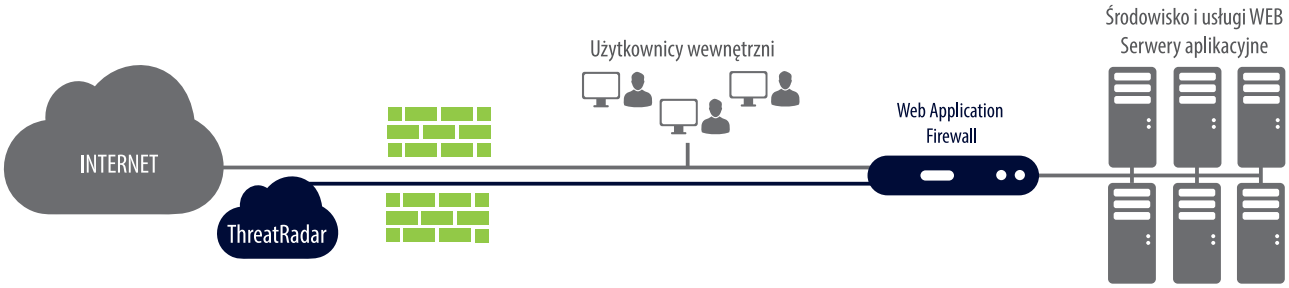
Trafford IT

Imperva

BEZPIECZEŃSTWO APLIKACJI WEB, BAZ DANYCH, PLIKÓW I APLIKACJI CHMUROWYCH

BEZPIECZEŃSTWO APLIKACJI WEB

Web Application Firewall (WAF) to skuteczna zapora aplikacyjna „rozumiejąca" strukturę aplikacji, jej poszczególne komponenty, a także przewidywane zachowanie użytkownika, wyszukując anomalie w ruchu WEB. Zastosowana technologia Dynamic Profiling automatyzuje proces zabezpieczenia poprzez automatyczną budowę profilu aplikacji, tworzenie zbioru reguł oraz listy akceptowalnych zachowań użytkownika. Zamknięty profil aplikacji nie eliminuje możliwości wykonywania planowych zmian w jej architekturze, gdyż system sam dostosowuje się do jej nowych elementów. WAF dysponuje także ogromną liczbą konfigurowalnych, wbudowanych polityk i reguł, dzięki którym wykrywana jest pełna gama ataków na aplikację WEB.



ThreatRadar Reputation Services to jedna z licencji uzupełniających Web Application Firewall, która zapewnia automatyczną klasyfikację adresów IP klientów korzystających z serwisu WEB. ThreatRadar przeciwdziała zautomatyzowanym atakom (np. phishing IP, szkodliwe adresy IP, adresy o złej reputacji) poprzez integrację wiarygodnych informacji na temat znanych źródeł ataków z systemami ochrony SecureSphere. ThreatRadar jest w stanie szybko i skutecznie zatrzymywać ruch sieciowy z potencjalnie groźnych źródeł, zanim jeszcze atak może zostać zainicjowany, bądź wzbogacić analizę podczas wystąpienia alertu.

BEZPIECZEŃSTWO BAZ DANYCH

Database Activity Monitoring (DAM) nieustannie monitoruje i kontroluje w czasie rzeczywistym wszystkie operacje wykonywane na bazach danych, dostarczając szczegółowych informacji na temat tego, *„kto?, co?, kiedy?, gdzie? oraz jak?"*. DAM kontroluje użytkowników uprzywilejowanych logujących się do bazy zdalnie, jak i lokalnie, ale także użytkowników standardowych, łączących się z serwerem za pomocą różnych aplikacji, nawet tzw. kontem „technicznym". System monitoruje odpowiedzi baz danych, w kontekście wycieku poufnych informacji oraz naruszeń bezpieczeństwa, a w krytycznych sytuacjach ma możliwość blokowania tych odpowiedzi. Dodatkowo budowany jest profil bazy danych, dzięki czemu wykrywane są wszelkie anomalie związane z podejrzanymi zapytaniami.

Discovery and Assessment Server (DAS) jest unikalnym, rozbudowanym skanerem podatności w bazach danych. Wykorzystuje gotowe, wbudowane polityki analiz podatności w konfiguracji, bazach danych oraz w platformie na jakiej pracują. Dzięki temu pomaga organizacjom w identyfikacji i eliminacji słabych punktów. System wirtualnych poprawek może blokować próby wykorzystania wykrytych podatności, zapewniając tym samym natychmiastową ochronę bez konieczności aktualizacji bazy. Technologia ta ogranicza do minimum czas, w którym system wystawiony jest na ataki, jak również znacząco zmniejsza ryzyko naruszenia bezpieczeństwa danych podczas testowania i dostarczania poprawek do nich. DAS potrafi skanować i wykrywać wszelkie instancje baz danych, które są wystawione w sieci, odnajdując nieautoryzowane środowiska testowe z realnymi danymi.

User Rights Management for Databases (URMD) automatycznie gromadzi informacje na temat praw użytkowników dla heterogenicznych baz danych. System zarządzania prawami użytkowników umożliwia ich łatwe przeglądanie, identyfikację pracowników ze zbyt dużymi, czy też wielokrotnie zagnieżdżonymi uprawnieniami, ograniczając tym samym wyciek danych. Ułatwia także wykazywanie zgodności z regulacjami takimi jak: SOX czy PCI.

CounterBreach to dodatkowy moduł korzystający z logów audytowych rozwiązania Imperva DAM. Przy pomocy algorytmów machine learning, CounterBreach buduje model korzystania z danych przez użytkowników. Uwzględnia nie tylko ich aktywność, lecz również dane, po które sięgają oraz sposób, w jaki to robią. Po zbudowaniu modelu, system jest w stanie wykryć wszelkie anomalie, dzięki czemu działy bezpieczeństwa mogą szybko reagować na ryzykowne zachowania użytkowników.

MASKOWANIE DANYCH

Maskowanie i zaciemnianie wrażliwych danych jest bardzo istotną częścią polityki bezpieczeństwa. Używając zaawansowanych algorytmów maskowania, Imperva Camouflage zamienia wrażliwe dane na fikcyjne, zachowując przy tym ich pełną wartość logiczną i statystyczną. Zamaskowane dane mogą służyć m.in. w rozwoju systemów, procesie testowania, czy w systemach nieprodukcyjnych, bez ryzyka wycieku danych wrażliwych. Dodatkowo dane bez obaw mogą być wysyłane do firm zewnętrznych, outsourcingowych, a zaciemnione bazy danych nie muszą być zgłaszane do urzędów – np. do GIODO.

BEZPIECZEŃSTWO PLIKÓW

File Activity Monitoring (FAM) monitoruje i kontroluje w czasie rzeczywistym wszystkie operacje wykonywane na plikach, nie ograniczając przy tym wydajności i dostępności serwera plików, bądź dysków sieciowych. FAM udostępnia szczegółowe informacje dotyczące nazwy użytkownika pliku, do którego uzyskiwany jest dostęp, folderu macierzystego, czasu dostępu, wykonanej operacji itp. Aby zapewnić podział obowiązków, informacje te przechowywane są w zewnętrznym, zabezpieczonym repozytorium i udostępniane poprzez widok „tylko do odczytu". System w pełni integruje się z Active Directory, wzbogacając zbierane informacje.

OCHRONA SHAREPOINT

Imperva SecureSphere for SharePoint to unikalne narzędzie dedykowane do zaawansowanej ochrony zasobów SharePoint. System jest połączeniem unikalnych cech ochrony SharePoint typu Web Application Firewall dla opublikowanych treści WEB, Database Activity Monitoring z dedykowanymi politykami ochrony SharePoint dla bazy danych MSsql oraz ochrony zasobów plikowych typu File Activity Monitoring skonfigurowaną specjalnie dla ochrony umieszczanych w tej aplikacji plików. Łącząc te trzy elementy, produkt daje olbrzymie możliwości ochrony tak skomplikowanej i rozbudowanej aplikacji.

KONTROLA I WIDOCZNOŚĆ APLIKACJI CHMUROWYCH

Imperva Skyfence Cloud Gateway zapewnia widoczność i kontrolę wykorzystania aplikacji w chmurze. Automatycznie wykrywa jej użycie, analizuje ryzyko i wymusza odpowiednie kontrole dla aplikacji SaaS oraz systemów produkcyjnych. Dzięki Imperva Skyfence użytkownicy mogą korzystać z aplikacji, których potrzebują, a dział IT jest w stanie zapewnić im odpowiednią ochronę.

1 **ODKRYWANIE**
Widoczność aplikacji używanych przez pracowników

2 **OCENA RYZYKA**
Ocena ryzyka kontekstowego aplikacji, użytkowników i konfiguracji zabezpieczeń

3 **OCHRONA I KONTROLA**
Zautomatyzowane zapobieganie zagrożeniom w chmurze i dostosowane do kontekstu egzekwowanie polityk

Zalety rozwiązania:

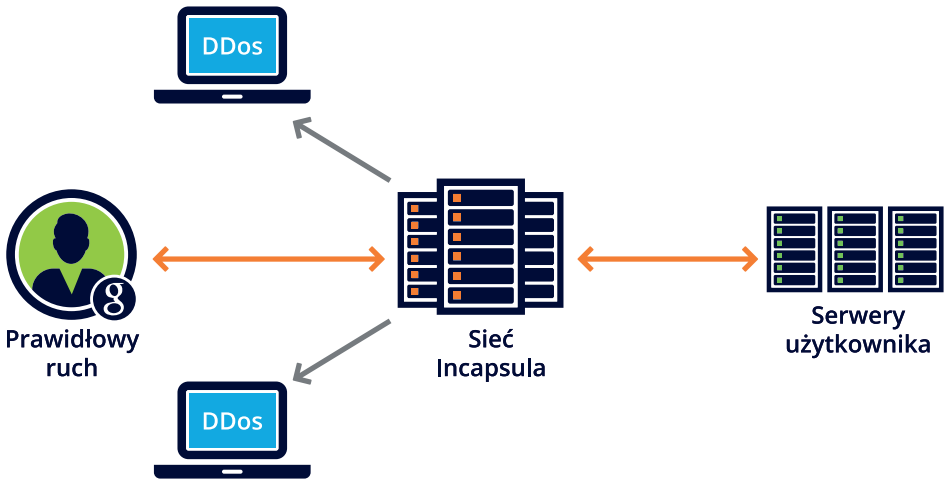
- Zapewnienie widoczności aplikacji, zarządzanie nimi, analiza i ochrona w jednym zintegrowanym rozwiązaniu.
- Elastyczność wdrażania przy pomocy urządzeń, maszyn wirtualnych oraz usług wykonywanych w oparciu o chmurę.
- Szczegółowe polityki dla różnych urządzeń końcowych umożliwiają kontrolę dostępu i ochronę danych dla zarządzanych i niezarządzanych telefonów komórkowych, tabletów i laptopów.
- Wbudowana integracja z katalogami przedsiębiorstwa oraz narzędziami SIEM i MDM.
- Dogłębne wsparcie dla aplikacji Office 365, AWS, Salesforce, Google Apps, Box i Dropbox – aż po obiekt danych i poziomy działania.

AUTOMATYCZNE PRZECIWDZIAŁANIE NAJWIĘKSZYM ATAKOM DDoS

Imperva Incapsula zabezpiecza strony internetowe, serwery DNS i całe łącza internetowe przed najpoważniejszymi i najbardziej inteligentnymi typami ataków DDoS – w tym atakami na poziomie sieci, protokołu i aplikacji (warstwy 3, 4 i 7) – ograniczając ich wpływ na działalność biznesową do minimum. Incapsula cechuje się natychmiastową wrażliwością już w pierwszych fazach ataku, a jednocześnie bardzo dokładnie odróżnia prawdziwe zapytania od ataku. Dzięki usłudze rozproszenia ruchu na ponad trzydzieści punktów obsługi, atak eliminowany jest już u źródła.

Usługa Incapsula sprawdza się nawet w atakach o największej skali i odpiera złożone ataki w warstwie aplikacji poprzez zastosowanie zaawansowanych i progresywnych mechanizmów obronnych. Usługa automatycznie i transparentnie reaguje na ataki DDoS z minimalną liczbą pomyłek tak, że odwiedzający stronę nawet nie wiedzą, że serwis jest celem ataku.

Incapsula obejmuje działające w czasie rzeczywistym panele do monitorowania i analizowania trwających ataków oraz dedykowane, całodobowe centrum NOC obsługiwane przez doświadczonych ekspertów ds. bezpieczeństwa, którzy zapewniają zachowanie dostępności usługi na poziomie biznesowym w czasie ataku oraz doskonałe wsparcie.



Imperva Incapsula wykrywa i reaguje na złożone ataki wykorzystujące słabe punkty aplikacji, serwera WWW i serwera DNS, a także ataki typu hit-and-run i zagrożenia stwarzane przed duże botnety.

System oferuje możliwość szybkiego, łatwego wdrożenia poprzez przekierowanie DNS, nawet dla jednej domeny. Wdrożenie modułu ochrony przed atakami DDoS nie wymaga instalowania sprzętu, oprogramowania, prac integracyjnych ani wprowadzania zmian w kodzie strony internetowej. Dzięki tak łatwemu mechanizmowi wdrożenia użytkownik jest chroniony już po kilku minutach i nie musi zmieniać obecnego dostawcy usług hostingowych ani infrastruktury aplikacji. Dla ochrony własnych zasobów DNS czy całego łącza istnieje możliwość przekierowania całej klasy adresowej poprzez routing BGP.