CHECK POINT + ALTAIR
THREAT PREVENTION FOR MOBILE IOT DEVICES

Benefits

- Inspect all communications to and from Altair LTE (Long-Term Evolution) chipsets on IoT devices with Check Point Capsule Cloud to prevent threats before they arrive into the device
- Offload security processing from IoT devices to Capsule Cloud
- Secure IoT devices with advanced threat prevention
- Increase visibility of threats targeting IoT devices

INSIGHTS

Security is key for the safe and reliable operation of IoT (Internet of Things) connected devices. Security concerns cover personal privacy, financial transactions, the threat of cyber theft, and safety. Network firewalls and protocols can manage the high-level traffic coursing through the Internet. IoT devices that usually have a very specific, defined mission with limited resources also have to be protected.

Applying common internet security practices in the IoT world requires substantial reengineering to address device constraints. Blacklisting, for example, requires too much disk space to be practical for IoT applications. Embedded devices are designed for low power consumption, with a small silicon form factor, and often have limited connectivity. They typically have only as much processing capacity and memory as needed for their tasks.

The endless variety of IoT applications poses an equally wide variety of security challenges. For example: tracking a device's location, turning on the camera and microphone, and extracting application data information. A smart meter - one which is able to send energy usage data to the utility operator for dynamic billing or real-time power grid optimization - must be able to protect that information from unauthorized usage or disclosure. Information that power usage has dropped could indicate that a home is empty, making it an ideal target for a burglary or worse.

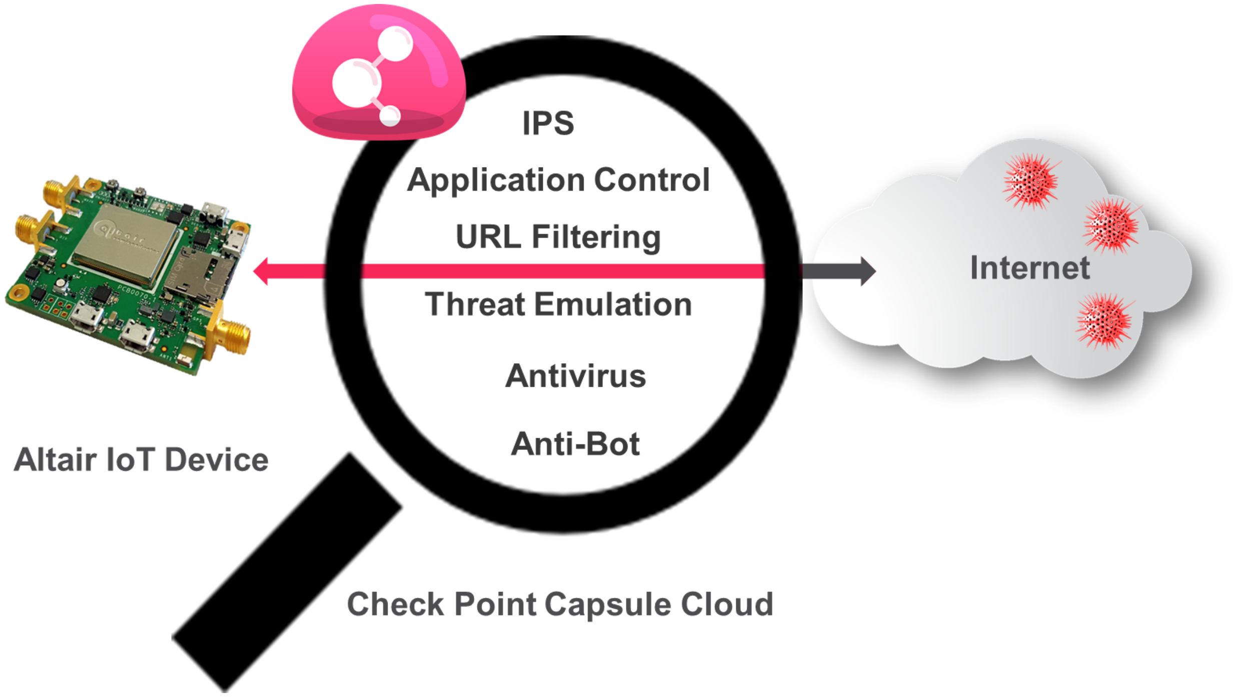
SECURE IOT DEVICE CONNECTIVITY

Altair Semiconductor chipsets are the main building blocks of cellular-connected IoT devices, and include an LTE modem, an MCU (Microcontroller Unit) running the device (user) application, and various sensors, including GNSS (global navigation satellite systems).

A BETTER APPROACH TO SECURING IoT DEVICES

Connecting Altair Semiconductor LTE chipsets to the IoT cloud through Check Point Capsule Cloud provides comprehensive IoT device security against new and growing threats to these mobile IoT devices. Capsule Cloud protects device content and information with advanced threat prevention and adaptive risk mitigation, and provides visibility and intelligence into the threats targeting IoT devices.

Altair connected IoT devices route all the traffic to the internet via Capsule Cloud. All communication from and to the device is inspected with Check Point Next Generation Threat Prevention, preventing threats before they arrive into the device. Using this technique we are also able to offload deep packet inspection processing needed to detect threats from IoT devices which have limited compute and storage resources to the cloud where processing power can be scaled as needed.



Altair connected IoT device protected with Capsule Cloud

ABOUT CHECK POINT

Check Point Software Technologies Ltd. (www.checkpoint.com), is the largest network cyber security vendor globally, providing industry-leading solutions and protecting customers from cyberattacks with an unmatched catch rate of malware and other types of threats. Check Point offers a complete security architecture defending enterprises – from networks to mobile devices – in addition to the most comprehensive and intuitive security management. Check Point protects over 100,000 organizations of all sizes.

ABOUT ALTAIR SEMICONDUCTOR

Altair Semiconductor, a Sony Group company, is a leading provider of LTE Internet of Things (IoT) chipsets. Altair has shipped millions of chipsets to date, commercially deployed in LTE networks globally. Altair's portfolio addresses the complete spectrum of market needs, from ultra-low-power low-cost IoT and M2M devices to super-high-throughput broadband access chipsets. These chipsets serve as the communications engine for connected "things," including wearables, automotive and transportation, smart homes, smart cities, manufacturing systems, retail, healthcare and pharma, energy and utilities.