Check Point Quantum IoT Embedded

You deserve the best security.
Secure your devices from within.

The need for security in the age of IOT

IoT Devices are shaping the new cyber landscape, from IP cameras and smart elevators, to routers, drones, medical devices, and industrial controllers. Any network-connected device is a potential vulnerability and is often targeted to disrupt services and operations.

Unprotected devices are exposed to malfunction, data and privacy breaches, device tampering and can be used to gain access to connected networks and launch attacks. The potential damage can affect both users and manufacturer; whether financial damage, reputation loss, or criminal liability in cases of device failure or user safety.

If you are in the business of building IoT devices, it is your obligation to give your customers the security they expect and deserve. Choosing the right solution will also allow you to present competitive advantages and meet developing regulations, allowing your focus to remain on business success.

Why do these vulnerabilities exist?

There are various reasons why vulnerabilities exist in today's IoT devices, including:

- Limited security expertise and knowledge among device makers can lead to a missing implementation of security best practices and a lack of "Secure by Design" methods
- Direct-to-Internet connections make devices easily accessible over the web, often without any security countermeasures in place and no control by device makers/operators over their deployment
- Usage of 3rd-party supply chain components may be classiffied as vulnerable
- Devices are often unmanaged and difficult to update for quick fixes

Protecting IoT Devices for Business Success

IoT devices can be attacked in multiple vectors (user interface, Ethernet, WiFi, Bluetooth, and others). To sustain attacks, you must implement innovative and proven security practices, like on-device embedded security software.

CHECK POINT QUANTUM IOT EMBEDDED

Quantum IoT Embedded is an end-to-end security solution for businesses building embedded consumer and IoT devices. From IP cameras and smart elevators, to routers, medical devices, and industrial controllers, our out-of-the-box solution protects IoT devices and the users against zero-day cyber-attacks – serving as the most powerful line of defense for your IoT devices.

Lightweight IoT Nano-Agent runs on firmware level with runtime pre-emptive protection, alongside with full management and Monitoring capabilities in Check Point Infinity Portal.

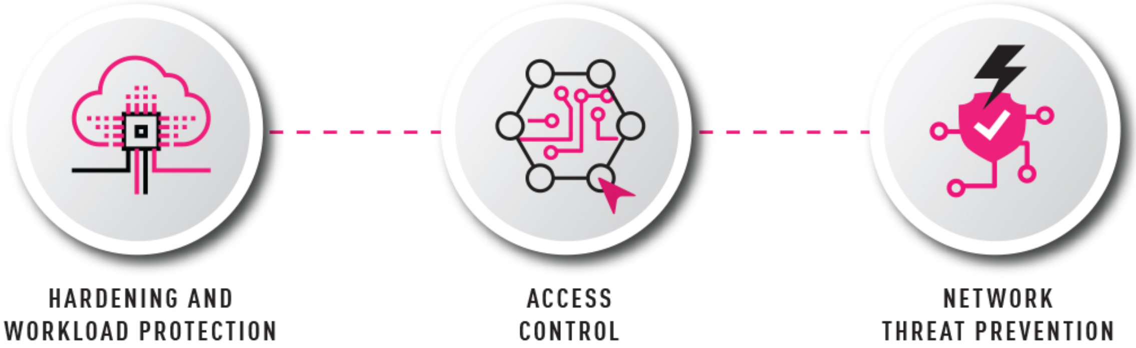
Thanks to cutting edge control flow integrity (CFI) technology, our Nano Agent® provides on-device runtime protection that checks whether a device is acting according to certain computing rules, blocking any deviations from expected behavior, such as unauthorized writes to certain parts of the firmware, or rogue processes that should not be spawned.

Multilayer Security Design for IoT Devices

Quantum IoT Protect Embedded empowers developers and manufacturers to secure smart devices through three layers of protection:

- **Hardening & Workload Protection ->** Through built-in standalone workload protection, firmware is evaluated and hardened to protect against any zero-day attack, known or unknown.
- **Access Control ->** Access control policies can be managed from cloud-based portals to validate incoming and outgoing traffic to the device. Our Nano-Agent® enforces the security policy with an enhanced AI Engine to ensure high reliability and zero false positives when controlling the traffic.
- **Network Threat Prevention ->** Within minutes, you can distribute virtual patches using signatures that block the attack vector, until you are able to develop, test, and release a full software update.

Quantum IoT Embedded Multilayer Protection



How does Quantum IoT Embedded work?

Our revolutionary Nano Agent® technology is installed on the IoT device/s, blocking any attack that may occur in the runtime process level. Through CFI technology, Nano Agent® allows you to fend off even the most sophisticated device attacks including shell injections, memory corruption, control flow hijacking, and even zero-day firmware vulnerabilities that have yet to be discovered. For example, these types of attacks are associated with some of the notorious exploits such as EternalBlue, Heartbleed, Shellshock, Bluebourne, Ghost, Venom, and ImageTragick.

With a lightweight, simple integration process we will create a frictionless agent to the embedded firmware. The agent has the ability to operate in an offline mode as a standalone solution or an online mode, which would be managed by the Check Point Infinity portal, or with an API from your own management portal.

Benefits

- On-device runtime protection blocks known and unknown (zero-day) cyberattacks.
- Cutting edge control flow integrity (CFI) technology and lightweight deployment
- 100% firmware coverage (including 3rd-party components)
- Lightweight, non-intrusive architecture means minimal impact on device performance
- Consolidated management, visibility, and logging with Check Point Infinity Portal or API
- Comply with the top standards and regulations for IoT security (NIST, CISA, UL, ETSI, and more)

Technical Specifications

- No need for source code – hardening of devices only requires the firmware binary image file.
- The lightweight nano-agent can be streamlined into your existing development pipelines before mass production and released to the market.
- Device-agnostic – Same solution for all devices.
- API – OpenAPI supports friendly DevOps methods.

Security Features

- Firewall and Access Control
- Privacy and User Data Protection
- IoT Runtime Threat Prevention:
    - Function Pointers Takeover Protection
    - Software Control-Flow Takeover
    - Dynamic-Memory Misuse Protection
    - Malicious Use of Shell Protection (Anti-Shell Injection)
- Network Threat Prevention
    - Virtual Patching
    - Anti-Bot

System Requirements

- CPU: ARM, x86, MIPS
- OS: Embedded Linux
- Storage: 1MB-30MB*
- Memory: 1MB-40MB*

**Size depends on firmware size and deployment type*

checkpoint.com/quantum/iot-protect/iot-device-security

Contact us

Worldwide Headquarters
5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com
U.S. Headquarters
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000
www.checkpoint.com