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, the Armis platform uses the existing infrastructure to discover and identify every device in any environment—enterprise, medical, industrial, and more. The platform 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 & IoT Device

As the Armis platform discovers devices in the environment, it provides Check Point with granular device attributes like the manufacturer, model, operating system, MAC address, and more. It also provides a risk analysis based on contextual understanding of a device’s behavior in your environment.
In the Check Point console, you can configure policies based on these attributes, and you can enable policy recommendations made by the Armis platform. 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.

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 avoid confusion or conflicts, Check Point 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 over two billion devices in the crowd-sourced Armis Device Knowledgebase and from premium, globally-shared threat intelligence feeds including the Check Point ThreatCloud.

When the Armis platform identifies a vulnerable device, it can trigger Check Point to activate 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 the Armis platform provides about each device directly in the Check Point console. With rich log records and dedicated IoT event reports, Armis and Check Point give 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.

For more information, visit armis.com/checkpoint.