STRAŻNIK+

Od narzędzia administracyjnego do centrum zabezpieczeń, organizacji i kontroli dostępu do sieci.

Do tej pory **Strażnik+** pozwalał organizować codzienną pracę administratorów i zapewniał ochronę najważniejszych elementów sieci: adresów IP, dostępów do usług czy urządzeń. IPAM, NAC, 2FA, wizualizacja sieci, obsługa gości czy centralizacja ustawień tworzyły zestaw usług, dzięki którym wiele organizacji porządkowało swoje środowisko i odzyskiwało nad nim kontrolę.

Teraz Strażnik+ z narzędzia skupiającego uwagę na porządkowaniu podstawowych elementów infrastruktury staje się **centralnym środowiskiem zarządzania**, które potrafi samodzielnie oceniać stan sieci, wykrywać anomalie i wspierać administratorów w tych domenach, które wcześniej wymagały żmudnej, ręcznej pracy. To kolejny krok, w którym **Strażnik+** nie tylko zbiera informacje, ale również wykorzystuje je do porządkowania konfiguracji i umożliwienia szybszej reakcji na zmiany.

Rezultatem jest bardziej świadome działanie samego systemu – **Strażnik+** przewiduje, czuwa i działa w sposób dużo bardziej uporządkowany. Ten kierunek rozwoju jest najbardziej widoczny, gdy patrzymy na trzy obszary, w których nowość jest najłatwiej dostrzegalna: operacyjny, bezpieczeństwa i organizacyjny.

Obszar operacyjny

Najważniejsze zmiany to:

- automatyczna migracja profilu użytkownika – coś, co w wielu środowiskach zajmuje wiele godzin i wymaga dużej uwagi, tutaj dzieje się automatycznie i bez ryzyka, że jakiś element zostanie pominięty;
- globalne wyszukiwanie obiektów, konfiguracja ustawień i reguł oraz organizacja zasobów odbywa się w jednym miejscu, co ułatwia kontrolę i eliminuje chaos wynikający z korzystania z wielu narzędzi,
- szybkie klonowanie dostępów sprawia, że przyjęcie do zespołu nowej osoby przestaje być procesem odtwarzanym ręcznie, ponieważ system przygotowuje odpowiedni zestaw uprawnień na podstawie już istniejącej roli;
- inteligentne wyszukiwanie w grupach dostępowych, które jest szczególnie pomocne w organizacjach z wieloma oddziałami, gdzie zależności między nimi nie są oczywiste.

Co równie istotne – narzędzia, które są przydatne w codziennej pracy i standardowo występują oddzielnie, **Strażnik+** łączy w jedną, kompletną całość i uzupełnia o funkcjonalności, które dotychczas w wielu organizacjach nie były dostępne.

Obszar bezpieczeństwa

To obszar, w którym różnica jest bardzo wyraźna. W poprzedniej wersji systemu najważniejsze funkcje bezpieczeństwa opierały się w dużej mierze na kontroli dostępu i rozsądnej konfiguracji.
W nowej — Strażnik+ sam weryfikuje, ocenia i blokuje to, co mogłoby zaszkodzić sieci.

Najmocniejsze elementy tego obszaru to:

- **zaawansowana weryfikacja FQDN,**
- **ochrona przed usunięciem powiązanych obiektów,**
- **dostępy wykluczające i natychmiastowe „cięcie ruchu”.**

Strażnik+ kontroluje urządzenia FortiGate pod kątem poprawności adresacji i wykrywa każde odstępstwo. Zła konfiguracja DNS to jedna z częstszych przyczyn problemów — system wyłapuje ją zanim zacznie wpływać na pracę sieci. Dodatkowo system zabezpiecza przed sytuacją, w której administrator nieświadomie wycina element blokujący wiele urządzeń. W tym przypadku **Strażnik+** pełni funkcję kontrolną, a mechanizmy, które dotąd były obecne raczej w wyspecjalizowanych produktach bezpieczeństwa stosuje je tam, gdzie pojawia się podejrzenie nadużycia lub ataku.

Strażnik+ działa proaktywnie dbając o spójność konfiguracji, sprawdzając zależności i natychmiastowo reagując na zagrożenia. To jakościowa zmiana, która wyróżnia rozwiązanie od **I-BS.pl** na tle rozwiązań od innych producentów.

Obszar organizacyjny

Nowy **Strażnik+** to nie tylko zmiana technologiczna. Nowe funkcje wpisują system w procedury zarządzania, kontrolę zgodności i pełną ścieżkę audytu, które są fundamentem pracy organizacji działających w reżimie regulacyjnym.

Najważniejsze zadania, które **Strażnik+** realizuje w tym obszarze

- **Wieloetapowe wprowadzanie zmian z rangami uprawnień** – funkcjonalność, bliższa systemom do zarządzania zmianami w dużych przedsiębiorstwach, pozwala zdefiniować role, wymagać akceptacji i chronić przed nieświadomymi zmianami.
- **Wnioski dostępowe z pełną ścieżką przepływu** – system pozwala na generowanie zunifikowanej procedury z dokumentacją każdego kroku w procesie nadawania uprawnień.
- **2FA, FIDO2 i obsługa gości z samorejestracją** – funkcjonalności przyjazne użytkownikom, ale zgodne z normami i audytowymi wymogami.

W nowej wersji **Strażnik+** staje się narzędziem, które nie tylko chroni sieć, ale wspiera ład organizacyjny, upraszcza raportowanie i zmniejsza liczbę zagrożeń.

Co wyróżnia **Strażnik+** na tle innych rozwiązań?

Strażnik+ to rozwiązanie wychodzące poza obszar typowego narzędzia administracyjnego. Z rozwiązania skupionego na porządkowaniu infrastruktury staje się **centrum kontrolowania dostępu** – środowiskiem, które samo weryfikuje stan sieci, wykrywa anomalie oraz automatyzuje zadania, które do tej pory wymagały wielu godzin pracy administratorów.

STRAŻNIK+

Na rynku jest niewiele rozwiązań, które łączą w jednym systemie takie obszary, jak: NAC, IPAM, VPN, kontrola konfiguracji, obsługa procesowa dostępów oraz integracja z FortiGate i urządzeniami sieciowymi. Dzięki temu **Strażnik+** staje się narzędziem, które pozwala patrzeć na dostęp w sposób globalny — od użytkownika i jego uprawnień, przez urządzenie, aż po proces zmian dbający o spójność i bezpieczeństwo konfiguracji. System nie tylko wspiera administratorów, ale przejmuje od nich część odpowiedzialności za utrzymanie środowiska w stabilnej i bezpiecznej kondycji.

Joanna Stępień
Specjalistka ds. Sprzedaży w I-BS.pl
tel.: **788 679 946**
e-mail.: **j.stepien@i-bs.pl**

I-BS.PL