



ARMIS + VIAKOO

AUTOMATICALLY DISCOVER AND REMEDIATE UNMANAGED AND IOT DEVICE RISKS

Even the largest organizations have difficulty finding every asset in their environments. And while a complete asset inventory provides the foundation for an effective security strategy, identifying and remediating the risks these devices pose is the best way to understand and reduce your attack surface.

The Armis® Agentless Device Security Platform integrates with the Viakoo® Action Platform to help resolve these problems and more. The Armis platform can see almost five times more assets than traditional IT and security products like vulnerability management, EDR, and CMDB. The platform also identifies security gaps and device vulnerabilities, detects threats and anomalous behavior, and automates policy enforcement.

Viakoo uses this information to remediate risks on devices automatically, ensuring they are operational, secured, and working as expected. The actions Viakoo takes include triggering firmware updates, forcing password rotations, refreshing certificates, and more. Together, this joint solution helps organizations realize the full value these devices offer in a safe, secure environment.

JOINT SOLUTION BENEFITS:



BETTER VISIBILITY

Every device visible, operational, and secured



GREATER VALUE

Solution benefits facilities, IT, and security teams



IMPROVED COMPLIANCE

Easier to prove and pass corporate or regulatory audits



ADVANCED PROTECTION

Reduce attack surface by finding and mitigating risks

Identify and classify devices in any environment

Bad actors see your environment as one interconnected attack surface, making pervasive visibility into every device in your environment a critical need. Armis discovers all devices in your environment—managed, unmanaged, OT, medical, and IoT—on or off your network and in your airspace—giving you the most comprehensive asset inventory available.

Armis is agentless and passive, which is vital because you can't install agents on unmanaged and IoT devices, and scanning them could cause them to fail. Even without an agent, Armis can identify the device type, manufacturer, model, IP and MAC address, OS, reputation, username, software, behavior, connections, risk factors, and more.

Like Armis, Viakoo is also agentless and passive. It performs application-based discovery, finding devices by first looking at the software applications that use IoT devices as sensors (e.g. video cameras), and then following the path from the application to the specific devices. This provides additional information about configuration, usage, performance, and device relationships (i.e. semantic correlation), yielding a full complement of device data.

Armis and Viakoo bidirectionally share device information, ensuring asset managers, IT staff, and security teams have all the information they need about every device they encounter.

Understand and respond to device risks

Busy security teams need to identify, prioritize, and mitigate vulnerabilities fast—not just for compliance with regulatory frameworks but to thwart bad actors from using at-risk devices to stage an attack.

Armis calculates a risk score for every device based on factors like known vulnerabilities, known attack patterns, and a device's behavior. Viakoo can use this information to identify out-of-compliance devices and eliminate risk by taking action like triggering a firmware update, a certificate refresh, or a forced password change.

This automated mitigation reduces risk and reduces costs by fixing vulnerable devices and returning them to service with an improved security posture.

Frictionless deployment & integration

The more quickly a platform fits into an organization's existing infrastructure, the sooner busy IT and security pros can start seeing value. Both the Armis and Viakoo platforms are agentless and don't require the installation of any hardware in your environment. They can install in as little as minutes, using the infrastructure you already have, with no network changes.

Armis integrates with Viakoo and your other IT security and management systems just as easily, from your firewall to your NAC to your SIEM, helping you get greater value out of your investments and more automated threat response.

ABOUT ARMIS

Armis is the first agentless, enterprise-class security platform to address the new threat landscape of unmanaged and IoT devices. Fortune 1000 companies trust Armis'our unique out-of-band sensing technology to discover and analyze all managed, unmanaged, and IoT devices—from traditional devices like laptops and smartphones to new unmanaged "smart" devices like video cameras, smart TVs, printers, HVAC systems, industrial robots, medical devices and more. Armis discovers devices on & off the network that connect and communicate via wired, WiFi, Bluetooth, Zigbee, and many other common protocols that are invisible to legacy security systems. Armis continuously analyzes endpoint behavior to identify risks and attacks, to protect critical information and systems. Through integration with your switches and wireless LAN controllers, as well as your existing security enforcement points like Cisco and Palo Alto Networks firewalls or network access control (NAC) products, Armis can quarantine suspicious and malicious devices.

ABOUT VIAKOO

Viakoo makes things work securely. Viakoo's vision is for every connected enterprise device to be 100% visible, operational, and secured. The agentless Viakoo Action Platform keeps distributed unmanaged and IoT environments secure and continuously operational at the lowest risk and cost. Automated device cyber hygiene is reliably updated at scale with firmware, passwords, and certificates to elevate security posture and system performance to enterprise IT expectations. Viakoo Inc. is a leader in cyber hygiene for connected devices, located in Mountain View, California, USA. Follow us on [Twitter](#), [LinkedIn](#), and [Facebook](#).

©2021 Armis, Inc. Armis is a registered trademark of Armis, Inc. All other trademarks are the property of their respective owners. All rights reserved.

20210216-1