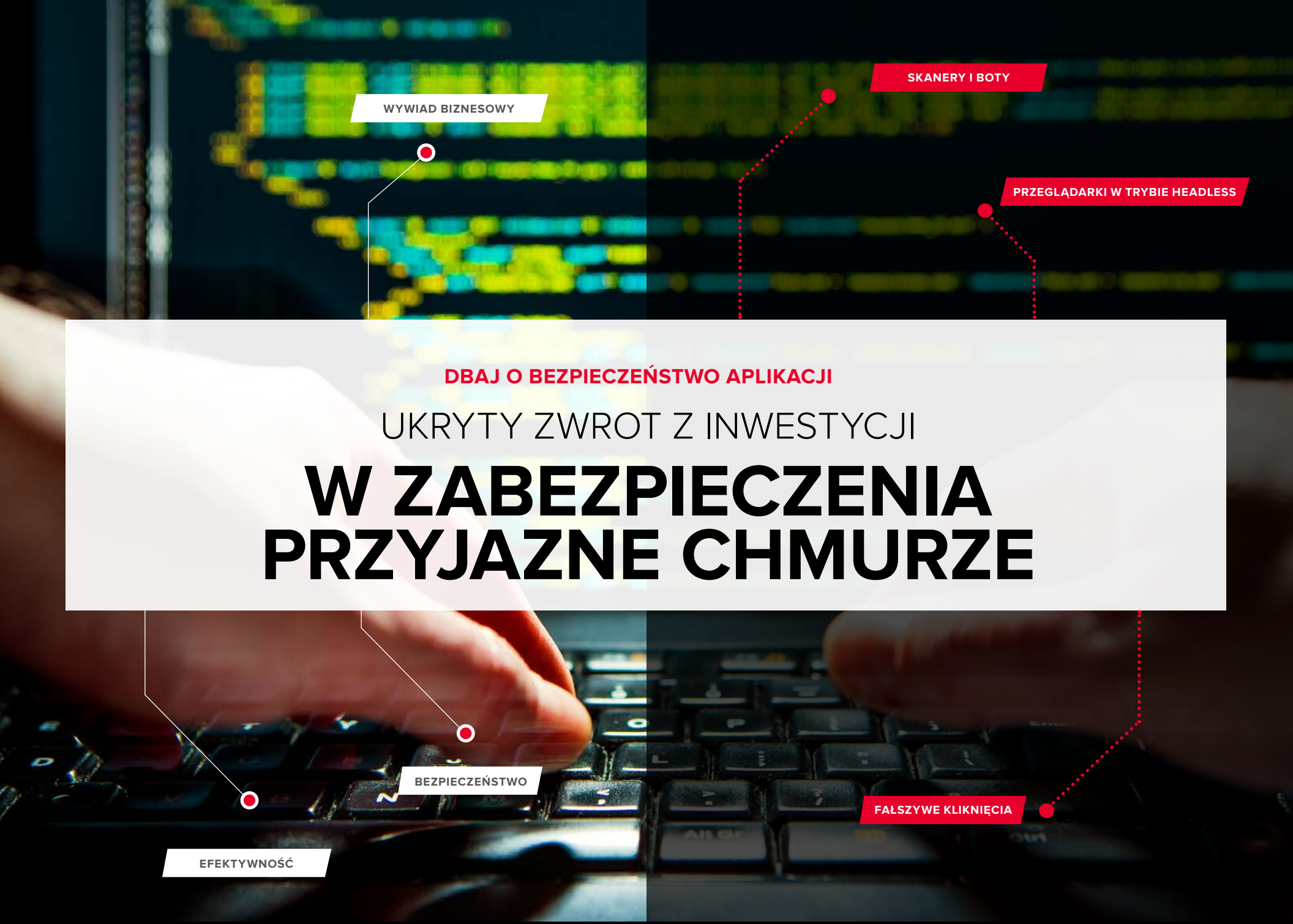


DBAJ O BEZPIECZEŃSTWO APLIKACJI

UKRYTY ZWROT Z INWESTYCJI

W ZABEZPIECZENIA PRZYJAZNE CHMURZE

WSTĘP

Czy wiesz, że firmy każdej wielkości przechodzą cyfrową transformację, przenosząc aplikacje i usługi do chmury, aby zwiększyć produktywność i przyspieszyć innowacje?

Wydawać się może, że każdego dnia pojawia się kolejny artykuł na temat Internetu rzeczy (IoT), analityki dużych zbiorów danych i architektur chmurowych oraz ich nieograniczonego potencjału dla firm chcących uzyskać przewagę nad konkurencją w cyfrowym świecie. Jeśli Twoja firma jest w trakcie transformacji cyfrowej (a prawdopodobnie tak jest), zapewne już korzystasz z zalet publicznej chmury, takich jak: ekonomia skali, prekonfigurowane rozwiązania, które można dopasować za pomocą kilku kliknięć, rozliczenia za usługi i nie tylko. Być może jednak nie słyszałeś, jak wspólny model bezpieczeństwa publicznej chmury wpływa na Twoje obowiązki związane z bezpieczeństwem i jak można go wykorzystać w środowiskach wielochmurowych.

Dostawcy usług w chmurze zazwyczaj świetnie radzą sobie w zakresie zarządzania fizycznymi centrami danych, infrastrukturą i systemami, które wydzierżawiasz. Nie mają jednak dużego wpływu na rzeczy, które tworzysz, wdrażasz lub umieszczasz w chmurze, czyli na Twoje aplikacje, usługi i dane. Według badań F5 Labs 53 procent przypadków naruszenia danych początkowo dotyczy warstwy aplikacji.[1] To ważna informacja, biorąc pod uwagę fakt, że każdy posiadacz karty kredytowej może zacząć korzystać z usług w chmurze do przechowywania danych lub zarządzania nimi — niezależnie od rozumienia konsekwencji związanych z bezpieczeństwem.[2]

Jak na to nie patrzeć, bezpieczeństwo w chmurze jest równie ważne jak bezpieczeństwo tradycyjnych centrów danych. Złożony charakter tych środowisk, a także unikalne architektury i różnorodne mechanizmy zabezpieczeń w chmurze wymagają racjonalnego podejścia do ochrony zasobów opartych na chmurze. Dobra wiadomość jest taka, że proaktywne zabezpieczenia w chmurze w rzeczywistości mogą pomóc Ci zoptymalizować procesy biznesowe i pozytywnie wpłynąć na Twoje wyniki finansowe. Wielu dostawców systemów zabezpieczeń oferuje rozwiązania chmurowe, które pozwalają przyspieszyć procesy rozwojowe przy jednoczesnym zapewnieniu bezpieczeństwa i usług oczekiwanych przez Twoich klientów.

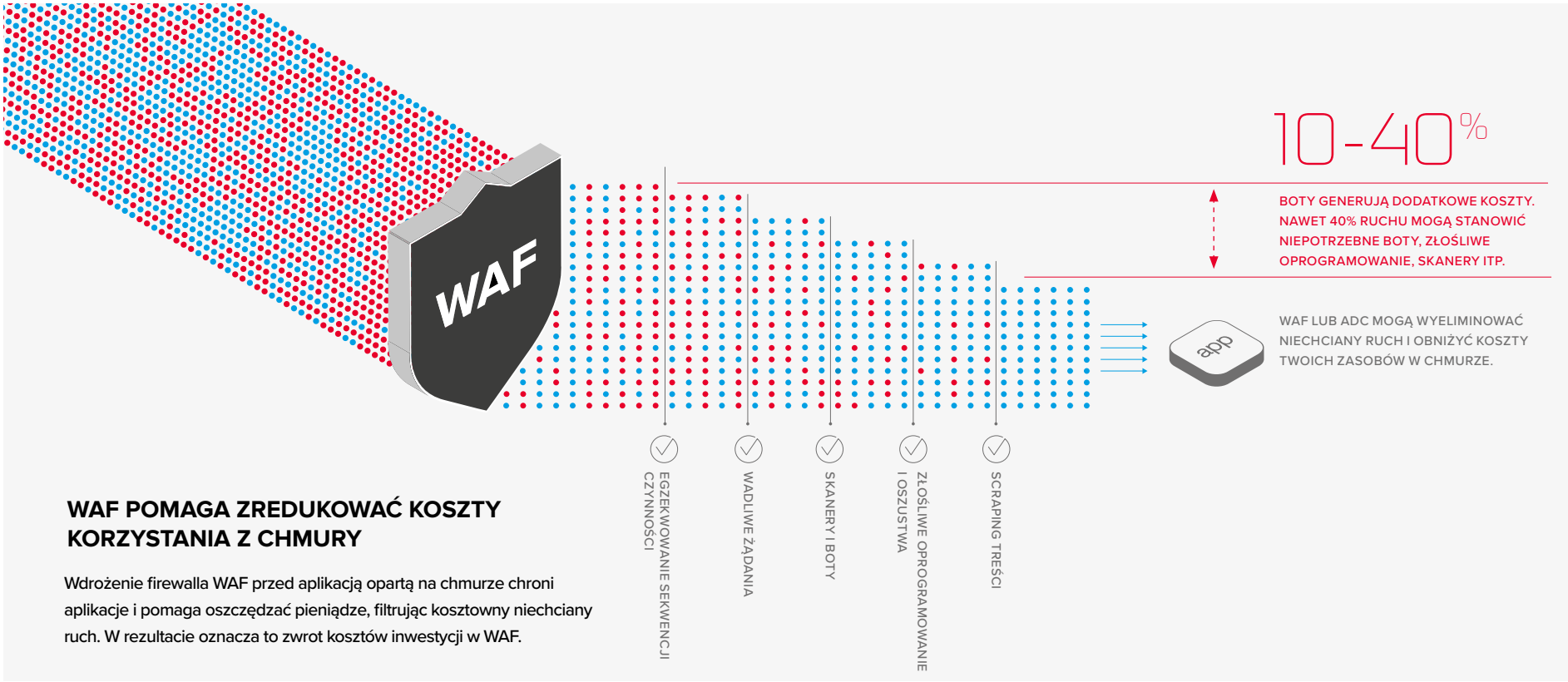
[1] https://f5.com/labs/articles/threat-intelligence/cyber-security/lessons-learned-from-a-decade-of-data-breaches
[2] https://www.theregister.co.uk/2017/10/10/accenture_amazon_aws_s3/

53%

WEDŁUG BADAŃ F5 LABS 53% PRZYPADKÓW NARUSZENIA DANYCH DOTYCZY WARSTWY APLIKACJI.[1]

ROZWIĄZANIA ZAPEWNIAJĄCE BEZPIECZEŃSTWO W CHMURZE MOGĄ **SAME NA SIEBIE ZAROBIĆ**

Sieci dostawców usług w chmurze są dobrze odwzorowane i udokumentowane, co oznacza, że boty i automatyczne skanery stanowią znaczną część ruchu dla aplikacji w chmurze. Jeśli rozliczasz się za faktyczne użytkowanie, ponosisz rzeczywiste, policzalne koszty za każdym razem, gdy bot zgłasza żądanie dowolnego zasobu związanego z Twoim kontem w chmurze. Prawdopodobnie już płacisz wysokie rachunki wynikające z ruchu pochodzącego z innych źródeł niż klienci. Jednak dzięki wdrożeniu odpowiednich narzędzi zabezpieczających Twoje aplikacje działające w chmurze, takich jak kontrolery dostarczania aplikacji (ADC) i firewalle aplikacji webowych (WAF), możesz nie tylko chronić te aplikacje, ale także filtrować niechciany ruch i ograniczać zasoby przydzielane do obsługi botów i skanerów. W przeciwieństwie do wielu tradycyjnych zabezpieczeń faktycznie znajdujących się w Twojej firmie, wykorzystywanie ADC lub WAF w chmurze może zapewnić wymierny zwrot z inwestycji, dbając jednocześnie o dostępność Twoich usług i ich bezpieczeństwo.



WAF POMAGA ZREDUKOWAĆ KOSZTY KORZYSTANIA Z CHMURY

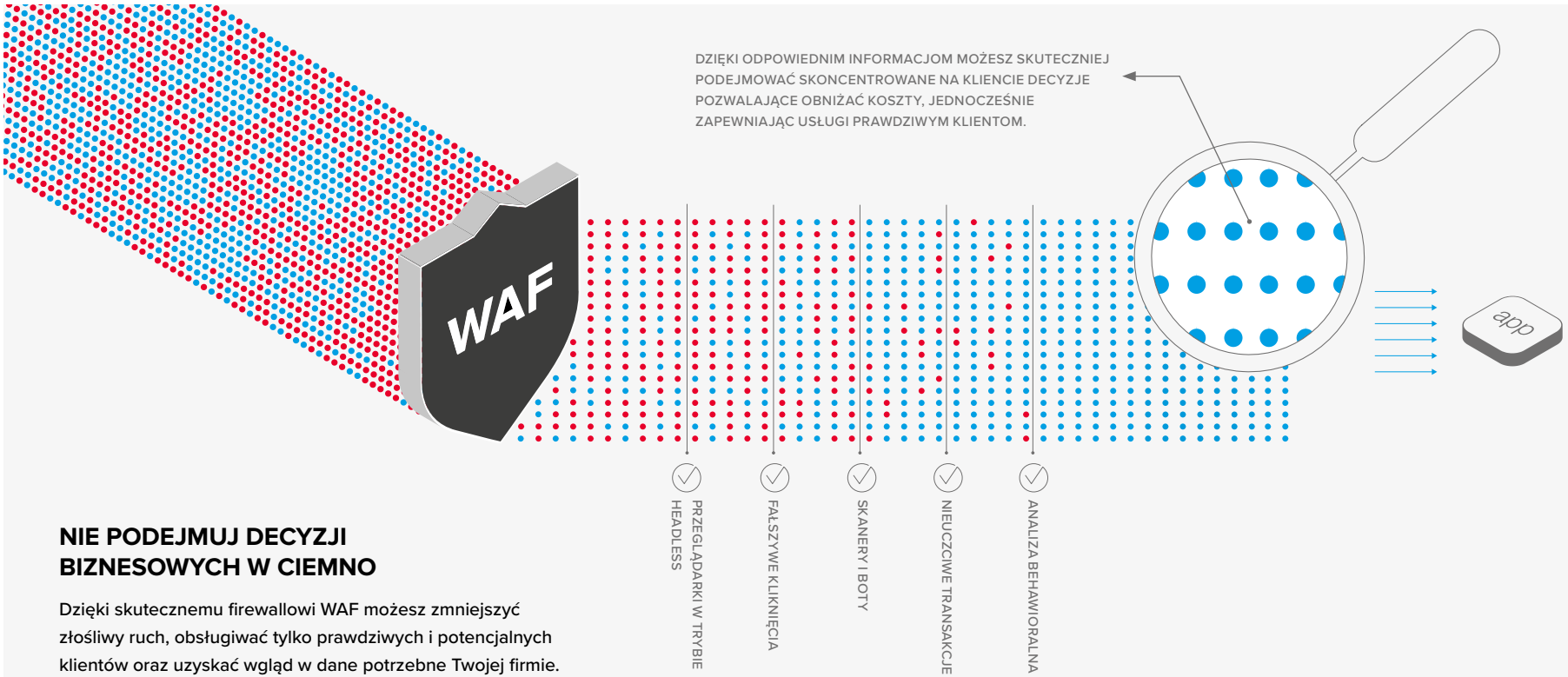
Wdrożenie firewalla WAF przed aplikacją opartą na chmurze chroni aplikacje i pomaga oszczędzać pieniądze, filtrując kosztowny niechciany ruch. W rezultacie oznacza to zwrot kosztów inwestycji w WAF.

ROZWIĄZANIA ZAPEWNIAJĄCE BEZPIECZEŃSTWO W CHMURZE MOGĄ **USPRAWNIAĆ WYWIAD BIZNESOWY**

Narzędzia bezpieczeństwa mogą być również źródłem informacji i umożliwiać wywiad biznesowy. Odpowiedni WAF lub ADC ułatwia analizę wzorców ruchu i danych do i z aplikacji internetowych w chmurze. Dostęp do takich informacji ułatwia podejmowanie decyzji związanych z zarządzaniem zasobami w sposób pozwalający obniżać koszty, jednocześnie zapewniając usługi prawdziwym klientom.

Dostępność jest podstawowym założeniem bezpieczeństwa aplikacji, ponieważ jeśli Twoja aplikacja nie jest dostępna dla Twoich klientów, nie ma czego zabezpieczać. Zastosowanie technologii ADC w chmurze nie tylko zapewnia wysoką dostępność, ale także pomaga uprościć coraz bardziej złożone architektury i maksymalnie wykorzystać silną strategię wielochmurową.

Odpowiedni partner dostarczy zarówno usługi ADC, jak i usługi bezpieczeństwa, w spójny i bezproblemowy sposób, w publicznych i prywatnych chmurach. Co więcej, zadba o odpowiednie zarządzanie ruchem i jego optymalizację w najbardziej opłacalny sposób.



NIE PODEJMUJ DECYZJI BIZNESOWYCH W CIEMNO

Dzięki skutecznemu firewallowi WAF możesz zmniejszyć złośliwy ruch, obsługiwać tylko prawdziwych i potencjalnych klientów oraz uzyskać wgląd w dane potrzebne Twojej firmie.

WYKORZYSTAJ ZALETY **SYSTEMU BEZPIECZEŃSTWA, KTÓRY JEST PRZYJAZNY DLA PROGRAMISTÓW**

Wszyscy powinniśmy dbać o bezpieczeństwo, ale właściciele i deweloperzy aplikacji nie zawsze muszą znać szczegóły zasad WAF, strategii obrony przed atakiem DDoS w warstwie 7 czy ochrony przed oszustwami internetowymi. Najczęściej potrzebują jedynie zapewnienia o poufności, integralności i dostępności danych w aplikacjach. Podobnie jak często łatwiejsze i efektywniejsze jest korzystanie z gotowych bibliotek kodu i narzędzi innych producentów, logiczne może być również wykorzystanie zaawansowanych usług i rozwiązań związanych z bezpieczeństwem, aby ograniczyć czas i wysiłek poświęcone na tworzenie oprogramowania. Mając to na uwadze, skuteczną i rozsądną politykę bezpieczeństwa można z łatwością pozyskać od specjalistów ds. bezpieczeństwa, którzy najlepiej ją rozumieją i którzy pomogą Ci nią zarządzać.

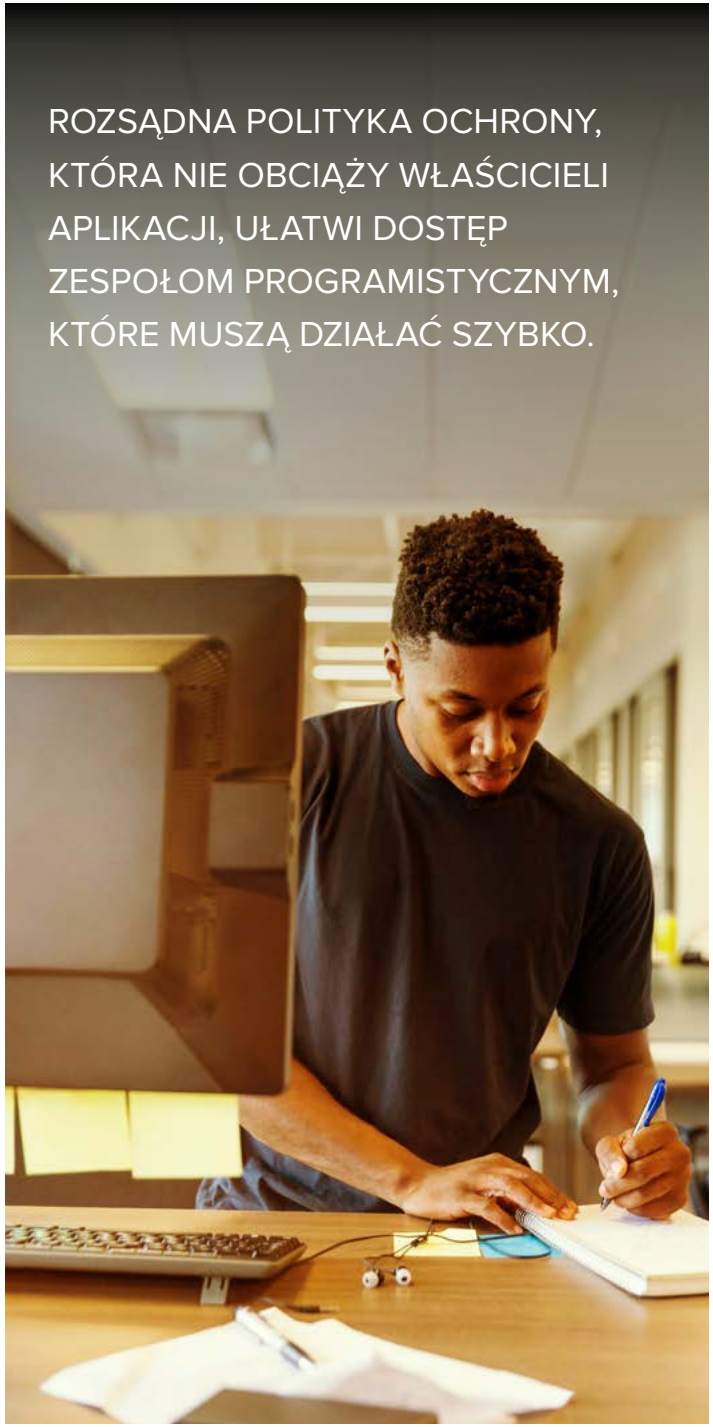
Aby jednak system zabezpieczeń był jednocześnie czynnikiem ułatwiającym biznes, musi być prosty i godny zaufania. Co więcej, musi być on zintegrowany z procesami programistycznymi w ten sam sposób, w jaki pracują programiści. Wymaga to rozsądnej polityki, która nie obciąży właścicieli aplikacji i ułatwi dostęp zespołom programistycznym, które muszą działać szybko. Jest to kluczowe, ponieważ jeśli polityka hamuje rozwój zamiast go ułatwiać, zespoły programistów mogą po prostu posłużyć się kartą kredytową i samodzielnie uruchomić aplikację w chmurze publicznej. To bywa kuszące pod presją potrzeby konkurencyjnej elastyczności i ścisłych terminów.

50%

W DUŻYCH FIRMACH SHADOW IT POCHŁANIA OBECNIE NAWET 50% WYDATKÓW.[3]

Ważne jest również umożliwienie właścicielom aplikacji i programistom interakcji z rozwiązaniami bezpieczeństwa i ADC w sposób, do jakiego są przyzwyczajeni. To oznacza interfejsy API, szablony i infrastrukturę jako kod. Zadbaj o to, by rozwiązania wdrażane w chmurze miały właściwą obsługę interfejsu API REST, pozwalając zwiększyć sprawność programową zgodnie z oczekiwaniami i potrzebami właścicieli aplikacji i zespołów DevOps (rozwoju i eksploatacji). Ich współpraca i wsparcie są niezbędne dla powodzenia każdego strategicznego programu ochrony.

[3] https://www.cio.com/article/3188726/it-industry/how-to-eliminate-enterprise-shadow-it.html



SZYBKIE CYKLE PROGRAMISTYCZNE WYMAGAJĄ **SILNYCH NARZĘDZI BEZPIECZEŃSTWA**

Nawet przy zastosowaniu zasad bezpieczeństwa ochrona Twoich aplikacji internetowych jest trudna, kosztowna i czasochłonna. Pomimo szerokiego rozumienia obszarów ryzyka, takich jak ataki XSS (cross-site scripting) i SQL injection, pozostają one wszechobecne ze względu na trudności w budowaniu systemów obronnych, które chroniłyby przed nimi przy każdej wysyłanej aplikacji. Co więcej, wiedza specjalistyczna, której wymagają bezpieczne praktyki kodowania i kompleksowa ochrona przed ryzykiem, staje się dla zespołów programistycznych coraz trudniejsza do zdobycia. Zgodnie z Raportem bezpieczeństwa ochrony aplikacji WhiteHat z 2017 r., większość aplikacji ma co najmniej trzy luki w zabezpieczeniach, z których prawie połowa jest krytycznych. Nienaprawione oznaczają zwiększone ryzyko utraty danych, kradzieży czy odmowy usługi.[4]

Mimo że ochrona aplikacji nie stała się łatwiejsza, pomocne mogą być takie narzędzia, jak firewalle WAF oparte na chmurze. Zespoły programistyczne mogą wykorzystać możliwości silnego WAFu, by bronić się przed zagrożeniami z listy OWASP Top 10 i atakami DoS w warstwie 7, wykrywać działanie botów i nim zarządzać, a także zapobiegać atakom typu zero-day. A wszystko to odbywać się może bez ingerencji w normalne cykle programistyczne. Analiza behawioralna także może być niezwykle skuteczna w identyfikowaniu wzorców i zarządzaniu ruchem do i z aplikacji webowych w chmurze. Podczas gdy funkcje te mogą być trudne do zbudowania i samodzielnego zarządzania, renomowany dostawca rozwiązań bezpieczeństwa sprawi, że wdrożenie tych usług będzie proste i skuteczne.

Co więcej, w 81 procentach naruszeń danych hakerzy wykorzystują skradzione lub słabe hasła, więc zarządzanie tożsamością powinno być kamieniem węgielnym polityki bezpieczeństwa każdej aplikacji.[5] Korzystając z tożsamości federacyjnej / pojedynczego logowania, możesz uwolnić zespół programistów od ciężaru kodowania, kontroli i utrzymania infrastruktury uwierzytelniającej, a jednocześnie ułatwić zadanie użytkownikom, którzy naprawdę nie chcą zarządzać kolejną nazwą użytkownika i hasłem, niezależnie od tego, jak fajna jest Twoja aplikacja.

[4] https://info.whitehatsec.com/rs/675-YBI-674/images/WHS%202017%20Application%20Security%20Report%20FINAL.pdf

[5] http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/

3

WIĘKSZOŚĆ APLIKACJI MA CO NAJMNIEJ TRZY LUKI W ZABEZPIECZENIACH.[4]

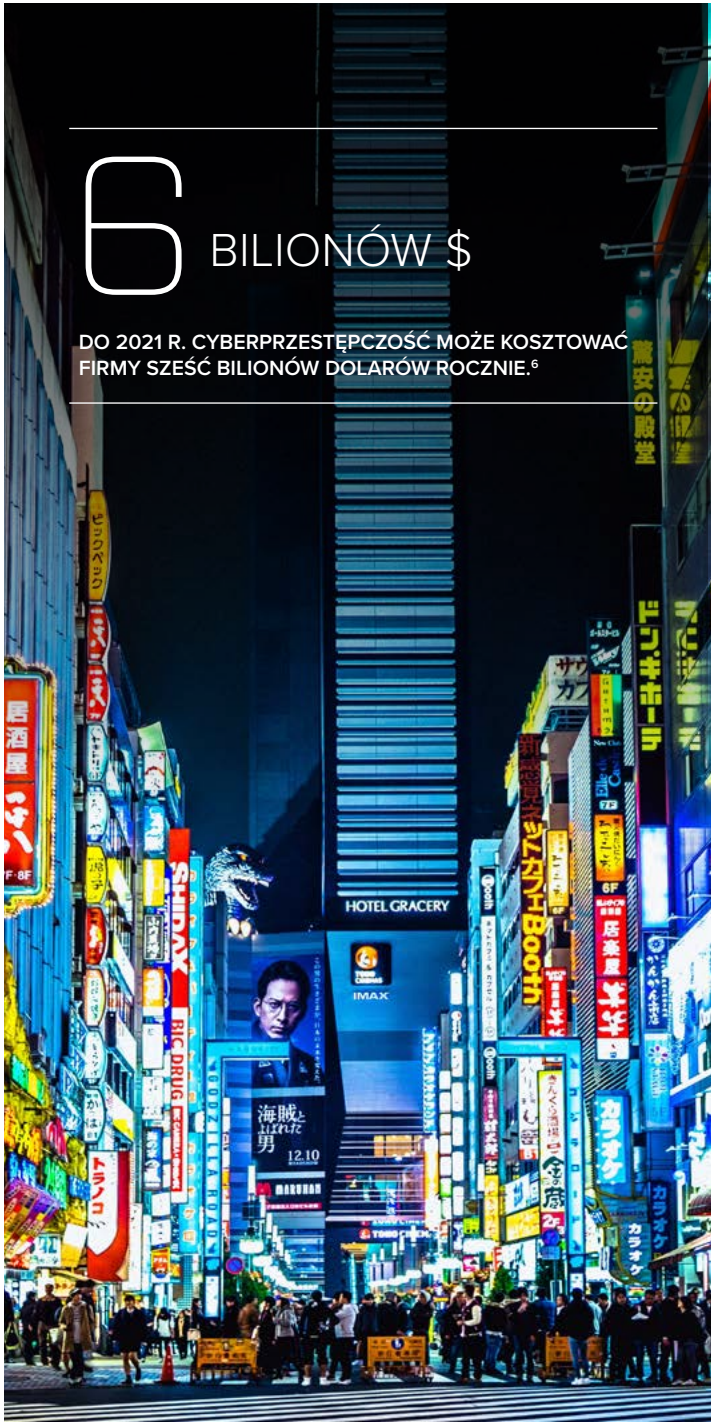
ZWIĘKSZ SPRAWNOŚĆ CHMURY Z

ZAUFANYM PARTNEREM

Dostawcy usług w chmurze czynnie konkurują o klientów, wprowadzając coraz więcej różnorodnych usług i narzędzi dla zespołów programistycznych. Jedni dostawcy oferują niedrogie długoterminowe przechowywanie archiwalne, a inni wprowadzają ulepszoną transmisję wideo. Sensownym dla danej aplikacji może być więc korzystanie z ofert w różnych chmurach. Ruchome polityki zabezpieczeń zapewniają większą elastyczność w przenoszeniu infrastruktury między różnymi dostawcami usług w chmurze, aby uzyskać dostęp do żądanych funkcji przy jednoczesnym ograniczaniu kosztów. Zaawansowany, przenośny ADC umożliwia dystrybucję płynnego obciążenia i zarządzanie nim, pozwalając wykorzystać te coraz powszechniejsze scenariusze wdrażania wielochmurowego.

Należy pamiętać o tym, że dostawcy usług w chmurze projektują systemy z myślą o zaspokojeniu potrzeb jak największej liczby klientów. Oznacza to, że ich architektura i procesy nie zawsze są optymalne dla Twoich konkretnych potrzeb. Do Ciebie należy zoptymalizowanie każdej chmury dla potrzeb własnej firmy, a pomoże Ci w tym zaufany zewnętrzny dostawca rozwiązań.

Aby bezpiecznie wdrożyć dowolną aplikację w dowolnym środowisku, musisz zadbać o to, aby Twoje rozwiązania bezpieczeństwa były gotowe do pracy w systemach wielochmurowych, wysoce programowalne i oparte na interfejsie API. Wykorzystanie wiedzy specjalistycznej zewnętrznego partnera pozwala uzyskać przenośność i użyteczność spójnych systemów bezpieczeństwa we wszystkich aplikacjach, bez konieczności zarządzania zastrzeżonymi narzędziami unikalnymi dla każdego środowiska chmury.



ROZSĄDNE ROZWIĄZANIA DLA
WIELOCHMUROWYCH PROGRAMÓW BEZPIECZEŃSTWA

W ankiecie z 2016 r. prawie trzy czwarte dyrektorów finansowych ds. technologii powiedziało, że przetwarzanie danych w chmurze będzie miało najbardziej wymierny wpływ na ich działalność w przyszłości.[6] Aby pomóc swojej firmie czerpać jak największe korzyści z chmury, potrzebujesz strategii umożliwiającej Ci kontrolowanie dostępu i tożsamości, dbanie o dostępność ważnych usług i zarządzanie lukami w bezpieczeństwie w częściach infrastruktury chmury, które pozostają pod Twoją kontrolą.

Zwiększenie bezpieczeństwa w chmurze będzie mieć jeszcze bardziej krytyczne znaczenie. Do 2021 r. koszty ponoszone przez firmy z tytułu cyberprzestępczości mogą wynosić sześć bilionów dolarów rocznie, co stanowi największy transfer bogactwa ekonomicznego w historii, nielegalnego lub innego.[7] Większość ludzi nie spodziewa się, że padnie ofiarą hakera. François de la Rochefoucauld, francuski arystokrata i pisarz żyjący w XVII wieku, lubił żartować, że „ci, którzy nie są zdolni do popełnienia wielkich zbrodni, nie podejrzewają o nie innych”.[8] Jeśli więc nawet nie podejrzewasz, że ktoś mógłby obrać sobie za cel Twoją firmę, hakerzy są zawsze gotowi wykorzystać ufność firm i właścicieli aplikacji — i niestety zbyt wielu kończy na ich celowniku.

Wykorzystanie odpowiednich narzędzi może nie tylko pomóc w obniżeniu kosztów, ale również zapewnić odpowiedni poziom ochrony dla sprawnego działania i sukcesu każdej aplikacji opartej na chmurze. Aby nie paść ofiarą fałszywego poczucia bezpieczeństwa, wybierz proaktywne podejście do ochrony aplikacji w tym nieprzewidywalnym wielochmurowym świecie.

Aby dowiedzieć się więcej na temat ochrony aplikacji, wejdź na f5.com/security.

[6] https://www.bdo.com/getattachment/022227f4-aa2e-4a8b-9739-b0ad6b855415/attachment.aspx?2017-Technology-Outlook-Report_2-17.p
[7] https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/
[8] https://books.google.com/books?id=D5B2BelDhOQC&printsec=frontcover#v=onepage&q&f=false

DBAJ O BEZPIECZEŃSTWO APLIKACJI

Aplikacje, które działają non stop, mogą pomóc we wzmocnieniu i przekształcaniu Twojej firmy — ale mogą także przyjmować rolę bramy do danych, których nie obejmie ochrona firewalli. A ponieważ większość ataków odbywa się na poziomie aplikacji, ochrona działalności Twojej firmy oznacza ochronę aplikacji, dzięki którym ta działalność jest możliwa.

Siedziba w USA: 401 Elliott Ave W, Seattle, WA 98119 | 888-882-4447 // Ameryki: info@f5.com // Azja i Pacyfik: apacinfo@f5.com // Europa/Bliski Wschód/Afryka: emeainfo@f5.com // Japonia: f5j-info@f5.com
©2017 F5 Networks, Inc. Wszelkie prawa zastrzeżone. F5, F5 Networks i logo F5 są znakami towarowymi F5 Networks, Inc. w Stanach Zjednoczonych i niektórych innych krajach. Inne znaki towarowe F5 wymienione zostały na f5.com. Wszelkie inne produkty, usługi lub nazwy firm wymienione w tym dokumencie mogą być znakami towarowymi niezależnych właścicieli, bez wyraźnego lub domniemanego potwierdzenia lub związku zatwierdzonego przez F5. EBOOK-SEC-176514946 12,17