Secure Architecture Recommendations Report

For Mid-Sized E-Commerce Company

Prepared by: Esther Ogunlana
Date: 25 November, 2024

Executive Summary

This report presents a comprehensive security architecture assessment and action plan for Fender, a mid-sized e-commerce business experiencing rapid growth. The analysis leverages the NIST Cybersecurity Framework (NIST CSF) to identify vulnerabilities, recommend mitigation strategies, and provide a phased roadmap for enhancing the organization's cybersecurity posture.

The assessment revealed several critical security gaps, including weak access controls, outdated endpoint security, and an unsegmented flat network architecture. These vulnerabilities increase the risk of cyberattacks, data breaches, and regulatory non-compliance. The recommendations focus on addressing these weaknesses through a structured approach based on the five core functions of the NIST CSF: Identify, Protect, Detect, Respond, and Recover (NIST, 2018).

Key recommendations include implementing network segmentation to isolate sensitive resources, upgrading endpoint security solutions, enforcing multi-factor authentication (MFA) for all critical systems, and deploying advanced intrusion detection and prevention systems. The action plan prioritizes these tasks based on risk impact and feasibility, aligning with NIST's guidance to adopt defense-in-depth strategies (NIST, 2020).

The proposed roadmap outlines a phased implementation strategy. Phase 1 addresses high-priority issues such as network segmentation and access control upgrades. Phase 2 focuses on medium-priority tasks, such as enhancing endpoint protections and deploying cloud-based security measures. Phase 3 ensures sustainability through continuous monitoring, incident response training, and regular compliance audits.

Adopting the NIST CSF enables Fender to proactively address its cybersecurity risks and establish a robust, scalable security framework. By following the outlined action plan, the organization will achieve significant improvements in protecting critical assets, maintaining compliance, and fostering customer trust. This strategic investment in cybersecurity safeguards the company's current operations and positions it for sustainable growth in a competitive digital marketplace.

In line with NIST's emphasis on adaptability and continuous improvement (NIST, 2018), the company must regularly review and update its security measures to keep pace with evolving threats and technologies. Implementing this framework represents a critical step toward achieving a secure and resilient operational environment.

Introduction

This report provides an evaluation of Fender's cybersecurity posture, identifies critical vulnerabilities, and outlines an actionable roadmap using the principles from NIST's Cybersecurity Framework (*NIST SP 800-53 Rev. 5*, 2020). This report focuses on practical and prioritized strategies for network security, endpoint protection, identity and access management (IAM), and incident response. While constraints such as budget and staffing may limit implementation speed, the proposed recommendations are designed to maximize security impact with available resources.

Current Security Landscape

Existing Architecture

- Flat network topology exposing internal resources to external threats.
- Shared servers for web hosting, payments, and databases.
- Outdated antivirus software on endpoints.
- Weak password policies and lack of multi-factor authentication (MFA).
- No intrusion detection/prevention system (IDS/IPS) or security monitoring tools.

Identified Vulnerabilities

- An unsegmented network increases the risk of lateral movement in case of a breach (*NIST SP 800-41 Rev. 1*).
- Weak access controls jeopardize sensitive payment and customer data (*NIST SP 800-53: AC-2*).
- Lack of incident detection mechanisms delays response to cyber threats (*NIST SP 800-61 Rev. 2*).

Risks

- Customer data breaches lead to reputational and financial damage.
- Non-compliance with data protection regulations (e.g., PCI DSS, GDPR).
- Downtime and revenue loss due to ransomware or denial-of-service (DoS) attacks.

Security Architecture Goals

Business Requirements

- Protect customer data and maintain trust.
- Ensure compliance with industry standards and regulations.
- Enable secure scalability to support future growth.

Security Goals

1. Minimize risk exposure through network segmentation and endpoint security (*NIST SP 800-53: SC-32*).
2. Ensure confidentiality, integrity, and availability of customer data (*NIST SP 800-53: SC-13*).
3. Establish a robust incident response capability (*NIST SP 800-61 Rev. 2*).

Security Architecture Recommendations

Network Security

- Segment the network into separate zones for public-facing services, internal systems, and guest access. This aligns with NIST's recommendation to implement secure enclaves for resource isolation (*NIST SP 800-53: AC-4*).
- Deploy robust firewalls to enforce traffic policies and block unauthorized access (*NIST SP 800-41 Rev. 1*).
- Implement IDS/IPS to monitor and detect malicious activities, as recommended by NIST for continuous monitoring (*NIST SP 800-137*).

Data Security

- Encrypt sensitive data at rest and in transit using strong encryption protocols (e.g., AES-256, TLS 1.2/1.3) to maintain data integrity (*NIST SP 800-57 Part 1 Rev. 5*).
- Back up data regularly and maintain a recovery plan to ensure business continuity (*NIST SP 800-34 Rev. 1*).

Endpoint Security

- Replace outdated antivirus software with modern endpoint detection and response (EDR) tools, following NIST's recommendations for endpoint protection strategies (*NIST SP 800-83 Rev. 1*).
- Enforce device encryption and regular patch management to mitigate risks from unpatched vulnerabilities (*NIST SP 800-40 Rev. 3*).

Identity and Access Management (IAM)

- Implement MFA for all administrative and user accounts, as outlined in NIST's guidelines on digital identity (*NIST SP 800-63B*).
- Enforce least privilege access and role-based access controls (RBAC) to restrict unauthorized activities (*NIST SP 800-53: AC-6*).

Incident Response

- Develop and test an incident response plan to ensure quick detection and mitigation of breaches (*NIST SP 800-61 Rev. 2*).

- Establish a Security Operations Center (SOC) or outsource to a managed security provider for continuous threat monitoring (*NIST SP 800-137*).

Implementation Strategy

The implementation stage represents the critical process of translating recommendations into actionable security measures to address the identified vulnerabilities within Fender's infrastructure. This stage leverages the phased approach outlined in the roadmap, focusing on practical execution within defined timelines and resource constraints.

The proposed actions include network segmentation, deploying advanced firewalls, implementing endpoint protection tools, enforcing identity and access management (IAM) policies with multi-factor authentication (MFA), and establishing robust incident response capabilities. Each phase prioritizes high-risk areas first, ensuring that critical threats are mitigated promptly while balancing feasibility and company resources.

By following the proposed roadmap, the company can systematically address vulnerabilities, ensure long-term protection of assets, and align its security practices with industry standards. This stage is not just an operational enhancement but a strategic investment in the company's sustainability and success.

Phase	Tasks	Responsible Parties	Timeline	Priority
Phase 1	Implement network segmentation and deploy firewalls	IT Team. Security Vendor	1-2 months	High
Phase 2	Upgrade endpoint protection tools and enforce patch management	IT Team	2-3 months	High
Phase 3	Configure IAM policies with MFA and RBAC	IT Team	3-4 months	High
Phase 4	Establish an IDS/IPS and log monitoring tools for real-time threat detection	IT Team, SOC	4-5 months	Medium
Phase 5	Develop and test the incident response plan, including regular employee training sessions	IT Team, HR	5-6 months	Medium

Conclusion

The proposed recommendations, guided by the NIST Cybersecurity Framework, will significantly enhance the company's security posture. Key measures such as network segmentation, Identity and Access Management (IAM) with Multi-Factor Authentication (MFA), and robust endpoint security directly address the vulnerabilities identified, aligning with NIST's risk management principles (*NIST SP 800-30 Rev. 1*). Implementing these measures will protect customer data,

ensure regulatory compliance, and strengthen the company’s ability to respond to emerging threats, securing its long-term growth and reputation

Video Presentation

[Video Presentation Link]

References

National Institute of Standards and Technology. (2012). *Computer security incident handling guide* (Special Publication 800-61 Rev. 2). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-61r2

National Institute of Standards and Technology. (2009). *Guidelines on firewalls and firewall policy* (Special Publication 800-41 Rev. 1). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-41r1

National Institute of Standards and Technology. (2013). *Guide to malware incident prevention and handling for desktops and laptops* (Special Publication 800-83 Rev. 1). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-83r1

National Institute of Standards and Technology. (2017). *Digital identity guidelines: Authentication and lifecycle management* (Special Publication 800-63B). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-63b

National Institute of Standards and Technology. (2018). *Framework for improving critical infrastructure cybersecurity* (Version 1.1). U.S. Department of Commerce. https://doi.org/10.6028/NIST.CSWP.04162018

National Institute of Standards and Technology. (2020). *Security and privacy controls for information systems and organizations* (Special Publication 800-53 Rev. 5). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-53r5