SEPIO

Managing Hardware Related Risks in Healthcare

A Sepio white paper

EXECUTIVE SUMMARY

The healthcare industry is a vital component of a nation's critical infrastructure. The various entities that make up the healthcare sector perform tasks ranging from day-to-day activities to life-saving operations. But while the majority of us depend on the industry for our well-being, malicious cyber actors view healthcare delivery organizations (HDOs) as attractive targets. From their mass data collection to their low tolerance for downtime, HDOs are the perfect victims. Further, as the COVID pandemic overwhelmed the industry, several new vulnerabilities arose, which cybercriminals exploited.

Despite the industry's high susceptibility to cyberattacks, HDOs tend to undertake a weak approach to cybersecurity. The lack of sufficient measures often stems from budgetary constraints and competing priorities. But, for many HDOs, the main cost of cybersecurity is its disruptiveness; additional barriers and protocols take time away from providing patient care. Nevertheless, with the industry so reliant on technology, cybersecurity has a direct effect on patient care.

THREAT ACTORS AND MOTIVES

State-sponsored actors

State-sponsored groups target HDOs to undermine an adversary's national security and political power. Healthcare facilities own IP on innovative drugs and medication that can take years to develop. By stealing such information from an adversary, the perpetrating state can boost its own healthcare efforts and, in turn, improve its political standing. Similarly, these threat actors target HDOs to gain insight into the country's national and international healthcare policy, in which the information gets used to advance the initiator's strategies.

Other attacks are more disruptive and can impact operational capabilities, causing a physical impact that puts patients' lives at risk. By disrupting critical infrastructure, state-sponsored groups threaten national security and harm the country's reputation both internally and externally.

Terrorists

Terrorists seek to harm a state's national security through psychological warfare. They aim to cause as much damage as possible to ensure a long-term psychological effect on society. Disruptive attacks on the healthcare industry can achieve this goal. The physical impact of an attack on HDOs permeates through society, even potentially causing fatalities. This has significant psychological consequences as the safety and security of the country, and its people, are at risk.

Cybercriminals

Most cybercriminals are motivated by monetary rewards. The healthcare industry is deemed a valuable target due to its low tolerance for downtime. Ransomware attacks can be successful if critical processes get disrupted as the victim entity is under immense pressure to restore operations.

Healthcare providers are also frequent targets of data theft as cybercriminals can generate substantial profits from healthcare data and IP.

Hacktivists

Some cyber threat actors carry out cyberattacks to make a statement. HDOs are often the target of those who oppose traditional medication or the methods in which healthcare entities operate. The healthcare industry might be a pawn in a larger protest against a government. By attacking one of the nation's core sectors, hacktivists have more leverage over their powerful opponent.

COVID

The COVID pandemic presented unique opportunities for threat actors to exploit – and they did. In 2020, the number of attacks on the healthcare industry increased by more than 50% from 2019 . With HDOs overwhelmed with patients – all suffering from a novel virus – cybersecurity took a backseat. Further, the initial chaotic response efforts meant new vulnerabilities arose and remained exposed. This allowed bad actors to infiltrate healthcare targets more easily; targets that were becoming more valuable. Data collection skyrocketed, and vaccine development generated sought-after IP.

Disruptive attacks had a more significant impact on national security as the healthcare industry was relied upon like never before. Any delays to response efforts, be that in hospitals or research labs, cost hundreds, if not thousands, of people their lives. Further, interruptions caused by a cyberattack shine doubt on the government's political capacity. The dependency on healthcare meant that even a minor disruption got heavily scrutinized, and the government's capabilities were put into question.

Attacks on healthcare rose by 55% between 2019 and 2020

Healthcare Breach Report, Bitglass, 2021

ATTACKS AND OUTCOMES

General overview

Due to the nature of the industry, cyberattacks targeting healthcare are more costly than the global average. Remediation efforts and downtime have a substantial financial effect as HDOs operate in time-sensitive environments. However, there are also many indirect costs associated with cyberattacks that healthcare entities must face. HDOs pay some of the highest regulatory compliance fines in the world, often in the seven-figure range, should they fail to secure their infrastructure. Additionally, reputational damage means healthcare providers often suffer from loss of business following a cyberattack. According to research by Morphisec, 27% of patients would switch healthcare providers if their current provider fell victim to a cyberattack. Efforts to repair the organization's reputation, if even possible, is another financial burden.

Ransomware

The healthcare industry mostly suffers from ransomware attacks, accounting for 28% of all cyber incidents in 2020 . According to research by Ponemon Institute, 43% of HDOs suffered a ransomware attack over the last two years .

Healthcare entities are highly sensitive to ransomware attacks because of the low tolerance for downtime. Further, ransomware attacks on HDOs put lives at risk; Ponemon Institute's research found that mortality rates rose by more than 20% as a result of ransomware4. Ransomware can target, or spread to, systems that life-saving equipment relies on, preventing such equipment from being used. Alternatively, ransomware might infect non-critical systems, but the chaos and disorder that ensues compromises patient health as a result.

43% of HDOs suffered a ransomware attack over the last two years

Ransomware caused a 20% increase in mortality rates

The Impact of Ransomware on Healthcare During COVID-19 and Beyond, Ponemon Institue, 2021

DISTRIBUTED DENIAL OF SERVICE (DDOS)

DDoS attacks, like ransomware, cause disruptions to operations. Often, DDoS attacks act as a cover-up for more sinister activities, such as ransomware and data breaches.

DDoS attacks on their own can be used for extortion purposes and to raise awareness of a specific cause. For this reason, hacktivists are often the initiators of DDoS attacks.

HDOs do not suffer from DDoS attacks frequently. However, when a DDoS does take place, it does not go unnoticed. Network outages cause major disruptions and, like with ransomware, impact services to patients. Typically, DDoS attacks on HDOs are carried out by hacktivists making a statement as there is often controversy surrounding the healthcare industry.

DATA BREACH

The healthcare industry is a frequent victim of data breaches, with such attacks rising by more than 50% from 2019 to 2020 . The troves of data collected are the primary reason HDOs are susceptible to data breaches; everyone requires healthcare, so the industry has one of the largest databases of Personally Identifiable Information (PII) in the world. Malicious actors target such data to sell on the dark web for identity theft purposes. Perpetrators might try to steal employee credentials as insider privileges allow for further malicious activity to take place. HDOs also collect Protected Health Information (PHI), which is the crown jewel of the healthcare industry.

PHI is usually what cybercriminals are after due to its high value. PHI cannot change as our medical history is ingrained within us, thus making it highly unique. With PHI, identity theft is much more nefarious, and, as a result, patient safety is at risk. An Electronic Health Record (EHR) is worth significantly more than credit card info on the dark web. As such, data breaches in healthcare cost an average of $10 million, compared to the global average of just over $4 million .

IP within healthcare is highly sought after by threat actors. The industry is constantly innovating and developing new medications that attackers try and get their hands on. The various COVID vaccines were highly desirable IP for state-sponsored actors seeking to advance their own efforts.

Financially-motivated actors were, too, interested in obtaining the ingredients. Research by Check Point found that vaccines were getting sold on the dark web for hundreds of dollars . In an effort to make money, malicious actors are seriously endangering the buyers.

Data breaches on the healthcare sector rose by 51%

2021 Indentity report, Constella, 2021

LAYER 1 VISIBILITY CONCERNS

To carry out the above-mentioned attacks (and more), threat actors often turn to hardware-based attacks. Hardware security is a poorly covered realm of cybersecurity; existing security solutions, such as NAC, EPS, IDS, or IoT Network Security, fail to provide Layer 1 visibility. As such, HDOs lack complete asset visibility, and with this comes the inability to detect vulnerable or Rogue Devices. This blind spot allows hardware attack tools to bypass security protocols, even those as stringent as Zero Trust. Without knowing what is operating within the infrastructure, the organization has limited control over its assets and is thus very susceptible to hardware-based attacks.

Hardware-based attacks require physical access to the organization. Rogue Devices must be used within the target's infrastructure for the attack to place. However, there are several vulnerabilities within the healthcare industry that increase accessibility which, in turn, enable hardware-based attacks.

VULNERABILITIES

Interconnected environment

HDOs operate in highly interconnected environments. Such environments enable lateral movement; by hacking just one device, an attacker can gain control of more devices and/or the entire network. With an increasing number of devices used within healthcare, there is a growing number of entry points. Further, the integration of IT and OT through IoMT has made operational equipment more accessible.

Network segmentation can limit lateral movement and subsequently reduce the blast radius of an attack. However, research by Forescout found that segmentation efforts are seriously lacking within the healthcare industry . This is a significant risk as many accessible devices, such as smartphones and computers, operate on the same network segment as critical IoMTs. Further, a lack of Layer 1 visibility means HDOs are unaware of already-vulnerable IoMTs within their infrastructure, such as those powered by Raspberry Pis. As a result, these risky medical devices are not afforded sufficient protection, and other medical equipment on the same network segment is vulnerable.

Accessible devices

Many devices are easily accessible due to remote use. Remote environments are less secure, which increases susceptibility to hardware-based attacks. IoMTs possess remote capabilities, and the global shift to telework has forced remote use of traditional endpoints, such as laptops. Devices often have access to or store valuable information, making them attractive targets. Further, attackers can use such devices to gain deeper network access thanks to healthcare's interconnected environment.

Supply chain

Supply chains provide attackers with a gateway into the organization. Each supplier acts as an entry point, and all have varying security postures. When HDOs are highly secured, attackers use weaker suppliers as a pathway for Rogue Devices to get inside. Suppliers themselves are at risk of hardware-based attacks as they can provide access to valuable data. Information sharing between organizations and their suppliers means data access expands beyond the internal parameters. Further, the reliance on suppliers means an attack can have spill-over effects. During the COVID vaccine rollout, many distributors along the "cold chain" suffered data breaches that affected vaccine deliveries.

Additionally, medical equipment suppliers might manufacture their products using vulnerable devices, which go undetected once inside the healthcare organization. In doing so, suppliers exacerbate the hardware security risk. We recently found hundreds of Raspberry Pis operating within the environment of one of our healthcare clients, a fact they were previously unaware of.

HAC-1 Solution

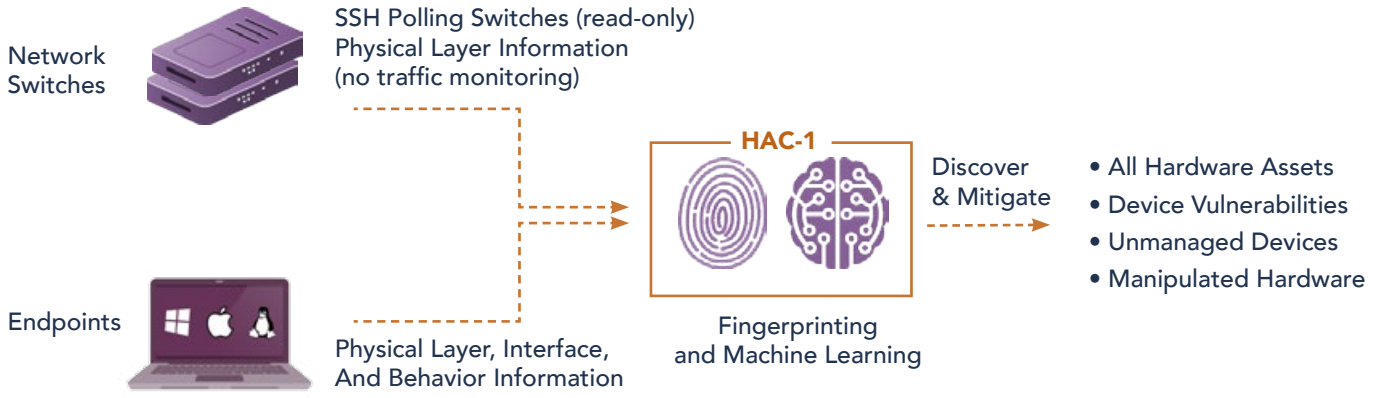
To reduce the risk of hardware-based attacks, and to improve the overall security posture, HDOs need to gain full visibility into their assets. Sepio has developed the Hardware Access Control (HAC-1) solution to provide a panacea to the gap in device visibility.

The HAC-1 solution uses Layer 1 information to calculate a digital fingerprint of all IT, OT and IoT assets – managed or unmanaged – meaning every device gets identified as what it truly is. Additionally, the comprehensive policy enforcement mechanism of the HAC-1 solution, combined with its Rogue Device Mitigation capability, means that any unapproved or rogue hardware is blocked instantly, preventing any hardware-based attacks from occurring.

With the HAC-1 solution in place, not only is the hardware level covered but, in doing so, current cybersecurity investments, such as NAC, EPS, IDS, or IoT Network Security, get put to better use, and Zero Trust Hardware Access is achieved.

HAC-1 requires no hardware resources and does not monitor any traffic; within 24 hours, we can provide organizations with complete asset visibility, identifying and blocking previously undetected rogue or vulnerable devices.

How It Works



HAC-1 - Visibility & Security of Hardware Assets

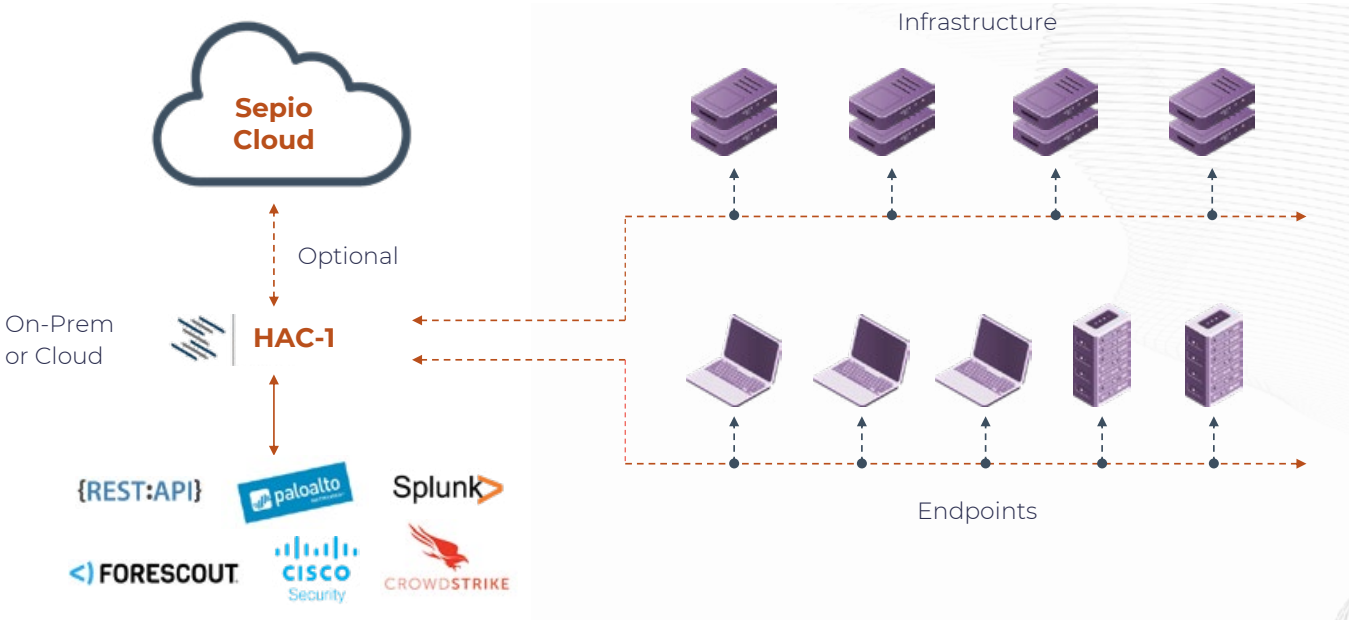
Main Benefits

Complete Visibility of all Hardware Assets: With all devices and anomalies detected, enterprises benefit from a greater overall cybersecurity posture. Gaining full visibility of all hardware devices from endpoint peripherals to connected devices (IT/OT/IoT), Sepio uses unique physical layer hardware fingerprinting technology and data augmentation from endpoints and networks.

Full Control through Predefined Policies: Enterprise-wide policies enable compliance, regulation and best practices. With predefined templates and no baselining or whitelisting, and no requirement for a clean environment start, Sepio provides a fast and easy setup.

Rogue Device Mitigation (RDM): Threat mitigation upon discovery of rogue or threatening devices. Integrations with existing security platforms such as NACs and SOARs for mitigation and remediation enhancements.

System Architecture



LEARN MORE

REFERENCES

1 Bitglass. (2021). Healthcare Breach Report 2021.

2 Morphisec. (2021). THE 2021 CONSUMER HEALTHCARE CYBERSECURITY THREAT INDEX.

3 IBM. (2021). X-Force Threat Intelligence Index.

4 Ponemon Institute. (2021). The Impact of Ransomware on Healthcare During COVID-19 and Beyond.

5 Constella. (2021). 2021 Identity Breach Report.

6 IBM. (2021). Cost of a Data Breach Report.

7 Check Point. (2021). Covid-19 'Vaccines' Touted for Just $250 on Darknet [Blog]. Retrieved from https://blog.checkpoint.com/2020/12/11/covid-19-vaccines-touted-for-just-250-on-darknet/

8 Forescout. (2020). Connected Medical Device Security: A Deep Dive into Healthcare Networks.


access denied