Project: Enterprise Network Security Transformation & Merger

Executive Summary

Designed and authored a comprehensive security architecture to facilitate the merger of two distinct organizations: a financial services firm and a medical software provider. The project focused on unifying disparate infrastructures into a hardened Hybrid-Cloud environment while adhering to a strict $50,000 first-year budgetary cap.

Problem Statement & Risk Analysis

Prior to the merger, both organizations faced critical security and infrastructure challenges:

Company A (Finance): Broad attack surface with open ports (21-90, 3389), weak password policies, and the use of end-of-life Windows Server 2012 systems.
Company B (Medical/Payments): Critical Remote Code Execution (RCE) vulnerabilities (dRuby, Java RMI, Ghostcat) and a lack of enforced Multi-Factor Authentication (MFA).

Proposed Solution: Zero-Trust Hybrid Architecture

The design utilizes a **Defense in Depth** strategy to create overlapping security layers:

1. Perimeter & Internal Defense

Cloud-Based Next-Generation Firewall (NGFW): Deployed as the primary internet-facing control for centralized threat intelligence and scalable edge protection.
Internal Micro-segmentation: Repurposed on-premises Fortinet and Sophos hardware to create internal security zones, strictly limiting lateral movement within the network.

2. Identity & Endpoint Security

Centralized IAM with MFA: Implemented a cloud-based Identity and Access Management system requiring MFA for all users, moving away from vulnerable password-only authentication.

Enterprise EDR: Deployed an advanced Endpoint Detection and Response solution (Sophos Intercept X) across all hosts for real-time threat hunting and automated remediation.

3. Regulatory Compliance

The architecture specifically mapped technical controls to meet high-stakes industry standards:

PCI DSS: Isolated the Cardholder Data Environment (CDE) using dedicated VLANs and strict firewall rules to protect payment information.

HIPAA: Secured Electronic Protected Health Information (ePHI) through dedicated segmentation, audit trails, and mandatory encryption for data at rest and in transit.

Budgetary & Strategic Results

Cost-Efficiency: Utilized a subscription-based OpEx model (Cloud services) to avoid high upfront hardware costs, keeping the project within the $50,000 first-year limit.

Scalability: The hybrid approach allows for a phased migration of critical workloads to the cloud while decommissioning legacy on-premises servers over time.

Technical Competencies

Hybrid Cloud Architecture, Zero-Trust Security (ZTNA), Network Segmentation, NIST, Cybersecurity Framework, Vulnerability Remediation, PCI DSS & HIPAA Compliance, EDR/SIEM Implementation