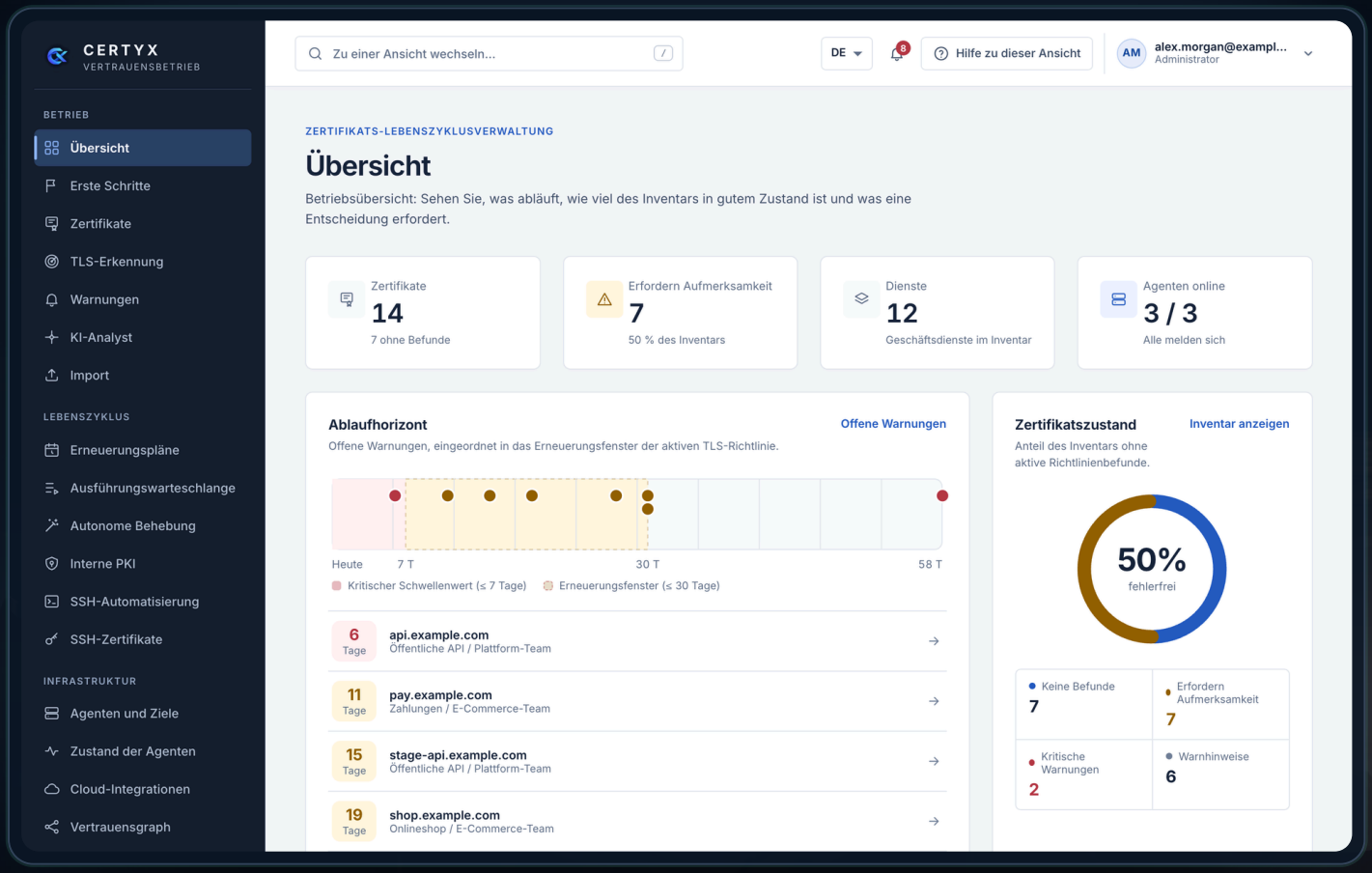
Volle Kontrolle über Ihre Zertifikate. Bevor kürzere Zyklen zum Problem werden.

CERTYX findet jedes Zertifikat in Ihrer Umgebung, ordnet Verantwortung zu und erneuert es über Freigabe, Bereitstellung und Verifizierung, während private Schlüssel in Ihrer Infrastruktur bleiben.



65.535
TCP-Ports je freigegebener Adresse

0
verwaltete private Schlüssel an CERTYX gesendet

5
Stufen von der Erkennung bis zur Verifizierung

3
Sprachen der Oberfläche

FUNKTIONEN

Eine operative Sicht – von der Erkennung bis zur verifizierten Erneuerung.

01 Erkennen
Freigegebene Bereiche scannen, PEM-Dateien importieren oder aus Cloud-Tresoren einlesen.

02 Bewerten
Richtlinienbefunde und Geschäftskontext zeigen, was zuerst zählt.

03 Erneuern
Fällige Erneuerungen laufen automatisch innerhalb von Leitplanken oder warten auf einen zweiten Administrator, wo Sie eine Freigabe verlangen.

04 Ausführen
Der Agent erzeugt den Schlüssel lokal, bezieht das Zertifikat und installiert es.

05 Verifizieren
CERTYX prüft das tatsächlich ausgelieferte Zertifikat und benachrichtigt die Verantwortlichen.

TLS-Erkennung
Agents in Ihrem Netzwerk scannen freigegebene IPv4-Bereiche auf beliebigen TCP-Ports, setzen unterbrochene Scans fort und melden den Fortschritt. Ausschlüsse und Parallelität bleiben unter Ihrer Kontrolle.

Richtlinienbewertung
Jedes Zertifikat wird auf Ablaufschwellen, Mindestschlüssellänge und schwache Signaturen geprüft – mit einer Erläuterung zu jedem Befund.

Automatische Erneuerung
Schlüssel und CSRs entstehen auf dem Host, der das Zertifikat nutzt. ACME, DigiCert CertCentral oder Vault PKI stellen es aus, mit Vier-Augen-Freigabe, wo Sie sie verlangen; die Bereitstellung auf Nginx, Apache, HAProxy, Tomcat, Kubernetes und weiteren Diensten wird verifiziert und kann zurückgerollt werden.

SSH-Zertifikate
Inventar von OpenSSH-Zertifikaten, genehmigte Signaturprofile und von Agents verteilte Widerrufslisten.

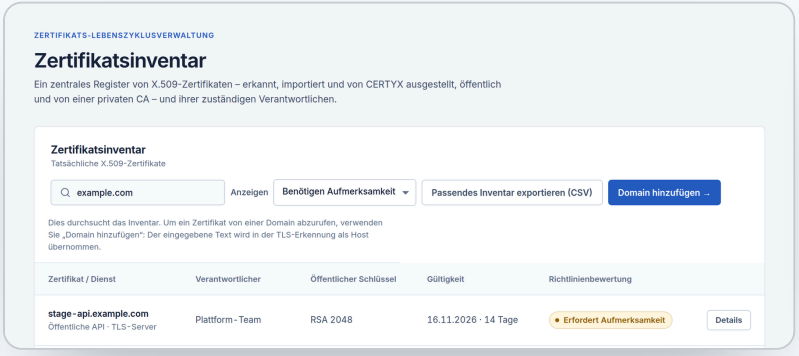
Cloud-Tresore
Schreibgeschützter Import aus Azure Key Vault, AWS ACM und Google Certificate Manager über Ihre eigene CLI-Sitzung. In CERTYX werden keine Cloud-Anmeldedaten eingegeben.

Autonome Behebung
Richtlinien reagieren auf ablaufende oder schwache Zertifikate, Ersetzungen und Agenten offline: Probelauf, Vorschläge zur Vier-Augen-Genehmigung oder automatische Genehmigung innerhalb von Leitplanken. Jede Entscheidung wird mit Gründen protokolliert.

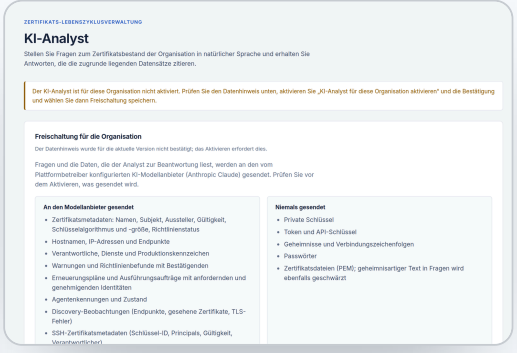
KI-Analyst
Fragen Sie in natürlicher Sprache zu Ihrem Zertifikatsbestand. Antworten stützen sich auf schreibgeschützte Daten Ihrer Organisation und zitieren die verwendeten Datensätze. Freischaltung pro Organisation; Schlüssel und Geheimnisse werden nie gesendet.

CERTYX Mobile
Zertifikatszustand, Warnungen und unterstützte Freigaben auf iOS- und Android-Geräten, die Ihr Administrator mit einem Einmalcode aktiviert hat.

SIEM in offenen Standards
Fortlaufender Export des Sicherheitsjournals an Splunk, IBM QRadar, ArcSight, Microsoft Sentinel, Elastic, Cribl oder OpenTelemetry in CEF, LEEF, RFC 5424, NDJSON, OCSF, ECS oder Splunk CIM.



Inventar mit Verantwortlichen, Diensten und Richtlinienbefunden



AI Trust Analyst: ausdrückliche Zustimmung und Kontrolle der Datenverarbeitung

SICHERHEIT UND DATENSCHUTZ

Ihre Organisation. Ihre Grenzen.

Datensicherheit entscheidet, welchem Anbieter Sie Ihre Zertifikate anvertrauen. Diese Schutzmaßnahmen sind in CERTYX eingebaut.

Security by Design

Das Sensibelste erreicht uns nie: Private Schlüssel und CA-Zugangsdaten bleiben bei Ihnen, die Daten jeder Organisation bleiben getrennt, und jede privilegierte Aktion, auch unsere, hinterlässt Nachweise, die Sie sehen.

Wird nie an CERTYX gesendet

Private Schlüssel verwalteter Zertifikate · CA-Zugangsdaten · Cloud-Zugangsdaten

Getrennte Organisationen

Eigene Datenbank und eigene Datenbankrollen für jede Organisation, mit erzwungener Row-Level-Security auch in der gemeinsamen Plattformschicht

Ihre Schlüssel bleiben Ihre

Private Schlüssel verwalteter Zertifikate werden in Ihrer Infrastruktur erzeugt und aufbewahrt und nie an CERTYX gesendet

Vertrauenswürdige Agenten

Agenten nutzen gegenseitiges TLS mit registrierten Identitäten und nur ausgehende Verbindungen; signierte Pakete und Updates werden geprüft

Verschlüsselte Geheimnisse

Gespeicherte Geheimnisse sind verschlüsselt, an Ihre Organisation gebunden und werden von der API nie zurückgegeben

Starke Anmeldung

MFA für Administratoren, phishing-resistente Passkeys, Firmenanmeldung mit Microsoft Entra ID, Okta, OpenID Connect oder SAML 2.0 sowie SCIM

Netze und Sitzungen

Anmeldung auf Wunsch nur aus Ihren Netzen, kurze Sitzungen und eine Sitzungsliste mit sofortigem Widerruf

Rollen und vier Augen

Rollen Auditor, Operator und Admin; konfigurierbare automatische oder Vier-Augen-Freigabe für Erneuerungen, unabhängige Prüfung und Rollback

Betreiberzugriff unter Ihrer Kontrolle

Plattformbetreiber arbeiten mit minimalen Rollen und Step-up-Bestätigung; Zugriff auf Ihre Organisation braucht Ihre Freigabe oder ein protokolliertes Break-Glass

Manipulationssicheres Journal

Hash-verkettetes Sicherheitsjournal, stündlich signiert in nur einmal beschreibbarem Speicher verankert, das auch jede Aktion von Plattformbetreibern in Ihrer Organisation zeigt

SIEM ohne Lücken

SIEM-Export zu Splunk, IBM QRadar, Microsoft Sentinel, Elastic, ArcSight, Cribl und OpenTelemetry in CEF, LEEF, RFC 5424, NDJSON, OCSF, ECS und Splunk CIM über TLS, mit Ereignisgestaltung je Ziel und ohne stillen Datenverlust

KI unter Kontrolle

AI Trust Analyst nur nach Freischaltung durch Ihren Administrator: nur lesend, mit Quellen, private Schlüssel und Geheimnisse werden nie gesendet

EU-Hosting, Verschlüsselung

Betrieb in der EU (AWS Frankfurt), TLS auf jeder Verbindung, Datenbank, Datenträger und Geheimnisse mit eigenen AWS-KMS-Schlüsseln, tägliche verschlüsselte unveränderliche Sicherungen, Cloud-Audit-Trail

Datenschutz und DSGVO Ein benannter Verantwortlicher, eine veröffentlichte Seite zur Auftragsverarbeitung (Art. 28 DSGVO) und kein Tracking ohne Einwilligung: optionale Webanalyse nur nach Einwilligung, nie auf Anmeldeseiten oder in der Konsole.

BEREITSTELLUNG UND LIZENZIERUNG

Sie wählen, wo CERTYX läuft.

Von CERTYX betrieben

Von uns in der EU betrieben (AWS Frankfurt): eine eigene Datenbank für Ihre Organisation, Daten und Geheimnisse mit eigenen AWS-KMS-Schlüsseln verschlüsselt, tägliche verschlüsselte Sicherungen in nur einmal beschreibbarem Speicher, Updates spielen wir ein. Sie installieren nur die Agenten.

Eigene Umgebung

In Ihrem Rechenzentrum oder Cloud-Konto, mit derselben Isolation und denselben Kontrollen. In Ihrem eigenen AWS-Konto gehören Ihnen die Verschlüsselungsschlüssel (AWS KMS) und der Cloud-Audit-Trail.

Der Vertrieb bestätigt, welche Optionen zu Ihrem Plan passen.



Übersicht in CERTYX Mobile

Zahlen Sie für das, was Sie verwalten – nicht für das, was Sie finden.

Die Lizenzeinheit ist eine verwaltete Zertifikatsfamilie. Erkennung und Importe erzeugen nicht verwaltete Datensätze ohne Kapazitätsverbrauch.

Erkennung und Importe	Nicht gezählt
Erneuerungen und Bereitstellungen	Gleiche Familie, keine zusätzliche Nutzung
Verwaltete Zertifikatsfamilien	**Lizenzierte Kapazität**

Arbeitet mit

Ausstellung
ACME · DigiCert CertCentral · HashiCorp Vault PKI

Cloud-Tresore
Azure Key Vault · AWS Certificate Manager · Google Certificate Manager

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

Firmenanmeldung
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

Alarme
Microsoft Teams · Slack · PagerDuty · Webhooks

Erleben Sie CERTYX mit Ihrer eigenen Umgebung.

Vereinbaren Sie eine Präsentation oder fragen Sie ein Pilotprojekt über das Kontaktformular auf unserer Website an. Sicherheitsfragen beantworten wir, bevor Sie entscheiden.

WEBSITE UND KONTAKTFORMULAR
https://certyx.space

VERTRIEB
sales@certyx.space

TECHNISCHER SUPPORT
support@certyx.space

Verantwortlicher für personenbezogene Daten: Rafał Będkowski, eine natürliche Person, die die Website Certyx (https://certyx.space) betreibt. Kontakt: support@certyx.space.

Die Verfügbarkeit hängt von Ihrem Paket, den konfigurierten Connectoren und den freigegebenen Bereitstellungszielen ab. Zertifizierungen, Service-Level und unterstützte Zertifizierungsstellen regelt Ihr Kundenvertrag. Die Abbildungen zeigen die CERTYX-Konsole und -App mit Beispieldaten.

© 2026 CERTYX · Ausgabe 1. November 2026 · 8550060f