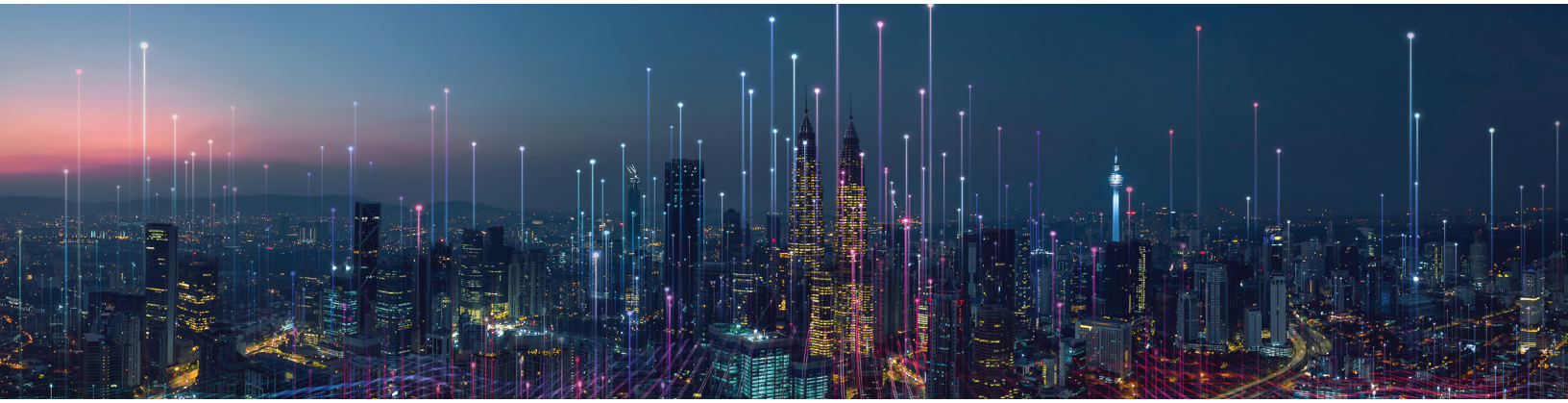
ARMIS + CHECK POINT

VISIBILITY AND PROACTIVE SECURITY FOR UNMANAGED AND IOT DEVICES



Enterprise networks typically include many different kinds of unmanaged and IoT devices. Many of them run on unpatched software, are misconfigured, or use unsecured communication protocols, which makes them extremely vulnerable and easy to hack. Most traditional security products can't see these devices, and the ones that can often don't know what to do with them because they can't identify them accurately. You need more than just an IP address to tackle threats in a way that's effective but not disruptive to critical equipment like medical and manufacturing devices.

Armis and Check Point provide superior visibility and security for unmanaged and IoT devices. Without any agents or additional hardware, Armis uses the existing infrastructure to discover and identify every device in any environment—enterprise, medical, industrial, and more. Armis analyzes device behavior to identify risks and threats and provides continuous device risk assessments.

The combination of the Armis platform's advanced device visibility and monitoring with Check Point's policy management and security gateways reduces your exposure to the risks of unmanaged and IoT devices and provides security teams with deeper device insights—all without disrupting business operations.

Create Policies for Any Unmanaged and IoT Device

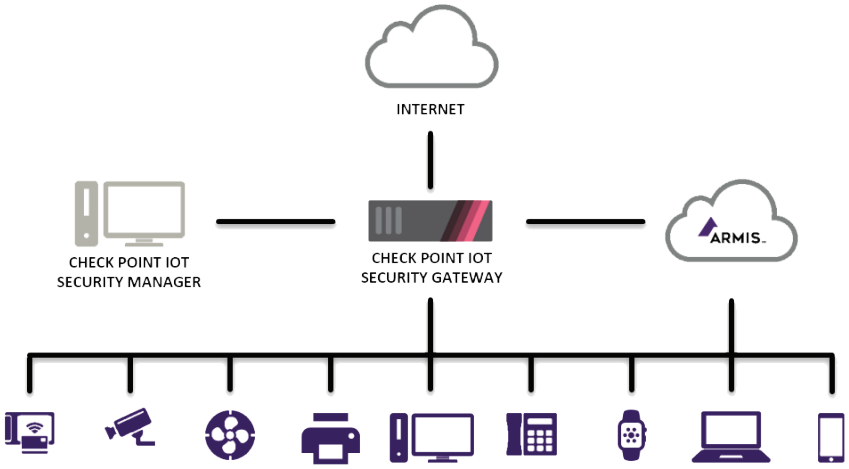
As Armis discovers devices in your environment, it provides the Check Point IoT Security Manager with granular device attributes like the manufacturer, model, operating system, MAC address, and more. Armis also provides a risk analysis based on a contextual understanding of a device's behavior in your environment.

In the IoT Security Manager console, you can configure policies based on these attributes, and you can enable policy recommendations made by Armis. This allows you to reduce your risk exposure proactively by ensuring your security gateway has policies for any device in your environment—policies that can react to changes in device attributes, behavior, and risk level.

KEY BENEFITS

- Reduce your exposure to the risks of unmanaged and IoT devices.
- Tackle threats effectively, without disrupting your business operations.
- No impact on your organization's network. No device scanning.

For example, you can set granular rules that restrict devices from using unapproved protocols, applications, and communication patterns. You can also set policies to alert on anomalies in device behavior or communication patterns. And to help avoid confusion or conflicts, the Check Point IoT Security Manager keeps policies for unmanaged and IoT devices separated from policies for your entire network.



Detect and Respond Quickly to Threats and Vulnerabilities

The solution uses continuous device analysis to detect threats and vulnerabilities associated with unmanaged and IoT devices (i.e., CVE's, unsupported operating systems, etc.). This analysis is based on information from the crowd-sourced Armis Device Knowledgebase and from premium, globally-shared threat intelligence feeds including the Check Point ThreatCloud.

When Armis identifies a vulnerable device, the Check Point IoT Security Manager activates security protections automatically, either through virtual patching (by installing the appropriate IPS signatures on the gateways) or through policy enforcement that isolates affected devices. This provides effective protection against unpatched devices, or devices running on unpatchable operating systems and software, all without disrupting critical processes and business operations.

Provide Security Teams Comprehensive Device Information

Security teams also can see the wealth of information Armis provides about each device directly in the Check Point IoT Security Manager console. With rich log records and dedicated IoT event reports, the Check Point Security Manager gives security teams a contextual understanding of device behavior and forensics for event investigation. That helps make security teams more well-informed when responding to threats without impacting critical devices, and without ever leaving the Check Point console.

ABOUT CHECK POINT

Check Point Software Technologies Ltd. (www.checkpoint.com) is a leading provider of cyber security solutions to governments and corporate enterprises globally. Its solutions protect customers from cyber-attacks with an industry leading catch rate of malware, ransomware and other types of attacks. Check Point offers a multilevel security architecture that defends enterprises' cloud, network and mobile device held information, plus the most comprehensive and intuitive one point of control security management system. Check Point protects over 100,000 organizations of all sizes.

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 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 smart TVs, webcams, printers, HVAC systems, industrial robots, medical devices and more. Armis discovers devices on and off the network, continuously analyzes endpoint behavior to identify risks and attacks, and protects critical information and systems by identifying suspicious or malicious devices and quarantining them. Armis is a privately held company headquartered in Palo Alto, California.

ARMIS
1.888.452.4011
armis.com