

**Rozproszone hybrydowe
centra danych wymagają
dodatkowych funkcji zapory
następnej generacji**

Spis treści

Streszczenie	3
Rozproszone centra danych zwiększają powierzchnię ataku	4
Zabezpieczanie hybrydowych środowisk IT	6
Wydajność a zarządzanie ryzykiem	7
Odporność i skalowalność	9
Automatyzacja i orkiestracja	11
Dobry wybór — integracja i najlepsza w swojej klasie zapora następnej generacji	12

Streszczenie

W wyniku rozwoju nowoczesnych centrów danych aplikacje i dane są w coraz większym stopniu rozproszone w infrastrukturze hybrydowej. Pomaga to wprowadzić poprawić elastyczność procesów o znaczeniu krytycznym dla przedsiębiorstwa, ale jednocześnie zwiększa powierzchnię ataku przy ograniczeniu widoczności i możliwości kontroli. Specjaliści ds. operacyjnych i inżynierii sieci potrzebują zatem zintegrowanych zabezpieczeń oferujących zaawansowane funkcje ochrony środowisk hybrydowych centrów danych IT. W szczególności potrzebują zapory następnej generacji (NGFW), która umożliwi zarządzanie ryzykiem krytycznym oraz zapewni skalowalność pozwalającą na rozszerzenie ochrony centrum danych na wszystkie części organizacji, odporność na zakłócenia ciągłości działalności biznesowej oraz funkcje automatyzacji i orkiestracji odciążające personel i skracające czas reakcji na zagrożenia.

Rozproszone centra danych zwiększają powierzchnię ataku

Obecnie użytkownicy biznesowi uzyskują dostęp do krytycznych aplikacji z coraz bardziej rozproszonych centrów danych, które rozciągają się na całą hybrydową infrastrukturę IT. Procesy i dane tych użytkowników funkcjonują w różnych systemach lokalnych, wspólnych lokalizacjach oraz chmurach prywatnych i publicznych, a tego rodzaju szerokie rozproszenie podatnych na zagrożenia treści tworzy w przedsiębiorstwie coraz większą powierzchnię ataku.

Aby niwelować to rosnące zagrożenie, specjaliści ds. operacyjnych i inżynierii sieci wdrażają punktowe rozwiązania zabezpieczające, aby usuwać pojawiające się luki w zabezpieczeniach i zachować zgodność z przepisami. Takie wyrywkowe podejście nie jest jednak w stanie usunąć wszystkich obecnych i przyszłych luk. Prawdopodobieństwo zakłócenia działalności biznesowej przez cyberprzestępców lub wystąpienie klęski żywiołowej rośnie, podobnie jak zwiększa się całkowity koszt posiadania i złożoność operacyjna zabezpieczeń w przedsiębiorstwie.



Średni całkowity koszt przestoju to 67,2 mln USD na przedsiębiorstwo w ciągu dwóch lat, wliczając w to uszczerbek na zaufaniu i reputacji¹.

Zabezpieczanie hybrydowych środowisk IT

Aby sprostać wyzwaniom związanym z rozszerzającą się powierzchnią ataku na centrum danych, wspomniani specjaliści muszą najpierw zintegrować zabezpieczenia stosowane we wszystkich obszarach swoich hybrydowych środowisk IT. Potrzebują również zapory następnej generacji (NGFW), która zapewni im kompleksową widoczność, mechanizmy kontroli i funkcje ochrony przed włamaniami (IPS), a także zaawansowane możliwości w następujących obszarach:

- **Wydajność.** Zarządzanie ryzykiem wymaga zabezpieczeń, które będą zdolne do obsługi wydajnych sieci, jednocześnie realizując zaawansowane funkcje bezpieczeństwa, które skutecznie pomogą zmniejszyć powierzchnię ataku.
- **Odporność i skalowalność.** W miarę rozwoju i dywersyfikacji hybrydowych środowisk IT zabezpieczenia centrów danych muszą zapewniać taką skalowalność, odporność i dostępność, aby zagwarantować ciągłość działalności biznesowej. Ogólna architektura sieci i zabezpieczeń powinna również chronić przed zakłóceniami spowodowanymi przestojami działania fragmentów sieci, np. związanymi z klęskami żywiołowymi.
- **Automatyzacja i orkiestracja.** Zintegrowana architektura zabezpieczeń powinna umożliwić inteligentną automatyzację w całej hybrydowej infrastrukturze IT. Zautomatyzowane reakcje na zagrożenia i funkcje szybszego zarządzania skrócą wówczas czas narażenia na ryzyko oraz zmniejszą obciążenie personelu, liczbę błędów ludzkich i koszty operacyjne.

Wśród najważniejszych obaw związanych z hybrydowymi procesami obsługi danych można wymienić obawy o bezpieczeństwo danych i zgodność z przepisami (71%), o wydajność (62%) oraz o łatwość zarządzania (53%)².

Wydajność a zarządzanie ryzykiem

Stosowane w centrach danych zapory są zazwyczaj wdrażane w częściach sieci o najwyższej przepustowości. Aby działać skutecznie, wdrożona w takim centrum zaporą następnej generacji (NGFW) musi być zdolna do obsługi zaawansowanych zabezpieczeń w warstwie aplikacji (L7) przy minimalnym wpływie na wydajność sieci. W tym celu należy zastosować **specjalne procesory obsługujące funkcje zabezpieczeń**, umożliwiające efektywne działanie funkcji bezpieczeństwa zapory NGFW bez tworzenia w sieci „wąskiego gardła”.

Zabezpieczenie nowoczesnego rozproszonego centrum danych wymaga również uzyskania widoczności wszystkich wdrożonych zabezpieczeń we wszystkich środowiskach (w systemach lokalnych, wspólnych lokalizacjach, chmurach itp.) oraz wszystkich użytkowników, aplikacji i urządzeń. Ponad jedna trzecia (34%) przypadków naruszenia bezpieczeństwa pochodzi obecnie z zaufanych źródeł wewnętrznych³, kontrola dostępu w sieci wewnętrznej jest zatem koniecznością. Specjaliści ds. operacyjnych i inżynierii sieci mogą to osiągnąć poprzez **segmentację sieci**, która jest rozwiązaniem na tyle skalowalnym i elastycznym, że obejmuje wiele przypadków zastosowań (w tym dynamiczną weryfikację uprawnień użytkowników, urządzeń i aplikacji). Sama segmentacja może jednak nie zapewniać wielu krytycznych funkcji zabezpieczeń przed zaawansowanymi zagrożeniami (na przykład mechanizmów inspekcji treści). Wdrożona w centrum danych zaporą musi być zatem zdolna do obsługi różnych form segmentacji, wymiany informacji o zagrożeniach z zabezpieczeniami innych firm oraz inspekcji treści i automatycznej ochrony przed zagrożeniami.

Aby poradzić sobie z rosnącą liczbą i złożonością dzisiejszych zagrożeń, trzeba wdrożyć zabezpieczenia zdolne do wymiany informacji w czasie rzeczywistym w ramach zintegrowanej architektury zabezpieczeń. Jednocześnie powinny one wykorzystywać mechanizmy sztucznej inteligencji do identyfikacji nieznanych zagrożeń oraz ochrony przed nimi. Co ważne, wspomniane **mechanizmy sztucznej inteligencji** muszą mieć zastosowanie do zasobów cyfrowych we wszystkich lokalizacjach.

77%

**przedsiębiorstw stosuje
obecnie w pewnym stopniu
niezintegrowane ze sobą punktowe
rozwiązania zabezpieczające⁴.**

Odporność i skalowalność

Rozwój innowacji cyfrowych bezpośrednio wpływa na bezpieczeństwo. W miarę postępującej decentralizacji procesów w ramach hybrydowej infrastruktury informatycznej zapewnienie bezpieczeństwa wymaga **skalowalności**, aby móc chronić kolejne nowe aplikacje i procesy, nie tylko uruchamiane lokalnie, ale również wdrażane w chmurze i na maszynach wirtualnych.

Zabezpieczenia centrów danych muszą również uwzględniać wymagania stale rosnącego ruchu szyfrowanego i nieszyfrowanego. Ponad 72% całego ruchu w sieci to obecnie dane zaszyfrowane (wzrost o prawie 20% r/r⁵). Większa ilość zaszyfrowanego ruchu wymaga zaawansowanej widoczności uzyskiwanej za pomocą narzędzi inspekcji ruchu HTTP i HTTPS.

Rozproszone centra danych są szczególnie podatne na ataki prowadzone za pomocą zaszyfrowanych pakietów danych. Ochrona przed takimi atakami wymaga wdrożenia zabezpieczeń pozwalających na **inspekcję danych szyfrowanych przy użyciu protokołu Secure Sockets Layer (SSL) / Transport Layer Security (TLS)** (a także korzystanie z bezpiecznego środowiska testowego i różnego rodzaju przynęt i wabików), które obsługują ogromny ruch realizowany między użytkownikami i systemami oraz w ramach systemów bez ograniczania wydajności aplikacji. Chodzi tu przede wszystkim o najnowsze funkcje inspekcji **TLS 1.3**⁶.

Pod względem odporności i dostępności wdrażane rozwiązanie musi zapewniać możliwość przełączania awaryjnego w czasie rzeczywistym. Wbudowane **mechanizmy klastrowania opartego na redundancji N+1** oferują w pełni nadmiarową architekturę eliminującą każdy punkt awarii. Niezawodność rozważanego rozwiązania w warunkach rzeczywistych mogą również potwierdzić **testy przeprowadzane przez niezależnych ekspertów branżowych**.

60%

**ataków będzie przeprowadzanych
za pośrednictwem zaszyfrowanego
ruchu⁷, a 28% naruszeń
bezpieczeństwa wiąże się ze
złośliwym oprogramowaniem⁸.**

Automatyzacja i orkiestracja

Utrzymujące się niedobory specjalistów ds. cyberbezpieczeństwa sprawiają, że wiele zespołów jest bardzo mocno obłożonych pracą. Zmniejszenie złożoności operacyjnej jest zatem kluczem do obniżenia kosztów operacyjnych i zmniejszenia tego obciążenia, aby personel techniczny mógł bardziej skupić się na wynikach biznesowych i optymalizacji. Efektywna zaporą w centrum danych powinna zatem umożliwiać **optymalizację procesów** w celu usprawnienia wykonywania zadań z zakresu wdrażania i zarządzania.

Zintegrowana architektura zabezpieczeń to podstawa umożliwiająca wymianę informacji o zagrożeniach i zautomatyzowane reakcje, które koordynują działanie zabezpieczeń w ramach infrastruktury hybrydowych. Obsługująca **otwarte interfejsy programowania aplikacji (API)** zaporą NGFW pozwala m.in. na automatyzację procesów, orkiestrację i synchronizowanie działania zabezpieczeń w kontekście nieaktualizowanych aplikacji i zmian zachodzących w środowiskach DevOps. Zaporą ta powinna być również zdolna do **stosowania logiki biznesowej, która na bieżąco weryfikuje użytkowników, urządzenia i aplikacje** w celu automatyzacji procesów bezpieczeństwa (takich jak przydzielanie zasobów i kontrola dostępu). Zmniejsza to obciążenie personelu i koszty operacyjne przy jednoczesnej poprawie wydajności operacyjnej i skuteczności zabezpieczeń.

Funkcje zapory NGFW, które pomagają zautomatyzować **procesy związane z raportowaniem zgodności z przepisami i procesy audytu**, mogą również przyczynić się do zmniejszenia obciążenia pracą personelu technicznego, zachowując jednocześnie zgodność ze zmieniającymi się przepisami wykonawczymi i branżowymi oraz normami bezpieczeństwa takimi jak przepisy i normy Narodowego Instytutu Standaryzacji i Technologii (NIST) oraz Center for Internet Security (CIS).

Ponad połowa decydentów z branży IT (54%) uważa, że problemy z zatrzymaniem wartościowych pracowników utrudniają wdrażanie modelu hybrydowego⁹.

Dobry wybór – integracja i najlepsza w swojej klasie zaporą następnej generacji

Powierzchnia ataku przedsiębiorstwa rozszerza się w miarę rosnącego rozproszenia centrów danych, które ewoluują w kierunku hybrydowej infrastruktury IT. Mimo oczekiwania wzrostu wydajności takich centrów danych, specjaliści ds. operacyjnych i inżynierii sieci nie mogą iść na kompromis między bezpieczeństwem a zaspokajaniem potrzeb użytkowników. W obliczu rosnących kosztów, ryzyka i prawdopodobieństwa przestoju działania sieci przedsiębiorstwa muszą ponownie rozważyć zabezpieczenia nowoczesnych centrów danych.

Aby zapewnić zarówno bezpieczeństwo, jak i wydajność, trzeba zatem wdrożyć zintegrowaną architekturę zabezpieczeń opartą na niezawodnej zaporze następnej generacji (NGFW), która zagwarantuje odpowiednią wydajność, odporność, skalowalność i możliwość automatyzacji.

¹ Filip Truta, „[Downtime Can Cost a Company up to \\$67 Million Over Two Years, Threatening Brand Reputation](#)”, Security Boulevard, 21 lutego 2019 r.

² Alison DeNisco Rayome, „[91% of tech leaders say hybrid cloud is 'ideal' IT model](#)”, TechRepublic, 15 listopada 2018 r.

³ „[2019 Data Breach Investigations Report](#)”, Verizon, kwiecień 2019 r.

⁴ „[The CIO and Cybersecurity: A Report on Current Priorities and Challenges](#)”, Fortinet, 23 maja 2019 r.

⁵ John Maddison, „[Encrypted Traffic Reaches A New Threshold](#)”, Network Computing, 28 listopada 2018 r.

⁶ Alex Samonte, „[TLS 1.3: What This Means For You](#)”, Fortinet, 15 marca 2019 r.

⁷ Omar Yaacoubi, „[The hidden threat in GDPR's encryption push](#)”, PrivSec Report, 8 stycznia 2019 r.

⁸ „[2019 Data Breach Investigations Report](#)”, Verizon, kwiecień 2019 r.

⁹ Alison DeNisco Rayome, „[91% of tech leaders say hybrid cloud is 'ideal' IT model](#)”, TechRepublic, 15 listopada 2018 r.



www.fortinet.com

Copyright © 2019 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 rękojnie, 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 działał 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).