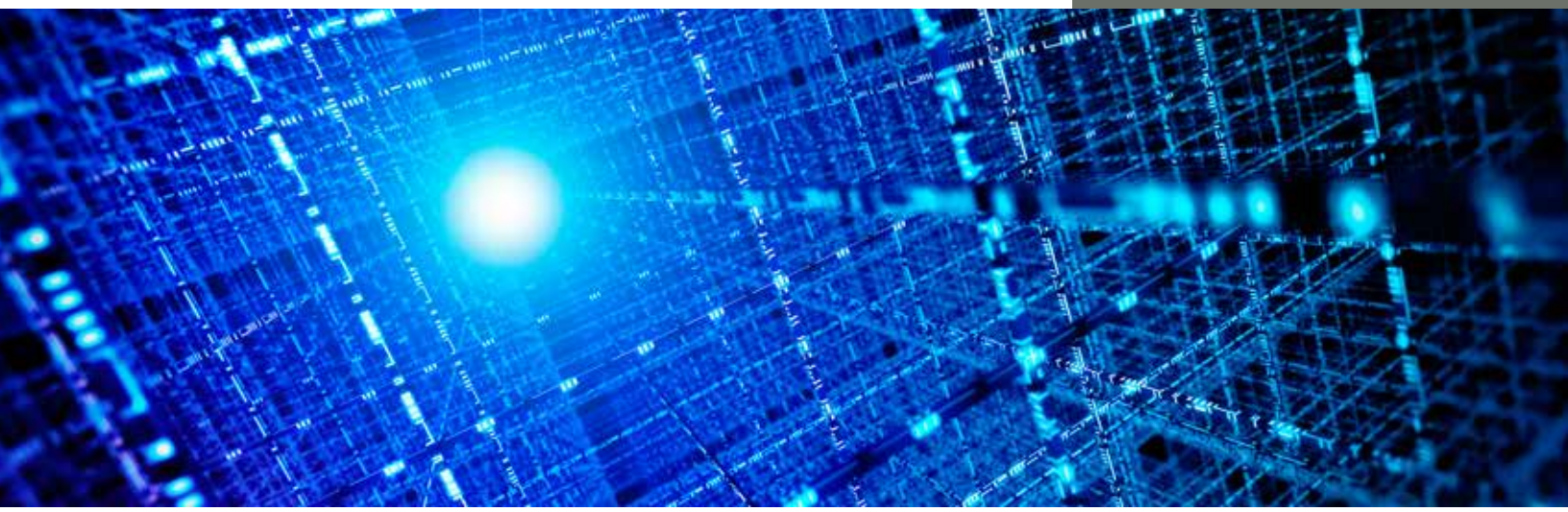


Fortinet Security Fabric

Segmentacja kompleksowa

Zmiany zachodzące obecnie w sieciach są najbardziej radykalnymi ze zmian wprowadzanych w ciągu ostatnich trzydziestu lat. Organizacje muszą zmagać się równocześnie z takimi zagadnieniami, jak polityka BYOD, Internet rzeczy, wirtualizacja, sieci SDN, usługi w chmurze, rosnąca liczba aplikacji, Big Data, a także oczekiwania pracowników nowej generacji, którzy chcieliby łączyć życie zawodowe i prywatne, korzystając z jednego, samodzielnie wybranego urządzenia z natychmiastowym dostępem do danych w dowolnym momencie i z dowolnej lokalizacji.

Spowodowało to wykładniczy wzrost obszaru ataku, który muszą mieć na uwadze organizacje. Na przykład

- Internet rzeczy oraz rozwiązania chmurowe oznaczają dla organizacji konieczność uwzględnienia obszaru ataku, który w wielu przypadkach może nie być widoczny dla działu IT
- Wiele spośród urządzeń związanych z Internetem rzeczy to urządzenia bez interfejsu, które służą do uruchamiania prostych protokołów łączności i nie można uruchomić na nich klienta ani nawet zastosować poprawki. Ich zabezpieczenia oparte są wyłącznie na sieci dostępu.
- Dane biznesowe o znaczeniu krytycznym oraz dane zastrzeżone są przenoszone do rozwiązań chmurowych i zarządzane przez strony trzecie. Ta tendencja, określana mianem „Shadow IT" (systemy IT pozostające poza kontrolą organizacji), jest coraz powszechniejsza i w wielu organizacjach trudno nawet ustalić, gdzie obecnie znajdują się dane ani jakie zabezpieczenia są stosowane w celu zapewnienia ich ochrony.
- Przekształcenia zmierzające do wytworzenia cyfrowego modelu biznesowego sprawiły, że sieci rozciągają się obecnie poza wyznaczone granice, co oznacza, iż dzisiejsze sieci i związane z nimi zabezpieczenia przestają mieć granice.
- Urządzenia prywatne wykorzystywane przez pracowników do celów służbowych (w ramach polityki BYOD) są wyjątkowo mobilne, używane są na nich równocześnie profile osobiste oraz służbowe, przez co stanowią one realne zagrożenie, ponieważ dostęp do danych o decydującym znaczeniu uzyskiwany jest w miejscach publicznych, a także w związku z możliwym zgubieniem lub kradzieżą urządzenia.

Sprawę komplikuje dodatkowo wzrost liczby produktów pełniących funkcję zabezpieczeń punktowych wbudowanych w sieci rozproszone. Wraz ze wzrostem stopnia złożoności sieci mamy skłonności do dodawania kolejnych rozwiązań zabezpieczających w środowiskach, które już są przeciążone. Wiadomo jednak, że złożoność nie sprzyja bezpieczeństwu. Nakładające się na siebie rozwiązania zabezpieczające z osobnymi interfejsami zarządzania i brakiem sensownego sposobu gromadzenia informacji o zagrożeniach oraz udostępniania ich urządzeniom w sieci są raczej mało przydatne. Wiele spośród nowych rozwiązań nigdy nie zostaje w pełni wdrożona ze względu na niewystarczającą liczbę pracowników, którym należałoby zlecić instalowanie, zarządzanie, optymalizowanie i aktualizowanie kolejnych skomplikowanych urządzeń.

Zamiast tego reakcją na wzrost stopnia złożoności środowisk sieciowych powinna być prostota. Do zapewnienia bezpieczeństwa w tego rodzaju ewoluujących środowiskach potrzebne są trzy rzeczy:

1. Segmentacja — w sieciach należy wprowadzić inteligentną segmentację z zastosowaniem funkcjonalnych stref bezpieczeństwa. Segmentacja kompleksowa — od Internetu rzeczy po chmurę oraz w ramach środowisk fizycznych i wirtualnych — zapewnia dogłębną analizę ruchu sieciowego związanego z komunikacją lateralną w sieci rozproszonej, ogranicza rozprzestrzenianie się złośliwego oprogramowania oraz umożliwia identyfikowanie zainfekowanych urządzeń i poddawanie ich kwarantannie.
2. Wspólny system informacji — informacje o zagrożeniach lokalnych i globalnych powinny być udostępnianie pomiędzy urządzeniami, a reakcje urządzeń powinny być koordynowane centralnie.
3. Uniwersalne polityki — scentralizowane zasady zabezpieczeń, w ramach których ustalane są poziomy zaufania pomiędzy segmentami sieci, informacje o zagrożeniach gromadzone są w czasie rzeczywistym, ustalane są jednolite zasady zabezpieczeń, a egzekwowanie zasad jest odpowiednio koordynowane.

Platforma Fortinet Security Fabric umożliwia zintegrowanie technologii stosowanych w punkcie końcowym, warstwie dostępu, sieci, aplikacjach, centrum danych, zawartości i chmurze w ramach jednego rozwiązania zabezpieczeń opartego na współdziałaniu, którym można zarządzać za pośrednictwem jednego interfejsu. Rozwiązanie to opiera się na pięciu głównych zasadach:

- **Skalowalność: platforma Fortinet Security Fabric zapewnia przedsiębiorstwu ochronę — od Internetu rzeczy po chmurę.**

  Wszechstronna strategia zabezpieczeń powinna być głęboka (wydajność i inspekcja szczegółowa), a równocześnie powinna obejmować szeroki zakres (działać kompleksowo). Potrzebna jest możliwość skalowania zabezpieczeń w zależności od wymogów związanych z wielkością i wydajnością, skalowania lateralnego z ciągłym śledzeniem i zabezpieczaniem danych, począwszy od Internetu rzeczy i punktów końcowych, poprzez sieć rozproszoną, po chmurę. Fortinet Security Fabric to rozwiązanie zapewniające nieprzerwaną ochronę w całym przedsiębiorstwie rozproszonym — od Internetu rzeczy po chmurę, a także kontrolowanie danych pakietowych i protokołów aplikacji oraz dogłębną analizę treści nieustrukturyzowanych, przy czym wszystkie te działania muszą dorównywać szybkości łączy.

- **Przepływ informacji: platforma Fabric jest rozwiązaniem całościowym z perspektywy polityk i logowania, co umożliwia stosowanie segmentacji kompleksowej w celu obniżenia ryzyka związanego z zaawansowanymi zagrożeniami.**

  Potrzebny jest nie tylko wgląd w to, jakie dane napływają do sieci i wypływają z niej, ale również w to, w jaki sposób dane poruszają się po sieci, gdy znajdą się już wewnątrz niej. Platforma Fortinet Security Fabric umożliwia zastosowanie kompleksowej segmentacji sieci, pozwalając na dogłębną analizę i weryfikację ruchu sieciowego oraz ustalanie kto i co dociera do jakich miejsc docelowych, dzięki czemu można obniżyć ryzyko związane z zaawansowanymi zagrożeniami.

- **Bezpieczeństwo: informacje o zagrożeniach lokalnych i globalnych oraz informacje związane z łagodzeniem skutków ataków mogą być udostępniane pomiędzy poszczególnymi produktami w celu skrócenia czasu niezbędnego do zapewnienia ochrony.**

  Zabezpieczenia powinny obejmować potężne narzędzia zapewniające ochronę poszczególnych miejsc i funkcji w sieci, jednak w celu uzyskania rzeczywistej widoczności i kontroli niezbędna jest współpraca tych elementów w ramach zintegrowanego systemu zabezpieczeń. Platforma Fortinet Security Fabric jest opartym na współpracy rozwiązaniem całościowym z perspektywy polityk i logowania, co umożliwia rozpowszechnianie pomiędzy poszczególnymi elementami informacji o zagrożeniach globalnych i lokalnych oraz informacji dotyczących łagodzenia skutków ataków.

- **Skuteczność: w systemach chmurowych typu Big Data informacje o zagrożeniach i dane sieciowe są korelowane, by uzyskiwać w czasie rzeczywistym informacje umożliwiające skuteczne przeciwdziałanie zagrożeniom.**

  Samo wykrycie podejrzanego ruchu czy zablokowanie złośliwego oprogramowania przy użyciu zabezpieczeń nie wystarczy. Niezbędny jest ujednolicony zbiór informacji o zagrożeniach oraz scentralizowane zarządzanie, które umożliwia dynamiczne dostosowywanie zabezpieczeń w przypadku wykrycia zagrożenia w dowolnym miejscu — nie tylko w samej sieci, ale w dowolnym miejscu na świecie. W systemach chmurowych firmy Fortinet typu Big Data informacje o zagrożeniach są korelowane z danymi sieciowymi w celu dostarczenia informacji zapewniających skuteczne działanie wszystkich urządzeń zabezpieczających w ramach platformy Security Fabric w czasie rzeczywistym.

- **Otwartość: dobrze zdefiniowane, otwarte interfejsy API umożliwiają partnerom dostarczającym wiodące technologie dołączanie do platformy.**

  Skutecznie działająca platforma Security Fabric umożliwia oczywiście najpełniejsze wykorzystanie dotychczasowych inwestycji w technologie zabezpieczeń. Dlatego właśnie w firmie Fortinet opracowano szereg dobrze zdefiniowanych, otwartych interfejsów API, dzięki którym partnerzy technologiczni mogą dołączać do platformy Fortinet Security Fabric.

  Dzięki połączeniu tych technologii platforma Fortinet Security Fabric może dynamicznie dostosowywać się do ewoluującej architektury sieci, a także do zmieniających się zagrożeń.

Przyjrzyjmy się bliżej pięciu najważniejszym elementom platformy Fortinet Security Fabric, którymi są: skalowalność, przepływ informacji, bezpieczeństwo, skuteczność i otwartość.

1. Skalowalność

Aby spełnić wymogi związane z wielkością i wydajnością, nie wystarczy, by zabezpieczenia były skalowalne. Potrzebne jest skalowanie lateralne z ciągłym śledzeniem i zabezpieczaniem danych, począwszy od Internetu rzeczy i punktów końcowych, poprzez sieć rozproszoną, po chmurę.

Platforma Fortinet Security Fabric zapewnia trzy niezbędne elementy, którymi są:

1. Pojedyncza, ujednolicona platforma udostępniająca wspólne informacje o zagrożeniach, która umożliwia inteligentną współpracę pomiędzy urządzeniami zabezpieczającymi i dynamicznie dostosowuje się do nowych zagrożeń.
2. Zarządzanie z jednej konsoli wszystkimi technologiami zabezpieczeń, niezależnie od miejsca ich wdrożenia, w celu zapewnienia scentralizowanego koordynowania polityk i reakcji na zagrożenia oraz rozproszonego egzekwowania w czasie rzeczywistym.
3. Jedno źródło informacji dotyczących bezpieczeństwa oraz aktualizacji, w ramach którego informacje lokalne zostają powiązane z globalnymi usługami informacyjnymi, co umożliwia reagowanie w czasie rzeczywistym na znane i nowe zagrożenia.

Skalowalność w chmurze

Upowszechnianie się wirtualizacji oraz usług chmurowych powoduje przekształcanie się sieci. Z migracją do rozwiązań chmurowych wiąże się wiele konkretnych problemów związanych z zabezpieczeniami, które można rozwiązać wyłącznie poprzez zastosowanie platformy zabezpieczeń:

1. **Wirtualizacja i chmura prywatna.** Z wirtualizacją mamy wprawdzie do czynienia już od jakiegoś czasu, jednak stanowi ona nadal w wielu sieciach podatny na zagrożenia i w znacznym stopniu nieobjęty ochroną obszar. W strategii umożliwiającej zapewnienie bezpieczeństwa w środowiskach zwirtualizowanych należy wziąć pod uwagę wiele czynników.

   Pierwszym z nich jest fakt, że w około 40% organizacji wirtualizacja kończy się wdrożeniem wielu środowisk wirtualnych. W celu zapewnienia nieprzerwanej i spójnej ochrony we wszystkich tych zwirtualizowanych środowiskach rozwiązania zapewniające bezpieczeństwo muszą działać we wszystkich najważniejszych środowiskach wirtualnych.

   Kolejne wyzwanie polega na tym, że niektóre z rozwiązań wirtualizacyjnych powodują rozziew pomiędzy zasobami fizycznymi a wirtualnymi, który należy wyeliminować poprzez zastosowanie rozwiązań zapewniających ujednolicony przepływ informacji oraz egzekwowanie zabezpieczeń niezależnie od urządzeń przetwarzających dane.

   Wiele nowych ataków jest ukierunkowanych konkretnie na maszyny wirtualne, przy czym ich obecność jest maskowana wirtualnymi rootkitami. W wielu organizacjach ruch pomiędzy maszynami wirtualnymi często nie jest kontrolowany, co sprawia, że maszyny wirtualne, procesy biznesowe i transakcje są wyjątkowo podatne na ataki.

   Wirtualizacja umożliwia również szybkie wdrażanie nowych zasobów do obsługi prcesów biznesowych oraz dynamiczne skalowanie w celu zarządzania nagle zwiększającymi się przepływami danych. Zabezpieczenia w środowiskach zwirtualizowanych muszą być szybko realizowane, a ich skala musi być szybko dostosowywana, by transakcje i procesy biznesowe o decydującym znaczeniu nie były zakłócane ani niepotrzebnie przekierowywane w celu przeprowadzenia kontroli.

   Dzięki zabezpieczeniom platformowym w organizacjach możliwe jest tworzenie polityk zabezpieczeń, które zapewniają ciągłość ich działania na styku środowisk fizycznych, wirtualnych i chmury prywatnej.

2. **Centra danych SDN nowej generacji.** Również w centrach danych można zaobserwować szybkie zmiany, takie jak wdrażanie sterowanych programowo sieci nowej generacji oraz środowisk chmur prywatnych. W tych nowych architekturach możliwe jest błyskawiczne dostarczanie zasobów, powiązywanie usług oraz usprawnianie procesów biznesowych przy równoczesnym eliminowaniu kosztów związanych z zarządzaniem warstwą fizyczną portów, serwerów przełączników.

   W tego rodzaju nowych centrach danych niezbędne są dedykowane rozwiązania zabezpieczające dostosowane do konkretnych architektur. Ponadto te nowe środowiska działają równolegle z tradycyjnymi centrami danych, w związku z czym trudno jest wdrożyć jeden standard zabezpieczeń. Kolejnym utrudnieniem jest fakt, że w niektórych rozwiązaniach SDN trudno jest połączyć środowiska wirtualne i fizyczne, zatem ustanowienie i wyegzekwowanie ujednoliconych polityk bezpieczeństwa może nastręczać trudności.

   Zaletą jest to, iż możliwość wbudowania usług zabezpieczających bezpośrednio w łańcuchy transakcyjne pozwala wykorzystać je do automatycznego zapewniania zabezpieczeń ruchu wschód-zachód oraz dynamiczne skalowanie zasobów zabezpieczających.

   Podobnie jak w przypadku wirtualizacji, strategia platformowa umożliwia organizacji rozmieszczenie urządzeń zabezpieczających w różnych środowiskach architekturalnych przy równoczesnym zachowaniu scentralizowanych informacji o zagrożeniach oraz ujednoliconego egzekwowania polityk.

3. **Chmura publiczna i hybrydowa.** Wiele organizacji decyduje się na zastosowanie usług w chmurze do obsługi wszelkich zadań, od rozładowania wysokiego natężenia ruchu, czyli procedury zwanej „cloud bursting", po przeniesienie części lub całości infrastruktury do chmury z pewnego rodzaju oprogramowaniem, platformą lub infrastrukturą jako usługą.

   Z punktu widzenia zabezpieczeń wyzwanie polega na ustanowieniu i utrzymaniu jednolitych polityk bezpieczeństwa i na egzekwowaniu ich w odniesieniu do danych przesyłanych pomiędzy środowiskami lokalnymi a chmurowymi.

   Aby takie rozwiązanie mogło działać, niezbędne jest spełnienie dwóch warunków. Pierwszym jest nawiązanie współpracy z dostawcą usług, który może zastosować w obsługiwanym środowisku chmurowym tę samą technologię zabezpieczeń, jaka jest stosowana wewnątrz organizacji. Oznacza to konieczność wybrania wewnątrz organizacji rozwiązania, które jest rozpowszechnione w społeczności dostawców usług. Drugim jest działające w chmurze narzędzie do

zarządzania zabezpieczeniami będące w stanie przesyłać polityki oraz informacje związane z zabezpieczeniami pomiędzy urządzeniami zabezpieczającymi wdrożonymi w środowiskach rozproszonych.

W ramach platformy Fortinet Security Fabric dostępne są rozwiązania dla wszystkich tych środowisk, z uwzględnieniem rozwiązań zabezpieczających najpowszechniej stosowanych przez dostawców usług na rynku, które można połączyć w jedną spójną platformę zabezpieczeń w celu osiągnięcia pełnej widoczności i kontroli w całym środowisku rozproszonym.

Skalowalność do potrzeb sieci

W związku z tym, że dostęp do zasobów sieciowych uzyskuje coraz więcej urządzeń i aplikacji, wydajność ma decydujące znaczenie i spowolnienie sieci nie wchodzi w grę. W sytuacjach, gdy zabezpieczenia stają się wąskim gardłem, użytkownicy i administratorzy zdecydowanie nazbyt często zaczynają szukać rozwiązań zastępczych.

Tradycyjne rozwiązania zabezpieczające, których podstawą jest przetwarzanie oparte na procesorach, zwyczajnie nie dają się skalować w sposób umożliwiający dostosowanie skali do narastającego zapotrzebowania.

- Wydajność urządzeń zabezpieczających obniża się w przypadku dodania kolejnych narzędzi do przeprowadzania kontroli.
- Łańcuchowe łączenie urządzeń zabezpieczających w celu zapewnienia seryjnej kontroli ruchu nastręcza dodatkowe problemy związane z opóźnieniami oraz nadmiarowymi kontrolami tych samych danych lub zawartości aplikacji.

W urządzeniach zabezpieczających firmy Fortinet oraz w platformie Security Fabric zastosowano opatentowane moduły ASIC o wysokiej wydajności, za pomocą których odbywa się równoległe przetwarzanie ruchu. Oznacza to, że:

- kontrolowanie pakietów można usprawnić poprzez przekierowanie przetwarzania pakietów do procesora sieciowego;
- zawartość może zostać przekazana do nowego procesora typu content processor firmy Fortinet, który poddaje dane nieustrukturyzowane dogłębnej analizie pochłaniającej znaczące zasoby;
- procesor może być wykorzystywany jedynie do tradycyjnego przetwarzania danych i zarządzania politykami;
- uaktualnianie informacji o zagrożeniach oraz koordynowanie polityk może odbywać się bez wpływu na operacje o decydującym znaczeniu dla organizacji.

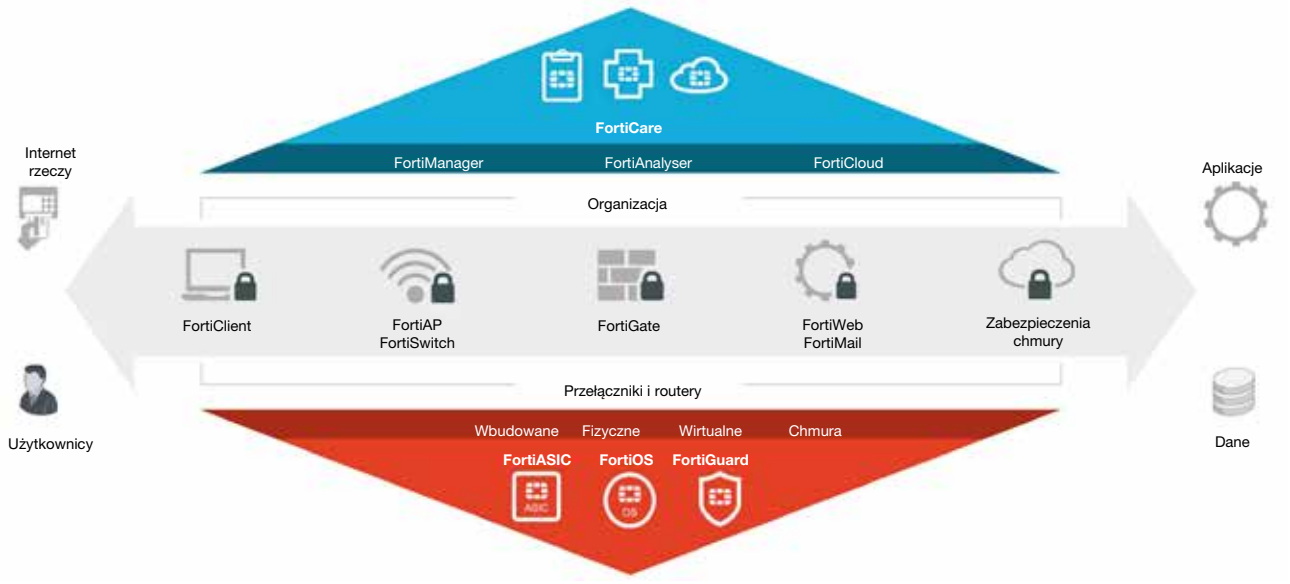
Efektem jest uzyskanie wyższej wydajności przy równoczesnym obniżeniu kosztów, zmniejszeniu opóźnień, obniżeniu zużycia energii oraz zmniejszeniu zapotrzebowania na przestrzeń serwerową.

Skalowalność zabezpieczeń dostępu

Kontrola dostępu ma decydujące znaczenie w każdej strategii zabezpieczeń. Gdy jest częścią platformy Security Fabric, urządzenia nawiązujące w ramach sieci połączenia, zarówno spoza sieci, jak i w jej obrębie, mogą być identyfikowane, śledzone i objęte ochroną, gdy uczestniczą w ruchu w środowisku sieciowym.

Wraz z polityką BYOD pojawiła się pierwsza fala nowych urządzeń stających się częścią sieci, jednak wraz z nastaniem Internetu rzeczy organizacje będą zmuszone zmierzyć się w ciągu następnych kilku lat z miliardami nowych urządzeń wykorzystujących protokół IP nieobsługiwanych przez użytkowników. Zabezpieczenia dostępu muszą teraz tym bardziej pełnić rolę pierwszego etapu zabezpieczeń, ponieważ:

- wielu z tych urządzeń nie można wyposażyć w niezależne zabezpieczenia;
- większość urządzeń w Internecie rzeczy nie ma interfejsów, co oznacza niemożność zainstalowania klientów czy poprawek błędnego lub niezabezpieczonego kodu oraz brak mechanizmów aktualizacji;
- na wielu spośród urządzeń prywatnych wykorzystywanych do celów służbowych nie można zainstalować klienta.



Wraz z postępującym rozmywaniem się krawędzi sieci, w zabezpieczeniach dostępu konieczne jest uwzględnienie więcej niż tylko dostępu do jej obrzeży:

- urządzenia mogą być lokalne lub zdalne i znajdować się wewnątrz sieci lub poza jej obrzeżem;
- aplikacje są przekierowywane bezpośrednio z urządzeń zdalnych do centrum danych lub chmury;
- zabezpieczenia dostępu pomiędzy segmentami sieci są niezbędne dla zapewnienia, że dostęp do zasobów o decydującym znaczeniu uzyskują wyłącznie upoważnieni do tego użytkownicy i urządzenia, a zainfekowane urządzenia nie są w stanie rozpowszechniać złośliwego oprogramowania w sieci w ramach komunikacji lateralnej;
- polityki zabezpieczeń i ich egzekwowanie muszą być dostosowywane dynamicznie do stale zmieniających się warunków.

Odpowiedzią na bardziej złożone problemy musi być prostota. Platformowe podejście do zabezpieczeń umożliwia organizacjom tworzenie i monitorowanie spójnej i ujednoliconej strategii w ramach wszystkich metod uzyskiwania dostępu, zarówno w sieciach przewodowych, bezprzewodowych, jak i w wirtualnych sieciach prywatnych (VPN).

2. Przepływ informacji

Widoczność ma decydujące znaczenie. Niestety w rzeczywistości wiele organizacji ma bardzo ograniczony wgląd w to, jacy użytkownicy i jakie urządzenia łączą się w danym momencie z ich siecią. Taki stan rzeczy był do przyjęcia dawno temu, gdy obrzeża sieci były sztywne i wyraźnie zdefiniowane. Jednak w związku z pojawieniem się w ramach sieci polityki BYOD, Internetu rzeczy, wirtualizacji, chmury oraz gotowych aplikacji brak odpowiedniej widoczności musi prowadzić do katastrofy. W skutecznej strategii przepływu informacji należy uwzględnić następujące elementy:

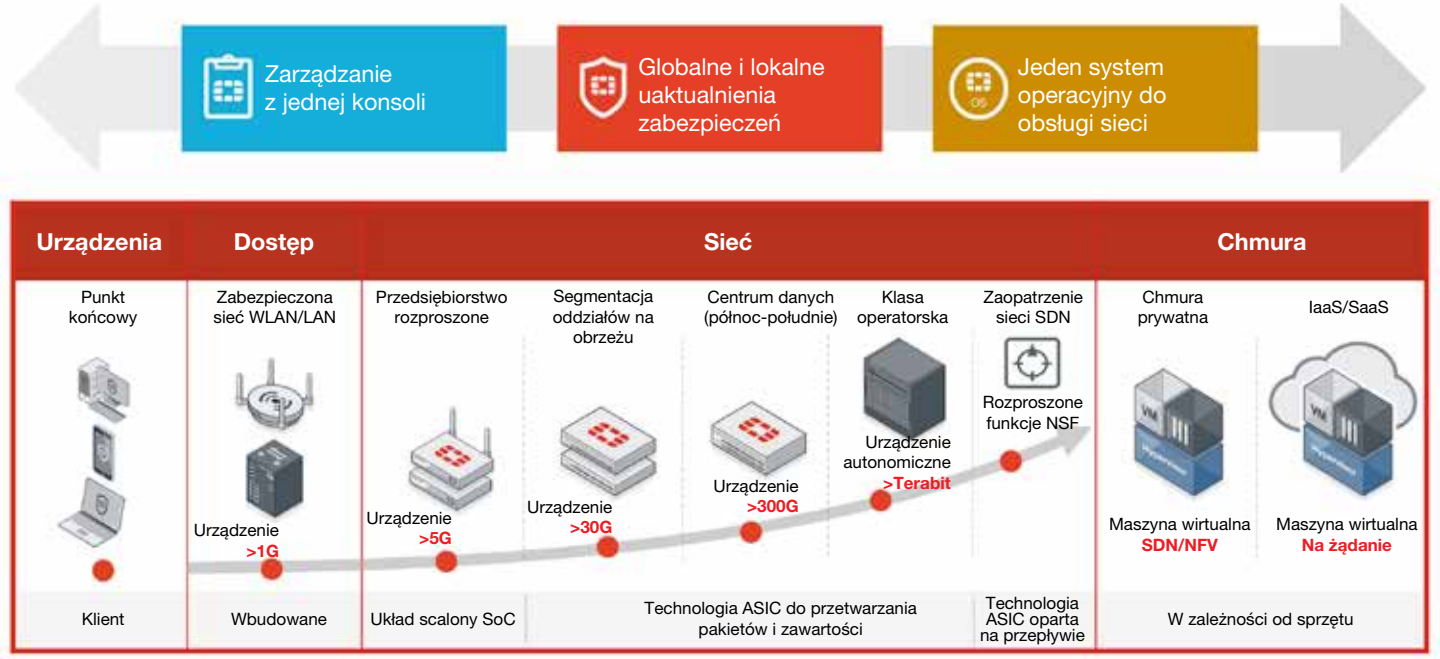
- Identyfikacja użytkowników — Kto korzysta z sieci? Jakie uprawnienia mają użytkownicy? Kiedy użytkownicy dołączają do sieci?
- Identyfikacja urządzeń — Jakie urządzenia korzystają z sieci? Do kogo należą? Jakie mają uprawnienia? W jaki sposób wykryć, że zaczynają zachowywać się w niewłaściwy sposób?
- Topologia fizyczna — W jaki sposób urządzenia łączą się z siecią? Z jakimi urządzeniami mogą lub nie mogą nawiązywać interakcji?
- Topologia sieci i aplikacji — Jakie polityki są potrzebne? W jaki sposób są rozpowszechniane i egzekwowane? Czy dysponujemy ujednoliconym widokiem całej sieci? Skąd wiadomo, że doszło do naruszenia polityki? Czy naruszenie wykryte w jednym urządzeniu może wywołać zautomatyzowaną reakcję na innym urządzeniu?

Możliwość udzielenia odpowiedzi na te pytania może stać się katalizatorem przy planowaniu, projektowaniu, wdrażaniu i optymalizowaniu skutecznej strategii przepływu informacji. Może również posłużyć jako ważny wskaźnik, umożliwiający ocenę technologii zabezpieczających wybranych do obsługi danej sieci.

Przepływ informacji — zalety platformy Fortinet Security Fabric

Konieczność zapewnienia wszechstronnej widoczności w całym przedsiębiorstwie rozproszonym, a także szczegółowej kontroli i zautomatyzowanych reakcji w wielu urządzeniach zabezpieczających były najważniejszym bodźcem do opracowania przez firmę Fortinet platformy Security Fabric. Ta platforma umożliwia powiązanie ze sobą danych, aplikacji, urządzeń i procesów biznesowych w celu zapewnienia przepływu informacji na poziomie niedostępnym dotąd w rozwiązaniach jakiegokolwiek dostawcy zabezpieczeń. Platforma Fortinet Security obejmuje:

- Zabezpieczenia klienckie w punktach końcowych



- Zabezpieczenia dostępu (w ramach sieci przewodowych, bezprzewodowych i VPN)
- Zabezpieczenia sieci
- Zabezpieczenia centrów danych (fizycznych i wirtualnych)
- Zabezpieczenia aplikacji (w ramach usług OTS i niestandardowych)
- Zabezpieczenia chmury
- Zabezpieczenia zawartości (poczta elektroniczna i strony internetowe)
- Zabezpieczenia infrastruktury (przełączniki i routery)

Platformę Fortinet Security Fabric stworzono z myślą o zapewnieniu integracji, współpracy i dostosowywania egzekwowania polityk w sieci rozproszonej oraz o dynamicznym konwertowaniu rzeczywistych danych, dzienników i zdarzeń na polityki.

3. Bezpieczeństwo

Aby zapewnić skuteczne działanie zintegrowanej strategi zabezpieczeń, niezbędne jest ustanowienie jednego źródła informacji. W złożonych środowiskach obsługiwanych przez wielu dostawców pojawiają się dwa problemy:

- brak jednolitego pojmowania wykrywanych lub poszukiwanych zagrożeń,
- niemożność udostępnienia skutecznych informacji o zagrożeniach innym urządzeniom zabezpieczającym.

Informacje o zagrożeniach muszą mieć charakter globalny

Wiedza to potęga. Skuteczność dowolnej strategii zabezpieczeń czy rozwiązania polega na zdolności rozpoznawania zagrożeń i reagowania na nie, a w szczególności na niespotkane dotąd zagrożenia. Nieustanne uaktualnianie informacji umożliwiających skuteczne działanie na podstawie zaufanego źródła, w którym informacje z całego świata są gromadzone w czasie rzeczywistym umożliwia reagowanie w ramach rozwiązań na najnowsze zagrożenia. Działa to jeszcze skuteczniej, gdy w ramach platformy Security Fabric współdzielone są te same informacje.

Laboratorium FortiGuard zajmujące się badaniem zagrożeń dostarcza urządzeniom działającym w ramach platformy Security Fabric informacje dotyczące zabezpieczeń z następujących źródeł:

- Threat Intelligence Exchange: Cyber Threat Alliance to konsorcjum złożone z czołowych dostawców rozwiązań zabezpieczających, którzy postanowili wspólnie udostępniać informacje o zagrożeniach związane z zaawansowanymi atakami oraz o motywach i taktykach stojących za nimi sprawców. Wspólnie zapewniają dostęp do najbardziej wyczerpujących informacji o zagrożeniach dostępnych na rynku.
- Zespół firmy Fortinet zajmujący się badaniem zagrożeń: ponadto badacze z zespołu firmy Fortinet prowadzą drobiazgowe badania nad nowymi zagrożeniami i lukami w zabezpieczeniach, aby zapewnić organizacjom rzetelne informacje na temat zabezpieczeń, umożliwiające podejmowanie skutecznych działań. Zespół firmy Fortinet odkrył i ujawnił więcej ataków typu zero-day niż którakolwiek z pozostałych organizacji na całym świecie.
- Informacje przekazywane na bieżąco w ramach rozwiązań firmy Fortinet: firma Fortinet dysponuje ponadto na całym świecie milionami urządzeń, które wykrywają i wskazują zagrożenia i złośliwe oprogramowanie w celu przekazywania w czasie rzeczywistym informacji o działaniach, tendencjach i pojawiających się problemach.

Przy użyciu tych zasobów informacje są gromadzone, korelowane i przekształcane w aktualizacje, które są stale przesyłane do wszystkich rozwiązań zabezpieczających dostępnych w ofercie firmy Fortinet. Zapewnia to w ramach platformy Security Fabric możliwość wykrywania najnowszych zagrożeń i reagowania na nie, niezależnie od tego, w którym miejscu w danej sieci rozproszonej występują.

Informacje o zagrożeniach muszą mieć również charakter lokalny

Oprócz informacji o charakterze globalnym w rozwiązaniach zabezpieczających należy brać pod uwagę to, co dzieje się w sieci lokalnej. Należy szybko identyfikować nietypowe zachowania, złośliwe oprogramowanie, nieznane urządzenia i nieupoważnionych użytkowników, aby umożliwić natychmiastowe zastosowanie w ramach platformy Security Fabric środków zaradczych, mających na celu zapewnienie ochrony sieci, ograniczenie rozprzestrzeniania się zagrożenia oraz zapewnienie dostępu do przydatnych informacji uzyskanych na podstawie badań.

Skuteczna strategia obsługi informacji lokalnych musi obejmować następujące elementy:

- Informacje o zagrożeniach należy gromadzić i korelować z siecią w czasie rzeczywistym. Wiele zagrożeń, takich jak zagrożenia typu APT, można wykryć jedynie po skorelowaniu i przeanalizowaniu wystąpienia szeregu pozornie ze sobą niezwiązanych zdarzeń.
- Informacje o zagrożeniach należy gromadzić na podstawie przychodzącego i wychodzącego ruchu sieciowego (północ-południe), danych przechodzących przez sieć lateralnie (wschód-zachód) oraz danych poruszających się w sieci poziomo (pomiędzy jej krańcami).
- Informacje o zagrożeniach muszą być udostępniane pomiędzy poszczególnymi urządzeniami, by umożliwiać skoordynowane reagowanie. W przypadku nakładających się na siebie rozwiązań zabezpieczających, w których wyszukiwane są różne rzeczy, alerty są sygnalizowane na różne sposoby, przy użyciu różnych protokołów i nie ma możliwości udostępnienia ani korelowania informacji o zagrożeniach z innymi urządzeniami, możliwości wykrywania ataków i reagowania na nie są mocno ograniczone.
- Jedno narzędzie do zarządzania umożliwia scentralizowane tworzenie polityk, ujednolicone zarządzanie nimi oraz ich rozproszone wdrażanie w wielu różnych rozwiązaniach zabezpieczających.

Tego rodzaju współpraca przy wykrywaniu i reagowaniu jest trudna, a może nawet niemożliwa do zrealizowania w przypadku pojedynczych produktów, nawet tego samego dostawcy, jeśli pomiędzy nimi nie są udostępniane ujednolicone informacje, ujednolicone zarządzanie i ujednolicone egzekwowanie polityk. Aby skutecznie reagować na pojawiające się obecnie wyrafinowane zagrożenia, niezbędna jest zintegrowana platforma Security Fabric oparta na współpracy.

Certyfikacja zabezpieczeń

Certyfikaty branżowe są dobrym wskaźnikiem zaangażowania dostawcy w tworzenie i obsługiwanie skutecznych rozwiązań zabezpieczających. Firma Fortinet prowadzi zdecydowaną kampanię, polegającą na uzyskiwaniu dla własnych produktów certyfikacji w najważniejszych niezależnych organizacjach certyfikacyjnych w celu zapewnienia klientów, że nasze technologie spełniają rygorystyczne wymogi bezpieczeństwa, są zgodne z wymogami prawnymi oraz reagują na najnowsze zagrożenia oraz ścieżki ataku.

Przy zapoznawaniu się z certyfikatami dostawcy przedstawiciele organizacji powinni być poinformowani o tym, które certyfikaty są naprawdę wartościowe. Dla przykładu na rynku dostępnych jest wiele testów, w których wystarczy zapłacić za otrzymanie certyfikatu, a także organizacji, które za odpowiednią opłatą przygotują raport potwierdzający, że produkt danego dostawcy jest najlepszym rozwiązaniem w swojej klasie. Takie raporty nie są miarodajne i firma Fortinet nie bierze udziału w ich pozyskiwaniu.

Oprócz certyfikatów wystawianych przez strony trzecie, informacje na temat tego, czy dane rozwiązanie nadaje się do monitorowania danego typu ruchu w konkretnym środowisku danej organizacji, można uzyskać z testów porównawczych. Firma Fortinet zdecydowanie poleca tego rodzaju porównania, ponieważ umożliwiają one oddzielenie funkcjonalności rozwiązania od działań marketingowych i sprzedażowych.

Wszechstronna oferta rozwiązań zabezpieczających firmy Fortinet stale uzyskuje najwyższe oceny w rygorystycznych, niezależnych testach, przeprowadzanych przez takie organizacje jak NSS Labs, a firma uzyskała więcej certyfikatów od organizacji nadzorujących niż którykolwiek z pozostałych dostawców rozwiązań na rynku zabezpieczeń.

Zabezpieczenia — zalety współpracy

Platforma Fortinet Security Fabric umożliwia współdziałanie różnych technologii zabezpieczających w celu skuteczniejszego zabezpieczania ewoluujących środowisk oraz rozwiązywania nowych problemów z bezpieczeństwem.

- Zapory — firma Fortinet udostępnia bogatą ofertę wiodących rozwiązań tego rodzaju na rynku, w tym urządzeń fizycznych o wysokiej wydajności, rozwiązań wirtualnych oraz rozwiązań chmurowych
- Advanced Threat Protection Framework — w ramach infrastruktury ATP firmy Fortinet dostępne są zaawansowane rozwiązania zabezpieczające, takie jak środowiska testowe czy zabezpieczenia poczty elektronicznej, stron internetowych i klientów
- Zabezpieczenia centrów danych — szybko działające urządzenia zabezpieczające do obsługi ruchu północ-południe, dynamiczne, skalowalne urządzenia zwirtualizowane do kontrolowania i zabezpieczania ruchu wschód-zachód oraz zabezpieczenia aplikacji z dogłębnym badaniem bezpieczeństwa procesów biznesowych i transakcji. Te rozwiązania są również w pełni zintegrowane z wiodącymi architekturami centrów danych SDN oraz ACI nowej generacji
- Zabezpieczenia chmury — firma Fortinet dostarcza rozwiązania do ochrony środowisk chmur prywatnych, chmur publicznych, takich jak AWS oraz Azure, w których świadczone są usługi chmurowe, takie jak XaaS i rozwiązania typu cloud-bursting oraz hybrydowe rozwiązania chmurowe działające w siedzibie/poza siedzibą organizacji
- PLS TRANSLATE (I could not put comment here; remark window is not working)): Secure Access Architecture — różnego rodzaju narzędzia do kontroli dostępu, bezpieczne przełączniki oraz narzędzia do egzekwowania polityk, zapewniające ujednolicone i wysoko wydajne zarządzanie dostępem w sieciach przewodowych i bezprzewodowych
- Architektura Connected UTM — wydajne rozwiązania UTM firmy Fortinet dla małych i średnich przedsiębiorstw oraz oddziałów firm obejmujące kompleksowe narzędzia zabezpieczające połączone z zarządzaniem w chmurze na potrzeby zdalnych wdrożeń w lokalizacjach, które nie dysponują obsługą techniczną

4. Skuteczność

Platforma Fortinet Security Fabric została opracowana pod kątem reagowania w czasie rzeczywistym poprzez skuteczne wykorzystanie informacji dotyczących zagrożeń. Udostępnia funkcje współpracy pomiędzy oferowanymi przez firmę Fortinet technologiami zabezpieczeń, co zapewnia większą widoczność i szybsze reagowanie, jeden system operacyjny, by umożliwić uproszczenie kontroli, oraz oparte na chmurze narzędzie do zarządzania i organizowania, które umożliwia scentralizowanie kontroli w ramach dynamicznego i mocno rozproszonego środowiska sieciowego.

Komponenty platformy Fortinet Security Fabric o decydującym znaczeniu to:

- FortiManager — zarządzanie i organizowanie za pomocą jednej konsoli;
- FortiCare — usługi reagowania na zdarzenia o znaczeniu krytycznym;
- FortiCloud, FortiGuard+, Cloud FortiSandbox — rozszerzenie platformy Security Fabric na rozwiązania chmurowe;
- Zwirtualizowane wersje rozwiązań zabezpieczających Fortinet, które współpracują ze wszystkimi wiodącymi środowiskami wirtualnymi;
- Pełna integracja ze wszystkimi wiodącymi architekturami SDN oraz chmurowymi;
- Ujednolicone, najpowszechniej stosowane zabezpieczenia dostawców usług umożliwiające egzekwowanie polityk pomiędzy infrastrukturami w obrębie organizacji i poza nią.

5. Otwartość — ekosystem obejmujący rozwiązania partnerów firmy Fortinet

Oczywiście w ramach organizacji poczyniono już inwestycje w infrastrukturę sieciową i platformy oraz produkty zabezpieczające, będące niezbędnym elementem mechanizmów zabezpieczających. Rozszerzenie funkcjonalności i inteligencji platformy Fortinet Security Fabric na wiodące rozwiązania podmiotów trzecich ma decydujące znaczenie dla wielu przedsiębiorstw.

Firma Fortinet jest zaangażowana w tworzenie interaktywnej społeczności rozwiązań zabezpieczających. Jest to jeden z powodów, dla których jesteśmy aktywnym członkiem organizacji Cyber Threat Alliance i dla których opracowaliśmy również solidny program partnerski, zrzeszający wiodących dostawców technologii zabezpieczających w celu rozwiązywania złożonych problemów związanych z zagrożeniami.

Firma Fortinet opracowała szereg interfejsów API, które umożliwiają naszym partnerom łączenie się z platformą Fortinet Security Fabric w celu dodatkowego zwiększenia widoczności organizacji klienta oraz usprawnienia kontroli i reagowania. Tego rodzaju punkty integracji interfejsów API obejmują następujące elementy:

- Hypervisor (środowisko wirtualne)
- Sieć SDN
- Chmura
- Sandbox
- Logowanie
- Zarządzanie politykami

Omawiana integracja to nie tylko umożliwienie rozwiązaniom stron trzecich gromadzenia lub przekierowywania danych i ruchu. Rozwiązania partnerskie, które można zintegrować z platformą Fortinet Security Fabric są w stanie aktywnie gromadzić i udostępniać informacje o zagrożeniach oraz instrukcje dotyczące łagodzenia skutków ataków, dzięki czemu możliwe jest sprawniejsze pozyskiwanie informacji o zagrożeniach, zwiększenie ogólnej świadomości zagrożeń oraz rozszerzenie reagowania na zagrożenia na całość rozwiązań.

Podsumowanie

Ewolucja sieci w przedsiębiorstwach oraz przejście do cyfrowego modelu biznesowego to obecnie jeden z najbardziej problematycznych aspektów zabezpieczeń sieciowych. W związku z istotnymi zmianami w tendencjach informatycznych i rozwiązaniach sieciowych, które pociągają za sobą zmiany w wielu infrastrukturach biznesowych, architekturach i praktykach, organizacje szukają innowacyjnych rozwiązań do ochrony sieci, które umożliwią im uwzględnienie tych zmian.

Platforma Fortinet Security Fabric jest w stanie zapewnić strategię skalowalności, bezpieczeństwa, przepływu informacji, skutecznego wykorzystania informacji dotyczących zagrożeń oraz otwartości, która jest potrzebna w organizacji, by zapewnić bezpieczeństwo, elastyczność, skalowalność, współpracę, łatwość dostosowania oraz zarządzanie niezbędne w środowiskach fizycznych, wirtualnych i chmurowych.

Więcej informacji o platformie Fortinet Security Fabric można znaleźć na stronie http://www.fortinet.com/aboutus/why-fortinet.html

SIEDZIBA GŁÓWNA
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
Stany Zjednoczone
Tel.: +1 408 235 7700
www.fortinet.com/sales

BIURO SPRZEDAŻY — REGION EMEA
905 rue Albert Einstein
Valbonee
06560, Alpes-Maritimes,
Francja
Tel.: +33 4 8987 0500

BIURO SPRZEDAŻY — REGION APAC
300 Beach Road 20-01
The Concourse
Singapur 199555
Tel.: +65 6513 3730

BIURO SPRZEDAŻY — AMERYKA ŁACIŃSKA
Paseo de la Reforma 412 piso 16
Col. Juarez
C.P. 06600
México D.F.
Tel.: 011-52-(55) 5524-8428

Polska
ul. Złota 59/6F
Budynek Lumen II (6 piętro)
00-120 Warszawa
Polska

22 kwietnia 2016 r.