



Quantum IoT Protect

```
1000:6522001A120  
746049: C617074 64654561 6520786C  
042806: 22 64 72205 FF 021064207669418  
7207278 637472706 28076 74286769  
F2049001176 655 86 628174596 873  
682E 05768056 0796F70207 04F7 65207  
28069 007007 5207261646 7465642  
1 61694828 927473886 7263 0000 372 7  
571E20457 07 16C4C7920 742073746  
74602 68 61746946A7286974207460 3786  
0079636C0 20746809 746697 02  
61746946 859740027064669 9456474607  
307070460072 7070726 06 061746  
07280004 0626 6368206 07 2072616  
86174609730706976 07320616273672  
6460C732080 286974 076 073 6974206  
06 172 06 61 682E2041 2869742081  
72616469417 02 3207468632 572677920  
E2 0000 207068 02 0707 2466 0000 06005  
7220646620 0616348424 96 32E705  
56A072470206 06 206070737 626 077 5  
69701 0747020 76 060 05200617469  
07 660070706 06F6204696 4702 9603  
63648646 63604 06C61607 20616E  
F7073207 06063747270 02 70726 06 5636064  
6166 0200361606 6265207 06 F77620 10206
```

YOU DESERVE THE BEST SECURITY

SOLUTION BRIEF QUANTUM IOT PROTECT

AN EVER-EXPANDING ATTACK SURFACE

Integrated into every aspect of our lives, internet of things (IoT) devices and operational technology (OT) assets automate and streamline operations. Yet every time a smart device is added to our network, it expands the attack surface. This is because connected devices are inherently vulnerable and easy to hack. This explains why 67% of enterprises have already experienced an IoT-related security incident, carried out to infiltrate enterprise networks or for the purpose of device manipulation or destruction.

EASY TO HACK, BUT DIFFICULT TO PATCH

And while IoT environments have become increasingly complex, IT security solutions have remained far behind, with limited visibility and control over IoT devices and their associated risks.

When it comes to securing these devices, the challenge lies in the huge variety of communication protocols they deploy, as well as the fact that they are inherently vulnerable due to several reasons:

- Run on legacy OSs
- Hardcoded or weak passwords
- Difficult to patch
- Physically accessible
- OS misconfigurations
- No built-in security
- Unsecured communication protocols

QUANTUM IOT PROTECT

Encompassing network- and device-level IoT security, Quantum IoT Protect prevents IoT cyber attacks, adapting protections to any IoT or OT device across smart-office, smart-building, healthcare and industrial environments. Delivering zero-trust profiles tailored per device, the solution uses real time threat intelligence, 60 innovative security services, and on-device runtime protection to deliver a complete, end-to-end prevention-first strategy for an evolving cyberphysical attack surface.

SMART BUILDING



SMART ELEVATOR

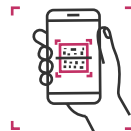


THERMOSTAT



HVAC

SMART OFFICE



BADGE READER



CAMERA



ROUTER

INDUSTRIAL



RTU



HMI



SENSOR

HEALTHCARE



X-RAY



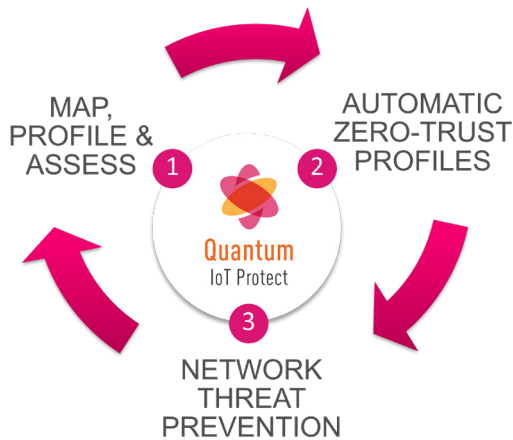
ULTRASOUND



MRI

AUTONOMOUS ZERO-TRUST THREAT PREVENTION

Check Point Quantum IoT Protect is now integrated directly into the Quantum Security Gateways with R81.20, providing customers with autonomous threat prevention for both network and on-device protection. Quantum IoT Protect enables organizations with:



WHY CHECK POINT FOR IOT SECURITY

Quantum IoT Protect is the leading IoT security solution needed to prevent cyber attacks:

- Automates everything from discovery to threat prevention
- Multi-layered cyber defense solution to protect IoT devices
- Best threat prevention against the latest and most evasive IoT cyber attacks
- IT and IoT consolidated into unified Infinity cybersecurity architecture
- Choice of SMB/branch, enterprise-scale and ruggedized security gateways

BENEFITS

- **Instantaneously map, profile, and assess risk** for any connected IoT device
- **Minimize the attack surface** with full IoT visibility and block zero-day attacks with zero-trust profiles
- **Prevent malicious IoT traffic** with 1000s of protections, over 60 security services, and real-time threat intelligence
- **Block access to and from infected devices** with proven security gateways
- **Harden IoT device firmware** to prevent zero-day runtime attacks



TIGHT INTEGRATION WITH LEADING IOT DISCOVERY PLATFORMS

By integrating with a wide range of third-party IoT and OT (Operational Technology) discovery platforms, our solution supports a vast array of device profiles across different IoT and OT environments, including medical devices.

Strategic and other leading technology partners seamlessly integrate with Check Point using the Quantum IoT Protect API, providing users with the ability to conveniently view and secure their IoT and OT devices from a single platform.

INNOVATIVE PARTNERSHIPS WITH INDUSTRY-LEADING DEVICE VENDORS

From IP Cameras and smart elevators, to routers, medical devices and industrial controllers, Check Point provides on-device runtime protection against zero-day cyber-attacks - serving as the most powerful line of defense for device manufacturers, enabling them to produce "Secure by Design" devices.

AVAILABLE ON



PART OF CHECK POINT INFINITY

Check Point IoT Protect is part of [Check Point Infinity](#), the only fully consolidated cyber security architecture that protects your business and IT infrastructure against Gen VI multi-vector 'Nano' cyber-attacks across networks, IoT devices, endpoint, cloud and mobile. Check Point Infinity delivers unprecedented protection against current and potential attacks—today and in the future.

CONTACT US FOR A DEMO TODAY

Don't leave your IoT security to chance. Get the visibility you need and the security you deserve. [Contact us for a demo today](#), or [get in touch to discuss](#) your IoT security needs.

Worldwide Headquarters

5 Ha'Soleim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100

U.S. Headquarters

959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000

www.checkpoint.com