ESOFT

Leader in Professional ICT Education

Kingston University London

Revolutionizing Revenue Cycle Management: A Next-Gen Firewall-Powered Network Upgrade.

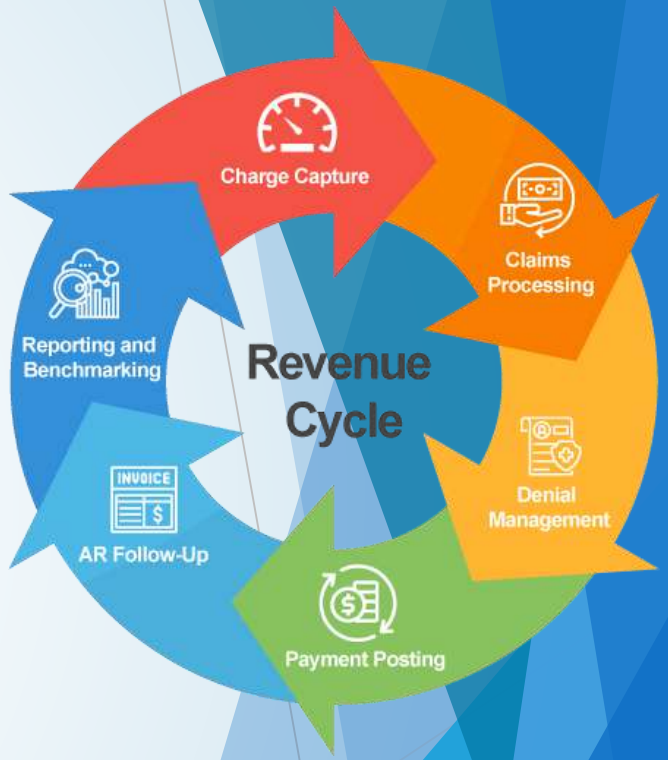
Introduction

- What is Healthcare RCM ?

  Revenue cycle management (RCM) is basically the process healthcare systems use to keep track of the money they earn from patients. It starts from the moment a patient schedules an appointment or visits the healthcare facility and continues until they pay their bill in full. In simple terms, it's about managing all the steps involved in getting paid for the services provided to patients.

  Real world example – Tricare healthcare data breach Sep 2011 has affected 5 million patient data.

- RCM demands robust and secure infrastructure to protect sensitive data.
- Traditional security measures struggle against evolving cyber threats.
- Modern network solutions are crucial for RCM operations.



Background and Motivation

Legacy Health likely utilizes a traditional network security system that include some of the following elements:

- **Firewalls**: These act as a first line of defense, filtering incoming and outgoing traffic based on predefined rules. However, traditional firewalls may not be equipped to handle the sophistication of modern cyberattacks.
- **Intrusion Detection Systems** (IDS): These systems monitor network traffic for suspicious activity, but their effectiveness can be limited by the ability of attackers to evade detection methods.
- **Anti-virus software**: This software protects against known malware threats, but it may not be able to detect zero-day attacks or other emerging threats.

Challenges

Legacy Health's current network security solution might be facing several challenges that hinder its effectiveness:

- Vulnerability to Cyberattacks: Traditional security measures like firewalls and IDS may not be sufficient against sophisticated cyberattacks like malware, phishing attempts, and ransomware attacks that exploit vulnerabilities in outdated systems.
- Increased Risk of Data Breaches: Outdated infrastructure and limited detection capabilities can increase the chances of unauthorized access to sensitive patient and financial data, leading to costly data breaches.
- Operational Inefficiencies: Manual network management tasks and a complex network architecture can consume valuable IT resources. This can lead to slow troubleshooting, delayed responses to security incidents, and hinder the scalability needed for future growth.
- Limited Compliance Capabilities: Evolving healthcare data privacy regulations, like HIPAA, require robust security measures. The existing system might struggle to keep pace with these changing compliance requirements.

Aim and Objectives

- Aim
  - Significantly improve the network security and operational efficiency of Legacy Health's RCM environment by utilizing next-generation firewalls with AI-based threat detection and redesigning the entire network infrastructure.

- Objectives
  - Enhance data protection to reduce security risks and potential data breaches.
  - Optimize operational efficiency.
  - Redesign the network infrastructure for improved performance.
  - Enhanced VoIP services.
  - Establish a foundation for future scalability.
  - Disaster Recovery and Business Continuity.

Literature Review

Related Work	Applied Domain	Nature/challenges of data set / research background	Used Algorithms/ Methodologies	Accuracy/Advantages	Limitations

Problem

Legacy Health's RCM department is facing issues related to their current network infrastructure. Here's a breakdown of the problems:

1.**Outdated Network**: The existing network infrastructure is likely outdated and may not be equipped to handle the security demands of today's digital landscape. This could lead to vulnerabilities that hackers could exploit.

2.**Security Challenges**: The outdated network might lack advanced security features, making Legacy Health susceptible to data breaches, malware attacks, and unauthorized access to sensitive patient and financial information.

3.**Operational Inefficiency**: The current network design might be complex and cumbersome, leading to inefficiencies in network performance, data flow, and potentially higher IT administration overhead.

4.**Scalability Limitations**: The existing infrastructure might not be flexible enough to adapt to future growth in data volume, users, or evolving RCM needs. This could hinder Legacy Health's ability to scale their operations efficiently.

5.**Compliance Concerns**: Outdated network infrastructure might not meet the latest industry standards for healthcare data privacy. This could put Legacy Health at risk of non-compliance with regulations like HIPAA (Health Insurance Portability and Accountability Act) in the US or similar regulations in Sri Lanka.

6.**Integration Difficulties**: The current network might struggle to integrate with newer technologies or applications required for modern RCM practices. This could hinder Legacy Health's ability to adopt new tools and technologies that could improve efficiency or patient care.

Solution

- Planning and preparation : encompassing detailed network infrastructure assessment, defining project scope and timelines, and obtaining necessary approvals. This phase also involves the careful selection and procurement of the AI-based threat detection engine, NGFW, and manageable switches, ensuring compatibility with existing infrastructure and meeting Legacy Health's specific security requirements.
- Custom-Designed Network Architecture :Implement physical segmentation by dividing the network into dedicated zones (e.g., DMZ,) using physical separation methods like VLANs or separate physical switches.
- Next-Generation Firewalls (NGFWs): Legacy Health will implement state-of-the-art NGFWs at crucial network points, offering advanced features like
  Deep Packet Inspection, Intrusion Detection system, sandboxing & AI-Driven Threat Detection.
- End Point Management System : FortiClient or Bitdefender Gravity zone license for 200 endpoints.
- Enterprise Sever : Deploy 2 Enterprise servers for Primary Domain & VM
- Fiber Optic Infrastructure Upgrade : Implement new fiber optic cabling to connect the 1000F Series NGFWs and other critical network devices to the new internet connection point. This high-bandwidth infrastructure will significantly improve data transfer speeds and network performance.
- Implement Multi-Factor Authentication (MFA) for all office 365 user accounts to strengthen access security.
- Automate network monitoring - provide real-time insights into network health and identify potential issues proactively.

Uniqueness and My Contribution

Primary Focus of the Project

- Revolutionize Legacy Health's RCM Network Security : The project's core objective is to completely overhaul the outdated network infrastructure and enhance network security using cutting-edge technologies.
- Enhance Operational Efficiency: Redesigning the network architecture will streamline network performance, improve data flow, and automate routine tasks. This will lead to increased operational efficiency and reduced IT administration overhead.

how my proposed solution for the Legacy Health RCM network overhaul can effectively address the existing issues

1.**Modernized Infrastructure**: My solution replaces the outdated infrastructure with a custom-designed network architecture, ensuring compatibility with modern security protocols and improved performance for RCM operations.

2. **Advanced Security Features**: my propose implementing state-of-the-art Next-Generation Firewalls (NGFWs) with features like deep packet inspection, intrusion prevention, and sandboxing. This provides a multi-layered defense against cyber threats, significantly enhancing security compared to the existing network.

3. **AI-Powered Threat Detection**: Integrating AI adds another layer of security by analyzing network traffic patterns for anomalies and suspicious activity in real-time. This proactive approach identifies threats before they can cause damage, surpassing basic security measures in the existing network.

4. **Network Optimization**: The custom network architecture streamlines data flow and prioritizes critical RCM traffic, leading to improved network performance compared to the existing inefficient design.

Research Methodology

- Requirements Gathering: Define specific needs, objectives, and functionalities required for the new network. This involves collaborating with stakeholders from Legacy health production staff, IT, and security departments.
- Design: Here, you'll design the network architecture, selecting appropriate NGFWs, AI tools, and network segmentation strategies.
- Development/Implementation: In this phase, the new network infrastructure is built and configured according to the design. Testing and integration with existing systems are also conducted.
- Verification and Validation: Thorough testing ensures the new network meets performance and security objectives. User acceptance testing verifies that the network functions as expected for Legacy health staff.
- Deployment and Maintenance: The new network is deployed, and ongoing maintenance plans are established to ensure security updates, troubleshooting, and user support.

Implementation / Technologies

Hardware Requirements

- **New Network Switches**

  TL-SL5428E

  2x Jetstream 24-Port 10/100Mbps + 4-Port Gigabit L2 Managed Switch.

- **New Cat6a or Cat7 Cables**
  Faster Cat 6a or Cat7 cables needed for connecting network devices within each VLAN and to the FortiGate 1000F Series NGFWs.
- **Fiber Optic Infrastructure**
  High bandwidth fiber optic cabling needed
- **Cisco Router** - C881 Branch Router
- **Server Requirements** - HPE proliant dl380 gen10

Software Requirements

- FortiGate Operating System and Licensing
- End Point Management System -Forticlient or Bitdeffender Gravitiy zone license for 200 endpoints.

Additional Software

- FortiManager if needed for centralized management

Ethical Issues

- Patient Data Protection: The project deals with sensitive patient information. Therefore, I need to ensure the highest level of data security throughout the entire process. This includes secure data storage, access controls, and robust encryption measures.
- Zero-Day Attacks: Even with advanced security measures, the project might still be susceptible to unforeseen zero-day attacks targeting new vulnerabilities.
- Data Breach: Despite security measures, there's always a risk of a data breach if unauthorized individuals gain access to sensitive patient information.

Project Plan

Phase Name	Description
Problem Analysis	A thorough analysis of Legacy Health's RCM network infrastructure is necessary to identify existing security vulnerabilities and define essentia requirements for a secure and future-proof environment
System Design	system design leverages NGFW, AI threat detection, and redesign of the network for enhanced security and optimized network performance.
Implementation	implementing NGFW, AI threat detection, configuring new enterprise servers will increase the security and performance of Legacy Health's R network infrastructure
Evaluation	Evaluation will provide data-driven insights to optimize Legacy Health's RCM network, facilitating continuous improvement of security and performance
Documentation and Reporting	Prepare project documentation and final report.

Milestone Number	Milestone Name	Deliverables	Planned Completion
M1	Problem Analysis	Problem statement, requirements specification.	7 Days
M2	System Design	Redesign network architecture, and NGFW implementation	20 Days
M3	Implementation	Implementation of NGFW and migration of network	60 Days
M4	Evaluation	test results, simulation results & performance evaluation report.	30 Days
M5	Documentation	Final project report, and user documentation.	7 Days

Future Work

- Future work
  - Suggestions can be given for further enhancement

References