ARMIS

OVERCOMING THE CYBERSECURITY ASSET MANAGEMENT CHALLENGE

Table of contents

COMPLEXITY. FRAGMENTATION. LOSS OF CONTROL.

Today, “more” is on the rise. More assets, more platform variations, more API integrations, more apps, more processes, and more users. The continuous innovation in device technology delivers convenience and the promise of better productivity, collaboration, and efficiency, but it also results in more risk.

The proliferation of assets across organizations has increased the need for better visibility of those assets to properly manage your risk posture and threat landscape. Unfortunately, management of all assets is strewn across multiple IT and security solutions. The “great silo-ization” of legacy tools means a fragmented landscape, with neither complete visibility nor a single source of trusted information. And that means IT and security teams struggle to understand what assets they truly have—and to ensure policies are properly enforced, risk is managed, and assets are protected.

Complexity. Fragmentation. Loss of control.

There may be a debate on just how many devices are connected to networks. Estimates from Gartner and Cisco suggest that by 2021, there will be 25 billion to 50 billion connected devices in use.

But there is no debate about the growing complexity and lack of visibility with which IT and security teams contend.

Today, almost every organization relies heavily on connected assets and devices to conduct all aspects of business. This is done through managed devices (laptops, desktops, and servers), smartphones and BYOD, virtual assets, cloud services, and even IoT devices (the “great unmanaged”). The result is billions of devices connecting to critical data and infrastructure, with more continuously being brought online every day.

The COVID-19 pandemic has also contributed to the rise of the complexity issue of more and varying types of assets. Beyond the assets in the workplace, the sudden shift to remote work and a massively distributed operational model for enterprises, IT teams have had to rapidly increase the pace of digital transformation to support business continuity efforts.

The primary facilitator has been these assets, and as 5G adoption has become more prevalent and accessible, companies that invested in device usage were better equipped to limit disruption. According to research from McKinsey, COVID-19 actually helped accelerate the adoption of connected devices because standard organizational barriers that typically limit innovation were removed to expedite productivity efforts. Visibility and control across disparate tools is necessary—and missing for most organizations.

Can you see all the assets in your environment?

- ✔ How many assets do I have—how accurate is my CMDB?
- ✔ How many managed vs. unmanaged assets do I have?
- ✔ What is the distribution of assets by site or department?
- ✔ Do I have any laptops missing an agent?
- ✔ Do I have any out-of-warranty devices? If so, where are they and who is using them?
- ✔ How many users (by asset type) do I have and where are they located?
- ✔ How many unsanctioned applications are in my environment?
- ✔ How many cloud assets (by provider) do I have?
- ✔ Do I have any users or admins not adhering to password rotation rules?
- ✔ Are there any devices reported missing that appear on my network?
- ✔ Do I have any AD users whose password needs to change?
- ✔ Do my laptops have encryption hard drive enabled?
- ✔ How many vulnerable assets do I have (by CVE severity, business unit or location?
- ✔ How many devices running unpatched OSs or applications?

More devices. More tools. More complexity.

In the parlance of corporate-speak, we might call all this asset and device proliferation a game-changer. And that would be accurate. But it doesn't capture the repercussions of what is happening as a result of this rapid, mass adoption, which is tremendous complexity.

Every device that comes online has multiple elements that IT teams need to consider and account for— operating system, application, user access, network connectivity, patches, and updates. And these are just the basics. Multiply all those variations with the number of devices currently in use by a company, THEN keep adding as new ones are added daily. Before you know it, you're dealing with layers of complexity that create blind spots among and between all these assets, and that is preventing IT teams from applying the necessary management and security to protect their critical data.

Common blind spots

Laptops, Desktops, and Servers

Organizations still struggle to see all their desktops, laptops, and servers, as well as the state of those devices. IT can't always keep up with every deployed device across an organization, and across all the primary networks and subnets. EDR and vulnerability management solutions just don't identify or secure every device.

BYOD

Smartphones and tablets still proliferate across every organization. Regardless of MDM and EMM solutions, from corporate-issued to employee-owned to vendor devices, or other transient mobile devices, it means complete visibility and control has remained elusive.

Cloud Instances

As companies continue to move workloads to the cloud, their security visibility gap widens. IT teams are increasingly challenged with identifying activity and risk within cloud, multi-cloud, and hybrid environments. This creates a complicated landscape to manage, which leads to cloud visibility gaps, and ultimately, opportunities for attacks to target these blind spots.

Virtual Machines

Virtual machines are ubiquitous in organizations because they are easy to spin-up and put into use. To take advantage of this computing power, security is usually sacrificed for development speed. With each instance of unmanaged VMs—whether in the cloud, hybrid, multi-cloud, or on-prem—new layers of complexity are added to the task of managing risk.

IoT Devices

Every second of every day, 127 new devices get connected to the Internet. Whether the Enterprise of Things, IoT, IoMT, or IIOT, they are unmanaged devices that can't take agents and can't be secured by legacy solutions. And by this year, up to 90% of all devices across an organization will be unmanaged.

The critical question is this—do IT and security teams fully know and understand all the asset in their environment?

The simple answer is, no. And it's through no fault of their own. The task has become simply too overwhelming and specialized.

When Armis started in 2017, we saw that organizations were not seeing 40% or more of devices in their environment, and it has only grown since then. Device growth and adoption doesn't wait for security to keep pace, which has resulted in blind spots with more assets and devices. They are designed to connect to data sources with ease, virtual machines are spun up in an instant, and all of these unprotected connections become targets for attackers. Companies typically can't see those gaps, but that's precisely what cyberattackers seek.

These blind spots result from three key issues:

1 | Visibility

IT and security teams lack a real-time, complete picture of the assets in their environment

Too many organizations do not know how many assets they have. They use a variety of approaches, which still includes spreadsheets and manual counting. And the variety of single-purpose, siloed tools for device security suffer from limited scope and/or inability to provide enough information to satisfy the need for a complete, unified, and real-time list of all assets. Today, if an IT or security leader asks a simple question such as, "How many Windows hosts do we have?", they are likely to get very different answers depending on which team or tool they are asking. A different type of solution is needed.

An effective cybersecurity asset management has to start with the issue of **visibility** into all assets—volume, type, and applications. As with any security approach, security teams have to know what's in their environment in order to manage it. Speed and innovation are prized by business teams, but they create risks for security organizations. There will always be more assets, those devices will be updated with new versions, and more connections to applications and other technology resources creates a nightmare of variation and fragmentation. IT and security teams need a **single source of truth** that provides visibility of their entire landscape of compliance and security for all devices and assets.

Armis was launched specifically to provide enterprise IT and security teams with visibility to all assets—managed and unmanaged—all in an effort to eliminate the asset security blind spots that are ever-present and increasingly aggressive. By identifying all devices, both on and off the corporate network, and providing continuous information about their posture, Armis users are able to isolate threats and quickly remediate these security issues.

2 | Fragmentation

Traditional security tools provide only fragmented risk insights

IT and security teams use many existing tools in their security stack to protect individual services and devices, but that gives them a fragmented, incomplete picture of where threats exist. Security and compliance policies and configurations have to be managed for each asset and their corresponding services, identifying their operating systems, as well as applications running on those assets. And all of that has to be done while maintaining awareness and protection over always-changing internal and external threat landscapes.

All of this variation and change creates isolated views of the number of assets and security posture across the various tools being used, but it doesn't capture the entirety of the activity. This fragmented view creates gaps in visibility and enforcement, and cyberattackers seek these gaps. The only way to avoid this is by having a single source of truth for device security coverage that is inclusive of all assets and related information from all systems.

Here again, the concept of "more" actually complicates security efforts. More security tools being deployed for unique purposes leave blind spots to what's really happening. IT and security teams don't have a single view that allows them to identify and make sense of the state, configuration, and enforcement of policies for all assets—and that could lead to huge risk.

3 | Remediation

The inability to automatically enforce security policies effectively

Once a management or security issue is identified, a solution needs to be swiftly applied. However, most tools are optimized for either detection and alerting, or for deploying patches to fix known issues. These are incomplete in their efforts and lack the speed and process required to isolate and address attacks while they are in progress.

Companies often require an automated approach to enforcing policies and orchestrating the entire remediation process—from detection to enforcement. This includes alerting, investigating, and quarantining, or installing patches and updating code. It also must be real-time and continuous, collecting that data and analyzing it for threats that will improve their defensive positions and remediation in the future.

The result of these three key issues is that companies are too often blind to the entirety of their assets, their vulnerabilities, and unable to automatically take the corrective actions to protect themselves.

The traditional, centrally-managed tech "stack" is being replaced by a distributed and continuously-growing network of connected assets that are deployed rapidly and often without adhering to IT governance requirements. This includes a growing array of virtual systems and connected physical devices that are used to create, send, receive, and transact with critical data, such as:

- Laptops
- Servers
- Virtual machines
- Cloud instances
- Mobile devices
- Users
- Building automation systems
- IoT Devices

Those assets connect to sensitive data in a variety of way—on the network, in the cloud, via VPN, from home networks, through third-party supplier networks, via partner and other stakeholder systems—each of which demands unique security protocols. On top of that, each asset type is unique and requires its own set of security and compliance policies.

Visibility is everything

To illustrate the importance of visibility and the need for control as device proliferation accelerates, consider the emphasis put on it by two of the most important cybersecurity guides. First, the NIST Cybersecurity Framework (NIST CSF) states:

> *Organizations must develop an understanding of their environment to manage cybersecurity risk to systems, assets, data and capabilities. To comply with this Function, it is essential to have full visibility into your digital and physical assets, their interconnections, and defined roles and responsibilities, as well as to understand your current risks and exposure and put policies and procedures into place to manage those risks.*

Second, the Center for Internet Security (CIS) Critical Security Controls document starts with the problem of visibility and management of assets. It says:

> *Attackers, who can be located anywhere in the world, are continuously scanning the address space of target organizations, waiting for new and possibly unprotected systems to be attached to the network. They are particularly interested in devices which come and go off of the enterprise's network such as laptops or Bring-Your-Own-Device (BYOD) which might be out of synchronization with security updates or might already be compromised... Even devices that are not visible from the Internet can be used by attackers who have already gained internal access and are hunting for internal pivot points or victims.*

Why the growth of assets and devices correlates with increased risk

No Perimeter: Every asset or device has multiple ways it can be accessed—through VPNs, corporate networks, in the cloud, among others—and it creates easy connections to other devices, apps, and processes. This makes it convenient for users and administrators. It also, however, increases the digital footprint of the data being used by those devices, which creates a broader—and growing—potential attack surface.

No Control: Each asset type is unique, and even different asset types have multiple manufacturers, versions, and platform specifications. There's simply too much variance, and policy management across too many tools means no policy at all.

No Single Source of Truth: Asset information is fragmented across a variety of tools and they at most offer only partial insights into asset management and device security. This creates a false picture of the state of assets and their activities, which also means an inability to get a clear picture of risk.

Break down the silos. Get actionable insights.

The response from many organizations is to compartmentalize risk around general mitigation scenarios. But the application of more legacy security tools is now generating an inverse response to visibility and control due to the silos it creates, and how it does not deliver action insights. As we've seen, devices and assets operate in a dynamic, ever-changing environment that cannot be controlled without an asset-specific approach to security. Without that, devices will continue to be brought online and into corporate environments while lacking policy controls and policy enforcement, which will exponentially widen the problem of security and governance.

A FRAMEWORK FOR **EFFECTIVE** CYBERSECURITY ASSET MANAGEMENT

The ability to have a complete and unified view of assets becomes the first step in understanding and managing the true risk landscape of a particular environment. Many will look at network access control (NAC) products as a starting point, but that is not enough. That leaves most devices undetectable to those who are responsible for their security.

Today's IT and security management tools are also built to identify issues in specific spots: at the network perimeter, in a cloud environment, for a specific device or its applications, and other "locations" where risks tend to appear. They also tend to look at policies and controls in the context of review time. In other words, they report on the security state of an environment at the time of their review, and not in a continuous fashion.

This approach provides a unique lens into a distinct set of problems that creates isolated consoles with narrow views, leading to visibility gaps, perpetual ambiguities, and false precision. Security and IT teams are essentially seeing only what an individual vendor's tool is built to solve for.

Organizations need a complete solution and approach that is built to address the issue of all devices—managed and unmanaged. It must adhere to the following principles:

Comprehensive and complete asset discovery

Assets and devices operate without regard to a traditional perimeter, so the right solution must identify all types of assets, those that are physically-connected and those that are wireless, and it has to discover them whether they are on or off the network, on-premises, or virtual. To truly understand the security landscape of any organization, an asset management tool must be inclusive of everything that touches the environment including devices, applications, operating systems, and other systems and services—on premises and in the cloud. This means having the ability to use existing infrastructure, APIs, network connections, and other protocols to connect to all data sources.

Identification of gaps and delivery of actionable insights

With knowledge of all the assets in the environment, security and IT teams can begin the process of identifying and assessing asset details to actively manage risk—including which applications are on the assets or devices. In addition to knowing how policies are or are not being enacted, it is critical to understand the complete context associated with every asset including their users, configurations, and posture to ascertain any risks or compliance gaps. To do this effectively means ingesting and analyzing contextual data about those assets. Many security tools have these basic abilities, but they are compartmentalized to look at things like perimeter access, cloud storage, access control, or any of the other types of security disciplines alone. They are unable to identify issues in aggregate when they are unique to devices and assets.

Automated enforcement of security policies

Once a vulnerability, risk, or security gap is identified, it needs to be addressed immediately. This is a challenge to do manually consistently, even for small organizations with simple IT environments. What's needed is real-time policy enforcement and automated security that can orchestrate the necessary actions needed to isolate devices and initiate software updates, trigger alerts, and scan for vulnerabilities for the device under threat, and all the assets it touches.

Agentless approach

Many tools operate by deploying agents into environments and then correlating trends via activity that is collected by the agent. But IT and security professionals don't want yet another agent to install across all their assets. An agentless, but passive approach allows IT to build a comprehensive device inventory in real-time, ensuring that every asset, even transient ones, are accounted for.

Giving context to device and asset usage must include insights and evaluations of configurations, activities, and other anomalies, and it must focus on these types of activities:

- **Classification:** IT and security teams need a lens to the activity of assets, including access, incoming data, and outgoing data so they have a complete, comprehensive, and continuous accounting of devices in their environment. This includes every managed, virtual, unmanaged, and IoT device. It should aggregate device information across all IT and security management solutions. Additionally, it has to be able to identify devices on the network (both wired and wireless), along with devices that are off-prem.
- **Compliance:** By identifying compliance gaps, IT and security teams can immediately implement fixes that will both strengthen their security posture and will keep them compliant ahead of audits. While these are clearly safety measures, it's also important to recognize the business importance of maintaining compliance for these assets. Compliance and audit teams need to verify that security controls and practices meet a growing number of regulatory requirements and security frameworks. Given the ever-increasing number of unmanaged devices that can't accommodate a security agent or be scanned over the network, it is increasingly hard to answer questions like, "What devices are on my network?" or "What risks are in my environment?".

ARMIS DELIVERS **COMPREHENSIVE** CYBERSECURITY ASSET MANAGEMENT

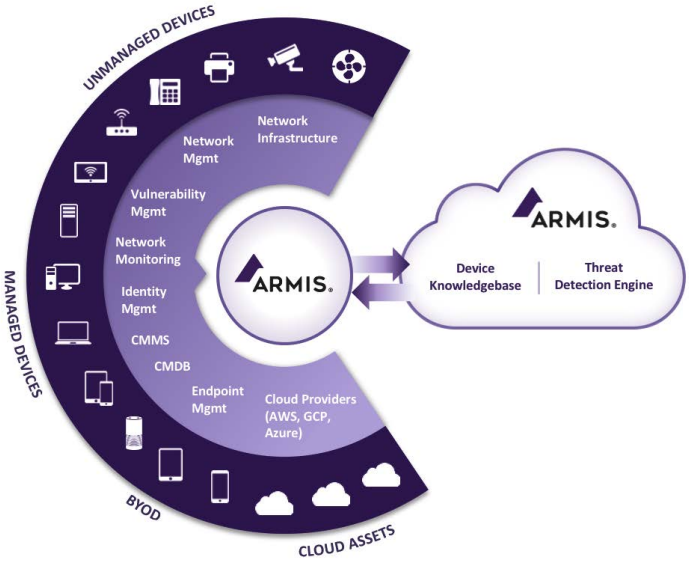
Armis' starting point for effective cybersecurity asset management starts by establishing a single, comprehensive, and accurate view of all assets and devices in an environment. It includes the range of devices that are currently connected to the environment, including all virtual instances and cloud services, as well as the growing number of unmanaged assets and IoT devices. It discovers assets and devices as they come online and in contact with any data source.

Armis Asset Management provides the following:

Delivers complete inventory of all assets

We identify and classify all assets (managed, virtual, cloud, or unmanaged) in the environment by combining data from other systems to create one source of truth. It brings together information from disparate sources through pre-built adapters, such as:

- Endpoint Management (EPP, EDR, UEM/EMM)
- Identity and Access Management (IAM) systems
- Common Vulnerability and Exposure (CVE) databases
- Cloud Services (Management, Infrastructure, Security)
- Network infrastructure (Switches, WLC's)
- CMDB/ITAM
- Cloud Providers
- DHCP/DNS
- Firewalls
- Mobile Device Management (MDM)
- Network Access Control (NAC)
- Network Monitoring
- Vulnerability Assessment

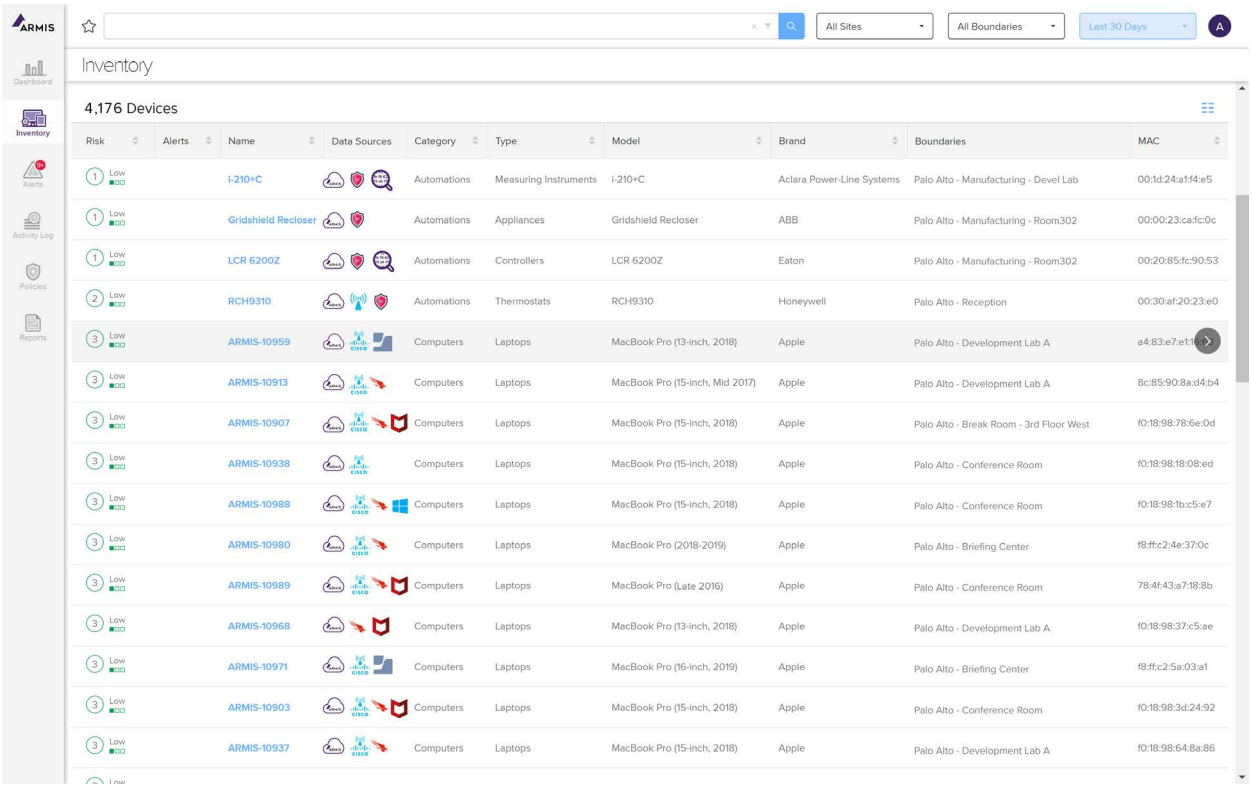


Armis ingests data from all the sources in your environment for superior visibility

Just a few of the solutions that work with the Armis Adapters

Identifies vulnerabilities and risks, and delivers actionable insights

Armis Asset Management helps reduce risks and security issues by identifying all devices, apps, and operating systems, and evaluates CVE's and severity levels and then assigns risk scores to all assets. As we have seen, many security tools are capable of ingesting and analyzing usage data. But the context needed for device behavior simply isn't available for tools that are compartmentalized to look at things like perimeter access, cloud storage, access control, or any of the other types of security disciplines alone.



Armis provides a complete inventory of all your assets

Through Armis' one-of-a-kind Device Knowledgebase, which is the largest in the world tracking more than 500 million assets daily, combined with our hundreds of available adapters to seamlessly integrate with existing IT and security solutions, IT and security professionals are provided with not only their assets, but the critical information and context of each asset.

Automates enforcement of security policies

With knowledge of all the assets in the environment and risks, IT and security teams can manage their assets and risks more effectively. Through Armis adapters and connections to existing IT and security management solutions, users can automatically orchestrate security policy enforcement such as notifying SOC systems, deploying endpoint agents, running a vulnerability scan, even blocking or quarantining devices.

Completely agentless and passive

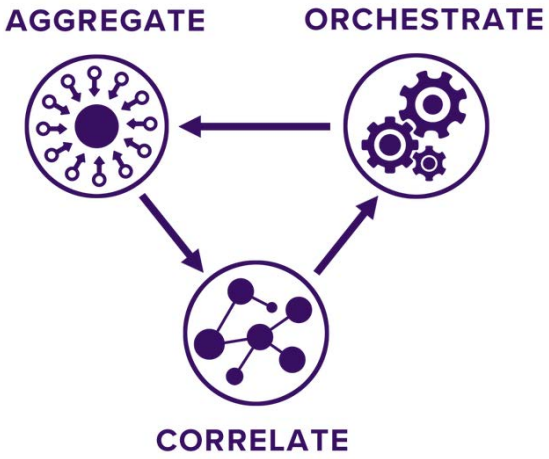
Unlike other security tools which require deploying agents into environments and onto devices, Armis is completely agentless. That simplifies and speeds deployment across one office, a campus, remote locations or even globally. And it is also completely passive, so it won't disrupt the operations of devices. Everything works in real-time, so discovery of assets and identification of issues and automated enforcement is continuous. This ensures that every device is inventoried.

With the Armis approach, data from devices is analyzed and risk is calculated according to scoring that is based on multiple risk factors. In addition to data based on the device, manufacturer, reputation, and known vulnerabilities. Activity and behaviors are evaluated, and behavior is compared against "known good" profiles of devices to identify issues and threats.

Aggregate. Correlate. Orchestrate.

By connecting to existing IT and security solutions and your network infrastructure, Armis delivers a trusted, comprehensive, and unified asset inventory of all devices. It integrates with hundreds of IT and security solutions, as well an organization's infrastructure.

If Armis identifies a vulnerability, risk, or security gap, it can automate security and policy enforcement. It orchestrates the necessary actions in conjunction with existing IT or security management solutions, or at the network level. This includes actions like blocking or quarantining a device, triggering a vulnerability scan, if appropriate, kicking off a process to install software, or feeding device risk data to a SIEM or CMDB.



Just ASQ for simple queries. Important insights.

Armis provides the Armis Standard Query (ASQ), letting you identify specific devices, their state, and any security gaps or exposures you may have. It's an easy "If this, then that" visual query builder that lets you create reports and get insights quickly. For example, you can create a query to identify which devices are running a version of an application or operating system that contains known vulnerabilities. Armis lets you track:

- Managed devices
- Unmanaged and IoT devices
- Mobile devices
- Virtual Machines
- Cloud Instances
- Specialized devices (medical, healthcare, manufacturing, OT, etc.)
- Users

Delivering 5X the visibility

Armis provides 5x the visibility of other tools because it has been purpose-built from its founding as a source for complete visibility and risk management. This provides administrators with unique device information. Armis records and keeps a history on everything each device does.

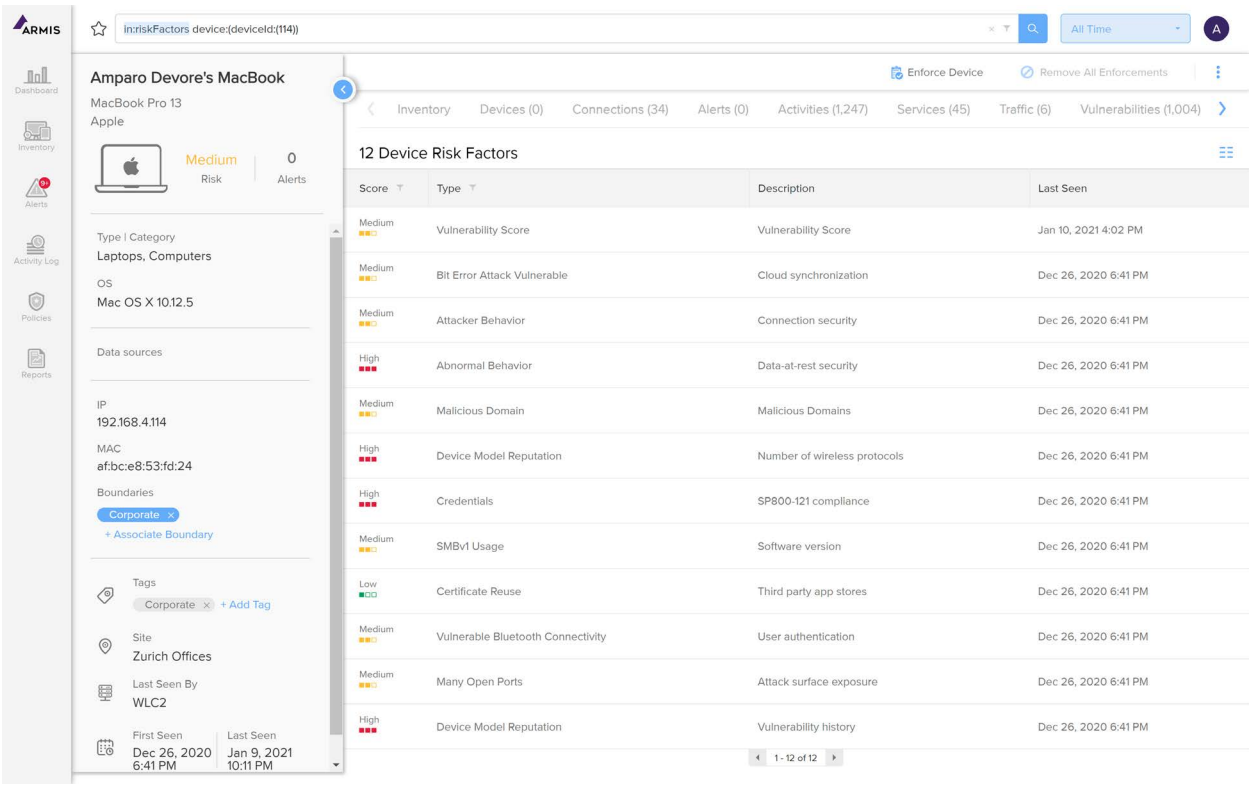
This data enables security teams to take proactive steps to reduce their attack surface. It also helps companies comply with regulatory frameworks that require them to identify and prioritize all vulnerabilities.

Unlike other vendors, Armis provides risk assessment for all devices automatically. There is nothing that an administrator will need to enter into the system—no policies or whitelists that need to be known in advance. Armis automatically generates a risk score based on the extensive knowledge in the Armis Device Knowledgebase combined with multiple threat intelligence feeds and machine learning.

The figure below shows the risk scoring of an Armis customer, with approximately 5,000 employees. Risk is reported according to certain security types and allows security and IT teams to pinpoint where they need to address gaps.

Solution	Armis Sees
Vulnerability Management Solutions	**3x**
EDR Solutions	**4x**
CMDB Solutions	**8x**

Data based on review of 28 sample Global 2000 customers with deployments of more than 10 locations each, and a combined visibility of over 110M devices.



Armis provides deep insights about risks associated with assets

Remediation to limit damage and harden the environment

Even with the best defenses, devices will be targeted for attacks. Effective IT and security tools can detect gaps and risk areas before they become a problem, but when an actual issue is identified, it needs to be addressed rapidly. But not all issues are alike, and Armis operates with the premise that isolating an issue means orchestrating a number of different processes that are critical to the remediation process.

The keys to incident response are speed and process. Speed should be addressed through automation based on the activity history of breached systems, and on a response to the attacks themselves. It also needs to be paired with a well-tested plan that identifies, isolates, and applies fixes to the issue. Armis approaches remediation by orchestrating these steps and processes:

- **Alerting:** The first step in addressing a problem is knowing about it. Armis notifies administrators via SIEM or emails in Splunk, QRadar, and others.
- **Initiate action:** Automated tickets should be created via standard systems like ServiceNow, Remedy or Jira, so the right teams can initiate action.
- **Evaluation** Tigger a scan to understand the vulnerability of new assets when they come online, in real time, not just during scheduled intervals.
- **Push updates:** Create or enrich asset information in various CMDBs and your other asset management platforms.
- **Quarantine:** Restrict device activity for those assets that are involved, but allow access for others.
- **Patch:** Deliver updates and patches to non-compliant devices.

Armis uses automated enforcement of security policy to continuously deliver remediation. When a vulnerability, risk, or security gap is identified, Armis initiates automated security and policy enforcement and orchestrates the necessary actions in conjunction with existing IT or security management solutions, or at the network level. It includes actions such as:

- Block or quarantine a device
- Trigger a vulnerability scan
- Deploy software
- Update device information
- Create an incident in a Ticket System
- Feed device data to SIEM
- Create a CMDB entry

Eliminate the enterprise security blind spot

Technology innovation and IT change deliver important efficiencies, but they add layers of complexity to the task of protecting organizational assets. As the number of assets increases, visibility into what's touching important organizational data decreases.

Faced with visibility challenges from the growing number of assets and complexity in tools to manage them, IT and security teams have a new tool. A solution that will identify assets and devices and overcome the issue of siloed solution. One that starts with asset discovery, which enables IT and security teams to identify critical security gaps. They can then apply automated enforcement of security policies to address risks with immediacy.

Modern organizations are certainly capable of keeping pace with IT change and innovation. With the right tools to deliver visibility in all their cloud and on-prem environments, across all platforms, and for any assets and devices, they can increase awareness of what needs to be protected. This gives them a continuous framework for asset and device cybersecurity that is always prepared to handle any threat to critical organizational data.

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.com

1.888.452.4011

20210112-1