YOU DESERVE THE BEST SECURITY

How Healthcare can Boost Its Cyber Defense and Close Security Gaps in 2023

CHECK POINT
INFINITY

Introduction

Hackers have made healthcare a top target. As a result, the healthcare industry experienced the highest number of ransomware attacks during Q3 2022, with one in 42 healthcare organizations suffering an attack – in spite of an 8 percent drop in ransomware attacks in Q3.

In addition, a survey[1] of 132 health care executives found that ransomware was the No. 1 cyber security threat, more so than insider threats or data breaches.

> "Approximately 30% of the world's data is currently being generated by the health sector, making the healthcare industry one of the most attractive targets to hackers."

Unfortunately, lives are at stake. Given the recent state of cyber attacks, hospitals are now beginning to see how cyber security doesn't limit itself as an IT requirement, but how critical it is in delivering patient care.

Hackers' access to private patient data opens the doors for them to alter the information, which could lead to profound consequences on patient health outcomes. For example, ransomware attacks in the past have forced hospitals to divert ambulances because their emergency rooms couldn't accept new patients, disrupt chemotherapy, delay reporting lab results, and postpone appointments for maternity patients.

With proper planning and investment, it's possible to prevent and mitigate these risks. In this paper, we discuss the challenges of securing a complex healthcare environment – and how you can leverage a consolidated security architecture to efficiently secure patient safety and hospitals operation.

[1] Jenni Bergal, "Ransomware Attacks on Hospitals Put Patients at Risk," PewTrusts, May 18 2022, https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2022/05/18/ransomware-attacks-on-hospitals-put-patients-at-risk

Challenges of securing a healthcare environment

Digital Transformation

Healthcare needs technology to help drive positive health outcomes. Without digital technology coming in and making the transformation that's much needed, hospitals will always be up against a lack of resources, lack of efficiency, lack of staff, lack of data, and lack of knowledge about what they're seeing in regard to IT operations.

For example, healthcare providers are striving for an integrated healthcare model. Data sharing is at the center of everything – from clinicians to organizations and patients – and client data sharing is pivotal to being able to provide an integrated healthcare model. However, healthcare organizations can't afford to leave cyber security as an afterthought to the digital transformation process.

And for better or for worse, we now have a recency bias of the speed with which we moved due to the pandemic. Because we've had a taste of how fast things could be in making real changes in how we can deliver care and embrace virtual care, there will be a bit of a struggle in taking a timeout and being more considerate of the security ramifications of speech. We need to balance speed and meaningful change with safety and risk aversion, particularly in the cloud.

Healthcare providers push their workloads into the cloud, and many entities didn't take a step back to make sure that these cloud workloads were designed with security in mind. Providers also didn't ensure that they had the right levels of privileged access to these devices. Expectations must be reset, and healthcare providers need to understand that not everything can be done as quickly as they were done in the past – at least not without sacrificing some level of baseline security.

Patient Records – Data Privacy and Confidentiality

When we think about why there are so many attacks on healthcare organizations, the reason is because that's where the gold is, at least in hackers' minds. Healthcare data is incredibly attractive and is a goldmine for hackers. When we think about all of the things that include images of patients, driver's licenses, insurance cards, social security numbers, and things that have absolutely nothing to do with medical data, but have everything to do with identity theft – all this data provides nefarious ways of taking advantage of people. Thus, data security must be at the forefront of any security team at a healthcare provider.

IoT Devices – Broaden the Attack Surfaces

With the advancement of technology, including IoT devices, you open yourself up to new risks. And these risks can put a wedge into achieving safe and secure medical care for your patients and staff.

IoT is broadening the attack surface. The minute you go into any hospital setting, you are surrounded by IoT devices: they are everywhere. Before you even enter the hospital building, you have smart cameras that are recording people walking in and out of the building, sensors that detect which cars or deliveries are coming in, and everything within the hospitals themselves, such as smart beds, smart sensors, MRI scanners, imaging machines.

The main concern is that these IoT devices don't always come under the control of the IT team. Many of these IoT devices still run legacy DOS operating systems, and some are still on Windows XP. These devices are not patched or monitored to the same extent as modern OSs, but they sit on our networks alongside other critical systems, causing the potential security risk to get bigger and bigger. Implementing an IoT security solution is essential to closing the IoT security gap.

Network Segmentation

It's surprising to hear how many flat networks there still are in the healthcare setting. There is zero segmentation between different areas of the network, which increases the level of risk and exposure.

When introducing new devices, make sure you put them into a segmented network in a place where it's safe and secure. This is much better than having to try and then retrospectively fix or segment the device onto that leg of the network.

Medical teams are the ones that bring in new medical devices, but the security teams must make sure they're engaged right at the start to ensure safe security, design, and operational needs around these devices.

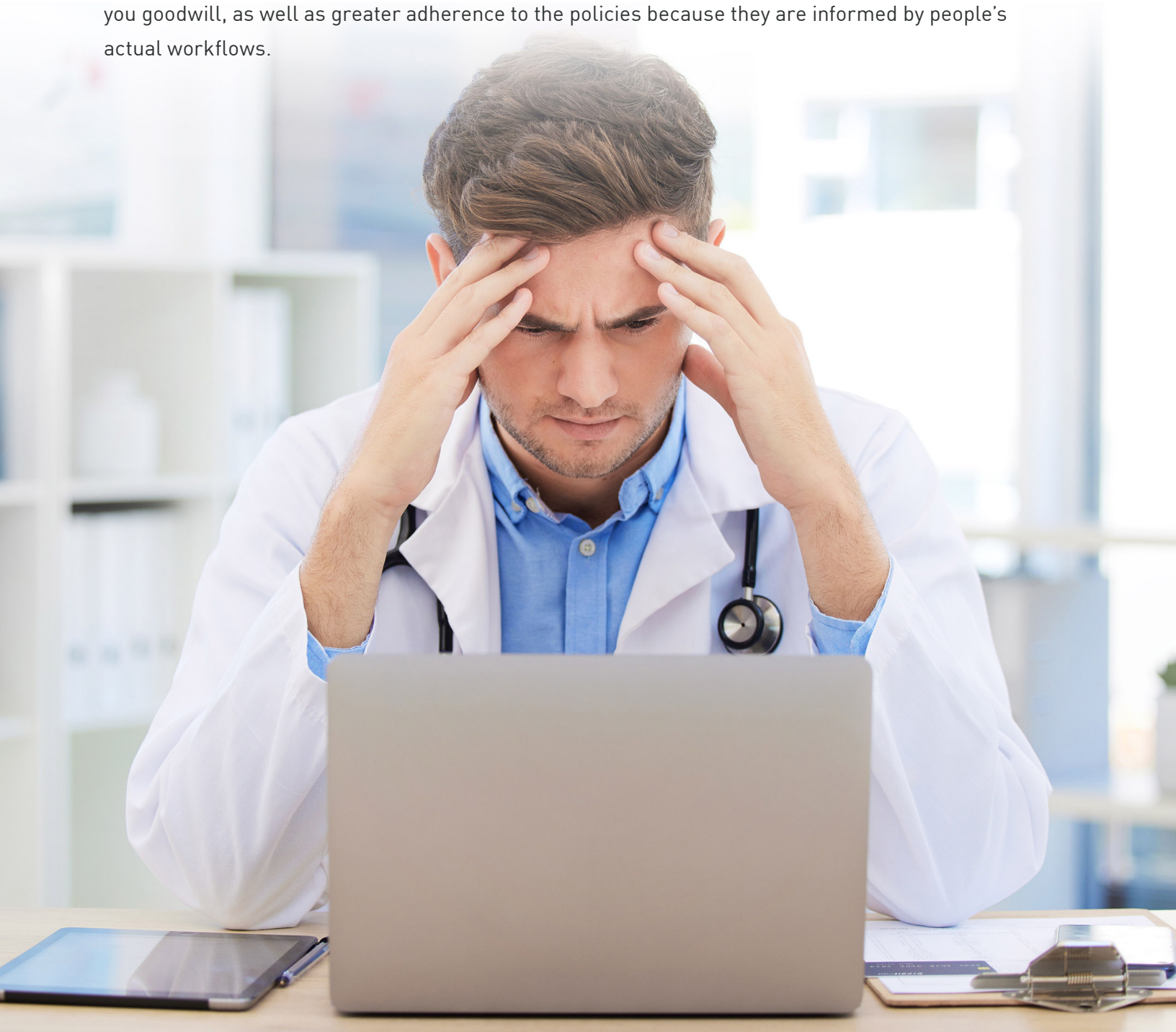
Why segment? First, network segmentation is considered a best practice and is cited in the National Institute of Standards and Technology (NIST) SP800-125.[2] Second, segmentation prevents attackers from moving laterally and infecting other devices if they were to gain access to a single device on an organization's network. Segmentation can also enable analysts to trace the path back to the point of entry, enabling the organization to patch the vulnerability and better secure the network in the future.

[2] "Guide to Security for Full Virtualization Technologies," National Institute of Standards and Technology, January 2011, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-125.pdf

Getting Buy-in from Internal Stakeholders

One mistake that IT teams can make is that they are so myopic in implementing cyber security that they forget to consider whether employees will follow the security procedures or not. It's critical to make cyber security not so cumbersome so that people will circumvent it. For example, some people may complain about multifactor identification being too cumbersome, so they think of other devices to access that data that is perhaps easier.

When creating security policies, make sure your clinical teams have representation, so that they at least have a voice and make their concerns heard as you're developing these processes. This buys you goodwill, as well as greater adherence to the policies because they are informed by people's actual workflows.



Opportunities in leveraging a consolidated security architecture

Digital Transformation

Because of the challenges discussed previously, there's a lot more conversation taking place around the consolidation of security solutions. Because the landscape is so complex and disjointed, you need to be looking at security in a slightly different way. Executives are asking if you can do more with less, and there is a huge ongoing cyber skills shortage across the world now. Thus, companies are starting to look at automation to come in and help find threats before they are exploited by malicious actors and to provide healthcare providers with a much simpler security landscape.

Security teams must think about how they can simplify, consolidate, and have more visibility across the entire network. There is a high-risk level associated with using too many vendors and systems and not having that full end-to-end visibility across your systems. Consolidation allows you to simplify your stack and take it down to a much smaller, more manageable supply chain. Because technologies will continue to evolve and become more complex in the future, the case for consolidation will only get stronger. A consolidated solution can secure these five key areas in your healthcare organization: IoT, cloud, data centers, apps used by staff, and patient records.

Protect and Segment IoT and Smart Medical Sensors

Medical IoT devices have done wonders for the medical profession. They facilitate improved care coordination, better data analytics, and more favorable patient outcomes. However, connected machines such as X-ray machines, picture archives, ultrasounds, PET scanners, CT scanners, and MRI machines are all vulnerable to cyberattacks. Secure overlays to protect and segment these insecure IoT devices are essential.

Secure Your Cloud Adoption

The rapid proliferation of medical and health technologies that consumers can interact with is driving healthcare providers into the cloud, specifically to new application workloads. There are so many workloads in the cloud that we can't really see what's there. Teams have difficulty seeing how many copies there are of the data, where it is, who has access to it, and visibility across the supply chain for parties that have remote access to that data.

For many healthcare use cases, modern workload architectures are an excellent choice, for several reasons. First, healthcare, and medical applications require large scale and high availability. Thus, serverless and container workloads make building and operating these applications much easier and less costly. Second, compliance and data privacy protection are critical to healthcare technology solutions. Third, centralized visibility across cloud-native environments gives you a comprehensive view of all the activity within your cloud network.

Strengthen Security at Data Centers

In the past, data centers focused on the redundancy and backup of core technologies and data. Now, security has become inextricably linked with data centers. Cyberattack onslaughts have pushed healthcare providers to step up their security at the network perimeter and prevent data center preaches where Protected Health Information (PHI) records reside.

Employ Mobile and Endpoint Security

Many employees use their mobile devices to access company applications as BYOD (Bring Your Own Device) policies proliferated in the past years. However, without a strong digital defense, threat actors can obtain sensitive information, and use it for extortion purposes or as material to sell on the dark web. One study[3] found that 30 popular health apps that allow healthcare providers to review patient charges and schedules were all vulnerable to API cyberattacks. To secure your organization, advanced mobile threat prevention is an absolute necessity.

> "71% of healthcare medical apps have a serious vulnerability."[4]

Protect Patient Records Confidentiality

Medical records are the crown jewel for hackers. Some Electronic Healthcare Records (HER) can be sold on the darknet for up to $1,000. From 2009 to 2022, there were over 342 million leaked records[5] from medical breaches in the US alone. Breaches can often lead to healthcare systems going offline, meaning medical workers are left without essential information required for their work. Securing patient records should be the No. 1 priority of all hospitals.

Fortunately, there is a solution to the major security challenges listed above. An integrated healthcare security solution can keep your patients safe and medical information protected. Check Point Infinity's consolidated architecture allows healthcare organizations to secure their entire workforce, network, cloud, mobile, IoT, and data – all at a predictable spend.

[3] Risks of Mobile Health Apps: Are Health Apps Putting PHI at Risk?", Compliancy Group, February 16 2021, https://compliancy-group.com/risks-of-mobile-health-apps-security/

[4] Sudipto Ghosh, "71% of Healthcare Medical Apps Have a Serious Vulnerability," AIThority, September 29, 2020, https://aithority.com/ait-featured-posts/71-of-healthcare-medical-apps-have-a-serious-vulnerability-91-fail-crypto-tests/

[5] Paul Bischoff, "Medical breaches accounted for 342 million leaked records from 2009 to 2022," Comparitech, August 24, 2022, https://www.comparitech.com/blog/vpn-privacy/medical-data-breaches/

Check Point Infinity

Check Point Infinity delivers the broadest set of security products and technologies to protect healthcare organizations in real-time against the latest generations of multi-vector cyberattacks across the network, endpoint, mobile, IoT, and cloud.

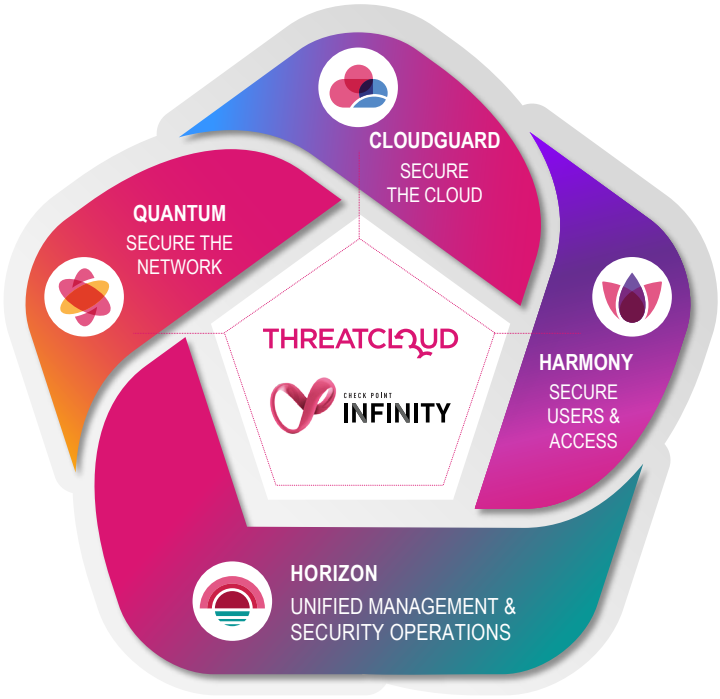


Figure 1: Check Point Infinity consolidated architecture

Infinity enables you to use the security products you need, in an annual subscription that includes:

- **Real-time Threat Prevention:** Protection against Advanced Persistent Threats (APTs) and unknown zero-day malware, using real-time sandboxing; ransomware protection; and anti-bot technologies, powered by integrated, real-time cloud-based threat intelligence and machine learning for identifying new threats.
- **Advanced Network Security:** The most advanced firewall, intrusion prevention, and application control, supporting networks of any size—from branch offices to global enterprises, and across both private and public cloud security offerings
- **Cloud Security:** Advanced threat prevention security in public, private and hybrid cloud, and SDN environments, with micro-segmentation for east-west traffic control inside the cloud.
- **Mobile Security:** Malware prevention on iOS and Android mobile devices, rogue network identification, secure containers, data protection and document encryption, and EMM integration.
- **IoT Security:** Identifies any IoT device on the network and assesses its risk, prevents unauthorized access to and from IoT devices with zero-trust segmentation, blocks IoT malicious intents with industry leading threat prevention security services.
- **Data Protection:** Anti-ransomware for known and unknown ransomware, data protection and seamless document encryption, browser security, a fully integrated endpoint protection suite and security forensics.
- **Integrated Security & Threat Management:** A unified security management environment supporting multi-device, multi-domain and multi-admin management, with complete threat visibility supporting collection, correlation and attack analysis, and reporting tools for compliance and audit.

- **Security Services:** Real-time security updates (ThreatCloud), software updates, hardware maintenance, 24x7 support and maintenance, and optional training classes, on-site professional service, consulting workshops, security checkups and incident response (based on selected package).

Figure 2: Check Point Infinity – a complete cyber security subscription model

In summary, Check Point Infinity Enterprise License Agreement future-proofs your security infrastructure by providing end-to-end coverage across all attack vectors.

Consolidation cuts complexity to reduce risks: the global cyber-skills gap grew by over 25% in 2022. Yet organizations have more complex, distributed networks and cloud deployments than ever before because of the pandemic. Security teams need to consolidate their IT and security infrastructures to improve their defenses and reduce their workload, to help them stay ahead of threats. Over two-thirds of CISOs stated that working with fewer vendors' solutions would increase their company's security.

Moving forward, a high percentage of companies plan to consolidate their security vendors to reduce complexity and optimize costs. To stay ahead of the cyber security curve, consider a consolidated solution.

To learn more about Check Point Infinity and Infinity ELA, please visit:

checkpoint.com/infinity

CHECK POINT INFINITY

ENTERPRISE LICENSE AGREEMENT

Quantum CloudGuard Harmony Horizon

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

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

www.checkpoint.com