International Journal of
Technology and
Systems
(IJTS)

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

Journal of Technology and Systems
ISSN: 2788-6344 (Online)
Vol. 7, Issue No. 4, pp 36 – 49, 2025
www.carijournals.org

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

Anjan Kumar Gundaboina

Senior DevsecOps and Cloud Architect, USA.

https://orcid.org/0009-0008-0298-1195

Accepted: 29th Apr, 2025, Received in Revised Form: 29th May, 2025, Published: 29th June, 2025

Abstract

Purpose: This work also involves conducting an assessment and improvement of endpoint defense initiatives in healthcare facilities, especially when it comes to cybersecurity issues with Windows types of workstations and Samsung medical/mobile devices. It touches on the growing danger of cyberattacks on patient records and the healthcare system caused by digitalization in the healthcare industry.

Methodology: The study presents a mixed-methods research design, where a complete vulnerability landscape, threat vectors and endpoint security products within healthcare settings will be reviewed. It invokes both simulation-based testing and empirical analysis to check the efficacy of a suggested multi-layered endpoint security architecture that is industry-specific to Windows and Samsung devices.

Findings: The suggested security model that incorporates the methods of encrypted storage, biometrics authentication, partitioned networking structure, and AI-based threat persistence identification augments ransomware, phishing, data misappropriation, and insider attacks considerably. The solution is then based on complying with the most important data protection standards, such as HIPAA and GDPR and shows a significant increase in endpoint resilience in simulations and practice tests.

A unique contribution to theory, practice, and policy: This study provides a new, flexible, next-generation endpoint defence model with healthcare systems in mind. It enhances cybersecurity practice proficiency by combining AI threat detection, asset-specific policies, and risk assessment conducted on a regular basis. The policy states that regulatory guidelines should be enhanced to require enhanced endpoint protection and achievement of a proactively focused cybersecurity culture at healthcare institutions.

Keywords: *Endpoint Security, Healthcare Cybersecurity, Patient Data Protection, Windows Security, Samsung Knox, Medical Device Security, HIPAA, GDPR, Threat Detection, Mobile Device Management (MDM)*

1. Introduction

Information technology has become increasingly integrated into healthcare as Electronic Health Records (EHRs) have become ubiquitous, mobile health apps have proliferated, telemedicine is being increasingly employed, and connected health devices have entered widespread use. It is an open secret that this shift to the digital space has boosted efficiency and has improved patients' treatment outcomes while concurrently posing a myriad of risks to healthcare providers.

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

Another prerequisite in the healthcare field is the proper protection of patient data, especially Windows laptops and the use of Samsung mobiles. These are common in healthcare facilities, making the probability of the attack high. Given the fact that patient information is considered rather personal and the ever-expansion of the IoT means a lot of devices 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.

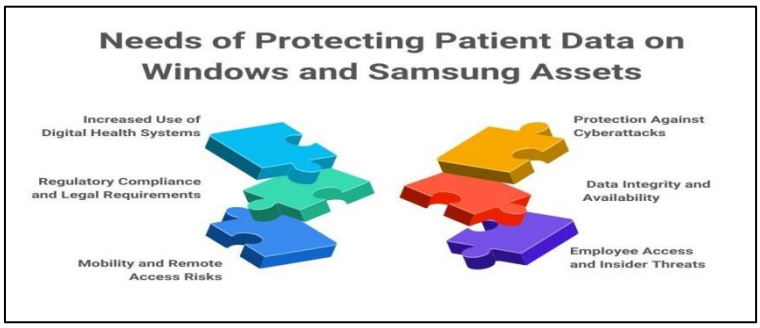

Figure 1:Needs of Protecting Patient Data on Windows and Samsung Assets

- **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 either Windows-based devices 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 kind of 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 organisations are governed by specific legislation, such as HIPAA in the USA and GDPR in Europe, among others. These policies require that patient information be protected and that any violation of this information is considered a violation of the law, potentially resulting in severe consequences, including penalties and loss of business. Since both 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 a 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 alongside nurses together with 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 risk of being lost or stolen outside controlled networks. Data protection on Samsung Knox devices remains secure because this mobile security solution protects information during times of theft and loss, as well as when unauthorised users attempt to access it. The protection of sensitive data requires endpoint protection on all remotely used Windows laptops, as these 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 alongside data exfiltration and malware and phishing incidents. Criminals take advantage of 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 require endpoint security systems that include 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, which eliminates the extent of a security breach.
- **Data Integrity and Availability:** The healthcare sector requires both exact patient data and easy data access at all times. Medical choices that healthcare workers must make depend on accurate patient records and their most recent updates. Results from patient data compromise, data corruption, or data 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 combined with Samsung devices mandate that data integrity should be given top priority. Patient data requires encryption security, alongside stable data storage and 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 both outside attackers and unauthorized hospital staff members. Trusted employees and 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 the core functions of these systems. The rapid growth of digital technology adoption in healthcare has led to a massive expansion of laptop, smartphone, tablet and medical device use in both 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 serve as fundamental targets for cybercriminals who want to steal medical information while disrupting healthcare facilities and executing ransomware tactics. 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, ensuring continuity in the event of hardware loss, theft, or when devices face compromise. The Mobile Device Management solution, named Samsung Knox, proves essential for healthcare staff by providing remote device deletion, along with location tracking boundaries and enforced security rules that protect sensitive information from unauthorised use and theft. Patient data located in healthcare devices makes these devices particularly vulnerable to cyberattacks due to their sensitive nature. The implementation of multi-factor authentication, security audits and access control systems protects data from breaches when used on these healthcare devices. A thorough endpoint security plan requires healthcare staff education on the protection of devices and threat recognition to achieve comprehensive defence 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 various connected devices, such as laptops, desktops, mobile phones, and tablets, that interact with central networks. Man-made devices, known as 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. EDR systems grant security teams the needed visibility together with response tools to track endpoint anomalies, which

allows 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 utilises malicious software to prevent users from accessing their information unless they pay a ransom, which often disrupts healthcare delivery operations. The illegal removal of patient records by attackers through data exfiltration results in privacy breaches as well as 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's preference for Microsoft Windows, especially older and unpatched versions, is because the operation system is commonly used globally. Another example is EternalBlue, which was to exploit the Microsoft SMB protocol which was 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, and 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 on the rise in healthcare facilities because of their enhanced security measures complimented by their mobile nature. Samsung Knox is primarily focused on security, which is implemented through a specific installation on Samsung's products, 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 so as 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 have to adhere to strict rules in handling patient's information to enhance patient privacy as well as 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. In the same regard, the General Data Protection Regulation (GDPR) in the EU 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 as per their requirements.

2.6. Existing Security Models

Although there are several frameworks that can offer general security, most models lack the capability to adapt to today's threats. Previous security solutions have included working with traditional security measures, which are often ineffective in the case of zero-day attacks, where an attacker does not adhere to standard patterns of behaviour, as seen with viruses, Trojans, etc. One of them is oriented towards the hybrid scenario, where 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 they are hit by security threats in real-time.

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, as well as secure cloud services. 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.

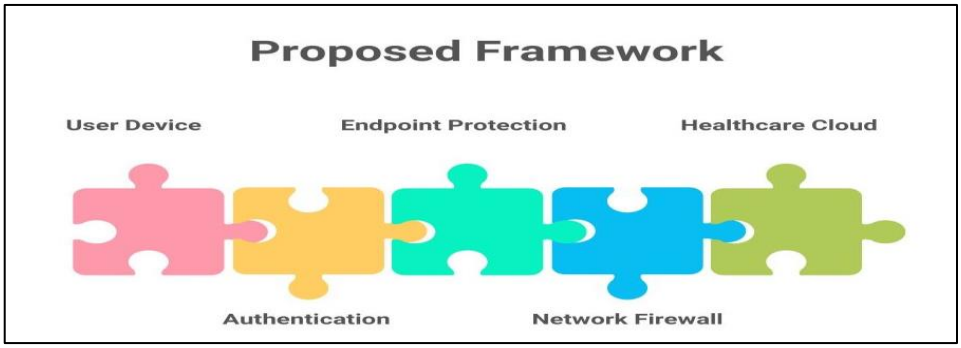

Figure 2: Proposed Framework

- **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 healthcare personnel to access 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.

- **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 having 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:** 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 as per the specified security policies in a bid to deny access to unauthorized entities and advancement of threats and allow only secure communication traffic to and from the network. It also may include Intrusion Prevention Systems (IPS) that are 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 handle a significant amount of 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 is effective in enhancing the fact that even if one layer is bypassed, others are put in place to detect, slow or prevent an invasion. In the context of healthcare, this multi-tiered approach is imperative for safeguarding important data and maintaining continuity of business during clinical practice.

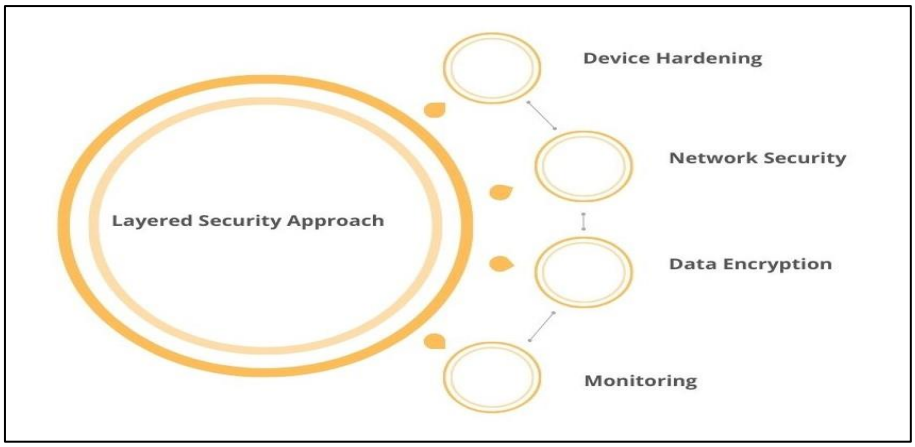

Figure 3: Layered Security Approach

- **Layer 1: Device Hardening:** Device hardening is an extended step of endpoint security in which changes to the settings of the device 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 services which are not required as well as 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 reduce the chances of a local attack or malicious code being introduced into a computer system.
- **Layer 2: Network Security:** In fact, 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. To do this, it gives the organization the capability to block lateral movement of the attacker in the network. Also firewall is applied to: It is also applied in order to achieve the goal of restricting access and inspection according to the explicitly set rules. In unison, these scripts and processes effectively put barriers around the data and applications that should not be accessed by anyone with ill intentions.
- **Layer 3: Data Encryption:** This implies that they apply AES-256 encryption for both data at rest and data in transit to ensure that patient information is secure and not subject to unauthorised 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 healthcare data protection acts such as HIPAA to overcome the 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 the monitoring done to ensure that security threats are discovered and mitigated immediately. SIEM tools are an asset in that they gather logs from endpoints, networks, and applications, analyse them for suspicious behaviours, and then provide alerts. SIEM systems give a holistic overview of an environment and help an organization react quickly to threats and reduce the impacts of the 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 the use of ML models. In the context of healthcare, these technologies are becoming crucial when it comes to the identification of abnormal conduct of devices, which might signify a security concern. Machine learning algorithms can then be trained to analyze all the data being produced by endpoint devices, network traffic flows and logs, as well as user activities, to be able to develop a behavior profile of a normal system. 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 as a way of tracking the behaviors of the medical devices, workstations, or mobile devices of the healthcare givers. For instance, if an endpoint is transmitting a high volume of data to an unknown external IP address or if there are frequent failed login attempts within a certain time frame, 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, and this will enable the organizations to intervene early enough before the threat turns into a huge breach. For this reason, adopting proactive measures against malicious attacks in care institutions, especially regarding The combination of ED countermeasures with machine learning capabilities, improves the total security of systems as it not only augments the EDR systems in effectiveness but also efficiency as well 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 the protection of 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 be helpful in establishing a framework for executing security policies on mobile devices, enabling remote device management and enhancing device security. The Knox Manage allows the administrators to fully control and manage the security policies of the mobile devices, which would ensure all the devices that are 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 that of 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 the healthcare industry, as mobile device theft raises severe concerns regarding data security and compliance with laws. Organizations can benefit from remote wiping as a way of addressing 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 aims to put restrictions around specific geographical locations, allowing the use of devices in limited areas of operation. In the settings of healthcare, this can be specifically useful for making certain 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 specific healthcare applications or a patient's record using GPS location, which increases the security of the healthcare application or 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 continues to increase and compliance standards become more stringent. When it comes to the examination of the organization's security plan, the organization should use objective and well-proven models, including the

NIST CSF frameworks, for the constant assessment of the organization's security plan. The NIST CSF is a handy framework that can be used to 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 course of 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 make sure that the security policies of the organization correlate with the developments in the field of cybersecurity. For example, there are some standards and legislation that are mandatory for healthcare businesses, for example, HIPAA in the United States and GDPR in the European Union, which require sound protection of the patient's 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 the organization is following the privacy and security standards of HIPAA and GDPR. There are ways for the system to monitor data access, receive consent from patients, assess the level of encryption, and notify of breaches. This task is performed continuously without the need for human interaction. This not only makes the work of the compliance teams easier but also minimizes the chances of errors that may be 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 confidence and privacy for the patients.

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 the use of mock phishing attacks and malware so as 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%

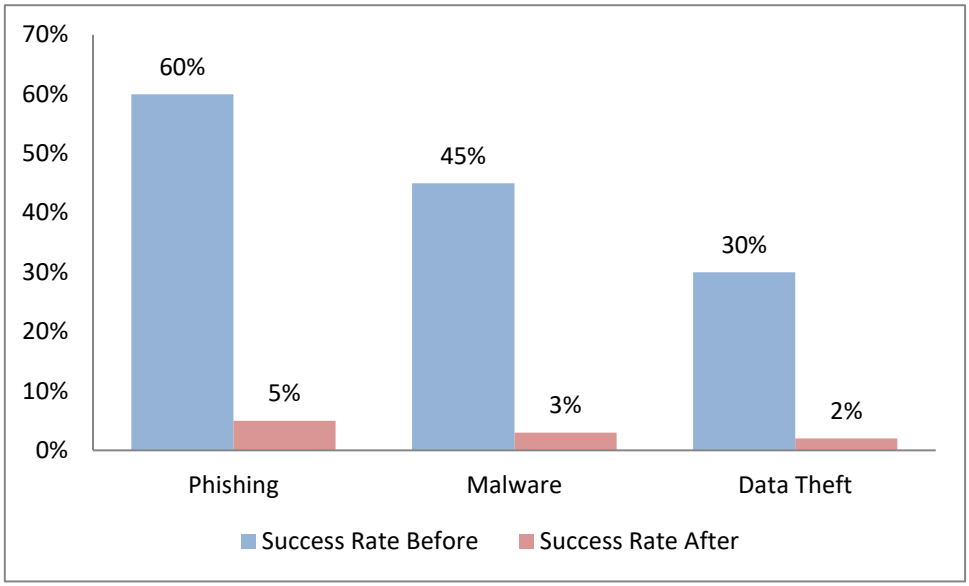

Figure 4: Graph representing Attack Simulation Outcome

- **Phishing:** The results include 60 percent success of the phishing attacks, 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 are efficient in safeguarding users.
- **Malware:** Each type was able to achieve this for 100% of its overall goal of infecting a device and potentially stealing or modifying data, with malware attacks, in particular, that target infiltration initially being successful in 45% of the cases. Endpoint protection solutions such as anti-malware software, as well as EDR tools, were established in organizations, with an average of 3% in malware attacks. With this increase, it is evident that proactive detection measures, together with 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 put in place, including encryption of data and access control and monitoring tools in network and endpoints, it 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.

- **Mean Time to Detect (MTTD):** Ideally, the MTTD is well-suited for any cybersecurity framework, as it can be defined as the time it takes from the moment the threat is detected to the subsequent actions taken. Prior to the deployment of 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 real-time analytics and AI monitoring tools were introduced within the company, the time it took to detect them was reduced 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 gives the security groups the ability to identify risks early, and this means that they can act before the threat infects many devices within the network. In such an environment, which includes the healthcare sector where seconds matter when it comes to safeguarding patient information, this can be a major boost.
- **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 a problem when there are too many of them, as they tie up the security teams and serve as noise in terms of 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, which is capable of evolving with time, was put into use, the number of false positives which were flagged by the system was cut down by 40%. This entails that the security teams will be in a position to address actual threats, as they will not be bogged down by false alerts, thereby 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 over-electiveness 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 in terms of 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 performing activities monitoring and analysis at the moment when they occurred and reacting to the threats which 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, which were sought out and addressed before they worsened. This multiple layer of protection greatly diminished the time taken in the identification of 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, makes the environment even more secure. MDM solutions are particularly relevant for mobile devices, as these 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 features and a security policy that minimises the risks of data breaches associated with lost or stolen mobile devices.

5. Conclusion

The use of Information Technology in healthcare has largely enhanced the level of efficiency during operations, patient treatment and maintenance of data, but it has also posed tremendous cybersecurity challenges. The complexity of the system where the data of patients is stored and processed on endpoint devices has risen, and securing endpoints is important. This research proves that a tiered endpoint security infrastructure which involves real-time breach detection, anomaly detection based on AI and encryption of data can significantly improve healthcare cybersecurity. Specifically, for the more common devices commonly used in an organisation, such as Windows laptops and Samsung tablets, customised solutions like Mobile Device Management (MDM) and compliance automation enhance defence within an organisation. Not only do these tools decrease the chances of breaching data, but they may also assist healthcare organizations in complying with the regulations. On balance, endpoint protection that is proactive means a significant reduction in the time of threat discovery and responding to it, which minimizes damage caused and strengthens patient confidence.

Recommendations:

- Install a layered endpoint security network that contains applications for threat detection, behavioral analytics, and real-time tracking.
- Employ Mobile Device Management (MDM) tools such as Samsung Knox to protect portable devices and apply security policy remotely.
- Encrypt data such that both data in storage processes and transmission are done in an encrypted form to prevent unauthorized access to patient data.
- Introduce automatic compliance audit tools to follow the requirements of such standards as HIPAA and GDPR.
- Establish a security-first mindset in healthcare facilities, including the focus on constant risk evaluations and employee education.

References

1. SANS Institute. (2020). *Endpoint Security: A SANS Survey*. Retrieved from https://www.sans.org
2. Symantec. (2021). *Internet Security Threat Report*. Retrieved from https://www.broadcom.com
3. Trend Micro. (2022). *EDR Solutions: Capabilities and Best Practices*. Retrieved from https://www.trendmicro.com
4. Ponemon Institute. (2021). *The Impact of Ransomware on Healthcare*. Retrieved from https://www.ponemon.org
5. U.S. Department of Health and Human Services (HHS). (2023). *Cybersecurity Best Practices for Healthcare*. Retrieved from https://www.hhs.gov
6. Verizon. (2023). *Data Breach Investigations Report (DBIR)*. Retrieved from https://www.verizon.com/business/resources/reports/dbir/
7. Kaspersky. (2021). *Threats to Healthcare IT Infrastructure*. Retrieved from https://www.kaspersky.com
8. Microsoft. (2017). *Customer Guidance for WannaCrypt attacks*. Retrieved from https://blogs.microsoft.com
9. Europol. (2018). *The Impact of the EternalBlue Exploit*. Retrieved from https://www.europol.europa.eu
10. Samsung. (2024). *Samsung Knox White Paper*. Retrieved from https://www.samsungknox.com
11. Deloitte. (2020). *Mobile Device Security in Healthcare*. Retrieved from https://www2.deloitte.com
12. U.S. Department of Health and Human Services (HHS). (2013). *HIPAA Security Rule*. Retrieved from https://www.hhs.gov/hipaa
13. European Union. (2016). *General Data Protection Regulation (GDPR)*. Retrieved from https://eur-lex.europa.eu
14. Gartner. (2021). *Adaptive Security Architecture for Endpoint Protection*. Retrieved from https://www.gartner.com
15. IBM Security. (2022). *X-Force Threat Intelligence Index*. Retrieved from https://www.ibm.com/security/data-breach/threat-intelligence