OPIS ROZWIĄZANIA

FortiOS — obsługa architektury Fortinet Security Fabric

Streszczenie

Przedsiębiorstwa na całym świecie nadal wdrażają nowe technologie, aby dotrzymać rosnącego tempa transformacji cyfrowej (DX). O ile transformacja taka otwiera nowe możliwości, rozszerza również powierzchnię ataku, która może być chroniona przez różne punktowe rozwiązania zabezpieczające niekoniecznie ze sobą skomunikowane.

Oferowany przez firmę Fortinet system operacyjny FortiOS pozwala na połączenie takich punktowych rozwiązań zabezpieczających w ramach architektury Security Fabric. Ma to na celu skuteczną ochronę całej infrastruktury sieciowej w ramach jednego adaptacyjnego systemu operacyjnego. Najnowsza wersja systemu FortiOS zawiera setki nowych funkcji, które zapewniają lepszą widoczność i kontrolę na całej powierzchni ataku; integrują korzystające z funkcji sztucznej inteligencji mechanizmy zapobiegania naruszeniom bezpieczeństwa w całej sieci na potrzeby nieprzerwanej ochrony i wykrywania zagrożeń; oraz służą do automatyzowania operacji, automatyzowania procesów i reagowania na zagrożenia.

Oprócz zmagania się z poważnymi niedoborami wykwalifikowanych pracowników i ograniczonymi budżetami, dyrektorzy ds. sieci stoją w obliczu rosnącej złożoności w każdym możliwym kontekście, mając do czynienia z coraz bardziej zaawansowanymi cyberzagrożeniami, coraz bardziej zróżnicowanymi zabezpieczeniami swoich sieci oraz coraz bardziej złożonymi wymogami wynikającymi z nowych przepisów prawa i standardów bezpieczeństwa. Dążenie do przeprowadzenia transformacji cyfrowej wszystkich obszarów działalności biznesowej wymaga bardzo szybkiego rozwoju sieci, aby aplikacje, dane i usługi mogły być szybciej udostępniane coraz bardziej zróżnicowanemu środowisku użytkowników, domen i urządzeń. Dochodzi do tego konieczność zabezpieczenia się przed zagrożeniami wynikającymi z korzystania z urządzeń związanych z Internetem rzeczy i infrastruktury chmurowej, w którym to przypadku powierzchnia ataku może nawet nie być widoczna dla działu IT.

Szacuje się, że do 2020 r. 25% wszystkich ataków będzie skierowanych przeciwko urządzeniom związanym z Internetem rzeczy[1].

Do 2020 r. 83% zadań w przedsiębiorstwach będzie wykonywanych w chmurze[2].

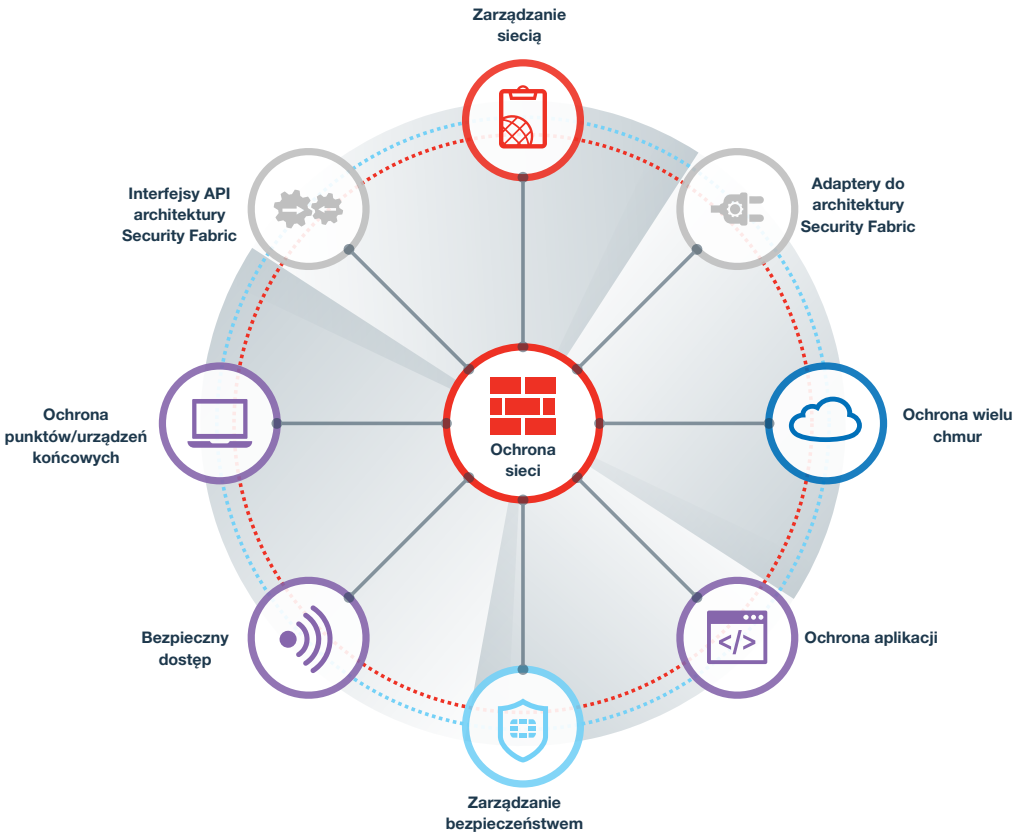
300 nowych funkcji systemu FortiOS 6.2, które zapewnią bezpieczną transformację cyfrową.

Ponad 75% przedsiębiorstw przyznaje, że wprowadza innowacje cyfrowe szybciej niż jest je w stanie zabezpieczyć przed cyberatakami[3].

Strukturalne podejście do bezpieczeństwa

Aby sprostać tym wyzwaniom, stosuje się czasem podejścia polegające na stosowaniu rozwiązań wielopunktowych i wieloplatformowych. Jak jednak wyglądałaby sytuacja, gdyby wszystkie dane i rozwiązania zabezpieczające z różnych środowisk przedsiębiorstwa były ściśle zintegrowane, zwarte i spójne niczym bezszwowa tkanina? Przedsiębiorstwo mogłoby wówczas widzieć, kontrolować i integrować zabezpieczenia całej swojej infrastruktury sieciowej i chmurowej oraz zarządzać nimi w ramach bezpiecznego cyfrowego modelu biznesowego. Ponadto mogłoby dynamicznie skalować i dostosowywać zabezpieczenia w miarę wdrażania kolejnych procesów i konieczności przetwarzania większej ilości danych. Jednocześnie byłoby zdolne do łatwego śledzenia i zabezpieczania danych, użytkowników i aplikacji w ramach różnych inteligentnych urządzeń, otwartych sieci i środowisk chmurowych.

Architektura Fortinet Security Fabric jest alternatywą efektywniejszą niż rozwiązania punktowe i platformowe. W jej ramach wszystkie zabezpieczenia są dla siebie dostępne w czasie rzeczywistym, aby zapewniać szeroko zakrojoną, zintegrowaną i zautomatyzowaną ochronę przed zaawansowanymi zagrożeniami. Sieciowy system operacyjny FortiOS zapewnia platformę służącą do wdrożenia i obsługi architektury Security Fabric. Najnowsza wersja tego systemu, FortiOS 6.2, zawiera ponad 300 nowych funkcji, które pomogą przedsiębiorstwu zrealizować ideę transformacji cyfrowej bez uszczerbku dla wydajności i bezpieczeństwa sieci.



Rys. 1. Architektura Fortinet Security Fabric.

Szeroki zakres — widoczność całej cyfrowej powierzchni ataku

Aby chronić przedsiębiorstwo, zabezpieczenia nie mogą funkcjonować samodzielnie jako izolowane urządzenia rozproszone w sieci. Architektura Security Fabric chroni całą powierzchnię ataku, aby powstrzymać ataki w wielu punktach. W tym celu system FortiOS 6.2 zapewnia większą widoczność i kontrolę nad całym otoczeniem, w tym punktami końcowymi, punktami dostępowymi, elementami sieci, centrum danych, chmurą, a nawet aplikacjami i samymi danymi. W połączeniu z segmentacją opartą na celach biznesowych, która logicznie rozdziela dane i zasoby, architektura Security Fabric chroni wszystkie ścieżki ataku, aby wykrywać i powstrzymywać złośliwe oprogramowanie, ilekroć próbuje się ono przedostać z jednej strefy sieci do drugiej. W ten sposób przedsiębiorstwa mogą chronić swoje sieci i dane.

Rozszerzone adaptery chmurowe i wirtualne w architekturze Security Fabric zapewniają pełną widoczność środowisk wielochmurowych, w tym chmur prywatnych, usług IaaS (infrastruktura jako usługa) i chmurowych mechanizmów kontroli. Chmurowe oprogramowanie pośredniczące FortiCASB-SaaS również zapewnia widoczność aplikacji SaaS i ich ochronę przed zaawansowanymi zagrożeniami. Dzięki takiej widoczności wielu chmur przedsiębiorstwo może skorelować ruch realizowany w swojej sieci i poza swoją siecią z poziomu jednej konsoli zarządzania zabezpieczeniami.

System FortiOS 6.2 obsługuje również rozwiązanie Fortinet Secure SD-WAN w ramach architektury Security Fabric, umożliwiając nadawanie aplikacjom priorytetów na potrzeby szczegółowej kontroli ruchu dotyczącego aplikacji SaaS, aplikacji Voice over IP (VoIP) i innych aplikacji o znaczeniu krytycznym. Inne nowości to między innymi funkcja kształtowania (ograniczenia) ruchu w celu zagwarantowania odpowiedniej przepustowości aplikacjom o znaczeniu krytycznym, funkcja bezobsługowego wdrożenia rozwiązania SD-WAN w oddziałach oraz funkcja tworzenia sieci VPN jednym przyciskiem myszy służąca łatwiejszemu korzystaniu z sieci VPN w celu uzyskania dostępu do chmury. Ponadto system FortiOS 6.2 korzysta z funkcji zapewniających użytkownikom odpowiednią jakość usług (QoE), dzięki którym nawet jeśli sieć wewnętrzną dotknęły problemy, użytkownik tego nie zauważy.

Integracja — zapobieganie naruszeniom bezpieczeństwa oparte na sztucznej inteligencji

Dla wielu przedsiębiorstw zabezpieczenie sieci stało się niezwykle złożonym zadaniem. Na bieżąco dodają one coraz więcej zabezpieczeń punktowych, aby eliminować nowe luki w zabezpieczeniach i ścieżki ataku. Zwiększa to z kolei presję na pracowników związaną z często ręcznymi procesami wdrażania, zarządzania i nadzoru. Dodatkowo nowe przepisy zwiększają wymagania w zakresie zapewnienia zgodności i sprawozdawczości. Złożoność tych wyzwań jest dodatkowo pogłębiana wskutek odczuwalnego na całym świecie niedoboru wykwalifikowanych specjalistów ds. bezpieczeństwa, zwłaszcza osób znających się na takich sprawach, jak bezpieczeństwo w chmurze, koncepcja DevSecOps i reagowanie na incydenty[4, 5].

Aby zapewnić kompleksową ochronę w warunkach rosnącej złożoności, wszystkie elementy infrastruktury zabezpieczeń przedsiębiorstwa

muszą ze sobą współdziałać w ramach jednego ujednoliconego systemu. Architektura Fortinet Security Fabric nie tylko zapewnia zintegrowane bezpieczeństwo w ramach urządzeń i systemów chroniących sieć rozproszoną, ale również pozwala na szybkie wykrywanie zaawansowanych zagrożeń. System FortiOS 6.2 oferuje wiele nowych inteligentnych funkcji, które umożliwiają precyzyjne wykrywanie zagrożeń w całej infrastrukturze. Przekazywane przez FortiGuard Labs dane uzyskane dzięki sztucznej inteligencji są rejestrowane przez architekturę Security Fabric, a następnie automatycznie przez nią rozsyłane do wszystkich wchodzących w jej skład urządzeń, co częściowo eliminuje negatywne skutki niedoboru personelu. Architektura ta może bowiem podejmować oparte na wynikach sprawdzonych analiz zautomatyzowane działania, takie jak usprawnianie komunikacji lub wdrażania poprawek, bez ograniczeń związanych z nadzorem lub interwencją człowieka.

Ponadto firma Fortinet na bieżąco udostępnia w ramach tej architektury nowe technologie i funkcje, umożliwiając jej skalowanie i rozwój w miarę pojawiających się potrzeb. System FortiOS 6.2 zapewnia obsługę protokołu TLS 1.3, aby zagwarantować niezakłócony, bezpieczny dostęp do Internetu. Nowe rozwiązanie FortiDeceptor oparte na podstępach (ang. deception-based security) pozwalające na wykrywanie aktywnych włamań i aktywnych hakerów.

Automatyzacja — operacje, procesy i reakcje

Integracja i automatyzacja idą w parze. Reakcja na wykryte zagrożenie musi być natychmiastowa, aby je zminimalizować. Architektura Fortinet Security Fabric minimalizuje czas upływający od momentu ataku do momentu jego wykrycia oraz od momentu wykrycia ataku do momentu podjęcia przeciwdziałań. Architektura ta zestawia również informacje o zagrożeniu, aby określić poziom ryzyka, oraz automatycznie synchronizuje skoordynowane przeciwdziałania. Ponadto odpowiednio rozsyła dane o wykrytych nowych zagrożeniach, dynamicznie izoluje zaatakowane urządzenia, wydziela segmenty sieci, aktualizuje reguły, propaguje nowe zasady i usuwa złośliwe oprogramowanie. Poza zmniejszeniem narażenia na ryzyko, zastąpienie ręcznych procesów bezpieczeństwa procesami zautomatyzowanymi pomaga również sprostać wyzwaniom organizacyjnym związanym z ograniczonym budżetem i brakiem wykwalifikowanych pracowników.

Nowe funkcje architektury Security Fabric

Architektura Fortinet Security Fabric oferuje również zestaw funkcji pozwalających na kompleksowe uproszczenie zarządzanie siecią, w tym m.in. możliwości zautomatyzowania procesu inwentaryzacji aplikacji na poszczególnych urządzeniach oraz zautomatyzowania reakcji na zdarzenia dotyczące bezpieczeństwa na przełącznikach Fortinet i w punktach bezprzewodowego dostępu do sieci. Zautomatyzowane procesy z dokonywaną na bieżącą oceną ryzyka pozwalają na łatwe konfigurowanie reakcji na podstawie wstępnie zdefiniowanych wyzwalaczy takich jak zdarzenia systemowe, alerty oraz statusy użytkowników i urządzeń. Takie reakcje (na przykład kwarantanna, powiadomienia lub korekty konfiguracji) i niestandardowe raporty zapewniają kontrolę w czasie rzeczywistym nad środowiskami związanymi z tymi procesami. Zautomatyzowane funkcje audytu są natomiast źródłem danych o tendencjach w zakresie zgodności z przepisami i standardami bezpieczeństwa, którym to danym towarzyszą zestawienia porównujące stan bezpieczeństwa przedsiębiorstwa ze stanem bezpieczeństwa podobnych do niego przedsiębiorstw w kategoriach rozmiaru i branży.

Tylko rozwiązanie firmy Fortinet zapewnia prawdziwą możliwość zarządzania z poziomu jednej konsoli wszystkimi rozwiązaniami wchodzącymi w skład danej infrastruktury (od rozwiązań własnych firmy Fortinet po zintegrowane z architekturą Security Fabric rozwiązania rozległego ekosystemu partnerów i innych firm). Wspomniana możliwość zarządzania z poziomu jednej konsoli dodatkowo upraszcza obsługę operacji i reakcji, które wykraczają poza zautomatyzowane zasady i reguły.

Inne nowe funkcje systemu FortiOS 6.2 obsługują najlepsze praktyki w zakresie audytu i zapewnienia zgodności, aby ułatwić przestrzeganie i wdrażanie najnowszych standardów i przepisów, począwszy od normami PCI DSS (Payment Card Industry Data Security Standard). System FortiOS ma również wbudowane reguły, dzięki czemu można uniknąć długotrwałych procesów tworzenia reguł, które mogą być trudne do wyegzekwowania i czasochłonne w śledzeniu.

Korzyści oferowane przez system FortiOS 6.2:

- Segmentacja oparta na celach biznesowych
- Secure SD-WAN
- Zadowolenie użytkownika końcowego
- Informacje o zagrożeniach uzyskane dzięki sztucznej inteligencji
- Zabezpieczenia oparte na podstępach
- Zautomatyzowana reakcja
- Najlepsze praktyki w zakresie audytu i zgodności z przepisami
- Zarządzanie z poziomu jednej konsoli

Zdolność do wykrywania zaawansowanych zagrożeń i naruszeń bezpieczeństwa jest niezbędna w kontekście 40% wzrostu liczby przypadków wykrycia nowego złośliwego oprogramowania[6].

Tylko 38% przedsiębiorstw korzysta z funkcji automatyzacji, sztucznej inteligencji i uczenia maszynowego[7].

Podsumowanie

Transformacja cyfrowa stawia przed przedsiębiorstwem wiele wyzwań w zakresie bezpieczeństwa. Tendencje w zakresie technologii obliczeniowych i sieciowych będą nadal stymulować zmiany w infrastrukturach, architekturach i praktykach biznesowych, podczas gdy cyberprzestępcy będą nadal rozwijać coraz to lepsze sposoby wykorzystywania luk w zabezpieczeniach. W tym kontekście przedsiębiorstwa muszą zastosować nowe podejście do zabezpieczenia całej swojej infrastruktury rozproszonej. Fortinet Security Fabric to inteligentna architektura bazująca na skalowalnych, wzajemnie połączonych zabezpieczeniach oraz wspomagana użytecznymi informacjami o zagrożeniach i otwartymi standardami API, która zapewnia nieprzerwaną ochronę najbardziej wymagających środowisk korporacyjnych.

System FortiOS 6.2 jest najnowszą wersją systemu operacyjnego zabezpieczeń sieciowych firmy Fortinet. Dzięki setkom rozszerzeń i dodatków funkcji, wzbogaca architekturę Security Fabric o większą widoczność i kontrolę całej powierzchni ataku. Zapewnia również zintegrowane, oparte na sztucznej inteligencji funkcje zapobiegania naruszeniom bezpieczeństwa sieci w celu wykrywania zagrożeń i zapewnienia nieprzerwanej ochrony. Ponadto udostępnia funkcje automatyzowania operacji, automatyzowania procesów i reagowania na zagrożenia, które szybko identyfikują i rozwiązują problemy związane z bezpieczeństwem, umożliwiając jednocześnie uproszczenie i zwiększenie wydajności zabezpieczeń.

[1] „25% Of Cyberattacks Will Target IoT In 2020", Retail TouchPoints, dostęp z dnia 21 marca 2019 r.

[2] Louis Columbus, „83% Of Enterprise Workloads Will Be In The Cloud by 2020", Forbes, 7 stycznia 2018 r.

[3] Kelly Bissell, et al., „The Cost of Cybercrime: Ninth Annual Cost of Cybercrime Study", Accenture and Ponemon, 6 marca 2019 r.

[4] „Cybersecurity Skills Shortage Soars, Nearing 3 Million" (ISC)[2], 18 października 2018 r.

[5] Dawn Kawamoto, „Top 8 Cybersecurity Skills IT Pros Need in 2018", Dark Reading, 18 grudnia 2017 r.

[6] Dane wewnętrzne z FortiGuard Labs.

[7] Kelly Bissell, et al., „The Cost of Cybercrime: Ninth Annual Cost of Cybercrime Study", Accenture and Ponemon, 6 marca 2019 r.

FORTINET

www.fortinet.com

15 lipca 2019; 09:09
D:\Projekty\Fortinet (United Kingdom)\P-344888\03_DTP (Multi)\Work\sb-fortiOS-6.2_A4\sb-fortiOS-6.2_A4

384970-0-1-PL