NAJWAŻNIEJSZE ZASADY I STRATEGIE ZABEZPIECZENIA CHMURY PRZEDSIĘBIORSTWA

Plan zapewnienia bezpieczeństwa w chmurze



STRESZCZENIE

Przedsiębiorstwa w coraz większym stopniu wdrażają różne procesy w wielu chmurach. Z kolei dane i usługi o znaczeniu krytycznym dla prowadzonej działalności są coraz bardziej rozrzucone po całej takiej rozproszonej infrastrukturze. Na bazie modelu współdzielonej odpowiedzialności jako zasady przewodniej przedsiębiorstwa pozostawiają ochronę sieci, pamięci masowej i warstw obliczeniowych w gestii dostawców chmur, natomiast same (lub ich użytkownicy końcowi) zajmują się zabezpieczeniem wszystkiego, co zostało zbudowane, wdrożone lub zapisane w chmurze. Ze względu na korzystanie z wielu chmur w większości przedsiębiorstw istnieją środowiska heterogeniczne, w ramach których narzędzia z poszczególnych rozwiązań chmurowych znacznie się od siebie różnią.

Taki stan rzeczy sprawia, że infrastruktura zabezpieczeń sieci w przedsiębiorstwach jest zazwyczaj złożona i niejednolita. Jedynym realnym rozwiązaniem tego problemu jest zastosowanie jednolitego rozwiązania w zakresie bezpieczeństwa, które będzie obsługiwać różne platformy chmurowe. W kontekście wdrażania aplikacji w chmurze przedsiębiorstwa muszą zatem stosować zabezpieczenia, które będą się cechować trzema kluczowymi atrybutami: 1) zdolnością do bezpośredniej integracji z produktami wszystkich głównych dostawców chmury, 2) posiadaniem szerokiego zestawu narzędzi zabezpieczających całą powierzchnię ataku oraz 3) możliwością centralnego zarządzania infrastrukturą zabezpieczeń i automatyzowania procesów bezpieczeństwa. Ponadto rozwiązania te muszą zapewniać jednolitą widoczność, kontrolę oraz możliwość zarządzania zasadami i zapewnienia zgodności z przepisami. Ponadto odpowiednia architektura zabezpieczeń musi radzić sobie z wieloma różnymi sytuacjami związanymi z bezpieczeństwem w kontekście różnych używanych przez przedsiębiorstwo chmur.

Przedsiębiorstwo korzysta średnio z **61** różnych aplikacji chmurowych, które stanowią 1/3 wszystkich używanych w nim aplikacji[1].

OPRACOWANIE

Transformacja cyfrowa (DX) jest źródłem niespotykanego do tej pory wzrostu akceptacji chmury i wiele przedsiębiorstw coraz większą liczbę swoich operacji biznesowych obsługuje w chmurze. Heterogeniczność powstających w ten sposób środowisk chmurowych zwiększa całkowitą powierzchnię ataku. W efekcie ochrona wspomnianych wdrożeń chmurowych staje się coraz trudniejsza. I choć w ciągu ostatniej dekady zaufanie publiczne do chmury istotnie wzrosło, bezpieczeństwo pozostaje jednym z głównych problemów dla liderów biznesowych i technologicznych w kontekście akceptacji chmury. W związku z tym kluczowe znaczenie ma uwzględnienie aspektów bezpieczeństwa już na etapie projektowania konkretnego rozwiązania chmurowego i całościowej infrastruktury chmurowej w przedsiębiorstwie.

MODEL WSPÓŁDZIELENIA ODPOWIEDZIALNOŚCI ZA BEZPIECZEŃSTWO CHMURY

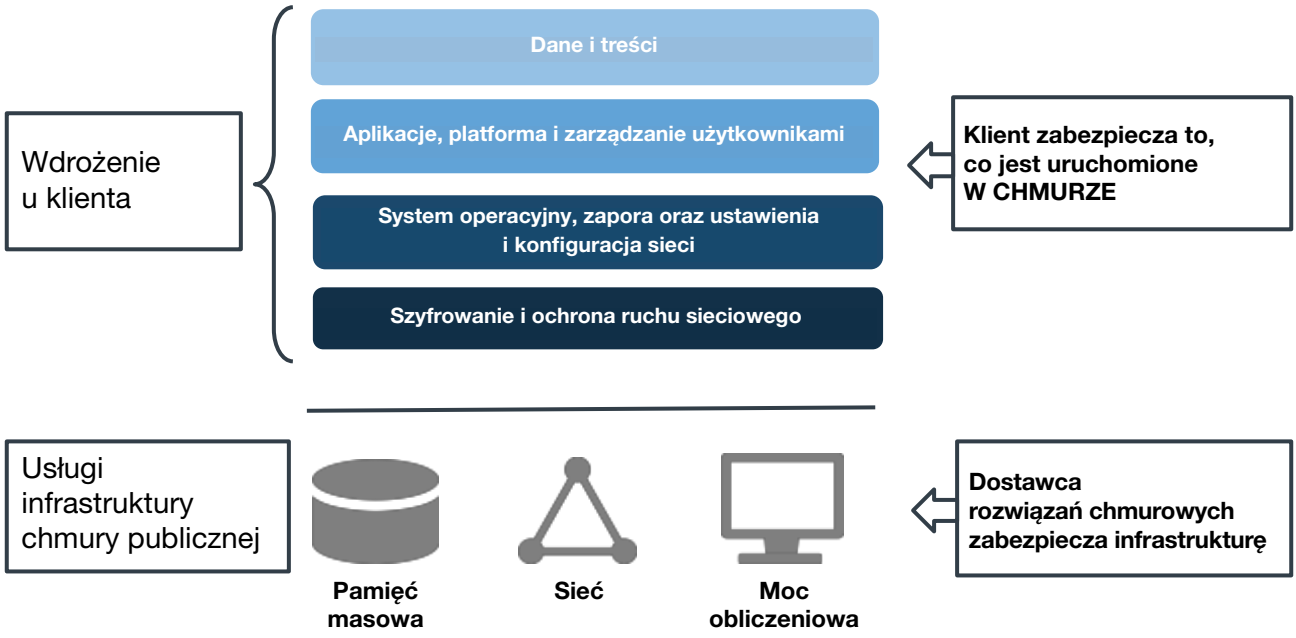
Dostawcy rozwiązań chmurowych dokładają wszelkich starań, aby chronić swoją infrastrukturę, ochrona danych i aplikacji hostowanych lub wdrażanych w chmurze leży jednak w gestii klienta (użytkownika końcowego). Mimo to klienci nie są w stanie wywiązać się ze swoich obowiązków (według prognoz do 2023 r. klienci będą odpowiedzialni za 99% przypadków awarii chmury). W wielu przypadkach sprawcą będzie błąd ludzki, który można przypisać niezrozumieniu modelu współdzielonej odpowiedzialności między dostawcami rozwiązań chmurowych a ich klientami[2].

Model współdzielonej odpowiedzialności jest często opisywany analogicznie do warstwowego modelu łączenia systemów otwartych (OSI). W tym przypadku dostawcy rozwiązań chmurowych chronią niższe warstwy fizyczne, zadaniem klientów jest natomiast ochrona warstw wyższych. Wspomniany model OSI nie zawsze bywa jednak wystarczający do opisania złożonych stosunków i obowiązków w zakresie bezpieczeństwa chmury. Na przykład klienci mogą tworzyć sieci nakładające się na sieć dostawcy rozwiązań chmurowych lub tworzyć inne warstwy abstrakcyjne, które pozwolą „złożyć" usługę z dostępnych jej elementów. Pomimo tych niuansów klient odpowiada za zabezpieczenie wszystkiego, co dodaje do infrastruktury chmurowej, i wszystkiego, czym zarządza w ramach tego środowiska chmury. Ponadto obecnie klienci muszą zabezpieczyć warstwę interfejsów API / zarządzania chmurą, jako że większość operacji związanych z chmurą jest wykonywana za pośrednictwem tego interfejsu.

KOMPLEKSOWY ZESTAW PODEJŚĆ W ZAKRESIE BEZPIECZEŃSTWA

W zależności od dostawcy rozwiązań chmurowych istnieją niewielkie różnice w sposobie opisywania modelu współdzielonej odpowiedzialności, największą z nich stanowi jednak sposób wdrażania macierzystych funkcji zabezpieczeń chmury i zarządzania nimi. Często różni dostawcy rozwiązań chmurowych uzyskują te same usługi w zakresie zabezpieczeń używając do tego różnych podejść i narzędzi. Na przykład usługi Amazon Web Services (AWS) rozszerzają zasady bezpieczeństwa na podstawie charakterystyki grup bezpieczeństwa związanych z zasobami chmury, podczas gdy usługi Google Cloud Platform (GCP) korzystają z zasad zapory oferujących równoważne funkcje, ale zarządzanych za pomocą różnych interfejsów. Wiele z tych różnic wynika z wyjątkowego sposobu, w jaki architektura każdej chmury jest zbudowana, oraz odmiennych filozofii dotyczących operacji chmurowych.

W przypadku klientów korzystających z wielu chmur domyślnym stanem bezpieczeństwa jest heterogeniczna architektura pozbawiona scentralizowanej widoczności i kontroli, co oznacza niespójne egzekwowanie zasad bezpieczeństwa i zarządzanie nimi. W tym kontekście każda chmura publiczna i prywatna, w tym lokalne centrum danych, staje się niezależnym silosem w ramach rozdrobnionej infrastruktury zabezpieczeń sieci.



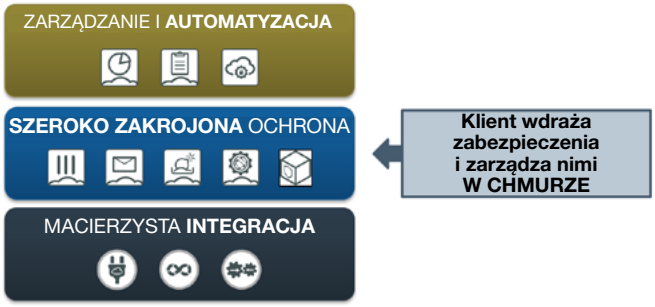
ZABEZPIECZENIE POSZCZEGÓLNYCH ZASOBÓW LEŻY W GESTII KLIENTA I DOSTAWCY ROZWIĄZAŃ CHMUROWYCH.

ISTOTNE ELEMENTY KOMPLEKSOWEGO ROZWIĄZANIA

Bez względu na typy i strukturę usług chmurowych używanych przez przedsiębiorstwo, heterogeniczne i niespójne zarządzanie zabezpieczeniami sieci powoduje zwiększenie ryzyka naruszenia bezpieczeństwa, wymaga bowiem większych umiejętności i większego nakładu czasu personelu IT. Ponadto zarządzanie takie utrudnia raportowanie kwestii zgodności oraz wymianę informacji o zagrożeniach w ramach całego przedsiębiorstwa.

Tymczasem obecne zagrożenia wymagają zastosowania jednolitego i spójnego podejścia do kwestii bezpieczeństwa chmury. Można tu wyróżnić trzy niezbędne elementy, które tworzą efektywne rozwiązanie zabezpieczające środowisko wielochmurowe.

- Macierzysta integracja
- Szeroko zakrojona ochrona
- Zarządzanie i automatyzacja



TRZY KRYTYCZNE ELEMENTY SKUTECZNEGO ROZWIĄZANIA ZABEZPIECZAJĄCEGO.

1. MACIERZYSTA INTEGRACJA

Macierzysta integracja dotyczy zdolności rozwiązania zabezpieczającego do stosowania klasyfikacji informacji opartych na chmurze w ramach całościowego zarządzania zasadami bezpieczeństwa i funkcjami egzekwowania tych zasad, jak również do wykorzystania macierzystych usług chmurowych w ramach wspomnianego rozwiązania. Poniżej przedstawiono niektóre z kluczowych funkcji macierzyście zintegrowanego rozwiązania zabezpieczającego chmurę:

- **Łączniki z chmurą.** Rozwiązania zabezpieczające muszą być zdolne do nawiązania połączenia z chmurą i reprezentowania w niej wszystkich zasobów w taki sposób, aby administratorzy zabezpieczeń mogli intuicyjnie definiować zasady i analizować zdarzenia dotyczące bezpieczeństwa. Rozwiązania te muszą również pozwalać urządzeniom zabezpieczającym na dynamiczne egzekwowanie zasad bezpieczeństwa zgodnie z ciągłymi zmianami zachodzącymi w infrastrukturze chmury.

  Zasoby chmury zazwyczaj korzystają z metadanych i etykiet w celu wskazania ich logicznej funkcji lub klasyfikacji informacji, łączniki takie mogą być zatem użyte w celu normalizacji różnych typów metadanych zasobów w wielu chmurach na potrzeby wdrożenia i egzekwowania spójnych zasad bezpieczeństwa. Bardziej zaawansowane wdrożenia łączników chmurowych identyfikują i wyszczególniają ogólny zestaw zasobów chmury, aby przedstawić je w bardziej kompleksowy sposób, na przykład w formie topologii sieci. Ułatwia to zespołom ds. bezpieczeństwa badanie stanu zabezpieczeń chmury i wdrażanie skutecznych zasad bezpieczeństwa.

- **Optymalizacja.** Aby dobrze obsługiwać zasoby chmurowe i gwarantować odpowiednią wydajność infrastruktury, zabezpieczenia muszą być zintegrowane z różnymi usługami chmurowymi i zapewniać zoptymalizowane rozwiązania programowe wykorzystujące najwyższą możliwą wydajność w chmurze. W ten sposób zabezpieczenia nigdy nie staną się wąskim gardłem podczas ochrony procesów odbywających się w chmurze. Dla każdego elementu takiego jak kontener lub maszyna wirtualna na konkretnym typie sprzętu powinno być zapewnione najbardziej odpowiednie rozwiązanie.

- **Skrypty dotyczące automatyzacji.** Przygotowanie się na nieplanowane zdarzenia w chmurze wymaga posiadania skryptów dotyczących automatyzacji. Umożliwiają one szybką reakcję na awarie systemu, zmiany infrastruktury lub poważne naruszenia bezpieczeństwa. Skrypty te muszą mieć dostęp do macierzystych funkcji automatyzacji każdej chmury i wykorzystywać je do spójnej automatyzacji procesów we wszystkich chmurach.

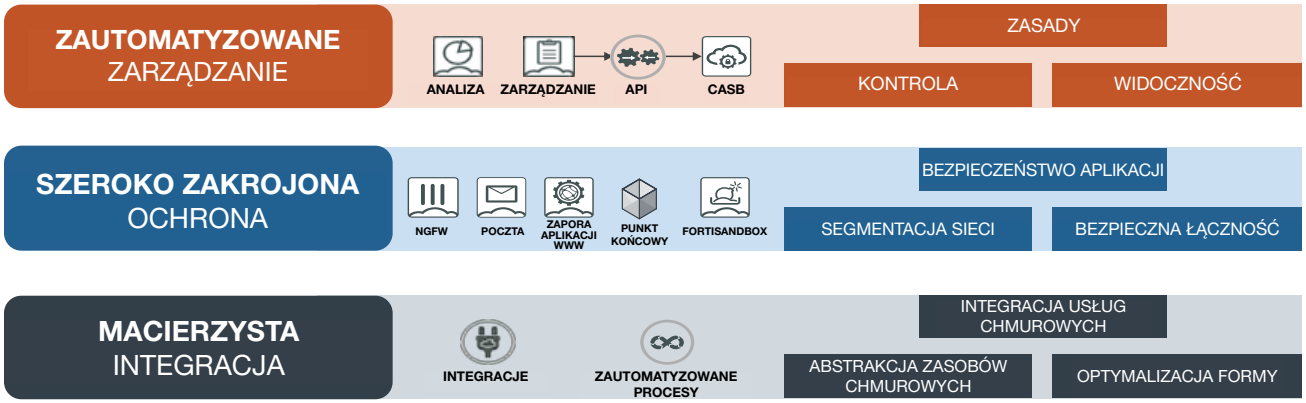
- **Kanały informowania o zagrożeniach.** Kompleksowe rozwiązanie zabezpieczające wiele chmur korzysta z dynamicznie importowanych z określonych kanałów informacji o zagrożeniach, które są na bieżąco blokowane. Kanały te zawierają obszerne informacje o zagrożeniach oparte na zdarzeniach, do których doszło w infrastrukturze dostawcy zabezpieczeń, w tym informacje o zagrożeniach zebrane ze wszystkich wdrożeń u klientów. Zdolność do integracji takich informacji o zagrożeniach z różnych chmur w połączeniu z informacjami o zagrożeniach pochodzącymi z innych źródeł jest niezbędna do ochrony całej infrastruktury przedsiębiorstwa.

- **Wysoka dostępność.** Każda chmura zapewnia wysoką dostępność, wykorzystując w tym celu różne funkcje. Podstawowe zabezpieczenia muszą obsługiwać każde środowisko chmurowe w sposób zapewniający spójne i przewidywalne egzekwowanie zasad bezpieczeństwa. W tym kontekście zabezpieczenia muszą obsługiwać różne schematy (aktywne/aktywne lub aktywne/pasywne), w sposób macierzysty integrując się z każdą chmurą w celu zapewnienia dostępności systemów o znaczeniu krytycznym dla przedsiębiorstwa.

- **Automatyczne skalowanie.** Jedną z podstawowych zalet infrastruktury chmurowej jest jej elastyczność i zdolność do udostępniania funkcji na żądanie. Obejmuje to możliwość skalowania wykorzystania zasobów w ramach chmury i poza chmurą na podstawie zgłaszanych potrzeb biznesowych i płacenia wyłącznie za wykorzystane zasoby. Macierzysta integracja z funkcjami automatycznego skalowania chmury pozwala infrastrukturze zabezpieczeń na skalowanie zasobów infrastruktury chmurowej na podstawie wolumenu i zapotrzebowania. Gwarantuje to stałą ochronę aplikacji.

- **Szablony konfiguracyjne.** Istotnym elementem integracji z modelem operacyjnym chmury jest możliwość tworzenia szablonów konfiguracyjnych, które pomagają administratorom zabezpieczeń w szybkim i dokładnym wdrożeniu rozwiązań zabezpieczających na różnych platformach chmurowych, zgodnie z różnymi procesami chmurowymi. Dzięki zastosowaniu wspomnianych szablonów można zmniejszyć prawdopodobieństwo popełnienia przez człowieka błędu w konfiguracji rozwiązań zabezpieczających, a także szybciej obejmować zabezpieczeniami i wdrażać nowe procesy.

- **Integracja z usługami.** Platformy chmurowe oferują usługi programowe i platformowe, które upraszczają korzystanie z różnych funkcji, ponieważ eliminują potrzebę opanowania przez użytkowników każdej z tych technologii. Kluczowe znaczenie ma tu zdolność rozwiązania zabezpieczającego do integracji z każdą platformą chmurową i zapewnienia ochrony w ramach modelu korzystania z usług macierzystych. W tym przypadku integracja rozszerza ochronę (jako funkcję podstawową) na większą liczbę przypadków użycia i usług, oferując podstawową ochronę zarówno w odniesieniu do środowisk eksperymentalnych, jak i środowisk niebędących jeszcze częścią szerzej rozumianego zarządzania zabezpieczeniami.



TRZY FILARY BEZPIECZEŃSTWA W WIELU CHMURACH: MACIERZYSTA INTEGRACJA, SZEROKO ZAKROJONA OCHRONA ORAZ ZARZĄDZANIE I AUTOMATYZACJA.

2. SZEROKO ZAKROJONA OCHRONA

Szybkie upowszechnianie się infrastruktury chmurowej na potrzeby obsługi aplikacji o znaczeniu krytycznym dla przedsiębiorstwa wymaga zastosowania nowych skoordynowanych i wielowarstwowych rozwiązań zabezpieczających. Jest to szczególnie prawdziwe w kontekście nieustannej ewolucji zaawansowanych zagrożeń oraz złożoności rozproszonych infrastruktur wielochmurowych. Przedsiębiorstwa korzystające z wielu chmur powinny mieć pewność, że każda część powierzchni ataku jest chroniona przed każdym rodzajem zagrożenia. Poniżej przedstawiono kilka kluczowych elementów ochrony sieci wchodzących w skład kompleksowego rozwiązania zabezpieczającego.

- **Ochrona przed zagrożeniami typu „zero-day”.** Według danych FortiGuard Labs nawet 40% nowych złośliwych programów obserwowanych danego dnia w 2018 r. służyło do przeprowadzania ataków typu „zero-day” lub było nieznanych. Wynikało to częściowo z faktu, że generowane automatycznie, jednorazowe złośliwe oprogramowanie jest coraz bardziej popularne wśród cyberprzestępców. Niezbędnym elementem strategii zabezpieczenia chmury jest zatem funkcja analizy zagrożeń w bezpiecznym środowisku testowym (sandbox), do którego trafia na obserwację potencjalne złośliwe oprogramowanie zanim zostanie przepuszczone do sieci przedsiębiorstwa.

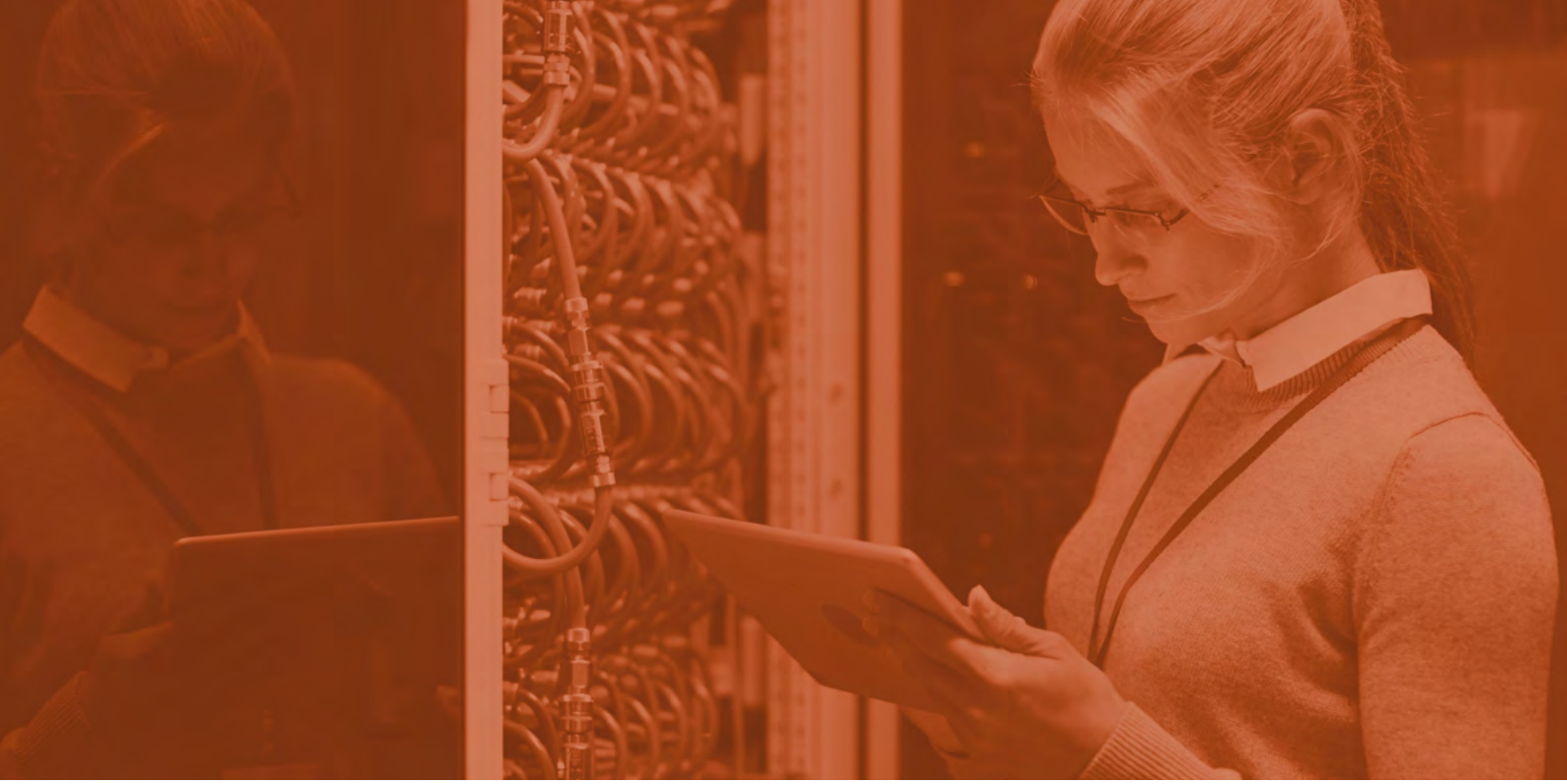
  Wspomniana analiza jest jednak czasochłonna i w dużym stopniu obciąża procesory, jeśli zatem większość ruchu nie będzie wstępnie filtrowana, może nastąpić bardzo duże spowolnienie działania systemu. Przed poddaniem ich analizie w bezpiecznym środowisku testowym wiele potencjalnych zagrożeń może być wykrytych dzięki zastosowaniu funkcji sztucznej inteligencji (AI) i uczenia maszynowego (ML). Zdolność do wdrożenia technologii sandboxingu w środowiskach IaaS i SaaS to ważna funkcja, która powinna być uwzględniona w każdej strategii zabezpieczenia wielu chmur.

- **Wirtualna sieć prywatna oparta na protokołach IPsec.** Zasadnicze znaczenie ma zdolność do rozszerzenia możliwości podłączania do chmury i w chmurach z różnych ośrodków. Ruch między środowiskami chmurowymi jest elementem występującym często, zdolność do izolowania ruchu i tworzenia spójnych zasad bezpieczeństwa sieci w całej infrastrukturze jest zatem kluczowym czynnikiem umożliwiającym ujednolicenie odmiennych środowisk chmurowych. Obsługa zarówno opartych na protokołach IPsec wirtualnych sieci prywatnych łączących ośrodki, jak i wirtualnych sieci prywatnych łączących wirtualne sieci chmurowe ma zatem zasadnicze znaczenie dla spójnej izolacji sieci. Wdrożenia wirtualnych sieci prywatnych powinny współdziałać z różnymi rozwiązaniami chmurowymi w zakresie wirtualnych sieci prywatnych i oferować różnym przedsiębiorstwom i jednostkom organizacyjnym odpowiednią dla nich elastyczność.

- **Wirtualna sieć prywatna oparta na protokole SSL.** Wirtualna sieć prywatna oparta na protokole SSL jest bardzo ważna dla zapewnienia dostępu do wybranych usług o znaczeniu krytycznym dla przedsiębiorstwa, niezależnie od tego, czy jest hostowana w chmurze, czy zainstalowana lokalnie. Zdolność do rozszerzenia infrastruktury zdalnego dostępu w przedsiębiorstwie do chmury zapewnia bezproblemowe możliwości podłączania bez względu na to, gdzie usługa jest hostowana.

- **Kontrola aplikacji.** Przedsiębiorstwa umieszczają w chmurze coraz bardziej różnorodne aplikacje, potrzeba uzyskania widoczności i zarządzania bezpieczeństwem na poziomie aplikacji staje się zatem coraz bardziej istotna. Ochrona jest lepsza, gdy jest realizowana w oparciu o faktycznie wykorzystywaną aplikację, a nie tylko w kontekście udostępnionych zasobów lub usług. Możliwość wdrożenia zabezpieczeń zdolnych do rozpoznawania aplikacji w chmurze, w różnych chmurach i w infrastrukturze chmury hybrydowej jest niezbędna do budowy sprawnej infrastruktury wielochmurowej bez uszczerbku dla jej bezpieczeństwa.

- **Definiowana programowo sieć rozległa (SD-WAN).** Obecnie przedsiębiorstwa badają, a wiele z nich już wdraża, definiowaną programowo sieć rozległą (SD-WAN), aby skorzystać z obniżonych kosztów łączności z Internetem i zwiększyć dostęp do aplikacji chmurowych. Zdolność do przekierowania ruchu do Internetu przez scentralizowaną infrastrukturę zabezpieczeń w chmurze zapewnia znaczne korzyści przedsiębiorstwom, które starają się ograniczać działania swoich fizycznych centrów danych. Obecność funkcji SD-WAN w chmurowych produktach zabezpieczających zyskuje na znaczeniu w miarę jak przedsiębiorstwa zaczynają wdrażać strategie wielochmurowe i tworzą infrastrukturę do obsługi takich wdrożeń.



- **Zapora akumulująca stan.** O ile zapora akumulująca stan jest uważana za funkcję podstawową, zdolność do segmentacji sieci i ruchu dotyczącego aplikacji z zachowaniem informacji o stanie pozostaje niezbędną funkcją izolacji sieci. W szczególności zdolność do egzekwowania spójnych zasad w wielu sieciach i infrastrukturach chmurowych z zachowaniem informacji o stanie daje przedsiębiorstwu możliwość pewniejszego przenoszenia aplikacji w ramach posiadanej infrastruktury.
- **Zapora następnej generacji (NGFW).** Przedsiębiorstwa umieszczają w chmurze coraz więcej aplikacji o znaczeniu krytycznym, wzrasta zatem zapotrzebowanie na zaawansowane ich zabezpieczenie. Musi ono wówczas zapewniać ten sam poziom ochrony dla usług chmurowych, co dla usług zainstalowanych lokalnie i obejmować m.in. funkcje ochrony przed włamaniami i złośliwym oprogramowaniem oraz filtrowania stron WWW.
- **Zapora aplikacji WWW (WAF).** Zapory te chronią zwłaszcza przed zagrożeniami dotyczącymi największej kategorii aplikacji i pomagają przedsiębiorstwu w spełnieniu wymogów w zakresie zasad zarządzania ryzykiem i wymogów regulacyjnych związanych z ochroną informacji o użytkowniku końcowym i zapewnieniem ciągłości działalności biznesowej. Kluczowe funkcje takiej zapory obejmują m.in. zapobieganie wyciekom danych, kontekstowe zrozumienie procesu działania aplikacji WWW i zależności między różnymi elementami aplikacji.
- **Bezpieczeństwo poczty elektronicznej.** Ze względu na fakt, że poczta elektroniczna to nadal najczęstszy sposób przesyłania złośliwego oprogramowania i że przedsiębiorstwa przenoszą swoje systemy poczty elektronicznej do chmury, to właśnie chmura jest często logicznym miejscem dla bramy pocztowej. Ponadto chmura pozostaje preferowaną infrastrukturą, w której wdraża się systemy tworzenia kopii zapasowych, a brama bezpieczeństwa poczty elektronicznej jest idealnym produktem do umieszczenia w chmurze na potrzeby tworzenia kopii zapasowych.

3. ZARZĄDZANIE I AUTOMATYZACJA

Ujednolicenie zarządzania infrastrukturą bezpieczeństwa sieciowego w przedsiębiorstwie sprawia, że widoczność i kontrola tej infrastruktury (od centrum danych do wielu chmur) staje się praktyczna i użyteczna.

Ponadto scentralizowane zarządzanie pozwala nie tylko na automatyzację procesów zarządzania cyklem życia zabezpieczeń, ale również na stosowanie spójnych zasad bezpieczeństwa w wielu chmurach. Celem tych działań jest umożliwienie zarządzania infrastrukturą chmurową i zainstalowaną lokalnie w podobny sposób w ramach wykorzystania tego samego poziomu widoczności i kontroli. W efekcie przedsiębiorstwo może osiągnąć założone cele w zakresie zarządzania ryzykiem i zapewnienia zgodności z przepisami.

Efektywne zarządzanie zabezpieczeniami i automatyzacja obejmuje cztery podstawowe elementy: widoczność, kontrolę, zasady i zgodność z przepisami.

- **Widoczność.** Uzyskanie widoczności zróżnicowanego zestawu aplikacji, sieci i infrastruktur w środowisku wielochmurowym to niezbędny element oceny stanu bezpieczeństwa. W kontekście zarządzania zabezpieczeniami takie oceny są zarówno punktem wyjścia, jak i bieżącym procesem w zarządzaniu zabezpieczeniami. Przedsiębiorstwo powinno być w stanie zidentyfikować zasoby rozmieszczone w całej swojej infrastrukturze, powiązać z nimi ruch, uzyskać informacje o tym, które aplikacje są wykorzystywane przez które zasoby, oraz zidentyfikować dane przesyłane przez sieć.

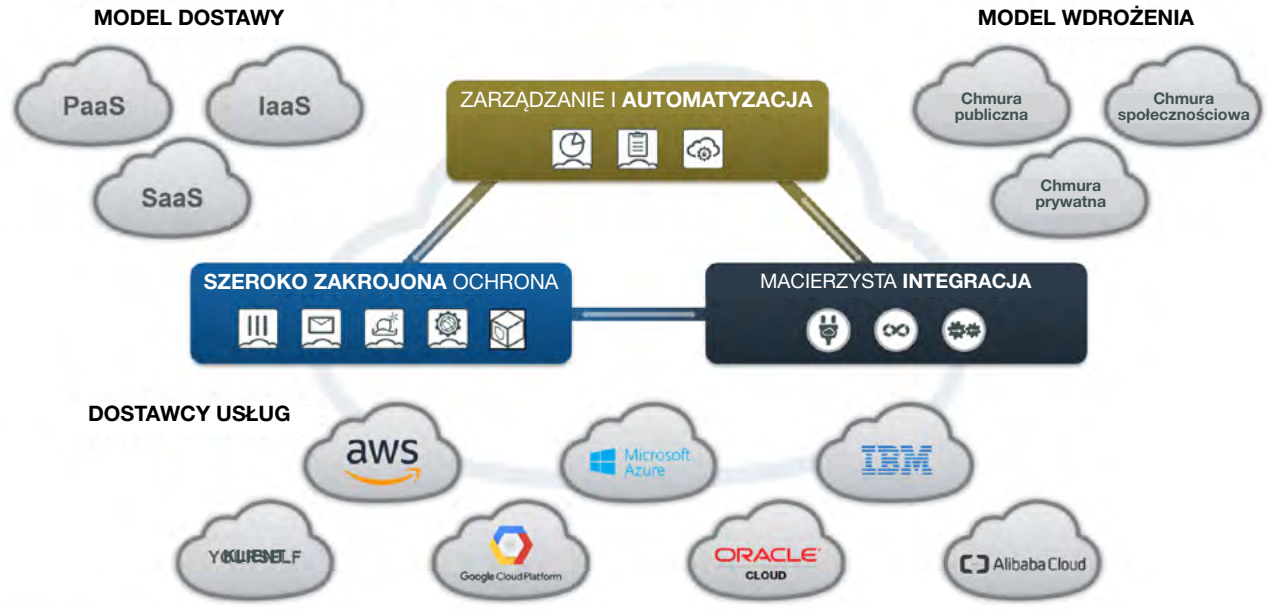
  Dzięki tym informacjom przedsiębiorstwo może zweryfikować, czy przyjęte zasady bezpieczeństwa są skuteczne i wystarczające, aby zapewnić odpowiednie zabezpieczenie infrastruktury. W środowisku wielochmurowym, w którym aplikacje komunikują się w ramach różnych infrastruktur, zdolność do centralnego śledzenia ruchu danych i rozumienia sekwencji zdarzeń zachodzących w każdym środowisku chmurowym często może zapewnić przedsiębiorstwu więcej informacji niż mogłyby to zrobić standardowe narzędzia zabezpieczające. Ponadto zdolność do powiązania w ramach jednej konsoli informacji o infrastrukturze zabezpieczeń z widocznością infrastruktury jeszcze bardziej upraszcza operacyjną obsługę całego systemu.
- **Kontrola.** Po uzyskaniu pełnej widoczności swojej infrastruktury zabezpieczeń przedsiębiorstwo powinno zastosować właściwe mechanizmy kontroli odpowiednich funkcji. Kontrola ta powinna obejmować stosowanie zmian konfiguracji i zasilanie infrastruktury zabezpieczeń odpowiednimi danymi o zasobach dotyczącymi stanu bezpieczeństwa w wielu chmurach. Narzędzia do zarządzania zabezpieczeniami powinny mieć spójną kontrolę nad szerokim

zakresem funkcji bezpieczeństwa. Ponadto ramy kontroli powinny obejmować funkcje bezpieczeństwa zapewniane przez każdą platformę chmurową, co powinno pozwolić administratorom i operatorom na stosowanie zmian bezpieczeństwa w całej infrastrukturze, niezależnie od używanej technologii.

- **Zasady bezpieczeństwa.** Dzięki funkcjom zapewnienia widoczności i kontroli, oferowanym przez pożądaną infrastrukturę wielochmurową przedsiębiorstwo uzyskuje istotne funkcje zarządzania bezpieczeństwem i może wdrażać spójny proces zarządzania zabezpieczeniami i egzekwowania zasad bezpieczeństwa w ramach całej infrastruktury. Na przykład scentralizowana widoczność i kontrola pozwala zespołowi ds. bezpieczeństwa na wdrażanie zasad opartych na aplikacjach niezależnie od lokalizacji poszczególnych składników aplikacji. Jako że motorem zmian w infrastrukturze jest ogólnie rozumiany cykl życia aplikacji, nakład pracy i czas poświęcony na interpretację tego, w jaki sposób zmiany aplikacji wpływają na infrastrukturę, zostają znacznie zredukowane. Zamiast tego zespoły ds. bezpieczeństwa mogą modyfikować ustawienia zabezpieczeń zgodnie ze zdarzeniami w cyklu życia aplikacji, aby zapewnić bardziej spójne zasady bezpieczeństwa.

  Na poziomie strategicznym, zamiast poświęcać mnóstwo czasu na rozważanie sposobu, w jaki zasady bezpieczeństwa powinny być implementowane na poszczególnych platformach chmurowych w sposób zgodny z wymogami przedsiębiorstwa, zespoły ds. bezpieczeństwa mogą szybko wdrażać odpowiednie zasady w ramach ujednoliconej warstwy zarządzania zabezpieczeniami, która jest oddzielona od warstwy technologii i pozwala na szybsze aktualizacje.

- **Zgodność z przepisami.** W ostatecznym rozrachunku aplikacje sieciowe oraz narzędzia i praktyki w zakresie zabezpieczania informacji pozwalają przedsiębiorstwu na zarządzanie ryzykiem związanym z obsługą aktywów cyfrowych i zapewnienie zgodności z regulacjami branżowymi. W szczególności utrzymywanie spójnego systemu bezpieczeństwa oraz automatyzacja związanych z nim operacji znacznie zwiększa zdolność przedsiębiorstwa do zapewnienia zgodności z przepisami. Ponadto centralizacja procesów zarządzania zabezpieczeniami, automatyzacja procesów oraz wymiany informacji o zagrożeniach daje przedsiębiorstwu możliwość szybkiego reagowania na pojawiające się zagrożenia oraz skuteczniejszego ograniczania ryzyka na całej powierzchni ataku bez konieczności wykonywania zbyt skomplikowanych działań.



KOMPLEKSOWE ROZWIĄZANIE OPARTE NA MACIERZYSTEJ INTEGRACJI, SZEROKO ZAKROJONEJ OCHRONIE ORAZ ZARZĄDZANIU ZABEZPIECZENIAMI I FUNKCJACH AUTOMATYZACJI MUSI DZIAŁAĆ W RAMACH RÓŻNYCH MODELI DOSTAW, RÓŻNYCH MODELI WDROŻEŃ ORAZ ROZWIĄZAŃ RÓŻNYCH DOSTAWCÓW USŁUG.

KONKRETNE PRZYPADKI DOTYCZĄCE OCHRONY CHMURY

Zabezpieczenia procesów i aplikacji chmurowych muszą być wdrażane w sposób intuicyjny, korzystny oraz zapewniający łatwą obsługę. Efektem końcowym powinno być rozwiązanie, które kompleksowo ograniczy ryzyko w konkretnym zastosowaniu. Poniżej przedstawiono kilka istotnych przykładów takich rozwiązań:

WEWNĘTRZNE ZABEZPIECZENIA IAAS

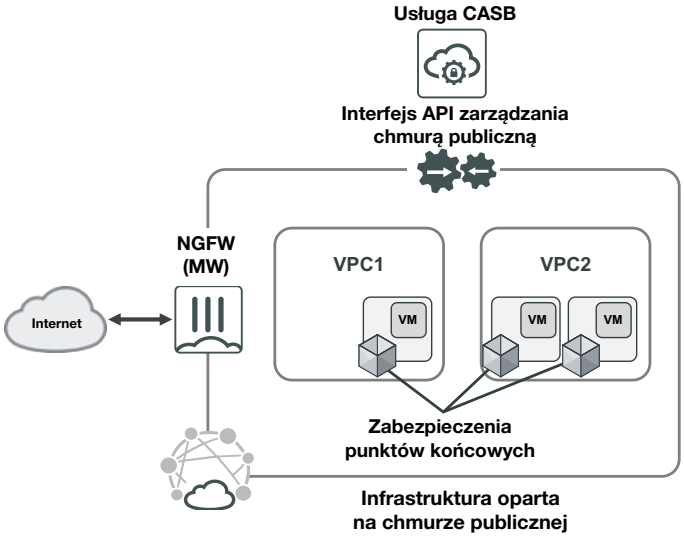
Dostawcy rozwiązań chmurowych chronią swoje infrastruktury, natomiast przedsiębiorstwa będące ich użytkownikami końcowymi muszą chronić swoje aktywa i aplikacje w chmurze. W przypadku wdrażania w chmurze konkretnych aplikacji zabezpieczenie odpowiedniej infrastruktury pomocniczej stanowi wyjątkowo trudne zadanie, które powinno zostać wykonane wewnętrznie w ramach trzech różnych wymiarów:

- Na poziomie procesów — za pomocą agenta kontrolującego spójność aplikacji i ruch wschód-zachód.
- Na poziomie sieci — za pomocą wbudowanej zapory NGFW zabezpieczającej ruch północ-południe, która oferuje również funkcje wirtualnej sieci prywatnej.
- Na poziomie interfejsów API — za pomocą usługi CASB (ang. cloud access security broker), ponieważ istnieje potrzeba, aby stanem bezpieczeństwa przedsiębiorstwa zarządzała osoba trzecia za pośrednictwem interfejsów API danej chmury.

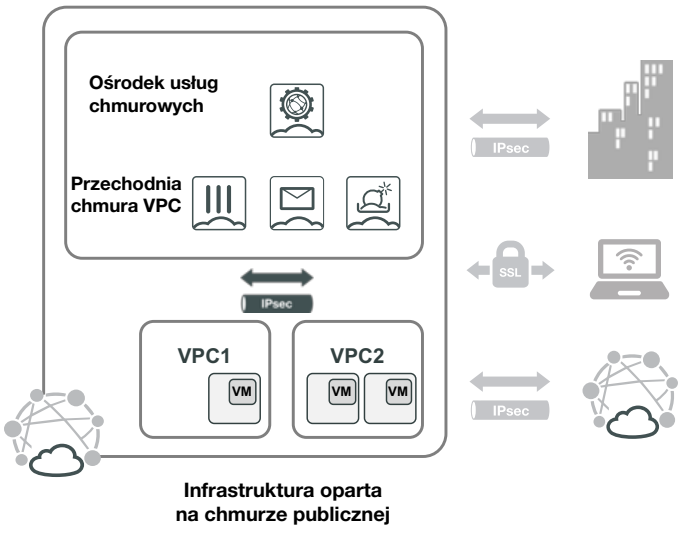
Różne produkty zabezpieczające te różne wymiary powinny ze sobą współdziałać i być zarządzane centralnie w ramach spójnych zasad bezpieczeństwa.

OŚRODEK USŁUG CHMUROWYCH

Przedsiębiorstwa mogą korzystać z wirtualnej sieci prywatnej w chmurze, aby zapewniać usługi współdzielone sieciom chmurowym i zainstalowanym lokalnie. Sieci i aplikacje, które zostały opracowane i są obsługiwane niezależnie przez różne jednostki organizacyjne, mogą być podłączane do ośrodka usług chmurowych za pośrednictwem wirtualnej sieci prywatnej, a następnie korzystać z usług współdzielonych takich jak zapora oparta na aplikacji, ochrona komunikacji aplikacji, zapora aplikacji WWW rozpoznająca kontekst i możliwości podłączenia aplikacji, zabezpieczenia poczty elektronicznej oraz usługi ochrony przed zaawansowanymi zagrożeniami korzystające z bezpiecznego środowiska testowego (sandbox). Wszystkie te funkcje mogą być zarządzane z poziomu chmury.



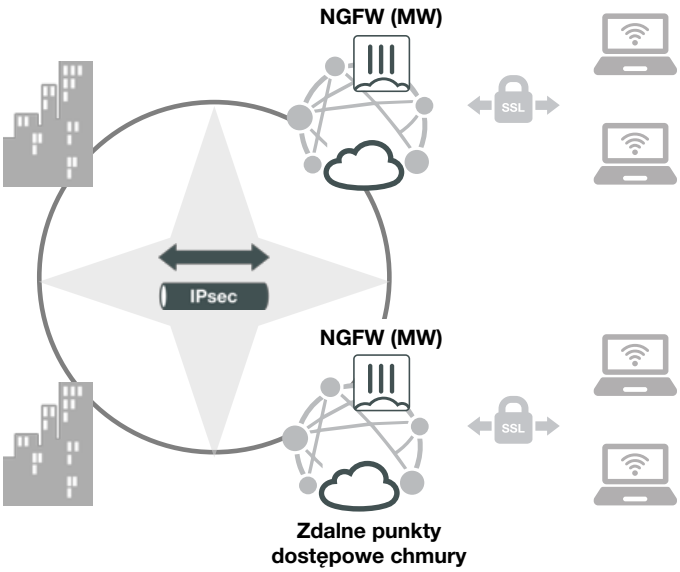
WEWNĘTRZNE ZABEZPIECZENIA IAAS



OŚRODEK USŁUG CHMUROWYCH

WIRTUALNA SIEĆ PRYWATNA ZAPEWNIAJĄCA DOSTĘP ZDALNY

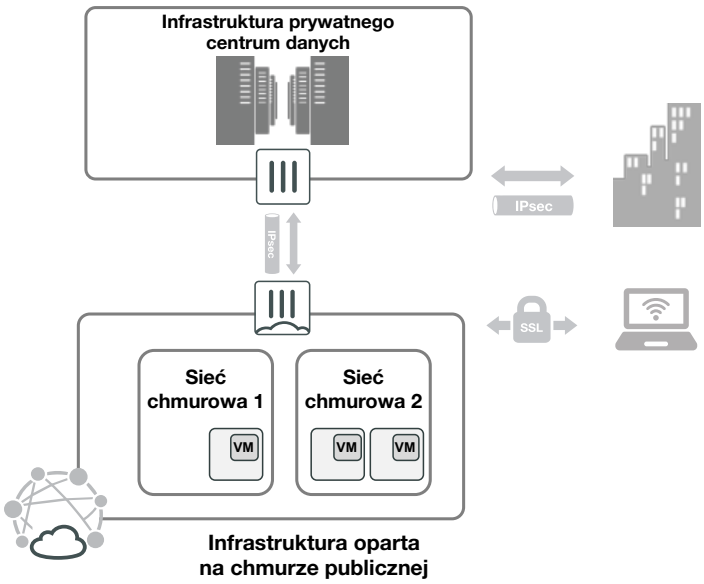
Dzięki globalnej obecności regionów chmurowych i centrów danych przedsiębiorstwo może na całym świecie tworzyć zapewniające zdalny dostęp punkty końcowe wirtualnej sieci prywatnej oraz dynamicznie wdrażać bramy na podstawie wymagań zgłaszanych przez użytkowników końcowych. Spójne zarządzanie różnymi takimi punktami końcowymi zapewnia elastyczność potrzebną do wdrożenia ich na całym świecie bez ponoszenia niepotrzebnych ogólnych kosztów zarządzania. Ponadto dynamiczny charakter chmury oznacza, że wdrożenie nie jest trwałe, może być bowiem w razie potrzeby inaczej skonfigurowane albo wyłączone. Ten scenariusz ma zastosowanie zarówno w przypadku, gdy aplikacje znajdują się w chmurze, jak i wtedy, gdy zostały zainstalowane lokalnie. Aplikacje zainstalowane lokalnie mogą nawiązywać połączenie z chmurą za pośrednictwem łączących ośrodki tunelów wirtualnej sieci prywatnej opartej na protokołach IPSec.



Zdalne punkty dostępowe chmury

CHMURA HYBRYDOWA

Wiele przedsiębiorstw wykorzystuje chmurę publiczną w celu zapewnienia infrastruktury dla rozwiązań IT w uzupełnieniu lokalnych centrów danych. Zazwyczaj nowe aplikacje są jednolicie wdrażane w chmurze publicznej, czasami jednak są wdrażane równolegle w chmurach publicznych i prywatnych. Ważne jest zatem, aby poszukiwane rozwiązanie oferowało obsługę zarówno chmury prywatnej, jak i publicznej. Ponadto musi ono oferować szybko działające, zaawansowane zabezpieczenia, które będą zdolne do przetwarzania bardzo dużych transferów danych. Fundamentalne znaczenie ma też zdolność do spójnego zarządzania zasadami bezpieczeństwa, która zapewnia, że migracje aplikacji między infrastrukturami nie powodują powstania niepotrzebnych ogólnych kosztów operacyjnych związanych z bezpieczeństwem i nie pojawią się potencjalne błędy ludzkie mogące narazić na szwank bezpieczeństwo przedsiębiorstwa. Ponadto zabezpieczenia muszą obejmować całą powierzchnię ataku i być skalowalne, aby można je było dostosować do zachodzących zmian.

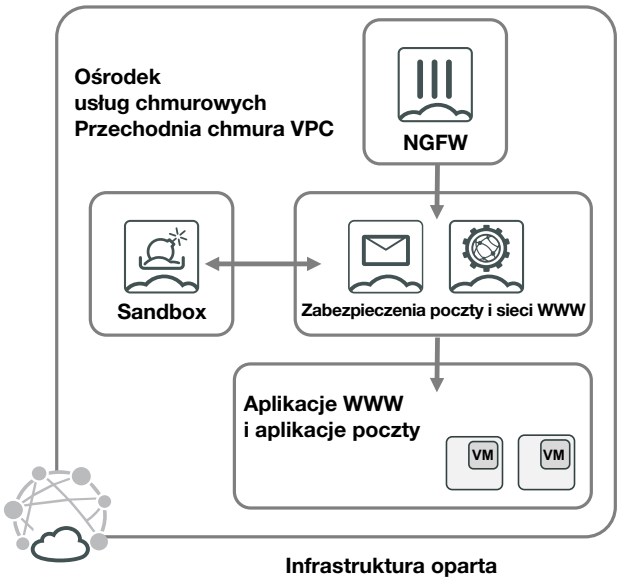


Infrastruktura oparta na chmurze publicznej

ZAAWANSOWANA OCHRONA APLIKACJI

Gdy przedsiębiorstwo wdraża w chmurach publicznych coraz to nowe aplikacje biznesowe o znaczeniu krytycznym zawierające dane wrażliwe, zapewnienie bezpieczeństwa na poziomie aplikacji staje się niezbędne, aby osiągnąć cele zarządzania ryzykiem i zapewnić zgodność z przepisami takimi jak unijne rozporządzenie o ochronie danych osobowych (RODO) lub normy PCI DSS.

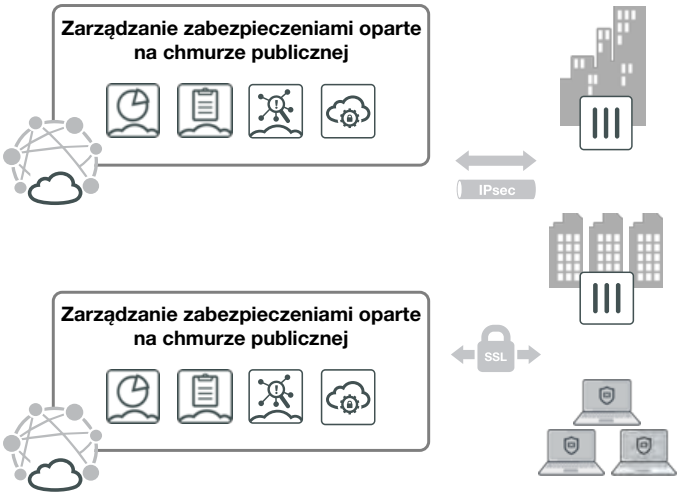
Rozwiązania zabezpieczające muszą oferować szerokie, wielowarstwowe zabezpieczenia właściwe dla aplikacji, aby przedsiębiorstwo mogło przenosić aplikacje do chmury w zależności od wymagań biznesowych, a nie dostępności zabezpieczeń, oraz wybierać platformy chmurowe w oparciu o sens biznesowy, a nie ograniczenia techniczne.



Infrastruktura oparta na chmurze publicznej

ZARZĄDZANIE ZABEZPIECZENIAMI Z POZIOMU CHMURY

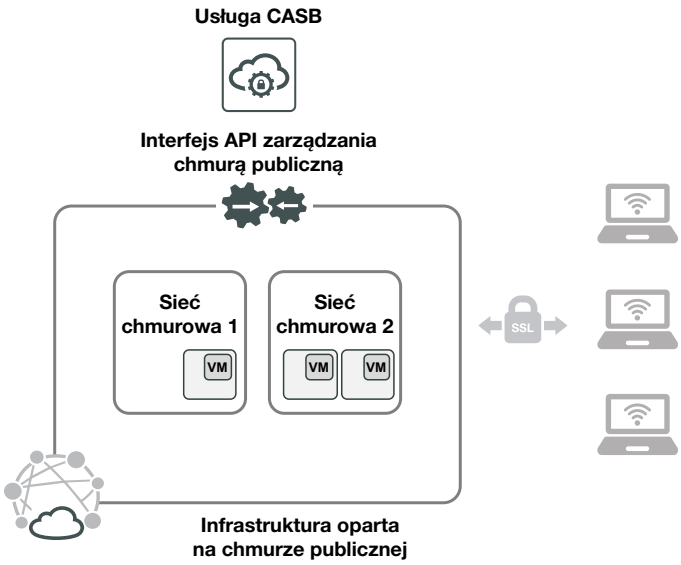
W miarę jak sieci przedsiębiorstw stają się globalne i rozproszone w wielu oddziałach, centrach danych i środowiskach chmury niezbędne stają się odpowiednie możliwości podłączania. Z tego względu przedsiębiorstwa muszą być zdolne do zarządzania zabezpieczeniami w sposób skalowalny i niezawodny, który upraszcza operacje i usprawnia zarządzanie cyklem życia zabezpieczeń. Rozwiązania do zarządzania zabezpieczeniami powinny korzystać z globalnej obecności najlepszych dostawców infrastruktur chmurowych oraz elastyczności zasobów pamięci masowej i zasobów obliczeniowych na potrzeby scentralizowanych systemów globalnego zarządzania zabezpieczeniami.



MONITOROWANIE I KONTROLA KORZYSTANIA Z CHMUR PUBLICZNYCH

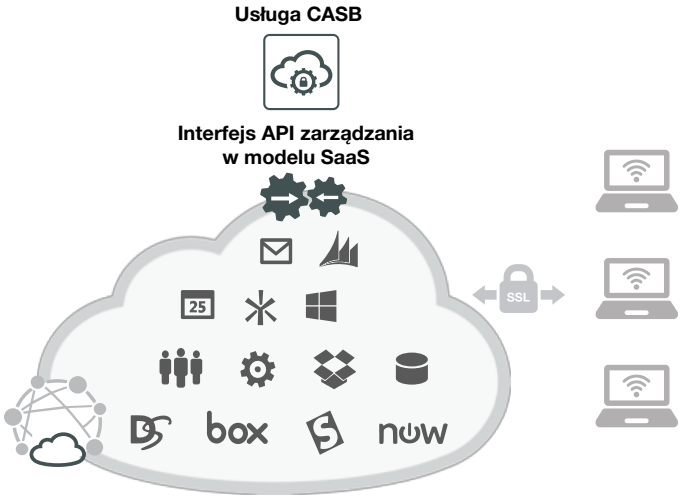
Korzystanie z chmury publicznej często nie jest monitorowane, a użytkownicy mogą wykonywać niemal każdą funkcję, chyba że ograniczają ich uprawnienia przypisane do pełnionej przez nich roli. Takie nienadzorowane podejście prowadzi do niezabezpieczonego i nieefektywnego kosztowo wykorzystania zasobów chmury.

Dzięki zastosowaniu usługi CASB do zarządzania stanem bezpieczeństwa zgodnie z wbudowanymi funkcjami infrastruktury zabezpieczeń w chmurze przedsiębiorstwo uzyskuje pełną widoczność zmian konfiguracji w różnych infrastrukturach chmury publicznej. Ponadto może podejmować lepsze decyzje i modyfikować zasady w zależności od wymogów biznesowych oraz egzekwować zasady dopuszczalnego użycia oraz zgodność z przepisami i normami bezpieczeństwa.



MONITOROWANIE I KONTROLA KORZYSTANIA Z APLIKACJI SAAS

Wraz z coraz intensywniejszym korzystaniem z aplikacji SaaS w przedsiębiorstwach i ich oddziałach, rośnie również potrzeba stosowania spójnych zasad bezpieczeństwa na poziomie użytkownika. Zabezpieczenia chmur muszą integrować mechanizmy kontroli bezpieczeństwa z umieszczonych na granicy sieci zapór służących do kontroli całego ruchu wychodzącego, w tym ruchu generowanego przez aplikacje SaaS. W tym przypadku złośliwe treści i niezabezpieczony dostęp mogą być często śledzone wyłącznie w drodze skorelowania różnych wektorów komunikacji. Na przykład współpraca nad konkretnym plikiem w aplikacji SaaS i wysłanie tego pliku pocztą elektroniczną może być śledzone jedynie przez kompleksową usługę CASB i wbudowany mechanizm ochrony taki jak zainstalowana lokalnie zapora.



MONITOROWANIE I KONTROLA KORZYSTANIA Z APLIKACJI SAAS

PODSUMOWANIE

Chmura oferuje przedsiębiorstwom ogromne możliwości biznesowe, ale bez wdrożenia odpowiedniej infrastruktury zabezpieczeń i ram operacyjnych stanowi ona poważne wyzwanie w zakresie bezpieczeństwa, które może mieć daleko idące skutki. Dane i aplikacje o znaczeniu krytycznym dla przedsiębiorstwa są rozproszone w wielu chmurach. Wskutek szybkiego, zdecentralizowanego wdrożenia usług chmurowych przedsiębiorstwo często uzyskuje heterogeniczny zestaw zasad i narzędzi z zakresu bezpieczeństwa zarządzanych w ramach poszczególnych silosów.

Model współdzielonej odpowiedzialności za bezpieczeństwo chmury nakazuje, aby dostawcy chmury chronili jedynie infrastrukturę bez uwzględnienia aplikacji wdrażanych i uruchamianych w chmurze oraz danych przechowywanych w chmurze, których ochrona leży w gestii użytkownika końcowego. Korzystanie przez poszczególnych dostawców rozwiązań chmurowych z różnych narzędzi i podejść do bezpieczeństwa nastręcza dodatkowych problemów dla przedsiębiorstw, które w celu ochrony swoich aplikacji muszą łączyć ze sobą te zróżnicowane rozwiązania ze swoimi narzędziami zabezpieczającymi.

Aby zabezpieczyć środowiska wielochmurowe, przedsiębiorstwa muszą przestrzegać trzech zasad:

- Macierzysta integracja z rozwiązaniami wszystkich głównych dostawców rozwiązań chmurowych
- Szeroki zestaw narzędzi zabezpieczających, które obejmują całą powierzchnię ataku
- Scentralizowane zarządzanie zabezpieczeniami, w tym automatyzacja procesów i wymiana informacji o zagrożeniach

Ze względu na brak jednolitości we wdrożeniach chmurowych istnieje bardzo dużo przypadków stosowania zabezpieczeń, które przedsiębiorstwo musi uwzględnić. Każdemu z tych przypadków towarzyszą wymogi bezpieczeństwa takie jak integracja wszystkich zabezpieczeń na całej powierzchni ataku, automatyzacja zabezpieczeń obejmująca wiele chmur, właściwe dla poszczególnych chmur ramy bezpieczeństwa ze scentralizowanym zarządzaniem zasadami bezpieczeństwa na potrzeby zapewnienia zgodności z odpowiednimi regulacjami, zabezpieczenia obejmujące cały cykl życia aplikacji oraz ośrodek usług chmurowych używany do świadczenia usług bezpieczeństwa itp.

[1] „Fortinet Threat Landscape Report Q3 2017", Fortinet, 17 listopada 2017 r.

[2] „Gartner Reveals Top Predictions for IT Organizations and Users for 2016 and Beyond", Gartner, 6 października 2015 r.

Copyright © 2018 Fortinet, Inc. Wszelkie prawa zastrzeżone. Fortinet®, FortiGate®, FortiCare®, FortiGuard® oraz niektóre inne znaki są zastrzeżonymi znakami towarowymi spółki Fortinet, Inc. Pozostałe nazwy związane z Fortinet zawarte w niniejszym dokumencie również mogą być znakami towarowymi lub zastrzeżonymi znakami towarowymi Fortinet. Wszelkie inne nazwy produktów lub spółek mogą być znakami towarowymi ich odpowiednich właścicieli. Przedstawione w niniejszym dokumencie parametry wydajności i inne dane uzyskano podczas testów laboratoryjnych w warunkach idealnych, faktyczna wydajność może być zatem inna. Na wartość parametrów wydajności mogą mieć wpływ zmienne sieciowe, różnorodne środowiska sieciowe i inne uwarunkowania. Żadne ze stwierdzeń zawartych w tym dokumencie nie stanowi wiążącego zobowiązania ze strony Fortinet, a Fortinet odrzuca wszelkie wyraźne lub dorozumiane gwarancje i rękojmie, z wyjątkiem gwarancji udzielonych przez Fortinet na mocy wiążącej umowy z kupującym podpisanej przez głównego radcę prawnego Fortinet, w której Fortinet zagwarantuje, że określony produkt będzie działać zgodnie z wyraźnie wymienionymi w takim dokumencie parametrami wydajności, a w takim przypadku wyłącznie określone parametry wydajności wyraźnie wskazane w takiej wiążącej umowie pisemnej będą wiązać Fortinet. Wszelka tego typu gwarancja będzie dotyczyć wyłącznie wydajności uzyskiwanej w takich samych warunkach idealnych, w jakich Fortinet przeprowadza wewnętrzne testy laboratoryjne. Fortinet w całości odrzuca wszelkie wyraźne lub dorozumiane przyrzeczenia, oświadczenia i gwarancje związane z tym dokumentem. Fortinet zastrzega sobie prawo do zmieniania, modyfikowania, przenoszenia lub innego korygowania niniejszej publikacji bez powiadomienia (zastosowanie ma najnowsza wersja publikacji).

21 maja, 2019 9:10 AM

270835-0-1-PL

wp-key-principles-securing-the-enterprise-cloud-A4