ENPM 686 INFORMATION ASSURANCE

FINAL PROJECT PAPER

ENHANCING HEALTHCARE NETWORK SECURITY

A MULTI-LAYERED DEFENSE AND RESILIENCE PLAN

INDEX

INTRODUCTION:

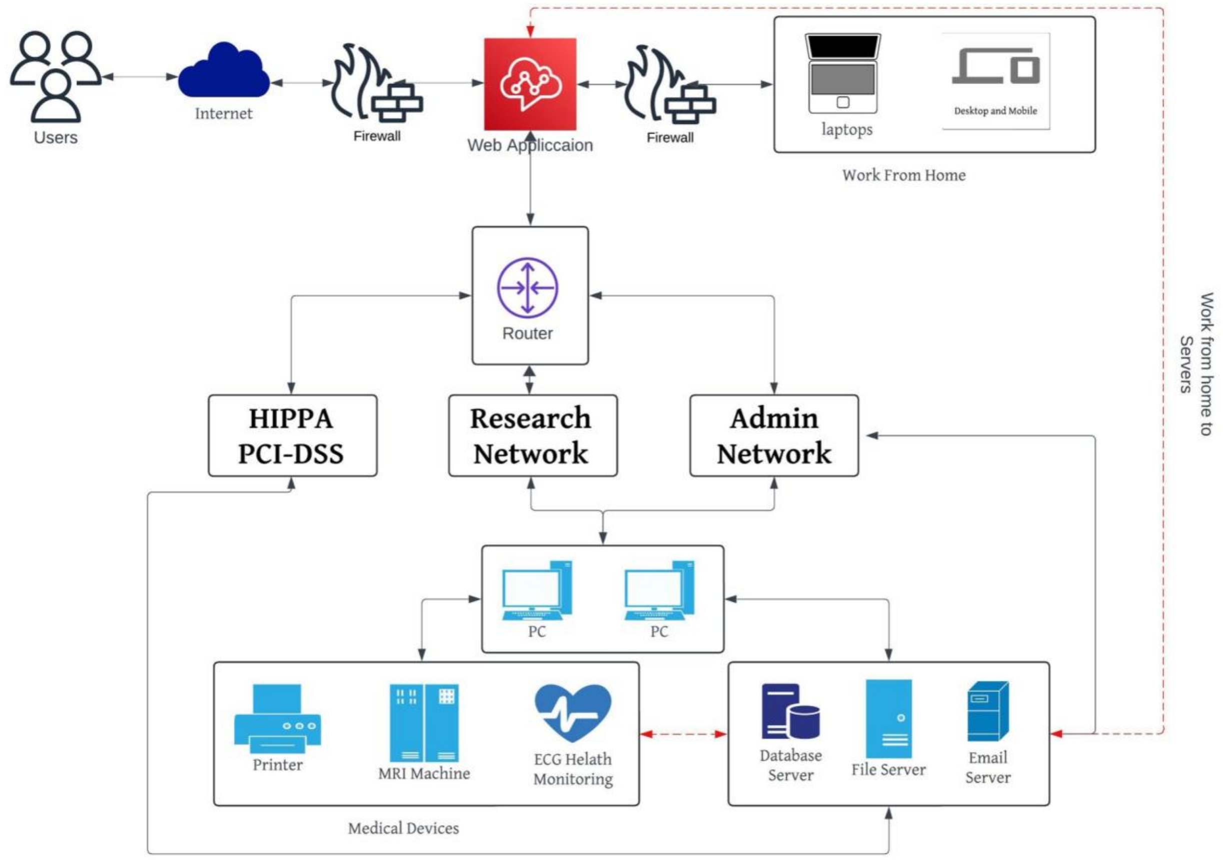
The healthcare industry is a prime target for cyberattacks due to the sensitive nature of patient data and the criticality of its operations. Recent incidents have highlighted the vulnerability of hospital networks to sophisticated and persistent threats, often resulting in prolonged unauthorized access, data breaches, and disruption of essential services. The consequences of such attacks can be severe, ranging from financial losses and regulatory penalties to compromised patient care and erosion of public trust. To address these escalating risks, a robust and comprehensive security strategy is paramount.

This paper proposes a multi-layered security plan designed to bolster the defenses of a compromised hospital network. Recognizing that prevention alone is insufficient, the plan adopts a defense-in-depth approach that combines proactive measures to prevent attacks, vigilant mechanisms for rapid detection, and resilient strategies to tolerate and recover from unavoidable security breaches. The plan acknowledges the heterogeneous nature of hospital networks, encompassing both Linux and Windows environments, and addresses the specific vulnerabilities inherent in each.

Furthermore, the plan recognizes the growing trend of remote work in the healthcare sector and the unique security challenges it presents. With a significant portion of the workforce accessing the network from various locations and devices, the plan emphasizes the importance of securing work-from-home environments. This includes implementing robust access controls, encryption protocols, and user education programs to mitigate the risks associated with remote work.

By integrating network segmentation, intrusion detection systems, endpoint protection, and a Zero Trust architecture, the plan aims to proactively identify and address vulnerabilities, limit the lateral movement of attackers, and minimize the impact of potential breaches. Additionally, the plan prioritizes web server security, recognizing its role as a critical entry point for attackers. A detailed analysis of the costs and resource requirements associated with implementing this comprehensive security plan is also provided, ensuring that the proposed measures are both effective and feasible within the hospital's budgetary constraints.

CURRENT NETWORK ARCHITECTURE:



The hospital network's perimeter consists of the internet, representing external users and potential threats. A firewall acts as the first line of defense, controlling traffic between the hospital network and the internet. A web application firewall (WAF) is also present to protect web applications from specific attacks like SQL injection and cross-site scripting.

The DMZ (Demilitarized Zone) houses public-facing applications, such as patient portals, allowing controlled access from the internet. A firewall separates the DMZ from the internal network, adding another layer of protection.

Within the internal network, a router directs traffic. The network is segmented into three zones: the HIPAA/PCI-DSS Zone, which stores highly sensitive data like patient records and payment information; the Research Network, containing devices used for research purposes; and the Admin Network, which includes administrative workstations and servers.

Various devices are connected to the network, including workstations used by staff, medical devices like MRI machines and ECG monitors, servers (database, file, and email), and a shared printer. The diagram also shows laptops and mobile devices used by employees working from home. These devices appear to have a direct connection to the internal servers.

PROBLEMS WITH THE CURRENT ARCHITECTURE:

The current hospital network architecture, as depicted in the diagram, presents a significant security risk due to several critical vulnerabilities. These vulnerabilities span across network security, host security, web server security, and work-from-home security, collectively creating a high-risk environment for the entire hospital infrastructure.

In terms of network security, the absence of proper segmentation is a major concern. The network appears to operate as a flat structure, with no distinct zones for different types of traffic, such as administrative, research, or public-facing. This lack of segmentation allows attackers to move laterally across the network once they gain access, potentially compromising sensitive data in other areas. Additionally, the firewall configuration is weak, potentially allowing unauthorized traffic to enter the network. The absence of an Intrusion Detection/Prevention System (IDS/IPS) further exacerbates the risk, as malicious activity can go undetected for extended periods, increasing the potential damage of an attack.

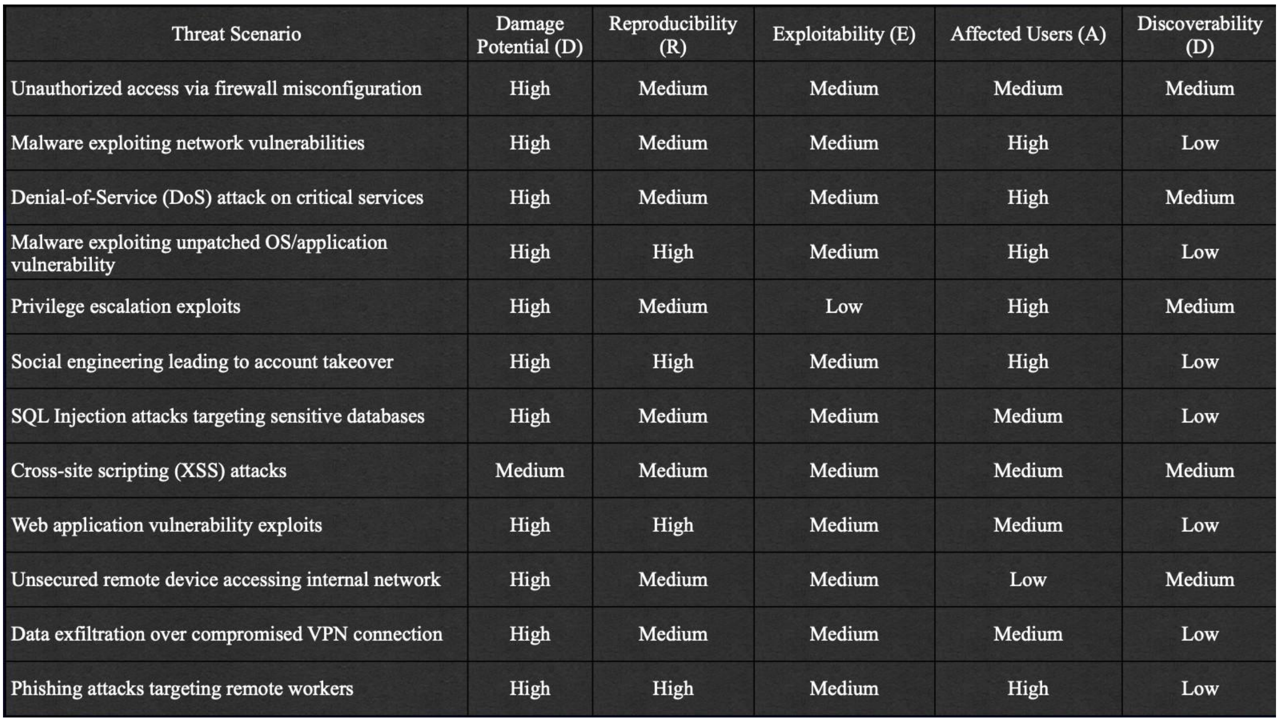
Host security is also compromised due to the presence of unpatched devices within the network. These unpatched devices are vulnerable to known exploits, providing attackers with an easy entry point into the network. Furthermore, the lack of endpoint protection leaves individual devices susceptible to malware and other threats, increasing the risk of data breaches and system compromise.

The web server security is another area of concern. The web server is directly exposed to the internet without a Web Application Firewall (WAF), making it a prime target for web-based attacks like SQL injection and cross-site scripting (XSS). These attacks can lead to data breaches, website defacement, and other serious consequences, potentially impacting the hospital's reputation and patient trust.

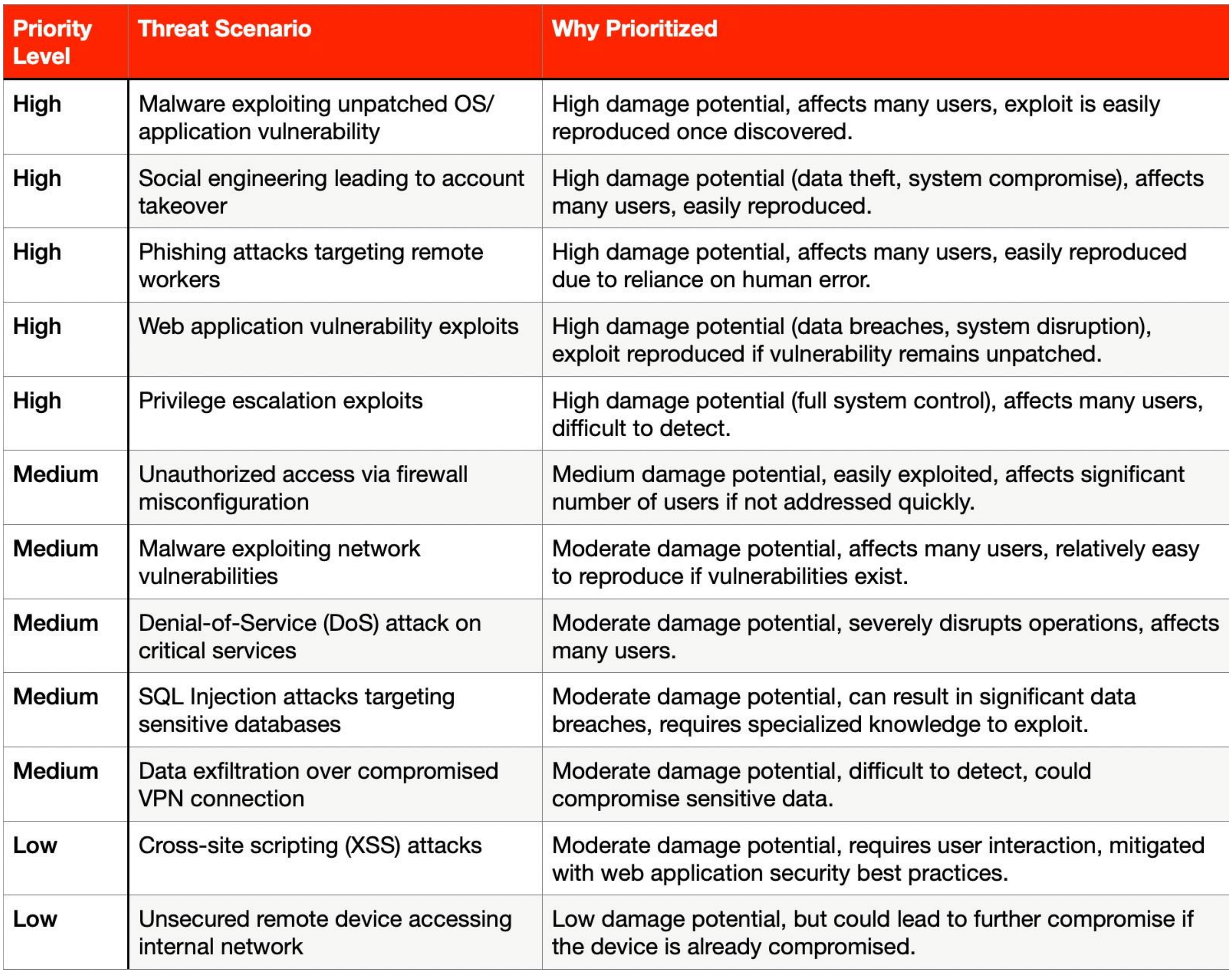
Finally, the work-from-home environment poses additional security risks. Remote devices, such as laptops, are directly connected to the internet without any additional security measures. This means that if a remote device is compromised, it can provide attackers with a direct pathway into the hospital network. The lack of multi-factor authentication and user education further exacerbates this risk, as it increases the likelihood of unauthorized access and successful phishing attacks.

In conclusion, the current hospital network architecture is riddled with vulnerabilities that expose it to a wide range of cyber threats. The lack of segmentation, weak perimeter defenses, unpatched systems, inadequate endpoint protection, and unsecured web server and work-from-home environments collectively create a high-risk environment. These vulnerabilities make it easier for attackers to gain access, move laterally within the network, and exfiltrate sensitive data, potentially leading to significant financial losses, regulatory penalties, and compromised patient care.

DREAD Model and Prioritizing Threats:



Threat Scenario	Damage Potential (D)	Reproducibility (R)	Exploitability (E)	Affected Users (A)	Discoverability (D)
Unauthorized access via firewall misconfiguration	High	Medium	Medium	Medium	Medium
Malware exploiting network vulnerabilities	High	Medium	Medium	High	Low
Denial-of-Service (DoS) attack on critical services	High	Medium	Medium	High	Medium
Malware exploiting unpatched OS/application vulnerability	High	High	Medium	High	Low
Privilege escalation exploits	High	Medium	Low	High	Medium
Social engineering leading to account takeover	High	High	Medium	High	Low
SQL Injection attacks targeting sensitive databases	High	Medium	Medium	Medium	Low
Cross-site scripting (XSS) attacks	Medium	Medium	Medium	Medium	Medium
Web application vulnerability exploits	High	High	Medium	Medium	Low
Unsecured remote device accessing internal network	High	Medium	Medium	Low	Medium
Data exfiltration over compromised VPN connection	High	Medium	Medium	Medium	Low
Phishing attacks targeting remote workers	High	High	Medium	High	Low



Priority Level	Threat Scenario	Why Prioritized
High	Malware exploiting unpatched OS/ application vulnerability	High damage potential, affects many users, exploit is easily reproduced once discovered.
High	Social engineering leading to account takeover	High damage potential (data theft, system compromise), affects many users, easily reproduced.
High	Phishing attacks targeting remote workers	High damage potential, affects many users, easily reproduced due to reliance on human error.
High	Web application vulnerability exploits	High damage potential (data breaches, system disruption), exploit reproduced if vulnerability remains unpatched.
High	Privilege escalation exploits	High damage potential (full system control), affects many users, difficult to detect.
Medium	Unauthorized access via firewall misconfiguration	Medium damage potential, easily exploited, affects significant number of users if not addressed quickly.
Medium	Malware exploiting network vulnerabilities	Moderate damage potential, affects many users, relatively easy to reproduce if vulnerabilities exist.
Medium	Denial-of-Service (DoS) attack on critical services	Moderate damage potential, severely disrupts operations, affects many users.
Medium	SQL Injection attacks targeting sensitive databases	Moderate damage potential, can result in significant data breaches, requires specialized knowledge to exploit.
Medium	Data exfiltration over compromised VPN connection	Moderate damage potential, difficult to detect, could compromise sensitive data.
Low	Cross-site scripting (XSS) attacks	Moderate damage potential, requires user interaction, mitigated with web application security best practices.
Low	Unsecured remote device accessing internal network	Low damage potential, but could lead to further compromise if the device is already compromised.

Assets to Protect in a Healthcare Network:

A. **Network Infrastructure:**

   A. Firewalls: Control network traffic flow and protect against unauthorized access.
   B. Switches: Connect devices within the network and facilitate communication.
   C. Routers: Manage traffic between different network segments and connect to external networks.

B. **Servers:**

   A. Web Server: Hosts the hospital's public-facing website and applications.
   B. Database Servers: Store and manage patient data, medical records, and other critical information.
   C. Email Server: Facilitates internal and external email communication.
   D. File Servers: Store and share files across the network.

C. **Workstations:**

   A. Desktops: Used by administrative staff, doctors, and nurses for their daily tasks.
   B. Laptops: Provide mobility for staff who need to access the network remotely.

D. **Medical Devices:**

   A. MRI Machines: Used for diagnostic imaging.
   B. ECG Monitors: Used for monitoring patients' heart activity.
   C. Other Medical Devices: Includes X-ray machines, infusion pumps, patient monitors, and other specialized equipment.

E. **Software Applications:**

   A. Web Applications: Used for patient portals, appointment scheduling, and other online services.
   B. Electronic Health Record (EHR) Systems: Centralized system for storing and managing patient medical records.
   C. Other Software: Includes billing software, inventory management software, lab result software, and other applications used in the hospital.

F. **Data:**

   A. Patient Data: Includes millions of patient records, medical histories, test results, and other sensitive information.
   B. Financial Data: Includes thousands of billing records, insurance claims, and payroll data.
   C. Other Sensitive Information: Includes research data, employee records, and other confidential information.

Core Security Strategy:

This comprehensive security strategy is designed to fortify our healthcare infrastructure against the evolving landscape of cyber threats. It integrates a defense-in-depth approach, zero-trust principles, and robust resilience and continuity planning. Our aim is to create an environment where patient data is protected, systems are resilient, and operations continue uninterrupted even in the face of adverse events.

I. Defense-in-Depth: Layered Protection for Comprehensive Security

Our defense strategy is built on the concept of layered security, where multiple safeguards are implemented at various levels to create a formidable barrier against cyberattacks.

1. **Network Security:**
   - **Advanced Firewalls:** We are upgrading our perimeter firewalls to incorporate Layer 3+ verification. This allows for granular control over incoming and outgoing traffic, enabling us to identify and block malicious activity with greater precision.
   - **Intrusion Detection and Prevention Systems (IDPS):** By deploying IDPS, we gain real-time visibility into network traffic, enabling us to detect and mitigate threats like DDoS attacks, malware, and other malicious activities promptly.
   - **Network Segmentation:** We are dividing our network into isolated zones, each with its security protocols. This segmentation limits the lateral movement of attackers, containing breaches and minimizing their potential impact.

2. **Endpoint Security:**
   - **Endpoint Protection Platforms (EPP):** We are deploying state-of-the-art EPP solutions on all devices, incorporating both signature-based and behavior-based detection mechanisms. This provides comprehensive protection against a wide range of threats, including ransomware, spear-phishing, and malware.
   - **Patch Management:** We have established a rigorous patch management process to ensure that all endpoints are promptly updated with the latest security patches. This proactive approach significantly reduces the window of vulnerability that attackers could exploit.

3. **Application Security:**
   - **Web Application Firewalls (WAF):** We are hardening our web servers with WAFs, which act as a specialized layer of protection against common web application attacks like SQL injection and cross-site scripting (XSS).
   - **Secure Development Practices:** We are embedding security into our software development lifecycle by enforcing secure coding practices and conducting regular security audits of web applications. This proactive approach helps us identify and remediate vulnerabilities before they can be exploited.

4. **Data Security:**
   - **Robust Encryption:** We are implementing strong encryption mechanisms to protect patient data both at rest (stored on servers) and in transit (across the network). This ensures compliance with HIPAA regulations and safeguards sensitive information from unauthorized access.
   - **Strict Access Controls:** We are enforcing granular access controls based on the principle of least privilege, ensuring that users only have access to the data and

systems necessary for their roles. This minimizes the risk of accidental or intentional data breaches.

5. Data Loss Prevention (DLP): By deploying DLP solutions, we can monitor and control the movement of sensitive data, preventing unauthorized sharing or exfiltration. This adds an additional layer of protection to our most valuable assets.

II. Zero Trust: Continuous Verification for Enhanced Security

We are embracing the Zero Trust security model, which assumes that no user or device is inherently trustworthy. This approach requires continuous verification and authorization throughout every interaction with our network and resources.

1. **Multi-Factor Authentication (MFA):** We are implementing MFA across all access points, including network logins, remote access, and privileged accounts. We are also integrating biometric authentication methods like fingerprint or facial recognition for an added layer of security.
2. **Least Privilege Access Control:** We are enforcing role-based access control (RBAC) to grant users access privileges based on their roles and responsibilities. Additionally, we are utilizing just-in-time (JIT) access provisioning, which grants temporary access to resources only when needed, further reducing the risk of unauthorized access.

III. Resilience and Continuity Planning: Preparing for the Unexpected

We understand that no security system is foolproof, so we have developed robust resilience and continuity plans to ensure that our operations can continue even in the face of a security incident or disruption.

1. **Backup and Recovery:** We have established regular backup schedules for critical data and systems, with backups stored securely offsite. We also regularly test our backup and recovery procedures to ensure their effectiveness.
2. **Incident Response Plan:** We have a detailed incident response plan in place to guide our actions in the event of a security incident. This plan outlines procedures for identifying, classifying, containing, mitigating, and analyzing security incidents, ensuring a swift and coordinated response.
3. **Business Continuity Planning:** We have identified critical business functions and resources necessary for maintaining healthcare operations. We have implemented redundancy and failover mechanisms to ensure the availability of these systems and services during disruptions. Additionally, we have enabled remote access capabilities to facilitate continued operations and collaboration in case of emergencies.

Network Security:

Network security is the initial barrier against cyber threats. We have implemented a range of measures to protect our network:

1. **Network Segmentation:** We have divided our network into isolated zones, such as patient record zones, administrative zones, research zones, and public web server zones. Each zone has specific security protocols tailored to its unique requirements. This segmentation helps to contain breaches and prevent lateral movement within the network.
2. **Firewalls with Deep Packet Inspection:** Our firewalls not only control traffic flow between zones but also use deep packet inspection to analyze network traffic patterns. This allows us to detect and block suspicious activity, such as malware or unauthorized access attempts.
3. **Intrusion Detection and Prevention Systems (IDS/IPS):** These systems continuously monitor network traffic in real time, looking for signs of malicious activity. IDS alerts us to potential threats, while IPS can actively block malicious traffic before it reaches its target.
4. **Secure Communication Channels:** We utilize encryption protocols and virtual private networks (VPNs) to secure communication channels both within and outside the hospital network. This ensures that sensitive data remains confidential and protected from eavesdropping or tampering.

Host Security:

Protecting every device within our healthcare network is crucial to defend against the ever-evolving landscape of cyber threats. Whether it's a workstation used by medical staff or a piece of specialized medical equipment, each endpoint could be a potential entry point for attackers. We are implementing a robust, multi-layered host security strategy to safeguard our infrastructure and sensitive patient data.

1. Endpoint Protection Platforms (EPP): The Frontline Defense Endpoint Protection Platforms (EPPs) are the frontline defense in our host security strategy. They provide a centralized defense mechanism across all workstations and devices, incorporating a multi-layered approach to protect against a wide range of threats
    A. Advanced Threat Detection: Modern EPP solutions go beyond traditional antivirus software. They combine signature-based detection (identifying known malware signatures) with behavior-based analysis (analyzing program behavior for anomalies). This hybrid approach allows us to detect and block even sophisticated, zero-day malware that evades conventional antivirus protection.

    B. Behavioral Analysis: Our EPPs scrutinize the behavior of programs running on our devices, looking for suspicious activities that may indicate the presence of malware. This proactive approach helps us to detect and stop new threats that haven't yet been identified and added to malware signature databases.

2. Vulnerability Scanning and Patch Management: Proactive Defense

Vulnerabilities in software, including operating systems and medical device software, pose significant risks. Our proactive defense strategy focuses on identifying and addressing these vulnerabilities before they can be exploited.

A. Automated Vulnerability Scanning: We regularly deploy automated vulnerability scanning tools to assess all devices within our network. These scans systematically identify known vulnerabilities in software components and libraries, enabling our security teams to prioritize remediation efforts.

B. Streamlined Patch Management: We have established a well-defined patch management process to ensure that identified vulnerabilities are addressed promptly. This process prioritizes critical vulnerabilities, applying patches within a predefined timeframe to minimize the window of opportunity for attackers.

3. Application Whitelisting: Restricting Unauthorized Software:

Unauthorized software installations can introduce significant security risks. To mitigate this, we have implemented application whitelisting across our network.

A. Authorized Application List: Our security administrators maintain a comprehensive list of approved applications that are allowed to run on hospital devices. This list includes essential operating system components, authorized medical software, and other necessary applications.

B. Restricted Execution: By blocking the execution of any application not explicitly included on the whitelist, we effectively prevent the installation and operation of unauthorized software, including potentially harmful malware.

Web Server Security:

Our hospital's website is a crucial platform for patients, staff, and external parties to access information and services. We have taken several measures to ensure its security.

A. Web Application Firewalls (WAFs): We have implemented WAFs to monitor and filter web traffic. WAFs inspect all incoming traffic, looking for patterns that indicate common web application attacks like SQL injection and cross-site scripting (XSS). They can also detect anomalies that may suggest previously unknown attacks, protecting our web server from both known and emerging threats.

B. Regular Security Testing: We conduct regular penetration testing and vulnerability scanning to proactively identify and remediate security flaws in our web server and application code. This helps us stay one step ahead of potential attackers.

C. Content Management System (CMS) Hardening: We ensure that our CMS software and associated plugins are always up to date with the latest security patches. We also disable unnecessary features and enforce strong password policies for CMS administrative accounts, further reducing the risk of unauthorized access.

Remote Security - Work From Home :

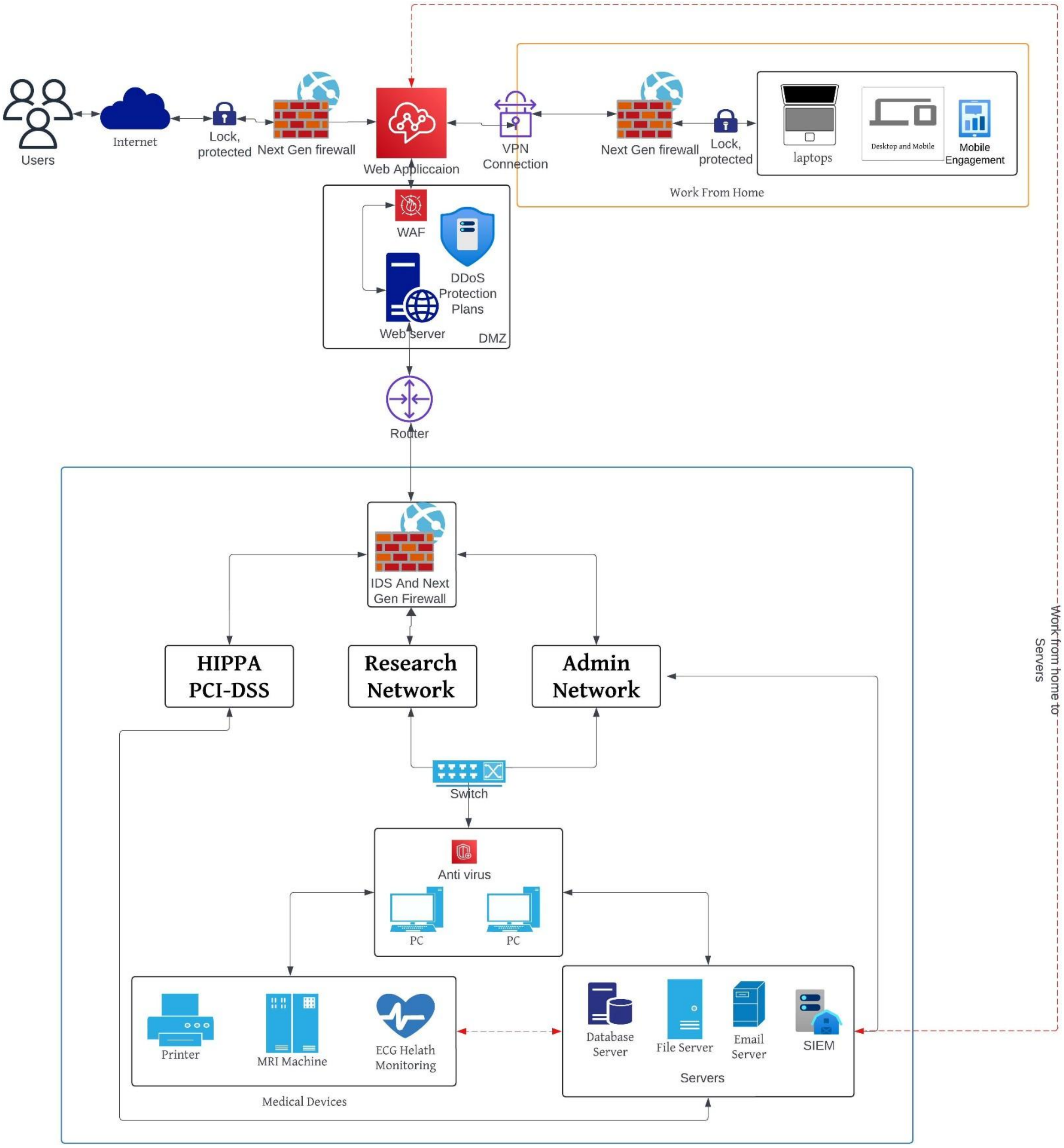
With the rise of remote work, we have taken steps to secure the devices and connections used by our staff working from home.

A. Mobile Device Management (MDM): Our MDM solution enables us to remotely manage and secure mobile devices used by our employees. This includes enforcing security policies, encrypting data, and remotely wiping devices if they are lost or stolen.

B. Virtual Private Networks (VPNs): We require remote employees to use VPNs to access our network. VPNs create a secure, encrypted tunnel over the public internet, protecting sensitive data transmitted between the remote device and our network.

C. Multi-Factor Authentication (MFA): We have implemented MFA for all remote access, requiring users to provide multiple forms of authentication (e.g., password and a code sent to their phone) to verify their identity. This significantly reduces the risk of unauthorized access in case of compromised credentials.

Proposed Network Architecture :



The enhanced network architecture diagram represents a significant improvement in security compared to the previous design, incorporating a multi-layered approach to protect the hospital's critical assets and sensitive data.

A. Network Segmentation and Firewalls :

The network is now divided into distinct zones: Administrative, Research, DMZ, and Work-from-Home. Each zone is isolated by next-generation firewalls (NGFWs), which provide granular control over traffic flow between zones. This segmentation significantly limits lateral movement, preventing attackers from easily accessing other areas of the network if one zone is compromised. The DMZ acts as a buffer zone, isolating the web server from the internal network and reducing the risk of unauthorized access to sensitive data.

B. Intrusion Detection and Prevention System (IDS/IPS) :

The inclusion of an IDS/IPS at the network perimeter provides an additional layer of security by monitoring incoming and outgoing traffic for suspicious activity. This system can detect and potentially block attacks before they reach the internal network, enhancing the overall security posture. The IDS/IPS system continuously analyzes network traffic patterns,looking for anomalies or signatures that match known attack patterns. If a potential threat is detected, the system can generate alerts for further investigation or even automatically block the malicious traffic.

C. Web Application Firewall (WAF) :

The WAF, positioned in front of the web server within the DMZ, acts as a specialized shield against web-based attacks. It filters incoming traffic, blocking malicious requests and protecting the web server from vulnerabilities like SQL injection and cross-site scripting (XSS). The WAF can also help to prevent denial-of-service (DoS) attacks, which can overload the web server and make it unavailable to legitimate users.

D. Endpoint Protection Platform (EPP) :

All devices within the network, including workstations, servers, and medical devices, are equipped with EPP software.This provides comprehensive protection against malware, viruses, and other endpoint threats, reducing the risk of compromise at the device level. EPP solutions typically include antivirus, anti-malware, firewall, and intrusion prevention capabilities.

E. Secure Remote Access :

The Work-from-Home zone is separated from the internal network and requires a VPN connection for access. This ensures that remote devices are not directly exposed to the internet and that all traffic between remote devices and the hospital network is encrypted. The VPN creates a secure tunnel through the public internet, protecting sensitive data from interception and unauthorized access.

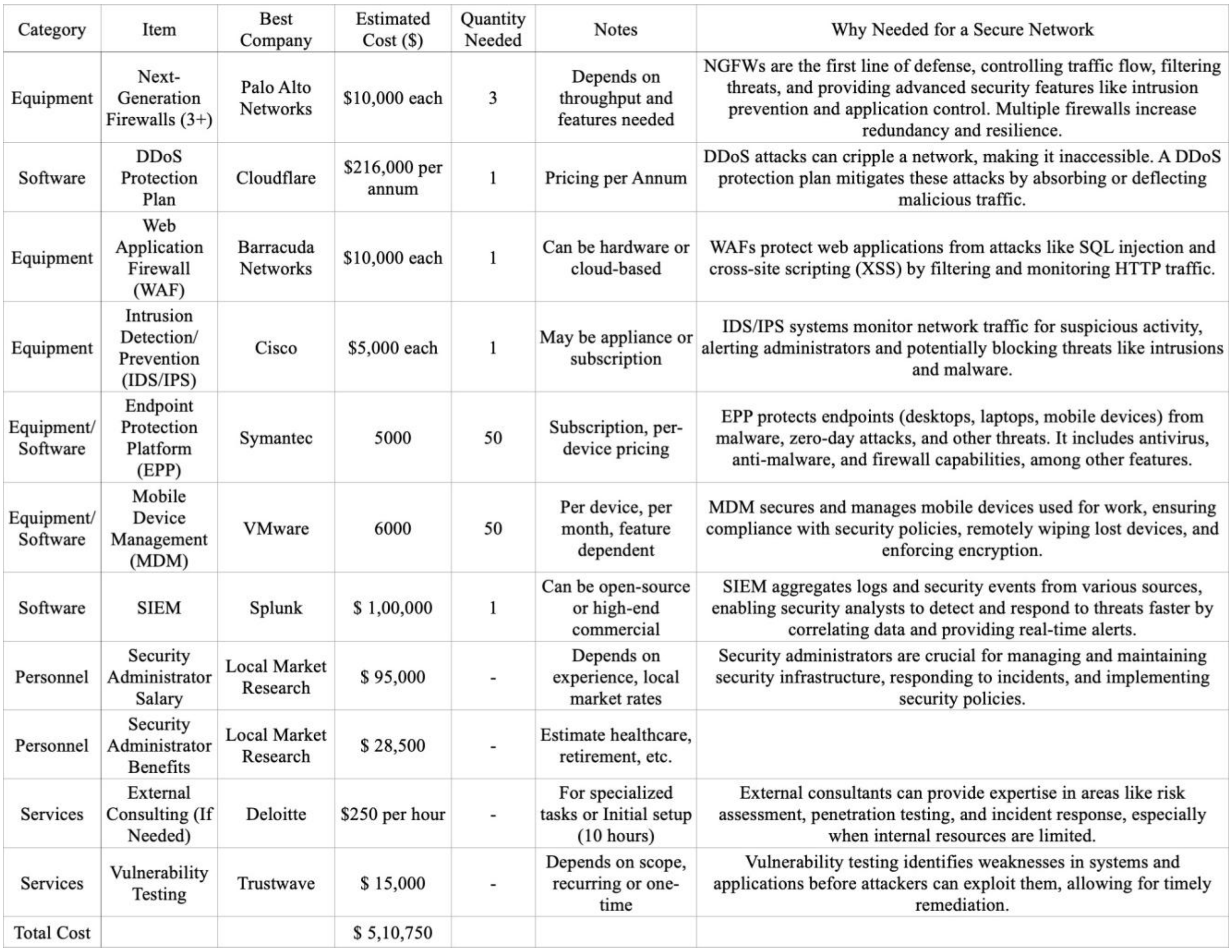
F. Additional Security Measures : In addition to the measures depicted in the diagram, the enhanced security architecture includes several other essential components:

1. Multi-Factor Authentication (MFA): MFA adds an extra layer of security for user accounts by requiring multiple forms of authentication, such as a password and a one-time code sent to a mobile device. This makes it much more difficult for attackers to gain unauthorized access, even if they have stolen a user's password.
2. Regular Security Testing: Penetration testing and vulnerability scanning are conducted regularly to identify and address weaknesses in the network before they can be exploited by attackers.
3. Security Awareness Training: Employees are trained on security best practices, such as identifying phishing emails and using strong passwords, to reduce the risk of human error leading to a security breach.
4. Backup and Disaster Recovery**:** A robust backup and disaster recovery plan is in place to ensure business continuity in the event of a security incident or other disaster. This plan includes regular backups of critical data and systems, as well as procedures for restoring operations in the event of an outage.

G. Centralized Log Management (SIEM) :

Although not visually represented in the diagram, the inclusion of a Security Information and Event Management (SIEM) system is crucial. The SIEM collects and analyzes security logs from various devices and systems, providing centralized monitoring and alerting for potential threats. This allows security personnel to quickly identify and respond to security incidents, minimizing the impact of an attack.

Cost Estimate :



Category	Item	Best Company	Estimated Cost ($)	Quantity Needed	Notes	Why Needed for a Secure Network
Equipment	Next-Generation Firewalls (3+)	Palo Alto Networks	$10,000 each	3	Depends on throughput and features needed	NGFWs are the first line of defense, controlling traffic flow, filtering threats, and providing advanced security features like intrusion prevention and application control. Multiple firewalls increase redundancy and resilience.
Software	DDoS Protection Plan	Cloudflare	$216,000 per annum	1	Pricing per Annum	DDoS attacks can cripple a network, making it inaccessible. A DDoS protection plan mitigates these attacks by absorbing or deflecting malicious traffic.
Equipment	Web Application Firewall (WAF)	Barracuda Networks	$10,000 each	1	Can be hardware or cloud-based	WAFs protect web applications from attacks like SQL injection and cross-site scripting (XSS) by filtering and monitoring HTTP traffic.
Equipment	Intrusion Detection/ Prevention (IDS/IPS)	Cisco	$5,000 each	1	May be appliance or subscription	IDS/IPS systems monitor network traffic for suspicious activity, alerting administrators and potentially blocking threats like intrusions and malware.
Equipment/ Software	Endpoint Protection Platform (EPP)	Symantec	5000	50	Subscription, per-device pricing	EPP protects endpoints (desktops, laptops, mobile devices) from malware, zero-day attacks, and other threats. It includes antivirus, anti-malware, and firewall capabilities, among other features.
Equipment/ Software	Mobile Device Management (MDM)	VMware	6000	50	Per device, per month, feature dependent	MDM secures and manages mobile devices used for work, ensuring compliance with security policies, remotely wiping lost devices, and enforcing encryption.
Software	SIEM	Splunk	$ 1,00,000	1	Can be open-source or high-end commercial	SIEM aggregates logs and security events from various sources, enabling security analysts to detect and respond to threats faster by correlating data and providing real-time alerts.
Personnel	Security Administrator Salary	Local Market Research	$ 95,000	-	Depends on experience, local market rates	Security administrators are crucial for managing and maintaining security infrastructure, responding to incidents, and implementing security policies.
Personnel	Security Administrator Benefits	Local Market Research	$ 28,500	-	Estimate healthcare, retirement, etc.	
Services	External Consulting (If Needed)	Deloitte	$250 per hour	-	For specialized tasks or Initial setup (10 hours)	External consultants can provide expertise in areas like risk assessment, penetration testing, and incident response, especially when internal resources are limited.
Services	Vulnerability Testing	Trustwave	$ 15,000	-	Depends on scope, recurring or one-time	Vulnerability testing identifies weaknesses in systems and applications before attackers can exploit them, allowing for timely remediation.
Total Cost			$ 5,10,750			

The estimated total cost for implementing the recommended security measures is $510,750. This includes the initial investment in hardware, software, and professional services, but does not include ongoing costs such as subscriptions, salaries, and potential future consulting or testing.

References:

1. https://www.cisco.com/c/en/us/products/collateral/security/firepower-2100-series/datasheet-c78-742473.html

2. https://itprice.com/cisco/fpr2130-ngfw-k9.html

3. https://www.barracuda.com/products/application-protection/web-application-firewall

4. https://www.manageengine.com/mobile-device-management/?network=g&device=c&keyword=cloud mdm solution&campaignid=10047966928&creative=611533394314&matchtype=p&adposition=&placement=&adgroup=100412379799&targetid=kwd-317301921777&gad_source=1&gclid=CjwKCAjwupGyBhBBEiwA0UcqaFrGwJa0kvQFZv742VdmaaHseZJcCcWtidX4LiTX2fCxkYWAuJu1whoC7GgQAvD_BwE

5. https://www.paloaltonetworks.com/network-security/next-generation- firewall

6. https://www.getapp.com/security-software/a/cloudflare/pricing/