# Security risk assessment report

**Part 1: Select up to three hardening tools and methods to implement**

To mitigate the vulnerabilities found in your social media organization, I have selected three fundamental practices and tools that address identity, access, and perimeter security issues in an integrated manner.

### 1. Multi-Factor Authentication (MFA) Implementation

- **Vulnerability Addressed:** Password sharing and lack of MFA.
- **Action:** Implement an identity provider (such as **Okta**, **Duo**, or **Microsoft Entra ID**) that requires a second authentication factor for all logins.
- **Method:** By requiring a temporary code or approval on a mobile device, password sharing becomes ineffective for attackers, as physical possession of the user's device becomes mandatory for access.

### 2. Privileged Access Management (PAM)

- **Vulnerability Addressed:** Default database passwords and lack of accountability.
- **Action:** Use tools like **HashiCorp Vault** or **CyberArk** to manage database credentials.
- **Method:** The PAM system automatically rotates passwords, eliminates the use of default credentials, and provides "Just-in-Time" access. This ensures that no one knows the actual database password, drastically reducing the risk of exposure.

### 3. Firewall Configuration with "Default Deny" Policy

- **Vulnerability Addressed:** Lack of traffic filtering.
- **Action:** Configure Next-Generation Firewalls (NGFW) such as **Palo Alto** or **Fortinet** to block any and all connections that have not been explicitly allowed.
- **Method:** Create a strict Access Control List (ACL). All inbound and outbound traffic is prohibited by default, and only essential ports (such

as 443 for HTTPS) are opened for specific IPs and services, preventing attackers from moving laterally through the network.

**Part 2: Explain your recommendations**

As a security analyst, I selected these measures because they target the **root cause** of the identified vulnerabilities, creating protection layers known as "Defense in Depth."

### 1. MFA Implementation (Multi-Factor Authentication)

Password sharing is both a cultural and technical issue. MFA solves this by requiring something the user **is** (biometrics) or something the user **has** (a smartphone or security key). Even if an employee shares their password, the attacker will not be able to obtain the dynamic code generated by the account owner's physical device, stopping the attack instantly.

### 2. Privileged Access Management (PAM)

Keeping default passwords on databases is like leaving a master key under the doormat. A PAM solution takes password control out of human hands and gives it to secure software. It automatically rotates the database password (e.g., every 24 hours) and requires administrators to "request" access from the system, logging exactly who did what and when.

### 3. Firewall with "Default Deny" Policy

Currently, your network is like a house without doors. Configuring the firewall with "Default Deny" flips the current logic: instead of trying to guess what is dangerous, we block **everything** and only open what is essential for the business. This prevents an attacker who has compromised one computer from spreading to other servers (lateral movement) or sending stolen data out of the network.