
FORTINET
OCHRONA SIECI
DLA KAŻDEJ CHMURY

SPIS TREŚCI

WSTĘP

W przypadku każdej odmiany chmury stosowane zabezpieczenia muszą spełniać inne, specyficzne wymagania. **Chmury publiczne** opierają się na infrastrukturze współdzielonej i dlatego muszą korzystać z jednego modelu zabezpieczeń. **Chmury prywatne** wymagają zabezpieczeń opartych na oprogramowaniu ze względu na brak widoczności ruchu między maszynami wirtualnymi (wschód-zachód) oraz usług wirtualnych. Trudność w zabezpieczaniu **chmur hybrydowych** polega na tym, że łączą one istotne zasoby wewnętrzne z zewnętrznymi łączami i źródłami danych, co zwiększa potrzebę segmentowania zasobów w sieci.

Rola dzisiejszych zabezpieczeń chmur nie ogranicza się tylko do ochrony przed atakami. Podczas ich opracowywania należy założyć, że prędzej czy później zostaną one w jakimś stopniu złamane – dlatego powinny pozostać odporne, by zagwarantować ochronę zasobów i użytkowników.

01 OCHRONA DOPASOWANA DO KONCEPTU CHMURY

Oferowane przez Fortinet zabezpieczenia chmur odzwierciedlają ich naturę, dzięki czemu są wystarczająco dynamiczne, by móc szybko się zmieniać w celu zapewnienia ochrony ich różnych wdrożeń – publicznych, prywatnych i hybrydowych.

Skalowalność – funkcje ochrony muszą reagować na skalowalność i elastyczność przepływów pracy w chmurze. Dlatego też kluczową funkcją zabezpieczeń chmurowych Fortinet jest automatyzacja. Zasady dotyczące ryzyka i dostępu są definiowane z góry, dzięki czemu urządzenia nowych użytkowników czy dodatkowe systemy zwiększające przepustowość środowiska chmury są konfigurowane automatycznie.

Jedna konsola – zasady, metody ich egzekwowania oraz automatyzacja muszą w równym stopniu obejmować zasoby statyczne i dynamiczne, zapewniając przy tym wgląd w ogólny stan ich zabezpieczeń z jednego miejsca. Nasze rozwiązanie jednakowo traktuje przepływy pracy i systemy o wspólnym profilu ryzyka, gdy dołączają do sieci i się od niej odłączają, niezależnie od tego, czy znajdują się one we własnym centrum danych firmy czy w centrum danych dostawcy.

Segmentacja – możliwość segmentowania systemów, przepływów pracy, a nawet poszczególnym komponentów sieciowych ma znaczenie krytyczne, jeśli chodzi o zarządzanie ryzykiem biznesowym. Stosowanie chmury przynosi nowe wątpliwości dotyczące zgodności z przepisami. W sytuacji, gdy dane mogą przemieszczać się w sieci, a nawet ją opuszczać przez chmurę prywatną, konieczne jest egzekwowanie ich zgodności z obowiązującymi przepisami w celu zagwarantowania możliwości monitorowania i kontrolowania konkretnych pakietów, aplikacji czy typów danych.

02 OCHRONA CHMUR PUBLICZNYCH

Najpoważniejsze obawy dotyczące bezpieczeństwa wzbudzają chmury publiczne. Dopiero niedawno liderzy biznesowi i użytkownicy zaczęli dopuszczać możliwość rezygnacji z kontroli nad wykorzystywaną infrastrukturą oraz współdzielenia systemów i przepustowości z nieznanymi osobami.

Rozwiązanie do ochrony chmur firmy Fortinet zapewnia bezpieczeństwo przepływów pracy w chmurach publicznych, gwarantując z jednej strony prywatność i poufność, a z drugiej – zalety płynące ze skalowalności, możliwości dokonywania pomiarów i szybkiego wprowadzania produktów na rynek.

Model ochrony współdzielonej – model ochrony współdzielonej udostępnia dwie kluczowe funkcje:

- Ochronę **„chmury”** obejmującą wszystkie centra danych udostępniane przez usługodawcę, do których ochrony jest zobowiązany.
- Ochronę **„w chmurze”** obejmującą wszystkie dane i aplikacje przechowywane w chmurze przez użytkownika subskrybującego usługi chmurowe, do których ochrony jest on zobowiązany.

Oferowane przez Fortinet zabezpieczenia chmur chronią komponenty klienta, takie jak dane i aplikacje, systemy operacyjne, systemy zarządzania dostępem i tożsamością, szyfrowanie i ruch sieciowy. Uzupełniają w ten sposób funkcje zabezpieczeń stosowane przez dostawcę, tworząc wspólnie kompleksowy i zgodny z przepisami system ochrony.

Integracja dostawcy – nasze rozwiązanie zostało też opracowane pod kątem ścisłej integracji z infrastrukturą zabezpieczeń dostawcy chmury publicznej, co umożliwia ochronę mocy obliczeniowej, pamięci masowej i połączeń sieciowych. Udostępnia poza tym jeden pulpit, na którym można wyświetlać obie strony i zarządzać wszystkimi aspektami ochrony.

Oferowane przez Fortinet zabezpieczenia chmur publicznych obejmują:

- Obsługę wszystkich pięciu najpopularniejszych platform chmur publicznych: AWS, Azure, Google, IBM i Oracle.
- Obsługę czołowych platform umożliwiających pracę w modelu Software-as-a-Service (oprogramowanie jako usługa), takich jak Office 365 i Salesforce.com. SaaS to inna główna forma chmury publicznej, która wymaga ochrony w takim samym stopniu co IaaS – Infrastructure-as-a-Service (infrastruktura jako usługa).
- Obsługę chmur używanych przez wiele podmiotów oraz domen wirtualnych umożliwiających segmentację sieci.
- Natywną synchronizację chmury, która pozwala na automatyczne skalowanie, zapewnianie wysokiej dostępności oraz segmentację.
- Rozbudowywany interfejs do zarządzania – interfejsy API umożliwiające dodatkową automatyzację i synchronizację chmury.

03 OCHRONA CHMUR PRYWATNYCH

Elementem, na który należy zwrócić szczególną uwagę w kontekście zabezpieczeń chmur prywatnych, jest wirtualizacja, ponieważ to właśnie na niej opierają się wszystkie formy przetwarzania w chmurze. Stanowi ona podstawę dla ułożonych warstwowo sieci sterowanych programowo (Software-Defined Networking, SDN) i innej infrastruktury opartej na oprogramowaniu, które razem tworzą dynamiczne chmury prywatne wykraczające poza granice tradycyjnych centrów danych.

Rozwiązanie Software-Defined Security firmy Fortinet uzyskało certyfikację czołowych platform SDN i wirtualizacji funkcji sieciowych (NFV), dzięki czemu można je stosować w każdym centrum danych przekształconym w środowisko chmurowe.

Software-Defined Security – rozwój sieci sterowanych programowo sprawił, że zasoby sieciowe nie są już fizycznie połączone z konkretnymi urządzeniami. Działają raczej jako usługi w centrum danych, które można uruchamiać na różnych elementach fizycznych i w różnych lokalizacjach. Zabezpieczenia chmur prywatnych firmy Fortinet też zostały opracowane tak, by świadczyć „usługi" ochrony, które można dynamicznie konfigurować i przydzielać. Takie rewolucyjne podejście pozwala na objęcie ochroną wszystkich koncepcyjnych warstw architektury sieciowej – od płaszczyzny danych, przez płaszczyznę kontroli, po płaszczyznę zarządzania.

Zabezpieczenia skoncentrowane na aplikacjach – chociaż wiele aplikacji korzysta z tej samej infrastruktury fizycznej w chmurze prywatnej, związane z nimi zagrożenia są różne. Zabezpieczenia chmur firmy Fortinet izolują dane i aplikacje w podlegających nieustannej konsolidacji centrach danych. Przy coraz większym ruchu między maszynami wirtualnymi w środowiskach zarządzanych programowo (wschód-zachód) nasze rozwiązanie zapewnia funkcje mikrosegmentacji, która pozwala jeszcze precyzyjniej rozdzielać poszczególne rodzaje ruchu.

Oferowane przez Fortinet zabezpieczenia chmur prywatnych obejmują:

- Obsługę czołowych platform SDN, w tym VMware NSX, Cisco ACI i OpenStack.
- Dodatkową synchronizację wirtualizacji funkcji sieciowych (NFV) na potrzeby akwizycji i sekwencjonowania usług w chmurach i środowiskach dostawców obsługujących wielu użytkowników.
- Obsługę wielu użytkowników i domen wirtualnych na potrzeby segmentacji sieci i wdrażania funkcji usług ochrony.
- Rozbudowywany interfejs do zarządzania – interfejsy API umożliwiające automatyzację i synchronizację chmury.
- Możliwość zarządzania z poziomu jednej konsoli.
- Niezrównany wybór produktów i usług oraz elastyczne opcje wdrażania.

04 CHMURA HYBRYDOWA

Większość organizacji przechodzi właśnie z centrów danych znajdujących się w ich siedzibach na usługi chmur publicznych, planując zarazem utrzymanie zarówno konwencjonalnego środowiska informatycznego, jak i wdrożenia chmury. Utworzenie chmury hybrydowej wymaga otwartej i bezpiecznej migracji dużych ilości danych i aplikacji, niezawodnej łączności między ośrodkami oraz rozciągnięcia topologii sieciowych na sieć WAN.

Rozwiązanie przeznaczone do chmur hybrydowych firmy Fortinet zapewnia działom ds. zabezpieczeń wgląd w cały ten obraz sieci, w tym możliwości kompleksowego zarządzania, segmentacji i ochrony połączeń zewnętrznych.

Zarządzanie z poziomu jednej konsoli – gdy zasoby znajdują się zarówno w obszarze fizycznym, jak i wirtualnym, specjaliści ds. bezpieczeństwa potrzebują jednego punktu, który zapewni im wgląd w ich działanie, oraz centralnych funkcji analitycznych informujących o zagrożeniach. Rozwiązanie do chmur hybrydowych firmy Fortinet zapewnia zintegrowany widok wszystkich systemów działających w chmurze oraz pozwala na centralne zarządzanie nimi. Umożliwia to śledzenie przepływów danych w całej sieci w formie, dzięki której podawane informacje są istotne i użyteczne.

Segmentacja – zabezpieczenia chmur hybrydowych Fortinet identyfikują jednostki biznesowe i krytyczne aplikacje niepowiązane bezpośrednio z mieszanymi środowiskami hybrydowymi oraz dzielą je na segmenty, by zminimalizować szkody w przypadku złamania ich zabezpieczeń. Umożliwiają również kontrolowanie stałego ruchu między segmentami chmury, co chroni przed utratą danych oraz zapewnia ich przesyłanie na podstawie określonych zasad i poziomu ryzyka.

Bezpieczna łączność – przenoszenie danych między różnymi lokalizacjami, ładowanie dużych zbiorów danych ze źródeł zewnętrznych oraz korzystanie z chmurowych usług analitycznych obsługiwanych przez inne firmy wymaga bezpiecznych połączeń z sieciami zewnętrznymi. Nasze rozwiązanie zapewnia właściwą ochronę takich niepowtarzalnych połączeń sieciowych, opartą na ich profilu ryzyka. Umożliwia także korzystanie z wydajnych funkcji sieci VPN, w tym też zapewnianie bezpiecznego dostępu tymczasowego do potrzebnych zasobów przy jednoczesnej ochronie reszty sieci.

Oferowane przez Fortinet zabezpieczenia chmur hybrydowych obejmują:

- Funkcje automatycznego skalowania wydajności zabezpieczeń sieciowych i planowania pojemności.
- Możliwość scentralizowanego zarządzania i automatycznej obsługi administracyjnej.
- Łączność między ośrodkami przez sieć VPN.
- Segmentację stałych połączeń.
- Pełną widoczność i kontrolę dzienników zabezpieczeń ułatwiającą zachowanie zgodności z przepisami.

PODSUMOWANIE

Fortinet jest jedyną firmą, która oferuje zabezpieczenia sieci, punktów końcowych, aplikacji, centrów danych, chmur i dostępu opracowane pod kątem współpracy w ramach zintegrowanej infrastruktury zabezpieczeń gwarantującej rzeczywistą, kompleksową ochronę.

Nasze specjalnie opracowane zabezpieczenia współpracują z kluczowymi produktami Fortinet w różnych modelach wdrożenia środowisk chmurowych, umożliwiając jednocześnie scentralizowane zarządzanie, otwartą integrację za pomocą interfejsów API, pomiary wykorzystania, synchronizację platform chmurowych i automatyzację.

Fabryka bezpieczeństwa Fortinet dynamicznie udostępnia informacje o zagrożeniach pozostałym systemom składającym się na połączoną infrastrukturę zabezpieczeń. Pozwala to znacznie ograniczyć liczbę punktów kontrolnych i nadmiarowych zasad w obiektach chmurowych oraz zapewnia kontrolę nad granicami wielowarstwowych zabezpieczeń.

www.fortinet.com