# Security risk assessment report

| Part 1: Select up to three hardening tools and methods to implement |
|---|
| I recommend implementing multi-factor authentication, firewall maintenance, and password policies. |

| Part 2: Explain your recommendations |
|---|
| Implementing multi-factor authentication will make it more difficult for malicious actors to access the network with brute force attacks by requiring identity to be proven using two or more authentication factors. MFA should be maintained regularly once set up. Firewall maintenance will be effective by blocking abnormal traffic and protecting against DDoD attacks. The firewall rules can be configured in response to the latest security incident to block known threats and then managed regularly thereafter. Password policies that prevent employees from sharing passwords and require default passwords to be changed to more complex, frequently updated passwords will prevent threat actors from being able to easily guess passwords or use brute force attacks to perform another data breach. Password policies should be implemented and reviewed yearly as part of an annual security audit. |