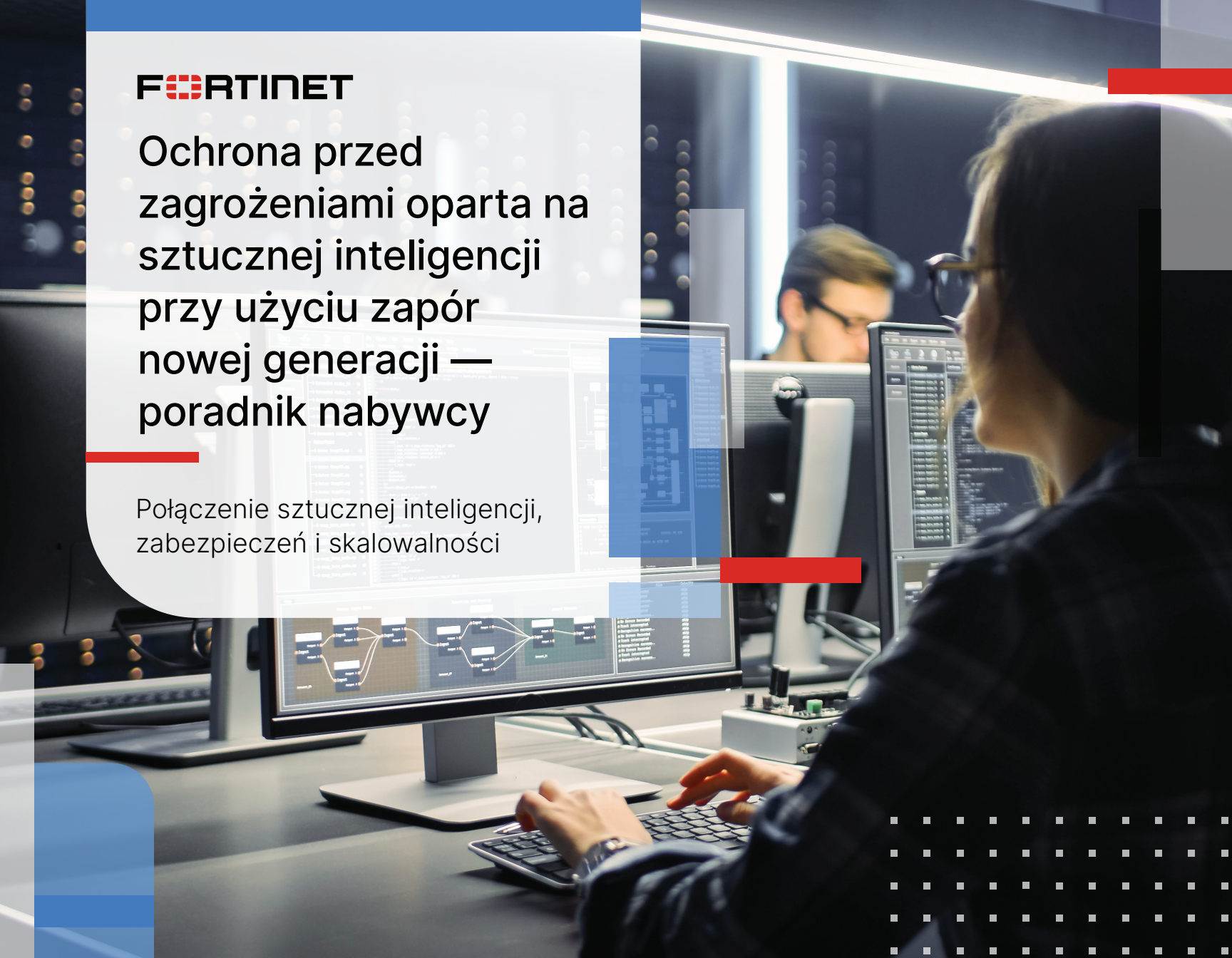


FORTINET

Ochrona przed zagrożeniami oparta na sztucznej inteligencji przy użyciu zapór nowej generacji — poradnik nabywcy

Połączenie sztucznej inteligencji, zabezpieczeń i skalowalności

Sytuacja pod względem zagrożeń

Posługiwanie się przez hakerów technologiami sztucznej inteligencji (AI) potęguje wyzwania stojące przed zespołami ds. bezpieczeństwa i IT odpowiedzialnymi za ochronę swoich organizacji. Cyberprzestępcy wykorzystują AI — od nowych exploitów, przez deepfake, po zaawansowane ataki phishingowe i inne taktyki — w celu penetrowania systemów obronnych i robią to szybciej oraz bardziej zdecydowanie niż kiedykolwiek dotąd. Oznacza to, że już mocno obciążone zespoły ds. bezpieczeństwa i IT będą tylko jeszcze bardziej odczuwać konieczność nadążania za przytłaczającą falą zagrożeń.

Kolejne technologie jednak oznaczają również, że zespoły te muszą się nauczyć korzystać z większej liczby konsol i zarządzać strumieniami alertów w celu ich klasyfikacji oraz prowadzenia analiz ataków. Niestety z perspektywy przepracowanych zespołów więcej zabezpieczeń niekoniecznie przekłada się na większą efektywność. I to jest problem.

Operacje na granicy możliwości

W miarę jak organizacje kontynuują inicjatywy cyfrowe w celu wsparcia swoich celów strategicznych i zwiększenia efektywności, nieuchronnie rozszerzają się powierzchnie ataku. Bez względu na to, czy chodzi o wdrożenia chmury, eliminowanie luk między infrastrukturą IT i OT, upowszechnianie się łączących się z siecią urządzeń z obszaru Internetu rzeczy (Internet-of-Things, IoT), czy pracę hybrydową, podejmowane działania jeszcze bardziej obciążają i tak już przeciążone zespoły ds. bezpieczeństwa i IT.

Bezpieczeństwo, skalowalność i efektywność

Rozszerzonym lub wzmocnionym zabezpieczeniom musi towarzyszyć większa efektywność. Obecne rozwiązania cyberbezpieczeństwa muszą pomagać zespołom ds. bezpieczeństwa i IT w skutecznym chronieniu organizacji przed różnymi zagrożeniami, w tym nowymi zagrożeniami opartymi na AI.

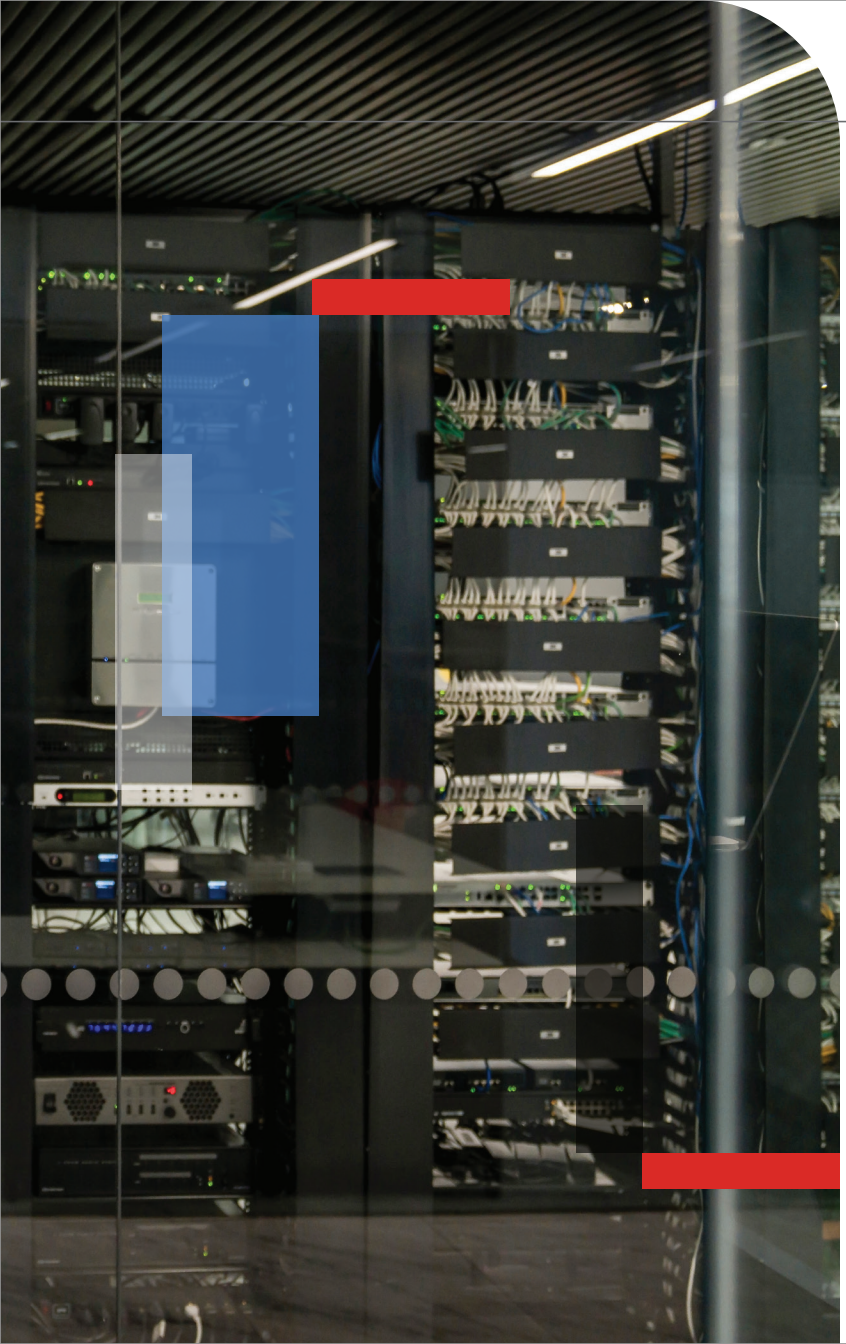
Rozwiązania te powinny jednocześnie wspomagać zespoły w skalowaniu ich działań. Odtąd ta zmiana perspektywy i wymagań powinna następować dwutorowo:

- Zespoły ds. bezpieczeństwa i IT powinny połączyć osobne plany w celu zintegrowania swoich działań w zakresie bezpieczeństwa.
- Dostawcy rozwiązań cyberbezpieczeństwa muszą oferować całościowe rozwiązania, które chronią przed nowo powstającymi zagrożeniami opartymi na AI oraz zwiększają efektywność.

Zapory hybrydowe w topologii mesh (hybrid mesh firewall, HMF) stanowią doskonały przykład możliwości połączenia funkcji zabezpieczeń opartych na AI i jednocześnie zwiększenia efektywności dzięki scentralizowanemu oraz skoordynowanemu podejściu do kwestii bezpieczeństwa. Te hybrydowe rozwiązania obejmują ochronę przed zagrożeniami i funkcje zabezpieczeń oparte na AI, aby pomagać organizacjom skutecznie walczyć z AI przy użyciu AI. Oferują również scentralizowane i skoordynowane podejście do ochrony rosnącej powierzchni ataku w sieciach, w tym środowisk IT i OT, lokalnych i chmurowych oraz różnych lokalizacji fizycznych.

Czym jest zapora hybrydowa w topologii mesh?

Zapora hybrydowa w topologii mesh (HMF) to scentralizowane i ujednolicone rozwiązanie do zarządzania, które upraszcza operacje z zakresu cyberbezpieczeństwa i stanowi logiczny krok w ewolucji zapór nowej generacji. W środowisku hybrydowym organizacje mogą wdrażać zapory lokalnie lub w chmurze z jednym systemem operacyjnym na potrzeby komunikacji i aktualnych informacji o zagrożeniach obejmujących wszystkie wdrożenia.



Wprowadzanie ujednoliconego i scentralizowanego zarządzania

- **Uproszczone zarządzanie:** konsoliduje zarządzanie zabezpieczeniami na jednej platformie w celu wyeliminowania złożoności zarządzania wieloma zaporami różnych producentów.
- **Spójny ogólny stan bezpieczeństwa:** zmniejsza ryzyko luk w zabezpieczeniach i podatność na ataki dzięki egzekwowaniu jednej polityki bezpieczeństwa w całej sieci, co pomaga organizacjom utrzymywać zgodność z wytycznymi dotyczącymi prywatności danych i przepisami.
- **Ulepszone zabezpieczenia:** umożliwia szybsze i bardziej precyzyjne reagowanie na incydenty związane z bezpieczeństwem dzięki wykorzystywaniu automatyzacji, sztucznej inteligencji i uczenia maszynowego do analizy ruchu sieciowego oraz skuteczniejszej identyfikacji ewentualnych zagrożeń.
- **Usprawnienie skalowania:** można dodawać nowe punkty egzekwowania polityki bezpieczeństwa stosownie do potrzeb, co eliminuje problemy związane z zarządzaniem i pozwala łatwo sobie radzić z rozwojem sieci lub wdrożeniami chmurowymi.
- **Lepszy wgląd:** zapewnia całościowy wgląd w stan bezpieczeństwa całej sieci, dzięki czemu można efektywniej identyfikować i rozwiązywać problemy.

Dlaczego analizy zagrożeń oparte na AI są ważne

Jednym z najlepszych zastosowań AI w cyberbezpieczeństwie jest udoskonalenie analiz zagrożeń. Technologie AI mają kluczowe znaczenie z perspektywy zbierania danych, analiz, korelacji i wreszcie przekształcania tych danych w przydatne informacje. Takie analizy zagrożeń oparte na AI można wykorzystywać w ramach integracji w celu kontrolowania szerokiej gamy wektorów ataków i samych zagrożeń — bez względu na to, czy atakujący korzystają z AI. Zastosowanie AI w danym rozwiązaniu oraz szeroki zakres źródeł danych i same dane nie są bez znaczenia. Im lepszy wgląd w dane ma dostawca rozwiązania, tym więcej mogą się dzięki nim nauczyć modele AI.

Ochrona przed zagrożeniami oparta na AI

Wykorzystanie możliwości AI w cyberbezpieczeństwie to nie tylko ulepszenie technologiczne. Jest to coraz pilniej potrzebna ewolucja, która może pomóc organizacjom wzmocnić mechanizmy obrony przed zupełnie nowymi zagrożeniami. Połączenie funkcji zabezpieczeń opartych na AI z większą efektywnością nieodłącznie związaną z rozwiązaniami zapór nowej generacji (new-generation firewall, NGFW) pomaga organizacjom zyskać większą odporność na zagrożenia. Zapory NGFW oferują następujące kluczowe możliwości w zakresie bezpieczeństwa:

Bezpieczeństwo sieci i plików

- **Zapobieganie włamaniom:** funkcja zapobiegania włamaniom przeprowadza dogłębną inspekcję pakietów ruchu sieciowego, w tym szyfrowanego, w celu wykrywania i blokowania najnowszych, dobrze ukrywanych zagrożeń oraz włamań na poziomie sieci.
- **Oprogramowanie antywirusowe:** oprogramowanie antywirusowe chroni przed najnowszymi zagrożeniami polimorficznymi, w tym ransomware, wirusami, oprogramowaniem szpiegującym i innymi zagrożeniami występującymi na poziomie treści.
- **Kontrola aplikacji:** mechanizmy kontroli aplikacji umożliwiają szybkie tworzenie polityk zezwalania na dostęp do aplikacji lub całych kategorii aplikacji albo odmawiania go bądź ograniczania.

Bezpieczeństwo przeglądania stron internetowych / DNS

- **Filtrowanie DNS:** filtrowanie DNS zapewnia spójną ochronę przed zaawansowanymi zagrożeniami opartymi na usłudze DNS. Funkcja ta zapewnia pełny wgląd w ruch DNS, a jednocześnie umożliwia blokowanie domen wysokiego ryzyka, w tym nowo zarejestrowanych złośliwych domen i domen zaparkowanych.
- **Filtrowanie adresów URL:** funkcja filtrowania adresów URL identyfikuje złośliwe adresy URL i blokuje dostęp do nich na poziomie użytkowników oraz aplikacji.
- **Ochrona przed botnetami oraz Command and Control (C2):** funkcje ochrony przed botnetami i C2 blokują nieautoryzowane próby komunikacji z zainfekowanymi serwerami zdalnymi w celu odbierania złośliwych informacji C2 lub wysyłania pozyskanych informacji.

Oprogramowanie jako usługa (SaaS) i bezpieczeństwo danych

- **Broker zabezpieczeń dostępu do chmury (cloud access security broker, CASB):** CASB chroni używane aplikacje SaaS, zapewniając obszerny wgląd w środowisko i szczegółową kontrolę nad dostępem do aplikacji SaaS, ich użytkowaniem oraz danymi.
- **Zarządzanie powierzchnią ataku:** funkcja zarządzania powierzchnią ataku ma na celu identyfikację, ocenę i monitorowanie zasobów sieciowych oraz powiązanej infrastruktury zabezpieczeń pod kątem ogólnej oceny stanu bezpieczeństwa organizacji.

Ochrona przed zagrożeniami zero-day

- **Środowisko testowe (sandboxing) plików:** sandboxing plików umożliwia zaawansowane analizy nieznanych plików w bezpiecznym środowisku w celu ustalenia, czy mogą one stanowić zagrożenie.

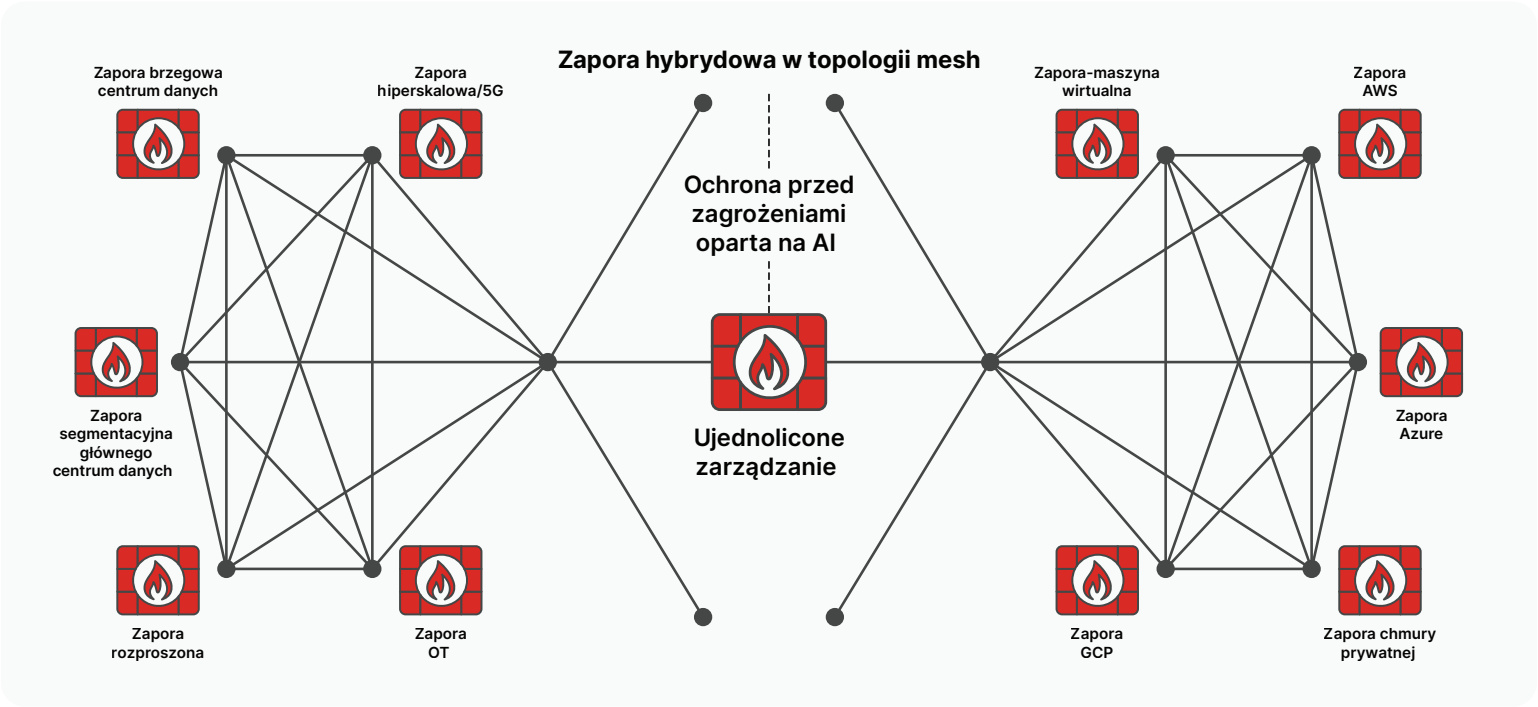
FORTINET

Kluczowe aspekty ujednoliconego i scentralizowanego zarządzania

Aby zadbać o ochronę złożonego środowiska hybrydowego, należy zacząć od głównej linii obrony: zapór. Przed zakupem rozwiązania cyberbezpieczeństwa, na przykład zapory NGFW z usługami opartymi na AI, należy wziąć pod uwagę następujące aspekty:

- **Potrzeby dotyczące sieci:** dokładnie oceń szczególne potrzeby środowiska sieciowego, takie jak rozmiar i złożoność sieci, dystrybucja obciążeń (lokalnie i w chmurze) oraz obecny stan bezpieczeństwa.
- **Funkcje zabezpieczeń:** oceń funkcje oferowane przez różnych dostawców, np. wykrywanie zagrożeń, szyfrowanie danych czy integracja z innymi narzędziami do ochrony.
- **Łatwość zarządzania:** sprawdź, czy dane rozwiązanie cyberbezpieczeństwa oferuje przyjazną dla użytkownika i scentralizowaną konsolę zarządzania, co pozwoli odciążyć zespół ds. bezpieczeństwa.
- **Skalowalność:** zwróć uwagę, jak łatwo można skalować rozwiązanie cyberbezpieczeństwa w celu obsługi przyszłego rozwoju sieci lub wdrożeń chmurowych.
- **Koszt:** uwzględnij opłaty licencyjne, stałe koszty subskrypcji oraz wszelkie niezbędne profesjonalne usługi w zakresie wdrożeń i konserwacji.
- **Reputacja producenta:** wybierz renomowanego dostawcę z udokumentowaną, potwierdzoną przez niezależne podmioty historią.

Dzięki starannemu przeanalizowaniu tych czynników wybierzesz zaporę NGFW, która zaspokoi Twoje potrzeby dotyczące bezpieczeństwa i zapewni najlepszą wartość inwestycji.



Ilustracja 1. Jak działają zapory HMF z ochroną przed zagrożeniami opartą na AI

Ważne pytania, które warto zadać dostawcy zapory NGFW

1 Poznanie możliwości dostawcy w zakresie badania zagrożeń

Analizy zagrożeń oparte na AI są niezwykle istotne. Zaczynają się od wyznaczonej grupy osób, które tworzą zespół dostawcy ds. badania zagrożeń (jeśli taki zespół w firmie istnieje).

- Czy w Państwa firmie istnieje zespół ds. badania zagrożeń, a jeśli tak, to jacy specjaliści wchodzą w jego skład i jaką pełni on rolę?
- Czy ten zespół uczestniczy we wdrożeniach technologii AI w Państwa firmie i w jakim stopniu?

2 Poznanie podstaw do formułowania informacji o zagrożeniach

Z perspektywy cyberbezpieczeństwa AI ulepsza analizy zagrożeń i płynące z nich informacje, więc należy znać zakres wglądu dostawcy. Trzeba się zapoznać ze skalą telemetrii i źródłami informacji oraz możliwościami AI, które pomagają przekształcić dane telemetryczne i inne w przydatne w praktyce informacje.

- Jaki wgląd w zagrożenia i powiązane źródła danych wykorzystuje Państwa firma do formułowania informacji o zagrożeniach, na których bazuje Państwa rozwiązanie?
- Jak jest wykorzystywana sztuczna inteligencja do formułowania informacji o zagrożeniach?

3 Poznanie zakresu wykorzystania AI

Warto wiedzieć, jak mocno angażuje się dostawca, by używać technologii i narzędzi AI w celu ulepszenia swojej oferty oraz efektów z perspektywy bezpieczeństwa.

- Jakie doświadczenie ma Państwa firma w wykorzystywaniu technologii sztucznej inteligencji w Państwa produktach, usługach i rozwiązaniach?
- Jakie konkretnie technologie sztucznej inteligencji zostały zastosowane w danym rozwiązaniu i jakie korzyści płyną z ich użytkowania?
- Czy mogliby Państwo wskazać źródła danych używane w produkcie, usłudze lub rozwiązaniu do szkolenia używanych technologii sztucznej inteligencji?

4 Poznanie funkcji zabezpieczeń wbudowanych w rozwiązanie

Na przykład zapory NGFW powinny udostępniać pewne kluczowe funkcje zabezpieczeń i integracje. Warto wiedzieć, co to za funkcje, co obejmuje kupowane rozwiązanie i jakie korzyści może ono zapewnić Twojej organizacji.

- Które z następujących funkcji zabezpieczeń zapewnia Państwa rozwiązanie?
  - Zapobieganie włamaniom
  - Oprogramowanie antywirusowe
  - Kontrola aplikacji
  - Ochrona przed phishingiem
  - Broker zabezpieczeń dostępu do chmury
  - Zapobieganie utracie danych
  - Sandboxing plików
  - Bezpieczeństwo przeglądania stron internetowych, w tym bezpieczeństwo DNS
  - Zarządzanie powierzchnią ataku
  - Bezpieczeństwo środowisk OT
  - Bezpieczeństwo środowisk IoT
  - Inne

Jak jest wykorzystywana sztuczna inteligencja w ramach wymienionych wyżej usług?

5 Czego warto poszukać w przypadku środowiska hybrydowego

Z perspektywy wyboru zapory NGFW kluczowe znaczenie ma ustalenie konkretnych potrzeb w zakresie bezpieczeństwa i środowiska sieciowego. Dlatego należy bez wahania prosić dostawców o demonstracje i wersje próbne, dzięki którym można się upewnić, że dane rozwiązanie spełnia określone wymagania. A jeśli w Twoim środowisku działają rozwiązania z różnych źródeł, koniecznie poszukaj zapory NGFW, którą można zintegrować z już używanymi zaporami różnych producentów.

Oto kilka istotnych cech, których należy szukać w zaporze NGFW:

Mechanizmy zabezpieczeń

- Zaawansowana ochrona przed zagrożeniami, która wykorzystuje technologie sztucznej inteligencji, w tym uczenie maszynowe, do identyfikowania i blokowania zaawansowanych cyberzagrożeń
- Szczegółowe egzekwowanie polityk w celu definiowania i egzekwowania spójnych polityk bezpieczeństwa w całej infrastrukturze IT
- Analizy zagrożeń i informacje o nich, dzięki którym można być na bieżąco z najnowszymi lukami w zabezpieczeniach oraz metodami ataków

Zarządzanie i skalowalność

- Scentralizowane zarządzanie, czyli zarządzanie wszystkimi zaporami i ich monitorowanie w jednej konsoli
- Zautomatyzowane wdrażanie i aprowizacja, dzięki którym można bez trudu wdrażać oraz konfigurować wszystkie zapory w całej sieci
- Łatwość skalowania, czyli dodawania lub usuwania zapór w miarę rozbudowywania lub redukowania sieci

Oszczędności finansowe i korzyści biznesowe

„Fortinet to nie tylko zapora. Połączenie szeregu komponentów sieciowych i zabezpieczeń zwiększa wydajność sieci oraz skuteczność zabezpieczeń. Największym atutem rozwiązania Fortinet jest to, że oferuje więcej funkcji niż tylko zaporę”.

— menedżer ds. sieci i bezpieczeństwa technicznego, branża zasobów naturalnych

318%

zwrot z inwestycji (ROI)

50%

redukcja przestojów sieci dzięki zwiększeniu wydajności sieci i bezpieczeństwa

6 miesięcy

zwrot kosztów w niespełna pół roku

50%[1]

wzrost produktywności zespołów ds. bezpieczeństwa i sieci

Nowy sposób myślenia

Sztuczna inteligencja weszła w kolejną fazę innowacji oraz negatywnego i pozytywnego wpływu na organizacje. Liderzy ds. bezpieczeństwa i IT muszą oceniać nie tylko to, jak rozwiązanie bezpieczeństwa oparte na AI spełnia założenia dotyczące cyberbezpieczeństwa, ale też jak zwiększa ono efektywność.

Zapory NGFW są ciekawym przejawem tego nowego sposobu myślenia. Oferują narzędzia do ochrony przed zagrożeniami oparte na AI, a jednocześnie centralizują wgląd w całą sieć hybrydową oraz pozwalają na koordynowanie i egzekwowanie polityk zapory. Efektem jest większe bezpieczeństwo ogólne oraz towarzyszący mu wzrost możliwości zespołu pod względem skalowania w celu sprostania wyzwaniom rodzącym się wskutek ewoluujących zagrożeń.

Jeśli myślisz o wdrożeniu zapory NGFW w swojej organizacji, zapraszamy do kontaktu z ekspertem Fortinet, który pomoże wybrać rozwiązanie zaspokajające potrzeby Twojej firmy dotyczące bezpieczeństwa i sieci.

Zadzwoń pod bezpłatny numer w USA: **+1-866-868-3678**

Sprzedaż dla administracji federalnej USA: **+1-833-386-8333**

Sprzedaż w Kanadzie: **+1-833-308-3247**

[1] The Total Economic Impact™ Of Fortinet NGFW for Data Center and AI-Powered FortiGuard Security Services Solution Cost Savings and Business Benefits Enabled by NGFW for Data Center and AI-Powered FortiGuard Security Services Solution (Raport dotyczący łącznego wpływu ekonomicznego rozwiązania Fortinet NGFW dla centrów danych i usług AI-Powered FortiGuard Security Services oraz oszczędności finansowych i korzyści biznesowych uzyskiwanych dzięki rozwiązaniom NGFW dla centrów danych i usług AI-Powered FortiGuard Security Services), Forrester, lipiec 2023.

FORTINET

www.fortinet.com

16 sierpnia 2024 7:33

2627272-0-0-EN