OPIS ROZWIĄZANIA

Niezawodna elastyczna ochrona dzięki rozwiązaniu Fortinet Dynamic Cloud Security

Streszczenie

Rosnące wykorzystanie chmury publicznej, zarówno w kontekście całkowitego wolumenu, jak i dywersyfikacji usług, nie jest tendencją jednokierunkową. Aby zaspokajać zmieniające się potrzeby biznesowe, przedsiębiorstwa stale przenoszą aplikacje i procesy między środowiskiem chmury a środowiskiem lokalnym i na odwrót. Tendencja ta została potwierdzona przez 74% respondentów niedawnego badania[1]. Aby zminimalizować potencjalne skutki wykorzystania luk w zabezpieczeniach tego dynamicznego środowiska, niezbędne jest ścisłe monitorowanie ruchu sieciowego, transakcji wykonywanych za pomocą stosowanych aplikacji oraz działania i konfiguracji platformy chmurowej. Służy do tego rozwiązanie Fortinet Dynamic Cloud Security, które oferuje macierzyście zintegrowane rozwiązania zabezpieczające sieci, aplikacje i platformy, aby ułatwiać i rozszerzać innowacje cyfrowe.

Zaspokajanie potrzeb dotyczących sieci chmur dynamicznych

Na bazie szerokiego, zintegrowanego i zautomatyzowanego charakteru architektury Fortinet Security Fabric rozwiązanie Fortinet Dynamic Cloud Security oferuje spójne zabezpieczenia i mechanizmy egzekwowania zasad bezpieczeństwa w formie ujednoliconego zarządzania bezpieczeństwem w ramach dowolnej infrastruktury chmurowej lub niechmurowej.

- W przypadku **chmur prywatnych** oferowane przez Fortinet rozwiązania zabezpieczające sieci, aplikacje i platformy mogą zostać bezproblemowo zintegrowane z systemami automatyzacji infrastruktury w celu egzekwowania zasad bezpieczeństwa uwzględniających dynamiczny charakter maszyn wirtualnych i innych procesów.
- W przypadku **chmur publicznych** oferowane przez Fortinet rozwiązania zabezpieczające sieci, aplikacje i platformy mogą zostać zintegrowane z chmurowymi usługami sieciowymi. Interfejsy programowania aplikacji (API) i chmurowe mechanizmy równoważenia obciążenia zapewniają kompleksowe bezpieczeństwo obejmujące całą powierzchnię ataku.
- W przypadku **chmur SaaS** oferowane przez Fortinet rozwiązania zapewniają widoczność i kontrolę przez integrację z interfejsem API chmury w celu ograniczenia ryzyka związanego z błędnymi konfiguracjami chmury SaaS.

Ujednolicona ochrona w ramach wszystkich dużych chmur obliczeniowych

Zmieniające się metody włamań wymagają zastosowania odpowiedniej ochrony przed zaawansowanymi zagrożeniami zdolnej do głębokiej weryfikacji zaszyfrowanego ruchu sieciowego i wykrywania zagrożeń typu „zero-day". Rozszerzając podstawowe zdolności macierzystych mechanizmów bezpieczeństwa dostawców chmur, oferowane przez Fortinet rozwiązanie zapewnia szeroki zestaw funkcji bezpieczeństwa obejmujący następujące elementy:

Bezpieczeństwo sieci dzięki zaporom następnej generacji (NGFW) FortiGate VM

- **Segmentacja sieci** chroni zarówno ruch z chmury do Internetu (północ-południe), jak i poboczny ruch z chmury do chmury lub wewnątrz chmury (wschód-zachód), zapewniając przewidywalną wydajność aplikacji. Zarządzane centralnie za pośrednictwem architektury Fortinet Security Fabric wirtualne zapory następnej generacji Fortinet spójnie stosują zasady zabezpieczeń we wszystkich hybrydowych środowiskach wielochmurowych. Wdrożone w chmurze publicznej rozwiązania FortiGate VM mogą bezpiecznie komunikować się

Fortinet Dynamic Cloud Security to rozwiązanie, które znacznie odchodzi od podejścia polegającego na zabezpieczeniach punktowych i zapewnia przedsiębiorstwom spójną ochronę w każdym miejscu, aby mogły bezpiecznie uruchamiać dowolne aplikacje w dowolnym miejscu.

Obsługiwane duże chmury publiczne

- Amazon Web Services (AWS)
- Microsoft Azure
- Google Cloud Platform
- Oracle Cloud
- Alibaba Cloud
- IBM

Obsługiwani dostawcy technologii chmur prywatnych

- VMware
- Microsoft
- Xen
- KVM
- Cisco
- OpenStack

i współdzielić spójne zasady z zaporami FortiGate NGFW o dowolnych parametrach stosowanymi w prywatnym centrum przetwarzania danych.

- **Mechanizmy zapobiegania zaawansowanym zagrożeniom**, korzystające m.in. z udostępnianych w rozwiązaniu FortiGate VM funkcji kontroli aplikacji i ochrony przed włamaniami (IPS), pomagają przedsiębiorstwom uniemożliwiać pojawiającym się w warstwie aplikacji zagrożeniom propagowanie się i niszczenie infrastruktur chmurowych. Udostępniane w rozwiązaniu FortiGate VM funkcje zapobiegania zaawansowanym zagrożeniom skutecznie blokują natomiast znane ataki.
- **Bezpieczna sieć SD-WAN** (definiowana programowo sieć rozległa) łączy w jednym chmurowym rozwiązaniu funkcje rozpoznawania ścieżek sieciowych z funkcjami bezpieczeństwa. Rozwiązanie Fortinet Secure SD-WAN pomaga przedsiębiorstwom uprościć łączność w chmurze przy jednoczesnym zapewnieniu bezpieczeństwa i obniżeniu kosztów, niezależnie od tego, czy sieć SD-WAN jest używana do łączenia ze sobą oddziałów w chmurze, czy do łączenia chmur z centrami przetwarzania danych.

Zapewnienie bezpieczeństwa aplikacji WWW za pomocą zapór aplikacji WWW (WAF)

W ramach wielowarstwowego podejścia opartego na uczeniu maszynowym rozwiązanie FortiWeb chroni przed znanymi zagrożeniami (na przykład OWASP Top 10) i atakami typu „zero-day" zarówno aplikacje WWW, jak i zewnętrzne interfejsy API. Korzystając z funkcji uczenia maszynowego, rozwiązanie FortiWeb identyfikuje nietypowe zachowania i ocenia, czy mają charakter złośliwy, czy niezłośliwy. W ten sposób można automatycznie uczyć aplikacje szybciej i dokładniej niż w przypadku ich ręcznego uczenia wymaganego przez większość zapór aplikacji WWW. Ponadto zaawansowane funkcje neutralizowania aktywności botów pozwalają na korzystanie z niezłośliwych botów, takich jak wyszukiwarki internetowe, przy jednoczesnym blokowaniu aktywności botów złośliwych. Warto również zauważyć, że w odpowiedzi na wymagania różnych klientów, rozwiązanie FortiWeb jest oferowane w ramach łatwego w użyciu modelu SaaS, jako kontener na platformie Docker lub jako maszyna wirtualna.

Widoczność ta pomaga administratorom zabezpieczeń i zespołom DevOps w efektywnej ocenie stanu bezpieczeństwa konfiguracji chmury, wykrywaniu potencjalnych zagrożeń wynikających z błędnej konfiguracji zasobów chmury, identyfikacji przypadków naruszeń zasad oraz generowaniu raportów dotyczących zgodności z przepisami.

Modele korzystania z rozwiązania Fortinet Dynamic Cloud Security

Fortinet Dynamic Cloud Security obejmuje rozwiązania FortiCWP, FortiWeb i FortiGate VM, które są dostępne w wielu formatach, takich jak maszyny wirtualne, narzędzia SaaS i kontenery Docker, aby jak najlepiej pasować do potrzeb i zastosowań zgłaszanych przez klientów. Ponadto różne rozwiązania są dostępne w modelu korzystania z licencji prywatnych do celów służbowych (bring-your-own-license, BYOL). Rozwiązania te można nabyć w ramach zwykłego łańcucha dostaw w chmurze, zazwyczaj na mocy licencji bezterminowych lub w modelu płatności za wykorzystanie (pay-as-you-go, PAYG).

Szeroki zakres formatów i opcji obniża całkowity koszt posiadania

Rozwiązania Fortinet Dynamic Cloud Security mogą obsługiwać szeroki zakres wymagań dotyczących zasobów i wydajności. Obejmuje on zarówno maszyny wirtualne o bardzo małych rozmiarach, które maksymalizują korzyści wynikające z architektur skalowanych w poziomie, jak i maszyny wirtualne o dużych rozmiarach, które korzystają z technologii akceleracji sieci o dużej pojemności w ramach różnych platform chmurowych i umożliwiają obsługę szeroko zakrojonego przetwarzania sieciowego na potrzeby aplikacji stanowych, które nie mogą być odpowiednio zaprojektowane przy użyciu architektur skalowanych w poziomie.

Macierzysta integracja optymalizuje mechanizmy zabezpieczeń w ramach hybrydowego ekosystemu wielochmurowego

Luki w zabezpieczeniach powstają w wyniku niezgodności zarówno między środowiskiem chmury a środowiskiem lokalnym, jak również między narzędziami chmurowymi a specjalnymi narzędziami bezpieczeństwa. Aby zminimalizować te luki, architektura Fortinet Security Fabric zapewnia spójność architektoniczną za pomocą integracji właściwych dla chmury. Integracje te sprawiają, że specjaliści ds. zabezpieczeń nie muszą znać konkretnych typów obiektów i konwencji nazewnictwa właściwych dla każdego środowiska chmurowego, elementy te są bowiem zastępowane przez jeden intuicyjny interfejs konfiguracyjny. Rozwiązania Fortinet oferują trzy rodzaje integracji:

- **Adaptery Fabric Connector** tłumaczą właściwe dla chmury obiekty bezpieczeństwa i nazwy usług na spójny format służący do zdefiniowania reguł zabezpieczeń w ramach całej architektury Fortinet Security Fabric.
- **Interfejsy API Fabric** standaryzują programowanie operacji zarządzania bezpieczeństwem w produktach Fortinet wdrożonych lokalnie i w chmurze.
- **Konfigurowane automatyczne reakcje** na wykryte przez produkty Fortinet zdarzenia dotyczące bezpieczeństwa mogą inicjować działania naprawcze bezpośrednio na różnych platformach chmurowych, wykorzystując funkcje tworzone bez konieczności posiadania przez operatora zabezpieczeń specjalistycznej wiedzy z zakresu działania chmury (serverless).

Wszystkie adaptery i interfejsy API firmy Fortinet zostały opracowane w ramach ścisłej współpracy z dostawcami usług chmurowych i są regularnie aktualizowane zgodnie ze zmianami zachodzącymi w poszczególnych środowiskach chmurowych.

Rys. 1. Elastyczność biznesowa zapewniana przez rozwiązanie Fortinet Dynamic Cloud Security.

Zarządzanie i automatyzacja

Przedsiębiorstwa stoją w obliczu coraz większych zagrożeń i trwałych niedoborów specjalistów ds. zabezpieczeń, Fortinet Dynamic Cloud Security oferuje im zatem mechanizmy zarządzania bezpieczeństwem i automatyzacji, które w jednolity sposób obejmują całe środowiska chmurowe. Mechanizmy te pomagają uzyskać odpowiedni poziom widoczności całej infrastruktury wielochmurowej, co warunkiem niezbędnym do zdefiniowania skutecznych zasad bezpieczeństwa i ostatecznego uzyskania kontroli nad całą infrastrukturą.

Wspomniane mechanizmy pomagają operatorom i administratorom zabezpieczeń w usprawnieniu rutynowych operacji z poziomu jednej konsoli. Udostępniają również interfejsy API, które pomagają zespołom DevOps i DevSecOps zautomatyzować operacje zarządzania bezpieczeństwem dla wszystkich rutynowych działań bez potrzeby jakichkolwiek dostosowań właściwych dla chmury. Mechanizmy te zatem nie tylko zwiększają efektywność operacyjną, ale także obniżają koszty szkoleń i rekrutacji, ponieważ w kontekście wszystkich chmur można korzystać z tych samych umiejętności zapewnienia bezpieczeństwa. Rozwiązania Fortinet Dynamic Cloud Security po prostu pomagają przedsiębiorstwom w zapewnieniu większego bezpieczeństwa sieci, aplikacji i platform chmurowych przy minimalnych kosztach ogólnych.

Opłacalne rozwiązania w zakresie bezpieczeństwa

Innowacje cyfrowe wymagają zabezpieczeń, które nadążą za tempem rozwoju infrastruktur chmury dynamicznej. Rozwiązania Fortinet Dynamic Cloud Security oferują następujące korzyści dla przedsiębiorstw, które chcą szybko i długoterminowo zaspokajać potrzeby swoje i swoich klientów:

- Możliwość skalowania od najmniejszych jednostek do największych wirtualnych urządzeń sieciowych o dużej pojemności (NVA)
- Łatwa adaptacja do różnych zastosowań i potrzeb bezpieczeństwa właściwych dla aplikacji lub prowadzonej działalności
- Technologie zabezpieczeń wykorzystujące najnowsze osiągnięcia w dziedzinie uczenia maszynowego i sztucznej inteligencji w celu zapewnienia infrastrukturom chmur dynamicznych stale optymalizowaną ochronę aplikacji WWW przed szybko zmieniającymi się zagrożeniami
- Oparte na prawdziwej synergii strukturalne podejście do bezpieczeństwa, które integruje bezpieczeństwo sieci, aplikacji i platform chmurowych w ramach jednego systemu, aby poprawić bezpieczeństwo sieci przedsiębiorstwa i uczynić je mniej podatnymi na błędy ludzkie

Wielokrotnie weryfikowane przez zaufane organizacje zewnętrzne składniki architektury Fortinet Security Fabric zostały wdrożone u ponad 425 tys. klientów na całym świecie[2]. Sukces ten w połączeniu z działaniami firmy Fortinet skupionymi na nieprzerwanie intensywne inwestycje w rozwój zabezpieczeń chmury, daje specjalistom ds. bezpieczeństwa pewność, że za pomocą rozwiązania Fortinet Dynamic Cloud Security będą mogli wdrożyć dowolne aplikacje w dowolnych chmurach.

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

[2] „Powering WAN Edge Transformation: Integrated Security and SD-WAN", Fortinet, IV kwartał 2019 r.

FORTINET

www.fortinet.com

23 kwietnia, 2020 9:40 AM

500499-0-1-PL

sb-FA-fortinet-dynamic-cloud-security-provides-seamless-flexible-protection-A4_PL