# Password and passkey management your clients will love.

Locke gives your clients post-quantum encryption, E2E encrypted account recovery, and phishing detection that 1Password, Bitwarden, and Keeper cannot match. You get a multi-tenant console, flexible billing, and a security story no other partner can tell.

### Security No One Else Offers

E2E encrypted recovery and post-quantum encryption protect credentials against both today's threats and tomorrow's quantum computers. No other vault does both.

### Flexible Partner Billing

Bill your clients directly and set your own margins, or let Locke handle billing and receive a 15% recurring commission. Per-seat pricing, predictable revenue.

### Deploy in Under 15 Minutes

Connect your existing identity provider, or use Armory (our cloud-native admin console) to configure a new client org from scratch. No infrastructure to stand up.

### All Clients, One Console

Manage every client from a single partner dashboard with client-isolated vaults, per-tenant audit logs, and the option to join their Trusted Circle as a recovery guardian.

## Comprehensive feature set

| CAPABILITY | LOCKE | 1PASSWORD | BITWARDEN | KEEPER | PROTON PASS |
|---|---|---|---|---|---|
| Password Management | Yes | Yes | Yes | Yes | Yes |
| Passkey Login to Vault | Yes | Beta | Yes | Yes | No |
| Post-Quantum Encryption | Yes | No | No | Partial | No |
| Secure Inboxes with Anonymous Emails | Yes | No | No | No | Yes |
| End-to-End Encrypted Recovery | Yes | No | No | No | No |
| Row-Level Encrypted Spreadsheet | Yes | No | No | No | No |
| Impersonation Detection to Stop Phishing | Yes | No | No | No | No |
| **Strong Single Logout (New)** | Yes | No | No | No | No |

Strong Single Logout remotely clears all third-party website cookies and site storage from connected browser profiles, instantly logging out of everything to prevent disgruntled employees from retaining access or attackers moving laterally. Competitive capabilities reflect public vendor documentation reviewed August 2026. Keeper's partial PQ status reflects its client-server transport rollout.

## Book a 20-minute technical walkthrough:

calendly.com/connor-lockeidentity

Or email: connor@lockeidentity.com

## Integrates with your identity stack

### SAML 2.0 SSO

SP-initiated SSO with Okta, Azure AD (Entra), OneLogin, and ADFS. End users get one-click login without a separate master password.

### SCIM Provisioning

Automatic user create, update, and deprovisioning from your IdP. IdP groups map directly to Locke vaults for role-based access.

### OAuth 2.0 + OpenID Connect

Full OAuth 2.0 with PKCE and OpenID Connect support, including post-quantum signed ID tokens via Dilithium3. You can register apps for clients directly in Armory.

### On-Prem Active Directory

LDAP passthrough for AD-only environments, no Azure AD Connect or Entra P1 licensing needed (save $6/user/month!). Sync users and groups directly from on-prem AD.

**Strong Single Logout to Instantly Revoke Access**

SCIM disables the account. Nuke Sessions clears the local access already left behind. From Armory, authorized partners can clear website cookies and site storage from a departing or compromised employee's connected browser profiles, reload open tabs, and revoke every Locke session.

## Choose your client's security model

### Zero-Knowledge with Passkeys RECOMMENDED

Keys are sealed to enrolled devices via passkeys, preserving full zero-knowledge with passwordless convenience. If a device is lost, Trusted Circle provides E2E encrypted recovery. No one (including Locke) can access plaintext credentials.

### Key Escrow CONVENIENCE

Symmetric keys sealed to an org escrow keypair backed by KMS, enabling one-click login from any device without device enrollment. The trade-off: Locke holds a recovery path via KMS, so it is not fully zero-knowledge.

## How Locke protects your clients' data

### Post-Quantum Cryptography

X25519Kyber768 hybrid key encapsulation with ChaCha20-Poly1305 AEAD. Ready today for the threats NIST says are coming by 2030.

### Zero-Knowledge Architecture

All encryption happens on the client's device. Locke never sees plaintext credentials. Not even our own engineers can access data.

### Trusted Circle Recovery

E2E encrypted recovery using threshold cryptography, with no recovery files to lose. As a partner, you can join clients' Trusted Circles as a recovery guardian.

### Impersonation Detection

Real-time phishing detection in the browser extension identifies impersonation attempts that blocklists miss. Secure Inboxes prevent phishing emails from arriving in the first place.

**Connor Peters**
Founder & CEO

Book a Meeting

Connect on LinkedIn

connor@lockeidentity.com
(585) 478-2678