

RAPORT

Trzy zastosowania owocujące transformacją oddziałów za sprawą rozwiązania Fortinet Secure SD-WAN



Streszczenie

Organizacje przechodzą z sieci rozległych (WAN) o ograniczonych możliwościach działania na architektury definiowanych programowo sieci WAN (software-defined WAN, SD-WAN), które oferują szybszą łączność, oszczędność kosztów i inne korzyści. Technologia SD-WAN jednak wiąże się również z pewnymi wyzwaniami, takimi jak wymagania dotyczące cyberbezpieczeństwa, z którymi trzeba się uporać przed przystąpieniem do wdrożenia.

Rozwiązanie Fortinet Secure SD-WAN jest wbudowane w zapory nowej generacji (Next-Generation Firewall, NGFW) FortiGate i udostępniane bez dodatkowych licencji. Nasze wysokowydajne rozwiązanie, wyposażone w jedyny w branży układ SD-WAN ASIC, zwiększa wydajność aplikacji, a jednocześnie oznacza bardziej ekonomiczne środowisko. Dokładna identyfikacja aplikacji przekłada się na pełny wgląd i kontrolę przy użyciu polityk biznesowych SD-WAN, zapewniając najlepszą obsługę kluczowych aplikacji czasu rzeczywistego i aplikacji do pracy zespołowej. Zintegrowane zabezpieczenia stanowią zaawansowaną ochronę przed wszelkiego rodzaju zagrożeniami.

Urządzenia NGFW FortiGate są dostępne w szerokiej gamie modeli na potrzeby obsługi lokalizacji o dowolnej wielkości — od małych oddziałów po hyperskalowe centra danych. Opcje w formie maszyn wirtualnych można bez trudu wdrażać w chmurach prywatnych i publicznych. Wszystkimi urządzeniami FortiGate można centralnie zarządzać.

Trzy typowe zastosowania pokazują, jak Fortinet zapewnia wszelkie zalety architektury SD-WAN bez obniżania poziomu bezpieczeństwa.

Wstęp

Łączność firmy ze światem zewnętrznym tradycyjnie oznacza jednego wybranego usługodawcę, który ma sprostać wszelkim potrzebom związanym z aplikacjami. Chociaż jest to kosztowne, da się takie połączenie kontrolować i chronić, jednocześnie zapewniając dostęp do najważniejszych zasobów. Infrastruktura ta ma poważne konsekwencje z perspektywy niezawodności dostępu do zasobów zewnętrznych ze względu na jeden punkt łączności, który może często ulegać awariom. Poza tym większe zapotrzebowanie na przepustowość ze strony rosnącej liczby użytkowników i generujących duży ruch aplikacji powoduje więcej zakłóceń oraz spore opóźnienia.

Wysyłanie całego ruchu z powrotem do centrum danych (tzw. backhauling) wprawdzie jest bezpieczne, jednak znacznie spowalnia działanie sieci i może być kosztowne. W obliczu szybkiego upowszechniania się aplikacji w chmurze, w tym aplikacji udostępnianych w modelu oprogramowania jako usługi (Software-as-a-Service, SaaS), takich jak Google i wideokonferencje, sensowniejsze jest uzyskiwanie do nich dostępu za pośrednictwem publicznego Internetu, zamiast wysyłania tego ruchu do i tak już obciążonego centralnego biura. Prowadzi to do rozszerzania łączności przy użyciu usług wielu dostawców lub tańszych łączy szerokopasmowych i innych opcji łączności internetowej.

Rozwiązania SD-WAN ewoluują, umożliwiając podejmowanie — z uwzględnieniem aplikacji — decyzji biznesowych dotyczących hybrydowych łączy WAN, w tym usługodawców oraz łączy szerokopasmowych i LTE. Dokładna identyfikacja aplikacji, wgląd w działanie sieci i niezawodne przełączanie ruchu aplikacji między najlepiej działającymi łączami WAN sprawiają, że SD-WAN jest obecnie najbardziej pożądaną technologią sieci WAN we wszystkich branżach. Jednak nawet po wdrożeniu SD-WAN ze względów bezpieczeństwa wrażliwy i krytyczny ruch aplikacji nadal był wysyłany do centrów danych. Ewentualnie w oddziale instalowano osobne rozwiązanie zapory na potrzeby inspekcji bezpośredniego dostępu do Internetu. Oznaczało to dodanie kolejnego punkтового produktu dla celów ochrony, przez co rosła złożoność sieci i zarządzania nią oraz odkładano w czasie wdrożenie rozwiązań chmurowych.

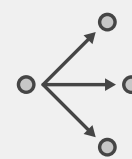
Wyzwania związane z technologią SD-WAN

Choć sieci SD-WAN cechuje szybsza i tańsza łączność niż tradycyjne sieci WAN, nie są one rozwiązaniem wszelkich bolączek. SD-WAN wykazuje zdolność do transformacji sieci obejmującej oddziały firmy, jednak w celu pełnego wykorzystania potencjału tej technologii trzeba stawić czoła kilku wyzwaniom. Mogą występować następujące problemy:

Niski komfort pracy użytkownika. Cyfrowe innowacje zwiększyły zapotrzebowanie na aplikacje SaaS i ujednoliconą komunikację jako usługę (Unified Communications-as-a-Service, UcaaS), w których przypadku wymagany jest dostęp do wielu chmur. Tradycyjne sieci WAN mają ograniczony dostęp lub stosowany jest w nich backhauling ruchu kluczowych aplikacji za pośrednictwem centrów danych. Oznacza to łączy WAN cechujące się dużymi opóźnieniami, co negatywnie wpływa na doświadczenia użytkowników.

Brak widoczności. Rozwiązania SD-WAN zwykle nie zapewniają wglądu w aplikacje na poziomie oddziałów. Może to powodować problemy związane z nieautoryzowanymi rozwiązaniami IT, w tym SaaS, co może generować zagrożenie i uniemożliwiać zachowywanie zgodności z przepisami. Poza tym użytkownicy z oddziałów mogą zużywać przepustowość na niepotrzebne aplikacje, np. Spotify czy YouTube.

Złożoność. W przypadku architektur SD-WAN mogą występować trudności z rozwiązywaniem problemów i zarządzaniem obejmującym wszystkie oddziały. Większość rozwiązań nie oferuje jednego interfejsu zarządzania umożliwiająccego skonsolidowany nadzór i kontrolę sieci w zdalnych lokalizacjach firmy. Zwiększa to obciążenie pracowników działu IT i często jest przyczyną luk, które mogą być wykorzystywane do ataków.



Firma Fortinet została uznana za lidera piąty rok z rzędu w raporcie Gartner® Magic Quadrant™ dotyczącym sieci SD-WAN z 2024 roku¹.

Problemy z bezpieczeństwem. Rezygnacja z połączeń MPLS na rzecz bezpośrednich szerokopasmowych połączeń internetowych wystawia organizacje na nowe zagrożenia wynikające z braku scentralizowanej ochrony zapewnianej przez backhauling ruchu za pośrednictwem centrum danych. Skuteczne wdrożenie sieci SD-WAN wymaga dodatkowych zabezpieczeń w infrastrukturze przedsiębiorstwa, które umożliwią ochronę tych połączeń i inspekcję intensywnego ruchu — a wszystko to bez obniżania wydajności sieci.

Fortinet Secure SD-WAN odpowiada na te wyzwania, łącząc funkcje sieciowe i zabezpieczenia w jednym ujednoliconym rozwiązaniu. Fortinet Secure SD-WAN jest dostępny w ramach urządzeń NGFW FortiGate. FortiGate łączy funkcje zapory NGFW i SD-WAN w jednym rozwiązaniu, które poprawia wydajność i bezpieczeństwo sieci WAN. Zapewnia skuteczną ochronę wszystkich placówek zdalnych dzięki konsekwentnemu wymuszaniu przestrzegania polityk i możliwości zarządzania wieloma rozwiązaniami w jednej konsoli. Trzy typowe zastosowania pokazują, jak Fortinet Secure SD-WAN może eliminować kluczowe wyzwania w środowiskach firmowych, a jednocześnie oferować większą wartość biznesową.



Oczekuje się, że w latach 2024–2030 rynek SD-WAN odnotuje CAGR na poziomie 38,9%, osiągając wartość ponad 42 mld dolarów do 2030 roku².

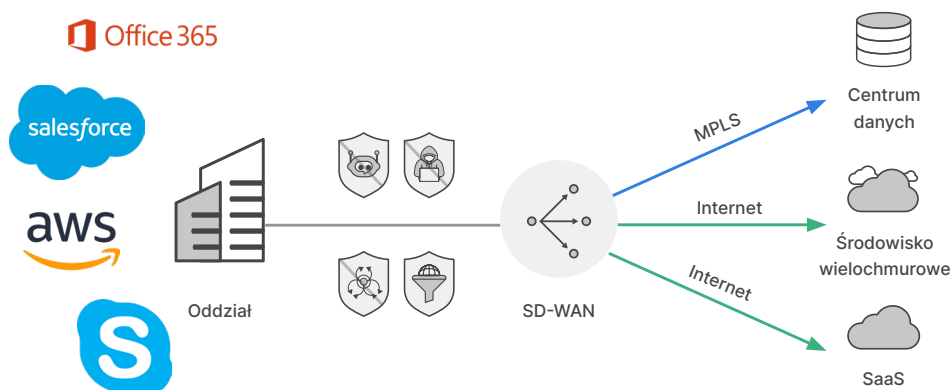


Zastosowanie: poprawa komfortu korzystania z aplikacji

Jeśli organizacja nie dysponuje rozwiązaniem Fortinet Secure SD-WAN, to w celu blokowania cyberzagrożeń musi albo wysyłać cały wrażliwy i krytyczny ruch aplikacji do centrów danych, albo zainstalować zaporę w oddziale. Niestety w obu tych przypadkach spada wydajność aplikacji w chmurze, a wzrasta trudność zarządzania.

Dzięki rozwiązaniu Fortinet organizacje mogą zastąpić wiele produktów punktowych funkcjami SD-WAN, ochrony i sieci zintegrowanymi w ramach jednego urządzenia — przykładą się to na uproszczenie sieci, niższe powiązane z nią koszty i łatwiejsze zarządzanie. Fortinet Secure SD-WAN zapewnia wysoki ogólny poziom bezpieczeństwa, dzięki czemu organizacje mogą uzyskiwać dostęp do aplikacji w chmurze za pomocą bardziej przystępnych cenowo, bezpośrednich połączeń internetowych o niskich opóźnieniach. Oznacza to większą niezawodność i umożliwia optymalną wydajność aplikacji, zapewniając użytkownikom lepsze doświadczenia. Stała kontrola kondycji sieci sprawia, że wybierane jest najlepsze dostępne łącze WAN (z uwzględnieniem zdefiniowanych przez użytkownika umów o poziom usług aplikacji), a degradacja sieci jest kompensowana właśnie przez przeniesienie ruchu na lepiej działające łącze WAN. Forward error correction (FEC) ogranicza utratę i duplikację pakietów, aby wspomagać transmisję w warunkach dużych opóźnień. Ponadto intuicyjne procesy polityk biznesowych ułatwiają konfigurację i zarządzanie potrzebami aplikacji dzięki możliwości elastycznego nadawania priorytetu aplikacjom o znaczeniu krytycznym dla firmy.

Jako część infrastruktury Fortinet Security Fabric zaporą FortiGate NGFW z rozwiązaniem Secure SD-WAN udostępnia zaawansowane funkcje zabezpieczeń w celu ochrony bezpośredniego dostępu do Internetu. Obejmuje to kompleksowe zapobieganie zagrożeniom, m.in. filtrowanie stron internetowych, skanowanie pod kątem złośliwego oprogramowania i zapobieganie włamaniom (intrusion prevention, IPS). Wykonywane są też czynności z zakresu wykrywania zagrożeń, na przykład inspekcja ruchu szyfrowanego SSL, a także sandboxing — dzięki integracji ze środowiskiem FortiSandbox.



Ilustracja 1. FortiGate z Secure SD-WAN potrafi przeobrazić architektury oddziałów firmy.

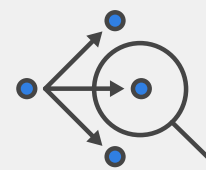
Wgląd i kontrola są istotne z perspektywy wdrożenia modelu SaaS na potrzeby pracowników rozproszonych oddziałów. Pracownicy mogą łatwo instalować aplikacje chmurowe bez udziału i zgody administratorów środowiska IT. Takie wymykające się kontroli nieautoryzowane korzystanie z rozwiązań IT może bezpośrednio przyczyniać się do przedostawiania się złośliwych zagrożeń do sieci oddziałów, generowania luk w zabezpieczeniach, a nawet naruszeń zgodności z przepisami dotyczącymi prywatności i regulacjami branżowymi. Secure SD-WAN obsługuje pełny wgląd w aplikacje i ich kontrolowanie dzięki kilku kluczowym funkcjom:

Rozległa znajomość aplikacji. Baza danych aplikacji dostępna w FortiGate obsługuje ponad 5000 sygnatur aplikacji i umożliwia dokładne wykrywanie krytycznych aplikacji czasu rzeczywistego. Taki poziom wglądu w aplikacje umożliwia administratorom systemów definiowanie polityk biznesowych z precyzyjnymi umowami dotyczącymi parametrów sieci (opóźnień, utraty pakietów i jitteru), ponieważ rozwiązanie SD-WAN automatycznie dba, by do przekazywania ruchu było wybierane jak najlepsze łącze WAN. Nowe aplikacje, w tym ruch szyfrowany oraz ruch aplikacji w chmurze, mogą być identyfikowane i klasyfikowane za pomocą opcjonalnej usługi kontroli aplikacji FortiGuard Application Control Service. Zapory NGFW FortiGate mogą na bieżąco otrzymywać aktualizacje informacji o zagrożeniach z FortiGuard Labs, co umożliwia bardziej efektywny routing generowanego przez aplikacje ruchu i ochronę przed zagrożeniami w czasie rzeczywistym.

Automatyczna analiza obejmująca wiele tras. Fortinet Secure SD-WAN stale monitoruje połączenia, więc jeśli w przypadku jakiejś aplikacji warunki przepustowości ulegną pogorszeniu, rozwiązanie to może płynnie przełączyć ruch na lepiej działające łącze WAN bez zakłócania dostępności aplikacji. W najgorszym przypadku zaś, tj. jeśli wszystkie łącza WAN ulegną degradacji, może poprawić warunki sieciowe za pomocą różnych zaawansowanych technik, np. forward error correction.

Utrzymanie wysokiej jakości działania aplikacji do komunikacji jest szczególnie ważne w przypadku oddziałów regionalnych i zdalnych biur, których produktywność w dużym stopniu zależy od interakcji i współpracy.

Śledzenie i raportowanie zgodności. Funkcje śledzenia i raportowania dostępne dzięki rozwiązaniu Secure SD-WAN pomagają dbać o przestrzeganie przepisów dotyczących prywatności, standardów bezpieczeństwa i regulacji branżowych, a więc i zmniejszają ryzyko kar finansowych oraz kosztów postępowań prawnych w przypadku naruszenia tych wymogów. Funkcje te śledzą aktywność zagrożeń w czasie rzeczywistym, ułatwiają ocenę ryzyka, wykrywają ewentualne problemy i pomagają je eliminować. Monitorują również polityki zapór i wspomagają automatyzację audytów zgodności z przepisami.



Zespół CyberRatings.org przeprowadził niezależny test rozwiązania Fortinet Secure SD-WAN metodą SD-WAN Test Methodology v2.0. W ramach jednego z testów mierzono jakość połączenia (quality of experience) podczas korzystania z usług Voice over Internet Protocol (VoIP) i aplikacji wideo. Rozwiązanie Fortinet Secure SD-WAN uzyskało najwyższe oceny za QoE w obszarze VoIP i wideo oraz ogólną ocenę „Polecane”³.



Zastosowanie: szybszy dostęp do chmur

Organizacje nadal realizują strategię ukierunkowaną przede wszystkim na chmurę i większość przedsiębiorstw ma jakieś obciążenia w chmurze. Ponieważ zaś coraz więcej aplikacji, takich jak Office365 i Salesforce, przenosi się do chmury, tradycyjne podejście polegające na backhaulingu ruchu przez starsze sieci WAN do centrum danych powoduje utrudnienia, co skutkuje niedobrymi doświadczeniami użytkowników aplikacji w chmurze.

Wykorzystanie rozwiązania Fortinet Secure SD-WAN do bezpośredniego połączenia z chmurami w celu obsługi aplikacji SaaS i środowisk wielochmurowych poprawia komfort użytkownika aplikacji biznesowych. Zintegrowane zaawansowane zabezpieczenia utrzymują wysoki poziom bezpieczeństwa oddziałów firmy nawet w przypadku bezpośredniego dostępu internetowego do chmury. Zarządzanie rozwiązaniami na brzegu sieci, chmurami i aplikacjami SaaS w jednej konsoli obniża koszty i upraszcza obsługę oddziałów.

Dostęp do wielu chmur w celu zapewnienia ciągłości biznesowej. Fortinet Secure SD-WAN zapewnia przyspieszoną łączność z aplikacjami SaaS i aplikacjami głównych dostawców chmur publicznych na całym świecie. Dzięki dogłębnej integracji z Azure Virtual WAN rozwiązanie Secure SD-WAN może być konfigurowane automatycznie, jest łatwe w użyciu i zapewnia widoczność całej rozproszonej infrastruktury. Jest ono dostępne jako urządzenie sprzętowe, wirtualizacja funkcji sieciowych na potrzeby wdrożeń lokalnych oraz urządzenie wirtualne w środowiskach Amazon Web Services, VMware Cloud, Azure, Google Cloud, Oracle i Alibaba Marketplace.

Zdalna łączność VPN. Wirtualne sieci prywatne (VPN) zapewniają bezpieczne zdalne połączenie sieciowe, tworząc dobrze zabezpieczony tunel w ramach mniej bezpiecznego transportu sieciowego (Internetu publicznego). Jednym z powodów popularności SD-WAN są korzyści oferowane przez sieci VPN w Internecie pod względem kosztów i wydajności w porównaniu z wydajnością i elastycznością sieci VPN MPLS.

Fortinet Secure SD-WAN zapewnia natywne zarządzanie zdalną łącznością VPN w celu utrzymania odpowiednich poziomów ochrony i inspekcji przy jednoczesnym zapewnieniu wysokich poziomów wglądu oraz kontroli. Dotyczy to danych i aplikacji przechodzących przez środowisko SD-WAN oraz obejmuje całą sieć rozproszoną.

W przypadku organizacji z wieloma lokalizacjami zdalnymi wysoce wydajna skala wirtualnej sieci VPN jest kolejną istotną cechą bezpiecznej i efektywnej sieci SD-WAN. Sieci VPN zawierają zwykle wiele tuneli na oddział. Ich wielokrotność występująca w przypadku dużej liczby oddziałów lub lokalizacji zdalnych może pogarszać wydajność sieci. Urządzenia FortiGate NGFW są wyposażone w zaawansowane, specjalnie zaprojektowane procesory zabezpieczeń, które zwiększają wydajność i skalowalność wirtualnych sieci VPN z dużą liczbą tuneli.



Zastosowanie: uproszczenie dzięki centralizacji zarządzania i kontroli

Wiele firm może być zainteresowanych wymianą swoich urządzeń WAN i LAN na rzecz rozwiązania zapewniającego głębszą integrację i prostsze zarządzanie operacjami w oddziałach. Osobne infrastruktury WAN i LAN zwiększają złożoność oddziału (oznacza więcej urządzeń do wdrażania i aktualizowania przy użyciu różnych konsol zarządzania). Taka struktura ogranicza również wgląd w operacje i kontrolę nad nimi, a jednocześnie zwiększa prawdopodobieństwo luk w zabezpieczeniach, które mogą być wykorzystywane do ataków.

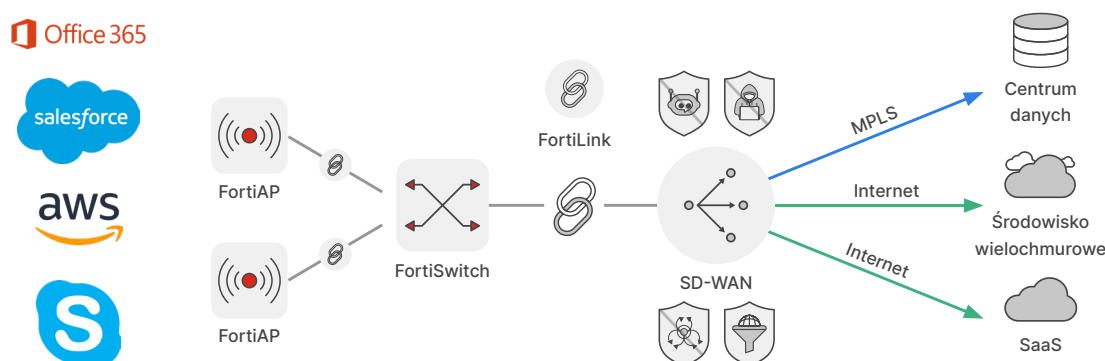
Zarządzanie w jednej konsoli. Fortinet udostępnia intuicyjny orkiestrator Secure SD-WAN jako część rozwiązania Fabric Management Center. Znacznie upraszcza to pracę zespołów IT dzięki scentralizowanym wdrożeniom, stosowaniu automatyzacji, aby oszczędzać czas, i oferowaniu polityk ukierunkowanych na cele biznesowe.

Fortinet Secure SD-WAN obsługuje rozszerzone analizy i raporty dotyczące sieci SD-WAN w ramach Fabric Management Center. Jedna konsola i szeroko zakrojone analizy sieci SD-WAN pomagają precyzyjnie dostosować polityki biznesowe i polityki bezpieczeństwa w celu zwiększenia komfortu użytkowników.

Model oddziału definiowanego programowo (software-defined branch, SD-Branch) eliminuje szereg wyzwań dzięki skonsolidowaniu operacji WAN i LAN w ramach jednego rozwiązania. Jako rozszerzenie infrastruktury Fortinet Security Fabric zaporę NGFW FortiGate z Secure SD-WAN można zintegrować z rozwiązaniami FortiAP i FortiSwitch za pośrednictwem protokołu FortiLink. Umożliwia to zespołom IT zarządzanie lokalnymi punktami końcowymi (np. urządzeniami Internetu rzeczy) podłączonymi do sieci LAN i automatyczne poddawanie kwarantannie urządzeń z symptomami naruszenia bezpieczeństwa. Wdrożenia SD-Branch przy użyciu rozwiązań Fortinet gwarantują głęboką integrację sieci WAN/LAN, prostotę, bezpieczeństwo i najniższy w branży całkowity koszt posiadania.

Automatyczne wdrożenia. Wdrożenie sieci SD-WAN powinno być tak proste jak włączenie funkcji i taką właśnie prostotę zapewnia obsługa automatycznego wdrożenia oferowana przez Fortinet Secure SD-WAN. Nowe oddziały można szybko podłączać oraz zabezpieczać, dysponując naprawdę niewielką wiedzą specjalistyczną — i bez dodatkowych nakładów pracy. Fortinet upraszcza infrastrukturę i obsługuje operacje w modelu SD-Branch dzięki skonsolidowanym funkcjom sieci WAN/LAN oraz zaawansowanym zabezpieczeniom. Żaden inny dostawca nie jest w stanie zapewnić takiej kombinacji możliwości.

Szybkie rozwiązywanie problemów. Ulepszone analizy dostępności łącza WAN, SLA dotyczących wydajności i ruchu generowanego przez aplikacje w czasie pracy, a także statystyki historyczne umożliwiają zespołom ds. infrastruktury rozwiązywanie problemów i szybkie eliminowanie zakłóceń działania sieci. Fabric Management Center oferuje zaawansowane funkcje telemetryczne zapewniające wgląd w aplikacje i wydajność sieci, co umożliwia szybsze rozwiązywanie problemów i ograniczenie liczby zgłoszeń do zespołu pomocy technicznej IT. Raporty na żądanie dotyczące środowiska SD-WAN zapewniają bardziej szczegółowy obraz zagrożeń, a także poziomy zaufania i dostęp do zasobów, które są niezbędne z perspektywy zachowania zgodności z przepisami.



Ilustracja 2. Ogólny model SD-Branch firmy Fortinet zakłada konsolidację infrastruktur WAN i LAN.

Korzystanie z zalet sieci SD-WAN

W związku z nieustającym rozwojem aplikacji SaaS, VoIP i wideo sieć SD-WAN może pomóc rozproszonym przedsiębiorstwom w czerpaniu korzyści z cyfrowej transformacji bez obniżania wydajności sieci czy produktywności użytkowników.

Z wyzwaniami związanymi z wydajnością i bezpieczeństwem, które często towarzyszą sieciom SD-WAN, można się uporać dzięki rozwiązaniu Fortinet Secure SD-WAN, natywnemu elementowi infrastruktury Fortinet Security Fabric i zapory NGFW FortiGate. Secure SD-WAN umożliwia organizacjom wdrażanie aplikacji w chmurze przy jednoczesnym szybkim nadawaniu priorytetu bezpieczeństwu. Pomaga też obniżyć koszty operacyjne, a zarazem zachować wysoką sprawność działania usług VoIP, wideo i IPsec VPN. Upraszcza również infrastrukturę sieciową oddziałów, ponieważ łączy funkcje sieciowe i zaawansowane zabezpieczenia w jednym, ujednoliconym rozwiązaniu.

¹ [2024 Gartner® Magic Quadrant™ dotyczący sieci SD-WAN](#), Gartner, 2024 r.

² [SD-WAN Market to Reach over \\$42 Billion by 2030](#) (Rynek SD-WAN ma osiągnąć wartość ponad 42 miliardów dolarów do 2030 roku), Prescient & Strategic Intelligence, 2024.

³ [2023 CyberRatings.org Enterprise SD-WAN Report](#) (Raport CyberRatings.org 2023 dotyczący sieci SD-WAN w przedsiębiorstwach), CyberRatings.org, III kwartał 2023 r.



www.fortinet.com