# PLATFORMA DO OCHRONY PRZED ZAGROŻENIAMI WEWNĘTRZNYMI

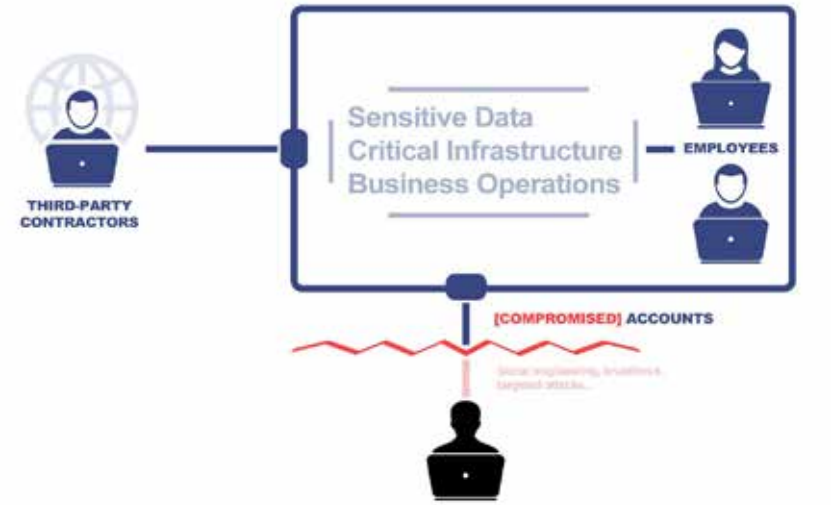
Zarządzaj dostępem. Monitoruj aktywność. Odpowiadaj na incydenty.

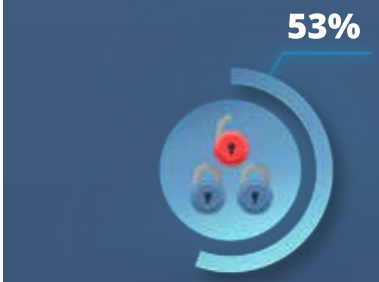
EKRAN®

## WYZWANIA ZWIĄZANE Z ZAGROŻENIAMI WEWNĘTRZNYMI

Podczas opracowywania zasad mających na celu ograniczenie ryzyka związanego z bezpieczeństwem informacji wewnętrznych, działy IT muszą rozważyć konkretne podejścia i narzędzia. Wykrywanie i badanie zdarzeń spowodowanych przez osoby wewnętrzne jest dość trudne z różnych powodów:

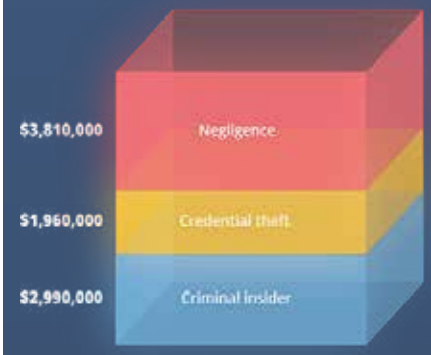
- Osoby wewnętrzne posiadają autoryzowany dostęp.
- Jedna osoba wykonuje nawet do 10 000 operacji dziennie, każdego dnia.
- Osoby wewnętrzne znają tajniki infrastruktury.
- Osoby wewnętrzne mogą współpracować i zacierać swoje ślady.




**53% ORGANIZACJI DOŚWIADCZYŁO ATAKÓW WEWNĘTRZNYCH W CIĄGU OSTATNICH 12 MIESIĘCY ***

* Według 2018 Threat Report by Crowd Research Partners




** Według raportu 2018 Cost of Insider Threats: Global Organizations by the Ponemon Institute

## W JAKI SPOSÓB EKRAN SYSTEM® ZWALCZA ZAGROŻENIA

Ekran System® to uniwersalna platforma ochrony przed zagrożeniami wewnętrznymi, która obejmuje trzy główne kontrole cyberbezpieczeństwa wewnętrznego: monitorowanie użytkowników, zarządzanie tożsamością i zarządzanie dostępem.

### Kontroluj dostęp do kont użytkowników

Ekran oferuje zarządzanie tożsamością i dostępem w ramach pojedynczczego agenta zainstalowanego na endpoincie. W jego skład wchodzi uwierzytelnianie dwuskładnikowe (2FA), jednorazowe hasła, zarządzanie kontami uprzywilejowanym i sesjami (PASM), integracja z systemami zgłoszeń i inne.

### Monitoruj i badaj aktywność

Ekran monitoruje, rejestruje i audytuje wszystkie działania użytkowników na krytycznych punktach końcowych, danych i konfiguracjach, wykorzystując indeksowane zapisy wideo zainicjowanych sesji.

### Wykrywaj zagrożenia i odpowiadaj w czasie rzeczywistym

Ekran zapewnia wysoce konfigurowalny podsystem ostrzegania, który obejmuje edytowalne reguły oparte na ogólnych wskaźnikach behawioralnych potencjalnych zagrożeń, a także moduł do wykrywania anomalii w procedurach użytkowników wewnętrznych, oparty na sztucznej inteligencji.

Gartner peerinsights™

> “One of the fastest solution that I have installed and configured. I can recommend EKRAN as a good, light and efficient User Monitoring Solution.

## DLACZEGO NASI KLIENCI WYBIERAJĄ EKRAN SYSTEM®

Zawiera trzy elementy kontroli bezpieczeństwa

Oferuje przejrzyste i elastyczne licencjonowanie

Działa w każdej konfiguracji i na każdej platformie

Wspiera wdrożenia na dużą skalę

## NAJWAŻNIEJSZE FUNKCJE EKRAN SYSTEM®

### ZARZĄDZANIE TOŻSAMOŚCIĄ

- Two-factor authentication (dane logowania + urządzenie mobilne)
- Dwukrotne uwierzytelnienie dla współdzielonych kont

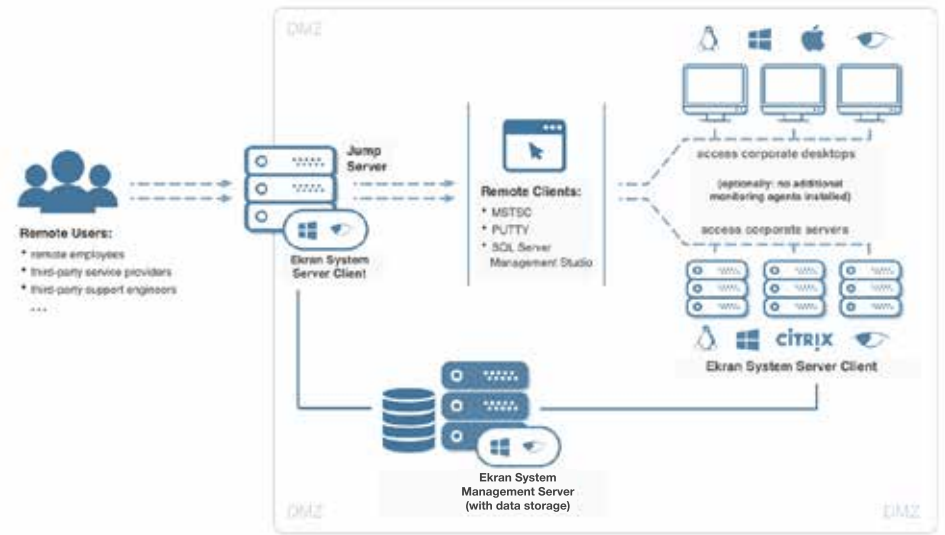
### ZARZĄDZANIE DOSTĘPEM

- Jednorazowe hasła
- Ręczne zatwierdzanie logowania przez nadzorcę
- Zarządzanie Hasłami (dostęp RDP i SSH)
- Integracja z systemami Help-Desk

### AUDYT I KONTROLA DZIAŁAŃ

- Nagrywanie sesji w formie indeksowanych zapisów video
- Zaawansowane opcje przeszukiwania i raportów
- Alerty oparte o reguły
- Ręczne i automatyczne odpowiedzi na incydenty
- Zarządzanie USB

## MIESZANY SCHEMAT WDROŻENIA




## BĄDŹ ZGODNY ZE STANDARDAMI I REGULACJAMI

Mentioned in NIST Special Publication

## WYBRANI KLIENCI

## NAJBARDZIEJ KOMPLETNY ZESTAW WSPIERANYCH PLATFORM

Windows macOS Linux UNIX® vmware CITRIX

## LICENCJONOWANIE

Ekran System® licencjonowany jest na podstawie monitorowanych endpointów oraz konsoli Standard i Enterprise. Wersja Enterprise zawiera dodatkowe funkcje integracji i utrzymania systemu.

Odwiedź nas na https://www.ekransystem.com

**Ekran System Polska**
ul. Gąsiorowskich 4/99,
60-704 Poznań