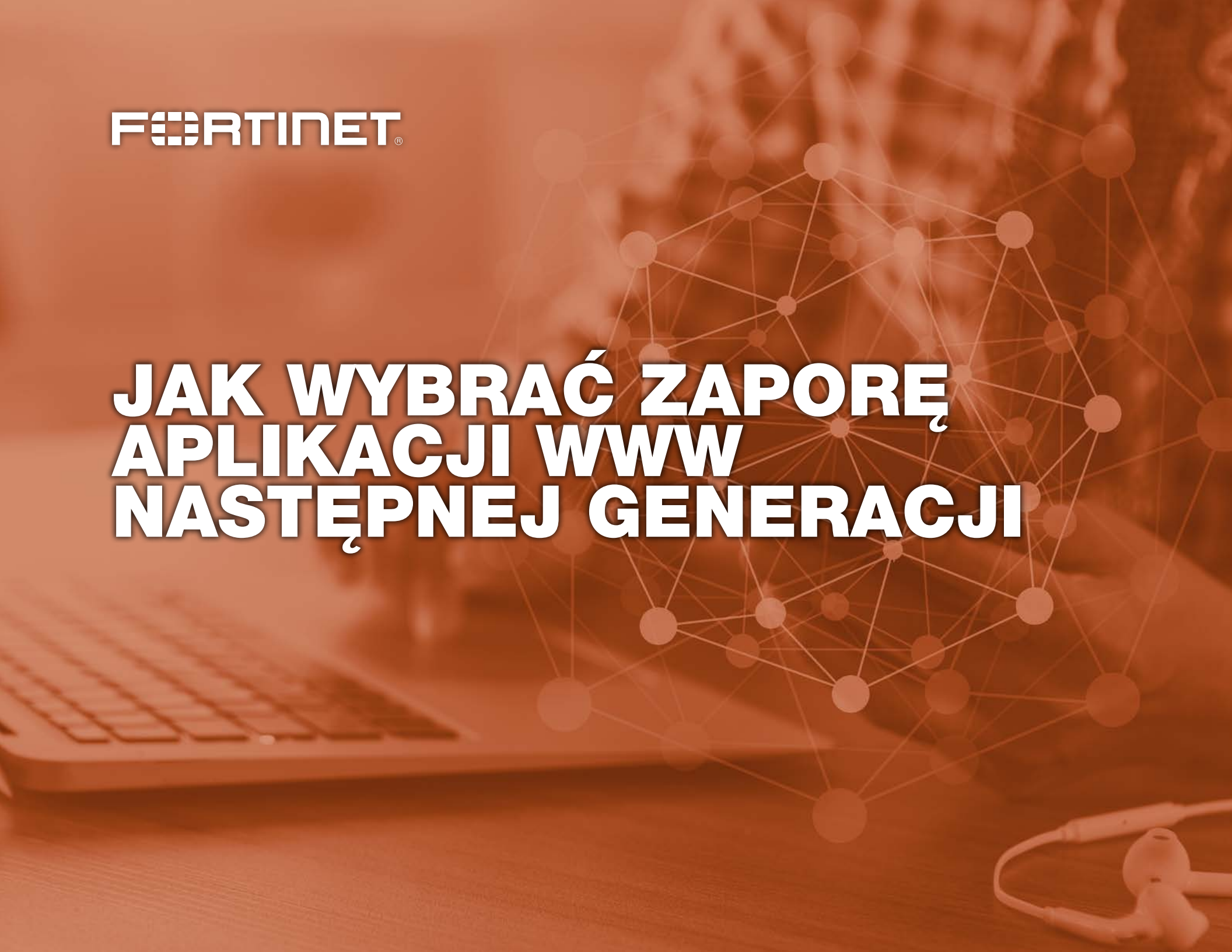


JAK WYBRAĆ ZAPORĘ APLIKACJI WWW NASTĘPNEJ GENERACJI

SPIS TREŚCI

STRESZCZENIE

Im bardziej przedsiębiorstwa korzystają z aplikacji WWW w ramach swoich podstawowych procesów biznesowych, tym ważniejszą rolę w zabezpieczaniu danych przedsiębiorstwa odgrywają zapory aplikacji WWW, czyli zapory służące do ochrony aplikacji WWW. Przed nabyciem takiej zapory przedsiębiorstwo powinno jednak rozważyć kilka różnych zapewnianych przez nią funkcjonalności.

Jedną z nich jest zestaw podstawowych funkcji zapory aplikacji WWW, który obejmuje funkcje ochrony przed wirusami i złośliwym oprogramowaniem, mechanizmy inspekcji, sygnatury oraz funkcje weryfikacji protokołów i reputacji infrastruktury IT. Ogromny wzrost liczby znanych i nieznanych zagrożeń przyczynił się jednak do powstawania luk w zabezpieczeniach oraz do stosowania mechanizmów uczenia się aplikacji (application learning) na potrzeby wykrywania zagrożeń opartego na analizie zachowania. Binarny charakter tych mechanizmów skutkuje zwracaniem dużej liczby fałszywych alarmów, które dokładają pracy i tak już przeciążonemu obowiązkami personelowi działu IT. Wiele osób zwraca się zatem ku funkcjom sztucznej inteligencji (artificial intelligence, AI) i uczenia maszynowego (machine learning) jako narzędzi zdolnych do poradzenia sobie ze wspomnianymi fałszywymi alarmami oraz do dokładniejszego wykrywania zagrożeń.

Zapory aplikacji WWW muszą być również zdolne do integracji z szerzej rozumianą architekturą zabezpieczeń przedsiębiorstwa oraz zapewniać funkcje przede wszystkim brane po uwagę podczas wybierania systemów zabezpieczających: skalowalność, wpływ na przepustowość i łatwość używania.

WYZWANIA DOTYCZĄCE BEZPIECZEŃSTWA APLIKACJI WWW

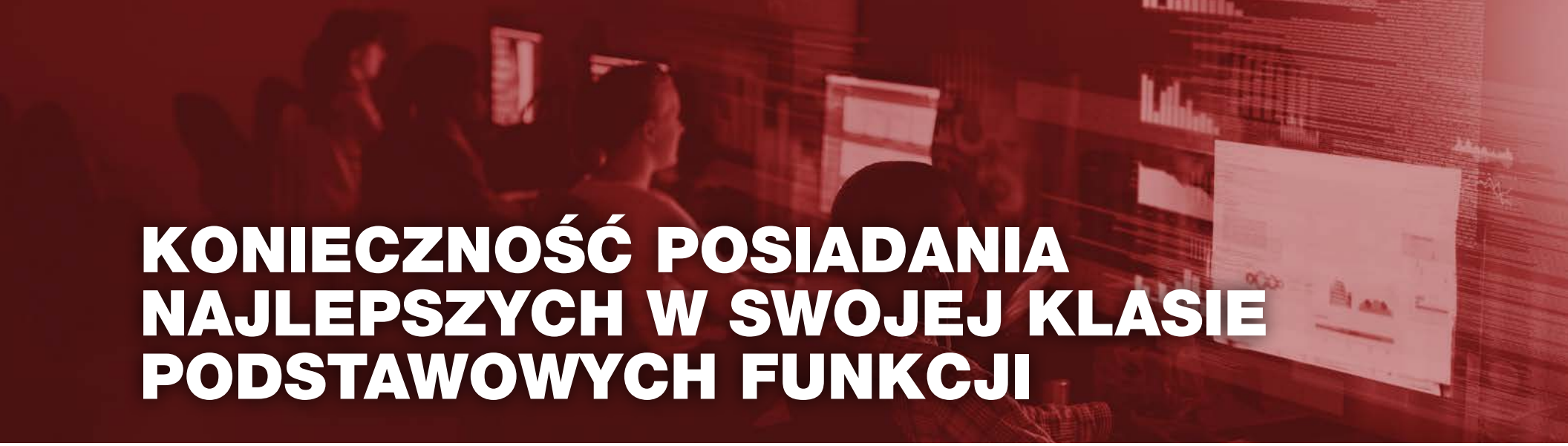
Przedsiębiorstwa korzystają z aplikacji WWW zainstalowanych lokalnie lub w chmurze w ramach wszystkich swoich obszarów. Gdy aplikacje te zawodzą, powstałe w ten sposób zakłócenia nie tylko negatywnie wpływają na działalność operacyjną przedsiębiorstwa, ale również dotykają całego łańcucha dostaw. Ponadto aplikacje WWW służą do przetwarzania i mają dostęp do danych krytycznych takich jak dane klientów i dane finansowe. Bez skutecznych zabezpieczeń dane takie mogą być narażone na niebezpieczeństwo.

Im bardziej przedsiębiorstwa korzystają z aplikacji WWW, tym bardziej potrzebują zapory do ochrony tych aplikacji przed zagrożeniami zewnętrznymi i wewnętrznymi. Wynika to z faktu, że w tym samym czasie zwiększa się zarówno powierzchnia ataku przedsiębiorstwa, jak i liczba i różnorodność cyberataków. Przyczyną niemal połowy (48%) wszystkich naruszeń ochrony danych są skuteczne ataki hakerskie na aplikacje WWW[1]. Przedsiębiorstwo, które korzysta wyłącznie z zapory i systemu ochrony przed włamaniami (IPS), jest niewłaściwie przygotowane do blokowania ataków, które mają coraz więcej postaci i korzystają jednocześnie z wielu wektorów ataku.

Przedsiębiorstwa potrzebują zapory aplikacji WWW, która skutecznie zidentyfikuje znane i nieznane zagrożenia oraz je powstrzyma, a jednocześnie zminimalizuje liczbę fałszywych alarmów, które mogą nadmiernie obciążać dostępne zasoby służące do odpowiedniego reagowania na zagrożenia. Niektóre technologie zapór aplikacji WWW nie są jednak zdolne do realizacji wspomnianych wymogów. Decydenci w kwestiach zabezpieczeń infrastruktury informatycznej (Chief Information Security Officers, CISO), którzy chcą poprawić zabezpieczenia używanych w przedsiębiorstwie aplikacji WWW, powinni zatem szukać rozwiązania oferującego:

- Doskonałe podstawowe funkcje zapory aplikacji WWW
- Zaawansowany mechanizm wykrywania zagrożeń opartego na analizie zachowania, który nie wymaga angażowania dużej liczby pracowników
- Odpowiednią skalowalność, która nie ogranicza przepustowości

[1] „2018 Data Breach Investigations Report", Verizon, marzec 2018 r.



KONIECZNOŚĆ POSIADANIA NAJLEPSZYCH W SWOJEJ KLASIE PODSTAWOWYCH FUNKCJI

Ataki na aplikacje WWW są tak zróżnicowane, że zabezpieczenia tych aplikacji zabeczenie ich muszą opierać się na kombinacji metod ochrony. Metody te muszą być zarówno zróżnicowane, aby chronić różne wektory ataku, jak i odpowiednio skorelowane. Zapora aplikacji WWW powinna zatem być zdolna do podjęcia odpowiednich działań w celu ochrony tych aplikacji, ilekroć wykryje zagrożenie.

1. Ochrona przed wirusami i złośliwym oprogramowaniem
Podstawowe mechanizmy zabezpieczeń, czyli mechanizmy wykrywające wirusy i złośliwe oprogramowanie, to kluczowe elementy każdej skutecznej zapory aplikacji WWW. Mechanizmy te muszą skanować cały ruch dotyczący aplikacji WWW pod kątem zagrożeń potencjalnie zdolnych do zainfekowania serwerów i innych urządzeń wchodzących w skład sieci przedsiębiorstwa.

2. Częste aktualizacje sygnatur
Każda zapora aplikacji WWW powinna oferować funkcje wykrywania sygnatur, które porównują zawartość przychodzących pakietów z sygnaturami znanych zagrożeń sieciowych. Zagrożenia te mogą obejmować botnety, zaawansowane zagrożenia i ataki typu DDoS (rozproszona odmowa usługi).

Aby zapewnić skuteczne wykrywanie zagrożeń za pomocą sygnatur sygnatur, zapora aplikacji WWW musi mieć:

1. Dostęp do zasobów dużej i uznanej organizacji zajmującej się badaniami zagrożeń.
2. Możność Możliwość importowania danych z badań nad zagrożeniami do swojej bazy danych służącej do wykrywania sygnatur (w sytuacji idealnej aktualizacja takiej bazy danych powinna odbywać się w czasie rzeczywistym).
3. Zdolność do przekierowywania potencjalnie złośliwych pakietów do bezpiecznego środowiska testowego (sandbox) lub innego rodzaju blokowania tych pakietów w celu uniemożliwienia im dostępu do sieci przedsiębiorstwa.

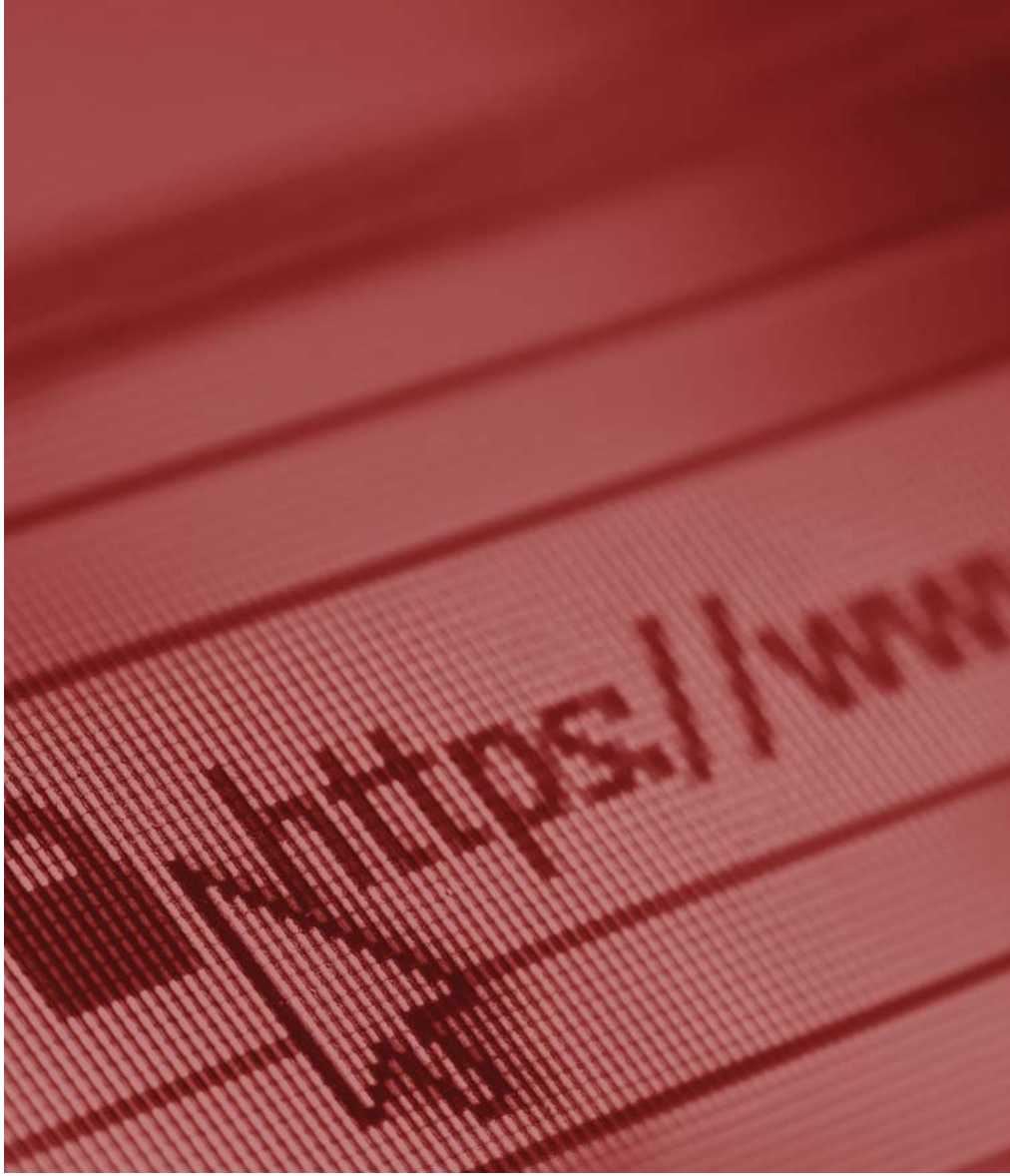
3. Weryfikacja reputacji adresów IP

Podobnie jak w przypadku wykrywania sygnatur, weryfikacja reputacji adresów IP polega na porównaniu ruchu przychodzącego ze znanymi zagrożeniami. Różnica sprowadza się do tego, że w przypadku weryfikacji reputacji nie sprawdza się zawartości pakietów przychodzących, ale ich źródło. Zapora aplikacji WWW ma czarną listę adresów IP znanych jako źródło botnetów i innych typów zagrożeń, aby porównywać ruch przychodzący do chronionych przez nią aplikacji pod kątem danych ze wspomnianej czarnej listy. Ilekroć w ruchu tym zostaną wykryte dane z czarnej listy, zostanie on zablokowany i nie będzie mieć dostępu do sieci przedsiębiorstwa.

Podobnie jak w przypadku wykrywania sygnatur, weryfikacja reputacji adresów IP wymaga, aby zapora aplikacji WWW miała dostęp do usługi oferującej informacje o zagrożeniach, która będzie zapewniać częste aktualizacje czarnej listy. Bardziej zaawansowane zapory aplikacji WWW są również zdolne do identyfikowania i dodawania do czarnej listy źródeł złośliwych pakietów oznaczonych za pomocą oferowanych przez te zapory mechanizmów wykrywania sygnatur.

4. Weryfikacja protokołów

Zapora aplikacji WWW musi być również zdolna do eliminacji niewłaściwego kodu HTTP. Ilekroć aplikacje korzystające z różnych protokołów komunikacyjnych wchodzą ze sobą w interakcje, pojawia się luka w zabezpieczeniach. Sprawnie przeprowadzony atak mógłby skutecznie ominąć nawet silne zabezpieczenia tych aplikacji, gdyby imitował protokół stosowany przez jedną z takich komunikujących się ze sobą aplikacji (na przykład udawał błąd w tłumaczeniu). Wszystkie

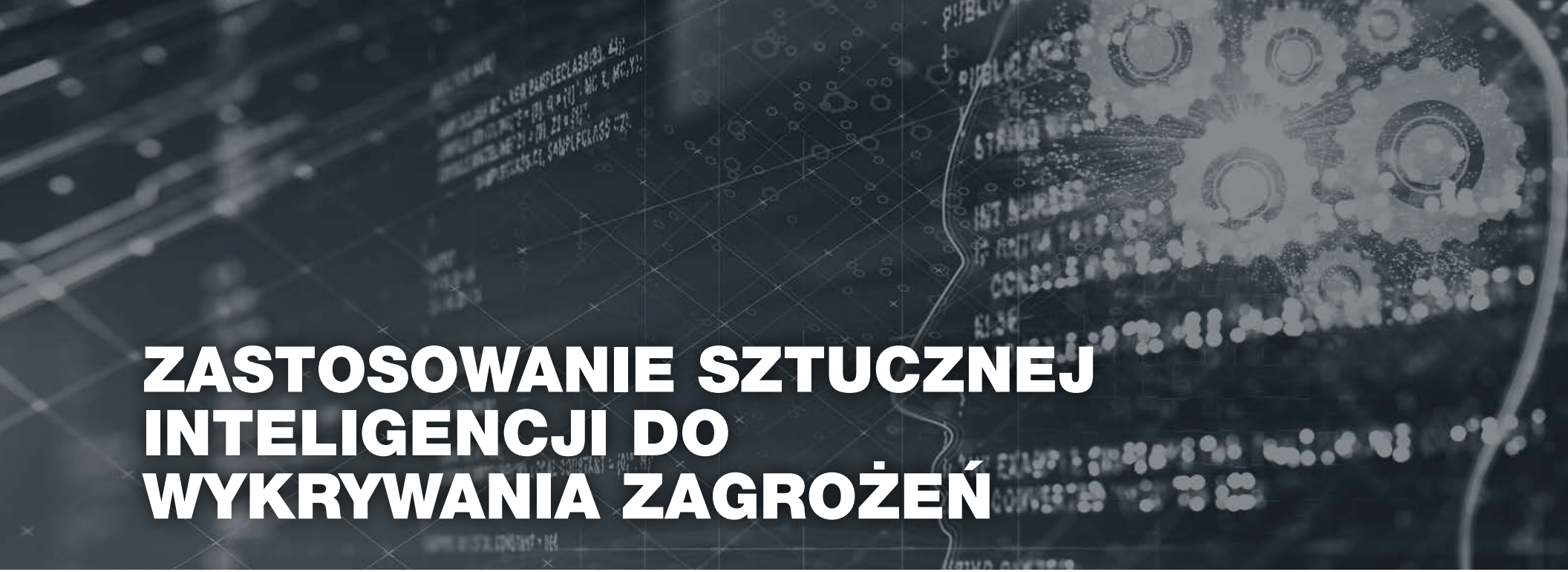


aplikacje WWW powinny być zgodne ze specyfikacją HTTP RFC. Aby powstrzymać tego typu ataki, zapora aplikacji WWW musi weryfikować dany protokół pod kątek kątem każdego kodu, który chroniona aplikacja WWW chce wykonać.

5. Integracja funkcji
Każda ze wspomnianych funkcji zapory aplikacji WWW jest niezbędna do ochrony tych aplikacji przed co najmniej jednym typem zagrożenia. Aby zoptymalizować tę ochronę, wspomniana zapora powinna być zdolna do dwojakiego zintegrowania tych funkcji:

Korelacja danych. Dane dotyczące sygnatur warstwy aplikacji, złośliwych botów, podejrzanych adresów IP i nowych wirusów powinny być skorelowane w taki sposób, aby informacje o zagrożeniach były współdzielone przez wszystkie funkcje. Jeśli na przykład zapora aplikacji WWW zidentyfikuje botnet, może dodać adres IP źródła tego botneta do czarnej listy adresów IP, automatycznie oznaczając odpowiednio przyszły ruch przychodzący z tego adresu.

Współdzielenie informacji o zagrożeniach. Zapora aplikacji WWW powinna również bezproblemowo wpisywać się w szerszą architekturę zabezpieczeń przedsiębiorstwa. Wielu cyberprzestępców stosuje polimorficzne złośliwe oprogramowanie i jednocześnie używa wielu wektorów ataku. Walka z takimi zagrożeniami wymaga realizowanego w czasie rzeczywistym współdzielenia informacji o zagrożeniach przez wszystkie elementy sieci przedsiębiorstwa. Na przykład atak może mieć na celu przejście przez luki w zabezpieczeniach w ramach różnych wektorów (m.in. punktów końcowych, poczty elektronicznej i usług chmurowych) oraz zastosowanie funkcji uczenia maszynowego w celu doskonalenia programów wykorzystujących te luki na podstawie pozyskanych informacji. W takich przypadkach zapora aplikacji WWW musi współdzielić informacje o zagrożeniach w czasie rzeczywistym z każdym elementem sieci przedsiębiorstwa (i odwrotnie), aby skutecznie obronić sieć przed wspomnianymi zagrożeniami.



ZASTOSOWANIE SZTUCZNEJ INTELIGENCJI DO WYKRYWANIA ZAGROŻEŃ

Zabezpieczenia korzystające z czarnych i białych list mogą wychwycić znaczną liczbę zagrożeń, ale wszystko i tak zależy od zawartości tych list. Innymi słowy, można tu wykryć tylko te zagrożenia, które zostały już wcześniej rozpoznane. Zważywszy, że dostawcy zabezpieczeń nie są zdolni do utworzenia sygnatur nieznanych zagrożeń, tradycyjne zabezpieczenia również nie są w stanie wykryć nowych ataków, w tym ataków typu „zero-day", ani im zapobiec.

Oprócz możliwości monitorowania zagrożeń w oparciu o wspomniane listy, większość zapór aplikacji WWW korzysta z funkcji wykrywania zagrożeń na podstawie zachowania. Funkcje te porównują zachowania użytkowników lub aplikacji z oczekiwanymi zachowaniami pod kątem ewentualnych anomalii (wykryte anomalie są odpowiednio oznaczane). Zapory, które zawierają technologie uczenia się aplikacji, monitorują reakcje na określone dane wejściowe w czasie i uczą się tego, jakich reakcji powinny oczekiwać w przyszłości.

Zapory te automatycznie tworzą profil struktury chronionej aplikacji oraz identyfikują sposób użycia tej aplikacji w przedsiębiorstwie. Następnie odpowiednio przypisują do charakterystyki tych profili zasady reagowania na zagrożenia. Zachowania inicjujące alert mogą całkowicie zablokować ruch przychodzący do aplikacji WWW lub przekierować go do bezpiecznego środowiska testowego (sandbox).

1. Problemy związane z uczeniem się aplikacji
Zapory aplikacji WWW korzystające z funkcji uczenia się struktury aplikacji niekoniecznie muszą być bardzo „inteligentne”. Tworzą one profil chronionej aplikacji na podstawie obserwacji wprowadzanych danych i innych aspektów zachowania użytkownika w kontekście poszczególnych parametrów tej aplikacji, w tym zakresów wartości wprowadzanych w polach formularzy, metod HTTP, plików cookie itp. Następnie w miarę zbierania kolejnych danych o zachowaniu użytkownika aplikacje te odpowiednio aktualizują wspomniane profile.

Problem polega na tym, że każde zachowanie, które nie mieści się w określonym profilu utworzonym przez zaporę aplikacji WWW (czyli każde zachowanie, którego zapora ta wcześniej nie zaobserwowała), inicjuje alarm, co skutkuje niezwykle dużą liczbą fałszywych alarmów w procesie wykrywania zagrożeń realizowanym przez tę zaporę. Ilekroć pojawia się nowy trend w zachowaniu użytkownika, ruch przychodzący do aplikacji może zostać zablokowany, dopóki człowiek nie zweryfikuje i nie zdecyduje, że nie jest to faktycznie zagrożenie. Z biegiem czasu takie nowe zachowanie stanie się oczekiwane, wiele działań nie stwarzających zagrożenia dla przedsiębiorstwa zostanie jednak oznaczonych jako niebezpieczne i będzie wymagać ręcznego procesu usuwania tych oznaczeń.

2. Korzyści płynące z zastosowania w zaporze aplikacji WWW funkcji uczenia maszynowego opartego na sztucznej inteligencji

Przedsiębiorstwa dysponujące ograniczonym personelem bezpieczeństwa powinny szukać sposobów na ograniczenie często wysokich wymagań wobec pracowników zajmujących się zarządzaniem funkcjami uczenia się aplikacji w zaporze aplikacji WWW. Jednym z obszarów, który takie ograniczenie umożliwia, jest uczenie maszynowe oparte na sztucznej inteligencji.

Funkcje uczenia maszynowego umożliwiają zaporze aplikacji WWW identyfikowanie odchyleń od zwykłego zachowania użytkownika lub aplikacji, ale nie jako przesłanki do natychmiastowego wszczęcia alertu, ale jako kontekstu do rozważenia kwestii bezpieczeństwa. Potencjalne alerty nie są oceniane z perspektywy prostego naruszenia albo nienaruszenia obowiązujących zasad, służą jedynie informowaniu obecnych w zaporze aplikacji WWW funkcji automatycznego obliczania prawdopodobieństwa o tym, że zachowanie użytkownika lub aplikacji stanowi zagrożenie wymagające odpowiedniej reakcji ze strony systemu bezpieczeństwa.

Niewiele zapór aplikacji WWW oferuje tego typu uczenie się maszynowe. Te, które to oferują, są zdolne do zainicjowania odpowiedniej reakcji na nietypowe zachowanie zgodnie z wcześniej zdefiniowanymi zasadami w zależności od prawdopodobieństwa pojawienia się zagrożenia ustalonego na podstawie wielu parametrów. Podejście takie może zasadniczo w pełni wyeliminować problem fałszywych alertów wywołany zastosowaniem funkcji uczenia się aplikacji. W ten sposób, w przeciwieństwie do przedsiębiorstw korzystających z funkcji uczenia się aplikacji, przedsiębiorstwa korzystające z funkcji uczenia maszynowego mogą uniknąć konieczności przenoszenia wartościowych pracowników do zadań polegających na weryfikacji fałszywych alertów.

Ponadto uczenie maszynowe umożliwia zaporze aplikacji WWW znacznie dokładniejsze klasyfikowanie plików i źródeł danych. W połączeniu z podstawowymi funkcjami zapory aplikacji WWW, funkcja uczenia maszynowego może wykryć prawie wszystkie uzasadnione zagrożenia. Pomaga to chronić sieć przed złośliwymi programami służącymi do skanowania, indeksowania, wydobywania i innego rodzaju kradzieży danych oraz innego typu nieznanymi atakami.

ZAGADNIENIA DOTYCZĄCE WYDAJNOŚCI I OPERACYJNOŚCI

Rzecz jasna zdolność zapory aplikacji WWW do ochrony aplikacji WWW w sieci przedsiębiorstwa jest kluczowa podczas podejmowania decyzji o wyborze właściwego rozwiązania. Nie jest to jednak jedyny element, który powinien zostać wzięty pod uwagę.

1. **Przepustowość.** Jakkolwiek istotne z biznesowego punktu widzenia może być bezpieczeństwo, tylko niewiele przedsiębiorstw może pozwolić na spowolnienie ruchu, aby w tym czasie zapora aplikacji WWW wykonała niezbędne porównania z czarnymi i białymi listami oraz profilami zachowań. Ponadto specjaliści ds. bezpieczeństwa oceniający takie zapory muszą znać nie tylko typową przepustowość dla swoich różnych opcji, ale również cechy swojej sieci i architektury zabezpieczeń, które mogą zmniejszyć przepustowość poszczególnych urządzeń w danym środowisku.
2. **Skalowalność.** W związku z obawami dotyczącymi przepustowości pozostają problemy niektórych zapór aplikacji WWW z obsługą bardzo dużego ruchu związanego z aplikacjami WWW. W dającej się przewidzieć przyszłości w większości przedsiębiorstw będzie nadal następować bardzo szybki wzrost ilości danych. Wspomniane zapory muszą być zatem wystarczająco skalowalne, aby móc obsługiwać na określonym poziomie przepustowości nie tylko bieżący, ale również przyszły ruch związany z aplikacjami WWW.
3. **Zasoby administracyjne.** Oprócz ogromnej ilości czasu pracy personelu, który może pochłonąć zajmowanie się fałszywymi alertami związanymi z procesem uczenia się aplikacji, przyszli nabywcy zapory aplikacji WWW powinni rozważyć łatwość użycia takiej zapory oraz nakłady pracy zespołu ds. bezpieczeństwa niezbędne w celu konfiguracji i dostrojenia zasad reagowania na zagrożenia.
4. **Raportowanie i zgodność.** Oferowane przez zaporę aplikacji WWW funkcje raportowania muszą być zgodne ze wszystkimi wymogami regulacyjnymi, w tym z mechanizmami zabezpieczeń określonymi w publikowanych przez Narodowy Instytut Standaryzacji i Technologii normach NIST 800, normami PCI DSS (Payment Card Industry Data Security Standard) itp.

Ocena zapór aplikacji WWW pod kątem wszystkich tych kryteriów wymaga czasu, ale wydaje się to być warte zachodu, zważywszy na ogromny potencjał w zakresie skutecznej i efektywnej ochrony danych i aplikacji WWW, który może zapewnić wybrane rozwiązanie.

www.fortinet.com