# Secure Architecture Report and Recommendations

Prepared by: Anastasiya Gruneva
Date: February 24th, 2025

# Table of Contents

# Executive Summary

As the company rapidly expands from a small business to a mid-sized e-commerce operation, its security infrastructure has not kept pace with its growth. A security assessment has revealed several critical vulnerabilities, including a flat network architecture, weak authentication controls, outdated endpoint security, and a lack of network monitoring. These issues expose the company to significant cybersecurity risks, such as data breaches, financial fraud, and operational disruptions.

To address these risks, this report proposes a structured security architecture strategy based on the NIST Cybersecurity Framework (CSF). Key recommendations include:

- **Network Segmentation:** Implement VLANs and a demilitarized zone (DMZ) to separate public-facing services from internal resources.
- **Identity and Access Management (IAM):** Enforce multi-factor authentication (MFA), implement role-based access control (RBAC), and establish strong password policies.
- **Endpoint Security and Patch Management:** Deploy centralized patch management, update endpoint security tools, and restrict administrative privileges.
- **Intrusion Detection and Network Monitoring:** Deploy an Intrusion Detection System (IDS) and integrate Security Information and Event Management (SIEM) for real-time threat detection.
- **Secure Data Storage and Encryption:** Encrypt sensitive customer data in transit and at rest, and migrate databases to dedicated servers with restricted access.
- **Incident Response and Recovery Planning:** Develop a formal Incident Response Plan (IRP), implement regular encrypted backups, and establish a disaster recovery strategy.

A phased implementation strategy has been recommended to ensure smooth adoption, minimize operational disruptions, and align with industry best practices such as PCI DSS and NIST SP 800-53. By adopting these measures, the company will significantly enhance its cybersecurity resilience, protect customer data, and maintain trust in its services.

# Introduction

## Purpose of the Report

This report aims to assess the company's current security posture, identify security gaps, and propose an action plan using the NIST CSF to improve cybersecurity resilience.

## Scope

Evaluates security risks related to network topology, systems and assets.
Planned growth from a small operation to a medium sized one in a few short months.

## Limitations

The assessment is based on available system architecture information.
Some recommendations may require additional budget and resource allocation.

# Current Security Landscape

Identified Security Weaknesses:

**Flat Network Architecture**
All devices, including public-facing services (e.g., e-commerce website, payment gateway) and internal resources, are on the same network segment. This increases the risk of lateral movement in case of a breach.

**Web & Payment Services on the Same Server**
The same server hosts the website, internal business records, and payment gateway, making it a single point of failure and increasing attack risks.

**Database & Web Server on the Same Machine**
A single physical server hosts both the e-commerce website and the customer database, increasing risk exposure.

**Weak Authentication & Access Controls**
Employees use simple username/password combinations.
Guest and employee wireless networks are not properly secured.

**Lack of Endpoint Security Maintenance**
Endpoint security solutions (antivirus, firewalls) are outdated and not regularly patched.

**Lack of Network Monitoring & Intrusion Detection**
No monitoring or intrusion detection system in place to identify potential threats.

**No Security Awareness Training for Employees**
Employees may fall victim to phishing attacks or inadvertently expose data.

**Unsecured Wireless Network**
The wireless network relies on weak username and password combinations.

**Lack of Secure Backup & Disaster Recovery Plan**
No mention of backups or disaster recovery strategy.

# Security Architecture Goals

Table 1. Full-Scale Mapping (*Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*, 2018)

| **Organization**: E-Commerce Company \| **Approach:** Internal Controls Approach | | | | | |
|---|---|---|---|---|---|
| **Function** | **Category** | **Subcategory** | **Profile** | | |
| | | | **Current** | **Target** | **Gaps** |
| Protect | Identity Management, Authentication and Access Control (PR.AC) | Network segmentation is implemented to limit access. (PR.AC-5) | All devices, including public-facing services (e.g., e-commerce website, payment gateway) and internal resources, are on the same network segment. | Network segmentation by separating the public-facing servers from internal resources using VLANs and a demilitarized zone (DMZ). The payment gateway and website should be isolated from the internal network. | Flat network architecture with no segmentation. |
| Protect | Identity Management, Authentication and Access Control (PR.AC) | Users, devices, and other assets are authenticated (e.g., singlefactor, multi-factor) commensurate with the risk of the transaction. (PR.AC-7) | - Employees use simple username/password combinations.<br>- Guest and employee wireless networks are not properly secured.<br>- The wireless network relies on weak username and password combinations. | - Implement multi-factor authentication (MFA) for employees accessing sensitive systems.<br>- Enforce strong password policies with regular updates.<br>- Set up role-based access control (RBAC) to ensure the principle of least privilege.<br>- Establish separate Wi-Fi networks for employees and guests. | Weak password policies.<br>No MFA.<br>No separate guest and employee wireless networks.<br>No RBAC. |
| Protect | Data Security (PR.DS) | Adequate capacity to ensure availability is maintained. (PR.DS-4) | - The same server hosts the website, internal business records, and payment gateway, making it a single point of failure and increasing attack risks.<br>- A single physical server hosts both the e-commerce website and the customer database, increasing risk exposure. | - Separate web and payment servers to enhance security. The payment gateway should be hosted in a secure, isolated environment following PCI DSS compliance.<br>- Deploy a dedicated database server with restricted access.<br>Encrypt sensitive customer data both in transit and at rest. | Lack of segmentation and redundancy.<br>Lack of data encryption. |

| | | | | | |
|---|---|---|---|---|---|
| Protect | Awareness and Training (PR.AT) | All users are informed and trained. (PR.AT-1) | Employees may fall victim to phishing attacks or inadvertently expose data. | Conduct regular security awareness training on phishing, password hygiene, and safe internet practices. | No training program for employees. |
| Protect | Maintenance (PR.MA) | Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools. (PR.MA-1) | Employee Devices - desktop computers or laptops, outdated, not patched software | Use centralized patch management (e.g., Windows Update, endpoint security). Implement basic endpoint protection (free or low-cost antivirus/EDR). Restrict admin rights and enforce strong password policies. | Regular patching. Updated EDR/antivirus. Strong password policy. |
| Detect | Security Continuous Monitoring (DE.CM) | The network is monitored to detect potential cybersecurity events. (DE.CM-1) | No monitoring or intrusion detection system in place to identify potential threats. | Deploy a SIEM (Security Information and Event Management) system or an Intrusion Detection System (IDS) to monitor network traffic and detect anomalies. | No intrusion detection system (IDS) or network monitoring. |
| Recovery | Recovery Planning (RC.RP) | Recovery plan is executed during or after a cybersecurity incident. (RC.RP-1) | No mention of backups or disaster recovery strategy. | Implement regular encrypted backups, store them offsite, and test disaster recovery procedures to ensure business continuity. | No disaster recovery plan in place. |

By implementing these security measures, the e-commerce company can significantly reduce its risk exposure and strengthen its overall cybersecurity posture. Addressing the identified gaps through network segmentation, strong authentication controls, security training, and continuous monitoring will help protect critical business assets, ensure regulatory compliance, and enhance customer trust. A proactive approach to cybersecurity, combined with regular assessments and updates, will create a more resilient and secure infrastructure for the organization's long-term success.

# Security Architecture Recommendations

To enhance the security posture of the mid-sized e-commerce company, we propose a series of security architecture improvements across various domains. These recommendations align with industry best practices and security frameworks such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) (*Cybersecurity Framework | NIST*, n.d.) and Payment Card Industry Data Security Standard (PCI DSS v4.0) (*Official PCI Security Standards Council Site*, n.d.).

## Network Security

Recommendation: Implement Network Segmentation

- **Issue:** The current flat network architecture allows all devices, including public-facing services and internal resources, to exist on the same network, increasing the risk of lateral movement by attackers.
- **Solution:** Implement network segmentation by creating separate VLANs for public-facing services (e.g., e-commerce website, payment gateway), internal resources, and employee workstations (*Guide to a Secure Enterprise Network Landscape*, 2022). Introduce a demilitarized zone (DMZ) for public-facing services (*NIST SP 800-41, Revision 1, Guidelines on Firewalls and Firewall Policy*, n.d.).

Recommendation: Deploy an Intrusion Detection and Prevention System (IDS/IPS)

- **Issue:** The company lacks network monitoring and an intrusion detection system, leaving it vulnerable to undetected threats.
- **Solution:** Deploy an Intrusion Detection and Prevention System (IDS/IPS) to monitor and block malicious activities in real time (*Security and Privacy Controls for Information Systems and Organizations*, 2020).

## Data Security

Recommendation: Encrypt Data at Rest and in Transit

- **Issue:** Sensitive customer data, including personal details and order history, is stored on an unencrypted database, making it a target for breaches.
- **Solution:** Implement AES-256 encryption for data at rest. Use TLS 1.3 for secure data transmission. Restrict access to sensitive data following the principle of least privilege (PoLP) (*Official PCI Security Standards Council Site*, n.d.).

## Endpoint Security

Recommendation: Centralized Patch Management and Endpoint Protection

- **Issue:** Employee devices run outdated software with unpatched vulnerabilities.
- **Solution:** Deploy a centralized patch management system to ensure timely updates. Implement endpoint detection and response (EDR) solutions for proactive threat monitoring. Restrict administrative privileges to limit unauthorized software installations (*CIS Critical Security Controls Version 8*, n.d.).

## Identity and Access Management (IAM)

Recommendation: Implement Multi-Factor Authentication (MFA) and Role-Based Access Control (RBAC)

- **Issue:** The company relies on simple username/password authentication, increasing the risk of unauthorized access.
- **Solution:** Enforce multi-factor authentication (MFA) for employee access to sensitive systems. Implement role-based access control (RBAC) to ensure employees only have access to necessary resources. Enforce strong password policies with periodic updates and complexity requirements (*Digital Identity Guidelines: Authentication and Lifecycle Management*, n.d.).

## Cloud Security

Recommendation: Secure Cloud-Based Services

- **Issue:** The company uses cloud services but lacks visibility into security configurations and data access.
- **Solution:** Enable cloud security posture management (CSPM) tools to continuously monitor misconfigurations. Apply least privilege access to cloud-based data storage. Implement logging and monitoring for cloud resources (*NIST SP 800-144, Guidelines on Security and Privacy in Public Cloud Computing*, 2011).

## Incident Response

Recommendation: Develop and Implement an Incident Response Plan (IRP)

- **Issue:** There is no documented plan for handling security incidents.

- **Solution:** Develop a formal incident response plan (IRP) aligned with NIST SP 800-61 (*Computer Security Incident Handling Guide*, n.d.). Conduct regular incident response drills and tabletop exercises. Implement security information and event management (SIEM) solutions for real-time threat detection.

By implementing these security recommendations, the e-commerce company will strengthen its security defenses, reduce the risk of cyberattacks, and ensure compliance with industry standards. A layered security approach involving network segmentation, strong IAM policies, endpoint protection, cloud security enhancements, and a robust incident response plan will significantly improve the company's security posture and resilience against threats.

# Implementation Strategy

To enhance the security posture of the e-commerce company, a phased approach will be followed to ensure systematic and effective implementation of security controls. Each phase will focus on a specific security domain, aligning with industry best practices such as NIST SP 800-53, PCI DSS, and CIS Controls.

## Phase 1: Immediate Security Enhancements (0-3 Months)

1. Network Segmentation & Infrastructure Upgrades

- Implement VLANs and a demilitarized zone (DMZ) to isolate public-facing services.
- Deploy a dedicated payment gateway server separate from internal resources.
- Install and configure a stateful firewall to enforce access controls.
- Resource Requirements: Network engineer, firewall appliance, VLAN-compatible switches.

2. Identity and Access Management (IAM) Hardening

- Enforce multi-factor authentication (MFA) for all employees accessing internal systems.
- Implement role-based access control (RBAC) to enforce the principle of least privilege.
- Require strong password policies with periodic resets.
- Resource Requirements: IAM administrator, policy enforcement tools, MFA licenses.

3. Endpoint Security and Patch Management

- Deploy centralized patch management for employee devices and servers.
- Upgrade and configure endpoint detection and response (EDR) solutions.
- Restrict administrator privileges on employee devices.
- Resource Requirements: IT administrator, patch management software, EDR licenses.

4. Security Awareness Training

- Conduct phishing simulations and cybersecurity awareness sessions for employees.
- Establish a security policy handbook covering best practices.
- Resource Requirements: Cybersecurity trainer, security awareness software.

## Phase 2: Intermediate Security Measures (3-6 Months)

5. Intrusion Detection and Network Monitoring

- Deploy an Intrusion Detection System (IDS) for real-time network monitoring.
- Integrate Security Information and Event Management (SIEM) for log aggregation.
- Establish continuous monitoring for unusual traffic patterns.
- Resource Requirements: SIEM software, IDS hardware, cybersecurity analyst.

6. Secure Wireless and Remote Access

- Implement separate guest and employee Wi-Fi networks.
- Enforce VPN access for remote employees with MFA authentication.
- Resource Requirements: Secure Wi-Fi controllers, VPN solution.

7. Secure Data Storage and Encryption

- Migrate customer databases to a dedicated database server with restricted access.
- Implement encryption for sensitive data in transit and at rest.
- Resource Requirements: Database administrator, encryption tools.

## Phase 3: Long-Term Security Maturity (6-12 Months)

8. Incident Response and Recovery Planning

- Develop a formal Incident Response Plan (IRP) and conduct tabletop exercises.
- Implement a secure backup strategy with encrypted offsite backups.
- Establish a Disaster Recovery (DR) plan and test it regularly.
- Resource Requirements: Security team, cloud backup service.

9. Cloud Security Enhancements

- Implement cloud security posture management (CSPM) to monitor configurations.
- Enforce Zero Trust Architecture (ZTA) principles for cloud access.
- Resource Requirements: Cloud security engineer, CSPM solution.

10. Compliance and Audits

- Conduct internal security audits to assess compliance with NIST, PCI DSS, and CIS standards.

- Engage third-party penetration testing services to evaluate vulnerabilities.
- Resource Requirements: Compliance officer, third-party security auditor.

By following this phased approach, the e-commerce company will significantly enhance its security posture, reducing risks associated with cyber threats. Regular assessments and iterative improvements will ensure continued protection of critical assets, customer data, and business operations.

# Conclusion

The security assessment highlights critical vulnerabilities that must be addressed to safeguard the company's infrastructure, data, and customer trust. Without immediate action, the company remains exposed to cyber threats that could result in financial loss, regulatory penalties, and reputational damage.

Implementing the recommended security architecture will provide a robust defense against potential attacks. Network segmentation, strong authentication controls, endpoint protection, continuous monitoring, and a solid incident response strategy will help mitigate risks and ensure business continuity.

Cybersecurity is not a one-time effort but an ongoing process. Regular security assessments, employee training, and adherence to industry best practices will help the company maintain a resilient security posture. By proactively investing in cybersecurity now, the company will be better positioned for sustainable growth and long-term success in an increasingly digital marketplace.

# Video Presentation

https://drive.google.com/file/d/1uYLJjrYjacErTpgwtHpuarril_Q0fpWq/view?usp=drive_link

# References

*CIS Critical Security Controls Version 8*. (n.d.). CIS Center for Internet Security. Retrieved February 24, 2025, from https://www.cisecurity.org/controls/v8

*Computer Security Incident Handling Guide*. (n.d.). NIST Technical Series Publications. Retrieved February 24, 2025, from https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

*Cybersecurity Framework | NIST*. (n.d.). National Institute of Standards and Technology. Retrieved February 24, 2025, from https://www.nist.gov/cyberframework

*Digital Identity Guidelines: Authentication and Lifecycle Management*. (n.d.). NIST Technical Series Publications. Retrieved February 24, 2025, from https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-63b.pdf

*Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*. (2018, April 16). NIST Technical Series Publications. Retrieved February 24, 2025, from https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

*Guide to a Secure Enterprise Network Landscape*. (2022, November 10). NIST Technical Series Publications. Retrieved February 24, 2025, from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-215.pdf

*NIST SP 800-144, Guidelines on Security and Privacy in Public Cloud Computing*. (2011, December 14). NIST Technical Series Publications. Retrieved February 24, 2025, from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf

*NIST SP 800-41, Revision 1, Guidelines on Firewalls and Firewall Policy*. (n.d.). NIST Technical Series Publications. Retrieved February 24, 2025, from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-41r1.pdf

*Official PCI Security Standards Council Site*. (n.d.). Retrieved February 24, 2025, from https://east.pcisecuritystandards.org/document_library

*Security and Privacy Controls for Information Systems and Organizations*. (2020, September 5). NIST Technical Series Publications. Retrieved February 24, 2025, from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf