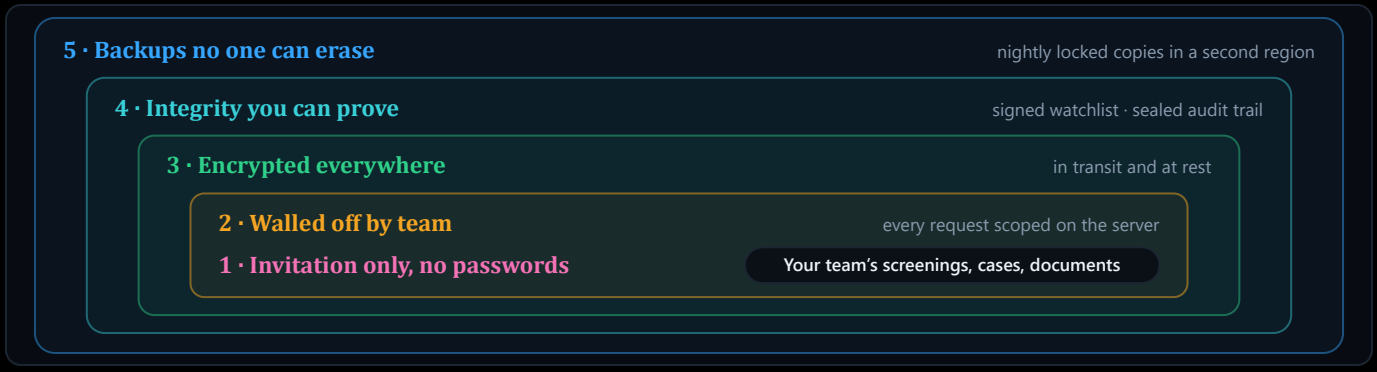
01 · Defense in layers

Your research security data, protected at every layer.

The people you screen, the cases you open and the documents behind them are some of the most sensitive records your institution holds. SYSWERX protects them in layers: who can get in, what each team can reach, how the data is encrypted, how every record proves it hasn't changed, and backups that no one can erase.



1 · Who can get in

Sign in
No passwords to steal

Accounts are issued by SYSWERX to the people your office names. Each sign-in is a link that works once, sent to that person's work email. There is no public sign-up.

Sessions
One session, signed out when idle

One active session per person, and an automatic sign-out after 30 minutes without activity, even if the tab is reloaded or put to sleep.

Roles
Need to know, built in

Lead, Analyst and read only Viewer. A restricted case is seen only by the people named on it, its owner and the team's Leads. Travelers and researchers see only their own form.

2 · Walled off by team · 3 · Encrypted everywhere

Isolation
Other teams never see your work

Browsers have no direct access to the database. Every read and write goes through the SYSWERX server and is scoped to your team. The scoring engine and the watchlist run only on the server and are never sent to a browser.

Encryption
In transit and at rest

TLS with HTTPS enforced on every connection, a strict content security policy on every page, and AES-256 encryption at rest for the database, your stored documents and every backup copy.

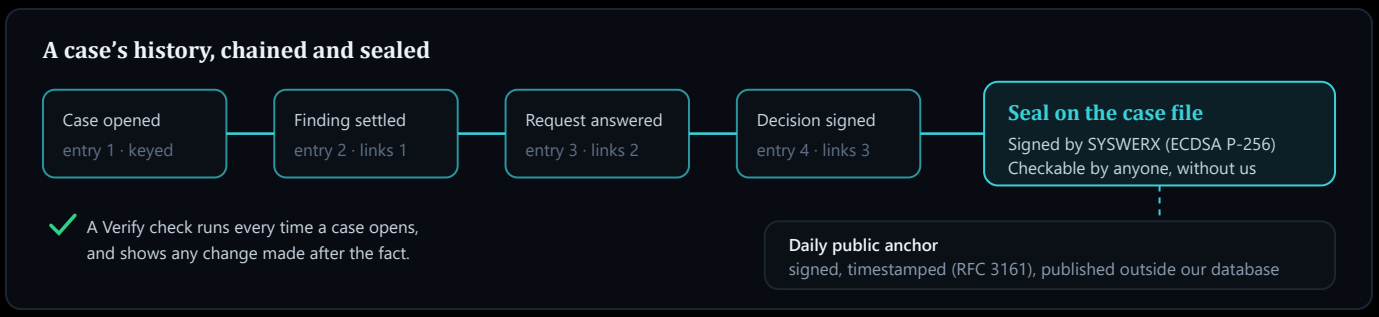
Where it runs

Application	Render, Oregon, United States, behind Cloudflare
Database and documents	Supabase on AWS, U.S. West (Oregon)
Backup copies	A separate, private AWS account, U.S. East (Ohio): a different region from the live data
Email and billing	Resend sends sign-in links and notices, never case content. Stripe handles billing, never researcher data.

02 · Integrity you can prove

Every record can prove it hasn't been changed.

A research security decision has to stand up to an auditor, a sponsor or counsel years later. SYSWERX doesn't ask you to take its word for that: the evidence is signed, the case history is sealed, and anyone can check the seal without us.



What makes it trustworthy

Signed watchlist
No false all clear
The watchlist is human verified, cited and digitally signed. If its signature doesn't verify, screening stops instead of reporting that nothing was found.

Audit trail
Tamper evident
Each case's history is a keyed chain: every entry is bound to the one before it, so an edit after the fact breaks the chain and shows up.

Repeatable
Every input kept
Each screening keeps the inputs it used, so it can be run again later and compared line by line. The scoring is fixed rules with citations, not a machine learning model.

Your documents, your storage

- **Kept on your own storage.** On request, program and researcher documents stay on your SharePoint, OneDrive, Box, Google Drive or network drive. We keep only the record.
- **We never get the file.** Its name, size and a fingerprint are worked out in your own browser. Our servers never reach the place it lives.
- **No credentials with us.** Your own sync apps sign in with their own second sign-in step. SYSWERX never sees a password or a byte of the file.
- **Stored copies, if you prefer.** Private, per team storage, opened only through the server, each upload, download and deletion logged.

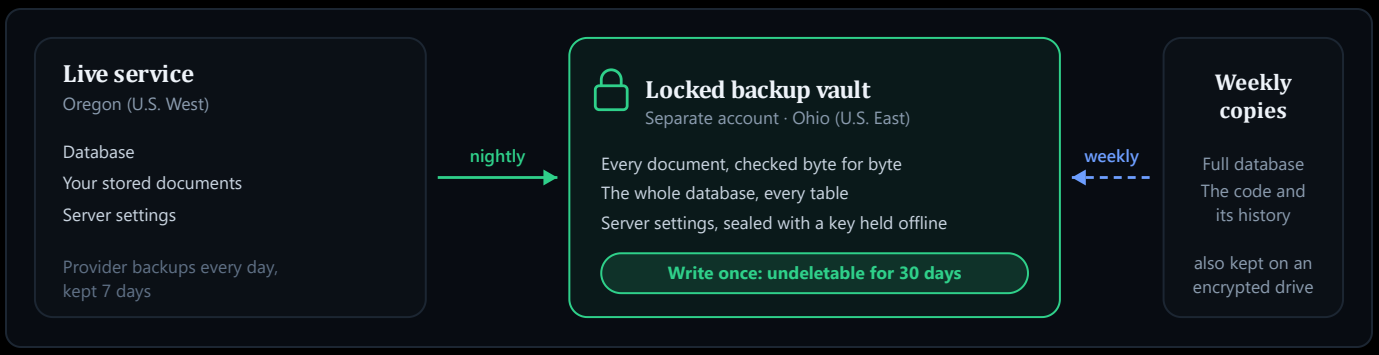
Fair by design

- **Ties, not people.** Nationality, ethnicity, national origin and name are never scoring inputs.
- **Never trained on your data.** No model makes or influences a score, and team data is never used to train one.

03 · Backups no one can erase

If the worst happens, your records come back.

Ransomware and stolen passwords target backups first. SYSWERX keeps several independent copies, and the most important ones are locked so that no one can delete or change them for 30 days. Not an attacker with a stolen key, and not SYSWERX.



How the backups are protected

Write once lock

Undeletable, even by us

Every backup copy is locked in compliance mode for 30 days. Earlier versions are kept for 90 days, so a file encrypted or changed by an attacker can be rolled back.

Least privilege

Keys that can add, not erase

The keys that write backups reach only the backup vault. They can add copies but can't change the lock or remove a locked copy.

Checked and watched

Verified every night

Each document copy is checked against its fingerprint, and every database file carries one. If a night's copy fails, or the last good copy is over 36 hours old, we're alerted by email.

The people and accounts that run SYSWERX

- **Two factor sign-in on every admin account.** Hosting, database, code, DNS, email and cloud accounts all require a passkey or an authenticator.
- **Secrets sealed, not stored.** Server settings are backed up only in encrypted form; the key that opens them is kept offline.
- **Protected code history.** The released code can't be overwritten by force or deleted, and a full copy of its history is backed up weekly.
- **Your data back, on request.** At the end of an agreement we return your data in a common format, then delete it.

SYSWERX does not hold a SOC 2 report or a FedRAMP authorization at this time. We answer institutional security questionnaires in writing, and the full detail is on our Trust page: syswerxintel.com/trust.html.

Two outside lookups, neither carrying researcher data: the tool pages load their typefaces from an outside font service, and this website looks up the owner of a visitor's network in the public internet address registry without storing the address.

Questions from your security review? Ask us directly.

support@syswerxintel.com · syswerxintel.com