OPRACOWANIE

Wdrażanie innowacji cyfrowych dzięki architekturze Fortinet Security Fabric

Kompleksowość, integracja i automatyzacja

Streszczenie

Przedsiębiorstwa szybko wdrażają inicjatywy z zakresu innowacji cyfrowych, aby intensywniej rozwijać swoją działalność, obniżać koszty, poprawiać wydajność i zapewniać klientom lepsze doświadczenia. Typowe przykłady takich inicjatyw obejmują przenoszenie aplikacji i procesów do chmury, wdrażanie w sieci przedsiębiorstwa urządzeń związanych z Internetem rzeczy oraz rozszerzanie zasięgu działalności o nowe oddziały.

Wspomnianemu rozwojowi infrastruktury towarzyszą również zagrożenia dla bezpieczeństwa. Przedsiębiorstwo musi zatem poradzić sobie z coraz większą powierzchnią ataku, zaawansowanymi zagrożeniami, rosnącą złożonością infrastruktury i coraz większą liczbą przepisów do uwzględnienia. Aby osiągnąć pożądane wyniki innowacji cyfrowych przy jednoczesnym efektywnym zarządzaniu ryzykiem i ograniczaniu złożoności, przedsiębiorstwo potrzebuje zatem platformy chroniącej przed cyberatakami, która zapewni widoczność całego środowiska oraz udostępni narzędzia umożliwiające łatwe zarządzanie zarówno bezpieczeństwem, jak i operacjami sieciowymi.

Architektura Fortinet Security Fabric spełnia te kryteria, ponieważ oferuje kompleksowe, zintegrowane i zautomatyzowane rozwiązania, w tym szczególnie zabezpieczone funkcje sieciowe, dostęp do sieci oparty na zasadzie zerowego zaufania, ochronę chmury dynamicznej oraz mechanizmy zabezpieczające korzystające ze sztucznej inteligencji (AI). Ofertę Fortinet uzupełnia ekosystem doskonale zintegrowanych rozwiązań innych producentów, które minimalizują luki w architekturze zabezpieczeń przedsiębiorstwa i maksymalizują zwrot z inwestycji we wspomniane zabezpieczenia.

84% dyrektorów ds. bezpieczeństwa uważa, że ryzyko cyberataków wzrośnie[1].

77% specjalistów ds. bezpieczeństwa stwierdza, że ich przedsiębiorstwo przeniosło aplikacje lub infrastrukturę do chmury mimo znanych obaw dotyczących bezpieczeństwa[3].

Innowacje cyfrowe przekształcają wszystkie sektory przemysłu

We wszystkich sektorach gospodarki na całym świecie, innowacje cyfrowe są uznawane za warunek konieczny rozwoju działalności i zapewnienia klientom lepszych doświadczeń. Dyrektorzy ds. informatycznych są zasadniczo pozytywnie nastawieni do swoich inicjatyw cyfrowych — 61% z nich stwierdza, że korzysta już z operacji związanych z chmurą, Internetem rzeczy i urządzeniami przenośnymi[2].

Z perspektywy dostawców usług chmurowych inicjatywy cyfrowe w kontekście IT i cyberbezpieczeństwa oznaczają szereg zmian w środowiskach sieciowych. Użytkownicy coraz częściej korzystają z urządzeń przenośnych i uzyskują dostęp do sieci przedsiębiorstwa z lokalizacji i punktów końcowych, które nie zawsze znajdują się pod kontrolą działu IT. Ponadto łączą się bezpośrednio z chmurami publicznymi w celu używania różnych aplikacji biznesowych takich jak Office 365. Z jeszcze większej liczby punktów końcowych korzystają urządzenia związane z Internetem rzeczy, które często znajdują się w odległych i nienadzorowanych lokalizacjach. Wreszcie stosowane zewnętrzne rozwiązania chmurowe obsługują liczne odległe oddziały, z których większość łączy się bezpośrednio z usługami chmurowymi i komórkowymi bez pośrednictwa centrów danych w przedsiębiorstwie.

Wszystkie te zmiany sprawiają, że dotychczasowa strategia ochrony sieci na jej granicy jest już nieaktualna, a dostawcy usług chmurowych muszą stosować nową strategię obrony obejmującą wiele warstw (ang. defense-in-depth).

Migracja aplikacji i procesów do chmury

Prawie każde przedsiębiorstwo zaczęło lub planuje przenosić niektóre swoje procesy i aplikacje do chmury. Decyzje te często wynikają z chęci obniżenia kosztów oraz poprawy skalowalności i efektywności operacyjnej na bazie elastyczności zapewnianej przez chmurę.

Dostawcy usług chmurowych oferują przedsiębiorstwom szeroki zakres modeli wdrożenia. Przedsiębiorstwa mogą zatem wybrać aplikacje udostępniane w modelu SaaS (oprogramowanie jako usługa), na przykład Salesforce lub Box, a aplikacje zaprojektowane i wdrożone w lokalnych środowiskach mogą zacząć być udostępniane w ramach modeli IaaS (infrastruktura jako usługa) lub PaaS (platforma jako usługa) takich jak Amazon Web Services (AWS), Google Cloud Platform (GCP), Microsoft Azure, Oracle Cloud Infrastructure i IBM Cloud.

Z obawy przed uzależnieniem się od jednego dostawcy usług chmurowych oraz w celu wdrożenia każdej aplikacji i każdego procesu w najbardziej odpowiedniej do tego chmurze, wiele przedsiębiorstw wdrożyło infrastrukturę wielochmurową. Wadą takiej swobody wyboru jest konieczność poznania specyficznych cech każdej używanej chmury. Ponadto poszczególne chmury muszą korzystać z różnych narzędzi do zarządzania swoim środowiskiem i swoimi zabezpieczeniami, co zmniejsza poziom widoczności i wymaga zastosowania wielu konsol na potrzeby zarządzania, w tym zarządzania zasadami, raportowania itp.

Wielość punktów końcowych w wielu środowiskach

Punkty końcowe są prawdopodobnie najbardziej podatnymi na zagrożenia elementami sieci dostawcy usług chmurowych. Więksi dostawcy mają tysiące pracowników, z których każdy korzysta z wielu urządzeń służbowych i prywatnych w celu uzyskania dostępu do zasobów sieciowych. Zapewnienie cyberhigieny i bieżącej aktualizacji zabezpieczeń punktów końcowych w kontekście wszystkich tych urządzeń to ogromne przedsięwzięcie. Do tego należy uwzględnić dynamicznie rosnącą liczbę urządzeń związanych z Internetem rzeczy. Do końca 2019 r. liczba takich aktywnych urządzeń przekroczyła 26,66 mld, a według szacunków ekspertów liczba ta wyniesie w 2020 r. 31 mld[5].

Urządzenia związane z Internetem rzeczy są obecnie używane w bardzo wielu kontekstach biznesowych. Zapewniają one spersonalizowane usługi klientom z branży detalicznej i hotelarskiej, śledzą stany magazynowe w przedsiębiorstwach z branży produkcyjnej i logistycznej oraz monitorują urządzenia w fabrykach i elektrowniach.

Urządzenia związane z Internetem rzeczy często były projektowane z myślą o wytrzymałości i wydajności kosztem bezpieczeństwa (słabsze zabezpieczenia i protokoły komunikacyjne). W przeciwieństwie do większości urządzeń sieciowych urządzenia związane z Internetem rzeczy są często instalowane w oddziałach, na otwartej przestrzeni lub w obiektach, w których na stałe lub okresowo nie ma personelu (na przykład elektrownie). Z tych niestrzeżonych miejsc wspomniane urządzenia często przesyłają krytyczne, wrażliwe dane do fizycznych centrów danych i usług chmurowych.

Rozszerzenie działalności na różnych rynkach w różnych krajach

W miarę rozszerzania swojego globalnego zasięgu (w drodze otwierania nowych zakładów, oddziałów i innych placówek satelickich) przedsiębiorstwa napotykają na coraz większe ograniczenia przepustowości sieci rozległych (WAN). O ile aplikacje SaaS, funkcje wideokonferencyjne i technologia VoIP (Voice over IP) zwiększają produktywność i umożliwiają świadczenie nowych usług, o tyle przyczyniają się również do bardzo dużego wzrostu natężenia ruchu we wspomnianych sieciach rozległych.

Od wielu lat główną technologią łączności stosowaną w sieciach rozległych jest niezawodny protokół MPLS (ang. Multiprotocol Label Switching). Za jego pomocą trudno jest jednak zoptymalizować wykorzystanie przepustowości sieci rozległej i zróżnicować poziom jakości usług wymagany w poszczególnych zastosowaniach. W rezultacie rozbudowa oddziałów i rozszerzenia usług mogą szybko doprowadzić do bardzo dużego wzrostu kosztów sieci rozległej.

W związku z powyższym przedsiębiorstwa zaczynają wdrażać definiowane programowo sieci rozległe (SD-WAN), które efektywnie wykorzystują protokół MPLS, połączenia internetowe oraz inne rodzaje łączy telekomunikacyjnych. Ponadto w sieci SD-WAN każdy rodzaj ruchu jest dynamicznie kierowany na optymalne łącze.

Cztery kwestie do uwzględnienia podczas projektowania architektury zabezpieczeń

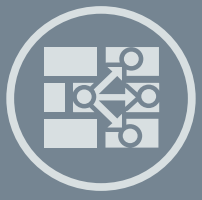
Przedsiębiorstwa entuzjastycznie podchodzą do inicjatyw cyfrowych, skutki ich wdrożenia dla bezpieczeństwa sieci są jednak często pomijane lub minimalizowane. W rzeczywistości prawie 80% przedsiębiorstw wdraża nowe innowacje cyfrowe szybciej niż jest w stanie zabezpieczyć je przed cyberzagrożeniami[9].

W związku z wdrażaniem wspomnianych innowacji cyfrowych dyrektorzy ds. IT muszą podczas projektowania architektury zabezpieczeń uwzględnić cztery następujące kluczowe czynniki:

Środowiska chmurowe są dynamiczne: 74% przedsiębiorstw przeniosło aplikacje do chmury, a następnie z powrotem zainstalowało je lokalnie[4].

84% przedsiębiorstw korzysta z wielu chmur. 81% z nich wskazuje na bezpieczeństwo jako główne wyzwanie w tym kontekście[6].

W latach 2017–2019 liczba przedsiębiorstw, w których doszło do naruszenia ochrony danych z powodu niezabezpieczonych urządzeń lub aplikacji Internetu rzeczy[7], wzrosła o 73%.



Rozwiązanie SD-WAN zapewnia większą wydajność i większe bezpieczeństwo przy niższych kosztach niż rozwiązania korzystające z łączy MPLS[8].

Zwiększająca się powierzchnia ataku

Wrażliwe dane mogą potencjalnie znajdować się w dowolnym miejscu i być przesyłane za pośrednictwem licznych łączy pozostających poza kontrolą przedsiębiorstwa. Aplikacje w chmurze są narażone na zagrożenia z Internetu, a każda nowa instancja chmurowa tworzy dodatkową powierzchnię ataku na przedsiębiorstwo. Urządzenia związane z Internetem rzeczy również rozszerzają tę powierzchnię o kolejne odległe lokalizacje, w których nie ma personelu. W takich nienadzorowanych fragmentach infrastruktury włamania mogą być niezauważone przez tygodnie lub miesiące i umożliwiać cyberprzestępcom sianie spustoszenia w systemach przedsiębiorstwa. Urządzenia przenośne i należące do użytkownika punkty końcowe „wzbogacają" powierzchnię ataku o element nieprzewidywalności, ponieważ użytkownicy łączą się za ich pomocą z siecią przedsiębiorstwa z różnych oddziałów, przestrzeni publicznych i krajów. W rzeczywistości rozległa migracja danych do chmury, szerokie zastosowanie platform mobilnych oraz ekstensywne wykorzystywanie urządzeń związanych z Internetem rzeczy zwiększa koszty naruszenia ochrony danych (w przeliczeniu na rekord) o setki tysięcy dolarów[10].

Taka rozszerzona, dynamiczna powierzchnia ataku demontuje niegdyś dobrze zdefiniowaną granicę sieci i chroniące ją zabezpieczenia. Napastnikom jest teraz o wiele łatwiej przeniknąć do sieci, a gdy im się to już uda, czeka na nich tylko niewiele barier utrudniających im swobodne i skryte realizowanie założonych celów. Z tego względu zabezpieczenia w przedsiębiorstwach wdrażających innowacje cyfrowe muszą mieć charakter wielopłaszczyznowy (z mechanizmami pozwalającymi na kontrolę każdego segmentu sieci), oparty na założeniu, że wcześniej czy później cyberprzestępcy sforsują zabezpieczenia na granicy sieci. Dostęp do zasobów sieciowych musi natomiast opierać się na zasadzie najmniejszego uprzywilejowania (least privilege) i stale weryfikowanym poziomie zaufania.

Zaawansowane metody włamań

Liczba stosowanych metod włamań szybko rośnie, ponieważ cyberprzestępcy nieustanne próbują ominąć lub sforsować tradycyjne cyberzabezpieczenia. Nawet 40% nowego złośliwego oprogramowania wykrytego w danym dniu to zagrożenia wcześniej nieznane (ang. zero-day)[15]. Bez względu na to, czy wspomniana sytuacja wynika ze zwiększonego wykorzystania wielopostaciowego złośliwego oprogramowania, czy też z dostępności narzędzi do tworzenia złośliwego oprogramowania, wzrost liczby ataków typu „zero-day" skutkuje spadkiem skuteczności tradycyjnych algorytmów służących do wykrywania złośliwego oprogramowania opartych na rozpoznawaniu sygnatur. Ponadto cyberprzestępcy nadal wykorzystują inżynierię społeczną, aby przełamać zabezpieczenia zapewniane przez mechanizmy statycznego zaufania stosowane w tradycyjnych podejściach do bezpieczeństwa. Z badań wynika, że w minionym roku 85% przedsiębiorstw było celem ataków wykorzystujących techniki phishingu lub inżynierii społecznej[16].

W miarę rosnącej złożoności cyberzagrożeń coraz trudniejsze staje się wykrywanie i eliminowanie skutków incydentów związanych z ochroną danych i naruszeń ochrony danych. W latach 2018–2019 czas wykrycia i powstrzymania przypadku naruszenia ochrony danych zwiększył się z 266 do 279 dni[17]. Oprócz posiadania zdolności do wykrywania prób i zapobiegania próbom takich ataków, przedsiębiorstwo musi być również w stanie szybko zidentyfikować i wyeliminować skutki udanego ataku. W minionym roku ponad 88% przedsiębiorstw zgłosiło co najmniej jeden incydent naruszenia ochrony danych, co oznacza, że na ataki są narażone wszystkie przedsiębiorstwa i że uzyskanie przez nie odporności na takie ataki ma charakter krytyczny[18].

Większa złożoność ekosystemu

Według niemal połowy ankietowanych dyrektorów ds. informatycznych rosnąca złożoność jest największym problemem w kontekście zwiększającej się powierzchni ataku[19]. Złożoność rośnie, ponieważ wiele przedsiębiorstw korzysta z niezintegrowanych ze sobą punktowych zabezpieczeń (typowe przedsiębiorstwo stosuje ponad 75 różnych rozwiązań zabezpieczających[20]).

Taki brak zintegrowanych zabezpieczeń oznacza, że przedsiębiorstwo nie może korzystać z zalet płynących z ich zautomatyzowania. W rzeczywistości 30% dyrektorów ds. informatycznych stwierdza, że podstawowym problemem z zakresu bezpieczeństwa w ich przedsiębiorstwie jest liczba stosowanych procesów ręcznych[21]. Bez zautomatyzowania zabezpieczeń przedsiębiorstwu potrzebnych jest również więcej specjalistów ds. cyberbezpieczeństwa do monitorowania i zabezpieczania infrastruktury informatycznej.

61% dyrektorów ds. bezpieczeństwa infrastruktury informatycznej stwierdza, że w ich przedsiębiorstwach wdrożono już rozwiązania chmurowe oraz korzysta się z Internetu rzeczy i operacji mobilnych[11].

Nawet 40% nowego złośliwego oprogramowania wykrytego w danym dniu to zagrożenia wcześniej nieznane[12].

Realizacja inicjatywy cyfrowych wymaga od działu IT wdrożenia w przedsiębiorstwie mechanizmów zabezpieczających 17 różnych typów punktów końcowych[13].

W ciągu ostatniego roku w ponad 33% przedsiębiorstw doszło do naruszenia ochrony danych o znaczeniu krytycznym dla prowadzonej działalności, co mogło prowadzić do wymierzenia kar na mocy stosownych przepisów[14].

Wiele przedsiębiorstw nie jest jednak w stanie pozyskać z rynku wspomnianych specjalistów. Szacuje się, że ponad 4 mln stanowisk związanych z cyberbezpieczeństwem jest obecnie nieobsadzonych i liczba ta stale wzrasta[22]. Wspomniany brak specjalistów również naraża przedsiębiorstwo na ryzyko — 67% dyrektorów ds. informatycznych uważa, że brak tych specjalistów obniża ich zdolność do dotrzymywania kroku tempu zmian[23].

Tymczasem atakujący dobrze rozumieją i odpowiednio wykorzystują te problemy.

Rosnące wymagania regulacyjne

Unijne ogólne rozporządzenie o ochronie danych (RODO) oraz kalifornijska ustawa o ochronie prywatności konsumentów (CCPA) to dwa najbardziej znane, choć nie jedyne akty prawne w zakresie ochrony danych. W każdym stanie USA obowiązują obecnie przepisy dotyczące zgłaszania naruszeń ochrony danych, a w wielu z nich wprowadzono dodatkowe mechanizmy ochrony prywatności konsumentów. Ze względu na naciski polityczno-społeczne oczekuje się, że w nadchodzących latach zakres wspomnianych przepisów będzie zwiększany, a kary za ich nieprzestrzeganie będą coraz surowsze i bardziej powszechnie stosowane.

Fortinet Security Fabric

- Kompleksowość
- Automatyzacja
- Integracja

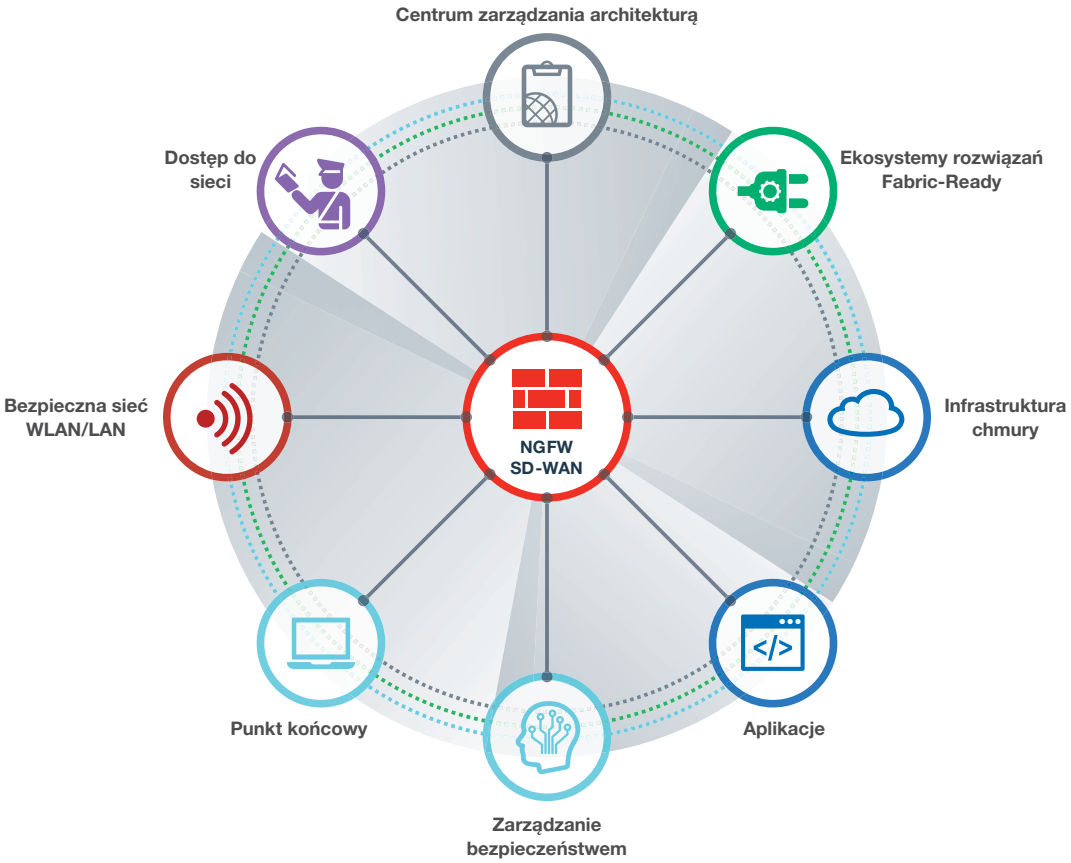
FORTINET Fabric-Ready

Przedsiębiorstwa muszą również przestrzegać standardów branżowych, co w wielu przypadkach nie jest łatwe. Wyniki stosownych audytów wskazują, że zgodnością z branżową normą PCI DSS (Payment Card Industry Data Security Standard) może pochwalić się niecałe 37% przedsiębiorstw[24]. Ze względu na zastąpienie normy PCI DSS normą PCI SSF (PCI Software Security Framework) zapewnienie odpowiedniej zgodności może okazać się dla tych przedsiębiorstw jeszcze trudniejsze.

Potrzeba uzyskania i utrzymania zgodności z przepisami istotnie wpływa na zdolność przedsiębiorstwa do osiągania celów związanych z transformacją zabezpieczeń. Na przykład spośród 71% przedsiębiorstw, które przeniosły aplikacje chmurowe z powrotem do lokalnych centrów danych, 21% zrobiło to w celu utrzymania zgodności z przepisami[25].

Architektura Fortinet Security Fabric

Architektura Fortinet Security Fabric stanowi odpowiedź na wspomniane wyzwania w zakresie bezpieczeństwa, ponieważ zapewnia przedsiębiorstwu szeroką widoczność i kontrolę całej cyfrowej powierzchni ataku, upraszcza obsługę wdrożonych produktów punktowych oraz udostępnia zautomatyzowane procesy przyspieszające działanie poszczególnych operacji.



Rysunek 1. Architektura Fortinet Security Fabric umożliwia niezawodne współdziałanie różnych technologii zabezpieczeń we wszystkich środowiskach oraz ich obsługę z poziomu jednej konsoli przy zastosowaniu jednego źródła informacji o zagrożeniach. Podejście to eliminuje luki w zabezpieczeniach sieci oraz przyspiesza reakcje na ataki i naruszenia.

Szeroka widoczność powierzchni ataku

Wraz z rozszerzaniem się (w związku z inicjatywami cyfrowymi) granic sieci przedsiębiorstwa zwiększa się również powierzchnia ataku. W tym kontekście architektura Fortinet Security Fabric zapewnia przedsiębiorstwu kompleksowe zabezpieczenia, pełną widoczność całej infrastruktury sieci oraz ochronę każdego segmentu sieci za pomocą bardzo szerokiej gamy wydajnych, bezpiecznych rozwiązań sieciowych przeznaczonych dla centrów danych, oddziałów i małych przedsiębiorstw oraz obsługujących produkty wszystkich głównych dostawców chmur.

Wszystkie komponenty mogą być konfigurowane, zarządzane i monitorowane z poziomu jednego scentralizowanego systemu zarządzania. Następuje eliminacja silosów powstałych wskutek zastosowania produktów punktowych, a pojedynczy interfejs obsługujący wszystkie komponenty infrastruktury zabezpieczeń zmniejsza obciążenie szkoleniowe dla ograniczonej liczby personelu. Wspomniany system zarządzania umożliwia również bezobsługowe wdrożenie komponentów w odległych lokalizacjach, co eliminuje konieczność wysłania personelu technicznego na miejsce wdrożenia i jeszcze bardziej obniża koszty operacyjne.

Zintegrowana architektura zabezpieczeń

Ze względu na fakt, że wszystkie komponenty są obsługiwane przez ten sam sieciowy system operacyjny FortiOS, architektura Fortinet Security Fabric umożliwia spójną konfigurację i spójne zarządzanie zasadami oraz bezproblemową komunikację w czasie rzeczywistym w ramach całej infrastruktury zabezpieczeń. Skraca to do minimum czas wykrywania i łagodzenia skutków ataków, zmniejsza zagrożenia dla bezpieczeństwa wynikające z błędów konfiguracji i ręcznej kompilacji danych oraz ułatwia szybką i odpowiednią reakcję na problemy dostrzeżone podczas audytu zgodności.

Architektura Security Fabric nie tylko integruje produkty i rozwiązania Fortinet, ale również zawiera wbudowane funkcje łączenia interfejsu programowania aplikacji (API) z mającymi status Fabric-Ready rozwiązaniami ponad 70 partnerów. Wspomniane funkcje zapewniają zatem głęboką integrację wszystkich elementów tej architektury.

Rozwiązania niewchodzące w skład ekosystemu partnerów Fabric-Ready można natomiast szybko i łatwo włączyć do architektury Security Fabric za pośrednictwem interfejsów API REST i skryptów DevOps.

Zautomatyzowane operacje, orkiestracja i reakcje na zagrożenia

Architektura Fortinet Security Fabric nie tylko zapewnia niezawodną integrację, ale również oferuje najlepsze w branży technologie uczenia maszynowego (ML), aby skutecznie przeciwdziałać szybko zmieniającym się metodom cyberwłamań. Ponadto udostępnia zaawansowane funkcje orkiestracji i automatyzacji zabezpieczeń oraz reagowania na incydenty (SOAR), proaktywnego wykrywania zagrożeń, korelacji zagrożeń, rozsyłania alertów o zagrożeniach oraz badania i analizy zagrożeń.

Aby przyspieszyć reakcje na incydenty bezpieczeństwa, trzeba również sprawić, aby pracownicy IT nie byli rozpraszani przez inne kwestie, takie jak zbieranie danych lub generowanie raportów wymaganych przez przepisy lub ścisłe kierownictwo przedsiębiorstwa. W tym kontekście architektura Fortinet Security Fabric udostępnia funkcje zautomatyzowanej agregacji dzienników, korelacji danych i generowania raportów na bazie wbudowanych szablonów.

Prawie połowa dyrektorów ds. bezpieczeństwa infrastruktury informatycznej stwierdza, że priorytetem realizowanej przez nich strategii w zakresie cyberbezpieczeństwa będzie integracja zabezpieczeń i doskonalenie narzędzi analitycznych[26].

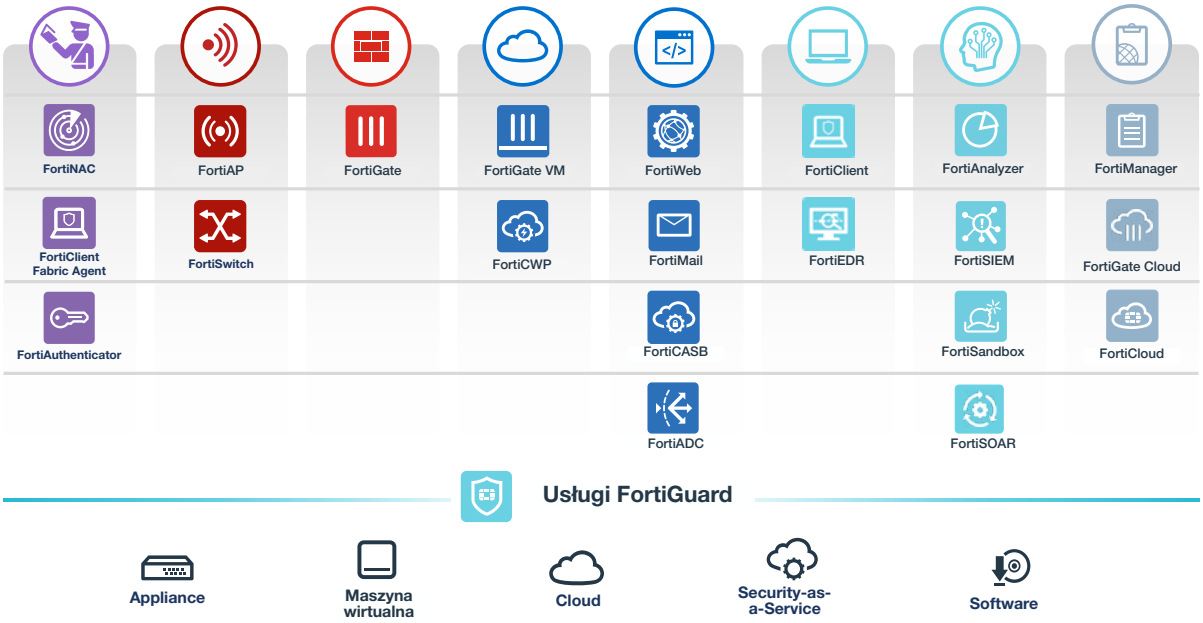
Według zewnętrznych opinii zapora następnej generacji (NGFW) FortiGate oferuje najlepszy stosunek ceny do wydajności w kontekście skanowania ruchu szyfrowanego (5,7 Gb/s dla protokołu SSL z blokadą 100% prób ominięcia zabezpieczeń[27]).

Szybsze wykrywanie przypadków i reagowanie na przypadki naruszeń może prowadzić do obniżenia całkowitych kosztów naruszeń ochrony danych o 25%[28].

Rozwiązania dostępne w ramach architektury Security Fabric

Architektura Fortinet Security Fabric oferuje rozwiązania w pięciu kluczowych obszarach: dostęp na zasadzie zerowego zaufania, zabezpieczenie sieci, ochrona chmury dynamicznej, operacje zabezpieczające oparte na sztucznej inteligencji oraz ekosystem rozwiązań partnerskich. Rozwiązania stosowane w każdym z tych obszarów są najlepsze w swojej klasie, były wielokrotnie nagradzane oraz zostały ocenione i zarekomendowane przez uznane podmioty zewnętrzne, takie jak NSS Labs i Gartner[29,30].

Rys. 2. Schemat koncepcyjny architektury Fortinet Security Fabric.



Rysunek 3. Kluczowe produkty w poszczególnych obszarach działania architektury Security Fabric.

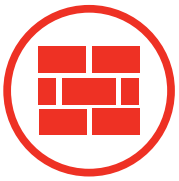
Dostęp do sieci oparty na zasadzie zerowego zaufania

W miarę wzrostu złożoności cyberzagrożeń stosowanie modelu zabezpieczeń skupionych na granicach sieci już nie wystarcza. Wskutek kradzieży tożsamości i działania złośliwego oprogramowania cyberprzestępcy mogą uzyskać dostęp do kont w sieci przedsiębiorstwa. Architektura Fortinet Security Fabric umożliwia wdrożenie modelu dostępu do sieci rozległej przedsiębiorstwa opartego na zasadzie zerowego zaufania.

Pierwszym etapem takiego wdrożenia jest wykrycie urządzeń podłączonych do wspomnianej sieci, które można przeprowadzić automatycznie za pomocą mechanizmów kontroli dostępu do sieci **FortiNAC** (NAC). Wykryte w ten sposób urządzenia są następnie skanowane pod kątem bezpieczeństwa, a zespół ds. bezpieczeństwa definiuje zasady, które mają być stosowane w odniesieniu do poszczególnych urządzeń. Po zatwierdzeniu dostępu urządzenia do sieci jest ono stale monitorowane w celu wykrycia wszelkich nietypowych zachowań, które mogłyby wskazywać na infekcję lub działania cyberprzestępców.

Jeśli przedsiębiorstwo jest zdolne do wykrycia urządzeń podłączonych do swojej sieci, może wówczas wdrożyć dostęp na zasadzie zerowego zaufania w celu określenia, kto z tych urządzeń korzysta. Serwer zarządzania tożsamością użytkownika FortiAuthenticator oferuje wbudowane mechanizmy uwierzytelniania i kontroli dostępu oparte na rolach (RBAC), co pozwala przedsiębiorstwu na wdrożenie w swoich sieciach zasad najmniejszego uprzywilejowania (least privilege) i rozdzielenia obowiązków. Tokeny FortiToken wprowadzają dwuetapowe uwierzytelnianie użytkownika, co sprawia, że skradzione dane uwierzytelniające nie zapewniają jeszcze przestępcy uwierzytelnionego dostępu do konta użytkownika.

Podłączone do sieci przedsiębiorstwa urządzenia można monitorować i sprawdzać pod kątem egzekwowania zasad za pośrednictwem tej sieci. Ze względu na fakt, że rosnąca liczba urządzeń w przedsiębiorstwie może być używana w trybie offline lub podłączona do innych sieci, warto skorzystać z rozwiązania **FortiClient** Fabric Agent, które zapewnia widoczność punktów końcowych i dynamiczną kontrolę dostępu zarówno w ramach sieci, jak i poza siecią przedsiębiorstwa.



Bezpieczeństwo infrastruktury sieciowej

W wyniku realizacji inicjatyw cyfrowych rozszerzają się sieci przedsiębiorstw i zwiększa się powierzchnia ataku, przez co potrzeba zabezpieczenia tych sieci staje się coraz bardziej paląca. Bezpieczeństwo infrastruktury sieciowej wiąże się ze ścisłą integracją infrastruktury sieciowej z architekturą zabezpieczeń przedsiębiorstwa, umożliwiając skalowanie i zmianę parametrów sieci bez uszczerbku dla jej bezpieczeństwa. Ponadto wspomniana integracja upraszcza zarządzanie siecią (minimalizacja liczby stosowanych rozwiązań punktowych) oraz zwiększa jej wydajność (urządzenia sieciowe i zabezpieczające są zoptymalizowane pod kątem współdziałania).

Zapewnienie bezpieczeństwa infrastruktury sieciowej jest jedną z podstawowych funcjonalności zapór następnej generacji (NGFW) **FortiGate**, które są pierwszą linią obrony przedsiębiorstwa przed zaawansowanymi zagrożeniami. Nie są to jednak zwykłe zapory, ponieważ dodatkowo oferują bezpieczną bramę sieciową (SWG), która identyfikuje i blokuje próby nawiązania połączenia ze złośliwymi lub podejrzanymi adresami URL. Jest to szczególnie istotne w obliczu faktu, że prawie jedna trzecia przypadków naruszenia ochrony danych wiąże się z atakami phishingowymi[31], które za pomocą złośliwych łączy lub załączników infekują punkty końcowe lub dokonują kradzieży danych uwierzytelniających użytkownika.

Zapory następnej generacji (NGFW) FortiGate przeprowadzają również deszyfrację i inspekcję danych szyfrowanych przy użyciu protokołu Secure Sockets Layer (SSL) / Transport Layer Security (TLS). Funkcja ta ma obecnie znaczenie krytyczne, ponieważ szacuje się, że 75% ruchu sieciowego w przedsiębiorstwach jest chronione za pomocą protokołów SSL/TLS, a około 82% złośliwego ruchu jest szyfrowana[32,33]. Zapory następnej generacji **FortiGate** korzystają ze specjalnych procesorów obsługujących funkcje zabezpieczeń (ang. security processors, SPU), aby nie obniżać wydajności sieci w związku z prowadzeniem wspomnianej inspekcji ruchu SSL/TLS. Zastosowanie w zaporach NGFW wydajnej inspekcji ruchu szyfrowanego pozwala również przedsiębiorstwu na uniknięcie ogólnych kosztów związanych z zakupem i wdrożeniem w swojej infrastrukturze sieciowej osobnych urządzeń temu dedykowanych.

Jeśli zagrożenia nie zostaną wykryte na granicy sieci, należy bezwzględnie uniemożliwić im działanie w sieci wewnętrznej, na przykład w drodze zastosowania segmentacji opartej na celach biznesowych. Podejrzane lub złośliwe połączenia wewnętrzne są wówczas domyślnie blokowane, a jeśli po infekcji zidentyfikowane zostanie zagrożenie wcześniej nieznane, informacja o nim zostanie rozpowszechniona w ramach architektury Security Fabric, aby zapewnić, że nie dojdzie do ponownej tego typu infekcji.

Aby było to możliwe, zabezpieczenia muszą być ze sobą zintegrowane w ramach całej sieci przedsiębiorstwa, w tym w oddziałach. Rozwiązanie **Fortinet Secure SD-WAN** zapewnia taką integrację zabezpieczeń i optymalną wydajność sieci w kontekście oddziałów. Zintegrowane w ramach rozwiązania SD-WAN zapory następnej generacji (NGFW) FortiGate przeprowadzają inspekcję ruchu w każdym oddziale. Poprawia to wydajność sieci przez zapewnienie bezpośredniego internetowego dostępu do usług i aplikacji SaaS, a także przyczynia się do obniżenia kosztów utrzymania sieci rozległej.

W ramach oddziału rozwiązanie **Fortinet Secure SD-Branch** pozwala przedsiębiorstwu na rozszerzenie widoczności i scentralizowane zarządzanie zabezpieczeniami aż do warstwy przełączania. Rozwiązanie to zawiera mechanizmy FortiNAC, oferujące bezpieczny dostęp przełączniki FortiSwitch oraz punkty dostępu bezprzewodowego **FortiAP** monitorowane i kontrolowane za pośrednictwem zapory następnej generacji (NGFW) FortiGate. Dzięki integracji zabezpieczeń w ramach całej swojej sieci rozległej przedsiębiorstwo upraszcza operacje, ponieważ eliminuje nadmiarowość i uzyskuje możliwość szybkiej, skoordynowanej reakcji na zaawansowane zagrożenia.

Ochrona chmury dynamicznej

W miarę postępów we wdrażaniu rozwiązań chmurowych niezbędne dla przedsiębiorstwa staje się rozszerzenie systemu zabezpieczeń o zasoby chmurowe. Architektura Fortinet Security Fabric pozwala na integrację różnych macierzystych rozwiązań chmurowych w celu ochrony każdej aplikacji i każdego środowiska wdrożeniowego.

Oferowane przez Fortinet rozwiązania zabezpieczające zapewniają bezpieczeństwo sieci, widoczność i kontrolę w chmurach zarówno publicznych, jak i prywatnych. Zapory następnej generacji (NGFW) FortiGate są udostępniane w postaci maszyn wirtualnych, aby zapewnić automatyzację zabezpieczeń chmurowych, łączność z sieciami VPN, segmentację sieci, ochronę przed włamaniami oraz bezpieczną bramę sieciową.

Oprócz ochrony przed złośliwymi treściami, przedsiębiorstwo musi również zapewnić, że jego wdrożenia w chmurze są odpowiednio skonfigurowane. Błędy w konfiguracji zabezpieczeń są głównym problemem w przypadku chmury publicznej, przy czym aż 99% problemów nie jest zgłaszanych[34]. Usługa analizy bezpieczeństwa w chmurze **FortiCWP** zapewnia odpowiednią widoczność i kontrolę w infrastrukturze chmury publicznej, w tym pozwala na monitorowanie konfiguracji oraz zapewnienie bezpieczeństwa danych i zgodności z przepisami, a także na zintegrowane zarządzanie zagrożeniami.

Po zabezpieczeniu infrastruktury chmury należy jeszcze zabezpieczyć działające w niej aplikacje. Typowym przykładem zastosowania chmur publicznych jest hosting aplikacji sieciowych i sieciowych interfejsów API. W tym przypadku odpowiednią ochronę zapewni **FortiWeb** — zapora aplikacji WWW (WAF), która za pomocą kombinacji mechanizmów wykrywania sygnatur, uczenia maszynowego i sztucznej inteligencji chroni aplikacje WWW przed zarówno znanymi, jak i nieznanymi zagrożeniami. Ze względu na fakt, że większość aplikacji WWW wykorzystuje interfejsy API do łączenia się z usługami sieciowymi i integracji z innymi narzędziami, zapora FortiWeb ma również kluczowe znaczenie w zabezpieczeniu tych interfejsów za pomocą mechanizmów sprawdzania poprawności schematów i zabezpieczeń OpenAPI w celu ochrony przed potencjalnie złośliwymi działaniami botów (analiza i pozyskiwanie danych bezpośrednio ze stron WWW).

Przedsiębiorstwa coraz częściej wdrażają również chmurowe rozwiązania pocztowe, takie jak Google G Suite i Microsoft Office 365. Ze względu na fakt, że ataki phishingowe są główną przyczyną incydentów związanych z bezpieczeństwem i naruszeń ochrony danych, zabezpieczenie takiego chmurowego rozwiązania pocztowego jest niezbędne. Służy do tego **FortiMail** — dostępne w postaci urządzeń fizycznych i wirtualnych lub usługi hostowanej rozwiązanie chroniące zarówno chmurowe, jak i zainstalowane lokalnie aplikacje poczty elektronicznej. Pozwala ono między innymi na blokowanie tradycyjnych i zaawansowanych ataków prowadzonych za pośrednictwem poczty elektronicznej oraz tworzenie kopii zapasowych w celu zapobiegania utracie informacji wrażliwych.

Oprócz korzystania z aplikacji WWW i poczty elektronicznej, wiele przedsiębiorstw wdraża aplikacje SaaS, takie jak Google G Suite, Box, Microsoft Office 365, Dropbox i Salesforce. W tym kontekście zastosowanie znajduje chmurowe oprogramowanie pośredniczące (CASB) **FortiCASB**, które pozwala na zarządzanie ryzykiem związanym z błędną konfiguracją zabezpieczeń, zapewnia scentralizowaną widoczność i administracyjną kontrolę, chroni dane w aplikacjach SaaS oraz gwarantuje, że konfiguracje aplikacji SaaS są zgodne z przepisami.

Operacje zabezpieczające oparte na sztucznej inteligencji

Rosnąca skala i złożoność cyberataków sprawia, że tradycyjne cyberzabezpieczenia są niewystarczające. Systemy wykrywania złośliwego oprogramowania oparte na rozpoznawaniu sygnatur są zdolne do wykrycia tylko połowy złośliwych ataków[35]. Aby poprawić tę statystykę, niezbędne staje się zatem zastosowanie mechanizmów uczenia maszynowego i sztucznej inteligencji.

Dzięki rozwiązaniu **FortiGuard AI** przedsiębiorstwo nie da się wyprzedzić cyberprzestępcom. Dział FortiGuard Labs zbiera dane o zagrożeniach z milionów czujników na całym świecie i współpracuje z ponad 200 organizacjami międzynarodowymi. Za pomocą ponad 5 mld węzłów FortiGuard AI identyfikuje charakterystyczne cechy zarówno znanych, jak i nieznanych zagrożeń. Ilość danych przetwarzanych przez FortiGuard Labs jest ogromna: codziennie jest to ponad 100 mld zapytań sieciowych, przy czym co sekundę blokowanych jest ponad 3600 zapytań o złośliwe adresy URL.

W miarę wzrostu złożoności ataków całkowite im zapobieganie nie jest możliwe. Uzyskanie zdolności do wykrywania zaawansowanych zagrożeń staje się zatem niezbędne, aby uniknąć naruszeń. Zdolność taką zapewniają funkcje uczenia maszynowego i sztucznej inteligencji zintegrowane z rozwiązaniami **FortiDeceptor, FortiSandbox** i **FortiInsight**, które pomagają przedsiębiorstwom identyfikować nieznane zagrożenia i złośliwe oprogramowanie oraz wykrywać i odpowiednio reagować na zagrożenia wewnętrzne.

W miarę zwiększających się cyberzagrożeń przedsiębiorstwo musi w coraz większym stopniu automatyzować swoje procesy, aby szybciej powstrzymywać i eliminować te zagrożenia. Za pomocą rozwiązań **FortiSIEM** i **FortiAnalyzer** przedsiębiorstwo może zatem uzyskać pełną widoczność swojej infrastruktury sieci oraz dostęp do wyników analizy bezpieczeństwa przeprowadzonej za pomocą mechanizmów sztucznej inteligencji. Na podstawie zebranych danych analitycy, przy wsparciu „wirtualnego analityka" **FortiAI**, mogą wówczas określić charakter i skutki zagrożeń. Nie poprzestaje się jednak na wykrywaniu zagrożeń i zapobieganiu im; oferowane przez rozwiązanie **FortiSOAR** funkcje orkiestracji i automatyzacji pozwalają bowiem eliminować skutki włamań, co pomaga przeciążonemu pracą personelowi centrum zarządzania bezpieczeństwem (SOC) skupić się na identyfikacji zagrożeń i innych krytycznych zadaniach.

W procesie reagowania na incydenty punkty końcowe również wymagają pomocy ze strony mechanizmów sztucznej inteligencji. Rozwiązania **FortiEDR** — do wykrywania zagrożeń i reagowania na nie w punktach końcowych (EDR) — i FortiClient zapewniają zaawansowaną ochronę punktów końcowych, która obejmuje funkcje skanowania pod kątem luk w zabezpieczeniach, wdrażania poprawek, wirtualnego wdrażania poprawek oraz zapobiegania wykorzystaniu luk w zabezpieczeniach zarówno w środowiskach podłączonych i niepodłączonych do sieci. Ponadto w przypadku zainfekowania punktu końcowego rozwiązanie FortiEDR uniemożliwia złośliwemu oprogramowaniu komunikację z serwerami zarządzającymi i kontrolującymi oraz działanie w sieci wewnętrznej. FortiEDR oferuje również oparte na analizie ryzyka funkcje reagowania na zagrożenia i eliminacji ich skutków online z obsługą zautomatyzowanych procedur naprawczych.

Centrum zarządzania architekturą

Architektura Fortinet Security Fabric upraszcza zarządzanie całą architekturą zabezpieczeń przedsiębiorstwa dzięki integracji wszystkich wdrożonych w nim zabezpieczeń punktowych tak, aby mogły być centralnie zarządzane i monitorowane.

Platforma scentralizowanego zarządzania **FortiManager** oraz scentralizowane funkcje logowania i raportowania rozwiązania **FortiAnalyzer** zapewniają widoczność z poziomu jednej konsoli oraz możliwość zarządzania całą infrastrukturą sieci przedsiębiorstwa, w tym funkcje analizy, automatyzacji procesów i zarządzania z poziomu jednej konsoli.

Funkcje te są uzupełnione przez oparte na interfejsach API możliwości integracji z produktami partnerów Fortinet o statusie Fabric-Ready. Dwanaście takich konektorów zapewnia ścisłą integrację z rozwiązaniami innych producentów, a funkcje integracji oparte na interfejsach API są dostępne dla ponad 135 partnerów o statusie Fabric-Ready. Integracja z produktami niepochodzącymi od wspomnianych partnerów może być natomiast łatwo przeprowadzona za pomocą interfejsów API REST i skryptów DevOps.

Wiele przedsiębiorstw wdraża rozwiązania chmurowe, potrzebują zatem rozwiązania zapewniającego jeden punkt dostępu i możliwość jednokrotnego logowania w celu prostszego korzystania z wielu chmur. Rozwiązanie **FortiCloud** udostępnia taką funkcję jednokrotnego logowania oraz portale do 15 rozwiązań Fortinet SaaS i MaaS (Metal-as-a-Service), a także portal usługowy **FortiCare**. Dzięki obsłudze produktów oferowanych przez wszystkich głównych dostawców chmury publicznej architektura Fortinet Security Fabric upraszcza każde wdrożenie wielochmurowe.

Dzięki wdrożeniu rozwiązań FortiManager, FortiAnalyzer i FortiCloud przedsiębiorstwo może całkowicie zintegrować swoje zabezpieczenia zainstalowane lokalnie i w chmurze. Integracja taka pozwala na zastosowanie automatyzacji i orkiestracji w celu uproszczenia zarządzania tymi zabezpieczeniami. Ponadto za pomocą wspomnianych konektorów i interfejsów API dział IT może w czasie rzeczywistym otrzymywać informacje o stanie sieci oraz zautomatyzować zarządzanie dziennikami sieciowymi i uprościć raportowanie z poziomu jednej konsoli.

Zarządzanie ryzykiem i wykorzystanie okazji

Wdrożenie innowacji cyfrowych pozwala przedsiębiorstwu na zwiększenie swojej wydajności i oszczędności oraz na lepszą obsługę klientów. Działanie to zwiększa jednak powierzchnię ataku na sieć przedsiębiorstwa, otwierając cyberprzestępcom nowe ścieżki ataku.

Dla przedsiębiorstw będących liderami w zakresie wprowadzania innowacji cyfrowych kwestie identyfikacji i akceptacji ryzyka oraz właściwego nim zarządzania mają kapitalne znaczenie. Podstawowym narzędziem w tym kontekście jest architektura Fortinet Security Fabric. Ujednolica ona zarządzanie zabezpieczeniami w ramach jednej konsoli, zapewnia widoczność rosnącej cyfrowej powierzchni ataku, integruje funkcje zapobiegania włamaniom oparte na sztucznej inteligencji, a także automatyzuje operacje oraz procesy orkiestracji i reagowania na zagrożenia. Ogólnie rzecz biorąc, umożliwia przedsiębiorstwu elastyczniejsze, wydajniejsze i sprawniejsze działanie na bazie innowacji cyfrowych bez żadnego uszczerbku dla bezpieczeństwa.

[1] Nick Lansing, „Making Tough Choices: How CISOs Manage Escalating Threats And Limited Resources", Forbes i Fortinet, 2019 r.

[2] „The CIO and Cybersecurity: A Report on Current Priorities and Challenges", Fortinet, 23 maja 2019 r.

[3] Jeff Wilson, „The Bi-Directional Cloud Highway: User Attitudes about Securing Hybrid- and Multi-Cloud Environments", IHS Markit, 2019 r.

[4] Ibid.

[5] Gilad David Maayan, „The IoT Rundown For 2020: Stats, Risks, and Solutions", Security Today, 13 stycznia 2020 r.

[6] „2019 State of the Cloud Report", Flexera, 2019 r.

[7] Larry Ponemon, „Third-party IoT risk: companies don't know what they don't know", ponemonsullivanreport.com, dostęp z dnia 4 lutego 2020 r.

[8] Nirav Shah, „SD-WAN vs. MPLS: Why SD-WAN is a Better Choice in 2019", Fortinet, 9 września 2019 r.

[9] Kelly Bissell, et al., „The Cost of Cybercrime: Ninth Annual Cost of Cybercrime Study", Accenture Security and Ponemon Institute, 2019 r.

[10] „2019 Cost of a Data Breach Report", IBM Security and Ponemon Institute, 2019 r.

[11] „The CIO and Cybersecurity: A Report on Current Priorities and Challenges", Fortinet, 23 maja 2019 r.

[12] Dane wewnętrzne z FortiGuard Labs.

[13] „6 Obstacles to Effective Endpoint Security: Disaggregation Thwarts Visibility and Management for IT Infrastructure Leaders", Fortinet, 8 września 2019 r.

[14] Dane z wewnętrznych badań Fortinet.

[15] Dane wewnętrzne z FortiGuard Labs.

[16] Kelly Bissell, et al.,„The Cost of Cybercrime: Ninth Annual Cost of Cybercrime Study", Accenture Security and Ponemon Institute, 2019 r.

[17] „2019 Cost of a Data Breach Report", IBM Security and Ponemon Institute, 2019 r.

[18] Dane z wewnętrznych badań Fortinet.

[19] „The CIO and Cybersecurity: A Report on Current Priorities and Challenges", Fortinet, 23 maja 2019 r.

[20] Kacy Zurkus, „Defense in depth: Stop spending, start consolidating", CSO, 14 marca 2016 r.

[21] „The CIO and Cybersecurity: A Report on Current Priorities and Challenges", Fortinet, 23 maja 2019 r.

[22] „Strategies for Building and Growing Strong Cybersecurity Teams: (ISC)² Cybersecurity Workforce Study, 2019", (ISC)², 2019 r.

[23] „CIO Survey 2019: A Changing Perspective", Harvey Nash i KPMG, 2019 r.

[24] „2019 Payment Security Report", Verizon, 2019 r.

[25] Jeff Wilson, „The Bi-Directional Cloud Highway: User Attitudes about Securing Hybrid- and Multi-Cloud Environments", IHS Markit, 2019 r.

[26] „Making Tough Choices: How CISOs Manage Escalating Threats And Limited Resources", Forbes i Fortinet, 2019 r.

[27] „Independent Validation of Fortinet Solutions: NSS Labs Real-World Group Tests", Fortinet, 14 października 2019 r.

[28] „2019 Cost of a Data Breach Report", IBM Security and Ponemon Institute, 2019 r.

[29] „Independent Validation of Fortinet Solutions: NSS Labs Real-World Group Tests", Fortinet, 14 października 2019 r.

[30] „Gartner Magic Quadrant Reports", Fortinet, dostęp z dnia 22 stycznia 2020 r.

[31] „2019 Data Breach Investigations Report", Verizon, 2019 r.

[32] Alex Samonte, „TLS 1.3: What This Means For You", Fortinet, 15 marca 2019 r.

[33] Robert Lemos, „Attackers Are Messing with Encryption Traffic to Evade Detection", Dark Reading, 15 maja 2019 r.

[34] Charlie Osborne, „99 percent of all misconfigurations in the public cloud go unreported", ZDNet, 24 września 2019 r.

[35] Robert Lemos, „Only Half of Malware Caught by Signature AV", Dark Reading, 11 grudnia 2019 r.

lipca 7, 2020 12:06 PM

570099-0-0-PL

wp-FA-fortinet-security-fabric-enables-digital-innovation-2132020-129AM_PL