ENPM686-0101 Final Paper

Group - 21

Uditraj Singh Rathore (UID: 119366295)

Jayraj A. Vakil (UID: 119188361)

Akshat Mehta (UID: 119229194)

Situation Analysis

Fortitude Financial Services has been facing major security issues affecting the trust of customers and operations. Having an employee strength of about 400 employees and with a customer base of roughly 200,000 users, protecting financial information is critical against major threats such as ransomware situations, phishing scams, supply chain vulnerabilities, SQL injections, and unauthorized transactions.

Previous breaches of security have caused sizeable damage to the company, affecting the finances and operations. One of these breaches involved a comprehensive phishing campaign which breached employee accounts, causing unauthorized access to customer data, with the company facing a revenue loss of $100,000 as a result of fraudulent transactions. In one other case, there was a supply chain breach affecting third-party vendor systems, causing reputational damage and data breaches, incurring a cost of $500,000 for customer compensation and remediation. Additionally, there was an unpatched software vulnerability which was exploited to initiate a ransomware attack on the company's servers, resulting in system downtime with a financial loss of $50,000 in terms of missed business opportunities and recovery activities.

To overcome these difficulties and to place Fortitude Financial Services as a cybersecurity leader, a thorough security policy is critical. The plan proposed involves using behavioral analytics to find anomalous user behavior, developing a zero-trust architecture to reduce unauthorized access, incorporation of threat intelligence platforms for quick threat detection, implementing endpoint detection and response solutions for fast incident response, and improving security awareness trainings to equip employees in detecting and reporting malicious activities.

Improving network security is important for protecting both administrative and technical operations. With a variety of systems in place, which includes those assisting with administrative functions and technical tasks, a holistic approach towards network security is critical. Proposed methods include implementation of advanced firewalls, network segmentation, and intrusion detection systems, as well as frequent vulnerability assessments to make sure of fast mitigation of potential weaknesses.

Cost-consciousness has been considered for the proposed security plan. With a budget of about $99,500, assigned for software licensing, equipment procurement, and security personnel salaries, the company aims to improve security measures while adhering to financial constraints.

Present Network Architecture

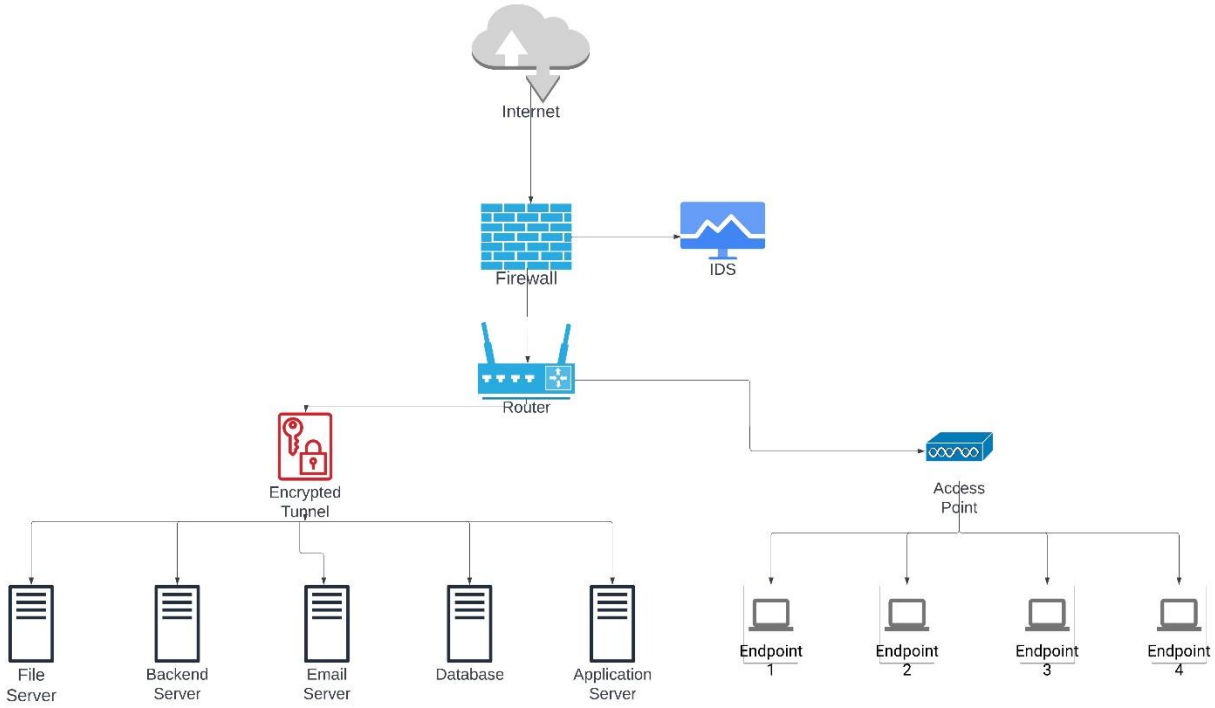

Figure 1. Present Network Architecture

Fortitude Financial Services has carefully crafted the network architecture to make sure that communication and data flow are efficient and secure in the company.

Acting as the main entry point for external connectivity is the Internet, protected by the combination of an Intrusion Detection System (IDS) and a Firewall, that continuously controls and monitors inbound and outbound traffic to prevent possible cyber-attacks and unauthorized access. After the mentioned security measures, there is a Router, responsible for data packet routing among network segments to ensure smooth communication. Before arriving at critical resources and servers, such as backend server, file server, database, email server, and application server, the data traffic has to go

through an encryption within an Encrypted Tunnel, protecting data integrity and confidentiality. Moreover, the gap between Router and Endpoints is bridged by an Access Point, providing wireless connectivity and seamless access to workstations or individual devices connected to the network.

This comprehensive architecture provides not only security of sensitive data but also a smooth operation of important services and functions of Fortitude Financial Services.

Risk Assessment and Prioritization

Let us make us of the DREAD methodology to perform a risk assessment and prioritize problems in our present network architecture. This technique will assist us in understanding the level of risks associated with each of the detected problem.

Major Cybersecurity Threats Facing Fortitude Financial Services:

1. Cyber Intrusions: Involving unauthorized access to the servers of the bank, resulting in possible modification of sensitive data or data theft.
2. Social Engineering: Manipulative tactics to trick employees into providing sensitive and confidential information or taking actions that compromise security.
3. Malware Attacks: Software created to damage, interrupt or get unauthorized access to computer systems.
4. Wire Transfer Fraud: Fraudulent transfer of funds from customers' accounts or the bank using deception and manipulation.

Cyber Intrusions

Risk Category	Rating
Damage Potential	9
Reproducibility	7
Exploitability	8
Affected Users	8
Discoverability	6
Total	**38**

A major risk is caused by cyber intrusions because of their ability to cause unauthorized access to sensitive information, resulting in terrible consequences such as identity theft, financial losses, and regulatory penalties. They have a high risk rating, highlighting their ease of execution and common frequency using vulnerabilities present in network defenses. The confidentiality and integrity of sensitive customer data is heavily threatened by such attacks, making it among the top priorities to protect. Banking servers and transaction systems are also critically dependent on robust measures and protections against such intrusion attacks, to provide security and availability of financial transactions, showing the major need for comprehensive and robust security measures such as encryption and advanced firewalls to protect these vulnerable points.

Social Engineering

Risk Category	Rating
Damage Potential	8
Reproducibility	6
Exploitability	7
Affected Users	7
Discoverability	5
Total	**33**

Even though social engineering is comparatively less discoverable and reproducible than other cyber attacks or threats, it still has a medium level risk due to the direct aiming towards the human element in security systems. Suck attacks cunningly manipulate employees, resulting in security protocols being compromised by them, eventually causing possible data breaches and unauthorized access. Assets such as email and communication systems pose risk of exposure, where malicious communications can look like legitimate, tricking employees into giving sensitive information. The results of risk assessment highlight the need for strengthening human-focused defenses using comprehensive verification processes and rigorous security training, to make sure that the staff are skilled enough to detect and respond to such measures and tactics.

Malware Attacks

Risk Category	**Rating**
Damage Potential	9
Reproducibility	8
Exploitability	8
Affected Users	7
Discoverability	7
Total	**39**

Malware attacks are dangerously common and simple to reproduce, making them a continuous threat to the company's cybersecurity. Such malicious programs can cause significant damage to software systems and compromise the integrity of data, making them a high-level priority for protective measures over all network systems and endpoints. The presence of malware shows the major need for frequent system upgrades and effective endpoint protection to mitigate the risk of infection. The high risk rating further proves the need for prioritization of robust security solutions such as automated

response systems and real-time threat detection targeted for protecting endpoint devices and workstations that act as common entry points for these attacks.

Wire Transfer Fraud

Risk Category	Rating
Damage Potential	10
Reproducibility	5
Exploitability	6
Affected Users	5
Discoverability	4
Total	**30**

Wire transfer fraud, even though happening less frequently than other cyber attacks and threats, possesses a major potential for quick financial damage, making it a medium level risk. This kind of fraud usually includes elaborate schemes to misdirect funds by alteration of transaction processes or tricking bank employees. Due to their focused impact on financial assets, protecting transaction systems from these frauds is critical and highlights its high prioritization. The bank's plan the mitigate this risk includes monitoring systems for suspicious activity, improving transaction security protocols, and enforcing stringent access controls, all targeted for safeguarding the crucial assets from unauthorized transfers and maintaining the security of high-stakes financial operations.

Proposed Solution

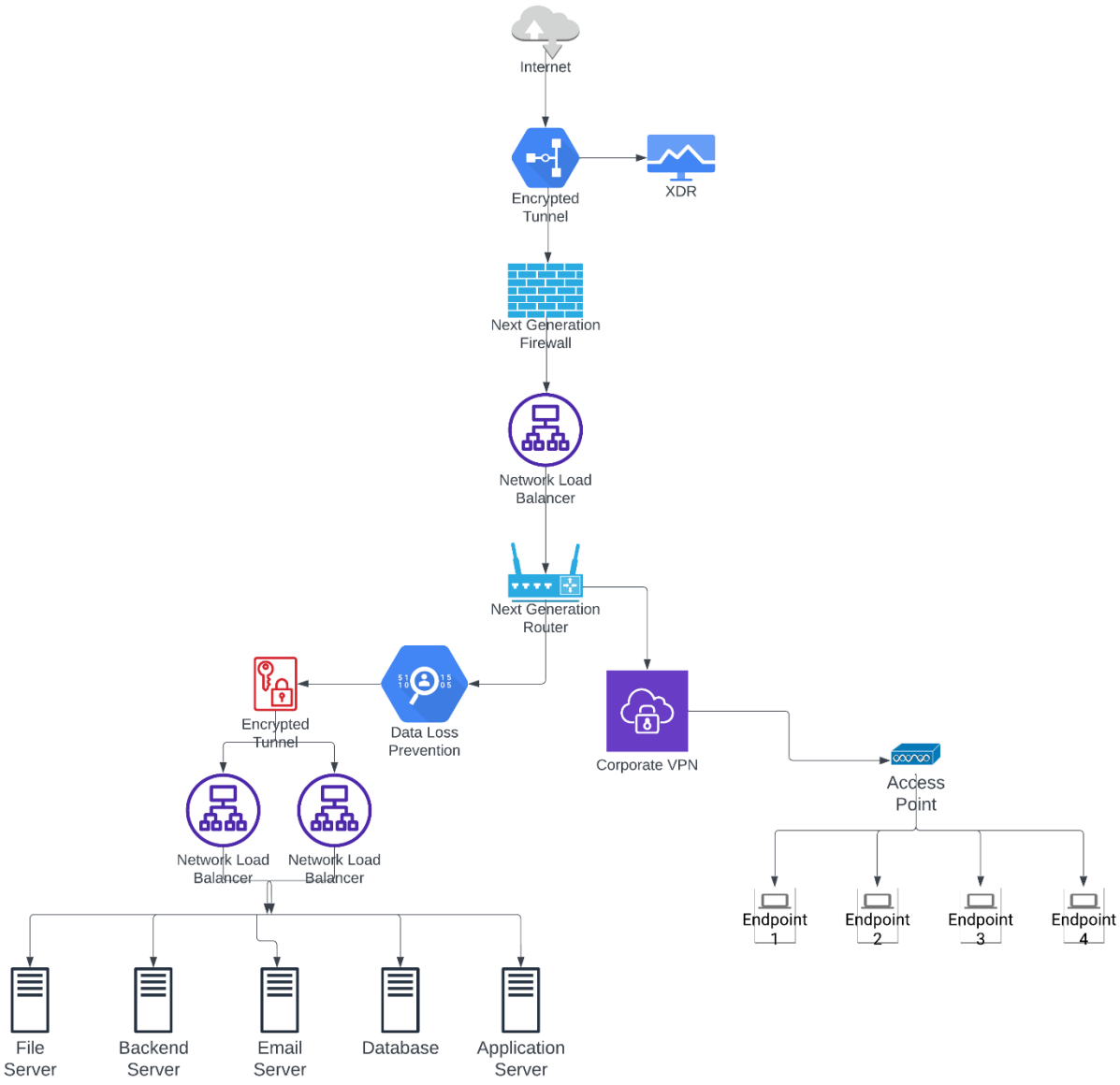

Figure 2. Proposed Network Architecture

Protecting Assets

1. Customer Data and Privacy

Next Generation Firewall and Encrypted Tunnel: The proposed measures at Fortitude Financial Services aim at secure transmission of data and a robust perimeter defense. The Next Generation Firewall (NGFW) provides inspection at the application level as well as threat intelligence, helping in blocking suspicious and malicious attempts for accessing customer data. SSL/TLS or IPsec is utilized by Encrypted Tunnels to safeguard transit data, preventing cybercriminals from getting access to sensitive information.

Extended Detection and Response (XDR): Fortitude Financial Services will utilize XDR for integrating data from networks, endpoints, and servers to find and respond to threats. XDR helps in detecting possible data breaches, by interpreting patterns across the company, providing quick mitigation and customer trust maintenance.

Data Loss Prevention (DLP): DLP systems at the company will monitor and block sensitive data in motion, in use, and at rest, depending upon predetermined policies. This assists in providing compliance with regulations such as GLBA and GDPR, and safeguards against unauthorized transfers or access of data.

Regular Security Audits and Compliance Checks: Comprehensive examinations of compliance with data protection laws and of security measures will be performed frequently. Such audits will assist in detecting vulnerabilities, making sure that Fortitude's defenses are always aligned with the newest security regulations and standards.

2. Transaction Systems and Banking Servers

Network Load Balancer: Important for distributing traffic over various servers to reduce outages and keep efficiency. It makes sure that transactional systems are always working, improving the reliability of the financial operations of Fortitude Financial Services.

Next Generation Firewall: Safeguarding banking servers by utilizing intrusion prevention and deep packet inspection to find and block threats, protecting the integrity of data and helping in system availability.

Multi-factor Authentication (MFA): MFA helps in protecting access to transaction systems by needing to provide multiple factors of verification, boosting the overall security, and majorly reducing the risk of unauthorized access.

Segmentation and Zero Trust Architecture: Enforces Zero Trust principles and network segmentation to safeguard crucial financial operations. This reduces the impact of breaches and protects transaction systems by verifying all attempts of access, irrespective of the origin.

3. ATM Systems

Corporate VPN: Protects transmission of data between ATMs and the network using encrypted tunnels, preventing interception of data, and making sure of the confidentiality of customer transactions.

ATM Dedicated Security Solutions: Advanced security measures, such as anti-skimming devices and advanced encryption help in safeguarding ATMs from digital and physical threats, protecting customer interactions and decreasing fraud risks.

4. Mobile and Online Banking Applications

Encrypted Tunnel: Utilizing SSL/TLS to protect transmitted data among banking servers and users, securing sensitive information such as transaction data and login information from cyber-attacks and threats.

Extended Detection and Response (XDR): Observes and safeguards online and mobile platforms by spotting unusual activities that could signal possible breaches, providing quick response to threats and maintaining the security of banking applications.

Enhanced Endpoint Protection: Employs machine learning and AI to find and mitigate threats on devices utilized to access banking applications, safeguarding against malware and other similar attacks.

Multi-factor Authentication (MFA): Fortifies user authentication processes, decreasing the risk of unauthorized access and improving the security of online and mobile banking platforms.

5. Email and Communication Systems

Next Generation Firewall: Refines incoming and outgoing communications to safeguard against phishing attacks and malicious content, protecting email and communication systems from possible breaches.

Regular Security Audits: Regular assessments and reviews of email security measures make sure that vulnerabilities are handled quickly, protecting the security and integrity of communication channels.

6. Workstations and Endpoint Devices

Extended Detection and Response (XDR): Delivers thorough threat monitoring over all endpoints, spotting, and mitigating risks quickly to keep data and network security.

Corporate VPN: Makes sure that remote access to the corporate network is protected, securing transmission of data from external environments, and decreasing the risks connected with remote access.

Enhanced Endpoint Protection: Provides real-time threat detection and response capabilities, protecting endpoints from advanced attacks and threats, making sure of the reliability of the operational infrastructure of Fortitude Financial Services.

Impact of Changes on Business Operations

Increased Operational Security and Efficiency: The integration of next-generation firewalls and extended detection and response (XDR) platforms will significantly bolster Fortitude Financial Services' security framework. These advanced systems will enhance the perimeter defenses and improve internal monitoring capabilities, resulting in a notable reduction in the frequency and severity of cybersecurity incidents. Consequently, business operations are expected to become more stable and efficient, minimizing disruptions and ensuring a smooth workflow.

Improved Compliance and Reduced Risk of Fines: Adopting robust data encryption and compliance-focused technologies, such as Corporate VPNs, positions the company to better meet regulatory requirements, including GDPR and GLBA. This proactive approach mitigates the risk of incurring costly legal fines and helps maintain the

company's positive reputation within the financial sector. Ensuring compliance not only protects the company financially but also builds trust with clients and regulatory bodies.

Enhanced Employee Security Awareness and Response: Deploying updated endpoint protection solutions and conducting regular security training sessions will transform employees into the first line of defense against cyber threats. As employees become more aware and responsive to potential security issues, the overall security posture of the company improves. This increased vigilance reduces the window of opportunity for attackers to exploit vulnerabilities, enhancing the company's ability to respond quickly and effectively to incidents.

Financial Savings from Averted Incidents: The proposed security enhancements are expected to prevent significant financial losses that can result from data breaches, malware infections, and other security incidents. For instance, protecting against malware could avert an estimated annual productivity loss of $150,000. Additionally, securing against skimming attacks could save an estimated $500,000 annually in fraud-related losses. These savings demonstrate the tangible financial benefits of investing in robust security measures.

Maintaining Customer Trust and Business Continuity: Prioritizing the security of customer data and transaction systems is crucial to preventing breaches that could lead to identity theft, loss of customer trust, and severe financial damage. By implementing a reliable and secure network architecture, Fortitude Financial Services ensures continuous service availability and maintains customer trust. Secure and uninterrupted operations are essential for sustaining long-term client relationships and ensuring business continuity.

Proposed Solution Cost

Item	Subtotal
Next-Generation Firewall (NGFW)	$10,000
Encryption Software Licensing	$30,000
Extended Detection and Response (XDR)	$7,500
Corporate VPN Solution	$14,000
Network Load Balancers	$3,000
Antivirus Software	$15,000
Professional Services	$20,000
Total	**$99,500**

The final estimated budget for the improvements is set at $99,500. This budget will be utilized for various investments in cutting-edge technologies including Extended Detection and Response systems and Next-Generation Firewalls, both picked due to their crucial roles in strengthening the defense of the bank. There are additional funds assigned for corporate VPN solutions, encryption software, antivirus software and network load balancers, providing a layered and robust security infrastructure. Professional services such as configuration, installation, and training, have been added to the budget, highlighting the bank's dedication to not only improving its technological defenses, but also making sure that its personnel are skilled enough to detect and respond to possible security threats. Such a comprehensive financial planning shows the proactive approach of the bank towards cybersecurity, by focusing on significant investments for high quality solutions that protect its client data and operations effectively.

Alternatives

Traditional firewalls were compared with Next-Generation Firewalls (NGFW). Even though we get basic protection with traditional firewalls by stopping unauthorized access based on ports and IP addresses, they still fall short against current advanced threat landscape. On the other hand, NGFWs give more in-depth capabilities of inspection, such as integrated intrusion prevention systems and application-level inspection. They help in detecting and blocking sophisticated cyber threats utilizing advanced threat intelligence, acting as a critical asset for financial institutions such as Fortitude Financial Services, where security requirements are dynamic and complex.

In relation to endpoint protection, the bank analyzed anti-malware solutions and standard antivirus with more advanced Endpoint Detection and Response (EDR) platforms. Only a basic level of protection is provided by standard solutions against known threats, but it does not have the capability to prevent advanced and new attacks. EDR platforms have been selected for their thorough monitoring capabilities, assisting in identifying and responding to previously unknown threats in real-time. Such a capability is important for financial institutions that are usually the targets of advanced and sophisticated cyber-attacks.

Conclusion

In conclusion, the comprehensive cybersecurity enhancements outlined in this proposal represent a strategic and necessary investment in the future security and stability of Fortitude Financial Services. By implementing advanced security measures such as Next-Generation Firewalls, Extended Detection and Response platforms, and robust encryption protocols, we are setting a new standard in cybersecurity for the financial sector. These

technologies, combined with a commitment to ongoing professional training and rigorous compliance checks, ensure that our infrastructure is not only protected against current threats but also prepared for future challenges. The planned investment of $99,500 is justified by the significant reduction in potential financial losses from cyber incidents and the invaluable preservation of customer trust. As we move forward, it will be crucial to continuously assess and evolve our security practices to stay ahead of threats. This proactive approach to cybersecurity will safeguard our operations, protect our clients' data, and maintain our reputation as a leader in the financial services industry.

References

1. Cisco Systems. (2023). Next-generation firewalls: Advancements in security technology. https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-next-generation-firewall.html
2. Gartner, Inc. (2023). Magic Quadrant for Endpoint Protection Platforms. https://www.gartner.com/en/documents
3. National Institute of Standards and Technology. (2022). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. https://www.nist.gov/cyberframework
4. Financial Services Information Sharing and Analysis Center. (2023). Cybersecurity trends in the financial sector. https://www.fsisac.com
5. Symantec Corporation. (2023). Protecting financial institutions from cyber threats. https://www.broadcom.com/company/newsroom/press-releases
6. McAfee Labs. (2023). Case study: Implementing effective cybersecurity measures in financial services. https://www.mcafee.com

7. Forbes Technology Council. (2023). Latest trends in cybersecurity for financial services. https://www.forbes.com/technology
8. IBM Security. (2023). The future of cybersecurity in financial services. https://www.ibm.com/security/data-breach/financial-services
9. Deloitte. (2023). Navigating the cybersecurity landscape in financial services. Deloitte Insights. https://www2.deloitte.com/us/en/pages/consulting/articles/cybersecurity-financial-services.html
10. Kaspersky. (2023). Cybersecurity in financial services: Managing the threat landscape. https://www.kaspersky.com/enterprise-security/financial