# Security risk assessment report

| **Part 1: Select up to three hardening tools and methods to implement** | |
| --- | --- |
| **1. Password Management System** Tool: Enterprise Password Manager (e.g., LastPass, Bitwarden)   * Purpose: Eliminates password sharing and strengthens password security by managing and generating strong, unique passwords.  **2. Firewall Management Software** Tool: Advanced Firewall Management (e.g., Palo Alto Networks, Cisco ASA)   * Purpose: Enhances network security by providing robust rule management, monitoring, and traffic filtering capabilities.  **3. Multifactor Authentication (MFA) Solution** Tool: MFA Implementation (e.g., Duo Security, Google Authenticator)   * Purpose: Adds an extra layer of security by requiring multiple forms of verification to access sensitive systems and data. | |
|

| **Part 2: Explain your recommendations** |
| --- |
| 1. Password Management System  Purpose: Prevents password sharing and enhances security by managing and generating strong, unique passwords.  Benefit: Reduces the risk of unauthorized access and strengthens compliance with security policies.  2. Firewall Management Software  Purpose: Improves network defenses by allowing precise control over traffic flow with customizable rules.  Benefit: Enhances threat detection and prevention capabilities, securing the network from unauthorized intrusions.  3. Multifactor Authentication (MFA) Solution  Purpose: Adds an additional layer of security by requiring multiple forms of user verification to access systems.  Benefit: Significantly lowers the chance of unauthorized access, even if passwords are compromised. |