Przepisy o ochronie danych

Zapewnienie zgodności z przepisami o ochronie danych jest kluczowym aspektem utrzymania bezpiecznego i godnego zaufania środowiska. Segura® oferuje kompleksowe rozwiązanie, które automatyzuje zarządzanie dostępem uprzywilejowanym, umożliwiając organizacjom skuteczne sprostanie wyzwaniom związanym z wdrażaniem regulacji kontrolujących oraz osiągnięcie dojrzałości w procesach audytowanych. Dzięki zarządzaniu zaszytymi hasłami, nagrywaniem sesji, ochroną przed kradzieżą danych, dostępem stron trzecich i nadużyciami uprawnień, Segura® umożliwia organizacjom spełnienie wymogów.

Kontrola audytu

Eliminacja zaszytych haseł (DSM)
Zmiany haseł są synchronizowane w plikach konfiguracyjnych i usługach zależnych, co zmniejsza ryzyko nieautoryzowanego dostępu wynikającego z haseł zaszytych w kodzie.

Nagrywanie sesji
100% sesji dostępowych jest rejestrowanych, co zapewnia pełną możliwość śledzenia działań. Zarejestrowane sesje mogą być wykorzystane jako dowód w audycie lub do analizy problemów.

Kontrola dostępu stron trzecich
Gwarantuje, że użytkownicy zewnętrzni mają dostęp wyłącznie do autoryzowanych zasobów, co zmniejsza ryzyko nieuprawnionych działań.

Zapobieganie nadużyciom uprawnień
Dzięki definiowaniu ograniczeń dostępu opartych na denylists i allowlists organizacje mogą skutecznie ograniczać ryzyko nadużycia uprawnień i utrzymywać bezpieczną infrastrukturę.

Ochrona przed kradzieżą danych
Segura® wspiera organizacje w separowaniu dostępu do danych wrażliwych i uprzywilejowanych, izolowaniu krytycznych środowisk oraz korelowaniu zdarzeń w celu identyfikacji podejrzanych zachowań – wszystko zgodnie z zasadami kontroli dostępu opartej na rolach (RBAC). Takie podejście umożliwia wczesne wykrywanie i ograniczanie potencjalnych naruszeń danych.

Odwiedź nas
w naszym Center of Excellence

/segura @segura.security

Wszystko, czego potrzebujesz do kontroli dostępu uprzywilejowanego

segura®

PAM, który chroni to, co ważne. Szybki we wdrożeniu, łatwy w użyciu.

Stworzona z myślą o złożoności rzeczywistego świata, Segura® dostarcza praktyczne rozwiązania w zakresie bezpieczeństwa tożsamości, które integrują się bezproblemowo i odpowiadają sposobowi pracy nowoczesnych zespołów. Ceniona w kluczowych sektorach i uznana przez Gartnera, KuppingerCole oraz Frost & Sullivan, Segura® jest konsekwentnie klasyfikowana wśród najlepszych rozwiązań PAM przez ekspertów ds. cyberbezpieczeństwa na całym świecie.

98% Recommendation 4.9 of 5 ★★★★★
Gartner Peer Insights Customers' Choice 2025

> **„Udało nam się wdrożyć to rozwiązanie w złożonym środowisku z 6 centrami danych w 3 różnych krajach w dość napiętym harmonogramie."**

Dyrektor ds. Bezpieczeństwa Informacji
Referencja zaczerpnięta z portalu Gartner Peer Insights.

DevOps & Secrets
Certificate Manager
★★★✓★ Privileged Access
Remote Access
Pa**word Manager
CIEM
EPM

Dlaczego Segura®?

← ZOBACZ, CO NAS WYRÓŻNIA

Obsługa klienta Premium
Segura® jest znana ze swojego podejścia skoncentrowanego na kliencie oraz wysoko ocenianego wsparcia, mogąc pochwalić się 98% wskaźnikiem rekomendacji na rynku.

Przewaga czasowa: dni zamiast tygodni
Nasza architektura oprogramowania full-stack zapewnia dostęp do wszystkich modułów przez jeden interfejs, umożliwiając spełnienie wymagań dotyczących cyberbezpieczeństwa nawet o 90% szybciej niż konkurencja.

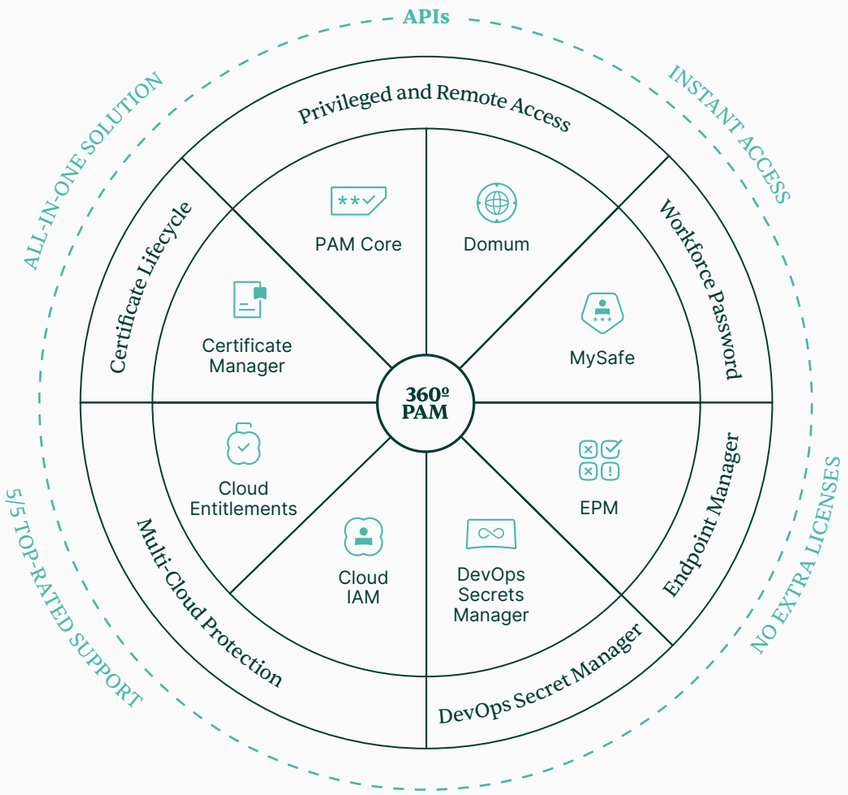
Brak ukrytych kosztów, tylko jasne korzyści
Nasze rozwiązanie PAM ma najniższy całkowity koszt posiadania (TCO) na rynku – nawet o 70% niższy niż u konkurencji – dzięki modelowi cenowemu all-inclusive i architekturze full-stack.

segura® | Futureproof Identity Security | segura. security

PRZEGLĄD ROZWIĄZANIA

Segura® PAM: Zwinny i prosty. Gotowy na przyszłość.

Bezpieczeństwo ze strategią. Innowacja z celem.



Rozwiązanie docenione przez najbardziej znanych

Gartner FORRESTER kuppingercole ANALYSTS

70%
Niższy koszt eksploatacji
Najbardziej opłacalne rozwiązanie PAM na rynku.

90%
Większy zysk
Szybkie wdrożenie w 7 minut, szybszy czas osiągnięcia wartości.

★★★★★
Najwyższa ogólna ocena 4,9/5 przy 98% rekomendacji w Gartner Peer Insights.

← ZESKANUJ, ABY OBEJRZEĆ DEMO

Wszystko, czego potrzebujesz do kontroli dostępu uprzywilejowanego

Kompleksowa platforma Identity Security

PAM Core
Najwyżej oceniane rozwiązanie do zarządzania dostępem uprzywilejowanym (PAM). Skutecznie chroni konta uprzywilejowane, kontroluje dostęp do krytycznych danych i zasobów oraz monitoruje i rejestruje działania w czasie rzeczywistym, generując raporty audytowe.

Domum Remote Access
Zapewnia bezpieczne środowisko dla firm, których działalność często odbywa się poza biurem, kontrolując zdalny dostęp dla pracowników, stron trzecich i klientów bez potrzeby korzystania z VPN.

MySafe
Menedżer haseł, który pozwala generować silne losowe hasła, a także przechowywać i zarządzać notatkami, plikami oraz sekretami API. To rozwiązanie umożliwia automatyczne uzupełnianie haseł w przeglądarce oraz wygodne udostępnianie haseł przez sieć i urządzenia mobilne.

EPM
Rozwiązanie EPM (Endpoint Privilege Management) dla systemów Linux, Windows i macOS, które pozwala użytkownikom końcowym uruchamiać aplikacje wymagające uprawnień administracyjnych bez konieczności podglądu poświadczeń. Dodatkowo automatycznie rotuje hasła, eliminując konieczność interwencji innych użytkowników.

DevOps Secret Manager
Ułatwia zarządzanie aplikacjami i sekretami w środowisku deweloperskim poprzez definiowanie polityk dostępu oraz udostępnianie, zmienianie i unieważnianie sekretów. Zapobiega to pozostawaniu poświadczeń, kluczy dostępu i innych poufnych informacji w postaci zakodowanej na stałe lub statycznej.

Certificate Manager
Scentralizowane zarządzanie wewnętrznymi i zewnętrznymi certyfikatami cyfrowymi, zapewniające pełny i scentralizowany widok wszystkich certyfikatów i ich statusu – od wykrywania i automatycznego skanowania stron internetowych, katalogów i serwerów WWW po generowanie certyfikatów i ich automatyczne odnawianie.

Cloud IAM
Zarządzanie tożsamościami, które pomaga kontrolować dostęp i podmioty w ramach dostawców usług chmurowych (CSP). Administrator modułu może centralnie zarządzać środowiskami chmurowymi, ograniczać dostęp i uprawnienia zgodnie z polityką firmy, zapewniać zgodność w dostępie do infrastruktury chmurowej oraz izolować, monitorować i nagrywać wszystkie sesje.

Cloud Entitlements
Rozwiązanie CIEM (Cloud Infrastructure Entitlements Management) do zarządzania uprawnieniami tożsamości w środowiskach multi-cloud, oferujące elastyczną analizę polityk. To rozwiązanie zapewnia pełną separację danych, nawet gdy wielu klientów korzysta z tej samej platformy.

Segura® Appliance
Rozwiązanie sprzętowe z niestandardowym systemem operacyjnym i wbudowaną, zastrzeżoną bazą danych, zapewniające zwiększone bezpieczeństwo i wydajność. Zostało zaprojektowane dla firm poszukujących wyższego poziomu bezpieczeństwa, gwarantowanej wydajności oraz scentralizowanego wsparcia dla oprogramowania i sprzętu.

PAM Load Balancer
Gotowe do wdrożenia i wstępnie skonfigurowane rozwiązanie, zaprojektowane w celu optymalizacji działania całego rozwiązania Segura®. Nasz load balancer wykorzystuje certyfikat SSL, który jest już zainstalowany na instancjach Segura®, dzięki czemu nie ma potrzeby instalowania oddzielnego certyfikatu SSL.

segura® | Futureproof Identity Security | segura. security