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 database of over 3.5 billion asset profiles.

Getting Active About Device Security

> Armis detection techniques include what is traditionally referred to as passive and active querying. While early ICS security technologies discouraged active querying to PLCs or DCSs due to potential system destabilization, Armis Centrix™ leverages new advancements to make active querying not only safe but a crucial element in fortifying an organization's operations.

Smart Active Querying with Armis Centrix™

How It Works

Active querying in OT (Operational Technology) environments involves the use of specialized technology to interact with and retrieve information directly from industrial devices, such as Programmable Logic Controllers (PLCs), Remote Terminal Units (RTUs), and other components. Unlike passive monitoring, which observes network traffic, active querying initiates communication with devices in their native language to gather specific information.

Armis Smart Active Querying starts with the identification of target devices, IP ranges, VLANs etc. within the OT 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 industrial 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 OT environment.

Key Benefits of Armis Smart Active Querying

Complete Situational Awareness

Challenge: Selectively sniffing traffic may result in delayed detection of security incidents.

Armis delivers: Armis provides a 360-degree view across the entire environment, conducting queries during low network utilization using the same stable methodology as an HMI querying a PLC. This ensures timely and granular situational awareness beyond traditional network traffic analysis.

Know Your Assets

Challenge: Traditional network monitoring may miss essential asset data residing on devices.

Armis delivers: Device querying retrieves detailed asset information, including logged-in users, hotfixes, firmware versions, and backplane details, enhancing overall asset identification and management.

Dormancy May Hide A Compromised Device

Challenge: Up to 50% of OT devices do not communicate on the network, leading to potential blind spots.

Armis delivers: Smart Active Querying ensures complete visibility, allowing direct information gathering from devices, even when dormant, to proactively mitigate attacks.

Contextualized & Rapid Incident Response:

Challenge: Passive monitoring may generate alerts, requiring additional context mining.

Armis delivers: Active querying of relevant devices in response to suspicious events provides contextual details, resulting in more meaningful alerts and accelerated incident response with drill-down capabilities.

Proactive Risk Management

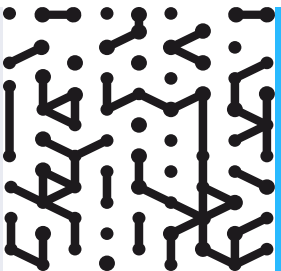
Challenge: Relying on network-only approaches may delay vulnerability awareness.

Armis delivers: Smart querying of servers and controllers for OS versions, firmware, and patch levels ensures up-to-date vulnerability management, preventing delays associated with incomplete device information passing over the network.

Validation of PLC/DCS Integrity

Challenge: Unauthorized changes via direct connections may go undetected with passive monitoring.

Armis delivers: Periodic capture of device snapshots and comparison to baselines through active querying validates controller integrity, identifying and preventing unauthorized changes.



Operational Resiliency

Challenge: Rolling back from an incident without tracing control device changes can be challenging.

Armis delivers: Capture of device configuration snapshots enables holistic backup to the “last known good configuration,” simplifying incident recovery and reducing costs.

Customizable Approach

Challenge: Traditional ICS lacks flexibility and compatibility with diverse control devices.

Armis delivers: Armis Centrix™ is fully customizable, working with a wide set of protocols and manufacturers across IT, OT, IoT, and IoMT. It promotes a vendor-agnostic approach, minimizing disruptions and ensuring compatibility with controller vendors.

Lower Total Cost of Ownership (TCO)

Challenge: Deploying network-only technologies at every intersection can be expensive.

Armis delivers: Armis Centrix™ optimizes efficiency by monitoring all routable sections of the network with zero footprint, reducing hardware and maintenance costs for a lower total cost of ownership.

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

Learn more at **armis.com**

ARMIS

Armis, the asset intelligence cybersecurity 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, secure, protect and manage all critical assets.

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 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