CHECK POINT IOT PROTECT FOR HEALTHCARE

SECURE HEALTHCARE RECORDS, ENSURE PATIENT SAFETY AND HOSPITAL OPERATIONS

HEALTHCARE IOT IS DIFFERENT

When it comes to securing internet of things (IoT) devices against cyber attacks, hospitals contend with unique challenges, owing to several unique characteristics:

- **Life-supporting devices**

  There are 10 to 15 medical devices per bed[1], such as infusion pumps and respirators, but many of these devices were designed with little to no security in mind.

- **Legacy operating systems (OSs)**

  Almost half of connected medical devices run on unsupported OSs that no longer receive security updates[2]. These include ultrasound machines, MRIs and more, and makes them low hanging fruit for cyber attacks, such as ransomware.

- **Lucrative health records**

  Compromised electronic protected health information (ePHI) records are sold in the underground for hundreds of dollars per record, making them an attractive target. Hospitals spend an average of $430 per record to mitigate each stolen medical identity[3].

- **Compliance and certifications**

  Even when hospital wish to upgrade the OSs underlying their medical devices, this proves difficult, due to operational considerations and the need to have devices retested and recertified for use.

- **Multiple IoT device types**

  Not only are their medical devices vulnerable to compromise, but smart office and building management systems (BMS) assets are prime targets, too, whether as a segue into the hospital network or as a target for manipulation and takeover.

[1] Source - HIPAA Journal, Irdeto
[2] Source - HealthIT security, CyberMDX
[3] Source - IBM Cost of a Data Breach Study

EASY TO HACK, HARD TO PATCH

By default, medical and healthcare prevents IoT are unattended, unmanaged and feature poor out-of-box security. This leaves them exposed for two major reasons:

- **First, these devices can be easily accessed** physically, from within the network, as well as remotely.
- **Second, they are inherently vulnerable** due to:
  - Weak passwords
  - No built-in security
  - Unpatchable architecture
  - Outdated and legacy firmware or software
  - Unmanaged operations

Since you can only protect what you can see, IoT security solutions have emerged to offer visibility and security for connected devices.

MEDICAL DEVICES


PATIENT BED


PATIENT MONITOR


CLINICAL STATION


X-RAY


ULTRASOUND


MRI

SMART OFFICE


BADGE READER


CAMERA

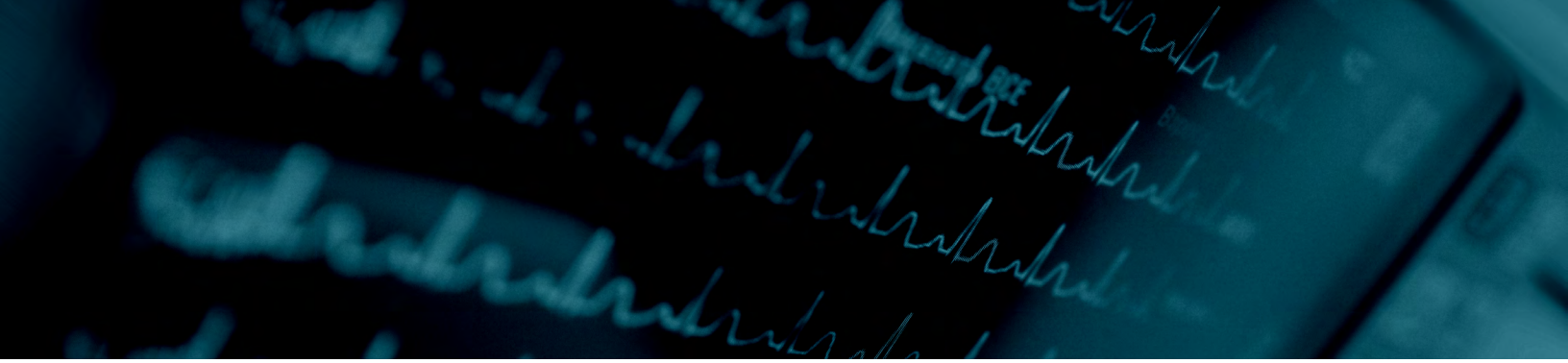

ROUTER

SMART BUILDING


SMART ELEVATOR


THERMOSTAT


HVAC



CHECK POINT IOT PROTECT FOR HEALTHCARE

Leveraging best-of-breed discovery engines, **Check Point IoT Protect for Healthcare** delivers the most powerful security for hospital environments, including medical, smart office and smart building devices, through deep IoT visibility and risk analysis, Zero Trust segmentation and proven multi-layered threat prevention.

CORE CAPABILITIES

Check Point IoT Protect for Healthcare offers:

- **Deep IoT device visibility and risk analysis**
  - Identify, classify and analyse every IoT device inside the network
  - Get granular fingerprints on each device, including brand, model, type, IP, MAC address and more
  - Expose risk indicators such as weak passwords, outdated firmware and known IT/IoT vulnerabilities (CVEs)
- **Intuitive Zero Trust segmentation**
  - Apply granular security rules based on device attributes, risks and IoT protocols
  - Easily create security rules based on dynamic grouping of devices
  - Gain single-pane policy management for IT and IoT, with a distinct IoT policy layer
- **Mitigation of known vulnerabilities, prevention of threats and zero-day malware**
  - Virtually patch devices running unpatched firmware and legacy operating systems
  - Identify and block unauthorized access to and from IoT devices and servers
  - Prevent the newest IoT-targeted malware attacks with real-time threat intelligence from ThreatCloud

WHY CHECK POINT FOR IOT SECURITY

Encompassing network and device-level IoT security solutions, **IoT Protect** prevents IoT cyber attacks, adapting protections to any IoT or OT device across smart-office, smart-building, medical and industrial environments, offering the:

- Broadest range of cyber security solutions to protect IoT devices
- Best threat prevention against the latest and most evasive IoT cyber attacks
- IT and IoT consolidated into unified Infinity cyber security architecture
- Choice of SMB/branch, enterprise-scale and ruggedized security gateways

BENEFITS

- **Minimize your IoT attack surface** with full IoT device visibility and granular policies
- **Prevent malicious IoT traffic** with over 60 security services and dynamic threat intelligence from ThreatCloud
- **Block access to and from infected devices** with proven security gateways

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—today and in the future.

CONTACT US FOR A DEMO TODAY

Don't leave your hospital IoT and network security to chance. Prevent the next cyber attack with the visibility and security you deserve. Contact us for a demo today, or get in touch to discuss your enterprise IoT security needs.