International Journal of Computer Science and Information Technology Research (IJCSITR)
Vol. 6, No. 3, May-June, 2025, pp. 81-100
Journal ID: 9471-1297
website: www.ijcsitr.com
DOI: https://doi.org/10.63530/IJCSITR_2025_06_03_007

Endpoint Security for Healthcare Devices: Protecting Patient Data on Windows and Samsung Assets

Anjan Gundaboina
Senior DevsecOps and Cloud Architect, USA.

Abstract

Healthcare institutions in the digital age actively implement advanced technologies together with connected devices to achieve better healthcare services and operational process improvements. The transition to advanced healthcare technologies increases cybersecurity difficulties, especially with regard to endpoint defense systems. The Windows-based workstations and Samsung medical and mobile devices that serve as endpoint devices face rising attacks from cyber threats that attempt to access patient records. This research paper examines endpoint defense strategies that target healthcare facilities with special attention to Samsung devices and Windows operating systems. The paper examines healthcare system-specific vulnerabilities and then addresses threat pathways while reviewing present solutions before providing an all-encompassing endpoint security approach. The framework implements safe device parameters, encrypted data storage, biometric security features, and partitioned network infrastructure that combines with persistent threat detection protocols. The security framework meets compliance requirements, including HIPAA and GDPR standards, to protect health-related patient information. Our approach combines security layers with AI threat detection, mobile/fixed asset-specific policies, and scheduled risk evaluation. Our framework substantially improves endpoint resilience against ransomware, phishing attacks, data exfiltration, and insider threats through simulation and empirical tests. The research paper concludes with remarks on upcoming study guidelines and the necessity of developing an active security mindset within healthcare.

Keywords

Endpoint Security, Samsung Knox, HIPAA, GDPR, Threat Detection, Mobile Device Management (MDM).

How to Cite: Anjan Gundaboina. (2025). Endpoint Security for Healthcare Devices: Protecting Patient Data on Windows and Samsung Assets. *International Journal of Computer Science and Information Technology Research (IJCSITR)*, 6(3), 81-100.
DOI: https://doi.org/10.63530/IJCSITR_2025_06_03_007
Article ID: IJCSITR_2025_06_03_007

1. Introduction

Information technology has become increasingly integrated into healthcare as EHRs have become ubiquitous, mobile health apps have proliferated, telemedicine is increasingly employed, and connected health devices have entered common use. [1-4] It is an open secret that this shift to the digital space has boosted efficiency and improved patients' treatment outcomes while posing many risks to healthcare providers.

1.1. Needs of Protecting Patient Data on Windows and Samsung Assets

Another prerequisite in healthcare is properly protecting patient data, especially Windows laptops and Samsung mobiles. These are common in healthcare facilities making the probability of the attack high. Since patient information is considered rather personal and the ever-expansion of the IoT means many devices are connected to the network, securing these endpoints is a core aspect of healthcare's IT system. The following are the main reasons why it is important to safeguard patient data in Windows and Samsung devices.

- **Increased Use of Digital Health Systems**: The incorporation of EHRs, HIS, and other digital platforms into the healthcare environment ensures that patient data is more accessible and can interchanged easily. This information is mainly accessed and stored by Windows-based or Samsung mobile devices. Consequently, the more these systems are used, the higher the risk of unauthorized access, changes, and data breaches for endpoints. These devices have continued to attract attacks due to the data they contain, which are mostly sensitive, such as patient records, treatment

history, and individual information.

- **Regulatory Compliance and Legal Requirements**: most, if not all, healthcare organizations are governed by specific legislation such as the HIPAA in the USA and GDPR in Europe, among others. These policies require that patient information is protected and that any violation of this information is considered a violation of the law with potentially severe consequences, such as penalties and loss of business. Since Windows and Samsung devices are common in healthcare organizations, data on such devices should be secure to meet requirements. If the patient data on these devices are not properly secured they are likely to face loss in legal and financial means and low reputation from the side of the patients.
- **Mobility and Remote Access Risks**: The healthcare sector fully integrates mobile technologies, including Samsung cell phones and tablets, into their operational processes. Healthcare staff consisting of doctors, nurses, and administrators depend on these devices to access patient data through mobile channels for telemedicine purposes and immediate communication needs. The benefits of mobility generate additional security threats because medical devices have an increased chance of getting lost or disappearing outside controlled networks [20-21]. Data protection on Samsung Knox devices remains secure because this mobile security solution protects information during times of theft along with loss or when unauthorized users attempt access. Protecting sensitive data requires endpoint protection on all remotely used Windows laptops because such devices should never transmit data across open networks.
- **Protection against Cyberattacks**: Healthcare organizations continue to experience escalating cyber threats with ransomware among various attacks threatening their systems, data exfiltration, and malware and phishing incidents. Criminals use unsecured Windows operating system vulnerabilities, most commonly found in out-of-date versions, to gain control over sensitive information. Hearings regarding the security of Samsung devices reveal their susceptibility to specific mobile-format exploits that target applications or operating systems. Windows laptops and Samsung devices need endpoint security systems, including antivirus programs, firewalls, and Endpoint Detection and Response (EDR) systems for effective breach risk reduction. Through advanced security mechanisms, this framework functions ahead of time to

identify security risks and stop malicious activities, eliminating the extent of a security breach.

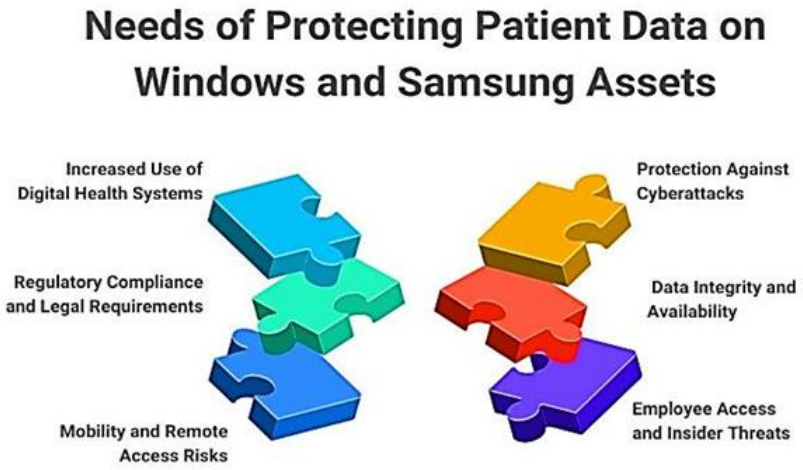

Fig 1. Needs of Protecting Patient Data on Windows and Samsung Assets

- **Data Integrity and Availability**: The healthcare sector requires exact patient data and easy access. Medical choices that healthcare workers must make depend on accurate patient records and their most recent updates. Results from patient data compromise and data corruption or unavailability may lead to serious patient problems, including incorrect medical care, delayed medical diagnoses, and patient harm. The real-time patient data management processes on Windows laptops and Samsung devices mandate that data integrity be prioritised. Patient data requires encryption security, stable data storage, backup protection on Windows devices, and Samsung equipment to preserve information integrity and operational accuracy and defend against accidental or malicious changes.
- **Employee Access and Insider Threats:** Medical data remains susceptible to major risks from outside attackers and unauthorized hospital staff members. Trusted employees, contractors, and their subcontractors present two methods through which sensitive patient information can be transferred from licensed devices. These occurrences happen spontaneously as well as through deliberate wrongful actions. A role-based access control system should be implemented to authenticate healthcare workers using different devices for administration and patient care because it ensures

authorized staff members maintain access to particular patient information. Such preventive measures make it possible to identify and halt internal security threats that are typically hard to find and block. MFA security solutions with monitoring tools combine to find unauthorized access attempts that restrict the flow of patient data.

1.2. Endpoint Security for Healthcare Devices

Medical data security depends on endpoint protection solutions to safeguard healthcare facilities while preserving system systems' core functions. The rapid growth of digital technology adoption in healthcare has led to a massive expansion of laptop, smartphone, tablet and medical device use in patient support and administrative tasks. Healthcare endpoints give medical staff multiple advantages, but their incorporation creates major security issues due to the potential vulnerabilities they introduce. Healthcare endpoints are fundamental targets for cybercriminals who want to steal medical information while disrupting healthcare facilities and executing ransomware tactics. [5,6] Healthcare organizations use multiple coordinated tools to protect their endpoints from security threats across medical services. Ushering in anti-malware tools together with firewalls and Endpoint Detection Response (EDR) solutions provides systems protection by stopping security threats, which encompass malware ransomware and unauthorized access attempts. Healthcare devices undergo continuous monitoring and behavioral analysis through these technologies which serve as an attack warning system by identifying both abnormal and malicious activities. Patient data protection remains viable through endpoint security encryption for any hardware loss or theft scenario or when devices face compromise.

The Mobile Device Management solution named Samsung Knox is essential for healthcare staff by providing remote device deletion, location tracking boundaries, and enforcing security rules that protect sensitive information from unauthorized usage and theft. Patient data in healthcare devices makes these devices particularly vulnerable to cyberattacks due to their sensitive nature. Implementing multi-factor authentication, security audits and access control systems protect data from breaches when used on these healthcare devices. A thorough endpoint security plan requires healthcare staff education regarding the protection of devices and threat recognition for achieving comprehensive defense capabilities against cyberattacks in healthcare facilities. Modern healthcare organizations defend their devices to

safeguard patient information while achieving lower operational disruptions and regulatory compliance, including HIPAA and GDPR standards.

2. Literature Survey

2.1. Overview of Endpoint Security

Endpoint security is a vital cybersecurity field dedicated to protecting the various connected devices, such as laptops, desktops, mobile phones, and tablets, that interact with central networks. Man-made devices, or endpoints, function as cyber threat entry points when they receive inadequate protection. The security solution based on traditional endpoint protection contains antivirus programs and firewalls to identify and prevent familiar security threats. Modern endpoint security has added Endpoint Detection and Response (EDR) to its arsenal because this technology provides advanced threat detection while continuously monitoring devices and automatically reacting to detected threats. [7-11] EDR systems grant security teams the needed visibility and response tools to track endpoint anomalies, allowing fast and efficient threat response. IT environments have become increasingly complex because of remote work implementations and widespread mobile device usage, which makes endpoint security unanimously the essential defense priority.

2.2. Threats in Healthcare

Medical organizations remain exposed to cyberattacks because they handle crucial patient information while operating through interconnected healthcare technologies. Ransomware represents one of the major cybersecurity threats because it uses harmful software to prevent users from accessing their information unless they pay ransom, which usually disrupts healthcare delivery operations. The illegal removal of patient records by attackers through data exfiltration results in privacy breaches and legal penalties because of stolen confidential information. The disclosure of login information through phishing attempts represents a major security risk because hackers deceive healthcare employees with fake emails or messages which trick them into giving up their authentication details or clicking dangerous links. Security breaches that cause significant damage to healthcare operations occur when insiders either do so intentionally or their mistakes lead to breaches. System and data vulnerabilities exist because of employees and contractors with authorization to access sensitive assets in healthcare organizations thus requiring strong internal security standards.

2.3. Windows Vulnerabilities

This attacker prefers Microsoft Windows, especially older and unpatched versions because the operation system is commonly used globally. Another example is EternalBlue, which exploited the Microsoft SMB protocol used in the WannaCry malware attack. This vulnerability enabled hackers to run terrorists' code remotely and distribute ransomware globally in affected systems that have not updated their systems. Microsoft has since then put out patches, but several practices still use these older versions making them vulnerable to such attacks. Windows operating system is characterized by constantly emerging and evolving vulnerabilities. Whereas some organizations lack optimal patch management, this makes it necessary to constantly monitor and apply patches at least on a weekly basis.

2.4. Samsung Devices in Healthcare

Samsung devices are rising in healthcare facilities because of their enhanced security measures complimented by the mobile nature. Samsung Knox is mostly focused on security, which is implemented through a specific installation in the products that Samsung produces, specifically mobile devices. Real-time kernel protection and secure boot, for example, keep the device safeguarded from the time when it is switched on. Specifically, Knox also provides data separation solutions to enable one to do both work and personal on one device in health care. Security features at this level are most useful in the clinical environment where mobility in accessing EHRs and telemedicine services is increasingly gaining popularity.

2.5. Regulatory Requirements

Healthcare organizations must adhere to strict rules in handling patient information to enhance privacy and avoid the law's consequences. The Health Insurance Portability and Accountability Act (HIPAA) in the United States has set several rules concerning the administrative, physical and technical requirements on how patient data should be secured and protected. HIPAA compliance also assists in protecting patient information and referring such information to those personnel who are legally allowed to access it. Similarly, the EU's General Data Protection Regulation (GDPR) guarantees overarching privacy rights such as the right to data access, correction, and portability. GDPR dictates that data controllers and processors should have robust measures in place for the protection of data and also report any breaches without delay. They show that healthcare facilities require strict security measures to be

implemented per their requirements.

2.6. Existing Security Models

Although several frameworks can offer general security, most models lack the capability to adapt to today's threats. Previous security solutions include working with traditional security measures, which are often ineffective in the case of zero-day attacks when an attacker does not have to stick to the standard patterns of behavior as is with viruses, Trojans, etc. One is oriented to the hybrid scenario, when endpoints are present in different systems, including the distributed corporate network, native cloud infrastructure and mobile devices. They, therefore, call for a flexible security system that can recognize and address risks in short time frames. In addition, most of the solutions out there are not integrated and do not have great automation capabilities, which makes it challenging for the security teams to deal with the incidents. An ideal modern security model needs to be proactive and require minimal constant updates from time to time depending on new trends, and most importantly, it needs to support a large number of end-point devices as the security threats hit them

3. Methodology

3.1. Proposed Framework

The suggested security framework will cover all protection needs concerning healthcare systems at the user level, authentication systems, endpoints, networks, and secure cloud services. [12-15] Every one of the layers described has its special function of maintaining the protection of healthcare data and adherence to the norms of current legislation.

- **User Device**: The user device represents the primary entry point in terms of information technology in the healthcare systems environment. It can include fixed workstation x86 PCs, blond laptops, tablet devices or smartphones used by the healthcare personnel in accessing Electronic Health Records (EHRs) and other reference patient information. Such devices must also have an enhanced level of access control that should not put them at risk of threats while at the same time having the basic security settings for the health facilities that are located in remote areas or those that are mobile.

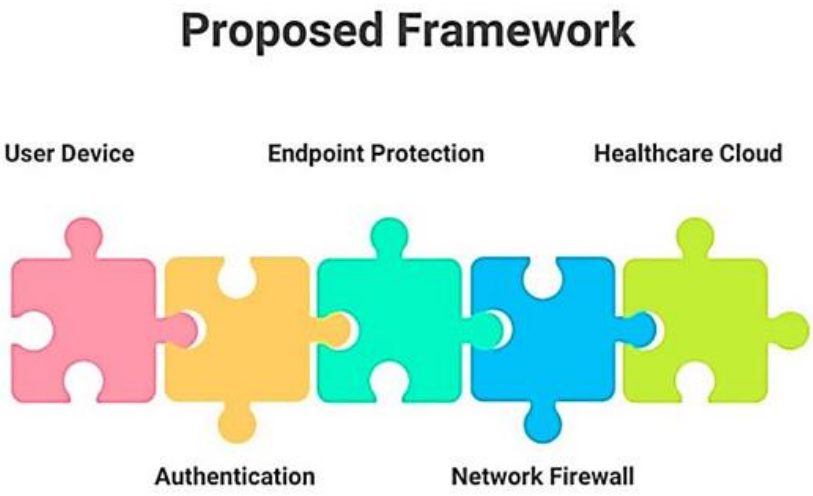

Fig 2. Proposed Framework

- **Authentication**: Authentication can be regarded as an initial barrier that controls who has access to the healthcare applications and network. Additional protective measures such as MFA biometric login, or smart card access are essential to avoid the vulnerability of being phished or to have the credentials stolen.
- **Endpoint Protection**: Endpoint protection works as an additional safeguard since threats that may arise within the device are recognized, prevented, and contained. Programs such as antivirus, anti-malware and EDR also keep the device on watch for the activities related to the subsequent steps. This is particularly so in healthcare facilities since endpoints can be breached or infected with ransomware.
- **Network Firewall**: It is a network device that separates the internal network of a healthcare entity from other networks. This is important since it will control the traffic that enters or exits the network per the specified security policies to deny access to unauthorized entities' advancement of threats and allow only secure communication traffic to and from the network. It also may include Intrusion Prevention Systems (IPS) used in the more rigorous traffic scanning.
- **Healthcare Cloud**: It is an essential element for providing services, some of which include EHRs, patient portals, imaging databases, and many others. Encryption should be used to secure cloud infrastructure because the data within such infrastructures must be protected. Adherence to standards such as HIPAA and GDPR

is also important because most cloud operations employ much patient data.

3.2. Layered Security Approach

The concept known as “defense in depth” provides an overall protection concept in which protective mechanisms are applied at various levels of an IT system. This effectively enhances the fact that even if one layer is bypassed, others are put in place to detect, slow or prevent an invasion. In health care, this multi-tiered approach is imperative to safeguarding important data and maintaining business continuity during clinical practice.

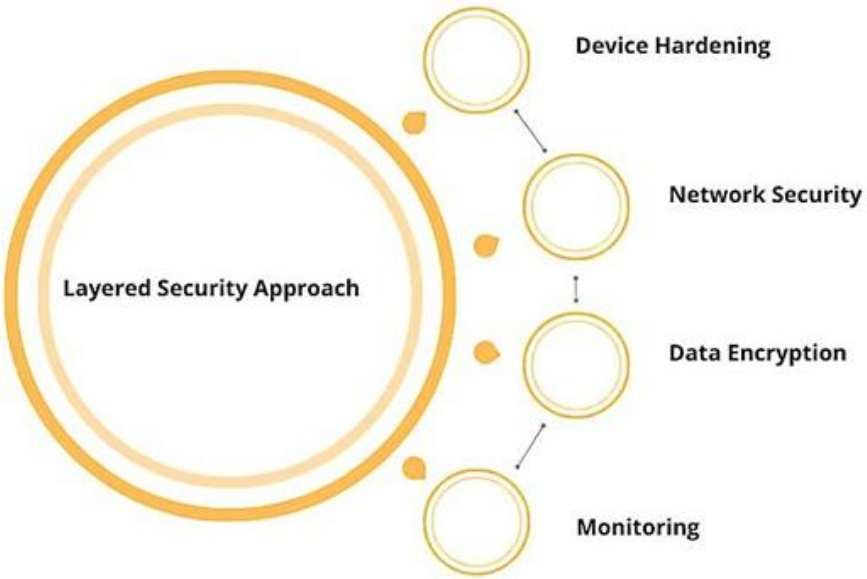

Fig 3. Layered Security Approach

- **Layer 1: Device Hardening**: Device hardening is an extended step of endpoint security in which changes to the device settings are made to provide minimal vulnerabilities for attackers to exploit. One of the most useful utilities developed for using Windows platforms is Group Policy, which enables the administrators to set policies such as password policies, disable ports and services that are not required, and block system functions. On mobiles and Samsung devices, Samsung Knox policies are of great benefit because they allow for securing the boot control, kernel control, and application isolation routines. These steps help to reduce the chances of a local attack or malicious code being lost on a computer system.

- **Layer 2: Network Security**: Network security strives to manage traffic and divide networks into compartments to prevent viruses affecting computer networks from penetrating. VLAN segmentation separates the network into independent areas to minimize the connection between important and other miscellaneous systems from the physical perspective. The organisation can block the attacker's lateral movement in the network to do this. Also firewall is applied to: It is also applied to restrict access and inspection according to the explicitly set rules. In unison, these scripts and processes effectively put barriers around the data and applications that no one with ill intentions should access.
- **Layer 3: Data Encryption**: This implies that they apply AES–two fifty-six encryption for both data at rest and in transit to ensure that patient information is secure and not subjected to unauthorized personnel. Such an encryption level guarantees that even if the data is intercepted or stolen, it cannot be understood without the right decryption code. In the case of healthcare institutions, encryption is mandatory to meet the requirements of the healthcare data protection acts such as HIPAA and to overcome General Data Protection Regulation and in addition, to regain the confidence of patients on digital platforms in the healthcare system.
- **Layer 4: Monitoring**: There is nothing as crucial as monitoring to ensure that security threats are discovered and mitigated immediately. SIEM tools are an asset in gathering logs from the endpoints, network and applications, looking into them for suspicious behaviors, and then providing alerts. SIEM systems give a holistic overview of an environment, help an organization react quickly to threats, and reduce the impact of a compromise or an attack.

3.3. AI-Powered Threat Detection

The use of AI popularly in the recent past and today has been in threat detection, especially with ML models. [16-19] In healthcare, these technologies are becoming crucial when identifying abnormal conduct of devices, which might signify a security concern. Machine learning algorithms can then be trained to analyze all the data produced by endpoint devices, network traffic flows and logs, and user activities to develop a normal system's behaviour profile. Once this baseline is in place, the algorithms can start seeing any variations from the standard averages, including login at different hours, accessing data which should not

have been accessed or an increase of traffic at odd times, which may be due to hackers, malware, or an insider threat. For instance, in healthcare, it is used by the health systems to track the behaviors of the medical devices, workstations, or mobile devices of the healthcare givers. If, for instance, an endpoint is transmitting a high amount of data to an unknown external IP or if there are frequent failed login attempts within some time frame, then the machine learning model can identify it as a potential threat and raise an alert. The first strength of ML-based detection is that it makes it easy for the model to learn from new data and improve the detection ratio by repeating cycles while minimizing false positives. In addition, threat detection systems done through AI are also preferred as they can work in real-time, enabling the organizations to intervene early enough before the threat turns into a huge breach. For this reason, adopting a proactive measure against malicious attacks at times in healthcare institutions, especially with regard to patient information and medical equipment, is advisable. The combination of ED countermeasures with machine learning capabilities improves the total security of systems as it augments the EDR systems in effectiveness and efficiency since the dependency of security teams on having to monitor endpoints decreases significantly.

3.4. Mobile Device Management (MDM)

MDM plays a prominent role in protecting smartphones, especially in healthcare organizations, as most people use mobile devices to use patient data, share information with other caregivers, and manage patients' records. Therefore, in this context, using Samsung Knox Manage can help establish a framework for security policies to be executed on mobile devices, enabling remote management of the devices and improving the security of the devices. The Knox Manage allows the administrators to fully control and manage the mobile devices' security policies, ensuring all the devices used in the organization meet the required standards. In this regard, through this platform, healthcare organizations can set several policies, for instance, requiring a strong password, enabling encryption and controlling the user from accessing certain applications or websites to ensure that data is secured all the time. Samsung Knox Manage's main capability is remote wipe, which allows an IT admin to delete all data on a lost or stolen device and, therefore, deny any chance for patients to get their hands on it. This is particularly drastic in healthcare since mobile device theft raises severe data and compliance law concerns. Organizations can benefit from remote wiping to address some of the challenges experienced mostly with lost or stolen devices, thus ensuring the privacy and security of

patients. Moreover, another capability that is found under the covers of Samsung Knox Manage is geofencing. Geofencing puts restrictions around certain geographical locations to allow the use of devices in limited areas of operation. In healthcare settings, this can be specifically useful for ensuring that only clinical devices are used in medical facilities or clinics and are not used by unauthorized persons in other places. This feature can also be used to limit some of the specific healthcare applications or the patient's record using GPS location, which increases the security of the healthcare application or the patient record in case the device is stolen.

3.5. Risk Assessment and Compliance Auditing

Risk analysis and compliance reviews are critical aspects of protecting a healthcare information technology environment, especially as IT malice increases and compliance becomes more strict. When examining the organization's security plan, the organization should use objective and well-proven models, including the NIST CSF frameworks, to constantly assess the organization's security plan. The NIST CSF is a handy framework that can evaluate cybersecurity risks and develop strategies to address them. Monthly assessments can help healthcare organizations identify any gaps or new threats and risks that have emerged in the month and take corrective action if needed. These include assessments of security controls, security control identification as well as security control adaption to mitigate existing security risks. They also ensure that the organisation's security policies correlate with the developments in cybersecurity. For example, some standards and legislation are mandatory for healthcare businesses, such as HIPAA in the United States and GDPR in the European Union, which require sound protection of patient records. The five FRS requirements mentioned above can be met with the help of automated compliance reporting tools. They can provide the organization with real-time compliance reports to check whether it follows the privacy and security standards of HIPAA and GDPR. There are ways for the system to monitor data access, receive consent from the patients, assess the level of encryption and notify the breaches. Well, this task is done continuously without the need for human interaction. This makes the work of the compliance teams easier and minimizes the chances of errors made by human personnel. On this basis, healthcare organizations can effectively manage their cybersecurity risks and compliance with the required NIST standards through monthly assessments and automatic reporting. These measures also protect patient identity, create documents of records of activity, and keep organizations ready for an external audit or regulatory assessment, which would

create patient confidence and privacy.

4. Results and Discussion

4.1. Simulation Setup

This simulation involved distributing 50 Windows-based laptops and 30 Samsung tablets in a controlled healthcare context to test the effectiveness of the developed security framework. The selection of these devices was due to the fact that they are the most used point in any healthcare facility. These include mock phishing attacks and malware to gauge the effectiveness of an organization's layered security arrangements.

Table 1: Attack Simulation Outcome

Attack Type	Success Rate Before	Success Rate After
Phishing	60%	5%
Malware	45%	3%
Data Theft	30%	2%

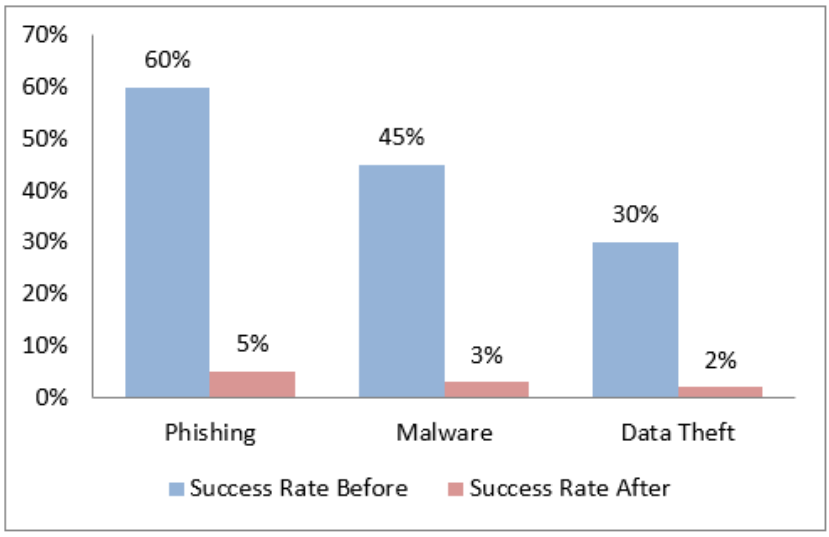

Fig 4. Graph representing Attack Simulation Outcome

- **Phishing**: The results include 60 per cent success of the phishing attacks that, usually include sending fake invoices as messages that aim at making users reveal their password and other account details before our security framework was established.

When agreed upon, layered security measures were implemented and put into practice, such as better filtering of emails, use of artificial intelligence in detecting fake emails and user awareness training on how to combat the emails. The success rate realized by the Phishing attacks drastically came down to only 5 %. The reduction of these numbers proved that the implemented security measures against social engineering attacks efficiently safeguard users.

- **Malware**: Each type achieved this for 100% of its overall goal of infecting a device and potentially stealing or modifying data, with malware attacks, particularly those that target infiltration, initially successful in 45% of the cases. Endpoint protection solutions such as anti-malware software and EDR tools were established in organizations, with an average of 3% in malware attacks. With this increase, it is evident that proactive detection measures and constant monitoring of the systems have gone a long way in containing the impact that malware would otherwise have on healthcare systems.
- **Data Theft:** In the case of data theft, the intruders try to steal sensitive data belonging to the patient and, prior to the increased security measures were successful in 30% of the test attempts. When further measures were implemented, including data encryption, access control, and monitoring tools in network and endpoints, it was reduced to 2%. This has shown the merits of multiple layers of defense mechanisms, including data encryption and restricting access to patient information.

4.2. Performance Metrics

Evaluation of the security framework involved two key factors: Mean Time to Detect and False Positives. These reflect the efficiency and efficacy of the security measures adopted in the organization to know how badly and to what extent the potential threats are recognized.

4.2.1 Mean Time to Detect (MTTD):

Ideally, the MTTD is well-suited for any cybersecurity framework since it can be defined as the time it takes from the moment the threat is detected and the subsequent actions taken. Before deploying the suggested security framework, it used an average of 2 hours to identify an intrusion while the threat penetrates deep and potentially causes much harm to the organization's information system. When the company began to use real-time analytics and AI monitoring tools, detecting them was cut short to fifteen minutes. This extent of enhancement

proves that the continuous automation, incorporation of machine learning, and monitoring of the platform increase the ability to alert users of possible fraudulent activities within a short span. The feature allows the security groups to identify risks early, which means they can act before the threat infects many devices within the network. This can be a major boost in such an environment, which includes the healthcare sector, where seconds matter when safeguarding patient information.

4.2.2 False Positives:

When measuring the capability of the AI security system, it is also important to look out for what comes close to the false positive rates that refer to actual instances of false declarations of an event as a threat. False positives are especially problematic when there are too many of them, as they tie up the security teams and serve as noise regarding actual threats. In the beginning, the system without such integration might have generated alerts for many normal activities that need no investigations. Nonetheless, when an AI model, capable of evolving with time, was put into use, the number of false positives flagged by the system was cut down by 40%. This entails that the security teams will be able to work on actual threats given that they will not be bogged down by false alerts, providing increased efficiency to the security operations. Through adjusting the proposed AI, the distinction between normal activities of the network and potential threats increases as the framework is focused on minimizing false negatives and maximizing the proportion of true positives, which enhances the effectiveness of threat detection.

4.3. Discussion

The data summarised in the tables shown below bring into evidence a general enhancement of the security conditions of the healthcare context after envisaging the layered endpoint security framework. This improvement is particularly relevant regarding the current condition of handling healthcare information since the exposure of this information could be harmful. Real-time analytics, the use of artificial intelligence tools for abnormality detection and the proactive search for threats were also significant factors in managing the effects of cyber threats. Real-time analytics offered the possibility of monitoring and analysing activities when they occurred and reacting to the threats that appeared. This helped to make an improved threat detection system that uses AI algorithms to learn the normal activities of users and devices and alert an organization if it observes unusual behaviors that may signify an attack.

Preventative threat measures also enhanced the pursuit of threats sought and addressed before worsening. This multiple layer of protection greatly diminished the time taken to identify the attacks, as shown by the decline in the Mean Time to Detect (MTTD) from two hours to 15 minutes. The rates of phishing, malware, and data theft attacks sharply declined after putting these measures into practice, proving that these measures are rather efficient in combating specific kinds of attacks. This is especially the case with respect to the healthcare industry, where patient information is often vulnerable to attacks. As the use of these mobile devices grows in healthcare facilities, the implementation of MDM solutions such as Samsung Knox made the environment even more secure. MDM solutions are quite relevant for mobile devices as such devices are more exposed and used in more open environments than PCs. Apart from providing the solution for remote management of devices and the ability to wipe them in case they are lost, Samsung Knox has such features security policy that minimises risks of data breaches associated with lost or stolen mobile devices.

5. Conclusion

This paper acknowledges that the use of Information Technology in hospitals today has brought about many advantages in terms of time, efficacy, patient outcomes, and data handling, among others but also radical new risks of security threats. Since patients' information can be stored and processed on numerous devices, the threat of cybercrimes and data leakage has never been significant. Endpoint security as such does not remain an IT solution; however it becomes the need of the hour to secure this healthcare framework. Our research has therefore established that an Oregon-based security framework designed for used devices, including Windows laptops and Samsung tablets, can change the whole outlook towards cybersecurity in healthcare. The layered security also includes components such as real-time threat monitoring, AI anomaly detection, and proactive threat hunting, thus greatly improving the ability to discover and mitigate threats in real-time. Real-time analytics, in particular, provide the advantage of constant vigilance of the activities happening in the network and the users interacting with the network and devices to alert the security teams the instant an anomaly is recognized. It further enhances threat detection by getting used to how every device behaves and alerting the system if there is a shift from normalcy, making detecting intrusion less likely. Such an aggressive stand assists healthcare organisations in shifting the Mean Time to Detect (MTTD), which threats from hours to minutes, enhancing the effectiveness of response in cyber incidents and

mitigating the resultant harm.

Data encryption and compliance automation are other important roles in ensuring healthcare organizations comply. This is evidenced by the research findings that imply that encryption decreases the risks of data theft in storage and transmission and consequently shields patient data from illegitimate access. Thus, automated compliance auditing tools allow healthcare providers to get the current security compliance status with the regulatory regulations and save time. In addition, with mobile applications in managing patients' health and administrative work, Mobile Device Management (MDM), such as Samsung Knox, is very helpful in protecting devices that are fairly vulnerable to security attacks since they are portable. Some other features include remote management of mobile devices, the option to wipe data off lost or stolen devices, and the application of security policies to mobile devices, providing them with ways of managing risk, a severe healthcare issue.

Therefore, the study supports the idea that healthcare organizations can benefit from a multi-tiered proactive, active mobile- and cloud-friendly and context-aware security system to help secure and protect patient data confidentiality, integrity, and availability. Due to the continuously growing threat levels, keeping the end-user endpoint protected is more important than ever. In doing so, healthcare organizations can not only achieve the objective of safeguarding the information but also gain the confidence of the patient so that the information that they provide will be safe in a current complex digital environment.

References

[1] Uzzaman, A. (2018). End-point information security in the healthcare industry. International Journal of Engineering & Technology, 7(4.36), 338-349.

[2] Martin, P. D. (2016). Securing medical devices and protecting patient privacy in the technological age of healthcare (Doctoral dissertation, Johns Hopkins University).

[3] Taylor, K., Smith, A., Zimmel, A., Alcantara, K., & Wang, Y. (2022, October). Medical Device Security Regulations and Assessment Case Studies. In 2022 IEEE 19th International Conference on Mobile Ad Hoc and Smart Systems (MASS) (pp. 742-747). IEEE.

[4] Clark, U. Y., & Baltezegar, J. G. (2018). Healthcare information security and assurance. Human-Computer Interaction and Cybersecurity Handbook, 257-270.

[5] Brannock, K. A. (2022). Cybersecurity Risk Associated with Endpoint and IoT Devices:

Examining Endpoint Print Device Security (Doctoral dissertation, Marymount University).

[6] Moosavi, S. R., Nigussie, E., Levorato, M., Virtanen, S., & Isoaho, J. (2018). Performance analysis of end-to-end security schemes in healthcare IoT. Procedia computer science, 130, 432-439.

[7] Williams, P. A., & McCauley, V. (2016, December). Always connected: The security challenges of the healthcare Internet of Things. In 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT) (pp. 30-35). IEEE.

[8] Moosavi, S. R., Gia, T. N., Nigussie, E., Rahmani, A. M., Virtanen, S., Tenhunen, H., & Isoaho, J. (2015, October). Session resumption-based end-to-end security for healthcare internet-of-things. In 2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing (pp. 581-588). IEEE.

[9] Walker-Roberts, S., Hammoudeh, M., & Dehghantanha, A. (2018). A systematic review of the availability and efficacy of countermeasures to internal threats in healthcare critical infrastructure. IEEE Access, 6, 25167-25177.

[10] Narayana Samy, G., Ahmad, R., & Ismail, Z. (2010). Security threats categories in healthcare information systems. Health Informatics Journal, 16(3), 201-209.

[11] Rahim, M. J., Rahim, M. I. I., Afroz, A., & Akinola, O. (2024). Cybersecurity threats in healthcare it: Challenges, risks, and mitigation strategies. Journal of Artificial Intelligence General Science (JAIGS) ISSN: 3006-4023, 6(1), 438-462.

[12] Aljuraid, R., & Justinia, T. (2022). Classification of challenges and threats in healthcare cybersecurity: a systematic review. Advances in Informatics, Management and Technology in Healthcare, 362-365.

[13] Spanakis, E. G., Bonomi, S., Sfakianakis, S., Santucci, G., Lenti, S., Sorella, M., ... & Magalini, S. (2020, July). Cyber-attacks and threats for healthcare–a multi-layer thread analysis. In 2020 42nd Annual International Conference of the IEEE Engineering in Medicine & Biology Society (EMBC) (pp. 5705-5708). IEEE.

[14] Jung, S. J., Myllylä, R., & Chung, W. Y. (2012). Wireless machine-to-machine healthcare solution using Android mobile devices in global networks. IEEE Sensors Journal, 13(5), 1419-1424.

[15] Mohapatra, D. P., Mohapatra, M. M., Chittoria, R. K., Friji, M. T., & Kumar, S. D. (2015). The scope of mobile devices in health care and medical education. International Journal of Advanced Medical and Health Research, 2(1), 3-8.

[16] Wang, B. X., Chen, J. L., & Yu, C. L. (2022). An AI-powered network threat detection system. IEEE Access, 10, 54029-54037.

[17] Prince, N. U., Faheem, M. A., Khan, O. U., Hossain, K., Alkhayyat, A., Hamdache, A., & Elmouki, I. (2024). AI-powered data-driven cybersecurity techniques: Boosting threat identification and reaction. Nanotechnology Perceptions, 20, 332-353.

[18] Moosavi, S. R., Gia, T. N., Nigussie, E., Rahmani, A. M., Virtanen, S., Tenhunen, H., & Isoaho, J. (2016). End-to-end security scheme for mobility-enabled healthcare Internet of Things. Future Generation Computer Systems, 64, 108-124.

[19] Arefin, S. (2024). Strengthening Healthcare Data Security with Ai-Powered Threat Detection. International Journal of Scientific Research and Management (IJSRM), 12(10), 1477-1483.

[20] Yaqoob, T., Abbas, H., & Shafqat, N. (2019). Integrated security, safety, and privacy risk assessment framework for medical devices. IEEE journal of biomedical and health informatics, 24(6), 1752-1761.

[21] Elahi, B. (2021). Safety risk management for medical devices. Academic Press.