

ARMIS + VIAKOO

Armis and Viakoo Deliver Automated IoT Security to Major Commercial Banks

Large commercial banks leverage a variety of Internet of Things (IoT) to drive business outcomes. In turn, these organizations are prime targets for hackers as their attack surface continues to expand.

Armis and Viakoo understand the IoT security needs of financial organizations and the criticality of an automated solution. The greatest challenge securing IoT infrastructure is consistently updating devices with the appropriate firmware, certificates, and the like traversing various network topologies.

Below is a case study addressing a commercial bank's IoT Security challenges.

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 regulatory audits



ADVANCED PROTECTION

Reduce attack surface by finding and mitigating risks

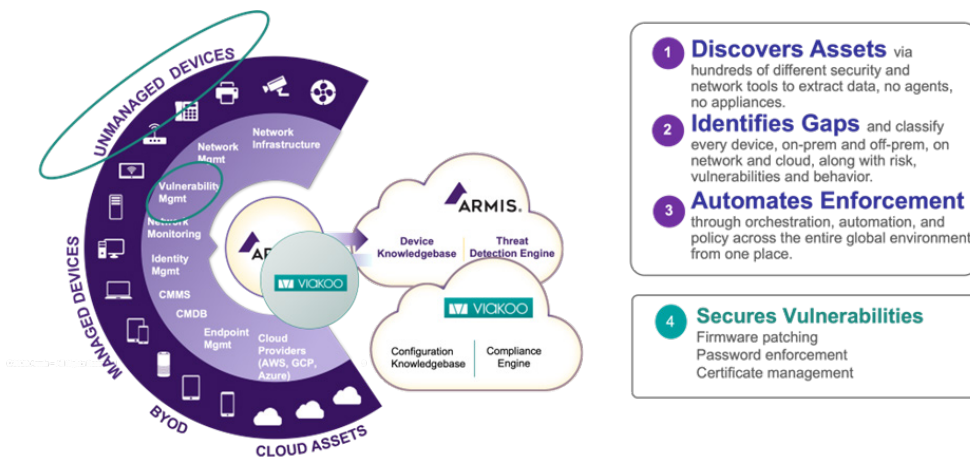
Situation

A large commercial bank was challenged with securing thousands of IP Cameras, access control points, printers, and the like. The bank's security staff and red teams were confronted with manually discovering IoT vulnerabilities and remediating them, taking up valuable time and generating significant manpower costs to keep IoT devices secure. Simply, this bank was not able to ensure that their IoT architecture was secure on a consistent basis.

Solution

Armis and Viakoo conducted a security assessment for the entire bank's IoT security posture and provided a blueprint to automate the security of all IoT devices which included the consistent discovery of vulnerabilities and remediation thereof.

Armis-Viakoo Joint Solution Architecture



- 1 Discovers Assets** via hundreds of different security and network tools to extract data, no agents, no appliances.
- 2 Identifies Gaps** and classify every device, on-prem and off-prem, on network and cloud, along with risk, vulnerabilities and behavior.
- 3 Automates Enforcement** through orchestration, automation, and policy across the entire global environment from one place.

- 4 Secures Vulnerabilities**
 - Firmware patching
 - Password enforcement
 - Certificate management

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](#).

OUTCOME

Today the bank is now monitoring and managing its' IoT security by leveraging the integrated Armis-Viakoo solution. They can easily see all vulnerabilities identified and automatically remediate them within hours if not minutes. This has drastically reduced costs, manpower, and provided the bank with clear visibility regarding the security status of its' IoT security posture enabling it to adhere to the bank's Zero Trust security policy.

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