ZYXEL
NETWORKS

Bezpieczeństwo sieci bez komplikacji



Wrzesień 2026

Uproszczenie bezpieczeństwa

Każda mała firma zasługuje na bezpieczeństwo sieci, któremu łatwo zaufać i którym jeszcze łatwiej zarządzać. To właśnie ta idea stoi za wszystkim, co robi Zyxel Networks – i dokładnie to wprowadzamy do świata cyberbezpieczeństwa.

łatwiej zarządzać. To właśnie ta idea stoi za wszystkim, co robi Zyxel Networks – i dokładnie to wprowadzamy do świata cyberbezpieczeństwa. Zbudowaliśmy naszą reputację, czyniąc technologie sieciowe dostępnymi dla MŚP, i stosujemy to samo podejście, aby zapewnić im bezpieczeństwo. Choć jesteśmy najlepiej znani jako twórca przełączników i sprzętu WiFi, mamy również długą historię i solidne doświadczenie w dziedzinie cyberbezpieczeństwa, wspierane przez własną globalną sieć współpracy w obszarze bezpieczeństwa oraz wieloletnie relacje z czołowymi dostawcami rozwiązań zabezpieczających.

W tym dokumencie wyjaśniamy, co robimy, aby uprościć bezpieczeństwo, dlaczego nasze podejście i propozycja wartości wyróżniają się na tle konkurencji oraz dlaczego ma to znaczenie dla instalatorów, integratorów i dostawców usług MSP obsługujących rynek małych firm.



Krajobraz zagrożeń ewoluował, więc stworzyliśmy ochronę, która nadąża za zmianami

Bezpieczeństwo cyfrowe zmieniło się znacząco od pierwszych dni internetu, gdy głównym zaleceniem było po prostu wybranie silnego hasła.

W ciągu ostatnich 40 lat wachlarz zagrożeń, o których muszą myśleć firmy, znacznie się poszerzył – od prób nieautoryzowanego dostępu i złośliwego oprogramowania po bardziej zwodnicze taktyki, takie jak phishing i ransomware.

W miarę jak zagrożenia się zróżnicowały, rosła również potrzebna ochrona przed nimi, a cyberbezpieczeństwo rozwinęło się w znaczącą, wyspecjalizowaną branżę.

Ten wzrost złożoności jest realny. Nie musi to jednak być ciężar, który małe firmy muszą dźwigać same.

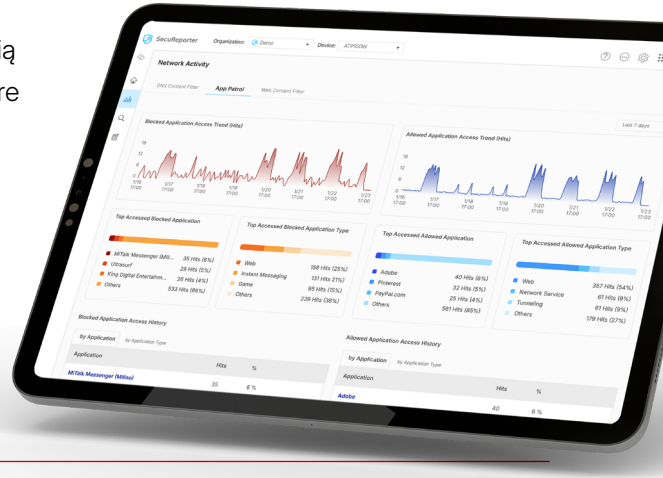
Połączona ochrona bez komplikacji

Uważamy, że odpowiedzią na coraz bardziej złożony krajobraz zagrożeń nie jest większa złożoność dla klienta – lecz inteligentna konsolidacja.

Łącząc ochronę przed pełnym zakresem zagrożeń w jednym rozwiązaniu, możemy zapewnić klientom końcowym odpowiedni poziom ochrony, który znacząco ogranicza ryzyko, bez konieczności stawania się ekspertami w dziedzinie bezpieczeństwa.

Dokładnie to zrobiliśmy z naszą serią zapór sieciowych USG FLEX H, które są wyposażone we wbudowaną ochronę opracowaną wspólnie z czołowymi, wyspecjalizowanymi dostawcami zabezpieczeń.

W połączeniu z naszym pulpitem i narzędziami raportowania SecuReporter oraz naszą bezpieczną platformą zarządzania w chmurze Nebula, oferujemy kompleksową usługę, która zapewnia MŚP, osobom prowadzącym jednoosobową działalność gospodarczą, a nawet pracownikom zdalnym ochronę, jakiej potrzebują, w przystępnej cenie – wraz z przejrzystym sposobem na wykazanie, że ochrona działa, oraz możliwością konfigurowania i zarządzania bezpieczeństwem zdalnie.



Ułatwiamy małym firmom dostęp do cyberbezpieczeństwa

Oprócz tego, że cyberbezpieczeństwo wydaje się złożone, wiele MŚP po prostu nie ma czasu na zbadanie, czego potrzebuje, a mniejsze firmy często nie dysponują dedykowanym personelem IT ani wewnętrzną wiedzą specjalistyczną w zakresie bezpieczeństwa cyfrowego. Znalezienie i zatrzymanie pracowników z odpowiednimi umiejętnościami może być również wyzwaniem.

Budżet jest również realnym czynnikiem – koszt sprzętu i odnowień licencji ma znaczenie dla firm o ograniczonych zasobach.

Właśnie dlatego skupiliśmy się na tym, aby nasze rozwiązania były przystępne cenowo i łatwe do uzasadnienia biznesowego, tak aby brak wewnętrznej wiedzy specjalistycznej lub ograniczony budżet nie musiały oznaczać, że firma pozostanie bez ochrony.



Dlaczego ochrona ma znaczenie

Gdy małe firmy podejmują odpowiednie środki ostrożności, znacząco zmniejszają ryzyko, że padną ofiarą cyberataku. Według 2026 SMB Cyber Readiness Index firmy ESET 64% ankietowanych organizacji w regionie EMEA spodziewa się cyberataku w ciągu najbliższego roku, a 44% doświadczyło incydentu związanego z cyberbezpieczeństwem w ciągu ostatnich 12 miesięcy. Dane te pokazują, że ataki są realnym zagrożeniem dla firm każdej wielkości i że przygotowanie się opłaca.

Odpowiedni poziom ochrony powinien odpowiadać potrzebom firmy i poziomowi jej ryzyka. Firma przetwarzająca osobiste dane finansowe prawdopodobnie posiada bardziej wrażliwe informacje niż na przykład kawiarnia czy salon fryzjerski – ale każda firma przechowuje dane warte ochrony, od danych bankowych po dane osobowe klientów i pracowników.

44% **organizacji w regionie EMEA doświadczyło incydentu związanego z cyberbezpieczeństwem w ciągu ostatnich 12 miesięcy**



Co muszą chronić MŚP

Dobrym punktem wyjścia jest zabezpieczenie styku sieci firmowej z internetem, w którym działa zapora sieciowa. Oprócz zabezpieczenia tego kluczowego punktu, wszystkie podłączone urządzenia powinny mieć jakąś formę ochrony i być na bieżąco aktualizowane. Najlepiej, aby aktywność sieciowa była również rejestrowana i regularnie przeglądana, a firmy odnoszą korzyści z posiadania polityki bezpieczeństwa, dzięki której pracownicy wiedzą, jak rozpoznawać i obsługiwać podejrzane wiadomości e-mail i linki.

Te kroki nie tylko zmniejszają ryzyko. Dają firmie solidną, praktyczną podstawę do zapewnienia bezpieczeństwa swoich systemów i danych.

Większość firm nadal będzie chciała mieć partnera, który przejmie codzienną pracę związaną z aktualizowaniem licencji i oprogramowania układowego oraz monitorowaniem i przeglądem bezpieczeństwa – i właśnie tutaj z pomocą przychodzą instalatorzy, integratorzy i dostawcy usług MSP.

Realna szansa dla specjalistów IT i instalatorów rozwiązań technicznych

Wiele MŚP samodzielnie konfiguruje swoje laptopy, komputery PC i podstawowe sieci WiFi lub zwraca się do lokalnego specjalisty IT. W przypadku monitoringu wizyjnego (CCTV), ochrony fizycznej, czujników pożarowych i inteligentnych technologii, takich jak systemy kontroli dostępu do drzwi, zazwyczaj polegają na wyspecjalizowanych instalatorach.

Dla tych małych, lokalnych firm konsultingowych IT i instalatorskich cyberbezpieczeństwo stanowi prawdziwą szansę – gotowe do uruchomienia źródło przychodów.

Zrozumiałe jest, że w przeszłości złożoność rozwiązań zniechęca niektórych partnerów, ponieważ nikt nie chce narażać na szwank cennej relacji z klientem. Nasze proste podejście do bezpieczeństwa usuwa tę barierę.

Dzięki serii USG FLEX H instalatorzy mogą zapewnić klientom całą potrzebną ochronę w jednym urządzeniu. Pięcioetapowy proces konfiguracji przed dostawą ułatwia konfigurację i instalację, a ustawienia domyślne są zaprojektowane tak, aby odpowiadały większości małych firm bez modyfikacji.

Proste wdrożenie, które naprawdę robi różnicę

Ta możliwość wdrożenia to prawdziwy wyróżnik – oszczędza wszystkim znaczną ilość czasu, wysiłku i kosztów. Klienci nie muszą czekać na wizytę inżyniera w celu przeprowadzenia instalacji technicznej; wystarczy podłączyć zaporę sieciową, a ona konfiguruje się samodzielnie.

Partnerzy nie muszą stawać się specjalistami, aby oferować to rozwiązanie, choć jeśli chcą, partner IT lub instalator może z łatwością skorzystać z naszej bezpiecznej platformy chmurowej Nebula, aby monitorować urządzenia klientów i wprowadzać zmiany zdalnie.

Po zainstalowaniu – i przy regularnej aktualizacji licencji bezpieczeństwa oraz oprogramowania układowego – zapora sieciowa nadal zapewnia kompleksową ochronę, wymagają niewielkiej dalszej ingerencji lub nie wymagając jej wcale.

W rzadkich przypadkach, gdy potrzebna jest pomoc, zespół Zyxel Networks służy spersonalizowanym wsparciem i doradztwem.



Seria zapór sieciowych USG FLEX H: kluczowe funkcje i korzyści

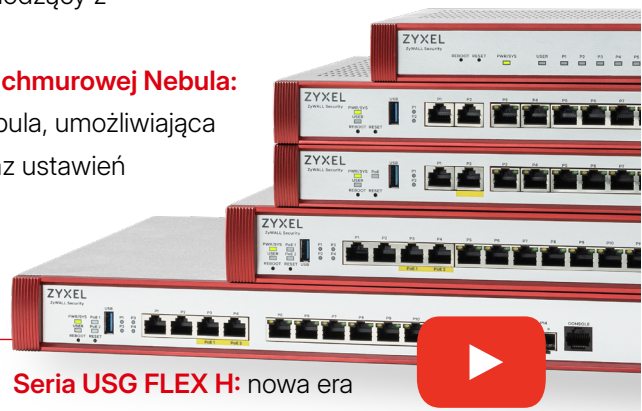
Seria Zyxel USG FLEX H została zaprojektowana z myślą o potrzebach małych firm o różnych rozmiarach i możliwościach budżetowych. Każdy model jest standardowo wyposażony w pełny zestaw funkcji bezpieczeństwa – nawet najmniejsza, najbardziej przystępna cenowo opcja zapewnia pełną ochronę. Główna różnica między modelami dotyczy szybkości i przepustowości, przy czym opcje wyższej klasy są przeznaczone dla firm o większej liczbie użytkowników i wyższych wymaganiach dotyczących przepustowości.

Co obejmuje rozwiązanie

Wszystkie te funkcje i możliwości są standardowo dostępne w każdym modelu serii USG FLEX H:

- **Wykrywanie zagrożeń oparte na AI:** analizuje globalne informacje o zagrożeniach w czasie rzeczywistym, aby wykrywać ewoluujące i coraz bardziej zaawansowane cyberataki oraz na nie reagować
- **Izolowanie plików w piaskownicy chmurowej (cloud sandboxing):** izoluje nieznane lub podejrzane pliki w bezpiecznym środowisku i analizuje ich zachowanie, zanim zostaną dopuszczone
- **System zapobiegania włamaniom (IPS):** skanuje ruch sieciowy w celu wykrywania i blokowania złośliwych elementów ruchu sieciowego, prób wykorzystania luk w zabezpieczeniach oraz prób uzyskania nieautoryzowanego dostępu
- **Filtrowanie treści internetowych:** filtruje i blokuje dostęp do złośliwych lub niewłaściwych stron internetowych
- **Kontrola aplikacji:** identyfikuje, klasyfikuje i kontroluje konkretne aplikacje, aby nadać priorytet ważnemu ruchowi i zablokować niezatwierdzone aplikacje
- **Wspólne wykrywanie i reagowanie (CDR):** łączy się z innymi urządzeniami sieciowymi, aby automatycznie poddawać kwarantannie lub blokować zainfekowane urządzenia na brzegu sieci
- **Rozbudowana obsługa VPN:** zarówno sieci VPN IPSec do połączeń punkt-punkt, jak i sieci VPN SSL do dostępu zdalnego
- **Samoochrona i reputacja IP:** chroni samo urządzenie zapory sieciowej, automatycznie wyłączając podatne na ataki porty, gdy nie są używane. Wykorzystuje również zewnętrzne listy blokowanych adresów i źródeł oraz filtrowanie na podstawie reputacji adresów IP, aby zatrzymać potencjalnie złośliwy ruch pochodzący z nieautoryzowanych źródeł
- **Bezpieczne zarządzanie za pomocą platformy chmurowej Nebula:** w zestawie znajduje się podstawowa licencja Nebula, umożliwiająca zdalną konfigurację i monitorowanie urządzeń oraz ustawień

Kliknij tutaj, aby uzyskać więcej informacji.



Seria USG FLEX H: nowa era w cyberbezpieczeństwie.

Pokazujemy skuteczność ochrony

To naturalne, że chce się widzieć wartość inwestycji, zwłaszcza jeśli firma nigdy wcześniej nie doświadczyła naruszenia bezpieczeństwa ani ataku.

Nasz oparty na chmurze pulpit analityki bezpieczeństwa, SecuRe porter, pozwala łatwo zobaczyć skuteczność ochrony serii USG FLEX H.

SecuReporter zapewnia czytelne wykresy i zestawienia przedstawiające aktywność w sieci, w tym potencjalnie złośliwą aktywność wykrytą w sieci. To prosty i elegancki sposób na wykazanie wartości wdrożonej ochrony.

Korzystając z SecuReporter, firmy mogą zobaczyć całą aktywność sieciową, w tym pliki oznaczone i umieszczone w piaskownicy w chmurze oraz zablokowane wirusy lub potencjalne próby ataku ransomware.

Dostarcza również szczegółowych informacji o zachowaniu użytkowników – na przykład o tym, kto kliknął złośliwy adres URL – pomagając firmom zidentyfikować obszary, w których ich polityka bezpieczeństwa lub szkolenia uświadamiające mogłyby wymagać większej uwagi.



Nasze doświadczenie i osiągnięcia w dziedzinie cyberbezpieczeństwa

Choć Zyxel Networks jest najlepiej znany jako dostawca przełączników sieciowych i punktów dostępowych WiFi, firewalle dostarczamy już od 1999 roku i mamy znaczące doświadczenie w dziedzinie cyberbezpieczeństwa.

Setki tysięcy firm na całym świecie ufają naszym rozwiązaniom w zakresie ochrony swoich sieci. Zarówno klienci końcowi, jak i partnerzy wiedzą, że mogą polegać na Zyxel Networks w kwestii zachowania prostoty bez uszczerbku dla bezpieczeństwa.

Zostało to docenione w całej branży. Podstawowy model USG FLEX 50HP otrzymał nagrodę Security Hardware of the Year w ramach PC Pro Excellence Awards 2025, a my uzyskaliśmy status Champion w badaniu bezpieczeństwa Professional User Ratings (PUR) 2026 przeprowadzonym przez niezależną organizację badawczą *techconsult*, na podstawie opinii tysięcy ekspertów ds. bezpieczeństwa.

Niezależne testy przeprowadzone przez The Tolly Group potwierdzają wysoką wydajność i skuteczność zabezpieczeń serii USG FLEX H, podkreślając jej doskonałe wykrywanie złośliwego oprogramowania oraz ogólną ochronę.

Zyxel Networks jest również zarejestrowanym podmiotem CVE Numbering Authority (CNA) – co stanowi uznanie za odpowiedzialnego dostawcę zabezpieczeń, który na bieżąco ocenia i usuwa zgłaszane luki Common Vulnerabilities and Exposures (CVE). Nasze produkty wspierają gotowość do zgodności ze standardami, takimi jak PCI-DSS (finanse), HIPAA (ochrona zdrowia) i CIPA (edukacja), a także są gotowe na wymogi RODO i NIS 2.







ZOBACZ PEŁNE RAPORTY TOLLY

Zyxel USG FLEX H-Series vs. Ubiquiti Dream Machine: ocena skuteczności ochrony antymalware zapory sieciowej/bramy:

www.tolly.com/publications/225150

Zyxel USG FLEX 100H vs. SonicWall TZ270: ocena skuteczności ochrony antymalware oraz licencji subskrypcyjnej zapory sieciowej:

www.tolly.com/publications/225151

Dlaczego jesteśmy inni – i dlaczego ma to znaczenie

Pozycja Zyxel Networks jako uznanego dostawcy cyberbezpieczeństwa wyróżnia nas wśród firm z branży sieciowej.

Żadna nowoczesna firma nie może funkcjonować bez bezpiecznej, niezawodnej łączności, a w przypadku MŚP jesteśmy jedną z nielicznych firm zdolnych zapewnić prostotę, wydajność i opłacalność, których potrzebują małe firmy.

Upraszczamy bezpieczeństwo

W miarę jak cyberbezpieczeństwo staje się coraz bardziej złożone, nasz cel pozostaje taki sam: uczynić je jak najprostszym dla MŚP oraz obsługujących je resellerów IT i instalatorów technicznych. Usuwamy bariery, sprawiając, że cyberbezpieczeństwo jest łatwiejsze do zrozumienia i łatwiejsze do dostarczenia – szybkie we wdrożeniu oraz łatwe do uzasadnienia biznesowego, zarządzania i wsparcia.

Dla MŚP oferujemy kompleksowe rozwiązanie, które nie idzie na kompromis w kwestii bezpieczeństwa i pozostaje aktualne oraz chronione. Dla partnerów IT i instalatorów oferujemy możliwość pogłębienia zaufania klientów, rozwijania ich biznesu oraz uzyskiwania stałych, powtarzających się przychodów.



Copyright © 2026 Zyxel i/lub jego podmioty powiązane. Wszelkie prawa zastrzeżone. Wszystkie specyfikacje mogą ulec zmianie bez powiadomienia. Mimo dołożenia wszelkich starań, aby informacje zawarte w niniejszej publikacji były dokładne, ani Zyxel, ani jego spółki zależne/powiązane nie ponoszą odpowiedzialności za jakiekolwiek błędy lub nieścisłości.

30/09/2026