SOLUTION BRIEF

# Armis Centrix™ Smart Active Querying for Intelligent IT, OT, IoT, and IoMT Security

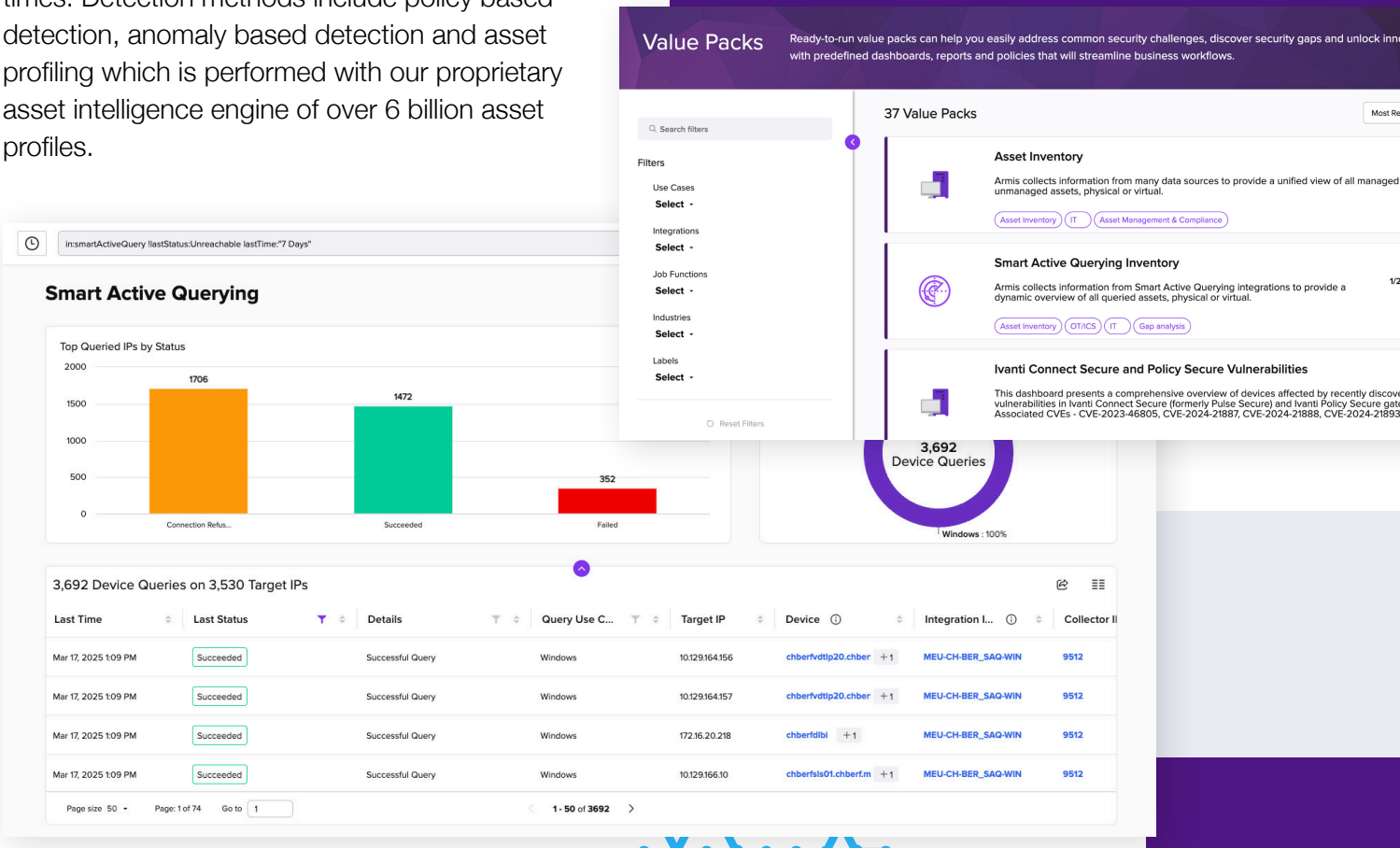
# Solution Brief

In today's world, complete asset discovery is more important than ever before. Achieving the best possible continuous visibility of your devices is foundational to the protection and management of your organization.

Armis goal is to provide extreme visibility into every device in the network; whether it is IT, OT, IoT or IoMT. One of the root causes for risk or vectors for a security breach is due to a lack of visibility within a siloed digital environment. Armis Centrix™ breaks this practice by utilizing a multi-discipline detection engine which not only discovers each asset in your organization, but also delivers deep context and insights so that you know the condition of your environment at all times. Detection methods include policy based detection, anomaly based detection and asset profiling which is performed with our proprietary asset intelligence engine of over 6 billion asset profiles.

## Getting Active About Device Security

> Traditional network monitoring may not capture essential asset data that resides on devices.
>
> Armis Smart Active Querying retrieves additional detailed asset information that compliments passive traffic inspection in a revolutionary, safe way.



# Smart Active Querying with Armis Centrix™

## How It Works

Unlike passive monitoring, which observes network traffic, active querying initiates communication with devices in their native language to gather specific information.

Active querying involves the use of specialized technology to interact with and retrieve information directly from the device. This includes both traditional IT as specialized equipment such as Programmable Logic Controllers (PLCs), Remote Terminal Units (RTUs), Building Management Systems (BMS), medical devices, and other components.

Armis Smart Active Querying starts with the identification of target devices, IP ranges, VLANs etc. within the network. This can involve discovering devices based on known protocols, IP addresses, or other device characteristics. Active querying is conducted using the native industrial device communication protocols. This ensures compatibility and minimizes the risk of disruption. The queries are formulated in the specific device's native device language, and emulates the queries made by an Human Machine Interface (HMI) to the device. The queries retrieve specific device information, including details such as device type, firmware version, configuration settings, logged-in users, and other relevant metadata. Security including encryption and authentication protects the process and the data being retrieved.

To ensure the safety and stability of the queried devices, active querying is typically read-only. Active querying is often performed during periods of low network utilization to minimize any potential impact on operational processes. Optimally timing polling intervals helps ensure that the querying process does not interfere with the real-time demands of critical systems. Armis Smart Active Querying solutions empowers administrators with customization options, allowing organizations to define query frequencies, policies, and specific IP ranges. This flexibility ensures that the active querying process aligns with the unique requirements of each specific environment.

# Key Benefits of Armis Smart Active Querying

## Complete Assets Profiling

For devices with limited visibility, you can trigger smart active querying to instantly retrieve deeper insights, ensuring a more complete and accurate device profile.

## Fast Deployment

Smart active querying helps you discover devices in new locations and identify gaps in sensor coverage, ensuring comprehensive visibility across your network.

## Discover Inactive or Volatile Devices

Discover new devices on the network with complete context, including detailed attributes like OS, firmware version, and installed applications.

## Retrieve Live Statuses on Demand

Security teams focused on mitigation can trigger smart active queries to instantly verify if a device's firmware or operating system has been updated, enabling faster incident resolution.

It promotes a vendor-agnostic approach, minimizing disruptions and ensuring compatibility with controller vendors.

## Smart Active Queries Compliment our Holistic Discovery Methods

Armis provides a multi-faceted approach to device discovery that is essential for organizations operating in sensitive environments. Active discovery, when combined with passive traffic inspection, integrations, and the Armis Asset Intelligence Engine, offers complete visibility, security and control over network assets. By incorporating active discovery with uptime and usage tracking, Armis empowers organizations to proactively oversee their assets, mitigate disruptions, and enhance the security and efficiency of their networks.

Armis Centrix™ revolutionizes active querying, providing a safe, effective, and comprehensive solution for enhanced IT, OT, IoT, IoMT and ICS security.

- Learn more at **armis.com**

**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