Check Point IoT Security Solution

Cyber Security Built for IoT

MAIN BENEFITS:
- Instantly secure all your existing IoT devices and safely implement new ones.
- Cut down security man hours with auto-detection and remediation of threats.
- Keep critical processes undisturbed with adaptive policies and no need to physically patch devices.

MAIN CAPABILITIES:
- Risk Analysis: expose all your IoT related risks.
- Auto-segmentation: minimize your risk exposure with auto-generated policies.
- Threat Prevention: Blocks known and Zero-day attacks.

TAILORED FOR DIFFERENT IOT ENVIRONMENTS:

**Smart Building**
- Camera
- Thermostat
- Elevator

**Smart Office**
- Printer
- Light Bulb
- TV

**Operational Technology (OT)**
- Barometer
- HMI & PLC
- Sensor

**Healthcare**
- PACS server
- Infusion Pump
- MRI
The IoT Security Challenge

While connecting Internet-of-Things (IoT) devices to your corporate network delivers clear benefits, it also exposes you to new cyber-threats. From IP cameras, and smart elevators, to medical devices and industrial controllers, IoT devices are inherently vulnerable and easy to hack. Many of these devices run on unpatched software, are misconfigured, or use unsecured communication protocols. Furthermore, organizations own extensive and diverse device inventories of multiple vendors, models, and functionalities, with many shadow un-managed devices (connected to the network without anyone’s knowledge). And while IoT environments have become increasingly complex, IT security solutions have remained far behind, with limited visibility and control over IoT devices and their associated risks. This security gap increases the risk of a successful cyber-attack where critical devices can be shut down, damaged, manipulated, or used to infect other systems on the network. It is time to take action and keep every device secure.

Check Point IoT Security Solution

Check Point offers the industry's most comprehensive cyber-security solution for different IoT environments, including Smart Office, Smart Building, Industrial, and Healthcare.

The solution enables organizations to prevent IoT related attacks and minimize their IoT attack surface. All in a way that is easily scalable and non-disruptive to critical processes.

Main solution capabilities:

- **IoT Risk Analysis:** Expose All your IoT Related Risks.
- **Auto-Segmentation:** Minimize your Risk Exposure with Auto-generated IoT Policies.
- **Threat Prevention – Block Known and Unknown IoT Related Attacks.**

SOLUTION COMPONENTS:

- **CHECK POINT SECURITY MANAGEMENT**
- **CHECK POINT SECURITY GATEWAYS**
- **IoT DISCOVERY ENGINE**
- **IoT NANO AGENT**
How it Works:

1. IoT Risk Analysis: Expose All your IoT Related Risks

The solution continually performs a comprehensive risk analysis of your entire IoT environment to expose all the risks associated with your devices at any given moment. From a single console, you can view all your IoT devices classified based on their risk level, and even drill down for a risk analysis per device.

IoT Risk Analysis is based on three sources:

a. **IoT Discovery** - by integrating with third-party IoT discovery platforms, the solution auto-identifies all your devices, tags them based on their attributes (e.g., device type, manufacturer, model, firmware version, and MAC address), and analyzes their behavior in real-time to detect anomalies. Powered by the industry's largest ecosystem of IoT discovery, it is capable of identifying hundreds of thousands of IoT device profiles across the enterprise, industrial and healthcare IoT environment (see some of our IoT discovery partners in figure 1).

b. **Firmware Risk Assessment** - exposing inherent security flaws associated with the firmware of every connected device (and also with embedded third-party components) including:
   - Weak credentials: easily brute-forced, publicly available, or unchangeable credentials.
   - Known vulnerabilities: list of all CVEs classified based on their severity and attack vector (Network/physical attack).
   - Suspicious listed domains
   - Hardcoded security flaws, such as operating system misconfiguration.

c. **IoT-specific Threat Intelligence** – the solution identifies IoT threat trends and malicious patterns via Check Point’s *ThreatCloud*, which aggregates threat indicators (IoCs) from over 100 Million gateways, endpoints, and IoT devices worldwide.

![Figure 1: Drill down for a risk analysis per device](image-url)
2. Auto-Segmentation: Minimize your Risk Exposure with Auto-generated IoT Policies

Based on the IoT risk analysis, the solution automatically generates and enforces a policy for every device in your environment. This automated process saves you months of manual policy configurations and ensures your IoT devices are secure from the first moment they connect to your network.

These auto-generated policies instantly minimize your IoT attack surfaces by creating network segmentation, one that allows only authorized access to (and from) your IoT devices and ensures devices use only communication protocols they were designed to use.

Example policy use cases:
- Allow AC systems to communicate only with the building management system.
- Allow medical imaging devices to communicate only with PAC servers.
- Prevent badge readers from communicating with HR systems.

In the auto-generated policy example (in figure 1): rule 5.1 allows IP cameras to communicate with a BMS (Building Management System) controller using only the ONVIF protocol and rule 5.2 allows Hikvision cameras to communicate with a specific internet domain (for firmware update).

![Figure 2: Auto-generated Policy Example for IP Camera](image)

The policies are highly granular and adaptive to any change in devices’ attributes, behavior, and risk level so they can secure thousands of IoT device profiles without disrupting critical processes.

Every policy can be manually modified within the Check Point security management console, in a separate IoT policy management layer (so that you can avoid confusion and conflicts with the security policies of your entire network).
3. Threat Prevention – Block Known and Unknown IoT Related Attacks

Based on the IoT risk analysis, the solution automatically activates security protections against known and Zero-day IoT related attacks, both for network-based and device-level attacks.

a. **On-Device Runtime Protection**: monitors the behavior of the device at run-time and blocks known and unknown device-level attacks before the device is compromised. Examples of attacks are shell injection, memory corruption, and control flow hijacking.

b. **Protect unpatched devices from known exploits**: automatically activates security protections against known CVEs through virtual patching, by installing the appropriate IPS signatures on the gateways (over 300 available signatures for IoT related threats). That allows effective protection against unpatched devices or devices running on legacy operating systems and software; without disrupting critical processes and business operations.