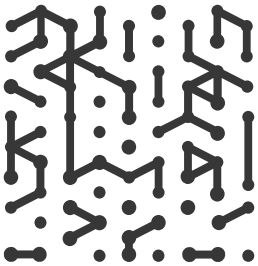
ARMIS®

WHITEPAPER

Overcoming The Cybersecurity Asset Management Challenge

Table of Contents



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 McKinsey suggest that in 2025, there will be 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.

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 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?

Visibility and control across disparate tools is necessary—and missing for most organizations.

More devices. More tools. More complexity.

In corporate terms, we might describe the proliferation of assets and devices as a game-changer—and that would be true. However, this term falls short of capturing the full impact of this rapid, large-scale adoption: an overwhelming increase in complexity.

Every device brought online introduces multiple factors for IT teams to address, including the operating system, applications, user access, network connectivity, patches, and updates—just to name the basics. Now, multiply these variables by the sheer number of devices already in use within an organization, and then compound the issue as new devices are added daily.

The result? A web of complexity that obscures visibility across these assets, creating significant blind spots. These blind spots hinder IT teams' ability to effectively manage and secure their environment, leaving critical data vulnerable to threats.

Can you see all the assets in your environment?

How many cloud assets (by provider) do I have?

Do I have any users or admins not adhering to password or encryption key rotation rules?

Are there any devices reported missing that appear on my network?

Do I have any AD users whose access rights needs to change?

Do my laptops have encryption enabled?

How many vulnerable assets do I have? Are they prioritized by asset criticality to the business unit or location?

How many devices running unpatched OSs or applications?

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

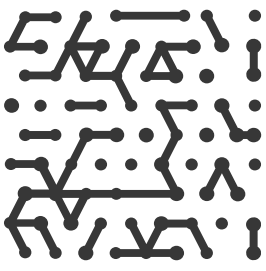
As companies continue to move workloads to the cloud, their security visibility gap widens. IT teams are increasingly challenged with identifying activity and risk within cloud, multi-cloud, and hybrid environments. This creates a complicated landscape to manage, which leads to cloud visibility gaps, 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. According to Armis Labs research, approximately 40% of devices within an organization are unmanaged. These include a wide range of assets such as Internet of Things (IoT) devices, Operational Technology (OT), medical devices, and other non-traditional IT assets that often lack proper visibility and security management.



The Enterprise Security Blind Spot

The critical question is this: do IT and security teams truly have full visibility, security and control of all the assets in their environment?

The straightforward answer is no—and it's not due to any shortcoming on their part. The challenge has simply become too vast and too specialized to manage effectively.

The rapid pace of device adoption and growth doesn't wait for security to catch up. This has led to significant blind spots as more assets and devices connect. These devices are built to seamlessly access data sources, virtual machines can be created in seconds, and all of these unsecured connections become prime targets for attackers. While organizations often remain unaware of these vulnerabilities, cyberattackers are actively exploiting them.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 inventory management. 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.

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 provides 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. 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

The average organization now manages approximately 76 tools in their security stack, each designed to protect specific services and devices. However, this fragmented approach results in an incomplete view of where threats exist. Security and compliance policies must be managed for each asset and their associated services, including identifying operating systems and the applications running on those assets—all while adapting to constantly evolving internal and external threat landscapes.

This complexity creates siloed and isolated views across the various tools in use, failing to provide a comprehensive picture of asset activity, behavior and security posture. These fragmented views leave gaps in visibility and enforcement which cyberattackers are quick to exploit.

The only way to address this challenge is by establishing a single source of truth for device security coverage. This must include comprehensive visibility into all assets, along with unified information from every system in use.

3 Remediation

The inability to identify and connect findings to the fix

Remediation is one of the most critical yet challenging aspects of effective asset management. The process goes beyond identifying vulnerabilities—it requires a swift, prioritized and coordinated action to address them before they can be exploited. However, organizations face significant hurdles in achieving this. Blind spots in their environment, particularly from unmanaged, IoT, and legacy devices, make it difficult to know where remediation is needed, what should be handled first and who is responsible to do it. Additionally, the fragmented nature of modern security stacks, with dozens of siloed tools, complicates the prioritization

and execution of remediation efforts. Resource constraints and the complexity of interconnected systems further exacerbate the issue, as IT and security teams struggle to balance vulnerability management with maintaining business continuity. The rapidly evolving threat landscape adds yet another layer of difficulty, leaving many vulnerabilities exposed for extended periods.

To overcome these challenges, organizations must adopt a proactive and streamlined approach to remediation. This starts with unified, real-time visibility into all assets, including managed, unmanaged, IoT, and operational technology (OT) devices. Automated tools are essential to identify, deduplicate, contextualize, prioritize, assign and mitigate vulnerabilities based on risk factors such as exploitability and business impact, ensuring teams focus on the most critical issues. Integrated workflows that connect existing tools, like ticketing systems, enable seamless communication and action across teams, while scalable automation accelerates patching and policy enforcement to reduce human error. Solutions like Armis provide the comprehensive asset visibility and threat intelligence necessary to guide these efforts, while also ensuring that remediation actions account for dependencies and operational needs. By adopting this centralized, intelligence-driven approach, organizations can transform remediation into an efficient, proactive process that minimizes risk and strengthens their security posture.

Visibility is Everything

NIST Cybersecurity Framework (NIST CSF) states:

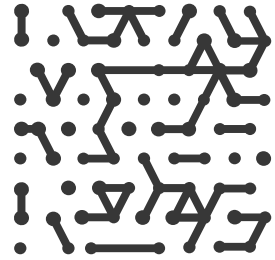
> *Organizations must develop an understanding of their environment to manage cybersecurity risk to systems, assets, data and capabilities. To comply with this Function, it is essential to have full visibility into your digital and physical assets, their interconnections, and defined roles and responsibilities,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

In an asset-rich environment, visibility is the cornerstone of effective cyber exposure management and security. Without full awareness of every asset within the environment—managed, unmanaged, IoT, operational technology (OT), and cyber-physical systems (CPS)—it is impossible to adequately assess risk, prioritize vulnerabilities, or implement effective defenses. Visibility provides the critical context needed to understand the attack surface, track asset behavior, and identify exposures in real-time, forming the foundation upon which all other security efforts are built.

From a cyber exposure management and security perspective, visibility must extend beyond simple asset discovery to include detailed insights into each asset's configuration, vulnerabilities, software versions, network connections, and operational role. With a real-time, unified view of all assets, organizations can

map their entire attack surface, correlate risk across systems, and establish a proactive security posture that evolves alongside their environment.

Solutions like Armis enable this critical visibility by delivering a complete inventory of all connected assets and their associated security states. This capability empowers IT and security teams to not only identify gaps in their defenses but also to prioritize remediation efforts based on real-world risk. Furthermore, visibility supports ongoing compliance, ensuring organizations can demonstrate control over their assets and security posture. In today's hyper-connected world, visibility isn't just a security best practice—it is an operational necessity for protecting critical infrastructure, sensitive data, and business continuity.



A Framework For Effective Cybersecurity Asset Management

Effective cyber asset management requires a comprehensive and unified approach to identifying, monitoring, and securing every asset within an organization's environment. The foundation of this framework lies in achieving complete visibility across all asset types—managed, unmanaged, IoT, OT, and cyber-physical systems whether physical or vistual. Without this visibility, organizations cannot accurately assess their attack surface or effectively manage the risks associated with it.

Key pillars in aligning with this approach include:

Real Time Asset Discovery & Classification

Organizations need a solution that continuously identifies all assets within their environment and provides granular details about each device, including its type, location, operating system, applications, network behavior, and associated vulnerabilities. This level of detail ensures that IT and security teams have the contextual intelligence required to evaluate asset criticality and prioritize risks effectively.

Assess Risk

A robust asset management framework must include the ability to assess risk in real time by analyzing asset behavior against known baselines and leveraging up-to-date threat intelligence. This enables organizations to detect anomalies, identify active vulnerabilities, and evaluate the potential impact of each threat based on the asset's role within the business.

Automate

Automation is another essential element of the framework. As asset environments grow increasingly complex, manual processes are not sufficient to maintain security and operational efficiency. Automated workflows can streamline critical tasks, such as vulnerability management, policy enforcement, and incident response, reducing the burden on IT and security teams while ensuring consistent execution.

Orchestration

Finally, an effective framework must integrate seamlessly with existing tools and processes. Cyber asset management is not an isolated function; it needs to complement and enhance other security and IT systems, including SIEMs, CMDBs, vulnerability scanners, and endpoint protection platforms. This integration ensures that asset insights inform broader security strategies, from compliance reporting to threat detection and remediation.

Armis protects the entire attack surface and manages the organization's cyber risk exposure in real time

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 Centrix™ provides the following:

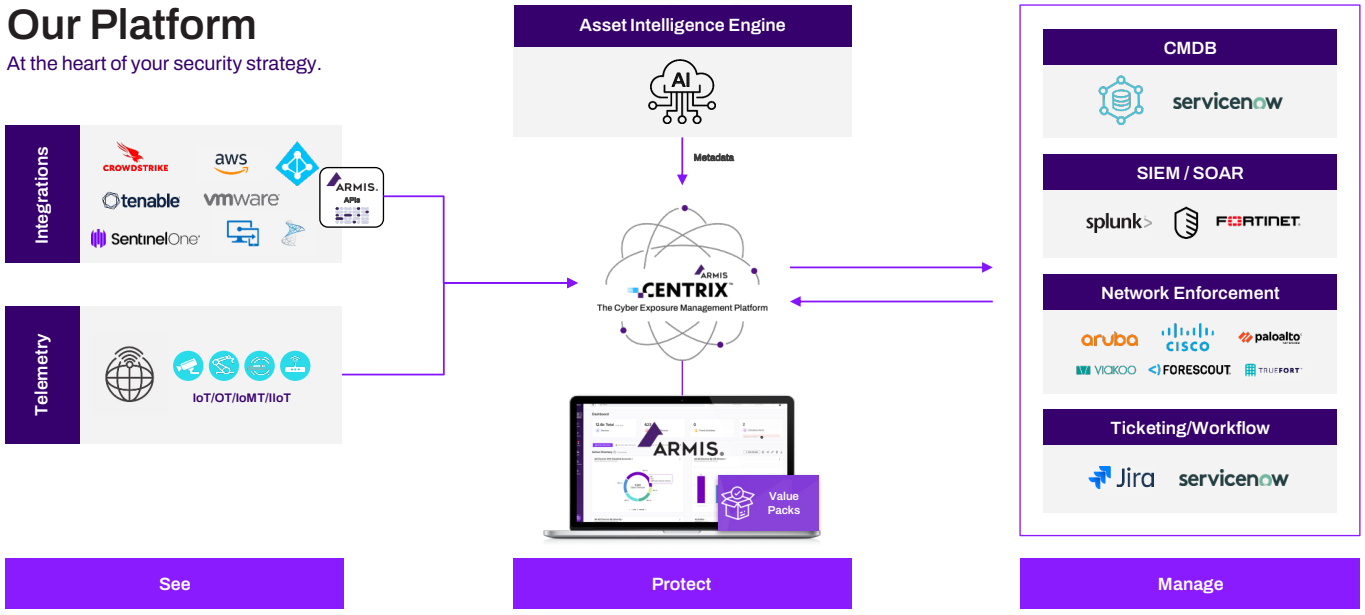
Delivers complete inventory of all assets

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

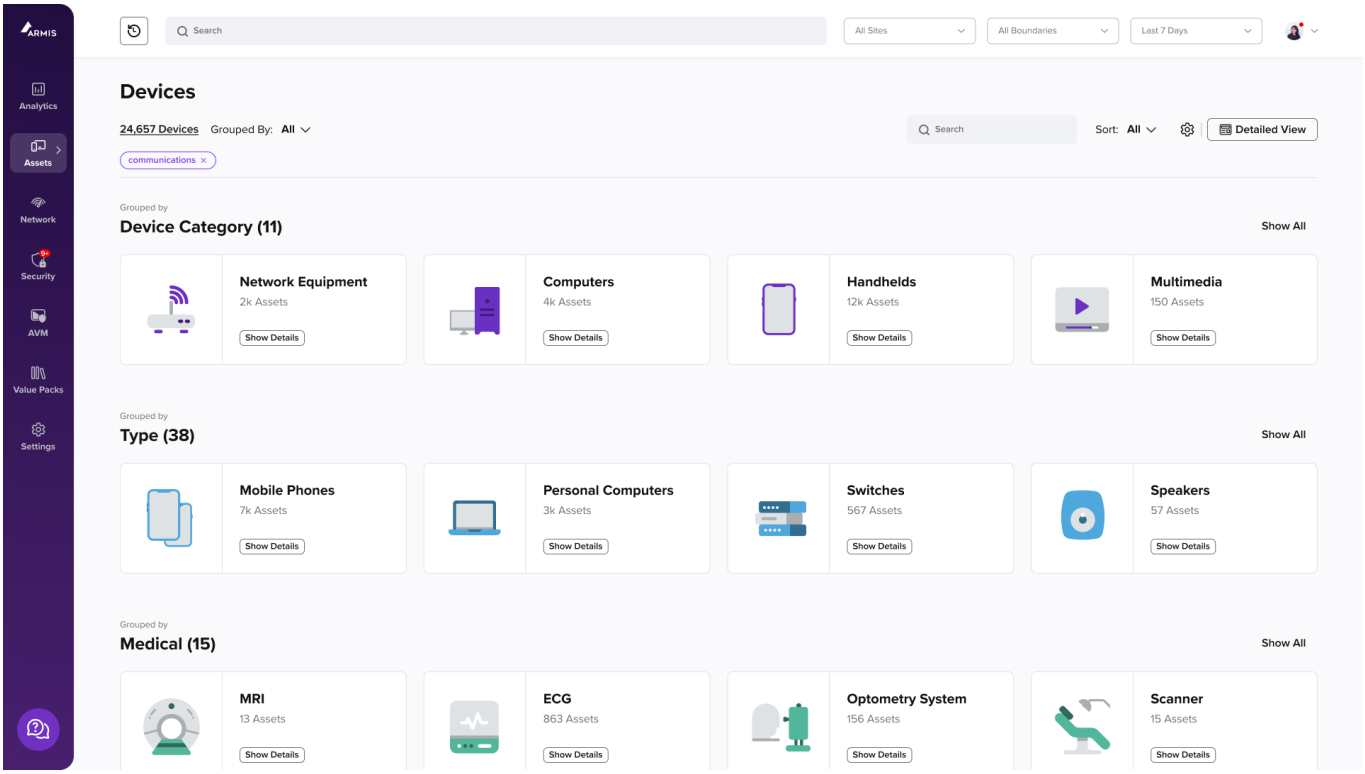
Our Platform

At the heart of your security strategy.



Identifies vulnerabilities and risks, and delivers actionable insights

Armis helps reduce risks and security issues by identifying all devices, apps, and operating systems, and evaluates early warning alarms, CVE's and severity levels by asset criticality to the business 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.



Through Armis' one-of-a-kind AI-driven Asset Intelligence Engine, which is the largest in the world tracking more than tracking more than 5 billion devices, combined with our hundreds of available integrations 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, firewalls, SIEM and SOAR, running a vulnerability assessment, even blocking or quarantining devices.

Flexible and non intrusive

Organizations across every industry rely on sensitive systems that can't be disrupted. Armis Centrix™ can be deployed without loading agents that could steal clock cycles or destabilize the machines that they run on. Armis uses sophisticated passive and active techniques to see, protect and manage all your assets. By monitoring all managed and unmanaged devices and maintaining a comprehensive device inventory of all assets, Armis fills the gaps left by conventional security solutions, enabling complete visibility.

With Armis Centrix™, 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, known vulnerabilities and asset criticality to the business. Activity and behaviors are evaluated, and behavior is compared against "known good" profiles of devices to identify issues and threats.

See. Protect. Manage.

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 assessment, 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
- Users
- Specialized devices (medical, healthcare, manufacturing, OT, etc.)

Delivering the visibility to keep your organization resilient

Armis provides unprecedented visibility of other tools because it has been purpose-built as a source for complete visibility security and control. This provides administrators with unique device information. Armis records and keeps a history on everything each device does.

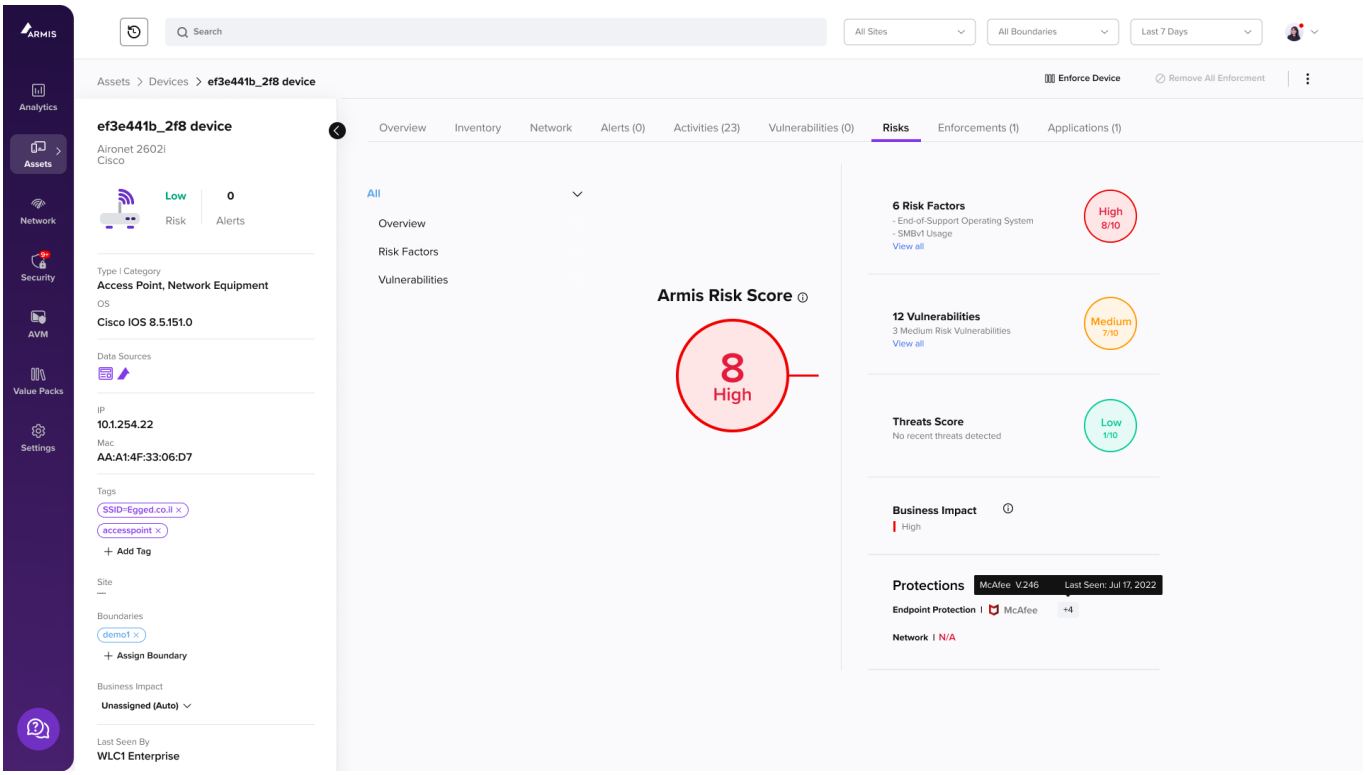
This data enables security teams to take proactive steps to reduce their attack surface. It also helps companies comply with regulatory frameworks that require them to identify and prioritize all vulnerabilities.

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 AI-driven Asset Intelligence Engine 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.



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:** Trigger a discovery process 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 security 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 in a prioritized fashion.

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:

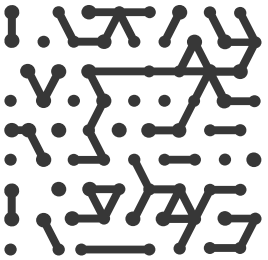
- Block or quarantine a device
- Trigger a vulnerability discovery process
- Deploy software
- Update device information
- Create an incident in a Ticket System
- Feed device data to SIEM/SOAR or other device in the security stack
- Create a CMDB entry

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 comprehensive 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.



Armis, the Cyber Exposure Management and Security Company, protects the entire attack surface and manages the organization's cyber risk exposure in real time.

In a rapidly evolving, perimeter-less world Armis ensures that organizations continuously see, protect and manage all critical assets - from the ground to the cloud.

Armis secures Fortune 100, 200 and 500 companies as well as national governments, state and local entities to help keep critical infrastructure, economies and society stay safe and secure 24/7.

Armis is a privately held company headquartered in California.

1.888.452.4011

Website

Platform
Industries
Solutions
Resources
Blog

Try Armis

Demo
Free Trial