Application Protection Platforms (CNAPP) for Healthcare: Safeguarding Patient Data in Cloud Infrastructure

Anjan Gundaboina

Senior DevsecOps and Cloud Architect
USA.
anjankumar.247@gmail.com

Abstract:
The growth of cloud usage in the healthcare sector provides flexibility, scalability, and cost advantage, which is hard to find anywhere else but poses security threats. The primary issues are ensuring the privacy of patients' information, following laws such as HIPAA and maintaining the availability of services. CNAPPs can be defined as an effective solution for consolidating services, including Cloud Security Posture Management (CSPM), Cloud Workload Security Protection Platform (CWPP), and even Kubernetes Security Posture Management (KSPM). This paper will seize the opportunity to provide a comprehensive insight into CNAPPs in the healthcare environment regarding such issues as EHRs, medical imaging data and healthcare apps in cloud environments. We discuss the architectural structures and specifications of CNAPPs, their integration with strategically important healthcare IT assets and infrastructure, and present simulation results. Further, to support these findings, it also shows actual-world cases of CNAPP's application, describes practices for optimizing CNAPP implementation, and suggests application-specific methods for the healthcare sector. The findings show that integrating the cloud-native security framework can help in the fight against the current and future threats in the healthcare sector.

Keywords: CNAPP, Healthcare Security, Cloud Infrastructure, CSPM, CWPP, Data Encryption, Cloud-Native Security.

1. INTRODUCTION

Especially in the current era of digital health transformation, the cloud has become crucial to support healthcare operations related to greater efficiency, data management, and sharing as part of collaborative care. It enables services like telemedicine, EHR, mobile-based health application, [1-4] AI based diagnosis etc. However, it is worth stating that moving to the digital environment also opens up new attack opportunities.

1.1. Emergence of CNAPP

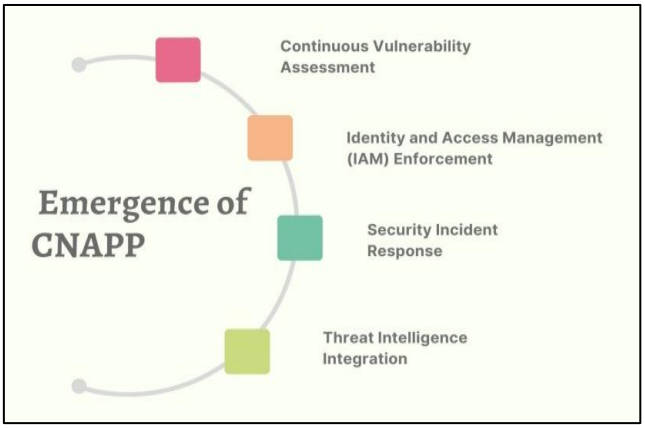

Fig 1. Emergence of CNAPP

Cloud-Native Application Protection Platforms (CNAPPs) are an amalgamation of products that work as a more comprehensive framework which guarantees protection from end to end. CNAPP capabilities include:

1.1.1. Continuous Vulnerability Assessment:

Ongoing scanning is a maneuver that has been integrated into CNAPPs since it helps organizations perform vulnerability scanning continuously to identify blind spots in the cloud systems. While most security programs conduct scans at intervals to inspect the system, CNAPP scans vulnerabilities and cleans up the system in real-time. This proactive approach meant that threats such as in applications, containers, and cloud configurations were identified before damaging results from acts of hackers were realized. This is much more important in healthcare, as patient data has to be shielded from novelties to protect against breaches of regulations such as HIPAA.

1.1.2. Identity and Access Management (IAM) Enforcement:

Implementing proper IAM is important in allowing only relevant users and systems access to sensitive health information. CNAPPs incorporate IAM policies using strong authentication mechanisms, user roles, and control models in cloud-natured apps to achieve these points. This includes the least privilege principle whereby users are given the least access privilege needed in carrying out their tasks. When implemented in the cloud environments, these controls help the CNAPPs maintain the patient data and other vital health care information secure regardless of where they are located or accessed.

1.1.3. Security Incident Response:

Security incident response is one of the critical features offered by CNAPPs to detect, contain or minimize the repercussions of security threats. CNAPPs include features that allow them to take prompt action as soon as there is a suspicion of an incident or after an incident has been spotted. Thus, the gap between the two stages is short. Thus, for healthcare organizations, timeliness is always of the essence in order to reduce the time taken and ensure the patient care systems do not face disruptions. CNAPPs can orchestrate with futures, enhance information sharing, and perform subsequent operations such as system isolation, traffic cessation, or data rollback, among other actions. This capacity helps to effectively respond to cases that occur so that they cause little disruption to the functionalities of the organization.

1.1.4. Threat Intelligence Integration:

Solutions for threat intelligence are another key component of CNAPP since they enable the systems to obtain constantly updated information about threats, pathways, and risks. CNAPPs collect threat intelligence data from external sources such as vendors, public databases, and threat-sharing organizations to improve their security posture. In healthcare, bearing in mind that cyber threats are not constant and will change makes it possible for CNAPPs to adapt to the new threats and apply the new security measures instantly. Related to that, CNAPPs can prevent connections to well-known malicious IPs and benefit from extensive experience identifying signs of unreported threats, including zero-day attacks, to safeguard cloud-native applications and workloads. This flexible defense capability enhances the general security plans and ensures that healthcare institutions can work adequately amid growing threats.

1.2. Challenges in Healthcare Cloud Security

Since healthcare systems manage a large volume of sensitive data, [5,6] many are exposed to cyber threats. Key security challenges include:

1.2.1. Unauthorized Data Access:

The main concern about the healthcare industry is that hospitals and other healthcare facilities possess a lot of data as well as information that patients present to the facilities during their health check-ups. This means that one can easily access and misuse this data by forging their identity or defrauding individuals or institutions seeking the website's services. Cybercriminals threaten healthcare organisations by compromising or hacking access control or phishing, credential stuffing, and insiders. It maps to the need for stronger identity and access management since most healthcare institutions have moved to cloud infrastructure, and as critical decision-making tools are migrated to the cloud, stronger authentication, the least privilege, and constant monitoring should be incorporated to reduce cases of unauthorized access to patient’s information.

1.2.2. Ransomware Attacks:

Ransomware attacks are among the healthcare system's most pressing problems. Ransomware is malware that aims to lock down the files and opt for monetary rewards in the form of decryption tokens. These attacks not only interfere with the normal functioning of hospitals by making patient records inactive but may also cause a significant loss of money and discredit an institution. The introduction of ransomware in healthcare systems is perilous to these organizations because they require constant access to data to provide services in response to medical emergencies and because records are highly valued in the black market. Proper security measures such as backup, network segmentation, and endpoint security can help prevent such attacks and provide staff awareness to look out for false emails, which are used in introducing the ransomware to the network.

1.2.3. Misconfigured Cloud Storage:

Cloud storage misconfigurations are arguably the most prevalent security menace that most healthcare firms face since these mistakes expose data to unauthorized access. Most of the time these misconfigurations arise as a result of inadequate configurations of cloud services or excessive permissions granted. Incorrect storing PACS on clouds can result in inadvertent disclosure of information, where specific patient details can be viewed freely or by people without permission to view them. From this, healthcare organizations on the cloud need constant monitoring of the environment, control of access, and other features that enable them to detect and solve misconfigurations on the cloud so that the data being used will always be secure and in compliance with the regulations.

1.2.4. Compliance Violations:

Healthcare organizations are bound by the legal requirements such as HIPAA, GDPR, and HITECH act obligation to safeguard the patient's data and information. These regulations have severe consequences if not adhered to, as compliance may lead to fines, legal suits, and a loss of clients among patients. But, it is relatively easy to say that managing compliance is a complicated process in the cloud environment. Since cloud infrastructures are malleable and the third-party service providers might also be intricate for compliance management, the regulatory requirements are evolving. These should be followed by continued security measures incorporated in compliance procedures, automated compliance monitoring, and staff training to keep in touch with the current laws. It becomes paramount for the healthcare organization to determine and implement solutions that align its operations with the frameworks to minimize incidences of compliance failures.

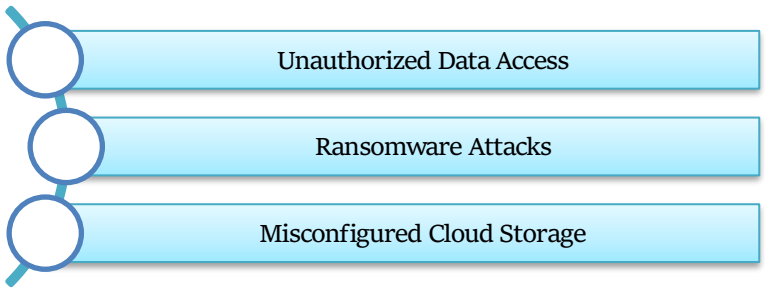

Fig 2. Challenges in Healthcare Cloud Security

1.3. Safeguarding Patient Data in Cloud Infrastructure

This case scenario makes protecting patient information in clouds a moot point for healthcare facilities since the use of clouds has some influence on securing health information. Since cloud environments are scalable, flexible and efficient for healthcare practitioners, they pose threats that result in unauthorized access, breaches, or violation of healthcare compliance. Thus, since patient information is sensitive, it must be protected against cybercriminals who can breach HIPAA or GDPR rules and penalties for violating them. However, when protecting patient data in the cloud, encryption is one of the most significant techniques that can be adopted. Encrypting information at the moment of transmission and storage prevents even those who tried to get unauthorized access from interfering with the data in the cloud. However, there is a critical need to implement strict IAM measures to limit access to data, mainly to users with the authority to access data based on job

descriptions. MFA also extends the effectiveness of these controls because they have an added layer on top of them. There is also a need to monitor the cloud infrastructure regularly since some problems, such as improper configurations, pose risks to patients' data insecurity and susceptibility to cyber threats. In addition, the healthcare organization needs to ensure that the cloud service provider follows the set security standards or certifications. This entails proper storage of data, protection of the application programming interfaces and dealing with an attack correctly. Security issues should also be monitored through periodic vulnerability scans and other security audit exercises to check the cloud infrastructure for any flaws. In this way, the layers of security measures should be implemented by the healthcare organization to ensure that the patient's data will be safe when stored in the cloud and that the organization will not experience data breaches, which can lead to the loss of patient trust and fines that come with violating the rules and regulations of the data's protection.

2. LITERATURE SURVEY

2.1. Cloud Security in Healthcare

Technologies such as cloud computing have impacted the healthcare industry, especially by managing large amounts of patient data. Nevertheless, the increased use of traditional paper-based documentation to automated or computerized documentation has brought this difficult security question. [7-10] Healthcare information compromise incidents are increasing and becoming more serious. Given the importance and sensitivity of its information, such as EHRs, diagnostic reports and personal information, health care is a hot target for cybercriminals. Conflicting security models in cloud services offer inadequate protection since they are based on perimeter-based security and static policies. This is to dispel the traditional security measures and develop more responsive security systems suitable for cloud technology.

2.2. Cloud Security Posture Management (CSPM)

CSPM is an essential aid to identifying misconfigurations within cloud infrastructures, as well as processes to correct them in a dynamic means. CSPM tools are the ones that run nonstop in order to supervise compliance in the cloud computing environment; one needs to adhere to security standards. Gartner in [3] projected that misconfigurations, which include exposed storage buckets IAM settings, are responsible for more than 95% of cloud security breaches. This statistic must be understood as a reference to the need to engage CSPM in anticipating problem identification. From this position, CSPM provides the necessary tool for security given that healthcare organizations need to conform to legal requirements such as HIPAA and similar standards.

2.3. Cloud Workload Protection Platforms (CWPP)

As the name suggests, Cloud Workload Protection Platforms (CWPP) aim to secure workloads running in different models of cloud computing infrastructures, such as VMs, containers, or serverless functions. In healthcare, such workloads can include and are most likely to involve the patient record, laboratory test results, diagnostic images and any other critical information required in daily practice. CWPP solutions are able to offer runtime protection, threat detection, and behavior of every stage for workload types at each stage. They also help the organizational management enforce policies in various organizations to minimize infringement of company policies regarding data leakage and unauthorized users. As with most healthcare organisations, CWPPs are particularly crucial in dynamic fields or where workloads are decentralised and continuously changing.

2.4. CNAPP Overview

CNAPP stands for Cloud-Native Application Protection Platform and is mentioned as the combination of both the CSPM and the CWPP systems. In recent whitepapers, [4]the CNAPP was set as an innovative evolution of cloud security, which provides end-to-end visibility and management of the infrastructure and the applications running in it. It is a CNAPP that covers the entire DevOps lifecycle, and means that security is built into the developers' pipelines. CNAPPs are, therefore, an excellent solution by integrating posture management, workload protection, and runtime security. This integrated model will be particularly useful for organisations in the healthcare sector that want to remain compliant, secure, and prepared for new threats.

2.5. CNAPP in Other Sectors

Some industries that face similar security and compliance requirements as the healthcare sector are sectors such as banking and finance which have adopted CNAPP solutions earlier. These sectors have used CNAPPs to help achieve improved threat identification, improve compliance reporting, and keep cloud systems secure. For example, CNAPP aids in the identification of risks, management of information, and streamlining of processes by offering integrative and operational features that help financial institutions handle multiple clouds. Successful CNAPP's deployment in these highly regulated settings proves the worth of CNAPP's today. Healthcare organizations should study the presented implementations to adopt and incorporate the most useful practices and strategies to enhance cloud resilience.

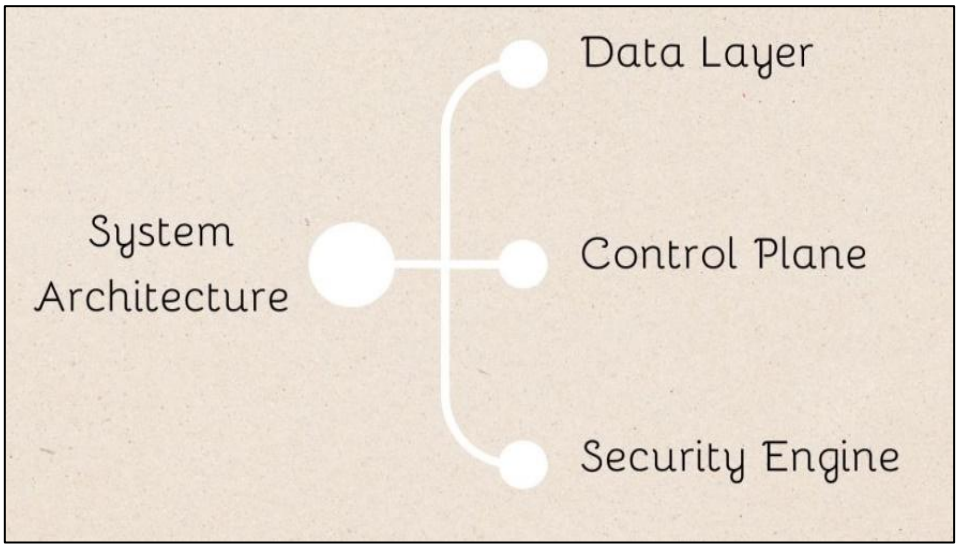

Fig 3. System Architecture

3. METHODOLOGY

3.1. System Architecture

- **Data Layer:** The data layer serves as the bottom layer of CNAPP's architecture, and its primary duty entails working directly with several important healthcare data sources, which are EHR systems, LIS, and other medical applications. [11-14] It also primarily provides a secure means of data streaming into the Xerox environment and enables the real-time monitoring of patient records, diagnostic images and clinical processes. This layer is necessary for data security and privacy and for following the rules and standards set for healthcare industries, such as HIPAA.
- **Control Plane:** The control plane provides security administrators with an interface for managing the app through which cloud security posture and response to incidents on the cloud can be programmed. Its benefit is the possibility of creating a single interface built within integration with the DevOps tools and operating the security processes. Thus, it aids substantially in achieving greater control, improved visibility, and easier management of distributed cloud resources.
- **Security Engine:** The security engine is the neural processing center of the CNAPP, and it deploys machine learning for threat identification, behavioral profiling and real-time anomaly detection. It constantly monitors cloud-hosted workloads and information traffic, searching for signs of threats, vandalism, and malicious behavior. Not only does it cover the aspect of alert generation and handling of potential incidents, but it also provides information about the possible threats and their potential for becoming a serious concern.

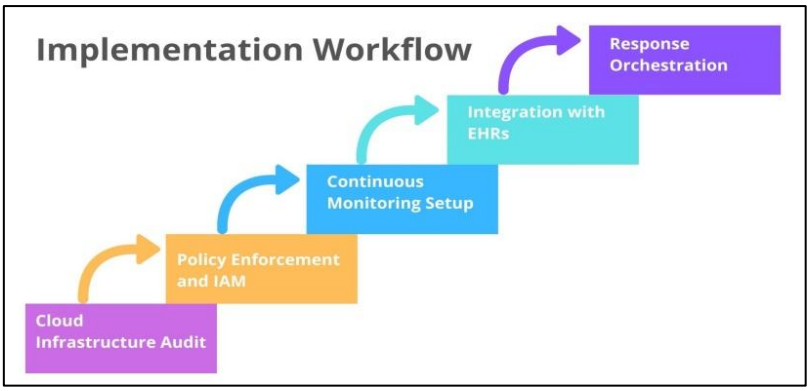

Fig 4. Implementation Workflow

3.2. Implementation Workflow

- Cloud Infrastructure Audit: The first process implemented when an organization deploys CNAPP is the assessment of the current cloud structures. This involves, for instance, discovering all the cloud assets, configurations, and current cloud services. The audit aims to reveal security threats, configuration problems and compliance weaknesses. In a healthcare context, it guarantees that every system hosted in the cloud processing patients' information is identified and tested in relation to compliance requirements.
- Policy Enforcement and IAM: After reviewing the infrastructure, the subsequent stage is to initiate the policy enforcement and IAM structures. This includes the segregation of duties where access is granted based on the principle of least privilege level, practicing multi-factor authentication and adherence to set compliance standards. The effective IAM approach is essential in health facilities due to insiders' increased health information theft.
- Continuous Monitoring Setup: A number of monitoring tools run continuously to monitor the entire cloud environment. These tools record the activities in a system, identify possible threats, and provide alarm when company policies are infringed. Continuous monitoring is being done within both the development and production phases of CNAPP, thus making it possible for the system to monitor threats around the clock and enable quick response.
- Integration with EHRs: One must understand that installation in the healthcare environment requires integration with EHRs and other clinical solutions. It means that while data related to patients is safeguarded, normal workflow is not interrupted. Thus, CNAPP components communicate with EHR databases through secure APIs and encrypted data pipelines in accordance with the protection of privacy laws.
- Response Orchestration: The last step then involves arranging for answers to be made automatically in response to the threats that have been identified. Response orchestration also means that CNAPP can autonomously perform pre-defined actions such as containing workloads, revoking credentials or alerting the security team. In healthcare, it is crucial because, much like in financial organizations, availability must be safeguarded to reduce the impact of incidents on patient care.

3.3. Data Encryption Strategy

The issue of strong encryption is crucial for implementing the CNAPP predisposing the safeguard of health data both in transmission and storage phases. CNAPP platforms collude with a dual encryption mechanism commonly using symmetric and asymmetric encryption to ensure security and efficiency. While traditional DES use two keys, one for encryption and the other for decryption, symmetric encryption is widely applicable to mass storage of large data such as EHRs, diagnostic images and lab reports in clouds through a single applicable key. However, algorithms like AES-256 are used because they are fast and highly resistant to brute force; hence, they can secure vast volumes of data, as in the health sector, without compromising the system's capability. Information exchange, like transferring information between two different EHR systems, a cloud application, medical devices, etc., is usually encrypted using asymmetric encryption. It involves using a public key for encrypting and a private key for decrypting the information and is most suitable when it comes to establishing secure links between distributed systems as well as networks. Each of these protocols is embedded within CNAPP to secure these data streams from eavesdropping, tampering, or intercepting through encryption of communication between the cloud services and the end users, for instance, TLS (Transport

Layer Security). Apart from the basic encryption, some CNAPP systems include Key Management Services (KMS) for securely handling the keys. These services enhance the spinning of keys, access control policies and auditing, thus bolstering the system's security. For various regulations like HIPAA, GDPR, and HITECH – within CNAPP, data encryption ensures unreadable data in the compromised cloud infrastructure. This multilevel approach strengthens patient and stakeholder confidentiality and integrity of health information and ensures that their data is protected against cyber threats.

3.4. Compliance Mapping

3.4.1. Access Control:

The authentication and authorization of information systems are essential to HIPAA, GDPR, and HITECH standards, and CNAPP platforms offer sufficient solutions for these requirements. CNAPP has built a rigorous identity and access management that would prevent unauthorized personnel from accessing healthcare information. [15-19] Control features such as role-based, multi-factor authentication, and privilege escalation alerts assist organizations in enforcing strict user rights. This complies with HIPAA's minimum requirements, GDPR's data protection in design, and HITECH, which requires Information access limitations.

3.4.2. Data Encryption:

Encryption is an integrated need in all three regulations, and CNAPP platforms meet this by ensuring data protection at every step. To achieve this, CNAPP uses symmetric and asymmetric encryption and the data is protected during its transmission and storage. This is important in safeguarding the clients' identity data and health information, respectively. HIPPA's technical calibration is augmented by encryption; implements GDPR's Article 32, and meets HITECH data break prevention standards. Furthermore, CNAPP's key management capabilities are useful in establishing sound encryption policies, including control measures such as access and frequency of key rotation.

3.4.3 Incident Reporting:

Another important compliance aspect is incident reporting; however, the SOPs on how to conduct it are varied depending on the standards. CNAPP uses threat detection, logging, and alerting features consistent with the requirements for breach notification under both HIPAA and GDPR. These instruments enable one to identify, prove and address the security breaches in the early stages. Thus, as mentioned earlier, there are breach notifications under HITECH. However, the implementation guidance for this act is not as progressive as those of the HIPAA and the GDPR; therefore, CNAPP gets a 'Partial' on this one. However, CNAPP considerably shortens response time and ensures that the collected data as an incident is ready for audit, allowing healthcare institutions to remain strategic and legal.

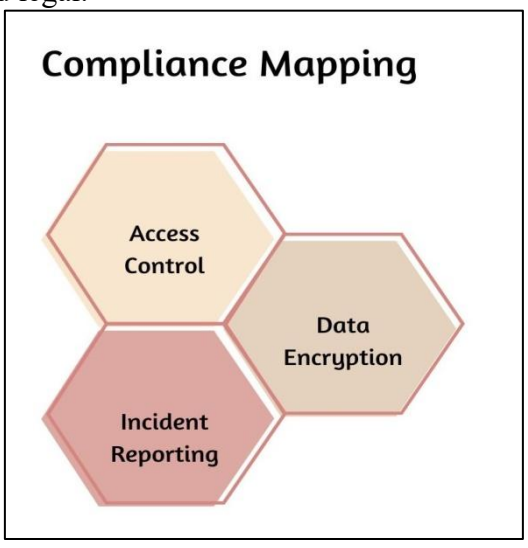

Fig 5. Compliance Mapping

4. RESULTS AND DISCUSSION

4.1. Case Study: Mid-Size Hospital Deployment

A CNAPP solution was introduced to a 300-bed hospital using a hybrid cloud system in such an environment. The deployment was intended to improve the hospital's protection status, bring efficiency to regulatory processes, and minimize cybersecurity-related operational threats. Various metrics that were recorded after the effective implementation of CNAPP are as follows:

Table 1: Case Study: Mid-Size Hospital Deployment

Metric	Improvement
Threat Detection Rate	98%
Reduction in Misconfigurations	85%
Compliance Audit Success	100%

- **Threat Detection Rate: 98%:** At the hospital, CNAPP enhanced the institution's capability to identify threats that threatened the system. With threat intelligence and powerful machine learning capabilities at its core, CNAPP constantly monitored the incoming data and network traffic to find out about real threats. The solution easily studied small signs so that threats could be addressed before they progressed with damaging consequences to the hospital. As such, this near-perfect detection rate of 98% means that the hospital could effectively prevent leakage of information while at the same time negating disruptions of operations and patient privacy. The high detection rate also lessened the burden on the hospital's cybersecurity team since the software could largely identify threats, and the information was concise and easy to understand.
- **Reduction in Misconfigurations: 85%:** Misconfiguration of cloud systems has become one of the most serious concerns, primarily because it is a potential source of leakage or breaches of different types of data. Before applying CNAPP, misconfigurations in the hospital's hybrid cloud environment, particularly in case finding, were routine and challenging to handle by standard means. The misconfiguration issues were identified and remedied before anyone knew due to CNAPP's continuous monitoring as well as the configuration management tools. This kind of automation lowered the misconfiguration risk by 85% and helped increase the security measures towards the cloud of the hospital. CNAPP lessened the corresponding threats of misconfiguration, which could have led to further instances of illegitimate access to the systems. In this regard, CNAPP facilitated the proper compliance of critical healthcare applications where possible vulnerabilities were eliminated.
- **Compliance Audit Success: 100%:** Healthcare organizations must adhere to laws such as HIPAA (Health Insurance Portability and Accountability Act) to effectively address patient's concerns and avert any legal implications. Thanks to compliance mapping and automated audit reports of CNAPP, the hospital was able to meet its regulatory compliance with much ease. It continued to check HIPAA, HITECH, and other regulating standards of the hospital and provided audit reports to demonstrate the hospital's compliance. Consequently, the hospital passed all compliance audits, which improved the consumers' confidence in the safety of patient information. This also helped in the lessening of compliance check processes and the possibility of human errors when marking them manually.

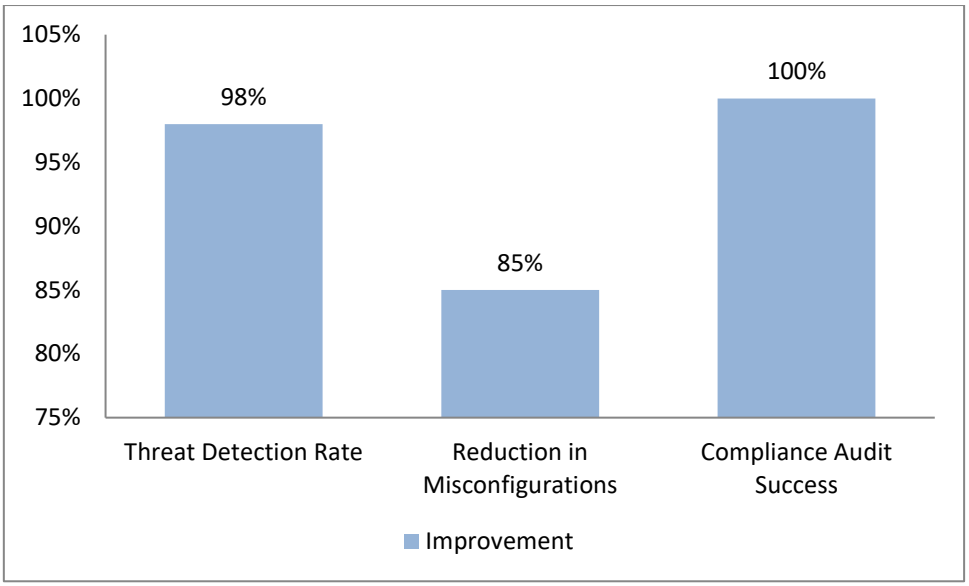

Fig 6. Graph representing Case Study: Mid-Size Hospital Deployment

4.2. Threat Simulation Results

The assessment was done through penetration testing to check how effective CNAPP is in combating cyber threats. As analyzing the results revealed, CNAPP was successful in preventing the following types of attacks:

- **SQL Injection Attacks:** Structured Query Language or SQL injection attacks can be considered one of the most notorious techniques of attackers to target web applications' flaws. They happen when the attacker enters SQL code into the input fields from where it is executed by the database and gains unfettered access to read, manipulate or delete data. When it came to penetration, CNAPP was effective in identifying and consequently neutralising SQL injections. The security engine of the platform was designed to oversee the database interactions and the input fields. In real time, it would identify potential exploits generated from certain queries. This deterred intruders from accessing the patient's information or tampering with the hospital's vital medical information record databases to maintain the genuineness of its databases and IT compliance with data protection laws.
- **Ransomware Payload Execution:** This paper focuses on ransomware since it is a relatively modern attack where hackers employ payloads to encrypt valuable data and request a ransom to provide the decryption key. As for CNAPP, it showed that it is possible to detect and mitigate ransomware payload execution. These are behaviors and traffic of files on the platform detected by the threat detection engine related to ransomware. It then prompted immediate containment actions such as quarantining affected systems and preventing payloads from running. By avoiding data encryption, CNAPP ensured that the hospital's health information remained open to the healthcare professionals thus cutting a major cost in patient care disruption. This aspect was most important in the healthcare industry, requiring reliable patient treatment information.
- **Privilege Escalation:** Privilege escalation usually results from attaining elevated access to a program or system through exploiting an existing fault or a loophole. More so, such attacks are disconcerting when data ownership is highly sensitive such as patients, medical records, and patient history. While testing the CNAPP tool, the authors proved it works well when fixing privilege escalation issues during the penetration testing phase. • It kept tracking the activities and range of accesses made within the platform to only allow the users to access the parts they were allowed to. Whenever attempts to escalate privileges were detected, CNAPP could mitigate such threats by raising alarms and avoiding changes to the status of users. This proactively helped protect healthcare data that unauthorized people should not access by keeping patients' data secure and whole.

4.3. Cost-Benefit Analysis

The first rollout of the CNAPP solution cost $150,000, whereby the amount was used to cater for expenses such as installation of the solution at the hospital, integration of the hybrid cloud framework that was in use by the hospital, and the training of the IT team on how to implement the solution. This was perhaps a tall order as it implied some considerable capital investment at the onset. However, in the long run, the cost-

benefit was tremendously off balance in favor of BIOS. One of the first improvements was in security, as security threats constitute one of the major issues to be addressed to minimize their impact and save money for healthcare organizations. As for the benefits, CNAPP prevented the hospital from falling victim to large-scale breaches, which could lead to hundreds of thousands in fines, legal fees, and loss of patient trust. When considering the benefits and costs, reducing costs associated with ransomware attacks, data breaches, and compliance violations was valuable for the hospital. It is now known that, on average, a healthcare data breach costs about $7 million, including fines, costs related to data breach, losses from the reduced revenues and damage to the reputation. Thus, CNAPP could have saved the hospital around $450,000 per each protected from one major data breach annually by preventing only one major data breach. Moreover, automation of compliance auditing and threat detection by CNAPP also freed up the time of the staff hence operating cost benefits. The management of time, when the team of IT of the given hospital was engaged in security incidents and compliance reports, allowed to save time, which was used more efficiently. This agency has shown that the CNAPP had returned on investment within the first few years of the contract. Since it formed the foundation to slouch in annual breach prevention, the hospital recorded a positive ROI while patients' record was safeguarded from databank vandals.

4.4. Discussion

This paper discusses the use of CNAPP in a 300-bed capacity hospital, making it strategic to demonstrate the ability of CNAPP as a cloud security solution needed specifically for health facilities. CNAPP can give a unified picture of the hospital's cloud status, which gives IT personnel complete visibility of data ingestion, settings, and usage across all cloud services used in the hospital. This is very important, especially in healthcare organizations where patient data contains sensitive information and compliance issues are critical. It means it is substantially easier to mitigate healthcare threats and misconfigurations in real-time through CNAPP and prevent extreme cases like ransomware attacks and the breach of health-related data. Furthermore, it means that CNAPP has all the features of a proactive defense when it comes to the threats associated with the constant evolution of new cyber threats. It makes security more preventive, minimizing possible threats that may harm the healthcare provider. The latter integration of the automated compliance mapping enhances customers' ability to meet strict legal standards like HIPAA and HITECH. CNAPP saves the hospital time on compliance audits so that the hospital does not violate any regulations at any one time. This capability lowers the likelihood of penalties for non-compliance so that it is not only expensive monetarily but also jeopardizes the organization's reputation. Concerning the financial value of CNAPP, the given value can be measured in terms of ROI. Effectively managing risks with regard to data breaches, uncontrollable losses, and timely reaction results in a large cost saving for the hospital. It is also possible to note an increase in operational efficiency – the time to respond to incidents and the number of unauthorized access events decreased categorically, which proves that with CNAPP, security is not only intensified, but also production processes are facili-tated. In the long run, the value of CNAPP is higher than the cost of deploying it, making the venture a prudent and essential step for healthcare providers who do not wish to compromise data security.

5. CONCLUSION

This paper reveals that firms can provide their healthcare environment with an effective protection system through CNAPPs since patient data remains threatened due to their nature as a source of record and regulatory compliance challenges integrated into cloud infrastructure solutions. By performing a literature survey, architectural modeling and empirical validation, it has been possible to establish CNAPP as a valuable solution for protecting health-sensitive data and meeting regulatory requirements to bolster healthcare organizations' security. CNAPP is an amalgamation of multiple safety tools rolled under a singular umbrella, which is beneficial for healthcare sectors to respond to various security issues on the same platform. This integration makes the security management process effective, and since all nodes are covered, it is hard for the hackers to find any weak links they could exploit.

As stated in the paper, CNAPP also offers the advantage of assessing vulnerabilities in the cloud environment and preventing possible attacks. This proactive security mode is more significant in maintaining the security of health facility data since data breaches in health facilities are disastrous since they can lead to loss of

reputation, fines, and, in the worst situation, leading to jeopardizing patient care. In this case, CNAPP's automated compliance mapping functionality guarantees that healthcare organizations comply with frameworks of laws such as HIPAA, GDPR, and HITECH to avoid incurring penalties for noncompliance and, at the same time, provide quality security to information. This was followed by testing specifically through case scenarios and threat modeling, which showed how CNAPP could identify and block different types of threats, ransomware, SQL injection and privilege escalation. Therefore, while service size and utilization demo have not changed much in the year, CNAPP remains an effective investment into cloud security for healthcare providers that want to decrease incident response time, limit potential intrusions, and ensure proper configuration.

As for the next steps, further work will be directed to the studies of using artificial intelligence (AI) to improve the identification of threats in CNAPP and provide more effective and intelligent responses to them. Also, the integration of CNAPP on the multi-cloud platforms will be investigated to ensure that the health care organizations can have secure and compliant policies from one cloud provider to another. Thus, developing these areas will help CNAPP grow further and offer better protection and performance in the healthcare cloud segment.

REFERENCES:

1. Casola, V., Castiglione, A., Choo, K. K. R., & Esposito, C. (2016). Healthcare-related data in the cloud: challenges and opportunities. IEEE Cloud Computing, 3(6), 10-14.
2. Amjad, A., Kordel, P., & Fernandes, G. (2023). A review of innovation in the healthcare sector (telehealth) through artificial intelligence. Sustainability, 15(8), 6655.
3. Malviya, R., Sharma, P. K., Sundram, S., Dhanaraj, R. K., & Balusamy, B. (Eds.). (2022). Bioinformatics tools and big data analytics for patient care. CRC Press.
4. Cybersecurity, C. I. (2018). Framework for improving critical infrastructure cybersecurity. URL: https://nvlpubs. NIST. Gov/nistpubs/CSWP/NIST. CSWP, 4162018(7).
5. Sharma, U., Bairagee, D., Singh, N., & Jain, N. (2022). Computational Cloud Infrastructure for Patient Care. In Bioinformatics Tools and Big Data Analytics for Patient Care (pp. 105-131). Chapman and Hall/CRC.
6. Djenna, A., Harous, S., & Saidouni, D. E. (2021). Internet of Things meets the Internet of threats: New concern cyber security issues of critical cyber infrastructure. Applied Sciences, 11(10), 4580.
7. Mehrtak, M., SeyedAlinaghi, S., MohsseniPour, M., Noori, T., Karimi, A., Shamsabadi, A., ... & Dadras, O. (2021). Security challenges and solutions using healthcare cloud computing. Journal of medicine and life, 14(4), 448.
8. CNAPP 101: An Intro to Cloud Native Application Protection Platforms, Wiz, 2025. online. https://www.wiz.io/academy/what-is-a-cloud-native-application-protection-platform-cnapp
9. Mehraeen, E., Ghazisaeedi, M., Farzi, J., & Mirshekari, S. (2017). Security challenges in healthcare cloud computing: a systematic. Global journal of health science, 9(3), 157-168.
10. Al-Issa, Y., Ottom, M. A., & Tamrawi, A. (2019). eHealth cloud security challenges: a survey. Journal of Healthcare Engineering, 2019(1), 7516035.
11. Chenthara, S., Ahmed, K., Wang, H., & Whittaker, F. (2019). Security and privacy-preserving challenges of e-health solutions in cloud computing. IEEE Access, 7, 74361-74382.
12. Boppana, V. R. (2019). Cybersecurity Challenges in Cloud Migration for Healthcare. Available at SSRN 5004949.
13. Cloud-Native Application Protection Platform: What's CNAPP in Cloud Security?, bigid, 2024. online. https://bigid.com/blog/what-is-cnapp/
14. Alenezi, M. (2021). Safeguarding Cloud Computing Infrastructure: A Security Analysis. Computer Systems Science & Engineering, 37(2).
15. Mehanoor, S. H., & Ahmed, S. (2024). Safeguarding Data and Ensuring Security in Digital Healthcare. In Transforming Gender-Based Healthcare with AI and Machine Learning (pp. 160-184). CRC Press.
16. Ganiga, R., Pai, R. M., MM, M. P., & Sinha, R. K. (2018). Private cloud solution for securing and managing patient data in rural healthcare systems. Procedia computer science, 135, 688-699.

17. Jimmy, F. N. U. (2023). Cloud security posture management: tools and techniques. Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online), 2(3).
18. Loaiza Enriquez, R. (2021). Cloud Security Posture Management/CSPM) in Azure.
19. MacDonald, N., & Croll, T. (2020). Market guide for cloud workload protection platforms. Gartner, Stamford, CT, USA, Rep. G 716192.
20. Kwon, J., & Johnson, M. E. (2013). Security practices and regulatory compliance in the healthcare industry. Journal of the American Medical Informatics Association, 20(1), 44-51.