

# Security risk assessment report

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

**Password Management System**  
**Firewall Configuration and Monitoring Tools**  
**Multifactor Authentication (MFA) Solutions**

## Part 2: Explain your recommendations

### 1. Password Management System

**Description:** A password management system helps in creating, storing, and managing strong, unique passwords for all users within the organization. This tool ensures that employees do not share passwords and adhere to the company's password policy.

### 2. Firewall Configuration and Monitoring Tools

**Description:** Properly configured firewalls with continuous monitoring tools are essential to control and filter the traffic that enters and exits the network. These tools help in identifying and blocking unauthorized access attempts and suspicious activities.

### 3. Multifactor Authentication (MFA) Solutions

**Description:** MFA adds an additional layer of security by requiring users to provide two or more verification factors to gain access to a system. This significantly reduces the risk of unauthorized access, even if a password is compromised.

By implementing these three hardening tools and methods, the organization can significantly improve its security measures, prevent future data breaches, and protect sensitive customer information. These proactive steps will help in mitigating risks, ensuring compliance, and maintaining the integrity and reputation of the organization.