Security risk assessment report

Part 1: Select up to three hardening tools and methods to implement
After assessing the organization's vulnerabilities, these are three recommended hardening tools that should be implemented. 1.) Multifactor Authentication (MFA) 2.) Update the admin password for the database / Set Password Policies 3.) Update the firewall to filter traffic coming in and out of the network

Part 2: Explain your recommendations
Implementing MFA will require users to confirm their identity in more than one way (authenticator code, finger print, personal pin, etc..). This will greatly reduce the risk that a malicious actor can access the network by impersonating you through a brute force attack, while also reducing the possibility of employees sharing passwords. Stricter password policies will also greatly reduce the risk that a malicious actor can access the network. These policies may include restricting the amount of login attempts before suspending the account, requiring frequent password updates, or increasing password complexity (adding numbers, special characters, etc..). All of these changes will increase the difficulty of a malicious actor accessing the network. Updating the firewall configurations to filter incoming and outgoing traffic will help stay ahead of potential threats.