unshadow IT

Identity & Access | SaaS Governance | AI Security

nowa rzeczywistość wymaga nowego spojrzenia na bezpieczeństwo

Pomagamy firmom odzyskać kontrolę nad tożsamościami, dostępami i aplikacjami

Q2 2026

unshadowit.com

Trzy obszary, jedno wyzwanie

widoczność.

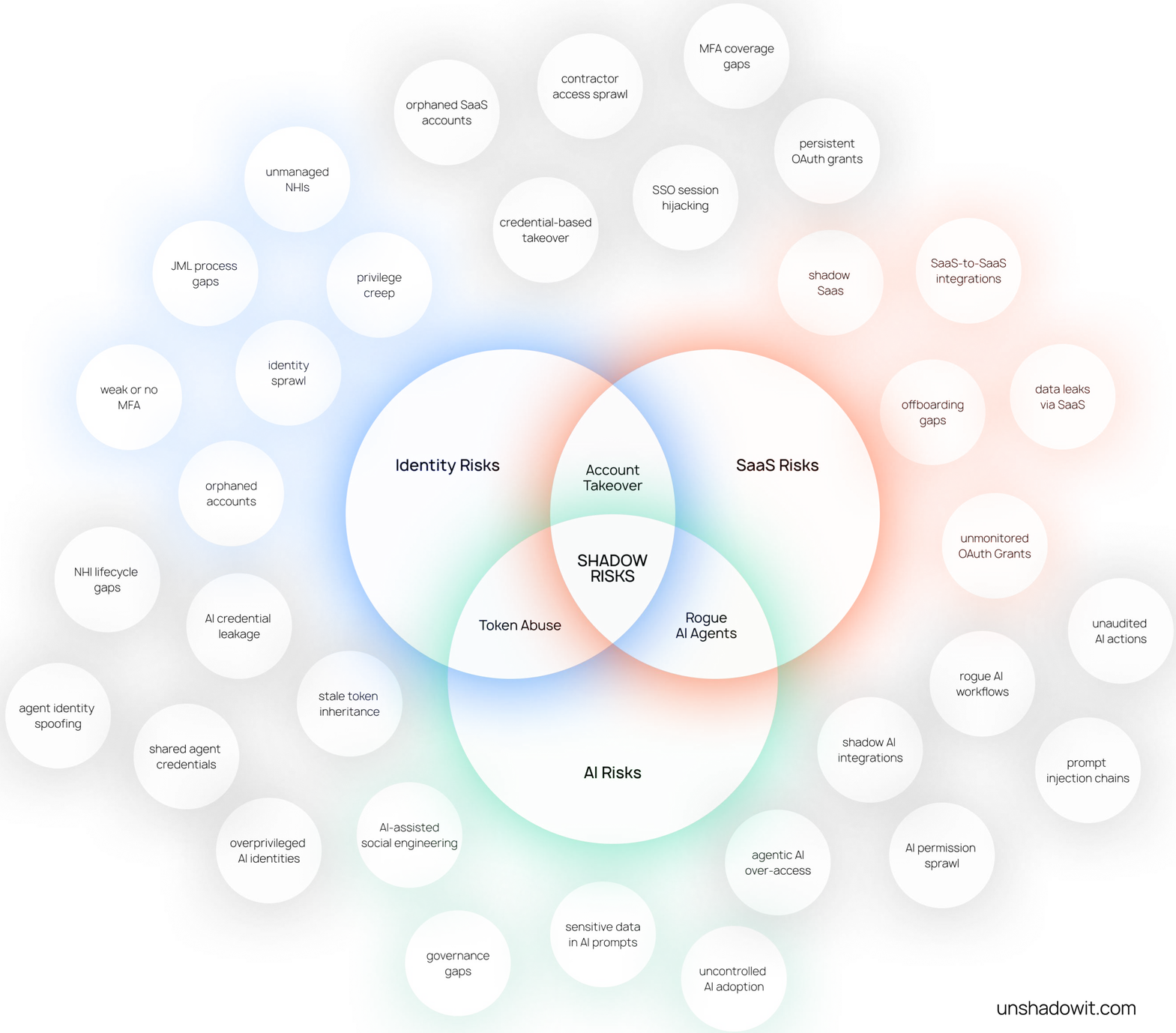
Nie możesz chronić tego, czego nie widzisz.

Większość organizacji ma już jakiś fundament identity — Active Directory, Entra, Google Workspace.

Problem w tym, że te systemy zostały zaprojektowane dla innej rzeczywistości i najczęściej nie zauważą:

- 150 aplikacji SaaS zakupionych przez marketing lub finanse,
- niewygaszonych triali z aktywnymi dostępami do firmowych danych,
- wrażliwych danych, które pracownicy wklejają do AI,
- integracji SaaS pozostawionych przez byłych pracowników,
- kont, które powinny być zamknięte miesiące temu...

Obecne rozwiązania nie zamykają dostępów w miejscach, których nie znają. I to właśnie tam pojawia się ryzyko.



Zacznij od widoczności, osiągnij pełną kontrolę

okta YeshID nudge Rublon LOG PLUS DRATA Layer X

Identity & Access

Przeprowadzamy organizację od rozproszonych dostępów i manualnych procesów do pełnej kontroli nad tożsamościami, od pierwszego dnia pracy do ostatniego.

- Identity & Access Audit
- SSO & Directory Management
- Multi-Factor Authentication (MFA)
- Identity Lifecycle Management (ILM)
- Joiner / Mover / Leaver Process Design
- Offboarding Automation
- Access Reviews & Recertification
- Tool Selection & Implementation

SaaS Governance

Przeprowadzamy organizację od niewidocznego i niezarządzanego stacku do pełnej inwentaryzacji, kontroli i procesów zatwierdzania aplikacji.

- SaaS Discovery & Inventory
- Shadow IT Identification & Risk Assessment
- SaaS Spend Optimization
- App Request & Approval Workflow
- Tool Selection & Implementation

AI Security

Przeprowadzamy organizację od niekontrolowanej adopcji AI do zarządzanego środowiska z pełną widocznością, politykami i kontrolami dostępu.

- Shadow AI Discovery
- AI Risk Assessment
- AI Acceptable Use Policy (AUP)
- Approved AI Tools Framework
- GDPR & AI Act Compliance Review
- AI Monitoring & Governance

YeshID
okta nudge

IAM
IGA
IDM
IdP

Rublon
okta

SSO
MFA
TOTP
SAML

AI Security
AI Control
AI DLP
ZTBS

LayerX
okta YeshID nudge

SaaS Discovery
SaaS Governance
SaaS Security
SSPM

nudge
YeshID

rozwiązania bezpieczeństwa dla nowoczesnych organizacji

GRC
DRATA

ITAM SAM ITSM
LOG PLUS

YeshID

IAM IGA IDM

Kompleksowa platforma do zarządzania wszystkimi tożsamościami i dostępami

Platforma zaprojektowana z myślą o organizacjach cloud-first. Automatyzuje pełny cykl życia tożsamości — od przyznawania uprawnień przy onboardingu, przez zarządzanie dostępami w trakcie zatrudnienia, po natychmiastowe odebranie uprawnień w momencie odejścia pracownika.

Wykrywanie shadow IT i OAuth

Skanowanie tokenów OAuth ujawnia wszystkie aplikacje używane przez pracowników, łącznie z tymi zainstalowanymi bez wiedzy IT

Automatyzacja cyklu życia tożsamości

Onboarding i offboarding wyzwalane automatycznie z HRIS lub katalogu — każde konto, każda aplikacja, w tym te bez obsługi SCIM

Mapa dostępów w czasie rzeczywistym

Aktualna inwentaryzacja każdej tożsamości (ludzie i konta NHI) względem każdej aplikacji w organizacji (Access Grid)

Just-in-Time Access przez Slack & Teams

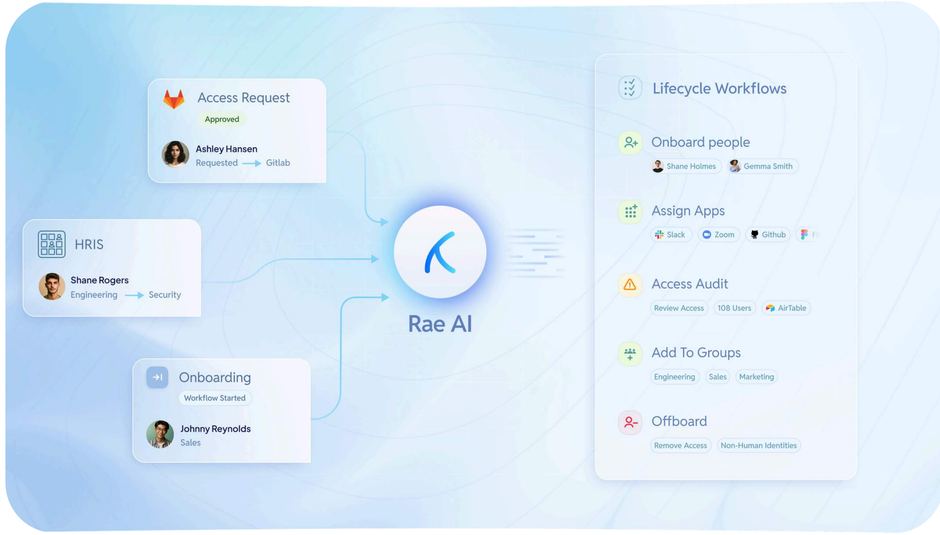
Pracownik wysyła request, manager zatwierdza inline, dostęp automatycznie wygasa — bez ryzyka pozostawienia "tymczasowego" dostępu na dłużej

Gotowe raporty dla audytorów

Logi każdego nadania i cofnięcia dostępu, eksport evidence dla SOC 2, ISO 27001, NIS2 i DORA jako efekt uboczny codziennej pracy

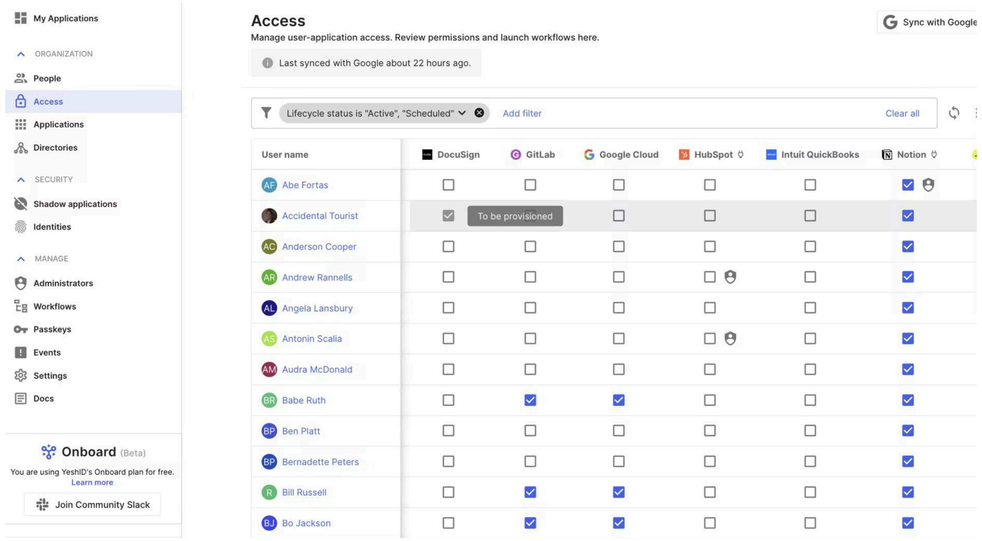
Governance bez SSO tax

Zarządza aplikacjami bez SAML i SCIM przez natywne API — pełna kontrola na standardowych planach, bez dopłat za enterprise tier



bignetwork SOULCYCLE THE CONVERSATION TigerData

Timescale ANJUNA Determinate Systems QUIVO SEVCO



Platforma zaprojektowana z myślą o organizacjach cloud-first.

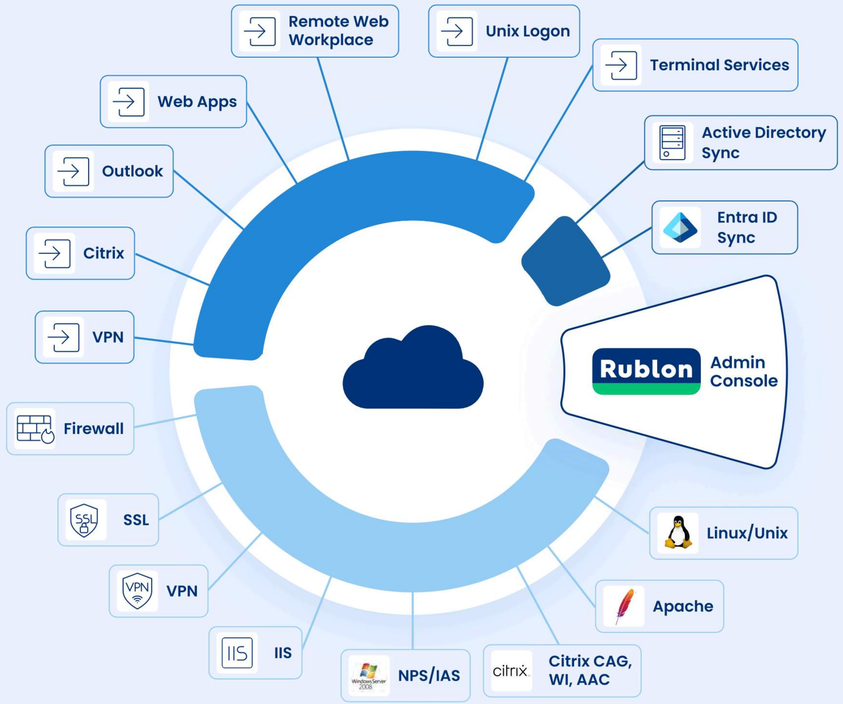
Rublon

MFA SSO TOTP SAML

Pełne zabezpieczenie przed nieautoryzowanym dostępem

Nowoczesna i elastyczna, platforma Multi-Factor Authentication (MFA), która pomaga zabezpieczyć się przed atakami phishingowymi oraz próbom przejęcia kont wprowadzając dodatkową, inteligentną warstwę weryfikacji tożsamości. System udowadnia, że zaawansowane bezpieczeństwo może być wdrożone w kilkanaście minut, oferując pracownikom najwygodniejsze metody logowania

symfonia · VIALUTIONS · Itmation · ZBĄSZYŃ miasto nad jeziorem · Bank Spółdzielczy w Przasnyszu Grupa BPS · Bełchatów Tylko dobre re:akcje · Urząd Gminy Łambinowice · PWiK Szczecinek · UMiG Kąty Wrocławskie



Wszechstronna ochrona logowania

Zabezpiecza nie tylko aplikacje w chmurze, ale jako jedno z nielicznych rozwiązań oferuje natywną ochronę dla Windows Logon, Pulpitów Zdalnych (RDP) oraz logowań do serwerów Linux (SSH)

Bezpieczny dostęp zdalny (VPN)

Integruje się z niemal każdym rozwiązaniem sieciowym (Cisco, Fortinet, Palo Alto, OpenVPN), wymagając dodatkowego potwierdzenia tożsamości przy każdym połączeniu z biurem

Najsilniejsze metody uwierzytelniania

Od błyskawicznych powiadomień push, przez kody QR i TOTP, aż po odporne na phishing klucze sprzętowe FIDO2 (np. YubiKey).

Logowanie bez hasła (Passwordless)

Umożliwia rezygnację z tradycyjnych haseł na rzecz biometrii i kluczy bezpieczeństwa, co drastycznie podnosi komfort użytkownika i poziom ochrony

Inteligentne polityki dostępu

Pozwala na definiowanie reguł adaptacyjnych np. wymagaj MFA tylko przy logowaniu spoza biura lub z nieznanych urządzeń

Skuteczna bariera dla ransomware

Większość ataków szyfrujących dane zaczyna się od przejęcia dostępu do VPN lub RDP. Rublon odcina tę drogę, uniemożliwiając hakerowi wejście do sieci nawet ze sprawnym hasłem pracownika

VPN poprzez RADIUS, LDAP, SAML	CISCO	FORTINET	MikroTik	WatchGuard
Microsoft własne konektory	Windows	Microsoft Remote Desktop Services	Office 365	Outlook
Web & Desktop własne konektory	vmware Horizon View	Jira	WordPress	Custom (SDK)
Cloud poprzez SAML	Google Workspace	salesforce	pingdom	zendesk
Linux własne konektory	debian	ubuntu	Red Hat Enterprise Linux	VERITAS

Nie pozwól, aby słabe hasło było najsłabszym ogniwem Twojej firmy.
Wybierz rozwiązanie, które łączy potężną technologię z prostotą użytkowania

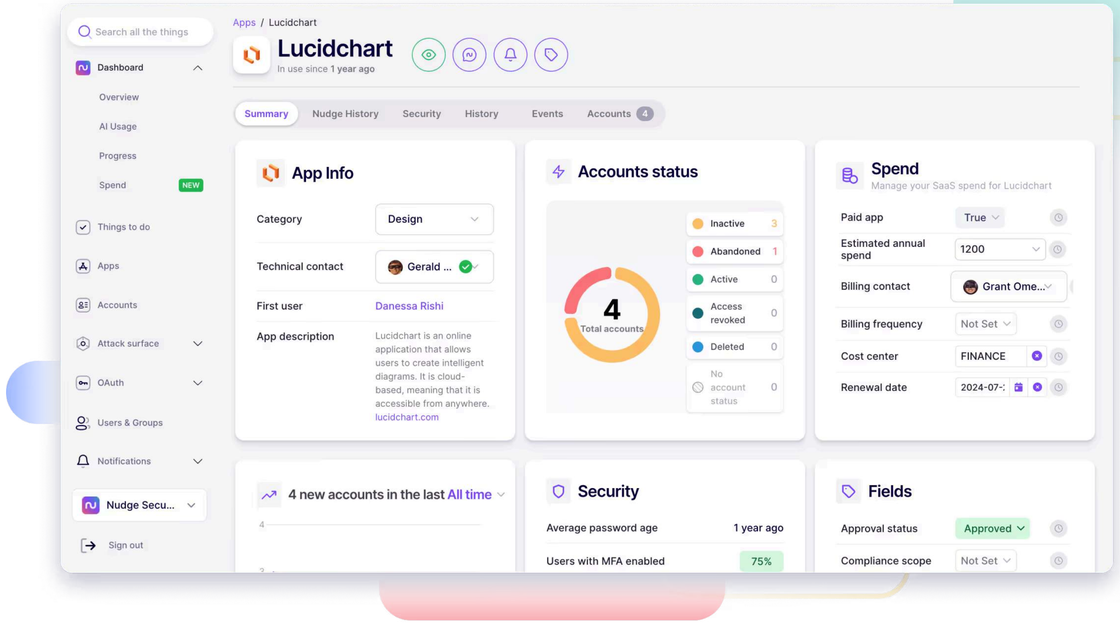
nudge

SaaS Discovery | SaaS Security | SSPM

Kompletna widoczność aplikacji SaaS oraz aktywne zarządzanie bezpieczeństwem

Platforma bezpieczeństwa SaaS, która łączy techniczny monitoring z aktywnym kształtowaniem zachowań pracowników. Automatycznie odkrywa wszystkie aplikacje używane w organizacji — łącznie z tymi, których IT nie zna — mapuje ich połączenia OAuth, ocenia powierzchnię ataku i wykrywa ryzyko tożsamości.

Wyróżnia się tym, że nie zatrzymuje się na inwentaryzacji: angażuje pracowników bezpośrednio poprzez celowane powiadomienia i rekomendacje, które pomagają im samodzielnie podejmować bezpieczniejsze decyzje.



Automatyczne odkrywanie shadow IT

Identyfikuje wszystkie aplikacje SaaS używane przez pracowników — w tym te założone bez wiedzy IT — bez agentów i bez konieczności zmian w sieci

Mapowanie OAuth i surface attack SaaS

Wizualizuje wszystkie integracje między aplikacjami, ocenia uprawnienia nadane przez pracowników i wskazuje największe ryzyka w ekosystemie SaaS

Monitoring po odejściu pracownika

Wykrywa konta byłych pracowników, które nadal mają aktywne dostępy do aplikacji SaaS — i ułatwia ich systematyczne usuwanie

Wykrywanie ryzyka tożsamości

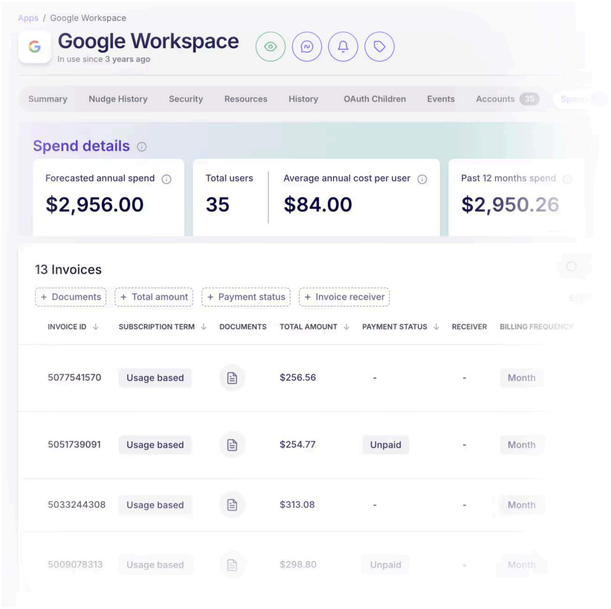
Identyfikuje konta bez MFA, współdzielone loginy, nieużywane dostępy i aplikacje bez umów DPA — szczególnie istotne przy RODO i NIS2

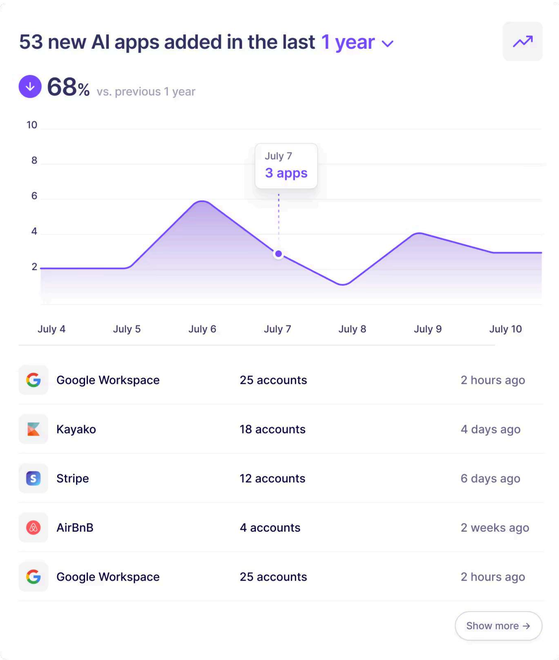
Budowanie kultury bezpieczeństwa

Łączy widoczność techniczną z edukacją w jednym narzędziu — bez potrzeby wdrażania osobnych kampanii phishingowych czy platform szkoleniowych

Aktywne angażowanie pracowników (nudges)

Zamiast blokować, może informować. Pracownicy otrzymują powiadomienia z kontekstem, dlaczego dane działanie jest ryzykowne i jak je poprawić.





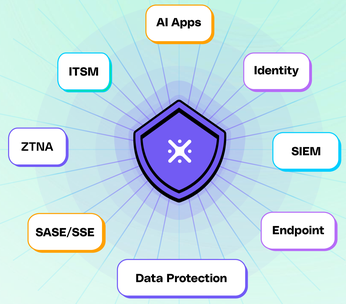
Twój zespół już teraz używa dziesiątek aplikacji, których nie zatwierdziłeś. Przejmij inicjatywę już teraz, zamiast czekać na przejęcie kont pracowników.

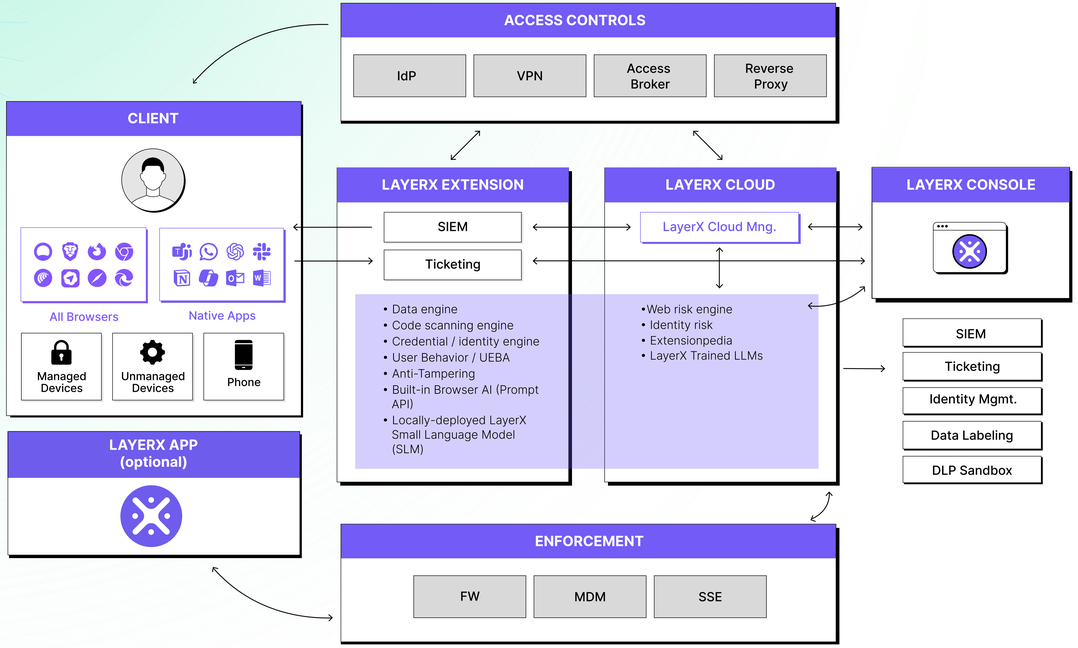
LayerX

AI Security | AI Control | ZTBS

Bezpieczeństwo AI bezpośrednio w przeglądarce Twojego zespołu

LayerX to platforma bezpieczeństwa działająca na poziomie przeglądarki, która chroni organizację przed wyciekiem danych przez narzędzia AI — takie jak ChatGPT, Gemini, Microsoft Copilot czy Claude. Działa jako rozszerzenie przeglądarki, bez VPN, bez agentów sieciowych i bez ingerencji w infrastrukturę. Widzi dokładnie co użytkownicy wklejają do promtów i może to kontrolować w czasie rzeczywistym — zanim dane opuszczą organizację.





Pełny audit log użycia AI

Komplet informacji o tym, kto, kiedy działa z jakim modelem i jakim typem danych. Gotowe do review polityk DLP i audytu zewnętrznego

Real-Time DLP dla AI

Wykrywa i blokuje wklejanie kodu źródłowego, PII, danych finansowych i dokumentów do ChatGPT, Gemini, Copilot, Claude i innych LLM

Blokada przesyłania plików do AI

Monitoruje nie tylko prompty tekstowe — również próby wysłania PDF, CSV i dokumentów do modeli przez interfejsy webowe

Bezpośrednio w przeglądarce

Wdrożenie przez Chrome/Edge extension. Bez agentów sieciowych, bez proxy, bez VPN. Dane widoczne w pierwszych godzinach.

Działa na BYOD bez MDM

Nie wymaga pełnego zarządzania urządzeniem. Wystarczy deployment rozszerzenia przez Google Workspace lub Intune

Integracja z SIEM / SOC

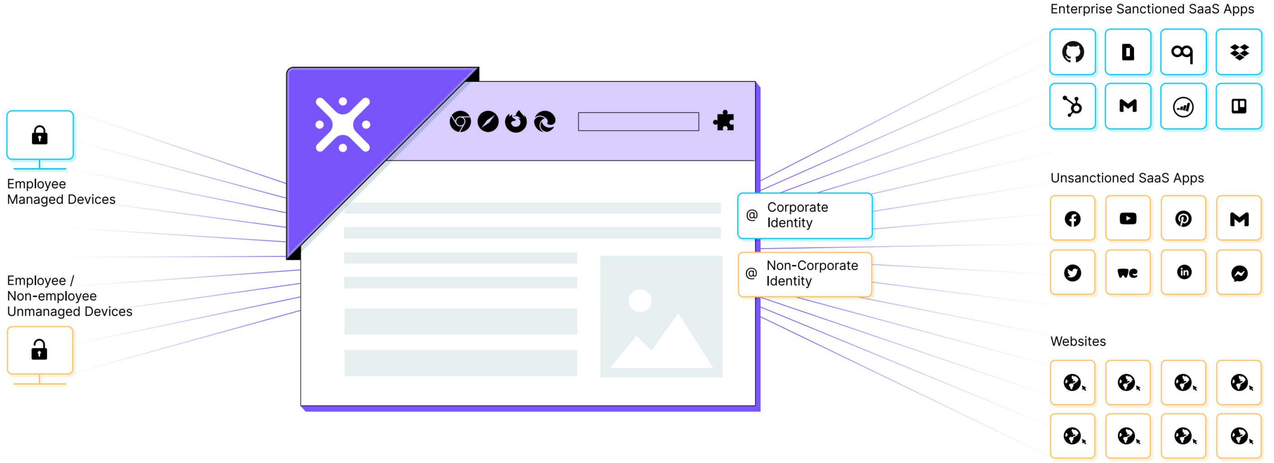
Logi z LayerX trafiają do Splunk, Microsoft Sentinel, Elastic i innych — 'AI usage risk' definiowane jako osobna kategoria zdarzeń

Wykrywanie Shadow AI

Identyfikuje nieautoryzowane modele i AI pluginy używane przez pracowników — łącznie z niszowymi narzędziami poza oficjalnym stackiem

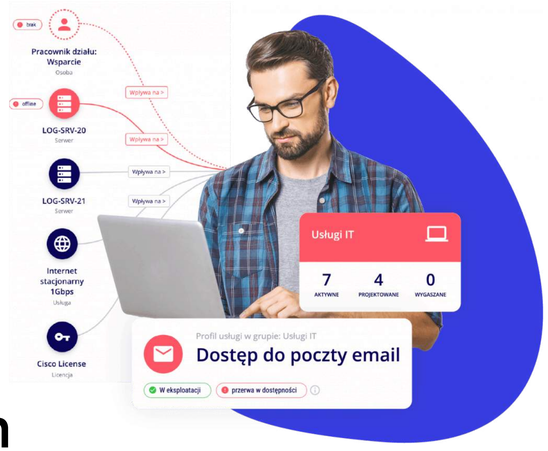
Tryb ostrzeżenia zamiast blokady

„Warn before send" — użytkownik widzi alert i świadomie podejmuje decyzję, zamiast otrzymać bezwzględną blokadę działania



LOG PLUS

ITAM SAM ITSM



Twoje centrum dowodzenia infrastrukturą i bezpieczeństwem

LOG Plus to oprogramowanie do zarządzania zasobami i usługami IT w organizacji. Zapewnia kontrolę nad infrastrukturą informatyczną, wykonanie samodzielnego audytu oprogramowania, monitoring pracy użytkowników i komputerów, możliwość zdalnych operacji i zarządzania stanowiskami pracy oraz wsparcie w zarządzaniu bezpieczeństwem.

Pełna inwentaryzacja zasobów (ITAM & CMDB)

Śledzi cały cykl życia każdego urządzenia – od momentu zakupu serwera, laptopa czy telefonu, po jego bezpieczną utylizację. Zawsze wiesz, kto, gdzie i na jakim sprzęcie pracuje

Optymalizacja licencji oprogramowania (SAM)

Automatycznie audytuje instalacje na komputerach pracowników, zestawia je z zakupionymi licencjami i alarmuje o nielegalnym oprogramowaniu lub nieużywanych, a opłacanych subskrypcjach

Nowoczesny helpdesk i automatyzacja (ITSM)

Obsługuje zgłoszenia pracowników (incydenty, awarie, wnioski) z wykorzystaniem intuicyjnych formularzy i graficznego edytora procesów (Workflow). Zero mailowego chaosu

Proaktywny monitoring i bezpieczeństwo

Oferuje funkcje klasy DLP (Data Loss Prevention) – kontroluje podłączane pendrive'y, monitoruje operacje na wrażliwych plikach, rejestruje wydruki i zarządza uprawnieniami na stacjach roboczych

Koniec silosów informacyjnych

Zastępujesz kilka drogich systemów (do inwentaryzacji, helpdesku, zdalnego pulpitu i monitoringu) jedną, spójną platformą, obniżając koszty utrzymania stacku technologicznego (TCO).

Zdalne zarządzanie stacjami (Remote Control)

Wyposaża administratorów we wbudowany, bezpieczny mechanizm (VNC), pozwalający na szybką pomoc techniczną i zdalne rozwiązywanie problemów użytkowników w czasie rzeczywistym

Kompleksowa platforma klasy IDM, ITAM, SAM i ITSM, stanowiąca fundament nowoczesnego zarządzania infrastrukturą IT oraz bezpieczeństwem informacji w organizacji

Elastyczna licencja

licencja wieczysta | subskrypcja

niezwykle wydajny

Widok ekranu ładuje się w **max. 3 sekundy nawet przy 50 000 zasobach**!

Integracje

Microsoft, ORACLE, IBM, SAP, vmware, Active Directory, Hyper-V, Azure, PostgreSQL

Platforma posiada wbudowaną, stale rozwijaną, listę natywnych konektorów do popularnych rozwiązań. LOG Plus oferuje również API Rest, umożliwiające zbudowanie niemalże każdej integracji.

All-in-one

43

modułów funkcjonalnych

Dostęp do wszystkich potrzebnych funkcji z jednego miejsca.

Skalowalny

Platformę można skalować od bardzo małych do bardzo dużych projektów!

Bezpieczny

Testowany pod kątem podatności
Szyfrowane logowanie
SSO

Dostępny przez

przeglądarki internetowe z dowolnego urządzenia!

1 h – Go live!

Błyskawiczne wdrożenie systemu za pomocą Virtual Appliance .

RE Polska, Grupa Azoty, PKP Cargo, Santander, NIK, Fiberhost, Votum SA, Mazowiecki Szpital Brodnowski, POZnań, Interia, dekpol, vectra, Miasto Toruń, Herbapol, GAZ system, Akademia Sztuk Pięknych im. Eugeniusza Gepperta we Wrocławiu, Akademia Techniczno-Humanistyczna w Bielsku-Białej, Koleje Mazowieckie, deatrans We care. More than u think

DRATA

GRC

Automatyczna dokumentacja
compliance w czasie rzeczywistym

Drata to platforma do automatyzacji compliance, która zastępuje ręczne zbieranie dowodów ciągłym monitoringiem całego stosu technologicznego. Łączy się z ponad 100 narzędziami — od AWS i GitHub po Okta i Jira — i automatycznie mapuje zebrane dane na kontrolki wybranych frameworków: SOC 2, ISO 27001, NIS2, DORA, HIPAA i innych

Stałe aktualizowanie rejestrów

Drata automatycznie pobiera dowody zgodności z podłączonych systemów — codziennie, nie tylko gdy audytor puka do drzwi

Ponad 20 frameworków jednocześnie

SOC 2, ISO 27001, NIS2, DORA, HIPAA, GDPR, PCI DSS i inne — jeden stack, jeden dashboard, mapa nakładania się kontrolek

Gotowe polityki i procedury do edycji

Biblioteka szablonów polityk bezpieczeństwa dostosowanych do wybranego frameworku — nigdy nie zaczynasz od zera

Ponad 100 gotowych integracji

Łączy się z AWS, GCP, Azure, GitHub, Jira, Okta, Slack i innymi — automatycznie mapuje kontrolki do dowodów z każdego narzędzia

Zarządzanie vendorami i dostawcami

Inwentaryzacja third-party vendors, ocena ryzyka, śledzenie statusu umów DPA i BAA — wymagane przez NIS2 i GDPR

Employee compliance tracking

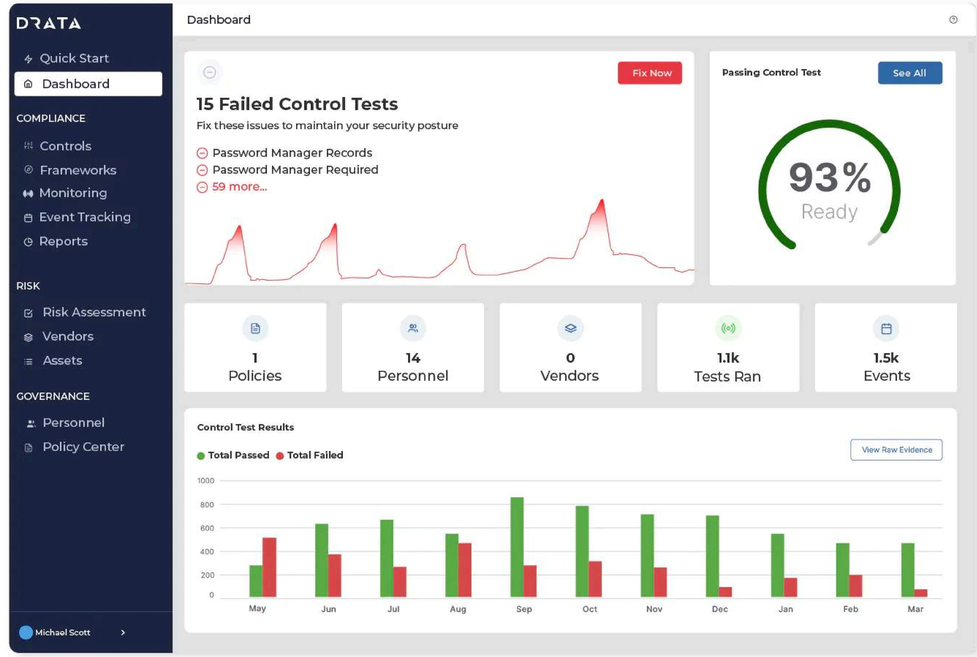
Automatyczne przypomnienia o szkoleniach security awareness, zbieranie podpisów pod politykami, status onboardingu — wszystko w jednym miejscu

Dashboard zgodności Real-Time

Widać które kontrolki są spełnione, które wymagają uwagi i ile brakuje do certyfikacji

Skraca czas do certyfikatu SOC 2

Firmy raportują uzyskanie SOC 2 Type I w 2–3 miesiące zamiast 6–12 przy tradycyjnym podejściu



Specjalistyczny partner cybersecurity.

Tożsamość, SaaS i AI

Skupiamy się na trzech obszarach, w których rośnie największe ryzyko w nowoczesnych organizacjach: zarządzaniu tożsamością, bezpieczeństwie SaaS i kontroli nad AI w środowisku pracy.

Nie sprzedajemy wszystkiego. Audytujemy, następnie rekomendujemy właściwe narzędzie, dostarczamy licencje, wdrażamy i pomagamy zarządzać — jako jeden partner, od początku do końca.

audytujemy

Zaczynamy od tego, co jest — nie od tego, co powinno być. Początkowy audyt daje pełny obraz środowiska bez żadnych zmian w infrastrukturze..

wdrażamy

Rekomendujemy właściwe narzędzie, niezależnie od portfolio i vendorów, dostarczamy licencję i przeprowadzamy wdrożenie.

utrzymujemy

Nie znikamy po podpisaniu umowy. Kwartalne przeglądy, bieżące wsparcie, dostęp do wiedzy o rynku — do Twojej dyspozycji.

Mamy doświadczenie z wdrożeń zarządzania tożsamością oraz dostępami uprzywilejowanymi w największych organizacjach — i wiemy, że każda decyzja zakupowa powinna zaczynać się od szczegółowej analizy infrastruktury, nie od broszury vendora.