Security risk assessment report

Part 1: Select up to three hardening tools and methods to implement
Multi Factor Authentication (MFA) Implementation • **Description**: Implementing MFA requires users to authenticate using at least two separate factors (such as a password and a mobile device code or biometric). **Firewall Configuration and Traffic Filtering** • **Description**: Configure firewalls to filter incoming and outgoing traffic based on strict security rules. Regularly update the rules to match current threat landscapes. **Password Policy Enforcement and Password Manager Usage** • **Description**: Establish strict password policies, requiring complex and unique passwords. Enforce the use of password managers to help employees securely generate and store passwords.

Part 2: Explain your recommendations
1. **Multifactor Authentication (MFA)**: ○ The use of MFA adds an extra layer of security to user accounts. Even if passwords are compromised, MFA ensures that the attacker would still need access to the second factor (e.g., mobile device) to log in. This is particularly important given the organization's problem of password sharing.

2. **Firewall Configuration**:
    - Firewalls that are correctly configured can detect and block malicious traffic, ensuring that both incoming and outgoing data is controlled and secured. With well-defined rules, the firewall can prevent unauthorized access to sensitive data and stop malicious software from communicating with command-and-control servers.
    -
3. **Password Policy Enforcement & Password Manager**:
    - By enforcing strong password policies and implementing password managers, employees will be discouraged from using weak or shared passwords. Complex passwords, coupled with regular updates, make it harder for attackers to guess or brute-force credentials. Password managers ensure that these complex passwords are easily stored and retrieved, further reducing the need to share them.