

Viakoo Action Platform™

Enterprise IoT Security
Automated Remediation and Repatriation

Current estimates show typically there are ~5-10 IoT devices per employee, or thousands to 100s of thousands in an enterprise, put to work solving business problems and delivering critical services to the organization. These IoT devices are smart, essentially miniature computers, consisting of operating systems and communications ports, needing to be managed like their cousin servers in the data center. Until now IoT devices have not been managed to the same standards of IT devices, and because of that have inadvertently created a massive attack surface for cyber hackers, leading to ransomware and data exfiltration. Many organizations deploy discovery tools to identify IoT device vulnerabilities and protect the network by port-blocking, but this also blocks the business from the value it was getting from the IoT device as it is unable to rejoin the network as a full, secure network citizen.

- Ensures IoT devices deliver their value to the business
- Remediates devices to a known safe state, ready for repatriation
- Repatriates devices as fully documented, operational and compliant
- Works with both Loosely and Tightly Coupled devices
- Viakoo is a trusted expert on IoT device hygiene

Viakoo delivers an automated, scalable solution that addresses IoT device remediation so devices can securely rejoin the network, becoming operational again, and delivering their value to the business.

The Viakoo Action Platform™ enables both Loosely Coupled and Tightly Coupled IoT devices to deliver the business value an organization

needs while eliminating the cyber threat they represent, with an enterprise-class solution that delivers full device remediation, repatriation, and compliance.

Tightly Coupled devices are members of collections of devices that work together as a team to achieve a specific business outcome.

Viakoo Action Platform

The Viakoo Action Platform delivers on the end goal of managing IoT devices to the same IT standard used in the data center. IoT devices that are secure with documented compliance mean lower risk and continuous remediation. The Viakoo Action Platform is an enterprise scalable, automated solution that reduces organizational risk, saves time and cost while enabling IoT device ROI. The flexible and modular solution allows you to start small and grow over time while delivering value at each step.

Take Control of Your Devices

- ~20% Critical CVE scores
- >50% Security patches needed
- >90% Certificates missing (802.1x)
- >50% Passwords using default settings

Eliminate IoT Risk with Viakoo Action Platform

The Viakoo Action Platform Solution

The Viakoo Action Platform solves the problem of managing 10,000s to 100,000s of IoT devices affordably. Delivered as a SaaS offering, the Platform has a series of modules that ensure

all devices are inventoried, in compliance with internal policy, are continuously remediated and repatriated as full network citizens. The Platform uses a “digital twin” model of IoT applications

and device infrastructure to maintain overall integrity. The Viakoo Action Platform ensures cyber hygiene 802.1x certificate provisioning and management, firmware upgrading, and password enforcement. Viakoo Action Platform

also ensures IoT devices are continuously operational and delivers alerts when failures occur. Devices are continuously tracked for compliance and audit purposes.

The Viakoo Action Platform Complete IoT Cyber Security Solution



Viakoo Action Platform Modules

Device Firmware Manager

Security patches are crucial for IoT device security. Security patches are made through IoT firmware upgrades and must be implemented continuously as they become available.

Device Firmware Manager automates the process of firmware updates on IoT devices, at scale across the enterprise. DFM provides

compliance reporting complete with a history of changes for audit purposes. A secure “chain-of-trust” ensures only valid and functional firmware is deployed, and complete automation allows for updates of thousands of devices wherever they live.

Device Certificate Manager

Certificates of Authenticity support Zero Trust implementations and thwart man-in-the-middle attacks.

Device Certificate Manager enables automation of the process of installing, managing, revoking, and updating device certificates such as 802.1x, TLS/LLS, OPC-UA and others. DCM provides detailed information on both managed and unmanaged IoT devices, their certificate status, and automates action to maintain them. A chain-of-custody process is incorporated to ensure device certificates cannot be modified or compromised.

Device Password Manager

Credentials, password strength and periodic rotation, are critical to IoT security and must be enforced continuously, at scale.

Device Password Manager automates the process of setting, maintaining, and managing IoT device passwords at scale. DPM automates verification of password and password policy management for thousands of IoT devices from a wide variety of vendors, providing password status, automated checking, and an audit trail for governance.

Viakoo Physical Security Modules

Please visit the Viakoo physical security website for a complete overview of our products and solutions to ensure physical security at www.physical.viakoo.com

Master the security of your cyber-physical systems with the Viakoo Action Platform.