BUYER'S GUIDE TO

IoMT SECURITY SOLUTIONS

Sponsored by Cyber Talk

TABLE OF CONTENTS

TABLE OF CONTENTS

Overview: The State of IoMT Security

More than 500,000 medical technologies are available in the market space, and hospitals in the US cumulatively operate as many as 15 million IoMT devices.[1,2] At present, roughly 10 billion IoMT devices permeate the global healthcare delivery environment.[3] More than 50 additional devices are connected each second and by 2028, a total of 50 billion devices are expected to touch networks.[4] But many of these devices really aren't secure. So, what can we do?

Advances in wireless technologies and software-based sensors have enabled healthcare organizations to transform their models of care. New medical devices enable real-time, automated patient diagnosis, treatment and monitoring. IoMT represents a critical enabler and can alleviate numerous challenges facing health care.

However, the pandemic has illuminated the complications within the concept of connected infrastructure. Newly introduced CT scanners, telemetry units, emergency quarantine units, smart beds, airflow devices, remote work, telehealth and more have magnified the scope of the threat.

During a professional survey of a hospital, a cyber security team discovered 17,000 networked medical devices that were missing a security patch. As a result, the hospital remained at eminent risk of a cyber attack. How can organizations stay ahead of these types of risks?

---

[1] "How the Internet of Medical Things is Impacting Healthcare" by Andrew Steger, Health Tech Magazine, Jan 16, 2020
https://healthtechmagazine.net/article/2020/01/how-internet-medical-things-impacting-healthcare-perfcon

[2] "82% of healthcare organizations have experienced an IoT-focused cyberattack, survey finds" by Heather Landi, Fierce Healthcare, Aug 29, 2019
https://www.fiercehealthcare.com/tech/82-healthcare-organizations-have-experienced-iot-focused-cyber-attack-survey-finds

[3] "COVID-19: What Healthcare IoT Cyber Security Learned from the First Wave" by Leon Lerman, IoT Now, Jul 6, 2020
https://www.iot-now.com/2020/07/06/103739-covid-19-what-healthcare-iot-cyber-security-learned-from-the-first-wave/

[4] Ibid.

Ahead of solving an issue, one must first fully grasp the nature of the issue and its implications. Get a brief overview of device risk levels and factors that inform risk, right here:

IoMT SECURITY THREATS, CLASS I, II OR III

Regulatory agencies have categorized IoMT devices based on the level of risk inherent in their use. Class III or active devices, which include implanted units, present outstanding risk. Healthcare delivery groups and their service providers should ensure that, when exploring security issues, the tracking, monitoring and security of these devices is prioritized. Class II devices, if disrupted, also present substantial risk and represent an area of concern for decision-makers. Class I devices are non-invasive and present minimal risk.

IoMT devices generally present risks for specific reasons. These include lack of IT admin visibility into networks, poor abilities to stand up to patching, use of legacy technologies, unknown or unaddressed vulnerabilities, ownership issues and more. In the next section, we'll explore these risks and what they might mean for your organization.

REGULATORY AGENCIES HAVE DEFINED THE FOLLOWING RISK CATEGORIES

A) Class I or non-invasive devices. Products in this risk category are rated as low to moderate risk. Examples include lab equipment analyzers and non-medicated sterile dressings.[5]

B) Class II or invasive devices. Products in this risk category are rated as moderate to high risk. Examples include ventilators and infusion pumps.[6]

C) Class III or active devices. Products in this category typically provide life-supporting functionalities. Example: Implanted devices; pacemakers, cerebral stimulators.[7]

[5] Risk Classification of Medical Devices - Medsafe
https://www.medsafe.govt.nz/regulatory/devicesnew/3-7RiskClassification.asp

[6] Infusion Pumps, FDA.gov
https://www.fda.gov/medical-devices/general-hospital-devices-and-supplies/infusion-pumps

[7] "The Internet of Medical Things—Anticipating the Risk", by Mohammed Khan, ISACA Journal, 1 Jul 2019
https://www.isaca.org/resources/isaca-journal/issues/2019/volume-4/the-internet-of-medical-things-anticipating-the-risk

Top IoMT Security Risks

IoMT devices represent likely targets for exploit due to the fact that the industry has not yet matured within the cyber security space. A series of issues abound, and include:

VISIBILITY

In contrast with other critical healthcare IT infrastructure, connected medical devices often remain untraceable via the healthcare group's security information and event management systems (SIEMs) or in medical inventory management systems.

Without comprehensive visibility, it's not possible to understand how many vulnerabilities might exist on a given system, much less how to go about patching them. How can you ensure complete protection if you cannot see 100% of your environment?

> Research indicates that an average of 30% of IoMT[8] devices are lost or unexpectedly removed from the network. This exacerbates the security challenge.

[8] "How to Mitigate COVID-19's Impact on Device Security and Patient Safety", by Jessica Davis, Health IT Security, Feb 26, 2021 https://healthitsecurity.com/features/how-to-mitigate-covid-19s-impact-on-device-security-and-patient-safety?__cf_chl_managed_tk__=pmd_34c43bf1b35d021cbb36138deaaedf17d8603895-1627674084-0-gqNtZGzNA02jcnBszQZ6

DIFFERENT MANUFACTURERS

Healthcare delivery groups do not rely on a single IoMT manufacturer or even a small network of manufacturers. Rather, there are a mix of devices on the market, from a wide variety of medtech producers. Manufacturers retain their own device-to-device communication protocols, each with unique security implications. In the event that IT professionals fail to fully understand and properly configure communication protocols, security gaps and vulnerabilities can manifest.

Worse, interoperability between devices is commonly achieved through improvised work-arounds. IT admins initiating interoperability projects frequently lack any expertise in security. As a result, vulnerabilities may be introduced by accident.

UNPATCHED DEVICES

Are attempts to patch hospital systems' IoMT devices doomed from the start? Hospitals continuously require access to all systems, especially on account of emergency patient reception. As a result, planning for down time is difficult. And, of course, unplanned downtime can put lives at-risk.

LEGACY INFRASTRUCTURE

Over 70% of IoMT devices run on unsupported Windows operating systems (such as Windows 7). Because these operating systems are no longer supported, they cannot be patched. System-wide computing infrastructure overhauls can be costly and complex, so legacy systems are often allowed to linger.[9]

In places where legacy IoMT security measures exist, they could be undermined by vulnerable, out-of-date or otherwise insecure configurations located elsewhere within the cyber ecosystem.

With legacy infrastructure, in some cases, there's no real fix. "A lot of the healthcare devices that we consider to be IoMT, those devices are built to last 10, 15, 20 years," says Russell Jones, a partner with Deloitte's Cyber Risk Services. Your best bet may be to "...upgrade to the next generation of device."[10] At the same time, multi-generational IoMT technology infrastructure on a single system further complicates security initiatives.

[9] Ibid.

[10] "What Makes IoMT Devices so Difficult to Secure?" by Andrew Steger, Health Tech Magazine, Feb 25, 2020 https://healthtechmagazine.net/article/2020/02/what-makes-iomt-devices-so-difficult-secure-perfcon

EXPLOITABLE VULNERABILITIES

Medical devices take an average of 5-6 years to go from a concept to a product that has received FDA approval. When the average device hits the market, the technology is already five years old. In the interim, similar existing technologies may have enabled cyber attackers to develop exploit methods that are applicable to these devices.

OWNERSHIP

Who's really responsible for safeguarding devices anyway? This hasn't been well-defined. Hospital personnel often regard manufacturers as largely responsible for device security, as they're responsible for device safety. Conversely, device manufacturers express that the responsibility lies with the healthcare delivery groups. This gap in expectations has often manifested when a cyber attack has hit. New regulations around IoMT have minimized this issue, but it still lingers today.

LAX SECURITY CONFIGURATIONS/PRACTICES

Fifty-six percent of all cyber security incidents in the health care space occur due to internal misconduct. Health care represents the sole industry where cyber damage is more commonly inflicted by insiders rather than outsiders. One way to address part of this risk? Passwords.

The use of hard-coded and unchanged default, credentialed passwords represents a top vulnerability associated with IoMT. The need to eliminate these types of passwords in order to enhance security has been expressed by at least a handful of security professionals. "This practice presents formidable security risks, especially as embedded passwords may remain outside of IT's visibility schema," says expert Mitchell Muro.

OTHER DIFFICULTIES/CHALLENGES

- Absence of network segmentation and threat intelligence
- IT professionals may fear making changes to or directly interfacing with network architecture
- Bring Your Own Device (BYOD) cellphones, tablets and laptops on a network
- Disruption to cyber operations, as such can result in life-and-death situations
- Lack of general cyber awareness among staff

Top IoMT Security Solutions

Connected medical devices now represent an integral suite of tools for medical professionals and staff. In order for providers and patients alike to continue deriving benefit from these tools, the technology environment and security management around these devices must be effective.

How are healthcare leaders rethinking infrastructure in the wake of the coronavirus pandemic and increased reliance on IoMT? Leaders are looking at new steps that organizations can take in order to stay ahead of threats. Expert recommendations below:

8 Considerations for Optimizing IoMT Security

1) Visibility and Inventory

Ahead of an attempt to protect security devices, healthcare delivery organizations need to discover existing IoT devices on the network. Obtaining granular visibility capabilities, so that unmanaged devices become apparent, is essential.

> Granular device visibility can prevent lateral intrusions and malware attacks.

WHAT VALUE DOES VISIBILITY PROVIDE?

Granular device visibility enables organizations to monitor both medtech units and data traffic movement, allowing for the prevention of lateral intrusions and malware attacks. In addition to greater security, visibility can also yield long-term cost savings. With more data around what's on a network, decision-makers can better track existing devices and cut unnecessary equipment purchases. Visibility also enables organizations to better handle "shadow IT" devices; i.e., unsanctioned devices added to the network by hospital staff, third-party vendors, patients or visitors.

After enhancing visibility, organizations need to inventory devices on the network. Your organization may want to select a security solution where these two steps can be combined, thereby accelerating and simplifying processes.

WHY SHOULD YOU TRACK INVENTORY?

Beyond merely keeping IoMT devices secure, adequate tracking of inventory can facilitate instantaneous knowledge of a device's location, potentially saving a patient's life in an emergency.[11] With clear-cut, real-time tracking tools, staff members do not need to waste precious minutes searching for equipment.

Better inventory tracking can also lead to lower operational overhead. Research indicates that an average of 30% of IoMT devices are lost or unexpectedly removed from the network on a routine basis. This exacerbates the security challenge and contributes to unnecessary expense.[12]

Get a modern IoMT solution that provides granular visibility, combined with artificial intelligence-generated security policies, which can auto-identify and classify assets. Tagging mechanisms can then be used to create recommended policies for similar groups of devices.

[11] "Asset Tracking Significant to IoMT Availability, Security" by Elizabeth O'Dowd, HIT Infrastructure, Aug 4, 2017
https://hitinfrastructure.com/news/asset-tracking-significant-to-iomt-availability-security?__cf_chl_managed_tk__=pmd_fafa35baa2acb664bce0d103f7955faa1e5b0522-1627340273-0-gqNtZGzNAzijcnBszQa0

[12] "How to Mitigate COVID-19's Impact on Device Security and Patient Safety", by Jessica Davis, Health IT Security, Feb 26, 2021
https://healthitsecurity.com/features/how-to-mitigate-covid-19s-impact-on-device-security-and-patient-safety

2) Auditing for Known Vulnerabilities

As of February 2020, 32% of healthcare leaders admitted to never having audited medical IoT. In acing the basics, ensure that your organization audits all devices for known vulnerabilities.[13]

Once the auditing process is complete, and vulnerabilities have been identified, implement appropriate patches. Depending on the nature of the equipment, organizations may wish to patch devices with a security overlay using network IPS, which enables "virtual patching" of vulnerable devices. Alternatively, organizations may wish to dispose of unused devices that present risk.

"If you're taking a reactive approach rather than a proactive approach, and you don't audit for existing vulnerabilities, you've already lost half the battle," says cyber security expert Itzik Feigelvitch.

3) Security Segmentation

Ninety-nine percent of device-to-device communications are unnecessary. Security through segmentation represents a best practice, and according to experts, its importance "cannot be overstated."[14] Creating a separation between patient data and the remainder of the IT network allows for a clearer understanding of network traffic and improved anomaly detection. In turn, IT staff can then better evaluate unusual movements or a compromised IoMT unit. In addition, segmentation can prevent threats from moving laterally across networks, instead leaving the threat isolated.

ALREADY HAVE A SEGMENTED NETWORK?

You're probably thinking about whether or not additional segmentation is necessary. Some healthcare systems go as in-depth as segmenting devices by type, which can be required by the manufacturers (Mfgs), while others segment by floor or hospital department, which typically isn't enough.

[13] "Will Recent IoMT Medical Device Concerns Make a Change in Healthcare in 2020?", Sensato, Feb 25, 2020 https://www.sensato.co/post/will-recent-iot-medical-device-concerns-make-a-change-in-healthcare-in-2020

[14] "What Makes IoMT Devices so Difficult to Secure?" by Andrew Steger, Health Tech Magazine, Feb 25, 2020 https://healthtechmagazine.net/article/2020/02/what-makes-iomt-devices-so-difficult-secure-perfcon

4) Create an IoMT Security Overlay

Ensure that your organization has the right security policies in place to secure IoMT devices. This means adding a zero trust security overlay to better manage IoMT network access control and reduce risks.

Tagging devices with classification data and risk-level enables admins to use firewalls for threat prevention, while applying tailored/specific access rules. Risk scores enable security admins to triage IT estates so that they can create a plan that allows them to secure their most vulnerable IoMT assets first. Pushing specific policies to firewalls permits restricted network access to only that needed by the device and provides stronger overall security.

For example, if an infusion pump is appropriately tagged, a provider can control its access to other parts of the network. The provider may also implement specific communication policies that, for example, only enable the device to communicate with its dedicated gateway and server. With certain port and protocol restrictions, admins can also govern which devices the infusion pump communicates with, and can determine that it should only communicate with pre-defined manufacturer-established ports and protocols. When discovery processes are in sync with network security policy, then any changes are monitored and the security policy remains up-to-date.

5) BYOD Policies: Should Be Clearly Defined and Enforced

While BYOD can increase productivity, efficiency and help streamline workflows for care providers, it can also present security concerns due to the fact that these devices largely remain 'out-of-reach' for IT admins. BYOD devices may transmit sensitive patient data, from electronic health records to real-time patient monitoring information.[15]

While the precise implications of BYOD on patient health have yet to undergo rigorous evaluation, researchers at the School of Computing and Information Systems and the Centre for Digital Transformation of Health, both within the University of Melbourne, determined key elements of a BYOD policy, as outlined below.[16]

[15] "Hospital Bring-Your-Own-Device Security Challenges and Solutions: Systematic Review of Gray Literature", Tafheem Ahmad Wani, Antonette Mendoza, Kathleen Gray, JMIR Mhealth Uhealth, Jun 18, 2020 https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7333072/

[16] Ibid.

Key elements of a hospital's bring-your-own-device policy.

Item	Description
Key definitions	Scope, purpose, and governance structure of the BYOD[a] program, along with the definition of important terms used in the policy.
Service provision	Specifies the process of enrollment, registration, and deregistration.
Access control	Defines who will have access to what information and when. This is particularly important for personal health information, where the principle of least privileges must be applied. Only the required information must be supplied and only when needed, especially when it comes to patient data.
Data storage	Specifies what hospital data are allowed to be stored on BYOD devices and how. If backup is involved, the policy should also advocate for separate backup of personal and hospital data.
Incident reporting	Defines the procedure for reporting cases of breaches, including cases of theft/loss of device. Employees must report such cases to the IT[b] department, especially if patient data are involved, and the IT department must report it to government agencies in case of major breaches.
Legislation and noncompliance	Defines applicable privacy or health care laws as well as actions or penalties in case of noncompliance with the policy or in case of breaches caused by employee's personal devices.
Education strategy	Strategies to train employees periodically to ensure secure user behavior. BYOD users should be constantly updated about latest cybersecurity threats. Policies should be disseminated through all means possible. Changes in policies should also be communicated.
Acceptable use	States the purposes for which BYOD devices could be used, whether clinical or nonclinical, and by whom. It defines reasonable use and prohibited activities.

HOW DO THE RECOMMENDATIONS HERE ALIGN WITH YOUR BYOD POLICY?

Further recommendations from the group include use of secure messaging apps and the use of single sign-on (SSO). More broadly, BYOD threats are growing, and people, policies, regulations and technologies must remain in alignment in order to combat them. Opt to work with a security vendor that can advise on a BYOD policy or BYOD policy fine-tuning for your organization.

The chosen vendor should have a mobile threat defense solution that can protect mobile devices from malicious apps and network threats. You'll want to integrate mobile security with your MDM/UEM solutions to protect BYOD, other mobile devices, and endpoints from phishing, ransomware attacks, and other threats.

6) Know Who You're Working With

Chose trusted vendors for device delivery. Seek vendors who care about security and high-quality provider and patient experiences as much as you do.

Many healthcare organizations care about more than medical devices and want a vendor that can assist with all aspects of security; from IP cameras in networks, to printers, to building management systems. Vendors like Check Point are poised to help combat all of the challenges that regular enterprises contend with and those unique to the healthcare space. If you're interested in a product that can discover what's on your system and that can provide integrated, custom-capable security, consider security vendors with granular knowledge of IoMT and IoT network protocols. Also, choose vendors with tight integrations, making the tie between discovery and IoMT policy enforcement seamless.

7) One-Stop Shopping

A security vendor that can help you combat all threat types in a cohesive way not only provides stronger security, but also enables healthcare delivery organizations to obtain increased control over their digital device landscapes. A continuously monitored, comprehensive view of a cyber ecosystem strengthens IT's abilities to take decisive action, when needed, leading the IT team to fulfill its objectives more effectively.

In addition, a multi-modal product ensures that you won't have to stumble through integrations with a vast array of hardware and software components. Integrated solutions, like Quantum IoT Protect, are non-disruptive, easy to implement, and protect office, endpoint, mobile, IoT, IoMT and other business systems in a simplified way.

8) Multi-Layered Security

While we've just discussed a variety of technical security implementation options, don't overlook physical security. Devices that are not in use should be stored in designated spaces, rather than occupying the corners of vacant ICU rooms. Health care delivery groups may benefit from connecting physical security apparatuses to network operations.

Physical and digital security strategies go hand-in-hand. For example, organizations may want to consider restricting access to ports, so that bad actors cannot surreptitiously plug in and add devices. In addition or alternatively, IT admins may also consider preventing access with a physical cable, unless the user/device can be authenticated.

If implemented correctly, IoMT security will require continual management and expansion. While a difficult undertaking, you'll add-value as a leader and move towards your healthcare system's foremost goals; chief among them, excellence in patient care.

Other Considerations

INCIDENT RESPONSE AND ESCALATION

In the event that a security incident occurs, every player on your team should understand who to contact and how to operate. Organizations may want to keep a hard-copy of an incident response plan in a safe location, should network functions stop working. On a regular basis, be sure to update your incident response plan and to rehearse its orchestration with all stakeholders.

CYBER SECURITY AWARENESS TRAINING

Providing non-medical education in a healthcare setting can be a struggle, as healthcare professionals often want to focus on patient care. IT professionals who intend to offer cyber security training should consider how they can align themselves with the staff's thinking. IT professionals should emphasize how cyber security awareness contributes to improved patient outcomes.

For example, leaders can invoke the idea of 'do no harm', which is part of the physicians' Hippocratic Oath. Cyber security breaches can harm patients through the loss of privacy and through stolen identity information. The concept of 'do-no-harm' extends to all aspects of providing care, not just face-to-face interactions. Thus, daily actions that help protect IoMT do translate to care outcomes.[17]

This message may be best understood when coming from someone considered an authoritative professional colleague, rather than an IT staff member. Keep a pulse on how your staff responds to cyber security messages and adjust your outreach and programming accordingly. Ask external experts for programming advice, if needed.

[17] "Why All Healthcare Workers Need Cyber Security Training", by Mike Chapple, Health Tech Magazine, Oct 17, 2019 https://healthtechmagazine.net/article/2019/10/why-all-healthcare-workers-need-cybersecurity-training

The Role of Medical Device Manufacturers in Security

While medical device security within a healthcare setting in large part depends on the strategy and vision of an organization's IT team, medical device manufacturers also bear a certain degree of responsibility.

In 2017, a pacemaker device security audit revealed over 8,000 flaws, some of which analysts labeled "potentially deadly." On the manufacturing side, simple bugs in code and poor design left lives on the line. The device produced by one manufacturer revealed 3,715 flaws. A second manufacturer's device showed 2,354 flaws.

When examining a different product, this group of researchers discovered models that did not require physicians to authenticate programmers, and programmers were not required to authenticate device operations. As a result, anyone within a certain radius around the device could have manipulated it.

Clear guidelines concerning premarket regulations were established in 2018, and state that medical device manufacturers are responsible for taking cyber security measures. Manufacturers must embed security into the design and architecture of devices. And manufacturers' DevOps teams must integrate security into the development lifecycle, rather than tacking it on ad-hoc at the end of code development.[18]

The security-by-design approach helps. Medical device manufacturers can go beyond basics by exploring proactive means of identifying vulnerabilities, disclosing them and providing solutions. Manufacturers with strong risk management protocols in place can gain an edge over the competition. If your products are definitively more secure and safer to use with a patient population than those of your rival's, healthcare buyers will likely chose your brand, when given the option.

In the future, success as a vendor will depend on your ability to show buyers that you have prioritized their values — which include strong security and privacy measures.

[18] "IoMT Security: A Comprehensive Approach to Mitigate Risk and Secure Connected Devices", by Salwa Rafee, Security Intelligence, May 31, 2019 https://securityintelligence.com/posts/iomt-security-a-comprehensive-approach-to-mitigate-risk-and-secure-connected-devices/

Security by design takes time and careful review during development. Security assessments on firmware and code can be done to identify risks and vulnerabilities, and — at a minimum — should be incorporated into the design process.

COLLABORATIVE INITIATIVES

At the end of the day, device manufacturers and healthcare delivery groups need to engage collaboratively when it comes to effective security infrastructure development and improvements. Communication is key in zeroing in on solutions that deliver reward for all parties involved.

In 2020, the World Economic Forum reported that a cyber security researcher hacked her own pacemaker to expose its cyber vulnerabilities.[19] She discovered that a hacker could switch it off, make it malfunction, or falsify the information sent from the device to the physician. Resolving these types of issues requires a high degree of cooperation, solidarity and a commitment to championing first-rate outcomes for all.

Why Not an IoT Solution?

Your organization already has an IoT footprint; it includes Class II and Class III medical devices, building management systems, and physical security systems, like network connected video cameras. Organizations that already have IoT solutions in place may wonder about the value of investing in an IoMT solution. Here's what you need to know:

Traditional IoT security platforms often fail to fully 'understand' manufacturers' communication protocols. On this account, IoT security may only identify a selection of suspicious behaviors. It will not be able to pick up on all potential threats.

Security tools that offer a deep understanding of IoMT devices and network protocols, and that present 'expertise' within the clinical domain can provide higher quality device protection.

A solution that offers traditional IoT security can work for IoMT devices to an extent, but significant risks may continue to persist. An IoMT-specific solution clearly emerges as a stronger security choice. Nonetheless, choosing a discovery vendor with knowledge of both IoT and IoMT may enable you to make the best decisions for your organization.

[19] "This woman hacked her own pacemaker to show how vulnerable we are to cyberattacks", World Economic Forum, Nov 6, 2020 https://www.weforum.org/videos/this-woman-hacked-her-own-pacemaker-to-show-how-vulnerable-we-are-to-cyberattacks

Can I Integrate IoMT Security With Existing Cloud Security Technologies?

Cloud integration issues represent a substantial area of concern for many organizations. The majority of cloud integration issues emerge due to the learning curves around cloud and IoMT, respectively. "For some healthcare groups, medical organizations and innovative healthcare startups and service providers, leveraging IoT/IoMT, reference architecture in the cloud provides the ultimate innovation, agility, automation, scale and resiliency," reports Check Point security expert, Micki Boland.

Healthcare delivery organizations can approach IoMT technology as a new and separate line of business and business function. For the cloud component of IoMT, PHI/PII protection of bioinformatics and patient data, least permissions, strong IAM controls, multi-factor authentication, key management, continuous compliance and enforcement of governance, risk and compliance management protocols are must-haves.

If the option to work with an external, third-party cloud security vendor that supports multi-cloud and hybrid cloud environments is available, such a partnership can be worthwhile. A third-party cloud vendor can provide technical insights regarding the risk and invest in the expertise and resources to assist with comprehensive IoMT security endeavors. These third-party groups often work with well-known cloud security purveyors.

Conclusion

Medical devices have played a significant role in improving the quality of health and healthcare amidst the pandemic. IoMT presents opportunities that healthcare delivery organizations deem extremely valuable.

Although securing IoMT represents a continual work-in-progress for IT teams, the right IoMT security strategies and solutions can prepare your organizations for threats and help you avoid cyber attacks.

For IoMT security solutions that enable you to optimize existing security, connect with our team here.

Worldwide Headquarters
5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

U.S. Headquarters
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233

www.checkpoint.com