# Smart Active Queries from Armis Centrix™

Is fragmented visibility and incomplete understanding hindering your IT, OT, medical, IoMT and IoT security? Armis Centrix™ Smart Active Querying transcends passive monitoring to actively illuminate blind spots and silent threats in your environment.

Smart Active Queries are Answering Challenges Posed by Traditional Methods:

Traditional security approaches are failing to keep pace with the evolving threat landscape. Passive network monitoring can leave blind spots, hidden devices lurk undetected, and fragmented data creates ineffective responses to complex threats. Manual processes are still heavily relied on, leading to wasted resources and potentially dangerous decisions. This lack of transparency allows unauthorized changes to go under the radar, while siloed communication creates operational vulnerability. It's time to embrace more holistic methods: active querying that shines a light the shadows, contextualizes alerts, and empowers proactive defense.

Smart Active Queries from Armis Centrix™ at Work:

Unlike passive network monitoring, Armis Smart Active Querying actively engages IT, medical and industrial devices in their native language, retrieving detailed information on device type, firmware, configuration, and users. Conducted during low network activity with robust security measures, this read-only approach provides comprehensive visibility into dormant devices and hidden vulnerabilities, empowering administrators to customize queries and enhance operational resilience in any environment.
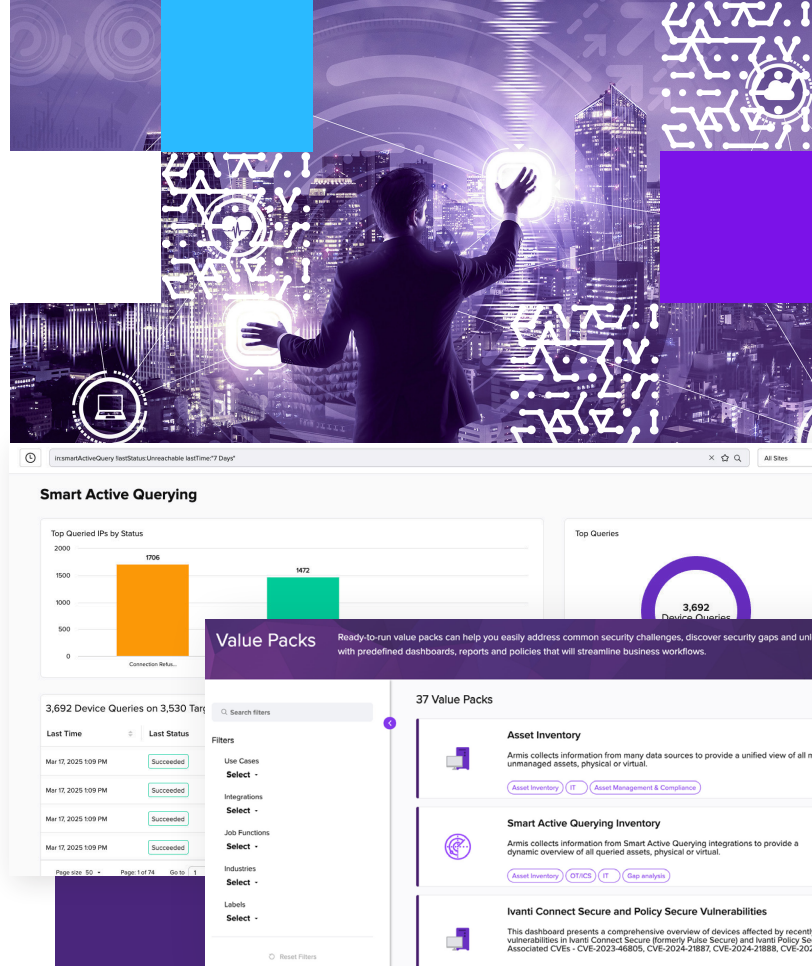
Armis Does Active Querying the **Smart** Way:

- We never blindly scan.

- We query in the language the device expects.

- We use our 6 bn+ Asset Intelligence Engine to contextualize your active query data.

- Our Smart Active Queries provide a more granular, advanced approach compared to traditional active methods today thanks to our AI-driven Asset Intelligence Engine.

- We don't send out queries haphazardly, we do it at preconfigured times on an interval that is smart for the device and when it will not impact operations.

- The queries we send are completely safe and gather data the same way devices query one another.

- Decide you want to turn off Smart Active Queries? With Armis you have total control.

- Tailor your approach to your specific needs by defining device inclusion/exclusion and setting optimal polling intervals for efficient collection.

10 Things with Smart Active Querying:

1. Granular Identification for Enhanced Visibility:

Comprehensive and accurate device identification, enabling deeper visibility, robust security, and granular control across your entire network.

2. Deep Dive Beyond the Surface:

Uncover detailed device information including firmware versions, configuration settings, logged-in users, and more.

3. Improve EOL/ Dormant Device Process:

Illuminate dormant devices that traditional methods miss, eliminating network blind spots and closing security gaps.

4. Full Contextual Awareness:

Gain complete situational awareness with comprehensive device behavior and status insights, including individual backplane configurations.

5. Rapid Response in Critical Environments:

React to security incidents swiftly and definitively with rich contextual data and the ability to rollback to a previously known 'good state'.

6. Proactive Vulnerability Management:

Stay ahead of evolving threats with automated vulnerability identification and prioritization, ensuring critical patches or mitigation actions are applied before exploitation becomes a risk.

7. Validating Device Integrity:

Verify device configurations and identify unauthorized changes in real-time, safeguarding your network from manipulation.

8. Operational Resilience:

Address potential threats before they escalate, significantly enhancing your operational resilience and minimize the impact of cyberattacks.

9. Customizable for Optimized Performance:

Tailor your active querying approach to your specific needs by defining device inclusion/exclusion and setting optimal polling intervals for efficient data collection.

10. Measurable ROI:

Invest in a solution that delivers a clear return on investment. Smart Active Queries from Armis Centrix™ help you reduce risks, minimize downtime, and improve operational efficiency.

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.

PROTECT
Take proactive measures, detect threats, stop attacks

SEE
Discover, contextualize, enrich and profile every asset

MANAGE
Establish workflows and track riskreduction

ARMIS CENTRIX™
The Cyber Exposure Management Platform

Attack Surface

Integrations | Telemetry | Asset Intelligence Engine