WhatIf

FOR ADVISERS, ATTORNEYS & AGENTS

SECURITY BRIEF FOR PROFESSIONALS

Your clients' information is locked *before it leaves their device.*

WhatIf is a private family vault for accounts, policies, documents and "who to call". It uses **zero-knowledge encryption**: each item is encrypted on the client's own phone or computer before upload. **WhatIf's servers store only the encrypted result, and WhatIf staff have no key to open it.**

Encrypted on the device
AES-256-GCM, with a new key for every item. Done in the browser.

WhatIf holds no keys
The server gets ciphertext and public keys. Staff can't read contents.

Shared one person at a time
Each item key is locked to each chosen person's own key.

The owner controls releases
Emailed the moment anyone asks. Can stop it during a waiting period.

The short version

Six facts you can repeat to a client

1. **Encryption happens on the client's device**
Names, account and policy numbers, passwords, notes and documents are encrypted in the browser **before upload**. The server receives only ciphertext, encrypted keys and public keys.

2. **WhatIf cannot read vault contents**
The keys are made and kept on the devices of the client and the people they share with. **No WhatIf staff member, admin tool or database query** can turn the stored data back into readable text.

3. **Lost keys cannot be recovered**
If a client loses every way to unlock (passkeys, passphrase and recovery code), **nobody can open the vault, including WhatIf**. That is why everyone prints a recovery code at signup.

4. **Each person sees only their part**
The client picks who sees each item. People see **only what is shared with them**, and they can't see who else is in the vault.

5. **"Just in case" items stay sealed**
Sealed items need **both** the person's own sign-in **and** a printed release letter. The owner is emailed as soon as anyone asks, and can stop it during a waiting period they choose.

6. **Built on independently audited providers**
Hosting, database, email and payments come from providers that hold **SOC 2 Type II** reports. WhatIf itself is **not** SOC 2 certified (page 5).

How to use this brief

Pages 2–3 are written so you can hand them to an IT reviewer

PAGE 2
The key hierarchy
Every lock, every key, and where each one lives.

PAGE 3
Unlocking & sharing
Unlock methods, approving people, release letters.

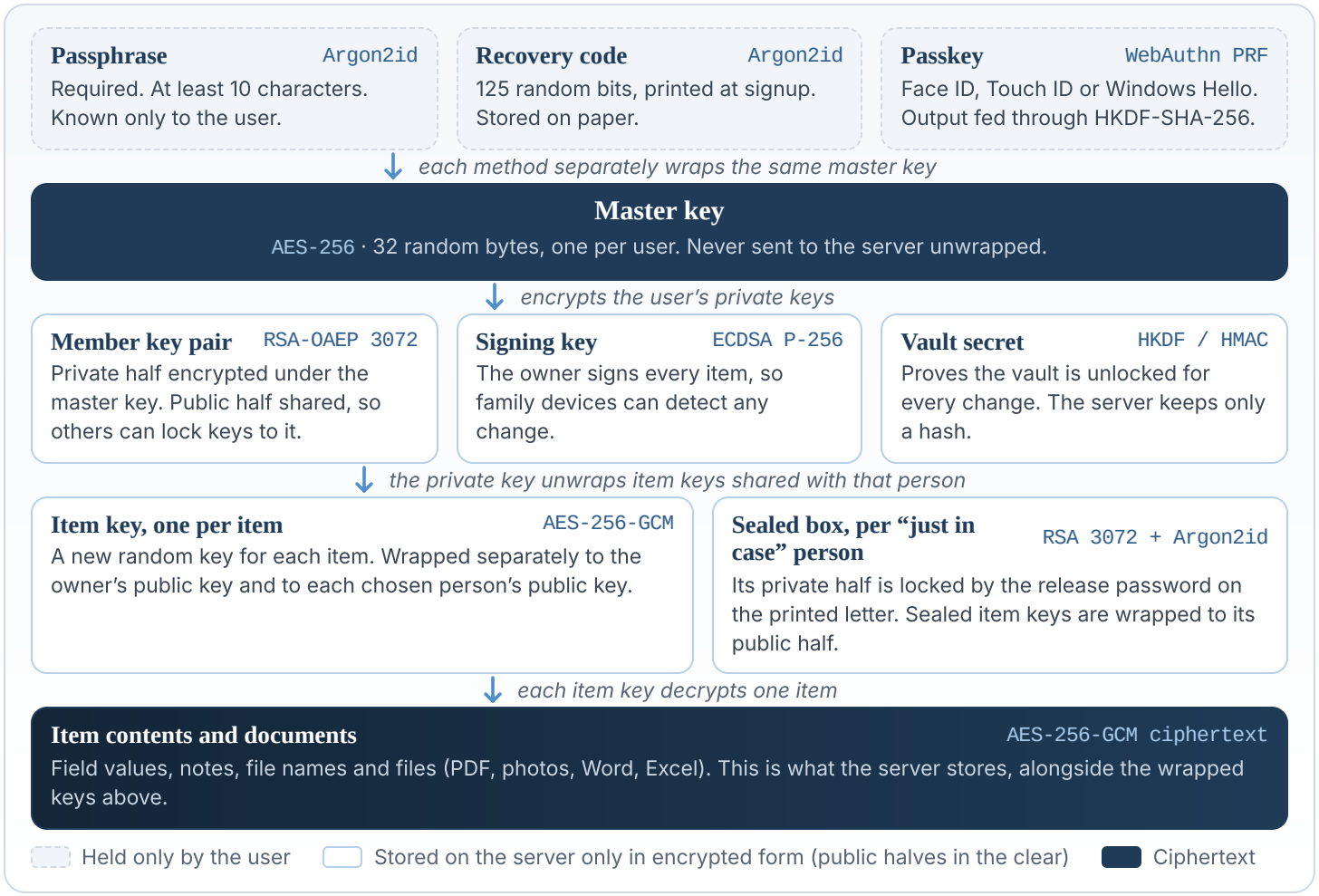
PAGE 4
What WhatIf can see
The readable data, the safeguards, and the limits.

PAGES 5–6
Hosting, FAQ & sources
Providers, audit reports, client questions, links.

Only the client holds the key. WhatIf can't open a vault, so it can't open one for anyone else either.

The key hierarchy: *every lock, and who holds its key*

All of this runs in the browser, using the standard **Web Crypto API**. Keys are created on the user's device. The server receives only encrypted data, keys that are themselves encrypted ("wrapped"), and public keys.



Technical summary *for an IT reviewer*

Taken from the app's source code

PURPOSE	ALGORITHM	DETAIL
Items and documents	`AES-256-GCM`	New key per item, random 96-bit IV. Each ciphertext is bound to its purpose and ID as additional data, so the server can't swap one item's data for another's.
Sharing	`RSA-OAEP 3072, SHA-256`	The item key is wrapped once for each person who may see it.
Passphrase, recovery code, release password	`Argon2id: 64 MiB, 3 passes`	Random 16-byte salt for each. Makes each guess slow and memory-hungry. Release passwords are generated (100 bits), never chosen.
Passkey unlock	`WebAuthn PRF → HKDF-SHA-256`	User verification required. A 32-byte PRF output becomes an AES-256 key. Biometrics never leave the device.
Integrity	`ECDSA P-256, SHA-256`	The signature covers the vault, item ID, category, type and a hash of the ciphertext.
"Remember this device"	`Non-extractable keys`	Optional. Keys the browser can use but can't export. Expire after 30 days; cleared at sign-out.

In plain English: a lock inside a lock. The client's unlock method opens one master key; that opens their private key; that opens only the items shared with them.

Email opens the door. *It never opens the vault.*

Signing in uses a **magic link** sent by email. It works once and expires in 15 minutes. That only gets someone to the door. Reading anything also needs one of the unlock methods below, so **an attacker with only the client's inbox still can't read the vault**.

Three ways to unlock

Each one separately protects the same master key

REQUIRED
Passphrase

Everyone must set one, as a backup to Face ID. Protected with Argon2id, so guessing is slow and costly.

`Argon2id` `10+ characters`

PRINTED AT SIGNUP
Recovery code

A random 25-character code the client prints and keeps safe. It opens the vault if devices and passphrase are lost.

`125 bits` `Argon2id`

OPTIONAL, EVERYDAY
Passkey

Face ID, Touch ID or Windows Hello. The device checks the face or fingerprint; **it never leaves the device**.

`WebAuthn PRF` `HKDF`

⚠ **Lost keys stay lost.** WhatIf has no copy of any key and no "reset" button. If a client loses every passkey, the passphrase **and** the recovery code, nobody can open the vault, including WhatIf. Advise clients to store the recovery code with their important papers.

Sharing, one person at a time

- For each item the owner picks **just me, everyone, or specific people**. The device wraps that item's key to each chosen person's public key.
- **The owner approves every person's key** before anything is shared with them. The app warns if a person's key changes.
- Each key has a **safety code**, a short fingerprint the owner and the person can compare out loud. This stops anyone, including the server, from swapping in a different key.
- The owner's list of approved keys is sealed with a key the server never sees, so the server can't quietly add one.
- People **can't see who else is in the vault**, items not shared with them, or totals that include others' items.
- Every change to a vault needs proof it is unlocked, not just a signed-in email.

Release waiting periods

- The owner chooses **no wait, or 1, 3, 7 or 14 days** for each "just in case" person.
- **The owner is emailed as soon as someone asks**, before anything starts. If that email can't be sent, nothing starts.
- The owner can tap **Stop** at any time during the waiting period. With no waiting period, items can open straight away.
- WhatIf emails only the owner. It doesn't check whether anyone has died, and it can't tell who is holding a letter.
- **Silent mode:** a person can be added without being told. WhatIf never contacts them; sealed items still need the letter.

Release letters: *"just in case" access*

Terms of Service, section 5.3

1 Seal & print
WhatIf generates a **100-bit release password**. The client prints it as a letter. WhatIf keeps no copy.

→

2 Leave it safely
With an attorney, with the will, or with a trusted friend. Treat it like a house key.

→

3 Ask, then wait
The person signs in and asks. **The owner is emailed** and can stop it during the wait.

→

4 Open with both
Opening needs **their own sign-in and the letter**. A new letter can be issued any time; the old one stops working.

✉ **A good fit for estate files.** A client can leave the release letter with their attorney, next to the will.

Just enough to run the service, *and nothing inside the items*

A few things must stay readable so WhatIf can send sign-in links, reminders and release alerts. The full list, and how long each is kept, is in the Privacy Policy at **whatif.easynow.life/privacy**.

What WhatIf can see

- **Email addresses** of the owner and the people they add.
- The vault's name, and the **names and relationships** of people added, plus their access settings.
- Each item's **category and type** (e.g. "Insurance · Life"), status, **dates** and expiry date.
- Who each item is shared with; counts and sizes of items and documents.
- When a release was asked for, opened or stopped.
- **Sign-in logs**: email, IP address and browser, kept 90 days.
- Billing status (not card numbers).

Tip: keep sensitive details out of names and relationships; put them inside items.

What WhatIf can't see

- Anything typed into an item: **account names, account and policy numbers**, routing numbers, passwords, 2FA keys, notes, "how to claim" steps.
- **Documents and their file names**, and the video message link.
- The client's **passphrase, recovery code and release passwords**.
- **Faces or fingerprints**. Passkey checks stay on the device.
- **Card numbers**. They go only to Stripe.

WhatIf can't hand readable contents to anyone, including law enforcement, family members or an estate, because it doesn't have the keys.

Other safeguards

Confirmed in the code and headers

No card data
Payments run on Stripe's own pages. Card numbers never reach WhatIf.

No readable bank numbers
Account numbers in items are encrypted. Partner payout fields reject anything that looks like a bank or routing number.

Discreet, untracked email
Emails never name an item or another person. No tracking pixels or per-person tracking links.

Strict Content Security Policy
Only the app's own scripts run. No framing, HTTPS-only (HSTS), no referrer, no analytics.

Families kept apart twice
By the app and by database row-level security. The server refuses to run if that could be bypassed.

Owner-only export
Only the owner can download everything. It is decrypted in the browser, never on WhatIf's servers.

If the database were stolen, the thief would get the readable items listed above and the vault contents as ciphertext, with no keys to open them.

The honest limit. The app is code WhatIf sends to the browser. Someone who took over its hosting could try to alter it. Those accounts use two-step sign-in.

Browser security headers *for an IT reviewer*

Sent on every app page (netlify.toml)

HEADER	SETTING	WHAT IT DOES
Content-Security-Policy	`script-src 'self'`	In the app, only WhatIf's own scripts run. No plug-ins; no other site can frame WhatIf.
Strict-Transport-Security	`max-age 2 years; preload`	Browsers connect only over HTTPS, including subdomains.
Referrer-Policy	`no-referrer`	Links out of WhatIf don't reveal which page they came from.
Permissions-Policy	`camera, mic, location off`	Turns off device features WhatIf doesn't need; allows passkeys only on WhatIf itself.

No ads, no app tracking, no AI training. WhatIf doesn't sell personal information or use it for advertising.

Where WhatIf runs, *and what each provider can hold*

WhatIf runs on infrastructure from providers that hold **SOC 2 Type II** reports. Servers and main providers are in the United States. Every provider below receives vault contents **only as ciphertext**.

PROVIDER	ROLE FOR WHATIF	WHAT IT CAN HOLD	INDEPENDENT REPORTS	RUNS ON
Netlify	Website hosting, server functions, Netlify Database	Everything WhatIf stores (vault contents only encrypted), plus request logs	SOC 2 Type II ISO 27001	AWS and Google Cloud (Netlify's subprocessor list)
Neon	The Postgres database behind Netlify Database, and its backups	The database (vault contents only encrypted)	SOC 2 Type II ISO 27001 ISO 27701	AWS and Azure; data encrypted at rest (AES-256)
Resend	Sends sign-in links, alerts and reminders	Recipient, subject and email text, which never names an item or person	SOC 2 Type II	Sends through Amazon SES (AWS)
Stripe	Subscriptions and payments	Card and billing details, entered on Stripe's pages; WhatIf never sees them	PCI DSS Level 1 SOC 1 & 2 Type II	Card vault in an isolated AWS environment
gold-api.com	Precious-metal spot prices	No personal information. The server requests one fixed price list for everyone.	None claimed	—

Other providers (the support inbox, currency and crypto price feeds, partner payouts) are listed in the Privacy Policy, section 7. None of them receives vault contents.

What the reports mean

- A **SOC 2 Type II** report is an independent auditor's review of how a company's security controls worked over a period of time.
- **PCI DSS Service Provider Level 1** is the highest level of the card industry's security standard. Stripe holds it, which is why WhatIf never handles card numbers.
- These reports cover the **providers**, not WhatIf's own code or company.

What WhatIf *has not* done yet

- **WhatIf itself is not SOC 2 certified** and has no SOC 2 report.
- No outside audit or penetration test has been done.
- Testing so far is internal: adversarial reviews of each feature, and 150+ automated tests. One browser test checks that item contents never leave the device unencrypted.

Why the encryption matters more than the audits. The keys never reach WhatIf or its providers. So even a full breach of Netlify, Neon or Resend would expose vault contents only as ciphertext, along with the readable service data listed on page 4.

Where the servers sit

From Netlify's and Neon's own documentation

- Netlify deploys server functions for new sites to **US East (Ohio)** by default, and creates a Netlify Database in the region that matches the functions.
- Traffic between the browser and WhatIf is encrypted (HTTPS, with HSTS). Neon encrypts stored data at rest with AES-256, underneath WhatIf's own encryption.

Audited infrastructure, zero-knowledge design. The providers are audited; the encryption means they never hold the keys.

Questions your clients *may ask you*

Short answers you can give, each based on the Terms, the Privacy Policy and the app itself.

Can WhatIf staff read my vault?

No. Contents are encrypted on your device and WhatIf has no key. Staff can see the service data listed on page 4, such as email addresses and item categories.

Can my adviser see my vault?

Not unless you add them as a person and share items with them. A partner who referred you sees only a masked email, plan status and dates, never anything in the vault.

What if WhatIf gets a court order?

It can only hand over vault contents in encrypted form, plus the readable service data. Where the law allows, WhatIf tells you first.

What if I forget my passphrase?

Use a passkey (Face ID or fingerprint) if you set one up, or your printed recovery code. If every unlock method is lost, nobody can open the vault, including WhatIf.

How will my family get in if I die?

Through release letters you print and leave with someone you trust. WhatIf doesn't check for a death; it emails you when someone asks, so you can stop an early request.

What if I stop paying, or want to leave?

The family keeps read-only access for 6 months; nothing is deleted automatically. The owner can download everything any time, decrypted in the browser.

Where is my data?

WhatIf's servers and main providers are in the United States. Vault contents are stored there only in encrypted form.

Does WhatIf sell or track my data?

No. No ads, analytics or trackers in the app or emails, and no AI training. Only the public website counts visits, if you allow it.

Sources

Provider trust and compliance pages, checked October 31, 2026

Netlify Trust Center (SOC 2, ISO, subprocessors): `https://www.netlify.com/trust-center/`

Neon security and compliance: `https://neon.com/security`

Netlify security: `https://www.netlify.com/security`

Netlify Database is powered by Neon: `https://neon.com/blog/netlify-db-powered-by-neon`

Resend SOC 2: `https://resend.com/security/soc-2`

Resend DNS setup (Amazon SES): `https://resend.com/docs/knowledge-base/route53`

Netlify function regions (US East, Ohio default): `https://docs.netlify.com/functions/optional-configuration`

Stripe security (PCI, SOC): `https://docs.stripe.com/security`

WhatIf Privacy Policy, section 7: `https://whatif.easynow.life/privacy`

Please note. This brief describes how WhatIf is designed and built as of October 31, 2026. It is not a guarantee, a warranty or legal advice. WhatIf stores and shares information; it is not legal, tax or financial advice and does not replace a will, trust or power of attorney. No system is perfectly secure. The Terms of Service (whatif.easynow.life/terms) and Privacy Policy (whatif.easynow.life/privacy) govern the service. Provider certifications are the providers' own and can change; check the sources above.