

Network Infrastructure and Security Plan for Nozama

Posted on October 9, 2018

View this essay online:

<https://academic-master.com/network-infrastructure-and-security-plan-for-nozama/>

Introduction

Nozama is a fictional online retailer selling printed books and e-books, so its network infrastructure must support continuous customer access while protecting payment, account, order, and digital-content data. A modern design should not reproduce an older model in which every service is placed on a separately purchased physical server. The stronger architecture is cloud-first and hybrid: customer-facing applications, managed databases, object storage, backups, monitoring, and scalable compute operate across redundant cloud availability zones, while office networks and employee devices connect through controlled identity-based access. The design should minimize the amount of payment-card data Nozama stores, rely on a reputable compliant payment provider, encrypt sensitive information, segment public and private systems, and plan recovery before the store launches. Security should follow current risk-management principles rather than depend on one firewall at the network edge. The most important design objectives are availability, confidentiality, integrity, scalability, maintainability, and rapid recovery. Those objectives translate business requirements into measurable service levels for checkout, e-book delivery, administration, customer support, inventory, and employee collaboration (NIST, 2024).

Architecture and Network Segmentation

Internet users should reach Nozama through resilient domain-name services, distributed-denial-of-service protection, a content-delivery network, and a web application firewall before traffic reaches a load balancer and application workloads operating in at least two availability zones. Customer-facing application instances should remain stateless where practical so capacity can scale automatically during promotions or seasonal demand. Databases, object storage, secrets, and administrative interfaces should remain in private network segments that are not directly reachable from the public internet. Firewall rules and cloud security groups should allow only required connections and deny other traffic by default. Development, testing, and production environments should also be isolated so that a compromised test system cannot become a path to customer records. The office network should use separate logical segments for managed employee devices, guest wireless access, printers, voice systems, and any operational equipment. Segmentation does not eliminate security risk, but it reduces an attacker's ability to move laterally and limits the number of systems affected by a single

credential or device compromise.

Identity, Applications, and Data Protection

Identity should be treated as the primary control boundary. Employees and administrators need centralized accounts, multifactor authentication, role-based permissions, prompt removal of access when responsibilities change, and stronger protections for privileged roles. Customer authentication should support long passwords, password managers, rate limiting, breached-password screening, secure recovery, and optional or risk-based multifactor verification. Applications should be built through a controlled software-development lifecycle with code review, dependency scanning, secrets detection, automated testing, and separate deployment stages. Databases should use encryption at rest, parameterized queries, managed credentials, restricted administration, and backups tested through restoration. E-books are better stored in encrypted object storage than on a shared file server; after a customer's purchase is verified, the application can generate a time-limited download link instead of exposing storage directly. Reading history deserves particular privacy attention because it can reveal political, religious, health, or personal interests. Nozama should collect only the data required for transactions, support, lawful obligations, and clearly explained personalization.

Payments, Endpoints, and Third Parties

Nozama should reduce payment risk by using a reputable payment service provider that hosts or tokenizes sensitive card entry, allowing the retailer to retain transaction references rather than full card details wherever possible. This can reduce PCI DSS scope, although the company still has responsibilities for website security, scripts, administrative access, policies, vulnerability management, and incident response. Third-party browser scripts used for analytics, advertising, reviews, or chat require particular oversight because compromised scripts can capture information from payment or account pages. Nozama should inventory and approve these components and monitor unexpected changes. Employee devices need centralized management, full-disk encryption, supported operating systems, automatic patching, endpoint detection and response, screen locking, and removal of unnecessary local administrator rights. Managed business email is preferable to maintaining a small independent mail server because mature providers can supply filtering, availability, retention, and authentication controls. Domain protections such as SPF, DKIM, and DMARC should reduce spoofing, while transactional customer messages should remain separated from marketing campaigns to protect deliverability.

Monitoring, Backups, and Incident Response

Security controls are incomplete without evidence that they are functioning. Nozama should centralize logs from identity systems, cloud administration, applications, endpoints, network security

controls, databases, payment workflows, and privileged activity. Alerts should prioritize events with clear business significance, including creation of new administrators, disabled security controls, unusual data exports, repeated authentication failures, payment-page changes, or access from impossible locations. Backups should be automated, encrypted, versioned, and isolated from ordinary administrator credentials so ransomware or account compromise cannot easily delete both production data and recovery copies. Recovery time objectives and recovery point objectives should be defined according to business impact; checkout and order data require more aggressive targets than archived internal documents. The incident-response plan should identify who can disable accounts, block traffic, isolate devices, contact providers, preserve evidence, notify customers or regulators, and restore systems. Exercises should test scenarios such as identity-provider outage, database corruption, ransomware, payment-provider disruption, and a major cloud-service failure rather than assuming backups alone guarantee continuity.

Governance, Cost, and Implementation

A practical infrastructure plan also needs financial and managerial discipline. Initial costs include application development, architecture, employee devices, office networking, migration, testing, legal and compliance review, and security implementation. Recurring costs include cloud compute, bandwidth, storage, payment fees, managed email, backups, monitoring, security services, software licenses, support platforms, staff, insurance, and periodic penetration testing. Cloud services should therefore be modeled under ordinary and peak demand, with budgets and alerts to prevent uncontrolled consumption. Technology ownership must be explicit: senior leadership owns business risk, technical staff own architecture and operations, security leadership coordinates controls and incidents, developers own secure code, and business owners approve access to data. Outsourcing a service does not outsource accountability. Implementation should proceed in phases, beginning with identity, logging, network boundaries, backup, payment design, and infrastructure-as-code foundations before customer data is introduced. Security testing and recovery exercises should occur before launch and continue after major architectural changes rather than being treated as one-time certification events.

Conclusion

Nozama's network should be designed as a resilient e-commerce system rather than as a collection of isolated servers. A cloud-first hybrid architecture provides elastic capacity, managed infrastructure, geographic redundancy, and easier recovery, while segmentation and identity-based access reduce unnecessary trust between systems. Public applications, private data stores, employee devices, payment functions, and development environments should be separated according to risk. Payment-card exposure should be minimized through tokenization and specialized providers, while e-books and customer information should use encrypted storage and controlled delivery. Security monitoring, tested backups, incident response, privacy governance, and endpoint management are as important

as web servers and bandwidth because availability and confidentiality depend on operational discipline after deployment. Nozama should therefore evaluate infrastructure through measurable outcomes: service availability, restoration performance, patching, vulnerability reduction, access reviews, incident handling, and customer impact. The strongest architecture is one that can grow without requiring security to be redesigned after every increase in traffic, staff, applications, or product features.

References

National Institute of Standards and Technology. (2024). *Cybersecurity Framework 2.0*.
National Institute of Standards and Technology. (2020). *Zero Trust Architecture*, SP 800-207.
PCI Security Standards Council. (2024). *PCI DSS v4.0.1*.
OWASP Foundation. (2021). *OWASP Top 10*.