes of unmanaged assets not only make it challenging and costly to properly design and architect asset-heavy environments, but manually maintaining unmanaged assets is expensive and contributes to constant vulnerability gaps. The Armis unified asset intelligence platform enables total visibility and smart management of all connected assets, whether they reside on-prem, in the data center, or in the cloud. The comprehensive visibility and capabilities give your team the insights that are essential to securely and efficiently realizing the promise of smart, IoT, IoMT, 5G, and edge assets to keep the business moving forward.

Frictionless and passive implementation

Armis delivers these benefits with an extremely low impact on your resources or technology. Our unified asset intelligence 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 assets in your environment. We use a virtual or hardware appliance that sits out-of-band to passively monitor traffic and collect data. It does not disrupt your systems, network, or the assets it is monitoring.

A deeper understanding of every asset and its relationships

Whether you search for a restaurant, store, hiking trail, or some other destination, today's best mapping apps and search engines provide more than a flat map to the spot. For example, if you search for coffee, you'll learn which shops are closest, their ratings, busy times, how to get there, see pictures, and more.

Similarly, Armis provides a clear, multi-dimensional map of your assets, starting with discovery. For each asset, Armis enriches the view with insights from the Armis Intelligence Engine and third-party data sources, such as the Food and Drug Administration for healthcare devices, to aid with understanding of what the assets are, how they are configured, who owns them, and their physical location. By

mapping out communications among assets, the Armis unified asset intelligence platform understands dependencies, business context, and the importance of different assets. The platform also aggregates data from key sources to detect vulnerable assets, providing real-time alerts on exploit attempts and essential data for prioritizing and planning mitigation efforts. You can even integrate the Armis platform with your existing security stack to automate responses to attacks. It all adds up to the most comprehensive asset visibility and security platform on the market.

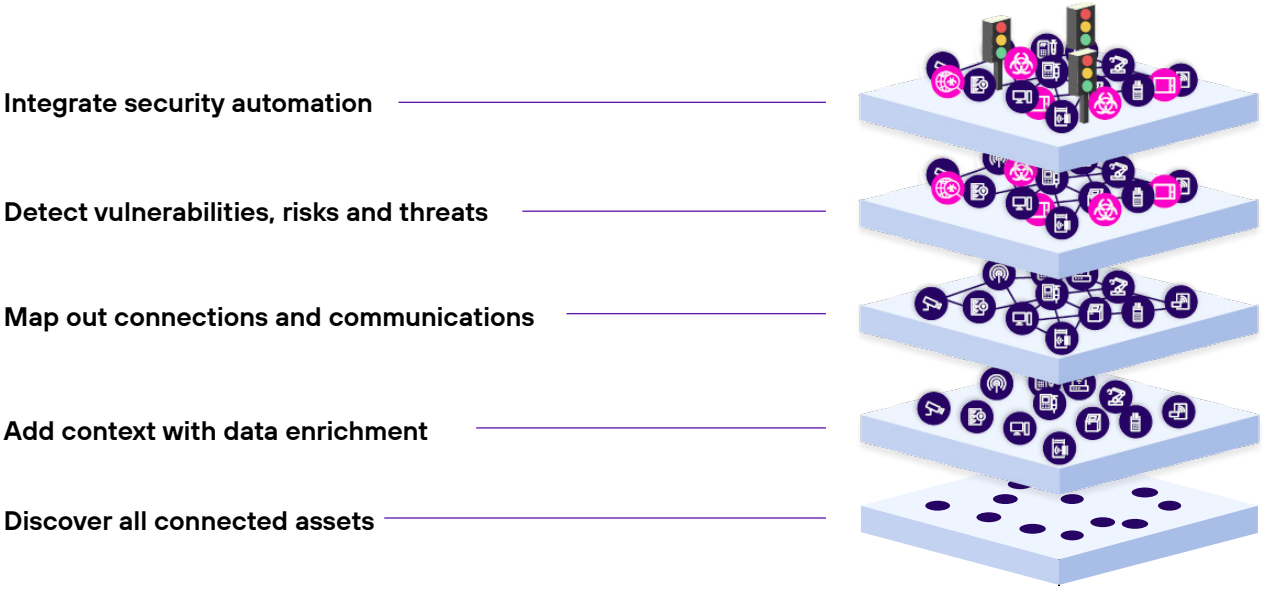


Figure 5: The Armis platform provides multiple views and added context for every connected asset.

About Armis

Armis is the leading unified asset visibility and security platform designed to address the new threat landscape that connected devices create. Fortune 1000 companies trust our real-time and continuous protection to see with full context all managed, unmanaged, and IoT devices, including medical devices (IoMT), operational technology (OT) and industrial control systems (ICS). Armis provides passive and unparalleled cybersecurity asset management, risk management, and automated enforcement. Armis is a privately held company and headquartered in Palo Alto, California.

armis.com
info@armis.com

202212004-1