BookShop Enterprises Zero Trust Architecture Gap Analysis

Networking Equipment

Asset	Current State	ZT Gap	Risk Level	Remediation
ISP Modem	Router mode, ISP managed, NAT/Firewall used	No org control, minimal monitoring, single trust boundary	High - potential to completely compromise perimeter	Switch ISP modem to bridge mode. L3 switch for routing. Add firewall for traffic inspection with allow/deny capabilities and add traffic monitoring.
Store Network Access	Single WPA3 network with password protection	No segmentation	Medium - limited defense in depth	Create separate VLANs. Create segmentation between internal and guest networks. Utilize ACL to manage traffic traversing network.
Guest Network	No separate guest network. Shoppers are provided access to single store network upon request.	No separation between internal and guest traffic.	Medium - guests are able to take any action on the network without monitoring.	Implement captive portal. Capture device MAC addresses. Use management panel to block devices with malicious activity.
ISP	Single ISP	No backup ISP option set up	Medium - BC risk	Arrange for backup internet connectivity
Access Points	5 APs using	No network	High - current	Implement

	WPA3 encryption	isolation, limited visibility into connected devices.	setup creates opportunities for lateral movement in the event of a compromise.	802.1X for employees and/or company devices. Use separate SSIDs for VLAN segmentation. WIPS/WIDS.

Security Gap & Remediation

Gap ID	Current State	Required State	Priority
N1	Single network exists. Used for internal use with some guests given access.	Implement micro-segmentation with deny-by-default ACLs.	Medium - excessive trust.
N2	No network monitoring	Implement SIEM for all network devices with real-time alerts.	High - invisible attacks possible.

Compliance

Requirement	Gap Reference	Notes
PCI DSS v4.0, 1.3	N1	Only wireless traffic with an authorized business purpose is allowed into the CDE.

Device Management

Type	Total Count	Managed	Compliant	Unknown
Company Laptops	12	12/12	12/12	N/A
BYOD Devices	13	0	N/A	13/13

Mobile phones	25	20/25	20/20	N/A

Security Gaps & Remediation

Gap ID	Finding	Risk Level	Affected Devices	Maturity Level	Remediation
D1	Unmanaged BYOD devices without compliance checks	High - non-compliant devices are vulnerable to attacks	13 user laptops	Traditional	Include compliance checks for all devices when attempting to access company resources
D2	Mobile phones not using Company Portal. No compliance checks	Medium - vulnerable devices create a pathway for malicious attacks to gain access to company resources on user devices.	20 mobile phones	Traditional	Deploy an agent on these devices to report device health status. [Research some more]
D3	All company laptops compliant, however, lack detection tools	Medium - devices under attack do not send automated alerts	13 company owned devices	Initial	Deploy agents on devices to generate alerts on potential threats

Compliance

Requirement	Gap Reference	Notes
PCI DSS v4.0, 2.2.7	D2	BYOD devices

Identity Management

Component	Current Implementation	Maturity Level
Authentication	All users are prompted to reset default password on initial sign in to cloud environment. Users provide preferred password to admin upon user creation for Bookshop app access.	Traditional
MFA Authentication	Users are prompted to set up MFA on initial sign into cloud environment. No MFA set up for Bookshop application access.	
User Deprovisioning	There is no set SLA for user deprovisioning requests	Traditional
Account Audits	Company takes a reactive approach to account audits.	Traditional
Privileged Access	Admins are granted permanent rights.	Traditional
Session Management	All accounts, including admin, never timeout. The session continues when the user accesses the portal again.	Traditional

Security Gaps & Remediation

Gap ID	Finding	Current state	Desired State	Risk Level
I1	No context-based factors for authentication	Password + MFA only	Password + MFA + Context for sensitive accounts (CA policy)	Low - Password + MFA handles most of the attempts at unauthorized access
I2	Static privilege assignment	24/7 access to admin privileges for privileges ops	Just-in-time access for Admin accounts needing higher	High - PAM solution needed for privileged solutions.

			privileges	Establish quarterly audit tasks
I3	Lack of session management	Users are timed out of sessions after 24 hours	Implement time outs for sensitive accounts after 6 hours of inactivity	Medium - session may be hijacked
I4	Account audit frequency	Accounts are audited only when an event occurs	Accounts should be audited every 90 days	Medium - disabled accounts could be used for unauthorized access. Accounts with changes roles may have leftover perms.
I5	User deprovisioning	No urgency or set SLA for user deprovisioning requests	Set SLA needed. Preferably 1 hour to disable users' access to all assets	Medium - malicious termed employees could use their active access to harm company
I6	Weak authentication	Password handling in the bookshop application lacks sophistication.	Implement SSO for authentication & authorization handling.	High - admins know users' passwords. No data at rest encryption. No MFA.

Compliance (double check)

Requirement	Status	Gap Reference	Notes
PCI DSS 8.3?	Compliant	I1	Password + MFA required for all users at minimum
NIST 800-63B	Compliant	I1	Authentication mechanisms meets criteria

ISO 27001 A.9.4	Non-compliant	I2	Privileged Access Management required
ISO 27001 A.5.18	Non-compliant	I4, I5	User account deprovisioning policy & account audit policy.

Data Flows

Name	Assets Involved	Data flow	Data Sensitivity	Encrypted?	Risk Level
Order lookups	Web app, bookshop-db	1. user input, 2. query construction, 3. database query, 4. data retrieval, 5. results displayed	Medium - potential PII from order information. Output includes name and address.	Yes - data being passed from web application to db is encrypted by TLS.	High - there are no controls in place to protect from injection attacks.
Adding Products	bookshop-db, web app	1. Admin auth, 2. Add Book, 3. Enter details, 4. Form submission, 5. Database insert, 6. Action logged	High - vulnerable to injection attacks & CSRF, no input validation, lacks RBAC, weak session management	Yes/No - Encryption is used for data in transit. No encryption for data at rest.	High - known and highly exploited web app attacks are possible.
User Management	bookshop-db, web app	1. Admin auth, 2. View users list, 3. Select action (deactivate, reset password, delete), 4. Action submission 5. Database, insert/update.	High - all employees have super admin access. Lacks proper logging.	Yes/No - Encryption is used for data in transit. No encryption for data at rest.	High - No RBAC, lack of encryption algorithms, missing least privilege implementation.

Security Gaps & Remediation

Gap ID	Current State	Desired State	Priority
DF1	Web application attacks possible	Application should be resistant to common web app attacks like injection attacks, XSS, CSRF.	High - these attacks are widely known and exploited with available fixes.
DF2	All employees have the same level of management access.	Implement RBAC and principle of least privilege.	High - sensitive customer data and user data is available to all employees.
DF3	Missing user management logging	Log all actions taken on user & customer management	High - no visibility into who did what and when within the application.

Compliance

Requirement	Gap Reference	Notes
ISO 27001, 8.15	DF3	Requires that activities taken within the application be logged meaningfully and stored for later access.
PCI DSS v4.0, 7.2.1	DF2	Requires the implementation of least privilege.
PCI DSS v4.0, 6.4.1	DF1	Requires the remediation of vulnerabilities present in public facing web applications.

**Data is encrypted during transit, but lacks 'at-rest' encryption in the database.*
**Shipping address is not sanitized. Vulnerable to XSS.*
**All admins/employees with access to admin panel have full functionality (separate duties in write up)*

Web Application

Component	Current Implementation	Risk Level
User Authentication & Session Management	Only password used for authentication. No rate limiting or incorrect sign-in attempts. Missing session management features. Possible to sign in using SQLi.	High - passwords are highly vulnerable by themselves. SQLi is a well-known and commonly executed web app attack.
Auditing	Missing audit logging.	Medium - important to be able to recreate a timeline of events.

Security Gaps & Remediation

Gap ID	Current State	Required State	Priority
W1	Single authentication method with no password strength requirements.	Implement MFA and password requirement of 12 character minimum with at least 1 character and 1 number.	High - high possibility of user breaches due to lack of protections.
W2	Missing user action audit logging.	Log user activities like password resets, updating profile information, account deactivations and deletions, sign in. Capture metadata like time, location, date, device.	Low

Database

Component	Current Implementation	Risk Level	Artifact
Credential Storage	Lacking encryption for user and admin	High - compromising database means	Appendix A, Appendix B

	credentials stored.	exposure of employee and user credentials.	
Payment Data	No evidence of encryption of Payment information.	High - PCI DSS violations: CVV storage, Payment card data stored without required protections	Appendix C
PII Protections	Single technical user with access to database. No shipping address display in order view. Satisfies control requirements.	Low - Access controls in place to limit damage in the event of a breach.	n/a
Log Audits	A reactive approach is taken to log audits. Need to distribute database duties for better oversight. Currently, only one user working in database.	Medium - access control limits damage, but audits are needed to rule out insider threats.	n/a
Secure storage methods	There is no input sanitization methods in place. Data is stored as received.	High - database is vulnerable to XSS attacks	n/a
Database Account Permissions	bookshopuser has full read/write/delete	High - this vulnerability makes frontend attacks possible. This service account should be limited to Stored Procedure EXECUTE only.	Appendix D
Input Validation & Parameterization	No input validation. Direct string concatenation in SQL queries. No output encoding.	High - vulnerable to highly exploitable web application vulnerabilities. Impact is catastrophic.	n/a

Security Gaps & Remediation

Gap ID	Current State	Required State	Priority
DB1	Lack of proper data storage	Tokenize card #, immediately stop storing CVV #s and card expiration date. Implement bcrypt encryption for password storage.	High - data storage practices are in violation of PCI DSS, GDPR, and ISO 27001.
DB2	No policies for auditing database actions taken on admin accounts.	Perform quarterly audits of database logs and immediate audit on reports of new incidents.	High - these audits help the company be able to identify early control failures.
DB3	bookshopuser account has read/write/delete permissions in database. This is excessive.	Implement the principle of least privilege for bookshopuser account. Limit to EXECUTE permissions on Stored Procedures	High - excessive permissions on this account makes it possible to execute web application attacks with devastating impacts on the database.
DB4	Missing critical data sanitization controls	Use input validation, parameterized queries, and output encoding to limit application attack vectors.	High - the absence of these protections leaves the database vulnerable to several well-known and frequently executed web application attacks.

Compliance & Standards

Requirement	Gap Reference	Notes
PCI DSS v4.0, 3.5	DB1	Card data should be unreadable wherever it is stored.
PCI DSS v4.0, 7.2.1	DB3	Requires the implementation of least privilege.

PCI DSS v4.0, 6.4.1	DB4	Requires the remediation of vulnerabilities present in public facing web applications.