CHECK POINT
Embedded IoT Security
Powered by Quantum IoT Nano Agent

INSIGHTS

Cyber threats and attacks are major global issues. SMBs (Small-to-medium business), SMEs (Small-to-medium enterprise) and home users are attractive targets for hackers. On average, every week 54% of organizations suffer from attempted cyber attacks targeting IoT devices. Governments recognize this as a real threat and are creating new regulations for security vendors and operators.

In March 2023, Biden administration release the new National Cybersecurity Strategy for the United States. In this document they state clearly: “We must rebalance the responsibility to defend cyberspace by shifting the burden from individuals, small businesses onto organizations that are most capable and best positioned to reduce risks.”

A new Cybersecurity strategy has been introduced by the European Commission in Europe. Its objective is to establish a secure and unrestricted Internet worldwide, with robust safeguards in place to protect the fundamental rights of individuals in Europe. This strategy incorporates three tools, namely regulatory measures, investment initiatives, and policy directives, all of which will tackle three key areas of action within the EU:

1. Resilience, technological sovereignty and leadership
2. Operational capacity to prevent, deter and respond
3. Cooperation to advance a global and open cyberspace

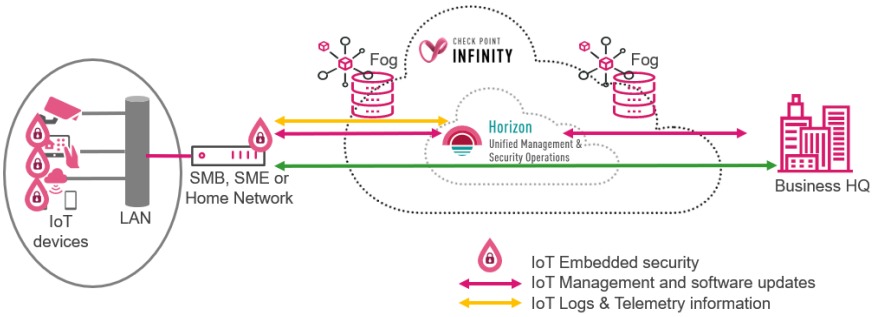
In both US and Europe, we see the same approach towards additional requirements on tech vendors and operators to ensure the cybersecurity of their infrastructures and their users.

IOT SECURITY LANDSCAP

As part of the increased awareness to cyber-attacks on IoT and connected devices, and to comply with new regulation, IoT vendors will have to maintain frequently their devices and to release security updates during the life time of the device. Operators will have to maintain the devices and to ensure that they get the recent updates on time and within a certain timeframe. What we call “patching” the devices. This is a huge overhead and in many cases not very effective and often too late.

A BETTER APPROACH TO SECURE IOT DEVICES

To help manufacturers and vendors to do more secure devices, Check Point introduced IoT Embedded Nano agent. The Nano agent is part of the device and protect in against cyber-attacks in real time. Users can leverage Check Point Horizon’s policy, a holistic dashboard shows the security maturity of your IoT device fleet in a single overview screen. Check Point Horizon is the first prevention-focused security operations platform with robust SOC operations.



CONCLUSION

The Nano Agent, a standalone solution, offers enterprise grade, zero-impact security. The IoT device is hardened with a reduced attack surface, minimizing the need for patches. This secure-by-design architecture ensures all sensitive data is secured as well as the privacy of the user. The Nano Agent uses the principles of zero trust, zero tolerance and provides an excellent security posture as part of a robust, easy to integrate, always on, hassle free and scalable security solution.

For more information, see Check Point’s Nano Agent Security Solution.