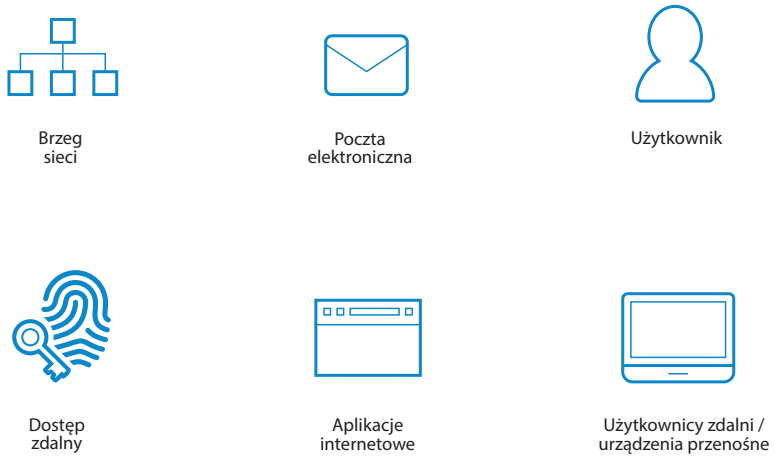
Barracuda Advanced Threat Protection

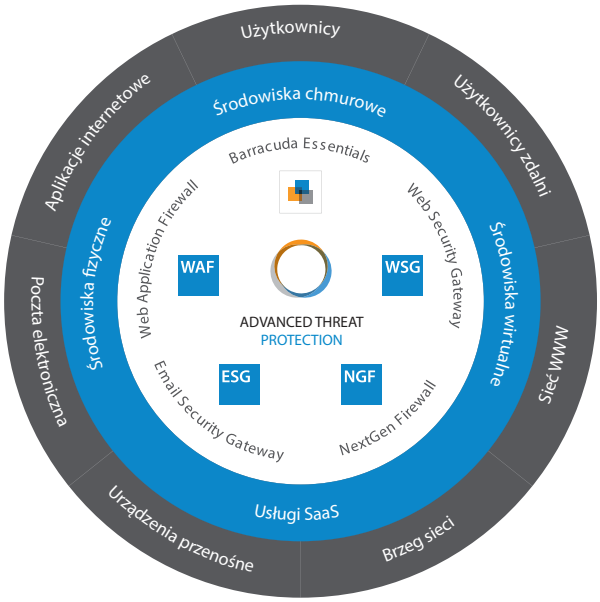
Współczesne zagrożenia wymagają stosowania wielowarstwowej ochrony

Złożony charakter współczesnych zagrożeń sprawia, że tradycyjne mechanizmy obrony, oparte na sygnaturach, stają się niewystarczające, przez co mogą narażać przedsiębiorstwa i instytucje na potężne szkody. Z kolei zaawansowane techniki obrony, takie jak badanie potencjalnych zagrożeń w wydzielonym środowisku (ang. sandboxing), są kosztowne i wymagają dużej mocy obliczeniowej. W tej sytuacji do zapewnienia kompleksowej i niezawodnej ochrony przed złożonymi zagrożeniami, jak oprogramowanie ransomware czy zaawansowane zagrożenia o długotrwałym działaniu (ang. advanced persistent threats) niezbędne są rozwiązania wielowarstwowe, które pozwalają stosować coraz to bardziej wyrafinowane techniki obrony, w celu uzyskania właściwej równowagi między dokładnością wykrywania zagrożeń, a szybkością reakcji. Docelowa architektura powinna zapewniać ochronę przed wszystkimi zagrożeniami z uwzględnieniem różnych wektorów zagrożeń i różnych środowisk wdrażania, jak infrastruktury fizyczne, wirtualne, usługi SaaS (ang. software-as-a-service - oprogramowanie jako usługa) czy platformy chmury publicznej.



6 najczęściej występujących wektorów zagrożeń w Internecie

Barracuda Advanced Threat Protection (BATP) to usługa oparta na chmurze, która zapewnia skuteczną ochronę przed szkodliwym oprogramowaniem (w tym oprogramowaniem ransomware) i zaawansowanymi cyberatakami. Rozwiązanie obejmuje kilka warstw wykrywania, w tym warstwy analizy na podstawie sygnatur, analizy statycznej i analizy behawioralnej, a także wszechstronne funkcje analizy w wydzielonym środowisku, które umożliwiają dokładne wykrywanie całej gamy zagrożeń polimorficznych. Udostępnianą w chmurze usługę zintegrowano ze wszystkimi rozwiązaniami zabezpieczającymi firmy Barracuda, obsługującymi poszczególne wektory zagrożeń, takie jak strony WWW, użytkownicy, sieci lokalne, pocztę elektroniczną i aplikacje, we wszystkich środowiskach. Ponadto usługa BATP automatycznie łączy się z globalną siecią analizy zagrożeń, w której gromadzone są dane z wielu różnych źródeł na całym świecie. Dzięki temu zapewnia ochronę w czasie rzeczywistym, obejmującą wszystkie wektory zagrożeń.



Usługa Barracuda Advanced Threat Protection (BATP)

Złożone zagrożenia trudno wykryć tradycyjnymi metodami

Współczesne ataki szybko stają się coraz groźniejsze - zarówno pod względem zasięgu, jak i wyrafinowania. Nowe odmiany szkodliwego oprogramowania, takie jak ransomware, są tworzone w sposób pozwalający uniknąć wykrycia ich tradycyjnymi metodami i często rozpowszechniane w ramach ukierunkowanych ataków typu „zero-hour".

Zdaniem czołowych analityków z branży, do 2023 roku w każdym kwartale może pojawiać się ponad 200 nowych odmian oprogramowania ransomware[1]. Osoby przeprowadzające tego rodzaju ataki mogą czerpać z nich ogromne zyski, a to dopiero początek - zgodnie z przewidywaniami do końca 2017 roku samo tylko oprogramowanie ransomware przyniesie przestępcom przychody w wysokości ponad 1 mld USD. W tej sytuacji wielu zwykłych użytkowników zaczyna gorączkowo szukać najlepszych sposobów na zabezpieczenie się przed nowego typu atakami.

Szkodliwe oprogramowanie - np. ransomware - wykorzystuje wiele wektorów zagrożeń

W celu uzyskania maksymalnego efektu, cyberprzestępcy coraz częściej rozpowszechniają szkodliwe oprogramowanie z wykorzystaniem wielu wektorów zagrożeń. Zdecydowanie najpopularniejszym kanałem jest poczta elektroniczna - zwłaszcza w przypadku ataków typu „phishing" i „spear phishing", których celem jest wyłudzanie danych. Firma IDC szacuje, że „do ponad 90% infekcji typu ransomware dochodzi w wyniku otwarcia niebezpiecznego załącznika w wiadomości e-mail".[2]

[1] *Analityk Michael Osterman, 2016 r.*
[2] *Raport „IDC Analyst Connection: Why SaaS-Based Productivity Tools Require Additional Threat Protection", 2017 r.*

Użytkowników można również skłonić do pobrania szkodliwych plików poprzez stosowanie metod socjotechnicznych, podszywanie się pod inne osoby, włamywanie się na strony internetowe czy podrabianie adresów internetowych (URL), a także przy użyciu innych technik. W sytuacji, gdy tak wielu pracowników korzysta z urządzeń przenośnych, a sieci stają się coraz bardziej rozproszone, sama zapora z funkcją bramy może okazać się niewystarczająca.

Należy pamiętać, że kompleksowa strategia bezpieczeństwa powinna uwzględniać wszystkie typy zagrożeń i wszystkie wektory ataków. Elementem skutecznej koncepcji ochrony przed zagrożeniami powinna być wewnętrzna wymiana wszelkiego rodzaju informacji na temat zagrożeń i ataków.

Badanie zagrożeń w wydzielonym środowisku nie jest efektywne

Najchętniej stosowaną metodą wykrywania zagrożeń typu „zero-hour" jest badanie podejrzanych elementów w kontrolowanych warunkach. Polega to zwykle na unieszkodliwieniu plików (załączników) w wirtualnym środowisku testowym, emulującym rzeczywiste środowiska punktów końcowych podatne na ataki.

Metoda ta bywa skuteczna, ale jej stosowanie w przypadku każdego załącznika może być bardzo czasochłonne z uwagi na duże wymagania związane z przetwarzaniem danych. W celu uniknięcia dużych opóźnień w dostarczaniu treści, przedsiębiorstwa muszą stosować bardzo duże i drogie wyspecjalizowane urządzenia do testowania w wydzielonych środowiskach. Czasami muszą zezwalać na dostarczenie niektórych załączników przed ich pełnym przeskanowaniem wystawiając się w ten sposób na ryzyko ataku. Niektóre zaawansowane zagrożenia są projektowane tak, aby wykrywać środowiska testowe działające wyłącznie w oparciu o maszyny wirtualne. Aby uniknąć wykrycia, szkodliwe oprogramowanie maskuje wszelką podejrzaną aktywność, przez co opisywana metoda analizy staje się nieskuteczna.
Ponadto wewnętrzne środowiska testowe znajdują się zwykle w centrali firmy, co wiąże się z koniecznością przesyłania załączników z innych oddziałów i placówek firmy, a także nie umożliwiają skalowania w miarę wzrostu natężenia ruchu (liczby placówek i użytkowników). Sprawy dodatkowo komplikuje fakt, że przedsiębiorstwa przenoszą swoją infrastrukturę do chmury, a tym samym muszą objąć zabezpieczeniami również tego rodzaju środowiska. W rezultacie jeszcze bardziej rośnie obciążenie lokalnego środowiska testowego.

Skuteczna ochrona dzięki usłudze Barracuda Advanced Threat Protection

W odpowiedzi na powyższe wyzwania Barracuda Networks postanowiła wykorzystać swoje kilkudziesięcioletnie doświadczenie w zwalczaniu zaawansowanego szkodliwego oprogramowania poprzez stworzenie platformy chmurowej, która zapewniłaby kompleksową ochronę przed wszelkiego rodzaju szkodliwym oprogramowaniem przy zachowaniu maksymalnej wydajności, zakresu działania, dokładności i bezpieczeństwa.

Wielowarstwowa ochrona

Barracuda Advanced Threat Protection (BATP) to zintegrowana usługa chmurowa, która łączy w sobie kilka warstw wykrywania zagrożeń oraz mechanizmy uczenia maszynowego. Poszczególne warstwy wykrywania zaprojektowano z myślą o stopniowym eliminowaniu zagrożeń różniących się dotkliwością i złożonością. Dzięki wstępnemu filtrowaniu w kolejnych warstwach usługa BATP umożliwia bardzo szybkie reagowanie na wszelkiego rodzaju ataki przy minimalnych opóźnieniach w ścieżce danych i bez naruszania obowiązujących zasad bezpieczeństwa. Poszczególne warstwy wykrywania automatycznie udostępniają sobie nawzajem wyniki analiz, co umożliwia przetwarzanie większej ilości danych na poziomie całej usługi, a tym samym pozwala na skuteczniejsze i szybsze reagowanie na nowe zagrożenia. Dzięki temu powtórne wystąpienia znanych już zagrożeń są szybko wykrywane przez niższe warstwy. Warstwy wymagające większej ilości zasobów - takie jak warstwa testowania w wydzielonym środowisku - mogą analizować nowo powstające warianty zagrożeń.

Warstwy ochrony:

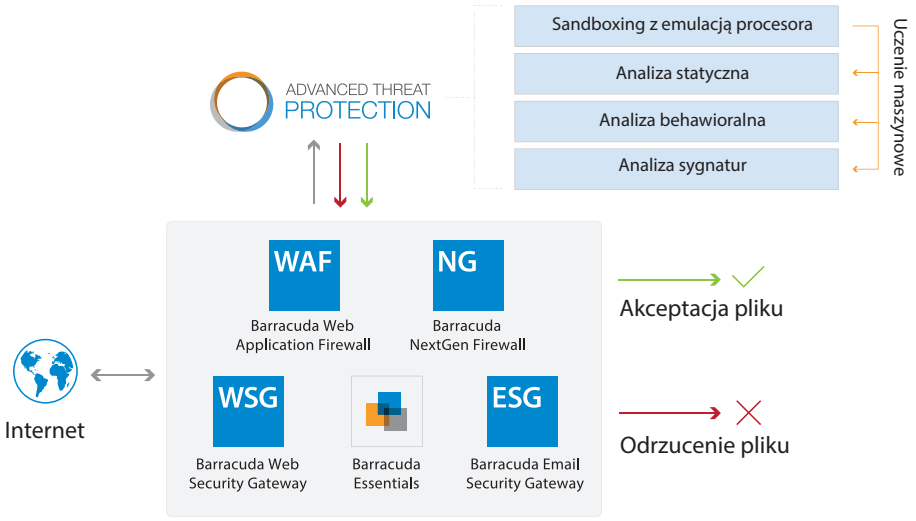
1. **Advanced Threat Signatures (Sygnatury zaawansowanych zagrożeń).**
   Firma Barracuda zbiera informacje o sygnaturach zagrożeń z ponad 250 tys. punktów końcowych (urządzeń wyspecjalizowanych i usług w sieci WWW), a także z innych źródeł, takich jak pułapki (ang. honeypot), boty indeksujące, pobierane pliki, wirusy, szkodliwe oprogramowanie (w tym programy szpiegujące), załączniki do wiadomości e-mail, sieci oraz dane aplikacji. Na podstawie wyników analizy zagrożeń powstaje ogromna baza danych sygnatur, która gwarantuje, że informacje o każdym nowym zagrożeniu pojawiającym się w „polu widzenia" trafiają natychmiast, w czasie rzeczywistym, do wszystkich produktów zabezpieczających.

2. **Analiza behawioralna i heurystyczna.**
   Polega na wykonywaniu w kontrolowanych warunkach określonych poleceń programistycznych, zawartych w budzącym wątpliwości fragmencie kodu lub skryptu. Zachowanie programu jest analizowane pod kątem typowych działań wirusów, takich jak replikacja, zastępowanie plików czy próby maskowania podejrzanego pliku. Za podejrzane uznaje się również zbyt długie ustawienia czasomierza, pętle programistyczne działające przez kilka dni oraz elementy kodu usiłujące uzyskać dostęp do rejestru lub funkcji pamięci.

3. **Analiza statyczna kodu.**
   Polega na badaniu fragmentów pliku wykonywalnego bez jego uruchamiania. Autorzy niebezpiecznego kodu próbują go zamaskować, aby zmylić mechanizmy wykrywania, takie jak oprogramowanie antywirusowe, a warstwa analizy statycznej pozwala zbadać i ujawnić wszelkie podejrzane konstrukcje kodu. Warstwa ta umożliwia bardzo skuteczne i szybkie wstępne filtrowanie szkodliwego oprogramowania przed przekazaniem podejrzanych plików do warstwy badania zagrożeń w wydzielonym środowisku.

4. **Badanie zagrożeń w wydzielonym środowisku z wykorzystaniem emulacji procesora.**
   Ostatnią warstwą ochrony jest sandboxing, wykorzystujący funkcje emulacji procesora. Umożliwia to unieszkodliwienie każdego załącznika, którego analiza we

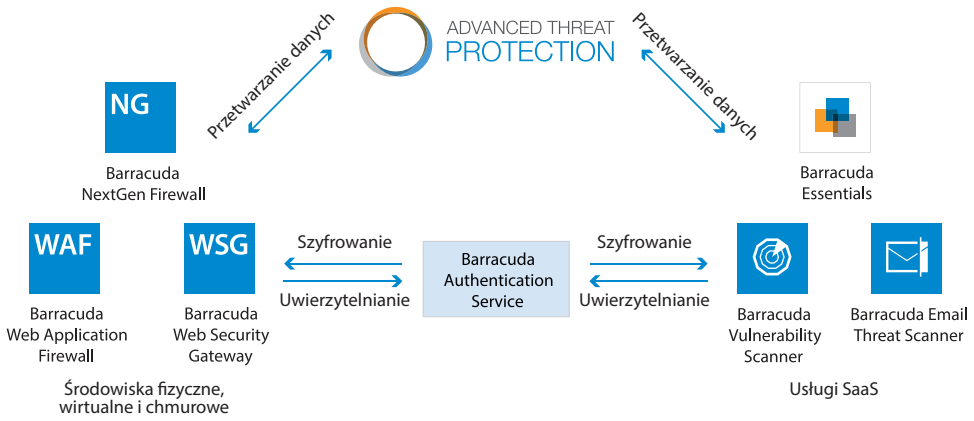
wcześniejszych warstwach nie przyniosła jednoznacznych rezultatów. Dzięki zastosowaniu technik emulacji, sandbox pozwala rozpoznać zagrożenia zaprojektowane z myślą o uniknięciu wykrycia przez tradycyjne środowiska testowe oparte na wirtualizacji. Wstępne filtrowanie plików w innych warstwach usługi BATP pozwala ograniczyć do minimum opóźnienia związane z przetwarzaniem złożonych zagrożeń w środowisku testowym.



Wielowarstwowa ochrona przed zagrożeniami

Rozproszona i skalowalna usługa działająca w chmurze

Usługa BATP w pełni wykorzystuje zalety globalnie rozproszonej i wysoce skalowalnej architektury mikrousług realizowanych w chmurze. Korzystają z niej wszystkie produkty zabezpieczające w ofercie firmy Barracuda, w tym rozwiązania do ochrony sieci lokalnych, aplikacji internetowych, poczty elektronicznej i sieci WWW. Dodatkową zaletą jest możliwość automatycznego zwiększania wydajności i poszerzania zasięgu usługi w odpowiedzi na coraz większy ruch generowany przez klientów firmy Barracuda na całym świecie. Usługa korzysta z doskonale zabezpieczonych kanałów komunikacyjnych w celu zapewnienia poufności i bezpieczeństwa transmisji danych.

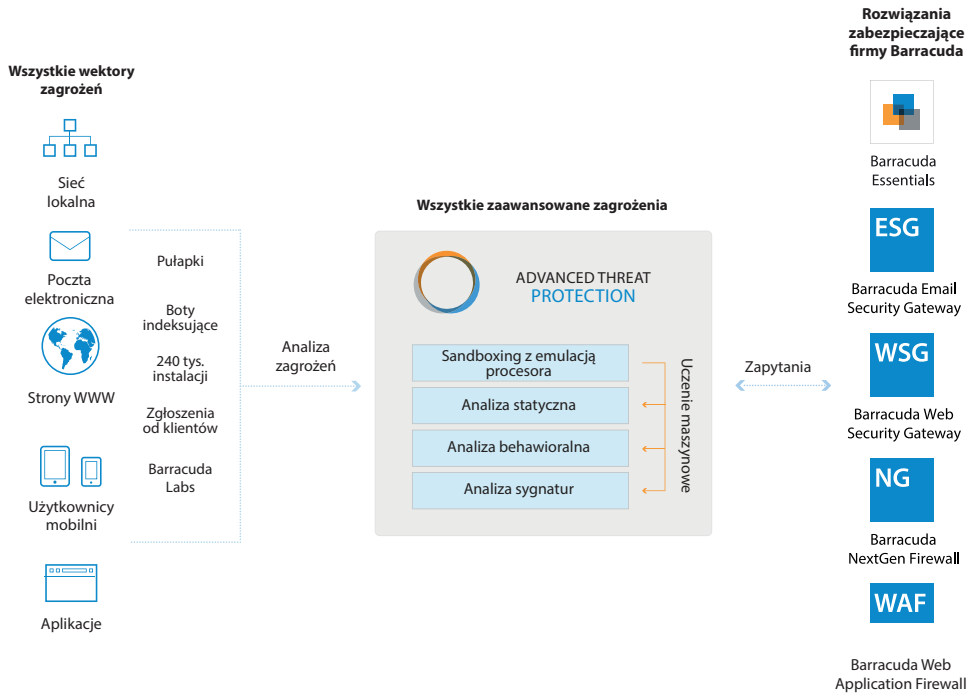


Architektura usługi BATP

Globalna sieć analizy zagrożeń

W związku z rozszerzeniem ochrony na wiele wektorów ataków, usługa Barracuda Advanced Threat Protection korzysta z rozbudowanej, globalnej sieci analizy zagrożeń. Trafiają do niej ogromne ilości zróżnicowanych informacji o zagrożeniach z ponad 50 mln punktów gromadzenia danych na całym świecie. Jednym z elementów infrastruktury wspomagającej funkcjonowanie usługi jest farma serwerów z akceleracją sprzętową, która w ramach procesu uczenia maszynowego przetwarza powyższe dane i analizuje ponad 900 atrybutów na każdy obiekt.

Wszystkie produkty marki Barracuda objęte usługą BATP stają się częścią wysoce zróżnicowanej sieci, która umożliwia udostępnianie wyników analiz obejmujących wszystkie wektory ataków w celu zapewnienia subskrybentom ochrony w czasie rzeczywistym. Na przykład, jeśli usługa BATP wykryje zagrożenie rozprzestrzeniające się początkowo za pośrednictwem poczty elektronicznej, ochrona jest natychmiast rozszerzana na wszystkie inne obsługiwane wektory ataków. Po zidentyfikowaniu nowego zagrożenia i utworzeniu sygnatury odpowiednia informacja jest przekazywana do warstwy drugiej. Dzięki temu kolejna próba wprowadzenia niebezpiecznego oprogramowania do sieci przedsiębiorstwa zostanie zablokowana, bez konieczności ponownego wysyłania plików do sandboxa. W przeprowadzonym w 2016 roku niezależnym teście technologii ochrony przed zaawansowanymi zagrożeniami firma Barracuda Networks jako jedyna uzyskała 100-procentową skuteczność bez fałszywych alarmów i niewykrytych zagrożeń.



Infrastruktura analizy zagrożeń firmy Barracuda

Podsumowanie

Stworzenie kompleksowej architektury zabezpieczeń zapewniającej ochronę przed dzisiejszymi złożonymi zagrożeniami wiąże się z wieloma wyzwaniami. Odpowiedzią jest usługa Barracuda Advanced Threat Protection, która w połączeniu z wyspecjalizowanymi rozwiązaniami zabezpieczającymi firmy Barracuda Networks oferuje przedsiębiorstwom łatwe w obsłudze, opłacalne, skalowalne i skuteczne narzędzia pozwalające stawić czoła tym wyzwaniom.

Informacje o dystrybutorze rozwiązań Barracuda Networks w Polsce:

DAGMA to **ogólnopolski dystrybutor firmy Barracuda Networks**, związany z marką od 2010 r. Firma DAGMA specjalizuje się w rozwiązaniach z zakresu bezpieczeństwa IT. W swojej ofercie posiada zarówno produkty do ochrony antywirusowej i antyspamowej, rozwiązania do backupu, aplikacje szyfrujące dane, a także urządzenia klasy UTM, Next-Generation Firewall oraz WAF.

DAGMA w zakresie swojej działalności **oferuje audyty bezpieczeństwa, doradztwo, wdrożenia oraz pełne wsparcie techniczne** dla rozwiązań ze swojego portfolio. Firma ma również własne Autoryzowane Centrum Szkoleniowe, które oferuje szkolenia w 7 miastach w Polsce.

DAGMA współpracuje z siecią **ponad 2000 partnerów handlowych i resellerów** dostarczając rozwiązania dla klientów końcowych.

Więcej informacji o produktach Barracuda Networks można znaleźć na stronie www.barracuda.com.pl.

DAGMA bezpieczeństwo it

Dystrybucja rozwiązań Barracuda Networks w Polsce:
DAGMA Biuro Bezpieczeństwa IT
ul. Bażantów 4/2
40-668 Katowice

tel. 32 793 11 00
faks 32 793 11 90
www.barracuda.com.pl
handel@dagma.pl