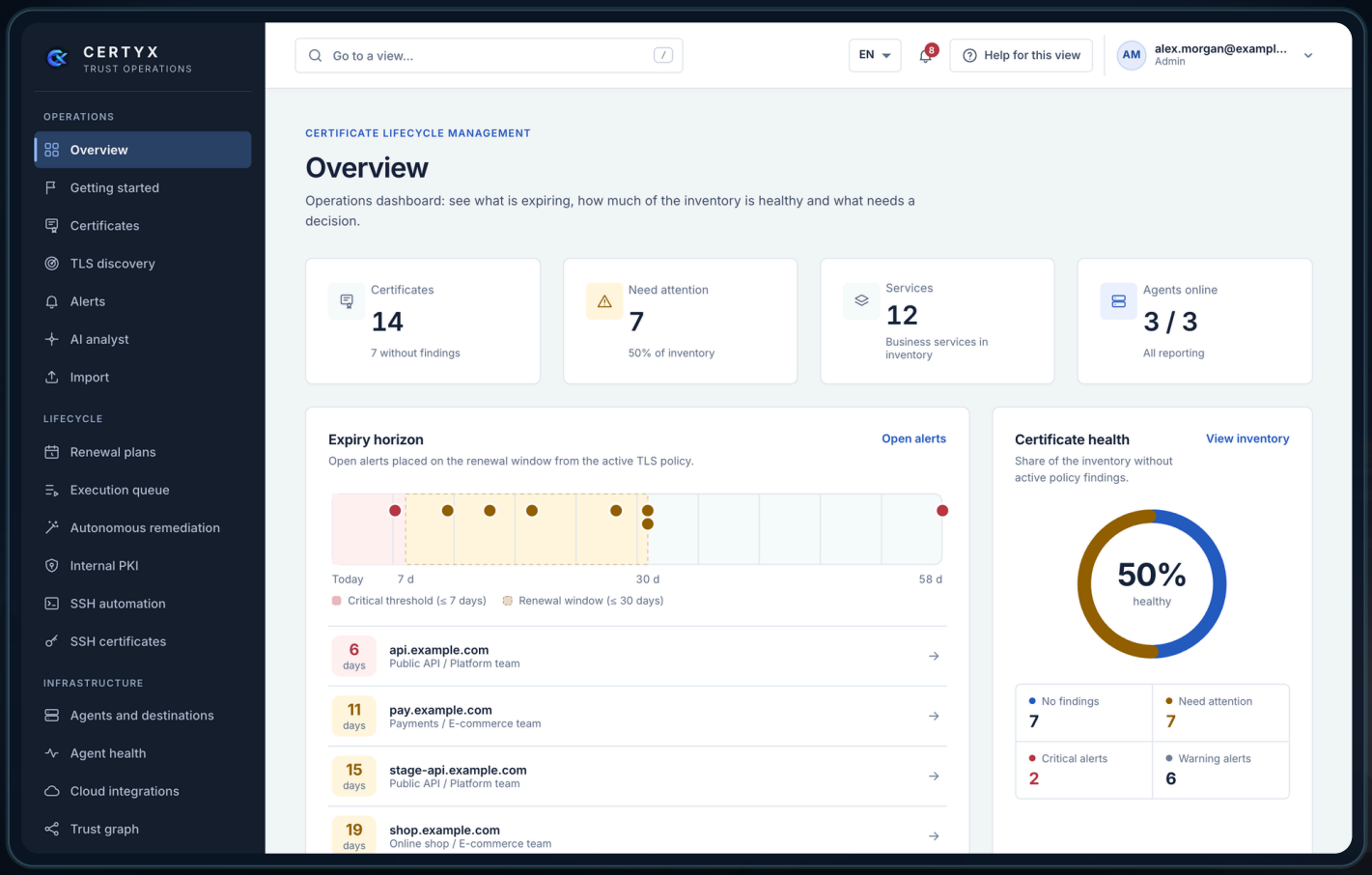
Full control over your certificates. Before shorter cycles become a problem.

CERTYX finds every certificate in your estate, assigns responsibility and renews it through approval, deployment and verification, while private keys stay in your infrastructure.



65,535
TCP ports per approved address

0
managed private keys sent to CERTYX

5
stages from discovery to verification

3
interface languages

CAPABILITIES

One operational view, from discovery to verified renewal.

01 Discover
Scan approved ranges, import PEM files or collect from cloud vaults.

02 Assess
Policy findings and business context show what matters first.

03 Renew
Due renewals run automatically within guardrails, or wait for a second administrator where you require approval.

04 Execute
The agent creates the key locally, obtains the certificate and installs it.

05 Verify
CERTYX checks the certificate actually served and notifies the owners.

TLS discovery
Agents inside your network scan approved IPv4 ranges on any TCP port, resume interrupted scans and report progress. Exclusions and concurrency stay under your control.

Policy assessment
Every certificate is checked against expiry thresholds, minimum key size and weak signatures, with an explanation of each finding.

Automatic renewal
Keys and CSRs are generated on the host that uses the certificate. ACME, DigiCert CertCentral or Vault PKI issue it, with four-eyes approval where you require it; deployment to Nginx, Apache, HAProxy, Tomcat, Kubernetes and other services is verified and can roll back.

SSH certificates
OpenSSH certificate inventory, approved signing profiles and revocation lists distributed by agents.

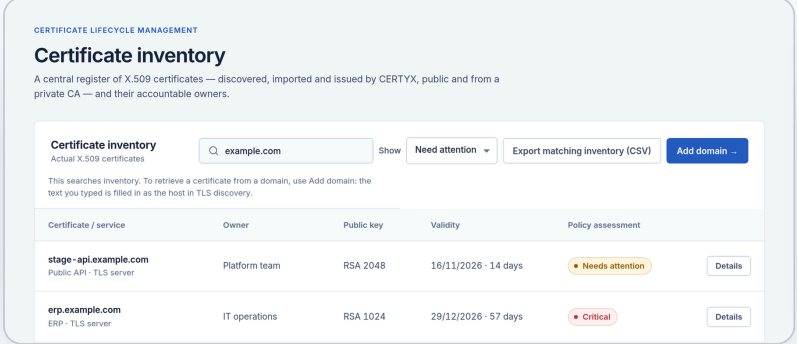
Cloud vaults
Read-only import from Azure Key Vault, AWS ACM and Google Certificate Manager using your own CLI session. No cloud credentials are entered in CERTYX.

Autonomous remediation
Policies react to expiring or weak certificates, replacements and offline agents: dry run, proposals for four-eyes approval, or automatic approval within guardrails. Every decision is logged with its reasons.

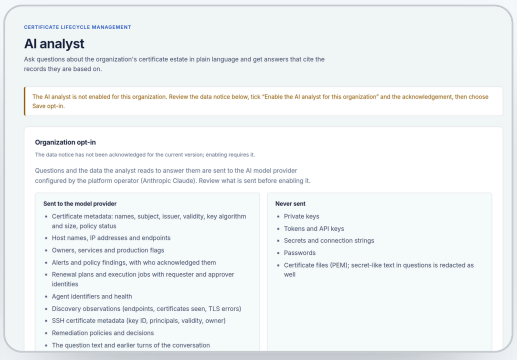
AI Trust Analyst
Ask about your certificate estate in plain language. Answers come from read-only, organization-scoped data and cite the records they use. Opt-in per organization; keys and secrets are never sent.

CERTYX Mobile
Certificate health, alerts and supported approvals on iOS and Android devices that your administrator activated with a one-time code.

SIEM in open standards
Continuous export of the security journal to Splunk, IBM QRadar, ArcSight, Microsoft Sentinel, Elastic, Cribl or OpenTelemetry in CEF, LEEF, RFC 5424, NDJSON, OCSF, ECS or Splunk CIM.



Inventory with owners, services and policy findings



AI Trust Analyst: explicit opt-in and control over data handling

SECURITY AND DATA PROTECTION

Your organization. Your boundaries.

Data security decides which supplier you can trust with your certificates. These are the protections built into CERTYX.

Security by design

The most sensitive material never reaches us: private keys and CA credentials stay with you, every organization's data is kept apart, and every privileged action, including ours, leaves evidence you can see.

Never sent to CERTYX

Private keys of managed certificates · CA credentials · cloud credentials

Isolated organizations

Separate database and database roles for every organization, with forced row-level security, also in the shared platform layer

Your keys stay yours

Private keys of managed certificates are generated and kept in your infrastructure and never sent to CERTYX

Trusted agents

Agents use mutual TLS with enrolled identities and outbound connections only; signed packages and updates are verified

Encrypted secrets

Stored secrets are encrypted, bound to your organization and never returned by the API

Strong sign-in

MFA for administrators, phishing-resistant passkeys, company sign-in with Microsoft Entra ID, Okta, OpenID Connect or SAML 2.0, and SCIM

Networks and sessions

Sign-in limited to your networks if you choose, short sessions and a session list with immediate revocation

Roles and four eyes

Auditor, Operator and Admin roles; configurable automatic or four-eyes approval for renewals, independent verification and rollback

Operator access under your control

Platform operators work with least-privilege roles and step-up confirmation; access to your organization needs your approval or an audited break-glass

Tamper-evident journal

Hash-chained security journal, anchored hourly with signatures in write-once storage, that also shows every platform operator action on your organization

SIEM without blind spots

SIEM export to Splunk, IBM QRadar, Microsoft Sentinel, Elastic, ArcSight, Cribl and OpenTelemetry in CEF, LEEF, RFC 5424, NDJSON, OCSF, ECS and Splunk CIM over TLS, with per-destination event shaping and nothing lost silently

AI under control

AI Trust Analyst only when your administrator enables it: read-only, sources cited, private keys and secrets never sent

EU hosting, encryption

Hosted in the EU (AWS Frankfurt), TLS on every connection, database, disks and secrets on dedicated AWS KMS keys, daily encrypted write-once backups and a cloud audit trail

Privacy and GDPR A named controller, a published data processing page (GDPR Art. 28) and no tracking without consent: optional web analytics only after consent, never on sign-in pages or in the console.

DEPLOYMENT AND LICENSING

Your choice of where CERTYX runs.

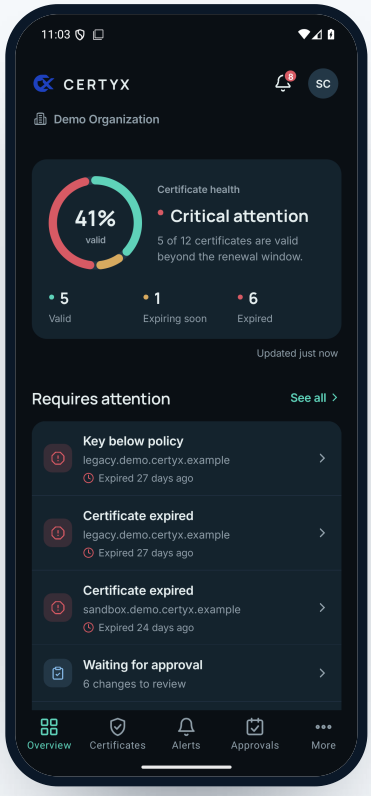
Hosted by CERTYX

Operated by us in the EU (AWS Frankfurt): a separate database for your organization, data and secrets encrypted with dedicated AWS KMS keys, daily encrypted backups in write-once storage, updates applied by us. You install only the agents.

Our own environment

In your data centre or cloud account, with the same isolation and controls. In your own AWS account, the encryption keys (AWS KMS) and the cloud audit trail are yours.

Sales confirms which options fit your plan.



CERTYX Mobile overview

Pay for what you manage, not for what you find.

The licence unit is a managed certificate family. Discovery and imports create unmanaged records that use no capacity.

Discovery and imports	Not counted
Renewals and deployments	Same family, no extra usage
Managed certificate families	**Licensed capacity**

Works with

Issuance
ACME · DigiCert CertCentral · HashiCorp Vault PKI

Cloud vaults
Azure Key Vault · AWS Certificate Manager · Google Certificate Manager

Deployment
Nginx · Apache · HAProxy · Tomcat · Caddy · Traefik · Envoy · Microsoft IIS · Kubernetes · Cribl · OpenSSH

Company sign-in
Microsoft Entra ID · Okta · OpenID Connect · SAML 2.0 · SCIM

SIEM
Splunk · IBM QRadar · ArcSight · Microsoft Sentinel · Elastic · Cribl Stream · Grafana Loki · Amazon Security Lake · OpenTelemetry

Alerts
Microsoft Teams · Slack · PagerDuty · Webhooks

See CERTYX on your own estate.

Book a presentation or request a pilot through the contact form on our website. We answer security questions before you decide.

WEBSITE AND CONTACT FORM
https://certyx.space
SALES
sales@certyx.space
TECHNICAL SUPPORT
support@certyx.space

Controller of personal data: Rafał Będkowski, a natural person operating the Certyx website at https://certyx.space. Contact: support@certyx.space.

Availability depends on your package, configured connectors and approved deployment targets. Certifications, service levels and supported certificate authorities are set out in your customer agreement. Screenshots show the CERTYX console and app with sample data.

© 2026 CERTYX · Edition 1 November 2026 · 8550060f