SafeConnect | Privileged Access Management

I-BS.PL

Dostęp uprzywilejowany pod pełną kontrolą.

Bez haseł, bez VPN, bez luk w audycie.

SafeConnect to system klasy *Privileged Access Management* (PAM), który pośredniczy w każdym uprzywilejowanym dostępie do infrastruktury klienta — serwerów Linux i Windows, urządzeń sieciowych (firewalli, switchy, routerów), aplikacji webowych i paneli administracyjnych oraz wirtualnych desktopów uruchamianych na żądanie.

Zamiast udostępniać administratorom bezpośrednie klucze SSH, hasła lub poświadczenia RDP, **SafeConnect** zapewnia jeden centralny portal dostępowy w przeglądarce, przez który realizowane są wszystkie połączenia.

SafeConnect upraszcza zarządzanie dostępem uprzywilejowanym i jednocześnie zwiększa poziom bezpieczeństwa, nadzoru oraz zgodności regulacyjnej.

Każda sesja jest:

- przypisana do konkretnego użytkownika,
- pozostająca pod stałą kontrolą,
- rejestrowana w trakcie całej sesji,
- analizowana pod kątem zagrożeń,
- audytowana w sposób odporny na manipulację.

Jak to wygląda w praktyce

Tradycyjny model dostępu uprzywilejowanego opiera się głównie na zaufaniu do administratorów oraz na poświadczeniach rozproszonych po całej infrastrukturze.

W praktyce prowadzi to do kilku istotnych problemów:

- brak pełnej kontroli nad tym, kto, kiedy i w jakim celu logował się do systemów krytycznych,
- brak nagrań sesji potrzebnych do analizy incydentów,
- przechowywanie haseł i kluczy w prywatnych menedżerach lub lokalnych plikach,
- trudność w szybkim odebraniu dostępu odchodzącemu pracownikowi lub zewnętrznemu wykonawcy,
- brak jednego, spójnego mechanizmu audytu i kontroli działań administracyjnych.

Co zmienia SafeConnect

SafeConnect wprowadza jeden, spójny model dostępu uprzywilejowanego oparty na centralnym punkcie kontroli i pełnej widoczności działań użytkowników.

- dostęp realizowany przez jeden portal zamiast bezpośrednich połączeń,
- brak ujawniania haseł i kluczy użytkownikom,
- każda sesja przypisana do konkretnej osoby i w pełni identyfikowalna,
- pełne nagranie i rejestracja działań dostępne do odtworzenia,
- możliwość natychmiastowego odebrania dostępu i zakończenia sesji,
- gotowy materiał dowodowy do audytu i wsparcie dla wymagań regulacyjnych.

Fundamenty działania SafeConnect

Eliminacja ryzyka wycieku poświadczeń
Poświadczenia są przechowywane w zaszyfrowanej bazie i nigdy nie są ujawniane użytkownikowi. System automatycznie wstrzykuje dane logowania w momencie zestawiania sesji.

Egzekwowanie zasad dostępu
Dostęp nie oznacza swobody działania. Każda sesja podlega politykom bezpieczeństwa i może zostać przerwana w dowolnym momencie.

Gotowość audytowa
Każda operacja jest przypisana do konkretnej osoby. Sesje są nagrywane i dostępne do odtworzenia bez dodatkowych narzędzi.

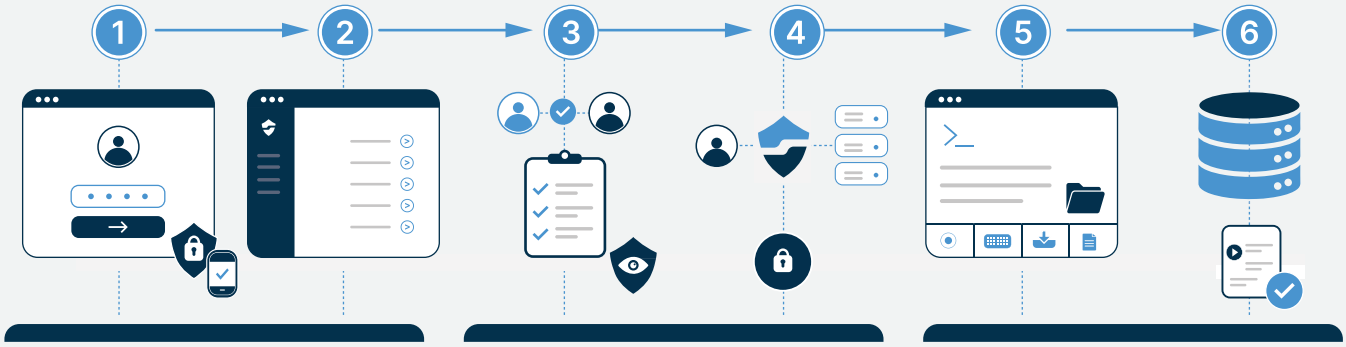
Lokalny kontekst wdrożenia
System rozwijany i wspierany w Polsce, z dokumentacją i obsługą dopasowaną do realiów organizacji działających lokalnie.

SafeConnect | Privileged Access Management

Z perspektywy użytkownika **SafeConnect** upraszcza dostęp do infrastruktury.
Z perspektywy organizacji — wprowadza pełną kontrolę nad każdą sesją.
Cały proces odbywa się w jednym środowisku, bez konieczności instalowania dodatkowego oprogramowania na stacjach roboczych czy serwerach.

SafeConnect umożliwia pracę z aplikacjami webowymi i panelami administracyjnymi bez ujawniania danych logowania. System uruchamia izolowane środowisko przeglądarki i automatycznie uzupełnia poświadczenia, także w aplikacjach o niestandardowym uwierzytelnianiu (np. Proxmox, FortiGate, Grafana). Użytkownik pracuje w gotowej, zalogowanej sesji, a poświadczenia pozostają po stronie systemu.

Dostęp może być realizowany również w formie tymczasowych pulpitów graficznych (VDI) uruchamianych na żądanie. Sesja odbywa się w odseparowanym środowisku, bez bezpośredniego dostępu do infrastruktury, co pozwala bezpiecznie realizować zadania administracyjne i dostęp zewnętrzny.



1. Logowanie do systemu
Dostęp realizowany jest przez przeglądarkę z wykorzystaniem uwierzytelniania wieloskładnikowego (2FA). Integracja z *Active Directory* lub LDAP zapewnia spójne zarządzanie tożsamością użytkowników.

2. Wybór systemu docelowego
Po zalogowaniu użytkownik widzi wyłącznie te zasoby, do których ma przypisane uprawnienia.

3. Weryfikacja dostępu
Dla systemów krytycznych wymagane jest dodatkowe zatwierdzenie. Mechanizm czterech oczu wiąże dostęp z konkretną zgodą i uzasadnieniem.

4. Zestawienie sesji przez proxy
Połączenie realizowane jest przez warstwę pośrednią. Użytkownik nie łączy się bezpośrednio z systemem docelowym, a cały ruch przechodzi przez **SafeConnect.**

5. Praca w kontrolowanym środowisku
Sesja jest monitorowana i rejestrowana w czasie rzeczywistym. Wszystkie działania są przypisane do konkretnego użytkownika i podlegają politykom bezpieczeństwa.

6. Zakończenie i zapis sesji
Po zakończeniu pracy pełny przebieg sesji pozostaje zapisany. Nagranie i logi są dostępne do odtworzenia jako materiał dowodowy.

Użytkownicy systemu SafeConnect

Administratorzy infrastruktury
Logowanie przez centralny portal i wybór systemu docelowego bez ujawniania haseł i kluczy dostępowych.

Managerowie i właściciele systemów
Zatwierdzanie dostępu, wgląd w raporty wykorzystania oraz kontrola zgodności działań z politykami organizacji.

Zespoły bezpieczeństwa i audytorzy
Dostęp do dziennika audytu, nagrań sesji i alertów bezpieczeństwa z możliwością analizy działań użytkowników.

Wykonawcy zewnętrzni
Dostęp czasowy do wybranych zasobów realizowany pod pełnym nadzorem i zgodnie z przyjętymi zasadami bezpieczeństwa.

I-BS.PL

Bezpieczeństwo zaprojektowane od podstaw

SafeConnect został zaprojektowany tak, że żaden dostęp nie jest udzielany automatycznie. Każde połączenie wymaga świadomej, udokumentowanej decyzji — w oparciu o uprawnienia, zatwierdzenie lub uzasadnienie biznesowe. Całość działa jako spójne środowisko, które kontroluje zarówno użytkownika, jak i samo połączenie — kto, kiedy, do czego i na jakich zasadach uzyskuje dostęp.

Szyfrowanie nagrań i danych sesji

Nagrania sesji są szyfrowane od momentu ich powstania, jeszcze przed zapisaniem na dysku. Model KEK/DEK sprawia, że dostęp do danych wymaga nie tylko uprawnień systemowych, ale także dostępu do kluczy kryptograficznych.
W praktyce oznacza to, że nawet administrator infrastruktury nie ma możliwości odczytania nagrań bez odpowiedniej autoryzacji.

Integralność audytu

Każdy wpis w logach jest kryptograficznie podpisany kluczem pochodnym z sekretu systemu. Klucz nigdy nie trafia do bazy danych — modyfikacja wpisu wymagałaby jednoczesnego dostępu do bazy i do środowiska uruchomieniowego aplikacji, co jest wykrywane podczas weryfikacji integralności.
Dzięki temu audyt nie opiera się wyłącznie na zaufaniu do administratora systemu, ale na mechanizmach, które pozwalają jednoznacznie potwierdzić autentyczność danych.

Ochrona danych w stanie spoczynku

System w stanie spoczynku pozostaje „zapieczętowany". Po restarcie dostęp do wrażliwych danych — takich jak poświadczenia czy nagrania — jest zablokowany do momentu ich świadomego odblokowania przez administratora.
Ten mechanizm eliminuje ryzyko automatycznego dostępu do danych po uruchomieniu systemu oraz ogranicza skutki potencjalnego przejęcia środowiska.

Kontrolowany transfer plików

Wymiana plików w trakcie sesji odbywa się w kontrolowany sposób, z pełnym zapisem operacji. Każdy transfer jest przypisany do użytkownika i stanowi część materiału audytowego.
To umożliwia jednoznaczną odpowiedź na pytanie: kto, kiedy i jakie dane przesyłał.

Analiza działań w czasie rzeczywistym

SafeConnect analizuje działania użytkownika w trakcie sesji, jeszcze przed ich wykonaniem. Oznacza to, że system może reagować nie tylko na skutki operacji, ale również na ich zamiar.
W przypadku wykrycia ryzykownych komend lub prób operacji na danych wrażliwych możliwe jest natychmiastowe przerwanie sesji lub zablokowanie konkretnego działania.

Kontrola dostępu uprzywilejowanego

Integracja z AD/LDAP
Wykorzystanie istniejącej infrastruktury tożsamości organizacji bez potrzeby tworzenia nowych kont użytkowników.

Precyzyjne zarządzanie dostępem
Użytkownik widzi i obsługuje wyłącznie systemy, do których ma przyznane uprawnienia, zgodnie z zasadą najmniejszych uprawnień.

Silne uwierzytelnianie (2FA)
Dodatkowy składnik logowania zwiększający bezpieczeństwo dostępu uprzywilejowanego i ograniczający ryzyko nieautoryzowanego dostępu.

Natychmiastowa dezaktywacja dostępu
Zmiana statusu użytkownika automatycznie kończy aktywne sesje i blokuje dalszy dostęp do systemów.

SafeConnect vs. podejście własne

Własne rozwiązania oparte na VPN, bastionach i skryptach często wydają się prostsze i tańsze na etapie startu. W praktyce wymagają jednak ciągłego utrzymania, ręcznego nadzoru oraz nie zapewniają spójnego modelu kontroli i audytu. Poniższe zestawienie pokazuje różnice pomiędzy podejściem budowanym wewnętrznie a rozwiązaniem zaprojektowanym jako spójny system zarządzania dostępem uprzywilejowanym.

Kryterium	In-house solution	SafeConnect
Koszt startu	Pozornie niski. W praktyce setki godzin pracy zespołu: projekt, testy, poprawki.	Przewidywalny koszt licencji i wdrożenia. Bez ukrytych nakładów.
Czas uruchomienia	Od kilku tygodni do kilku miesięcy. Iteracyjne poprawianie błędów i konfiguracji.	Gotowość w kilka dni roboczych. Automatyzacja wdrożenia.
Dostęp uprzywilejowany	Rozproszony: VPN, SSH, RDP. Brak jednego punktu kontroli.	Jeden portal. Każda sesja przechodzi przez kontrolowany punkt dostępu.
Poświadczenia	Hasła przechowywane lokalnie lub w menedżerach zespołowych. Ryzyko wycieku.	Poświadczenia zaszyfrowane. Użytkownik nigdy ich nie zna (credential injection).
Nagrywanie sesji	Najczęściej brak lub rozwiązania własne o ograniczonej funkcjonalności.	Wbudowane nagrywanie (SSH, RDP, Web) z odtwarzaniem w przeglądarce.
Szyfrowanie nagrań	Brak lub pliki w postaci jawnej na serwerze.	AES-256-GCM, model KEK/DEK. Brak dostępu nawet dla administratora systemu.
Integralność logów	Możliwość modyfikacji przez administratora (brak mechanizmów kontroli).	Każdy wpis podpisany kryptograficznie (HMAC). Wykrywanie manipulacji.
Integracja z SIEM	Ograniczona lub ręczna integracja	Automatyczne przekazywanie zdarzeń do systemów SIEM (centralny monitoring)
Workflow 4-oczu	Proces ręczny (e-mail, Slack, ticket). Trudny do udokumentowania.	Wbudowany mechanizm zatwierdzania, powiązany z konkretną sesją.
Kontrola w trakcie sesji	Analiza po fakcie (jeśli logi istnieją).	Reakcja w czasie rzeczywistym (DLP, możliwość przerwania sesji).
Raporty compliance	Ręczne zbieranie danych i mapowanie pod audyt. Czasochłonne.	Raport PDF jednym kliknięciem.
Odebranie dostępu	Wieloetapowe: VPN, konta, rotacja haseł. Ryzyko pominięcia elementu.	Jedno działanie – natychmiastowe zakończenie wszystkich sesji i dostępów.
Koszt utrzymania	Wysoki i trudny do przewidzenia. Aktualizacje, poprawki, ryzyko błędów.	Stały koszt wsparcia i aktualizacji producenta.

Poznaj pozostałe rozwiązania z rodziny Safe

SafeDR

Backup i odtworzenie środowiska w jednym systemie.
www.i-bs.pl/safedr

SafeGuard

Kontrola dostępu do sieci i komunikacji między zasobami.
www.i-bs.pl/safeguard

I-BS.PL

www.i-bs.pl/safeconnect

Chcesz dowiedzieć się więcej o rozwiązaniu?
Skontaktuj się z nami — odpowiemy na pytania i przedstawimy szczegóły oferty.

Joanna Stępień
tel.: 788 679 946
j.stepien@i-bs.pl

Bartłomiej Skoczylas
tel.: 728 403 586
b.skoczylas@i-bs.pl