Security risk assessment report

Part 1: Select up to three hardening tools and methods to implement
- MFA or 2FA for more secure passwords, and to ensure password sharing is eliminated - Set rules in the firewalls or a NGFW to ensure any known malicious data coming from outside sources is filtered out. - Add an IDS Intrusion detection system or IPS intrusion prevention system to detect or remove any known external internet threats from reaching the company's internal network where all the vital data and resources are located

Part 2: Explain your recommendations
- Since the company doesn't have MFA in place, this is a practical first step in preventing a breach. It is low-cost and only requires each employee to register their personal devices, and will also prevent password sharing. This will also ensure that even if the admin password is set to default, only authorized individuals can access the account.
- Firewall rules can ensure that any unwanted traffic from sources known to be malicious or harmful will be denied. Furthermore, they can be updated regularly to keep up with new threats. This hardening practice is necessary to reduce the load on security team, especially for repeat offenders or commonly known threats.
- And IDS or IPS would be a second line of defense after the firewall, greatly increasing security through alerts or automatic denial of transmission. Whichever one is implemented depends on cost vs risk for the company.