

SOLUTION BRIEF

Armis Centrix™ Metrics, Dashboards and Reports

Understand how teams and tools are performing. Demonstrate progress for executive stakeholder reporting.

The Problem

There are hundreds of security controls, as defined by common security frameworks by organizations such as the National Institute of Standards and Technology (NIST) and the Center for Internet Security (CIS).

Implementing these security controls, processes and procedures is a common practice by almost any organization in order to provide reasonable assurance that business objectives will be achieved and undesired events will be detected, corrected, and prevented.

However, identifying gaps in security controls and reporting progress can be difficult, if not almost impossible.

For example, next time a critical and long-tail vulnerability hits your attack surface:

How would you know if a company issued laptop did not have an endpoint security agent installed?

How would you know if an asset was not being scanned by a vulnerability scanner as scheduled, because it is hidden behind a firewall or in an unknown network segment?

Without clear dashboards and reliable reports on your security gaps and risks, it's like they never happened.



How Armis Helps

Armis Centrix™ provides a clear understanding of what's in your network, including physical and virtual assets and your software assets.

It identifies old operating systems that are no longer supported (EOL/EOS) and ensures that agent versions are up-to-date. With Armis you can monitor all of these in minutes, reducing your risk and avoiding the unnecessary cost that legacy systems entail.

Armis dashboards and reports help validate the implementation and proper operation of your existing security controls (EDR, vulnerability scanners, etc.) and identify gaps in deployment. It finds all assets that are not protected or are out of compliance and helps remediate the issues quickly.

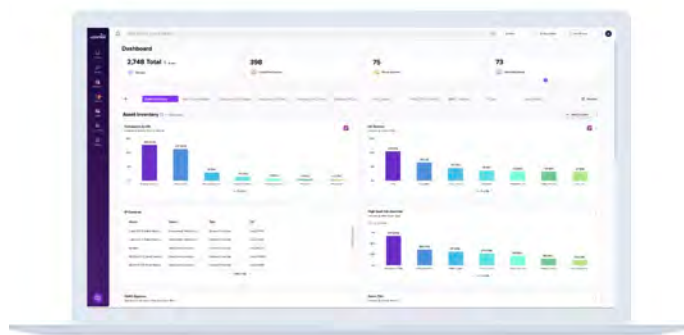
Our metrics, dashboards, and reports factor in asset inventory, network traffic, device behavior analysis, security alerts, compliance reports, and vulnerability reports. Curated Values Packs make it even easier with out-of-box policies, dashboards, and reports to streamline your business workflows and benefit from deployment best practices specific to your industry.

Examples include:

Endpoint Agent Verification: quickly find devices that are missing an endpoint agent.

Technical Debt: identify aging Operating Systems and hardware.

Vulnerability Gap Analyses: uncover devices not being scanned by assessment tools.



Users can enrich these metrics and reports and share these with relevant stakeholders while restricting access to sensitive information. Our user interface and experience are designed to be intuitive and dynamic, providing easy access to the information needed:

Navigate through different dashboards and reports and contextually drill down into specific data for analysis.

Visualize the environment through interactive network infrastructure maps showing device information, logical connections, and risk levels.

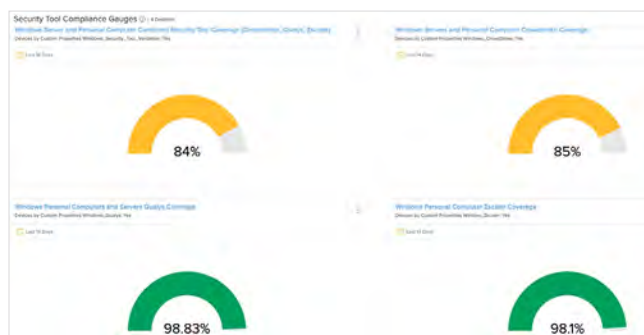
Users can also view the historical data of their environment using customizable retention policies. This enables data and trends analysis to help customers make informed decisions about their environment.

Advanced Use Cases - Made Easy

Below are a few examples of how Armis visualizes data and communicates a clear message about the progress of specific values over time.

Gauge Dashlets

The gauge visualization emphasizes the gap and helps you to focus on what matters first. Users can quickly customize any goal or KPI, and grasp progress in the blink of an eye to facilitate informed decision making.



Trend Over Time

Executive reports are all about data visualization: It helps to communicate a clear message about the progress of a value over time.

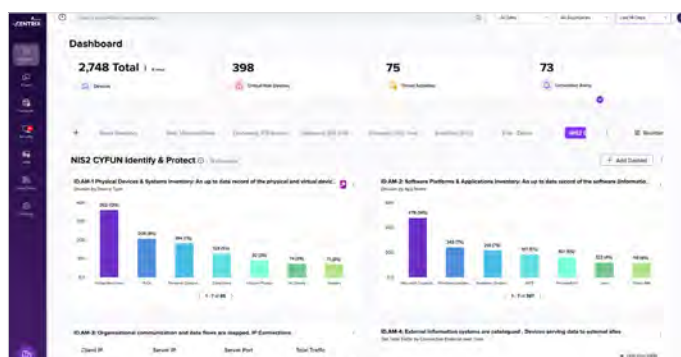
For example: CISOs may want to know if they have more devices with active endpoint agents compared to last month, so they can share progress with the CIO.

“Trend Over Time” is available for gauge and count dashlets in Armis Centrix™.

Dashboards

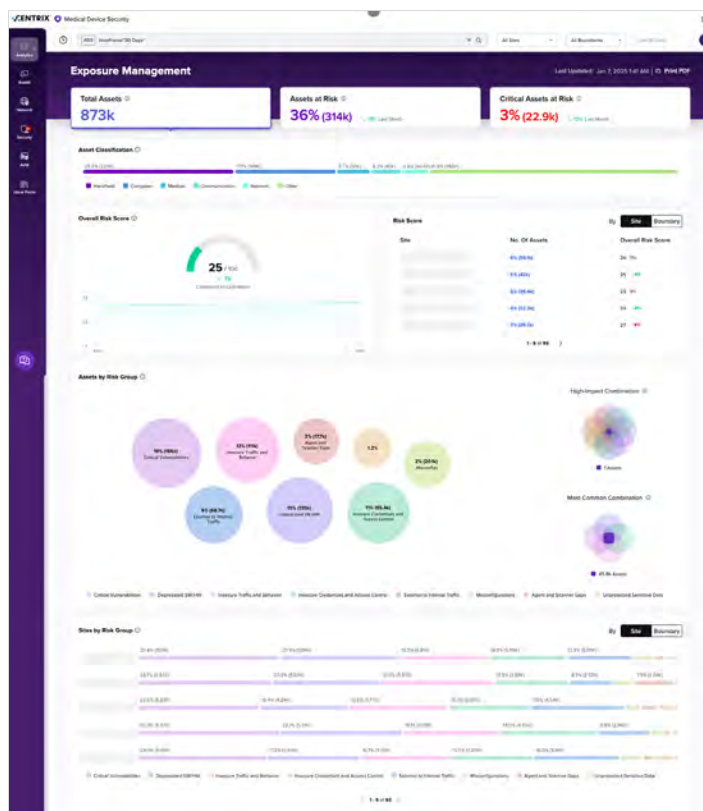
Armis users benefit from powerful visualization capabilities for reporting and dashboarding. The brains behind these representations is the Armis Standard Query (ASQ), supporting natural language input and thus can be purpose-built to meet the precise need.

Pivot tables are supported as well, eliminating the need to export the data to another tool for analysis.



The Armis Exposure Management dashboard, provides a comprehensive view of your attack surface and exposures, both globally and with the ability to compare across sites or boundaries. This dashboard enables executives to:

- Understand the exposure landscape across their attack surface and track progress in reducing risk.
- Identify high-risk areas within the business and uncover the most common exposures.
- Save time and manual effort in collecting the data for reporting.



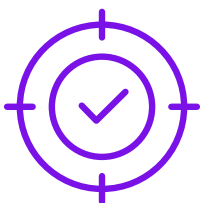
Executive Reports

C-level employees often don't have access to the Armis console. Instead, they are looking for a singular executive report that displays the dashboard data for reviewing purposes without having to log into Armis to get the information.

Armis offers the ability to export a Report as a PDF document, so it can easily be shared.

With easy deployment interfaces, an intuitive console navigation, and the dashboards and reports you need: we offer the fastest route to see, protect and manage all your assets - IT, IoT, OT and IoMT, whether managed or unmanaged.

With Armis Centrix™ you are informed in real-time, track progress effortlessly, and take actions to enhance your security posture.



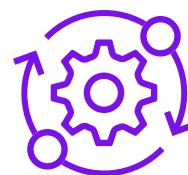
Focus

Cut through the noise and use data visualization to demonstrate progress.



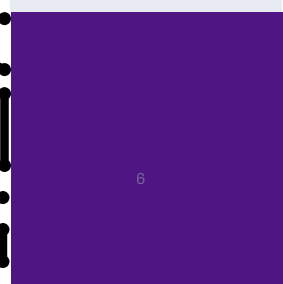
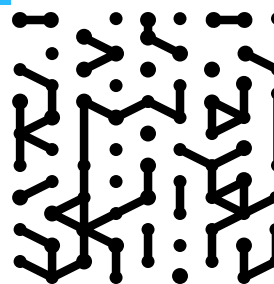
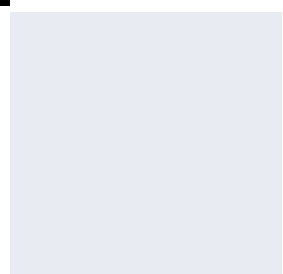
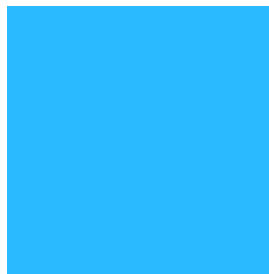
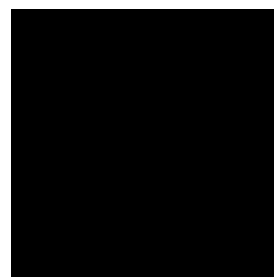
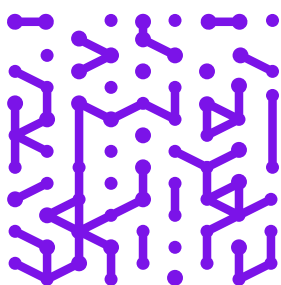
Efficiency

Less manual efforts, no more spreadsheets.



Impactful Actions

Make optimal use of existing resources.





Armis, the cyber exposure management & security company, protects the entire attack surface and manages an 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

