CyberQP vs.
Traditional Password Managers

Feature	Traditional Password Manager	CyberQP
Stores and shares passwords with team and clients	✓	✓
Password Generation Interface	✓	✓
Technician Password Manager	✗	✓
Automated Privileged Account Password Rotation (Integrations with Microsoft 365, Active Directory and Azure AD)	✗	✓
Self-Service Password Reset	✗	✓
Password Failover Measures	✗	✓
Self-Service End User Identity Verification	✗	✓
Documentation Tool/PSA Integrations	✗	✓

While traditional password managers play a key role in storing and sharing passwords with your team and clients, it becomes time consuming and difficult to update passwords, especially when you're regularly rotating credentials for multiple privileged accounts per client.

Managed Service Providers (MSPs) need a solution with more extended visibility and functionality than traditional password managers can provide.

That's why CyberQP solves those problems by building solutions to make Privileged Access Management easy for MSPs.

You can use our Privileged Access Management suite to secure your Azure AD (O365), local admin and service accounts for end users. Deploy CyberQP' agents and API integrations to automatically rotate these passwords on a daily, weekly or monthly basis.

You'll be able to randomly generate 99 character passwords or easy-to-read passphrases that can be stored in your password manager, or written back to your documentation tool (IT Glue or Hudu).

Trust CyberQP for stronger security, peace-of-mind, and automated solutions that eliminate hours of manual labor from your technician workflows.