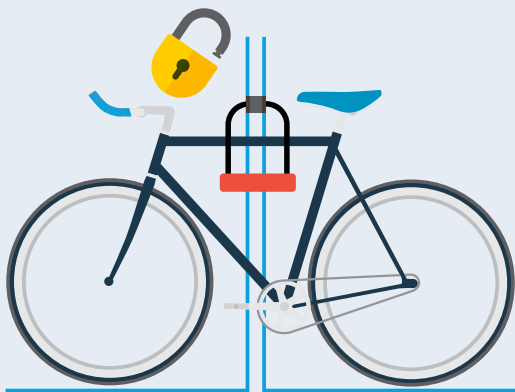


ARE YOU TRYING TO SECURE A CASTLE WITH A PADLOCK?

Uncovering the difference between consumer password managers and enterprise credential managers.

Many Service Desks are seeking solutions to secure credentials, a common target for hackers to try and steal in order to gain access to corporate networks. However, password management needs for help desk admins are substantially different than for regular individuals. Consumer focused products for storing website logins such as 1Password, LastPass or Dashlane are great for personal use but they don't address the needs of privileged users within an enterprise.



PASSWORD MANAGER

- The password manager encrypts password storage to offer users the ability to use a single master password for accessing a number of passwords used for different websites or services.
- Intended for stand-alone users, geared toward consumers.
- Primarily used for website login storage.
- Aids in creating new, complex passwords.
- Typically, no rotation features.
- Injects passwords into a website, and can be used to share passwords but the plain text password is exposed.
- Detect which passwords do not meet complexity standards.
- Each user has a separate instance of the manager.



VAULT ADD-ON FOR REMOTE SUPPORT

- ✓ The password manager encrypts password storage to offer users the ability to use a single master password for accessing a number of passwords used for different IT systems and endpoints.
- ✓ Best for multiple users and teams in security-minded organizations with security policies and compliance regulations to follow.
- ✓ Supports credential Storage for a variety of account types including admin and active directory accounts.
- ✓ Aids in creating new, complex passwords according to specified password policies.
- ✓ Rotates credentials automatically or manually including remotely across networks without a VPN.
- ✓ Inject credentials into end servers and systems and easily shares them with other members of the team without exposing credentials in plain text and tracks when the credential is accessed and by whom.
- ✓ Enforces password complexity standards, retrieves the password age, records who has accessed the password, and detects if a credential has been exposed.
- ✓ One central vault is used for the whole team.

Just like a castle needs a tiered security approach such as a moat and a drawbridge, the vast majority of companies need an enterprise grade password solution to meet their security requirements, especially if they are subject to external compliance mandates.