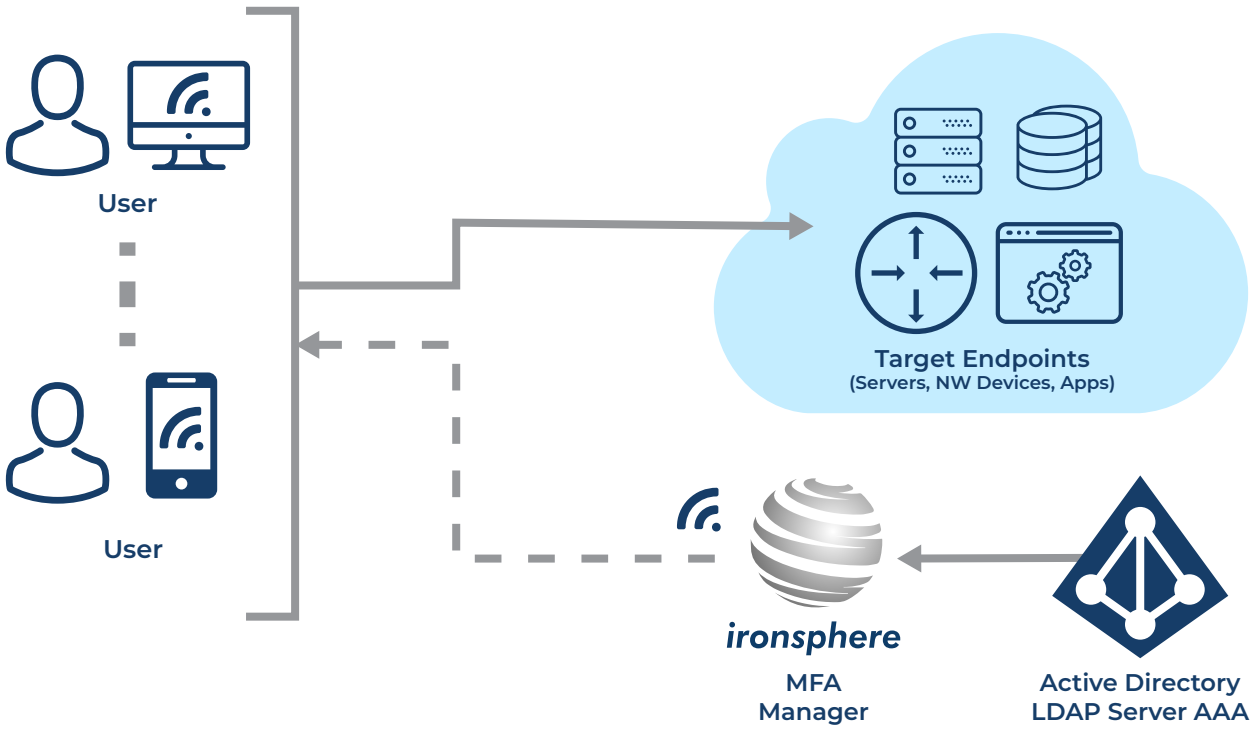
## MFA Manager

There are thousands of different types of accounts in an enterprise infrastructure; personal accounts (of employees, contractors, etc.), local administrative accounts, privileged user accounts, domain administrative accounts, emergency accounts, service accounts, application accounts. You may train your employees on cyber security and take many technical preventive actions, but accounts are still (and will continue to be) hacked/leaked/compromised.

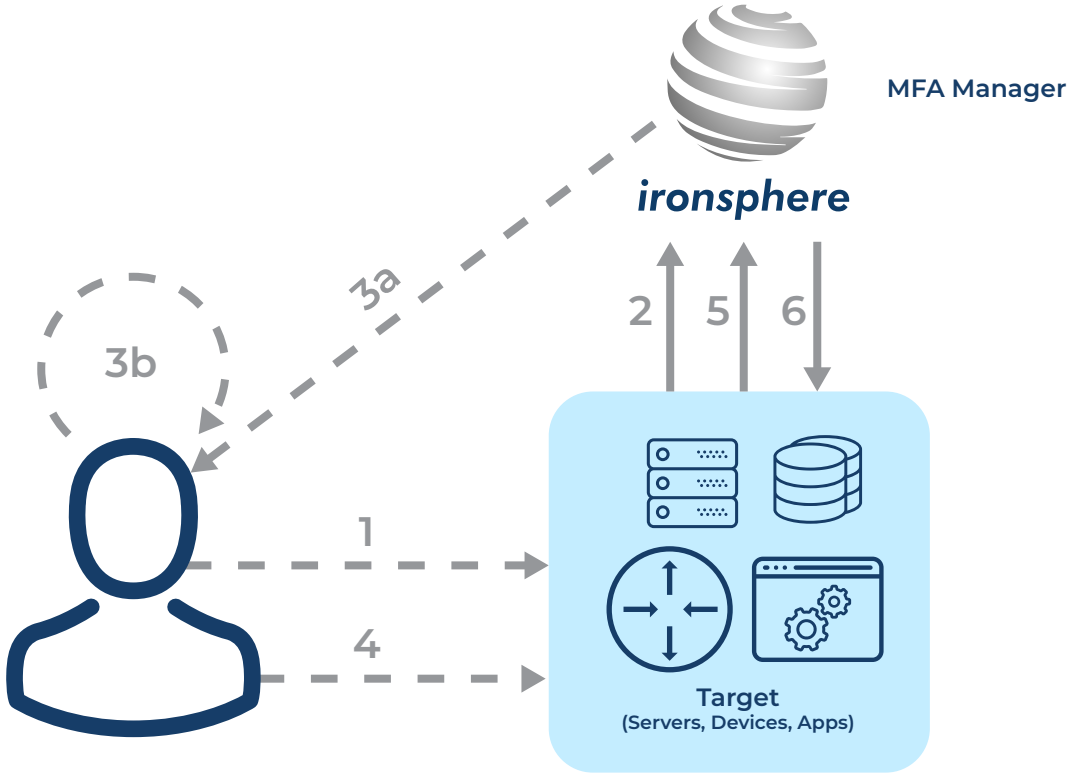
For example, socially engineered malware and phishing attacks are the most common attack types and there is nothing much you can do other than training employees, but they will still accidentally be victims of such attacks. Whatever preventive actions you take, you must have a plan B to prevent compromised accounts/identities from accessing critical data/assets of the enterprise.




## Benefits

- Even if an employee's account is compromised, it is still not possible to access the enterprise's critical assets/resources, unless the employee's mobile phone (or email account) is stolen as well.
- MFA provides another level of security, even if the password is weak or non-expiry.
- Password sharing becomes irrelevant because any passwords shared with colleagues are useless by leveraging the Ironsphere MFA solution.
- Auto lock user account when an employee terminates employment (integration with enterprise Active Directory or LDAP is required).

## How MFA Manager Works




**Step 1:** The user connects to the target host and enters a username/password.

**Step 2:** The target host sends the username/password to Ironsphere's MFA Manager.

**Step 3:** Ironsphere's MFA Manager generates a token (one-time use only), and then either (3a) sends the token to the user (via SMS/email/mobile-app) or (3b) the user generates the same token offline on its mobile app.

**Step 4:** User enters the token.

**Step 5:** Target host sends the token to Ironsphere's MFA Manager.

**Step 6:** Ironsphere's MFA Manager checks whether the received token is correct or not; if yes, access is granted.