Secret Server + Connection Manager

Encrypted password vaults like Secret Server store secrets for your IT infrastructure, applications, and services. Each time IT staff needs to resolve a service request they must access the password vault – or multiple vaults – to gather the credentials required for remote access.

By combining Secret Server with Connection Manager, Thycotic's remote session management solution, you can increase efficiency for your IT team and mitigate the risk of password exposure and misuse.

Save time resolving service requests

IT operations teams have limited time to act on service requests. Whether they're asked to change settings on firewalls or proxies, set up applications and containers, or help struggling business users, they must resolve requests quickly and securely.

Staff can't afford to spend time figuring out how to connect to different applications and operating systems. The time they take to search one or more password vaults for the right secret, or navigate connection protocols like SSH and RDP, is time that's better spent solving problems.

The combination of Secret Server and Connection Manager saves time by injecting credentials directly into a remote session. IT staff don't need to hunt through folders within multiple vaults to find secrets. They don't need to memorize host names, IP addresses, or any password information. They can even store favorites for commonly accessed secrets.

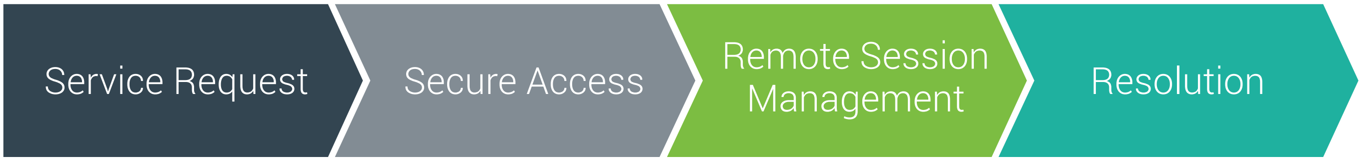
Reduce risk of exposing passwords

When password vaults and session management tools are disconnected, IT staff must manually inject a secret into a target system. Cutting and pasting secrets stores sensitive information in the memory of their system and increases risk of a breach.

The more people and systems accessing secrets, the higher the risk. In addition to internal IT staff, staff outside the firewall need access. Third parties access secrets for specific needs, such as system maintenance. Managed Service Providers need access to all infrastructure, as they monitor for events and tune systems.

Injecting secrets directly into sessions reduces risk of exposure. With the combination of Secret Server and Connection Manager, IT staff and partners can launch and manage remote sessions without ever seeing a password. They access only the secrets they require, regardless of how many vaults your company has. Secret use is limited so they can't change or remove passwords and time-bound to eliminate the need for standing privileges. When secrets are checked out, others won't be able to access them.

The new way of working


Service Request

Secure Access

Remote Session Management

Resolution

Steps to secure remote session management

- Connection Manager provides a single pane of glass to manage all remote sessions, across all systems and connection protocols.
- Users that require secrets access log into Secret Server using multi-factor authentication.
- Once connected, users can request access to secrets, provide a reason if required, and check them out. Users can select only those secrets that are valid for launching remote sessions.
- To launch a session, Secret Server automatically injects secrets and auto-fills usernames and passwords.
- If sessions are time-limited, they end automatically. If other users require access they must wait until secrets are checked back in.
- Secret Server records and logs all session activity to provide oversight and an audit trail, including for remote and third-party teams.

Rapid deployment and elastic scalability

Secret Server is available both on premise and in the cloud. Connection Manager is available on Windows and Mac OS. Integration is a wizard-driven, two-step process.

Convenience and intuitive design

Connection Manager provides a single pane of glass to manage all remote sessions, across all systems, and connection protocols. All vaults are included in one interface so there's no need to search multiple vaults. Users can have multiple tabs open at the same time to manage multiple sessions simultaneously. Ability to see recent connection history and store favorites saves time and effort.

Try Secret Server and Connection Manager for free at Thycotic

Thycotic is focused on the most vulnerable attack vector – privilege. With Thycotic you can adopt a multi-layered approach that covers your privilege security needs from endpoints to credentials, ensuring protection at every step of an attacker's chain. Connection Manager is an advanced remote connection management solution that provides one place to manage and interact with multiple remote sessions. Connection Manager can scale across hundreds of different connections to improve productivity, strengthen security and tighten compliance.