PARTNER BRIEF

Armis + Viakoo: Automatically Discover and Remediate Unmanaged and IoT Device Risk

Overview

Modern enterprises are powered by an ever-growing web of connected devices including laptops, cameras, sensors, building management systems, medical equipment, and countless other assets. These devices are vital to operations but often exist outside the reach of traditional security tools. As a result, organizations face expanding attack surfaces and hidden risks that can be exploited by threat actors.

To address this challenge, Armis and Viakoo have come together to deliver a joint solution that unites complete device visibility with automated remediation. Armis Centrix™ discovers and classifies every device in your environment, while continuously assessing their behavior, vulnerabilities, and risk posture. The Viakoo Action Platform then takes this intelligence and automatically remediates IoT device issues, ensuring each asset remains secure, compliant, and operational. Together, the joint solution helps organizations reduce risk, eliminate manual effort, and protect the integrity of the digital estate.

State of the Market

The connected enterprise has transformed the digital landscape. In most organizations today, more than half of the devices communicating across the network are unmanaged or IoT devices; assets that cannot run agents, are difficult to patch, and often fall outside IT's direct control. From IP cameras and badge readers to MRIs and programmable logic controllers, these systems play critical roles in operations but are frequently invisible to traditional IT and security solutions such as vulnerability management platforms, endpoint detection and response tools, or configuration management databases.

As the number of connected devices continues to surge, attackers are exploiting these blind spots to gain access to sensitive systems and data. Meanwhile, regulatory scrutiny and compliance mandates are tightening, putting additional pressure on organizations to maintain continuous visibility, security control, and compliance across every connected endpoint. The result is a growing need for automated solutions that not only identify risks but take meaningful, timely action to resolve them, without disrupting operations.

The Challenge

The first step in securing any environment is knowing what's there. IoT devices have become indispensable to modern business operations, connecting everything from security cameras and sensors to medical imaging systems and industrial control units. Yet, the same characteristics that make IoT technology powerful, its ubiquity, connectivity, and diversity, also make it a prime target for cyberattacks.

Most IoT devices were not designed with security as a foundational principle. They often run proprietary or outdated operating systems, lack native patching mechanisms, and cannot support endpoint protection agents. Many are installed and forgotten. They are frequently deployed by facilities or operational teams outside IT's purview and rarely inventoried. As a result, organizations are left with thousands of unmanaged and often unmonitored devices communicating across their networks.

Traditional security tools like vulnerability scanners and EDR platforms fail to detect or protect these assets, leaving blind spots in visibility and creating significant risk exposure. Even when IoT devices are discovered, updating or reconfiguring them can be complex and time-consuming, especially in large-scale or operationally sensitive environments such as hospitals, factories, or transportation hubs. The inability to identify vulnerabilities, apply patches, or enforce consistent security policies at scale means that many IoT devices remain perpetually vulnerable to exploitation.

Without automated visibility and remediation, organizations struggle to answer fundamental questions: What devices are connected to my network? Which ones are at risk? How can I fix them without disrupting operations? Until those challenges are addressed, IoT will remain one of the most critical and least controlled elements of the modern attack surface.

The Solution

The joint Armis + Viakoo solution is purpose-built to address the unique challenges of securing IoT environments, where devices are often unmanaged, agentless, and critical to operations. Together, the two platforms bridge the gap between visibility and action, allowing organizations to not only see every connected device but also automatically remediate risks before they can be exploited.

How It Works

Armis delivers unparalleled, deep situational awareness across all connected assets, managed or unmanaged, IT or IoT, medical or operational. Using non-intrusive active querying and passive analysis combined with AI-driven device profiling, Armis identifies every device in the environment and maps its relationships, behavior, and risk posture. Because it operates agentlessly, Armis can safely discover even the most sensitive IoT systems that cannot tolerate scanning or modification. The platform assigns a dynamic risk score to each device based on factors such as known vulnerabilities, behavioral anomalies, and asset criticality to the business, giving security teams the intelligence, prioritization and automation needed to quickly remediate unacceptable organizational exposure.

Viakoo complements this by turning insight into action. Leveraging the intelligence provided by Armis Centrix™, the Viakoo Action Platform automatically remediates device risks and enforces security best practices across the IoT ecosystem. This includes initiating firmware updates, rotating weak or default passwords, refreshing expired certificates, and ensuring configuration consistency, all without manual intervention or service disruption.

The integration between Armis and Viakoo is fully bidirectional, ensuring continuous data sharing and synchronization across platforms. When Armis detects a vulnerable or misconfigured device, Viakoo can take immediate corrective action. Likewise, Viakoo's remediation outcomes feed back into Armis, updating device posture and maintaining real-time accuracy across the asset inventory.

By combining comprehensive visibility with automated remediation, Armis and Viakoo enable organizations to secure their IoT footprint at scale, thereby reducing risk, improving compliance, and ensuring devices remain both operational and protected. This joint solution turns what was once an unmanageable challenge into a continuous, automated, and measurable security process for the connected enterprise.

This seamless coordination allows organizations to scale IoT security across thousands of devices effortlessly, reducing mean time to remediation, improving compliance, and dramatically strengthening the overall security posture of their connected environments.

Use Cases

The Armis and Viakoo joint solution applies across a wide range of industries and environments. In healthcare, it can automatically identify vulnerable medical devices, flag those out of compliance, and trigger secure credential or firmware updates, without taking critical systems offline. In manufacturing and industrial environments, it brings visibility to every connected sensor, robot, and control system, while ensuring security policies and configurations remain up to date.

For enterprise IT and corporate environments, the solution delivers complete oversight of IoT devices like cameras, printers, and smart building systems, which are common entry points for attackers. It automatically remediates misconfigurations or expired certificates before they can be exploited. The joint solution reduces the operational burden on security and IT teams by streamlining the process from detection to remediation.

Key Business Outcomes and Benefits

Organizations that deploy the Armis and Viakoo integration gain a unified view of their connected environment and an automated mechanism to keep it secure. This translates directly into measurable outcomes including: faster risk reduction, stronger security posture, improved compliance, and reduced operational overhead.

By using the existing network infrastructure and seamlessly integrating with other enterprise systems, the solution delivers immediate value without the complexity of re-architecting environments. Over time, it enables a more mature, proactive security model, where visibility, risk assessment, and remediation are continuous and automated rather than reactive and manual.

Conclusion

The combined power of Armis and Viakoo transforms how enterprises secure their connected world. By continuously discovering every device, assessing its risk, and automatically remediating vulnerabilities, the joint solution helps organizations protect their operations while unlocking the full potential of their connected technologies. With Armis and Viakoo, organizations gain the confidence to operate safely in a world that contains inherent cyber exposure risk.