STRAŻNIK+

Centrum zabezpieczeń, organizacji i kontroli dostępów sieci

Strażnik+ to rozwiązanie, które porządkuje całą komunikację w sieci i pozwala kontrolować każdy dostęp — od użytkowników i urządzeń, przez oddziały, aż po połączenia zdalne. Łączy funkcje IPAM, NAC, obsługę VPN oraz mechanizmy wykrywania zagrożeń, blokując nieautoryzowane podłączenia i chroniąc infrastrukturę.

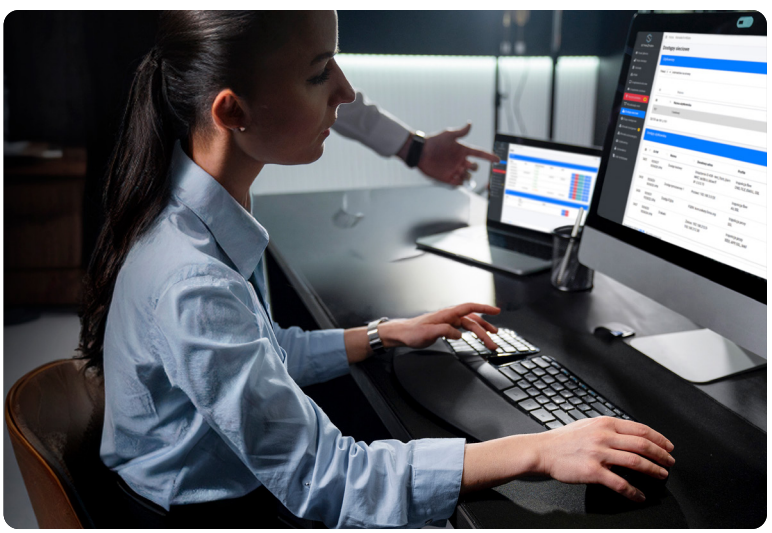
Wszystkie działania administratorów odbywają się z poziomu wygodnego interfejsu webowego, dzięki czemu zarządzanie uprawnieniami, adresacją i konfiguracją sieci staje się prostsze, przejrzyste i w pełni pod kontrolą.

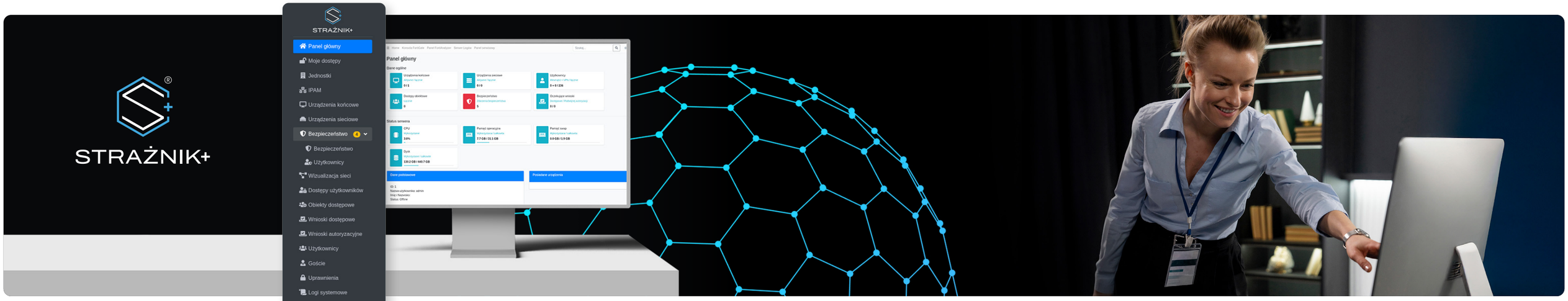
Najważniejsze korzyści dla organizacji:

- jedno centrum zarządzania dostępem i siecią — konfiguracja ustawień i reguł oraz organizacja zasobów odbywa w jednym miejscu, co ułatwia kontrolę i eliminuje chaos wynikający z korzystania z wielu narzędzi,
- mniej incydentów i większa pewność działania — klarowna logika dostępów ogranicza ryzyko pomyłek i nieprzewidzianych przerw w pracy,
- łatwiejsze utrzymanie rozproszonych jednostek — wszystkie oddziały działają według tych samych zasad, co eliminuje lokalne różnice i oszczędza czas,
- szybsze wdrożenia i zmiany w infrastrukturze — administratorzy natychmiast widzą, które elementy wymagają reakcji i mogą działać bez zbędnej zwłoki,
- lepsza organizacja pracy administratorów — uporządkowane procesy i czytelne widoki sprawiają, że codzienne zadania są krótsze i mniej obciążające,
- szybkie decyzje dzięki pełnemu wglądowi w sieć — dostęp do aktualnych informacji ułatwia ocenę sytuacji i planowanie dalszych działań,
- stała gotowość na audyty i kontrole — przejrzystość konfiguracji i historii działań oraz możliwość generowania raportów ułatwia spełnienie wymogów bezpieczeństwa i dokumentacyjnych.

Korzyści biznesowe:

- niższe koszty utrzymania — jedno centrum zarządzania zastępuje kilka narzędzi i ogranicza liczbę ręcznych działań,
- oszczędność czasu pracowników — automatyczna migracja, klonowanie dostępów i weryfikacja konfiguracji redukują ilość powtarzalnych operacji,
- mniejsze ryzyko błędnych decyzji i kosztownych przestojów — Strażnik+ wychwytuje nieprawidłowości jeszcze przed wdrożeniem zmian,
- szybsze wdrażanie nowych osób i reorganizacji — gotowe zestawy dostępów i jedno miejsce zarządzania upraszczają onboarding i zmiany strukturalne,
- lepsze wykorzystanie zasobów IT — zespół może skupić się na zadaniach rozwojowych zamiast na wielogodzinnej konfiguracji,
- płynne skalowanie organizacji — spójne zasady dostępu działają tak samo w małych jednostkach, jak i w złożonych środowiskach,
- przewidywalne koszty — ciągłe aktualizacje i wsparcie dostarczane w ramach jednego rozwiązania upraszczają planowanie budżetu.





Funkcjonalności

Dostępy indywidualne i grupowe
Dostępy mogą być nadawane użytkownikom indywidualnie lub grupowo, zarówno do zasobów wewnętrznych, jak i wybranych adresów URL. Istnieje także możliwość definiowania dostępów wykluczających, które blokują ruch w przypadku ataku lub ograniczają go do wskazanych zasobów.

Kontrola dostępów sieciowych
Strażnik+ pozwala przypisywać użytkownikom dostępy do wybranych fragmentów sieci indywidualnie lub grupowo. Dostępy są powiązane z konkretnym pracownikiem, a nie ze stanowiskiem, dzięki czemu niezależnie od miejsca logowania zawsze zostanie mu przydzielony odpowiedni zestaw uprawnień.

Zarządzanie dostępami
Dostępy do sieci mogą być nadawane per-użytkownik i per-grupa, co upraszcza zarządzanie uprawnieniami przy średniej i dużej liczbie pracowników. System pozwala także tworzyć dostępy harmonogramowe oraz tymczasowe, które wygasają automatycznie po upływie określonego przez administratora czasu.

Wnioski dostępowe
Użytkownicy mogą składać wnioski o nadanie dostępu do wybranych zasobów sieciowych. Wnioski są widoczne w interfejsie webowym i równocześnie wysyłane na adres e-mail administratorów, co przyspiesza ich obsługę i zmniejsza ryzyko pominięcia zgłoszenia.

Uwierzytelnianie dwuskładnikowe (2FA)
Uwierzytelnianie dwuskładnikowe (2FA) chroni konta pracowników przed włamaniem, nawet jeśli ich hasło zostanie przechwycone. Podczas logowania użytkownik podaje nazwę konta, hasło oraz 6-cyfrowy kod z aplikacji lub tokena, a system dodatkowo wspiera klucze bezpieczeństwa FIDO2, zapewniając najwyższy poziom ochrony.

Zarządzanie gośćmi
System ułatwia prowadzenie spisu gości oraz nadawanie im ograniczonych czasowo dostępów sieciowych, a uprawniony pracownik może generować dane logowania, którymi gość potwierdza swoją obecność w systemie. Dostępny jest również tryb samorejestracji, a dane gości mogą zostać zanonimizowane lub wymazane zgodnie z RODO.

Połączenia VPN do pracy zdalnej
Wszystkie dostępy nadane w systemie mogą być automatycznie tworzone również dla połączeń SSL-VPN. Dzięki temu pracownik korzystający z VPN otrzymuje dostęp do tych samych zasobów sieci wewnętrznej co w jednostce, bez dodatkowej konfiguracji i z zachowaniem najwyższych standardów bezpieczeństwa.

Moduł IPAM
Moduł IPAM z kaskadowym wyświetlaniem struktury sieci i VLAN umożliwia bieżącą kontrolę oraz porządkowanie adresacji urządzeń. Jest szczególnie przydatny przy złożonych hierarchiach, takich jak sieci obejmujące wiele oddziałów i różne grupy urządzeń.

Centralizacja adresacji i dostępów
Adresacja urządzeń w oddziałach i centrali jest nadawana automatycznie poprzez interfejs webowy, dzięki czemu nie ma potrzeby ręcznego tworzenia rezerwacji IP. Izolacja jednostek uniemożliwia dostęp do kluczowych zasobów w centrali w razie przejęcia urządzenia w oddziale, a zapasowa konfiguracja pozwala uwierzytelnionym wcześniej użytkownikom kontynuować pracę lokalnie, nawet przy braku połączenia z serwerem Strażnik+.

Wizualizacja sieci
Moduł przedstawia fizyczną strukturę sieci w formie graficznej, zapewniając przejrzysty podgląd wszystkich urządzeń. Każdy element jest interaktywny i pozwala przejść bezpośrednio do szczegółów wybranego urządzenia.

Wieloetapowe wprowadzanie zmian i hierarchia uprawnień
Zmiany wprowadzane przez administratorów mogą wymagać określonej liczby podpisów oraz odpowiedniej rangi na 10-stopniowej skali uprawnień osób zatwierdzających. Istnieje także możliwość oznaczenia zmian, które wymagają zgody superadministratora, co zapewnia dodatkową kontrolę nad kluczowymi operacjami.

Współpracuje ze switchami zarządzalnymi oraz urządzeniami FortiGate, wspierając aktualne wersje ich systemu (FortiOS).

NOWOŚCI

Rozszerzona identyfikacja urządzeń po MAC
System wykorzystuje inteligentne rozpoznawanie producentów urządzeń na podstawie adresów MAC i prezentuje te informacje zarówno na liście adresów, jak i w widoku szczegółowym. Dzięki temu administratorzy szybciej identyfikują typ podłączonego sprzętu, co ułatwia analizę środowiska, wykrywanie nieautoryzowanych urządzeń i utrzymanie porządku w sieci.

Automatyczna migracja profilu użytkownika
Funkcja automatycznej migracji pozwala przenosić wszystkie uprawnienia i powiązania użytkownika do nowego konta, np. po zmianie nazwiska lub aktualizacji danych w LDAP. System odtwarza dostępy, grupy, obiekty dostępu i urządzenia oraz przywraca odpowiednie elementy na FortiGate, dzięki czemu administrator nie musi ręcznie rekonstruować konfiguracji.

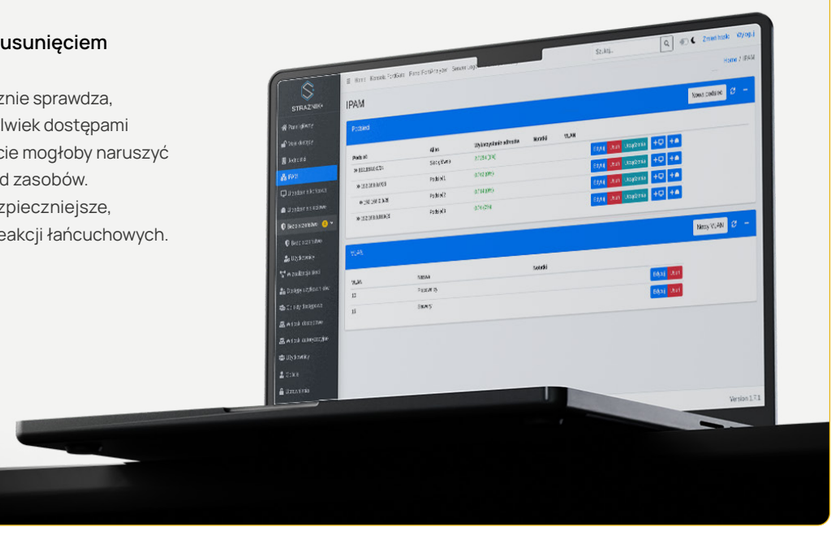
Szybkie klonowanie dostępów użytkowników
Funkcja szybkiego klonowania umożliwia tworzenie zestawu dostępów dla nowego użytkownika na podstawie istniejącego konta, odtwarzając konfigurację 1:1 — zarówno członkostwo w obiektach dostępowych, jak i uprawnienia indywidualne. Administrator może skopiować cały zestaw dostępów lub wybrane elementy, co znacząco przyspiesza onboarding i eliminuje ryzyko błędów przy ręcznym odtwarzaniu konfiguracji.

Inteligentne zabezpieczenie przed usunięciem powiązanych urządzeń
Mechanizm zabezpieczający automatycznie sprawdza, czy urządzenie jest powiązane z jakimikolwiek dostępami i wyświetla ostrzeżenie, gdy jego usunięcie mogłoby naruszyć konfigurację lub odciąć użytkowników od zasobów. Dzięki temu operacje porządkowe są bezpieczniejsze, bardziej przewidywalne i nie powodują reakcji łańcuchowych.

Zaawansowana weryfikacja dostępów z kontrolą FQDN
Mechanizm weryfikacji dostępów sprawdza poprawność rozwiązywania FQDN przez FortiGate, analizując konfigurację podczas tworzenia lub edycji dostępu i potwierdzając prawidłową interpretację adresów wykorzystywanych w politykach. Dzięki temu błędy są wychwytywane przed wdrożeniem, co zwiększa bezpieczeństwo i eliminuje problemy wynikające z nieprawidłowego DNS-u lub błędnych wpisów.

Globalne wyszukiwanie obiektów
Funkcja globalnego wyszukiwania obejmuje urządzenia, użytkowników, dostępy i inne obiekty, prezentując wyniki w przejrzystym widoku z podziałem na typy. Mechanizm rozpoznaje, czy podawany jest tekst, FQDN, adres IP lub podsieć, zwracając odpowiednie obiekty i ułatwiając szybkie poruszanie się po całym systemie.

Inteligentne wyszukiwanie w grupach dostępowych
Funkcja pozwala wyszukiwać grupy dostępowe na podstawie obiektów, które zawierają, dzięki czemu można szybko znaleźć grupy obejmujące konkretną podsieć, adres IP lub inny zasób. Dostępne jest również wyszukiwanie po użytkownikach, co ułatwia sprawdzenie, w jakich grupach znajduje się dana osoba i jakie uprawnienia z tego wynikają.



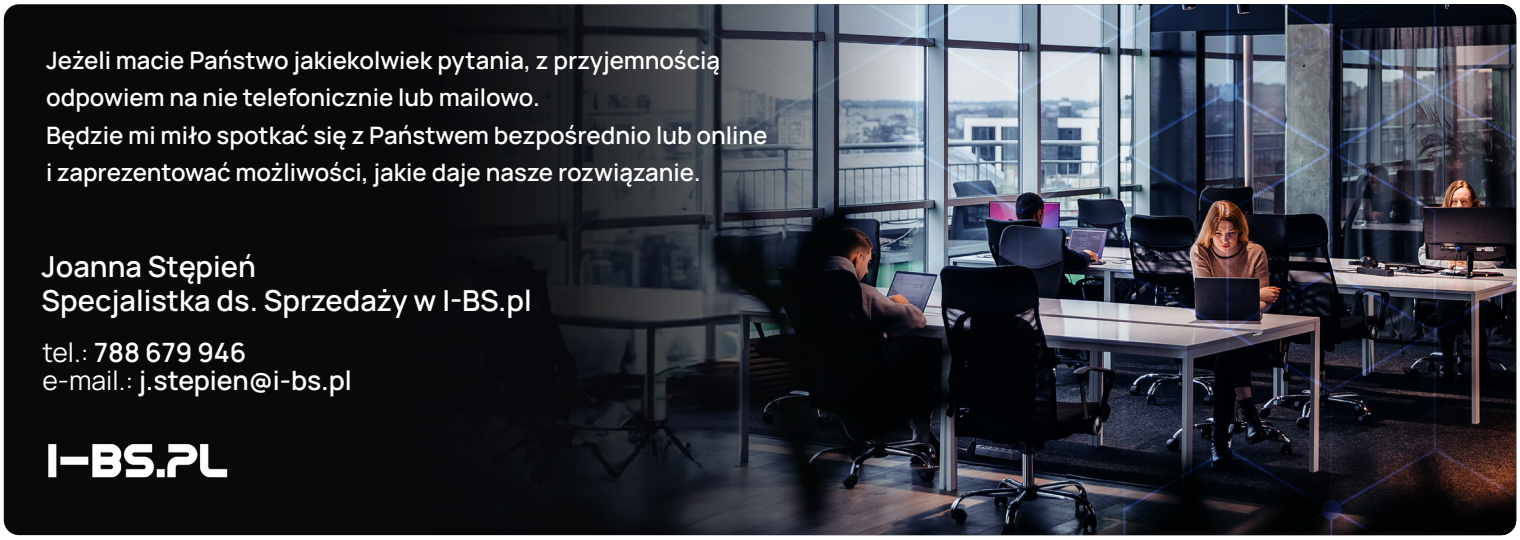
Stały rozwój i pewne wsparcie

Pełna kontrola nad procesem tworzenia **Strażnik+** pozwala szybko reagować na potrzeby użytkowników i dostarczać aktualizacje zgodne z obowiązującymi standardami bezpieczeństwa.

Zapewniamy wsparcie techniczne i regularne aktualizacje, aby **Strażnik+** pozostawał rozwiązaniem, na którym można polegać na co dzień.

Strażnik+ to w 100% polskie rozwiązanie, rozwijane z myślą o organizacjach pracujących w złożonych i rozproszonych środowiskach sieciowych.

Nasz zespół na bieżąco udoskonala system, dodając kolejne możliwości, które przekładają się na wygodę pracy administratorów i stabilność działania sieci.



Jeżeli macie Państwo jakiekolwiek pytania, z przyjemnością odpowiem na nie telefonicznie lub mailowo.
Będzie mi miło spotkać się z Państwem bezpośrednio lub online i zaprezentować możliwości, jakie daje nasze rozwiązanie.

Joanna Stępień
Specjalistka ds. Sprzedaży w I-BS.pl

tel.: 788 679 946
e-mail.: j.stepien@i-bs.pl

I-BS.PL