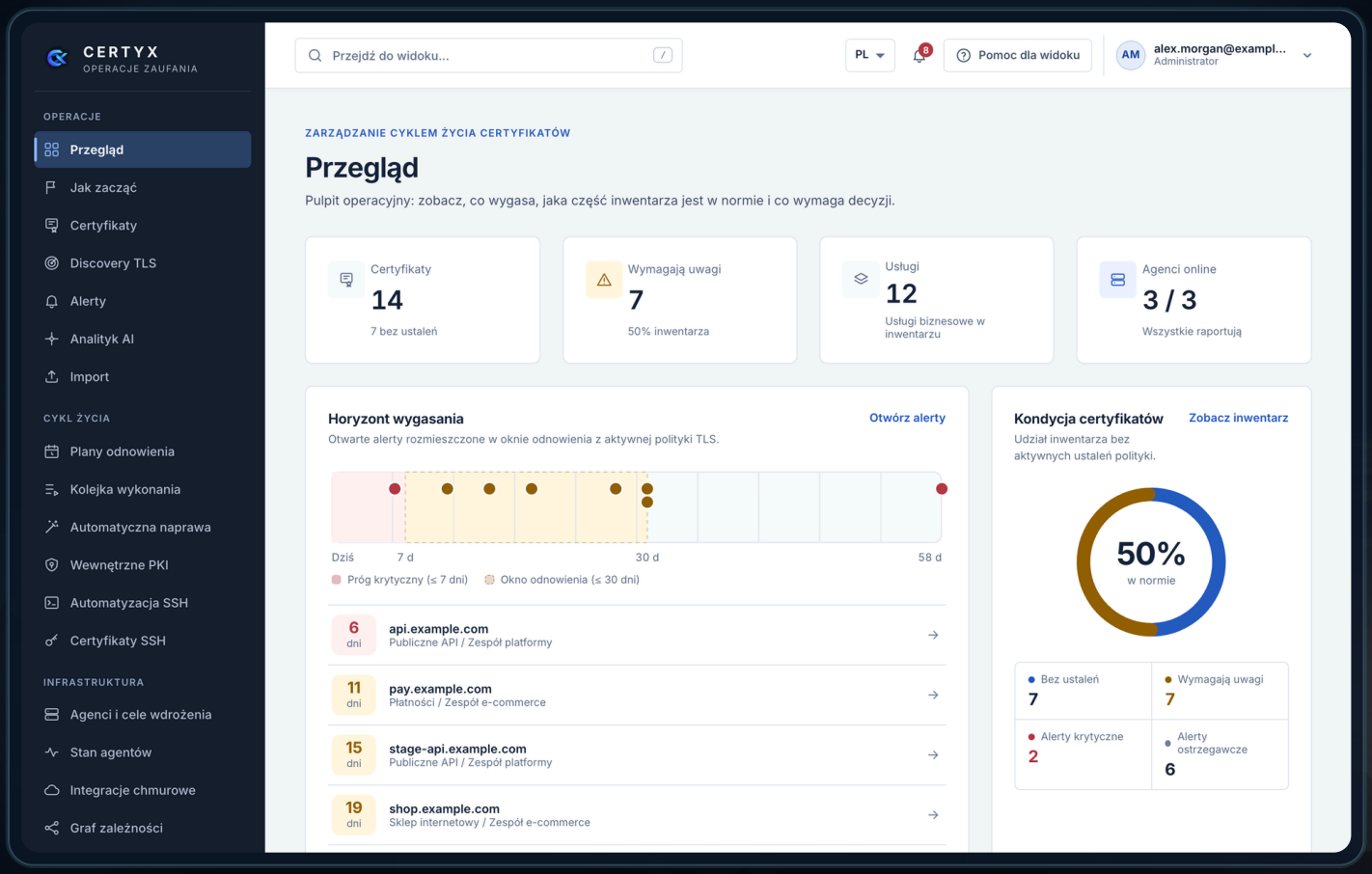
Pełna kontrola nad certyfikatami. Zanim krótsze cykle staną się problemem.

CERTYX odnajduje każdy certyfikat w Twoim środowisku, przypisuje odpowiedzialność i odnawia go przez zatwierdzenie, wdrożenie i weryfikację, a klucze prywatne pozostają w Twojej infrastrukturze.



65 535
portów TCP na zatwierdzony adres

0
zarządzanych kluczy prywatnych wysłanych do CERTYX

5
etapów od odkrycia do weryfikacji

3
języki interfejsu

MOŻLIWOŚCI

Jeden widok operacyjny — od discovery do zweryfikowanego odnowienia.

01 Odkryj
Skanuj zatwierdzone zakresy, importuj pliki PEM lub pobieraj z magazynów chmurowych.

02 Oceń
Ustalenia polityki i kontekst biznesowy pokazują, co jest najważniejsze.

03 Odnów
Należne odnowienia przebiegają automatycznie w ramach zabezpieczeń albo czekają na drugiego administratora tam, gdzie wymagasz zatwierdzenia.

04 Wykonaj
Agent tworzy klucz lokalnie, uzyskuje certyfikat i go instaluje.

05 Zweryfikuj
CERTYX sprawdza certyfikat faktycznie serwowany przez usługę i powiadamia właścicieli.

Discovery TLS
Agenci w Twojej sieci skanują zatwierdzone zakresy IPv4 na dowolnych portach TCP, wznawiają przerwane skany i raportują postęp. Wykluczenia i współbieżność pozostają pod Twoją kontrolą.

Ocena polityki
Każdy certyfikat jest oceniany względem progów wygasania, minimalnej długości klucza i słabych podpisów — z wyjaśnieniem każdego ustalenia.

Automatyczne odnawianie
Klucze i CSR powstają na hoście, który używa certyfikatu. Wystawia go ACME, DigiCert CertCentral lub Vault PKI, z zatwierdzeniem na cztery oczy tam, gdzie go wymagasz; wdrożenie w Nginx, Apache, HAProxy, Tomcat, Kubernetes i innych usługach jest weryfikowane i może zostać wycofane.

Certyfikaty SSH
Inwentarz certyfikatów OpenSSH, zatwierdzone profile podpisywania i listy unieważnień dystrybuowane przez agentów.

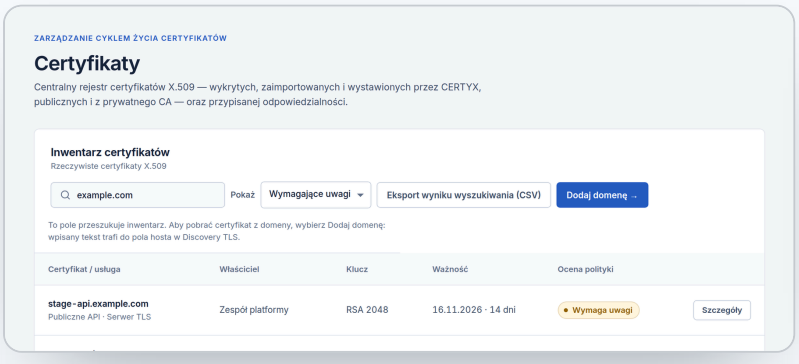
Magazyny chmurowe
Import tylko do odczytu z Azure Key Vault, AWS ACM i Google Certificate Manager przy użyciu Twojej sesji CLI. Żadne poświadczenia chmurowe nie trafiają do CERTYX.

Automatyczna naprawa
Polityki reagują na wygasające lub słabe certyfikaty, wymiany i agentów offline: próba, propozycje do zatwierdzenia przez drugą osobę lub automatyczne zatwierdzanie w granicach zabezpieczeń. Każda decyzja jest zapisywana z powodami.

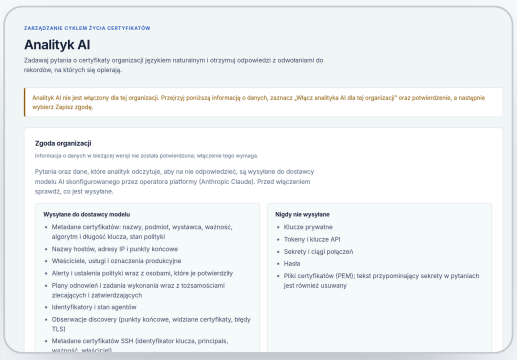
Analityk AI
Pytaj o swoje certyfikaty językiem naturalnym. Odpowiedzi opierają się na danych tylko do odczytu z Twojej organizacji i cytują użyte rekordy. Włączane przez organizację; klucze i sekrety nigdy nie są wysyłane.

CERTYX Mobile
Stan certyfikatów, alerty i obsługiwane zatwierdzenia na urządzeniach iOS i Android aktywowanych przez Twojego administratora jednorazowym kodem.

SIEM w otwartych standardach
Ciągły eksport dziennika bezpieczeństwa do Splunk, IBM QRadar, ArcSight, Microsoft Sentinel, Elastic, Cribl lub OpenTelemetry w formatach CEF, LEEF, RFC 5424, NDJSON, OCSF, ECS lub Splunk CIM.



Inwentarz z właścicielami, usługami i wynikami polityk



AI Trust Analyst: jawna zgoda i kontrola przetwarzania danych

BEZPIECZEŃSTWO I OCHRONA DANYCH

Twoja organizacja. Twoje granice.

Bezpieczeństwo danych decyduje, któremu dostawcy możesz powierzyć certyfikaty. Oto zabezpieczenia wbudowane w CERTYX.

Bezpieczeństwo w projekcie

To, co najbardziej wrażliwe, nigdy do nas nie trafia: klucze prywatne i dane dostępowe do CA zostają u Ciebie, dane każdej organizacji są od siebie oddzielone, a każda uprzywilejowana czynność, także nasza, zostawia ślad, który widzisz.

Nigdy nie trafia do CERTYX

Klucze prywatne zarządzanych certyfikatów · dane dostępowe do CA · dane dostępowe do chmury

Odizolowane organizacje

Osobna baza danych i własne role bazodanowe dla każdej organizacji, z wymuszonym row-level security także we wspólnej warstwie platformy

Twoje klucze zostają u Ciebie

Klucze prywatne zarządzanych certyfikatów powstają i pozostają w Twojej infrastrukturze, nigdy nie trafiają do CERTYX

Zaufani agenci

Agenci używają mutual TLS z zarejestrowaną tożsamością i wyłącznie połączeń wychodzących; podpisane pakiety i aktualizacje są weryfikowane

Szyfrowane sekrety

Przechowywane sekrety są szyfrowane, powiązane z Twoją organizacją i nigdy nie są zwracane przez API

Silne logowanie

MFA dla administratorów, odporne na phishing klucze dostępu (passkeys), logowanie firmowe przez Microsoft Entra ID, Okta, OpenID Connect lub SAML 2.0 oraz SCIM

Sieci i sesje

Logowanie na życzenie tylko z Twoich sieci, krótkie sesje i lista sesji z natychmiastowym unieważnianiem

Role i cztery oczy

Role Audytor, Operator i Administrator; konfigurowalne automatyczne zatwierdzanie lub zasada dwóch par oczu przy odnowieniu, niezależna weryfikacja i wycofanie zmian

Dostęp operatorów pod Twoją kontrolą

Operatorzy platformy pracują z rolami o minimalnych uprawnieniach i dodatkowym potwierdzeniem; dostęp do Twojej organizacji wymaga Twojej zgody lub audytowanego trybu awaryjnego

Dziennik odporny na manipulacje

Dziennik bezpieczeństwa z łańcuchem skrótów, kotwiczony co godzinę podpisem w pamięci jednokrotnego zapisu, który pokazuje także każdą czynność operatora platformy w Twojej organizacji

SIEM bez luk

Eksport do SIEM: Splunk, IBM QRadar, Microsoft Sentinel, Elastic, ArcSight, Cribl i OpenTelemetry w formatach CEF, LEEF, RFC 5424, NDJSON, OCSF, ECS i Splunk CIM przez TLS, z kształtowaniem zdarzeń dla każdego miejsca docelowego i bez cichej utraty zdarzeń

AI pod kontrolą

AI Trust Analyst tylko po włączeniu przez Twojego administratora: wyłącznie odczyt, ze źródłami, bez wysyłania kluczy prywatnych i sekretów

Hosting w UE, szyfrowanie

Hosting w UE (AWS Frankfurt), TLS na każdym połączeniu, baza, dyski i sekrety na dedykowanych kluczach AWS KMS, codzienne szyfrowane kopie jednokrotnego zapisu i chmurowy ślad audytowy

Prywatność i RODO Wskazany administrator danych, opublikowana strona o powierzeniu przetwarzania (art. 28 RODO) i brak śledzenia bez zgody: opcjonalna analityka tylko po wyrażeniu zgody, nigdy na stronach logowania ani w konsoli.

WDROŻENIE I LICENCJONOWANIE

Ty wybierasz, gdzie działa CERTYX.

Hostowane przez CERTYX

Obsługiwane przez nas w UE (AWS Frankfurt): osobna baza danych Twojej organizacji, dane i sekrety szyfrowane dedykowanymi kluczami AWS KMS, codzienne szyfrowane kopie zapasowe w pamięci jednokrotnego zapisu, aktualizacje wdrażamy my. Ty instalujesz tylko agentów.

Własne środowisko

We własnym centrum danych lub koncie chmurowym, z tą samą izolacją i kontrolami. Na własnym koncie AWS klucze szyfrujące (AWS KMS) i chmurowy ślad audytowy należą do Ciebie.

Dział sprzedaży potwierdza, które warianty pasują do Twojego planu.



Przegląd w CERTYX Mobile

Płacisz za to, czym zarządzasz — nie za to, co znajdziesz.

Jednostką licencji jest zarządzana rodzina certyfikatów. Discovery i importy tworzą rekordy niezarządzane, które nie zużywają limitu.

Discovery i importy	Nie są liczone
Odnowienia i wdrożenia	Ta sama rodzina, bez dodatkowego zużycia
Zarządzane rodziny certyfikatów	**Licencjonowany limit**

Współpracuje z

Wystawianie
ACME · DigiCert CertCentral · HashiCorp Vault PKI

Sejfy chmurowe
Azure Key Vault · AWS Certificate Manager · Google Certificate Manager

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

Logowanie firmowe
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

Alerty
Microsoft Teams · Slack · PagerDuty · Webhooks

Zobacz CERTYX na własnym środowisku.

Umów prezentację lub poproś o pilotaż przez formularz kontaktowy na naszej stronie. Na pytania o bezpieczeństwo odpowiadamy, zanim podejmiesz decyzję.

STRONA I FORMULARZ KONTAKTOWY
https://certyx.space

SPRZEDAŻ
sales@certyx.space

WSPARCIE TECHNICZNE
support@certyx.space

Administrator danych osobowych: Rafał Będkowski, osoba fizyczna prowadząca serwis internetowy Certyx (https://certyx.space). Kontakt: support@certyx.space.

Dostępność zależy od pakietu, skonfigurowanych konektorów i zatwierdzonych celów wdrożenia. Certyfikacje, poziomy usług i obsługiwane urzędy certyfikacji określa umowa z klientem. Zrzuty ekranu przedstawiają konsolę i aplikację CERTYX z przykładowymi danymi.

© 2026 CERTYX · Wydanie 1 listopada 2026 · 8550060f