**Secure Architecture Report and Recommendations**

James Kuzhilaparambil

Contents

[Executive Summary 3](#_heading=h.gjdgxs)

[Section 1: Introduction 3](#_heading=h.30j0zll)

[Section 2: Current Security Landscape 3](#_heading=h.1fob9te)

[Section 3: Security Architecture Goals 3](#_heading=h.3znysh7)

[Section 4: Security Architecture Recommendations 3](#_heading=h.2et92p0)

[Section 5: Implementation Strategy 4](#_heading=h.tyjcwt)

[Section 6: Conclusion 4](#_heading=h.3dy6vkm)

[References : 5](#_heading=h.1t3h5sf)

## Executive Summary

The current security landscape of the mid-sized e-commerce company reveals several vulnerabilities and gaps that need addressing to ensure robust protection of assets and data. This report outlines the goals of security architecture and provides detailed recommendations to mitigate identified risks.

### Section 1: Introduction

The purpose of this report is to provide a comprehensive set of recommendations to enhance the security architecture of the e-commerce company. The scope includes network security, data security, endpoint security, IAM, cloud security, incident response, and physical security. Limitations in the assessment include the lack of real-time data and potential changes in the threat landscape.

### Section 2: Current Security Landscape

The existing security architecture has several vulnerabilities:

* Flat Network Architecture: Increases risk of lateral movement by attackers.
* Single Server for Web and Database: Increases risk of data breaches.
* Outdated Antivirus Software: Makes employee workstations vulnerable to malware.
* Lack of Network Monitoring: No effective network monitoring or intrusion detection system.
* Simple Passwords for Wireless Network: Increases the risk of unauthorized access.
* Limited Access Controls: Insufficient access controls for the payment processing system.

### Section 3: Security Architecture Goals

The security architecture aims to:

* Protect customer data and payment information.
* Ensure compliance with industry standards and regulations.
* Support future growth and scalability.
* Enhance overall security posture to mitigate risks.

### Section 4: Security Architecture Recommendations

#### Network Security

* Implement Network Segmentation: Isolate public-facing services from internal resources.
* Deploy Separate Servers: Use separate servers for web and database functions.

#### Data Security

* Advanced Encryption: Implement advanced encryption methods and regular audits for customer data.

#### Endpoint Security

* Upgrade Antivirus Software: Use advanced endpoint protection and ensure regular updates.

#### Identity and Access Management (IAM)

* Role-Based Access Control (RBAC): Implement RBAC with multi-factor authentication (MFA) for the payment processing system.

#### Cloud Security

* Secure Cloud Services: Ensure cloud-based services are configured securely and regularly audited.

#### Incident Response

* Implement Network Monitoring: Use continuous network monitoring with automated alerts to detect and respond to security incidents.

#### Physical Security

* Enhance Physical Security Measures: Ensure physical access controls are in place to protect critical infrastructure.

### Section 5: Implementation Strategy

#### Phased Approach

1. Phase 1: Immediate Actions
   * Implement network segmentation.
   * Upgrade antivirus software.
   * Enhance physical security measures.
2. Phase 2: Short-Term Actions (1-3 months)
   * Deploy separate servers for web and database functions.
   * Implement RBAC with MFA for the payment processing system.
3. Phase 3: Long-Term Actions (3-6 months)
   * Implement advanced encryption methods and regular audits.
   * Secure cloud-based services and conduct regular audits.
   * Implement continuous network monitoring with automated alerts.

## Section 6: Conclusion

The key findings highlight significant vulnerabilities in the current security architecture. Implementing the recommended security measures is crucial to protect the company's assets and data, ensure compliance, and support future growth. The phased approach provides a clear roadmap for enhancing the security posture of the e-commerce company.

### References :

*Cybersecurity Framework | NIST*. (2024, October 21). NIST. https://www.nist.gov/cyberframework

*What is network segmentation?* (2024, July 30). Cisco. https://www.cisco.com/c/en/us/products/security/what-is-network-segmentation.html

Msmbaldwin. (2024, September 27). *Data security and encryption best practices - Microsoft Azure*. Microsoft Learn. https://learn.microsoft.com/en-us/azure/security/fundamentals/data-encryption-best-practices

Splashtop. (2024, September 3). *What is Role-Based Access Control (RBAC)?* https://www.splashtop.com/blog/role-based-access-control

*Endpoint Protection: Its Importance and How it Works*. (2024, October 16). SentinelOne. https://www.sentinelone.com/cybersecurity-101/endpoint-security/endpoint-protection/

*What is continuous monitoring? | CrowdStrike*. (n.d.). https://www.crowdstrike.com/en-us/cybersecurity-101/next-gen-siem/continuous-monitoring/

*Enterprise Security Architecture—A top-down approach*. (n.d.). ISACA. https://www.isaca.org/resources/isaca-journal/issues/2017/volume-4/enterprise-security-architecturea-top-down-approach

MicrosoftGuyJFlo. (2024, August 13). *Microsoft Cybersecurity Reference Architectures (MCRA)*. Microsoft Learn. https://learn.microsoft.com/en-us/security/adoption/mcra

*Cloud Security Alliance Enterprise Architecture Reference Guide | CSA*. (2021, May 18). CSA. https://cloudsecurityalliance.org/press-releases/2021/05/18/cloud-security-alliance-enterprise-architecture-reference-guide-v2-harmonizes-business-security-and-technology