Enterprise-level security for your Home Gateway

The gatekeeper of your network deserves the strongest security. When your Home Gateways embed cyber security protection as part of the core software, cyber threats don't stand a chance.

Why Home Gateways need security?

Home Gateways are critical gateways to the internet, making them prime targets for cyberattacks. Unsecured Home Gateways can be exploited for unauthorised access, allowing attackers to manipulate traffic, steal sensitive information, and use the device for malicious activities like botnets. Ensuring robust security measures in your home protects your privacy and safety of your home network.

Comply with international regulations like the Cyber Resilience Act (CRA), Radio Equipment Directive (RED), Network and Information Security Directive (NIS2), and Product Security and Telecommunications Infrastructure Act (PSTI). These regulations ensure devices have essential security features, reduce vulnerabilities, and prevent unauthorized access. Adhering to industry best practices and incorporating regulatory recommendations is crucial for maintaining compliance, enhancing network security, and safeguarding personal data from exploitation and misuse.

SECURITY BENEFITS

- Seamless, hassle-free, out-of-the-box soluitioin, no additional deployment required
- Comply with mandatory regulations, industry best practices and recommendations
- Reduce TCO and maintenance cost. Harden the device to mitigate potential future threats

SECURITY FEATURES

- **Security that doesn't impact device operations:** Runtime protection, that blocks even zero-day threats with no impact on device performance
- **Fend off the most sophisticated IoT device attacks:** including shell injections, memory corruption, and control flow hijacking
- **Prevent malware campaigns:** including ransomware, bot infections (Mirai), crypto mining and lateral movement as part of a larger more sophisticated nation-state attacks

A Secure First Line of Defense

Check Point and Heights Telecom are partnering to provide the industry's most secure Home Gateway solution. Heights Telecom specialises in leading-edge telecommunication solution. Heights Telecom is known for delivering innovative communication solutions to private and businesses consumers, with focus on high-speed internet, voice services and advanced networking technologies.

Home Gateways not only encompass Residential Gateways, Multimedia Gateways, Smart Home Gateways and other such points of network convergence as they are crucial in modern homes. They act as the connective tissue between personal devices and the wider internet, facilitating communication, entertainment, home automation and management of digital content.

Heights Telecom aims to enhance connectivity and streamline communication for its customers. The company prides itself on exceptional customer service and reliability, ensuring that customers have access to the latest innovations in telecommunications. As the demand for seamless connectivity grows, Heights Telecom continues to expand its offerings and technology to meet the evolving needs of the digital age.

Check Point Quantum IoT Protect Nano Agent solution provides a complete end-to-end solution for all security needs of device's manufacturers. From uncovering firmware security risks, to hardening their device with runtime protection, to managing their devices with granular policies. Heights Telecom gain the visibility, security and controls they need to offer customers highly secure connected products.

With embedded security in telecommuncation devices, Heights Telecom Cyber Security Service stands apart from other companies that are offering similar solutions. This build user trust and confidence in an ever evolving and dangerous cyber physical world.

The Safe Connection

Compliance with cybersecurity regulations in the telecommunications industry is a crucial step in protecting users and maintaining the integrity of communications networks. It ensure that the inrastructures of nations and countries remain clean and safe.

Non-compliance can lead to significant fines, loss of reputation, and erosion of customer trust, which can be far more costly than meeting regulatory requirements.

Regulations

- **EECC** (European Electronic communications Code)
- **Security Measures for OES** (Operators of Essential Services)
- EU toolbox for **5G security RCE Directive** (Resilience of Critical Entities)
- **ePrivacy Directive**
- **CSA** (Cybersecurity Act)
- **Data protection and privacy laws** (i.e., GDPR – General Data Protection Regulation and CCPA - California Consumer Privacy Act)
- **TSA** (Telecommunications Security Act)
- **DPA** (Data Protection Act)
- **UK GDPR** (General Data Protection Regulation)
- **RED** (Radio Equipment Directive)
- **NIS2** (Network and Information Security)
- **CAF** (Cyber Assessment Framework)

Avoiding reputational damage is crucial for ISPs and Telcos to maintain their credibility and public perception. Offering ease of operation by eliminating the need for emergency software updates. With one optional dashboard for in depth fleet management.

Compliance fosters innovation by setting a level playing field where new entrants can compete with established players, ultimately benefiting consumers with better services and prices.

Check Point IoT Protect Nano Agent solution

Revolutionary Check Point IoT Protect™ with Nano Agent® provides telecom devices, such as a routers and gatweays with runtime protection, enabling connected devices with built-in firmware security. Based on cutting edge control flow integrity (CFI) technology, the lightweight Check Point IoT Protect™ with Nano Agent® allows you to fend off 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. These attacks are associated with some notorious exploits such as EternalBlue, Heartbleed, Shellshock, Bluebourne, Ghost, Venom, and ImageTragick.

Summary

Check Point IoT Protect™ with Nano Agent® provides a dedicated security solution to harden the Home Gateway / CPE (Customer Premises Equipment) device with on-device runtime protection, preventing zero-day attacks. Once deployed on the Home Gateways, it monitors the inputs, outputs and state of the Home Gateway. It searches for both known attacks and anomalies that may indicate an attempt to exploit a zero-day vulnerability. If such an attack is detected, the Nano Agent can either block the attack entirely or alert the Home Gateway's security team.

The Nano Agent is easy to integrate using APIs into the CSP (Communications Service Provider) "clean pipe" system. A clean pipe system serves as a digital filtration process, scrutinizing incoming traffic to an ISP's (Internet Service Provider) or CSP's (Communication Service Provider's) network, aiming to remove malware, DDoS attacks, and other cyber threats before they can penetrate and propagate within the network.

The necessity for robust security measures in CSP clean pipe systems cannot be overstated. As the volume and sophistication of cyber threats escalate, these protections are pivotal in maintaining the integrity and reliability of communication networks. Without them, CSPs would be vulnerable to disruptions that could lead to loss of service, breach of sensitive data and severe financial and reputational damage. Therefore, the implementation of strong security controls within clean pipe systems is fundamental to safeguarding the digital ecosystem of users and maintaining uninterrupted and secure network services.

By offering proactive security the Communication Service Provider is making sure the Home Gateway is resilient to cyberattacks. The Nano Agent solution is very cost effective, eliminates expensive patch problems, incident resolving, service desk time and reputation damage.

About Check Point

Check Point Software Technologies Ltd. (www.checkpoint.com) is a leading provider of cyber security solutions to governments and corporate enterprises globally. Its solutions protect customers from cyber-attacks with an industry leading catch rate of malware, ransomware and other types of attacks. Check Point offers a multilevel security architecture that defends enterprises' cloud, network and mobile device held information, plus the most comprehensive and intuitive one point of control security management system. Check Point protects over 100,000 organizations of all sizes.

About Heights Telecom

Heights Telecom was founded in 2006. The company provides a range of telecommunications services, including high-speed internet Gateways, voice solutions, and managed IT services. Heights Telecom primarily serves residential customers and Business / SoHo organozatiosn seeking reliable, efficient and innovative communication solutions. The company focuses on delivering tailored solutions that meet the unique needs of each customer, ensuring a high level of service and support. Heights Telecom aims to enhance connectivity and streamline communication for its diverse clients, helping them thrive in an increasingly digital world.

Worldwide Headquarters
5 Shlomo Kaplan Street, Tel Aviv 6789159, Israel | Tel: +972-3-753-4599

U.S. Headquarters
100 Oracle Parkway, Suite 800, Redwood City, CA 94065 | Tel: 1-800-429-4391

www.checkpoint.com