Quantum IoT Embedded Nano Agent

Fortifying CPE Security

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)

THE CPE SECURITY BENEFIT FRAMEWORK

In an increasingly connected world, the security of Customer Premises Equipment (CPE), such as routers and modems, is not purely a technical concern but a comprehensive value proposition benefiting manufacturers, partners and end-users. CPE security is critical for safeguarding data, ensuring privacy and facilitating reliable connectivity. Let's discuss this multifaceted value-add that CPE security offers to each stakeholder.

UNLOCKING THE TRIO OF TRUST

I. Added value for manufacturers |

Brand integrity and trust: A manufacturer that embeds proactive security controls into their CPE devices is one that signals responsibility and reliability. Users are more likely to trust and remain loyal to brands that prioritize their security and safety.

Competitive advantage: In markets congested with generic equipment, those offering enhanced security controls can distinguish themselves. This differentiation often translates into a competitive advantage.

Reduction in support and management costs: Secure devices mean fewer vulnerabilities and fewer instances of customer complaints or software/firmware updates, leading to a significant reduction in support and costs.

Regulatory compliance: Manufacturers that proactively address security are better positioned to meet evolving regulatory (mandatory) requirements, avoiding potential penalties, legal fees and interruptions in the product process.

For manufacturers, embedding proactive security controls within the CPE not only safeguards their brand reputation but also fosters trust among consumers. By prioritizing security in product design and development, manufacturers can differentiate their offerings in a crowded marketplace and establish themselves as leaders in the field. Investing in CPE security enhances customer loyalty and satisfaction, as partners and users seek reliable, secure solutions to safeguard devices, data and privacy. Dedicated security improves overall equipment effectiveness [1].

$$A \; x \; P \; x \; Q \; = \; O$$

$$Availability \; x \; Performance \; x \; Quality \; =$$

$$Overall \; Equipment \; Effectivenesss$$

Figure 1: Formula overall equipment effectiveness

II. Added value for partners |

Enhanced product portfolio: Partners and resellers offering secure CPE solutions can present a broader, more compelling product portfolio to potential clients, enhancing their market position.

Customer confidence: By providing secure devices, partners cultivate trust and deepen customer relations, ensuring ongoing business opportunities and client retention.

Lower risk of liability: Distribution of secure CPE devices minimizes the risk of distributing compromised devices that could expose partners to legal liabilities or damage to their reputation.

Upselling opportunities: Security is a growing concern. Partners can upsell additional security services, i.e., monitoring increasing overall sales volume.

Partners within the telecommunications ecosystem can also significantly benefit from enhanced CPE security. It serves as bridge between manufacturers and end-users. Partners play a crucial role in delivering and managing CPE solutions. By aligning with manufacturers that prioritize security, partners can mitigate the risk of security breaches and data compromises. In addition, offering secure CPE solutions enables partners to capitalize on emerging opportunities in the cybersecurity market, driving revenue growth and profitability. Partners will enjoy the benefits from the joint profits [2] by incorporating dedicated CPE security.

$$Joint\ Profits\ =$$
$$(Total\ Revenue\ -\ Total\ Expenses)\ x\ Profit\ Sharing\ Ratio$$

Figure 2: Formula partner profits

III. Added value for the (end) user |

Protection of sensitive data: For the user, CPE security is the frontline defense in protecting their devices and data. Preventing attacks and cyber threats, directly be impacting their personal and professional activities.

Network reliability: Secure CPE ensures that users have a reliable network connection, free from disruptions that might be caused by security breaches or malware infections.

Peace of mind: Knowing that their CPE is secure allows users to interact with digital services confidently, whether for work, communication or entertainment.

Futureproofing: Users with secure CPE can be assured that they are prepared for future security challenges and will not need to invest in new equipment prematurely.

To protect networks and to sustain attacks, a proactive security solution must be implemented. This will block attacks on multiple factors like the user interface (UI), Wi-Fi and Bluetooth. With cyber threats becoming increasingly sophisticated and prevalent, users becoming more insightful when selecting CPE solutions. By choosing products that prioritize security, users can mitigate the risk of data breaches, identity theft and other cyber attacks. This ensures the security and confidentiality of their personal, sensitive information. Furthermore, secure CPE solutions offer users greater control over their network environment, empowering them to customize security settings following enterprise best practices. All this will improve the customer perceived value (CPV). [3]

$$CPV = PCB - TCC$$
$$Customer\ Perceived\ Value = Perceived\ Customer\ Benefit - Total\ Customer\ Cost$$

Figure 3: Formula customer perceived value

ENHANCING CPE RESILIENCE – THE NANO AGENT

The Nano Agent is dedicated security solution to harden the CPE device with on-device runtime protection, preventing zero-day attacks. Once deployed on the CPE, it monitors the inputs, outputs and state of the CPE. 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 CPE's security team. The Nano Agent is easy to integrate using APIs into the CSP (Communications Service Provider) "clean pipe" system. By offering proactive security the CSP is making sure the CPE is resilient to cyberattacks.

With the adaptation of secure by design principles at manufacturing phase, sensitive data (data in use and data in transit) as it is the privacy of the end-user secured. The Nano Agent solution is very cost effective, eliminates expensive patch problems, incident resolving, service desk time and more!

Plus, the Nano Agent enhances various key business metrics. It reduces the Churn Rate by keep customers happy and satisfied, they are less likely to switch to other partners and services. Churn Rate refers to the percentage of customers who stop using a product or service. An acceptable [4] Churn Rate is between 2% to 8%. The lower the Churn Rate the better. A low Churn Rate increases the Average Revenue per User (ARPU) as it provides VAS upsell and cross sell opportunities. The Nano Agent is offering a robust security posture, ensuring comprehensive protection throughout the complete network, with a reduced attack surface. This solution facilitates the expansion of CSP offerings, with compelling revenue streams with the option to enable CPE Value-Added Services (VAS).

Value-Added Services (VAS) are crucial for enhanced functionality and user experience of CPE devices.
VAS for CPE devices could be |

- Remote monitoring: real time tracking of CPE devices, device details and health checks.
- Maintenance alerts: timely notifications for device maintenance, reducing downtime and improved efficiency.
- Custom Alert profiles: tailored and personalized alerts for specific events.

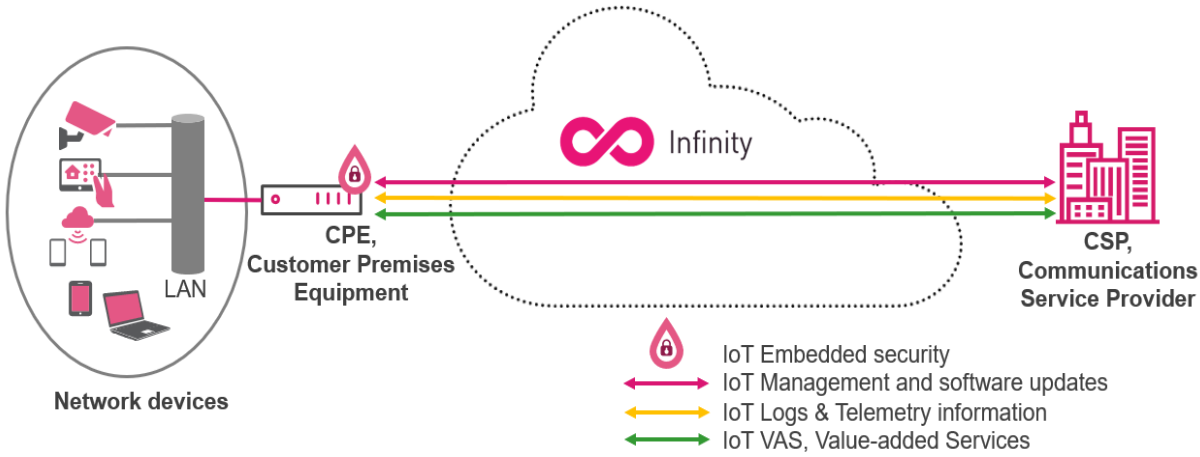

Figure 4: Nano Agent CPE deployment

WIN – WIN

In summary, enhancing CPE security is essential for the entire CSP and CPE ecosystem, extending beyond individual stakeholders. Prioritizing security in CPE design enables manufacturers, partners, and end-users to collectively mitigate cyber threats, fostering trust and resilience in the digital landscape. Integration of the Nano agent into CPEs enhances service models and offers manufacturers a competitive edge. Read more about the Nano Agent security controls with the best **ROI** (Return on Investment) and a low **TCO** (Total Cost of Ownership).

[1] https://www.oee.com/
[2] https://www.quora.com/What-is-the-formula-for-calculating-joint-profits-for-partners
[3] https://online.keele.ac.uk/what-is-customer-perceived-value/
[4] https://www.forbes.com/advisor/business/churn-rate/#:~:text=The%20ideal%20churn%20rate%20for,to%20five%20customers%20per%20month.

Author: Antoinette Hodes