Password Vault Comparison Guide

Date: February 20, 2026

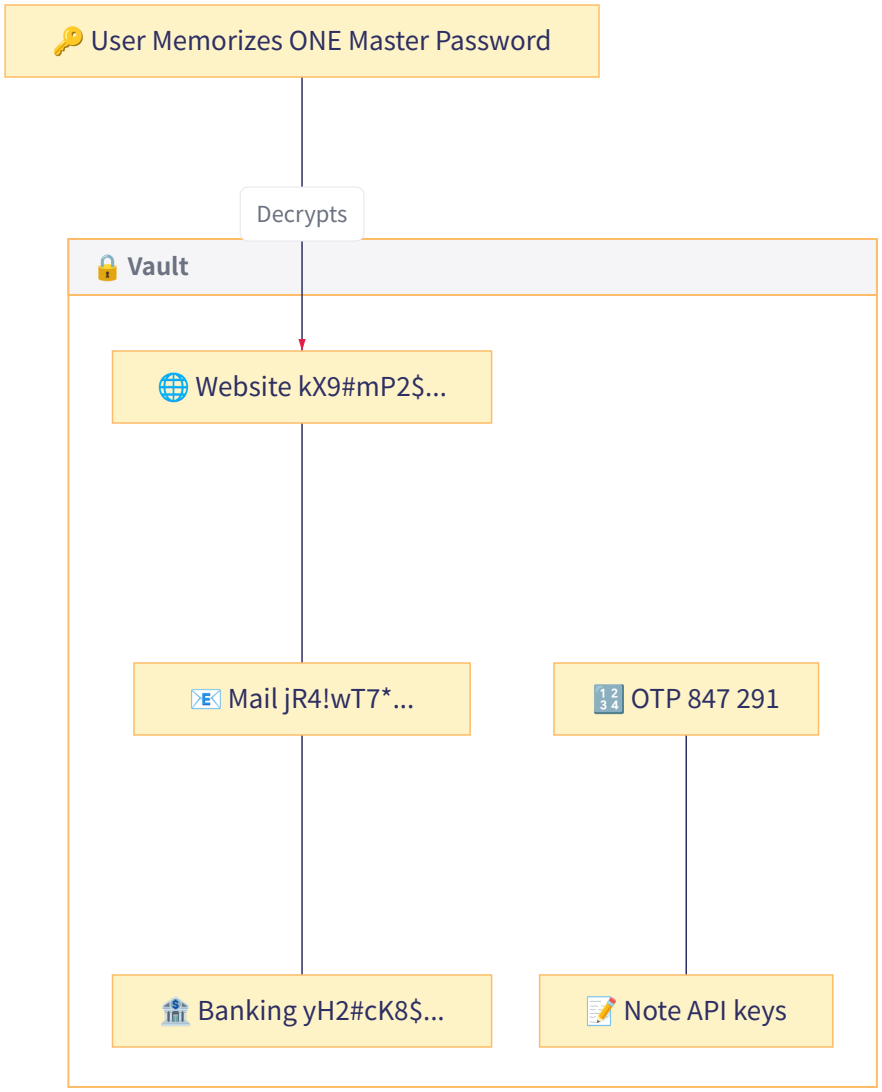
Executive Summary

Password managers are essential tools for protecting your digital identity. However, not all password managers are built the same way. This document compares leading solutions across security architecture, features, and practical considerations to help you choose the right solution for your needs.

Key Recommendation: Choose a solution based on your priorities—maximum security, maximum convenience, or a balance of both. All solutions discussed here are significantly better than not using a password manager.

Your Master Password: The Key to Everything

Your master password is the single most important credential you will ever create. It protects all your other passwords. Choose it carefully and protect it well.



The concept is simple:

- **One password to remember** — your master password
- **Hundreds of passwords you don't** — the vault generates and stores them

Each password inside the vault can be long, random, and unique. You never need to memorize `kX9#mP2$vL5@nQ8&jR4!` — the vault handles it. You only need to remember how to get in.

Choosing a Strong Master Password

The goal is a password that is **long enough to be secure** but **memorable enough that you won't forget it**.

Recommended approach: Use a passphrase

Instead of a complex string like `Tr0ub4dor&3`, use a phrase of random words:

```
correct horse battery staple
```

Or a memorable sentence with personal meaning:

```
My daughter Yuki was born in March 2019!
```

Why this works:

- Length matters more than complexity—a 25-character passphrase is stronger than an 8-character jumble of symbols
- You can actually remember it
- You can type it reliably

> **Consider How You'll Type It**
>
> You'll need to enter your master password on both desktop and mobile devices. Keep in mind:
>
> - **Symbols can be awkward on mobile:** Characters like `|`, `~`, `^`, or `\` often require multiple taps to find on phone keyboards. If you use symbols, stick to common ones easily accessible on mobile (like `!`, `@`, `#`, or `$`).
> - **Spaces work well:** A passphrase with spaces (`correct horse battery staple`) is easy to type on any device.
> - **Biometrics reduce typing:** Most password managers let you unlock with Face ID or fingerprint after the initial setup. Once enabled, you rarely type your master password on mobile—making a longer, more complex password practical.
>
> Test your master password on your phone before committing to it.

Avoid:

- Dictionary words alone (`password`, `sunshine`)
- Personal info easily found online (birthday, pet's name, company name)
- Patterns (`123456`, `qwerty`, `Password1!`)
- Reusing a password from another account

> **Critical: Back Up Your Master Password**
>
> If you forget your master password, you will lose access to all your stored passwords permanently. Most providers cannot recover your data—this is a security feature, not a limitation.
>
> **Write down your master password and store it in a secure physical location** (a safe, a safety deposit box, or with a trusted person). Do not store it digitally. This written backup is your safety net if you ever forget your password or become incapacitated and someone needs access on your behalf.

Inside the Vault: Let the Manager Do the Work

Once inside your password manager, you never need to remember individual passwords again. Let the manager generate long, random passwords for each account:

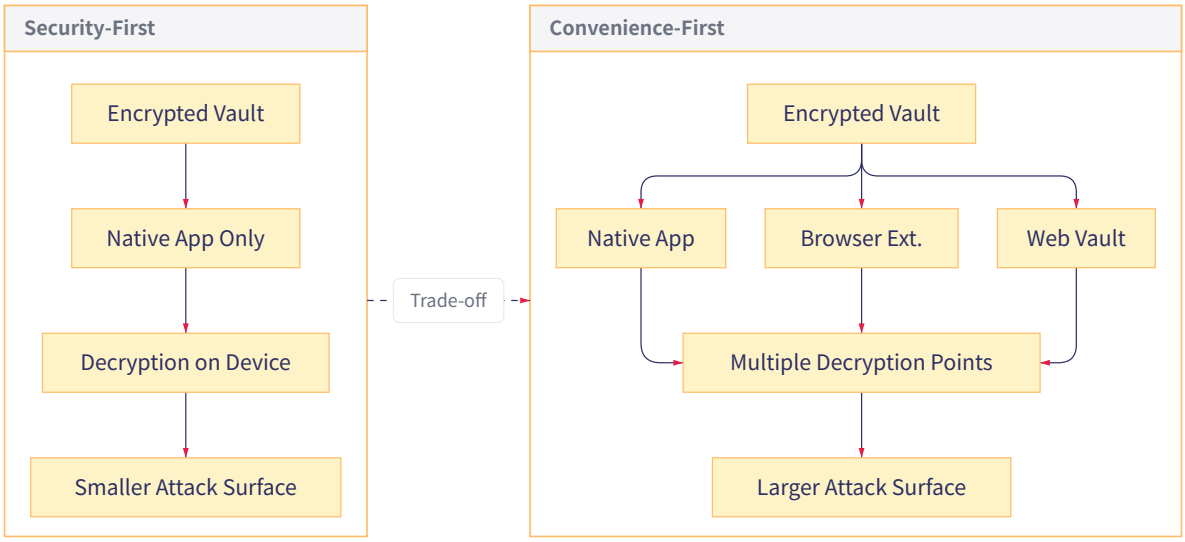
```
kX9#mP2$vL5@nQ8&jR4!wT7*
```

These are impossible to guess and impossible to remember—and that's fine, because you won't need to. The manager handles it.

Understanding Security Architecture

Before comparing individual products, it's important to understand the two fundamental approaches to password manager design.

Security-First vs. Convenience-First Design



Security-First Design:

- Decryption occurs only within the dedicated application
- No browser extensions or web interfaces that could be compromised
- Slower to add new features (each feature evaluated for security impact)
- Example: Codebook

Convenience-First Design:

- Multiple access points for seamless user experience
- Browser extensions enable one-click autofill
- Web vault allows access from any browser
- Security measures added to protect each access point
- Examples: 1Password, Bitwarden

Neither approach is wrong—they represent different priorities. The right choice depends on your threat model and usability requirements.

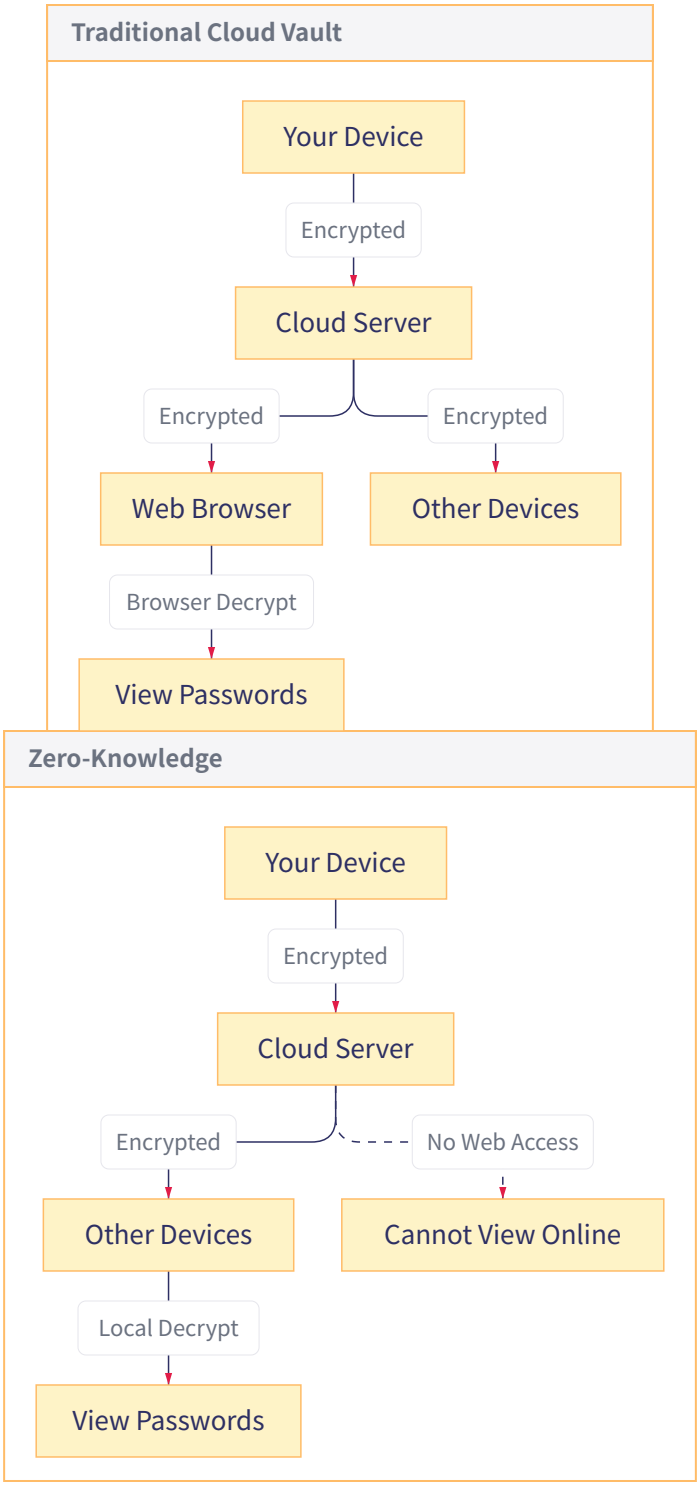
What is "Attack Surface"?

Think of your password vault like a house. The more doors and windows you add, the more entry points a burglar could potentially use. Each entry point is part of the "attack surface."

A security-first password manager is like a house with one heavily reinforced door. A convenience-first manager is like a house with multiple doors (front, back, garage, side)—more convenient for you, but each door needs its own locks and security measures.

Both can be secure, but the single-door approach has fewer things that could go wrong.

How Cloud Sync Differs by Solution



Traditional Cloud Vault (1Password, Bitwarden):

- Access your passwords from any web browser
- Convenient for accessing passwords on shared or temporary computers
- Decryption happens in the browser via JavaScript
- Requires trusting that the provider's servers won't serve malicious code

True Zero-Knowledge Sync (Codebook Cloud):

- Cloud is used **only** to move encrypted data between your devices
- No web interface—passwords can only be viewed in the native app
- Your data is encrypted with a **Sync Key** before it ever reaches their servers
- **Zetetic does not have your Sync Key**—they literally cannot decrypt your data
- Even if compelled by law enforcement or compromised by hackers, the provider cannot access your passwords

What is "Zero Knowledge"?

"Zero knowledge" means the service provider knows nothing about the contents of your data. They store your encrypted vault but cannot read it.

However, not all "zero knowledge" claims are equal:

Type	How it works	Provider Can Access?
Web Vault	Your password unlocks data in your browser. Provider's servers send you the decryption code.	Theoretically yes—they could send malicious code that captures your password
Sync-Only (Codebook)	A separate Sync Key encrypts data before upload. This key never leaves your devices.	No—they don't have the key and there's no web interface to attack

With Codebook Cloud, your Sync Key is generated on your device and stays there. Zetetic's servers only ever see encrypted blobs they cannot decrypt. This is architecturally different from services that offer web access.

Why Are Web Vaults Riskier?

When you log into a web vault (like 1Password.com or vault.bitwarden.com), your browser downloads JavaScript code from the provider's server, and that code decrypts your passwords.

The risk: You're trusting that the provider will always send you legitimate code. If their servers were compromised, or if a rogue employee made changes, or if law enforcement compelled them to modify the code for a specific user, the JavaScript could theoretically capture your master password. **This is not hypothetical paranoia**—it's why security researchers have long debated web-based password access. For most users, the risk is low. For high-security users (executives, journalists, activists), this architectural difference matters.

Password managers without web vaults eliminate this entire category of risk.

Solution Comparison

Overview Matrix

Feature	Codebook	1Password	Bitwarden	Apple Passwords
Architecture	Security-first	Convenience-first	Convenience-first	Platform-integrated
TOTP Codes	✓ Built-in	✓ Built-in	✓ Built-in	✓ Built-in
Browser Extension	✗ (by design)	✓	✓	⚠ Chrome/Edge only, unreliable on Windows
Web Vault	✗ (by design)	✓	✓	✗
Platforms	Win, Mac, iOS, Android	All + Linux	All + Linux	Apple only (Windows buggy)
Family/Team Sharing	✓ (new in 2026)	✓	✓	Apple users only
Open Source	SQLCipher (encryption)	✗	✓ Full	✗
Self-Host Option	Local-only available	✗	✓	✗
Breach Monitoring	✓ HaveIBeenPwned	✓ Watchtower	✓ Reports	✓ Basic
Price (Individual)	$60/year	$36/year	Free–$10/year	Free

What is TOTP?

TOTP (Time-based One-Time Password) is the technology behind those 6-digit codes that change every 30 seconds. When a website offers "authenticator app" as a two-factor option, it's using TOTP.

Modern password managers can store and generate these codes alongside your passwords, so you don't need a separate authenticator app for most accounts. You'll still see the term "2FA" (two-factor authentication) or "MFA" (multi-factor authentication) used interchangeably with TOTP in many contexts.

Business Pricing Comparison

For organizations, all three major solutions offer business-specific plans with administrative controls, centralized billing, and onboarding support. **If you are using these tools for business purposes, the business plans are required** and provide features essential for organizational management.

Team Size	Codebook Business	1Password	Bitwarden Teams	Bitwarden Enterprise
5 users	$225/year*	$240/year (Starter)	$240/year	$360/year
10 users	$450/year*	$240/year (Starter)	$480/year	$720/year
50 users	$2250/year*	$4,794/year	$2,400/year	$3,600/year
Per-user rate	From $5/user/mo	$7.99/user/mo	$4/user/mo	$6/user/mo

- Codebook Business starts at $5/user/month. Prices shown are 25% off, **with eSolia affiliate code**. Large teams may be eligible for a bigger discount.

Key Business Plan Features:

Feature	Codebook Business	1Password Business	Bitwarden Teams	Bitwarden Enterprise
Centralized billing	✓	✓	✓	✓
User management dashboard	✓	✓	✓	✓
Sharing permissions	✓	✓	✓	✓
SSO integration	✗	✓	✗	✓
Directory sync (SCIM)	✗	✓	✗	✓
Self-hosting option	✗	✗	✓	✓
Free Families for users	✗	✓	✗	✓

Business Plan Links:

- **Codebook Business:**https://www.zetetic.net/codebook/business/
- **1Password Teams/Business:**https://1password.com/pricing/password-manager
- **Bitwarden Business:**https://bitwarden.com/pricing/business/

Note: Volume discounts are typically available from all vendors for larger deployments (generally 100+ users).

Detailed Profiles

Codebook (by Zetetic)

Philosophy: Maximum security through minimal attack surface.

Strengths:

- 25+ year track record with no breaches
- SQLCipher encryption (used by NASA, Samsung, Fortune 500 companies)
- No browser extension or web vault means no browser-based attack vectors
- **True zero-knowledge cloud sync:** Codebook Cloud encrypts your data with a Sync Key that is generated on your device and never uploaded. Zetetic cannot see your passwords, cannot be compelled to hand them over, and cannot be hacked in a way that exposes your data.
- Even your master password isn't used for cloud encryption—a separate, fully random Sync Key protects against password-cracking attacks
- Responsive, personal customer support from a company focused solely on security

> ⓘ **Why the Separate Sync Key Matters**
>
> Most people choose memorable (and thus somewhat guessable) master passwords. Advanced attackers can try billions of password guesses against encrypted data.
>
> Codebook Cloud doesn't encrypt your sync data with your master password. Instead, it uses a completely random Sync Key—a long string of random characters that's impossible to guess. This key lives only on your devices. Even if someone stole the encrypted data from Zetetic's servers, cracking it would be mathematically infeasible.

Considerations:

- Autofill via Secret Agent requires slightly more interaction than browser extensions
- No Linux support
- Smaller company (though stable for 25+ years)
- Less brand recognition than larger competitors

Best for: Users who prioritize security architecture over seamless convenience; organizations with strict security requirements; privacy-conscious individuals; anyone who wants their provider to have zero ability to access their data.

1Password

Philosophy: Best-in-class user experience with strong security measures.

Strengths:

- Excellent, polished user interface across all platforms
- Browser extension autofill works reliably
- Secret Key adds extra encryption layer beyond master password
- Travel Mode can hide sensitive vaults when crossing borders
- Strong enterprise management features
- Never experienced a data breach

Considerations:

- No free tier (14-day trial only)
- Web vault means passwords can be decrypted in browser context
- Closed-source (relies on third-party audits for verification)
- Higher price point

Best for: Users who prioritize seamless experience; families who need easy sharing; enterprises requiring management features.

Bitwarden

Philosophy: Transparent, open-source security accessible to everyone.

Strengths:

- Fully open-source and regularly audited
- Generous free tier with unlimited passwords and devices
- Self-hosting option for complete control
- Browser extension and web vault for convenience
- Strong organizational features at reasonable prices
- Active development with frequent updates

Considerations:

- User interface less polished than 1Password
- Autofill can be inconsistent on some platforms
- Web vault means passwords can be decrypted in browser context (see earlier section on web vault risks)
- VC funding raises questions about future direction (though open-source code would survive any company changes)

Best for: Budget-conscious users; open-source advocates; organizations wanting self-hosted option; technical users comfortable with less polished UI.

> **What Does "Open Source" Mean for Security?**
>
> Open-source software publishes its complete code publicly. Anyone can inspect it for security flaws or hidden backdoors. This transparency means:
>
> - Independent security researchers can (and do) audit the code
> - Backdoors or malicious code would be discovered quickly
> - You don't have to trust the company's claims—you can verify
>
> Bitwarden is fully open-source. Codebook uses SQLCipher, which is open-source encryption, though the application itself is not. 1Password and Apple Passwords are closed-source.

Apple Passwords (iCloud Keychain)

Philosophy: Seamless integration within Apple ecosystem.

Strengths:

- Free and built into Apple devices
- Zero setup required for Apple devices
- Face ID / Touch ID integration is seamless
- Passkey support
- Strong encryption

Considerations:

- Only works reliably within Apple ecosystem
- **Windows support is problematic:** iCloud for Windows exists but has well-documented issues:
  - Passwords app frequently crashes on Windows 11
  - Approval/sync process often fails in a loop (2FA codes accepted but nothing happens)
  - Sync can break after iOS or Windows updates
  - Autofill in Edge/Chrome extensions is inconsistent
  - Requires specific conditions: same network, VPN disabled, Windows Hello enabled
  - Troubleshooting is difficult with limited diagnostic tools
- No Android support whatsoever
- Cannot share passwords with non-Apple users
- Limited control and export options
- Browser extension only available for Chrome and Edge (not Firefox)

Best for: Apple-only organizations with no Windows PCs and no need to share outside Apple ecosystem. Not recommended for mixed Apple/Windows environments due to reliability issues.

Browser-Based Managers (Chrome, Edge, Firefox)

Philosophy: Convenient, integrated with existing workflow.

Strengths:

- Already available, no additional installation
- Free
- Syncs with browser account

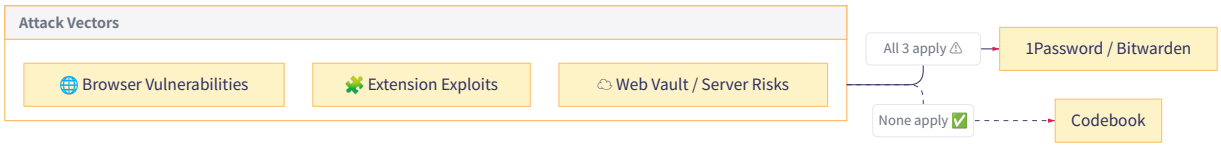
Considerations:

- Single point of failure (browser account compromise = all passwords exposed)
- No true zero-knowledge architecture
- Limited to browser context
- No TOTP support
- Provider (Google, Microsoft) can potentially access data

Best for: Users who will not adopt a dedicated solution; temporary measure while transitioning to a proper password manager.

> ⓘ **Why Browser Password Managers Are the Least Secure Option**
>
> When you save passwords in Chrome, they're tied to your Google account. This means:
>
> 1. **Google can access them:** Unlike dedicated password managers, browser-stored passwords are not truly "zero knowledge." Google can (and does, for sync purposes) process this data.
>
> 2. **One password unlocks everything:** If someone gains access to your Google/Microsoft account (through phishing, password reuse, or a data breach), they get your email AND all your passwords simultaneously.
>
> 3. **No separation of concerns:** A dedicated password manager is a single-purpose security tool. A browser is a complex application that visits untrusted websites, runs unknown JavaScript, and has a massive attack surface.
>
> Browser password managers are better than nothing, but they're the weakest option for anyone taking security seriously.

Security Architecture Comparison



Summary: Codebook's architecture eliminates entire categories of network and browser-based threats by design. Solutions with browser extensions and web vaults have additional vectors that must be defended.

What About Malware on Your Device?

You may wonder: "If malware gets on my computer, can't it steal my passwords?"

The answer is nuanced. A locked vault with a strong master password is extremely difficult to crack—the encryption used by these tools (AES-256, SQLCipher) would take longer than the age of the universe to brute-force.

The real risk from malware is capturing your master password:

- A keylogger could record you typing your master password
- Screen capture software could see your passwords when displayed
- Memory-scraping malware could read passwords while your vault is unlocked

How to protect yourself:

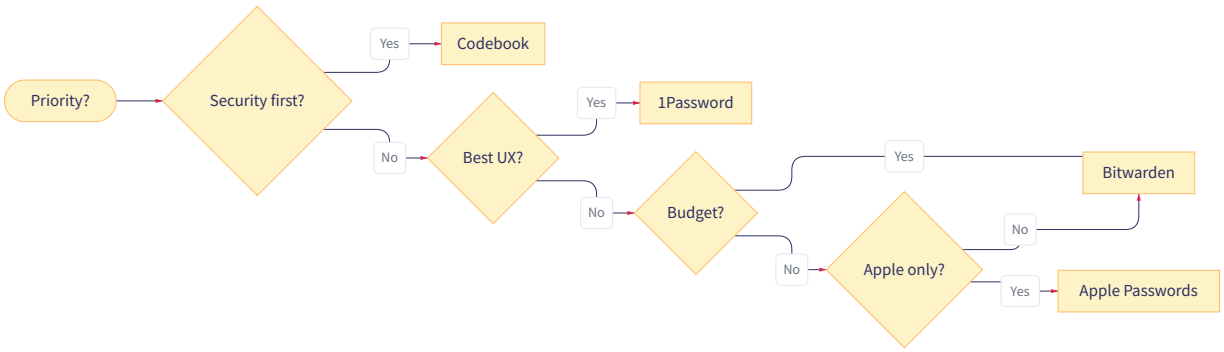
- Use a strong, unique master password (see previous section)
- Keep your operating system and software updated
- Don't install software from untrusted sources
- Lock your vault when not actively using it
- On mobile, use biometrics (Face ID, fingerprint) instead of typing your master password

Bottom line: If your device is compromised by sophisticated malware, no password manager can fully protect you. But this is true of any security tool. The vault encryption itself remains strong.

Note: This does not mean 1Password or Bitwarden are insecure—they implement strong protections for each access point. The diagram shows the architectural difference in network-facing attack surface.

Decision Framework

Choose Based on Your Priorities

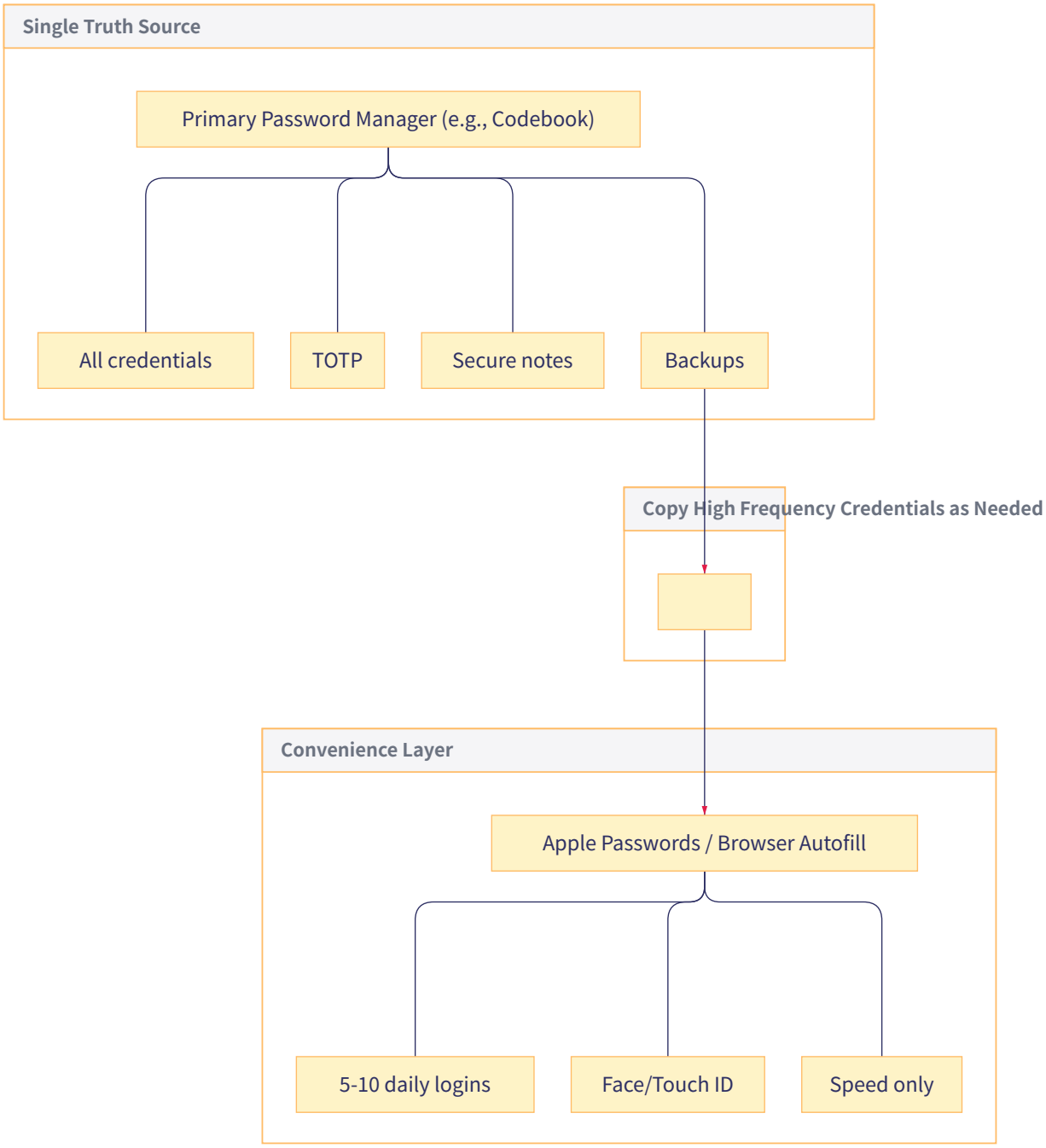


Quick Reference

If you value...	Choose...
Maximum security, minimal attack surface	Codebook
Seamless experience, polished UI	1Password
Open source, budget-friendly, self-host option	Bitwarden
Apple ecosystem integration, zero setup	Apple Passwords

Advanced: The Convenience Layer Pattern

Some users find an effective middle ground by using a security-first vault as their authoritative source while adding a thin "convenience layer" for frequently-accessed sites.



Why This Works

- **Security architecture preserved:** Your authoritative vault maintains maximum security
- **Frictionless daily use:** Face ID autofill for the handful of sites you access constantly
- **Resilience:** If the convenience layer breaks, you don't care—the real data is in your primary vault
- **No version confusion:** Primary vault is always the source of truth

The Discipline Required

1. **Update primary vault first**, then copy to convenience layer if needed
2. **Keep the convenience layer minimal**—only truly high-frequency logins
3. **Never store anything exclusively in the convenience layer**
4. **Periodic cleanup**—remove stale entries from convenience layer

When to Consider This Pattern

- You've chosen a security-first solution but want smoother autofill for a few sites
- You access certain sites dozens of times daily
- You're disciplined enough to maintain the primary-first habit

This pattern addresses the "but I want one-tap autofill" concern without abandoning security-first architecture.

Important Notes

Microsoft Authenticator Update

As of August 2025, Microsoft Authenticator no longer functions as a password manager. Microsoft removed all password storage and autofill features. The app continues to work for:

- Multi-factor authentication (MFA) push notifications
- Time-based one-time passwords (TOTP)
- Passkeys

If you previously stored passwords in Microsoft Authenticator, that data is no longer accessible. Please ensure you have migrated to an alternative solution.

Multi-Factor Authentication Recommendation

Regardless of which password manager you choose, we recommend:

- Using your password manager's built-in TOTP for most accounts
- Using Microsoft Authenticator specifically for Microsoft 365 MFA where required by Conditional Access policies

This separation ensures your password vault and MFA are not dependent on a single application.

Next Steps

1. **Evaluate** your priorities using the decision framework above
2. **Trial** your preferred solution (most offer free trials)
3. **Export** your current passwords from existing sources (browser, etc.)
4. **Import** into your new password manager
5. **Enable** two-factor authentication on critical accounts
6. **Delete** passwords from less secure locations (browser storage, etc.)

> **Don't Forget Your Backup Keys**
>
> Depending on which solution you choose, you may need to securely store:
>
> - **Master Password:** Write it down and store in a safe place (all solutions)
> - **Sync Key:** Codebook Cloud generates a separate key for sync—back this up too
> - **Secret Key:** 1Password provides an Emergency Kit PDF—print and store it
> - **Recovery Codes:** Many services provide one-time recovery codes—save these
>
> Store these physical backups where a trusted family member could find them if needed. A fireproof safe or safety deposit box is ideal.

We are available to assist with migration, setup, and training for any of these solutions.

Contact Us

eSolia Inc.
Shiodome City Center 5F (Workstyling)
1-5-2 Higashi-Shimbashi, Minato-ku
Tokyo 105-7105, Japan

Phone	03-4577-3380
Email	hello@esolia.co.jp
Web	https://esolia.co.jp/en
Hours	Monday-Friday, 9:00-18:00 JST
