



## Bezpieczeństwo aplikacji webowych

### Chroń swoje kluczowe aplikacje webowe

*Wiodące na rynku rozwiązanie Imperva SecureSphere Web Application Firewall:*

- » Automatycznie „uczy się” struktur danej aplikacji webowej i oczekiwanych zachowań użytkownika
- » Aktualizuje systemy ochrony w środowisku Web w oparciu o odnajdywanie i analizę aktualnie pojawiających się zagrożeń
- » Przy pomocy ThreatRadar identyfikuje ruch sieciowy pochodzący z potencjalnie niebezpiecznych źródeł
- » Tworzy wirtualne poprawki dla aplikacji poprzez integrację ze skanerem podatności
- » Zapewnia wysoką wydajność, możliwość wdrożenia typu drop-in, a także przejrzyste, adekwatne do danego przedsiębiorstwa raportowanie i system ostrzeżeń
- » W pełni wspiera normę PCI DSS 6.6

### Produkty

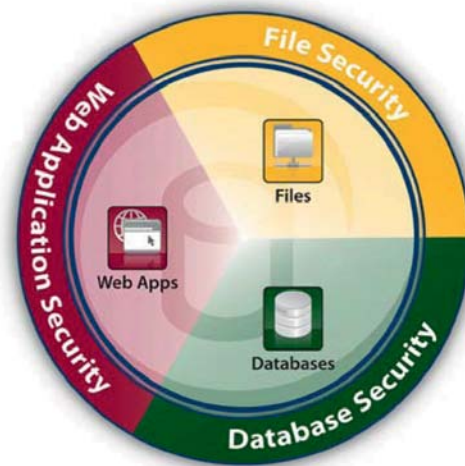
**SecureSphere Web Application Firewall**

**ThreatRadar**

## Wiodące mechanizmy kontroli i ochrony plików

Aplikacje webowe są głównym celem ataków ze względu na łatwość, z jaką można uzyskać do nich dostęp. Ich niebagatelna wartość wynika z faktu, iż z ich poziomu możliwy jest dostęp do cennych danych. W celu zwalczania złożonych i rozproszonych ataków przedsiębiorstwa muszą chronić swoje witryny webowe przed nowymi i wciąż powstającymi zagrożeniami, przy zachowaniu wysokiej wydajności i nieprzerwanego działania aplikacji.

Wiodące na rynku rozwiązanie SecureSphere Web Application Firewall całkowicie odmieniło sposoby zabezpieczania aplikacji przez przedsiębiorstwa dzięki zautomatyzowaniu ochrony webowej i wprowadzeniu elastycznego, przejrzystego procesu wdrożenia. Ze swymi kompleksowymi opcjami ochrony i niskim nakładem administracyjnym, SecureSphere stanowi idealne rozwiązanie zabezpieczające cenne zasoby sieciowe przy jednoczesnym zachowaniu zgodności z normami i regulacjami, jak PCI DSS.



### Automatyczne „poznawanie” aplikacji i zachowań użytkownika

Aby skutecznie wykrywać ataki, zapora firewall aplikacji webowych musi „zrozumieć” strukturę aplikacji, jej poszczególne komponenty, a także przewidywane zachowanie użytkownika. Będąca w trakcie procesu patentowego technologia Dynamic Profiling firmy Imperva automatyzuje ten proces poprzez profilowanie chronionych aplikacji oraz tworzenie zbioru reguł, czy też „białej listy” akceptowanych zachowań użytkownika. Z biegiem czasu automatycznie włącza ona w profil aplikacji planowe zmiany w jej architekturze. Technologia Dynamic Profiling eliminuje potrzebę manualnego konfigurowania i aktualizowania niezliczonych aplikacyjnych URL, parametrów, plików cookie oraz metod.

### Oparte na analizach reguły polityki bezpieczeństwa

Opierając się na badaniach ośrodka Imperva Application Defense Center (ADC), organizacji o międzynarodowej renomie prowadzącej badania nad bezpieczeństwem danych, SecureSphere oferuje najbardziej kompletny spośród dostępnych zestaw sygnatur aplikacji i reguł polityk bezpieczeństwa. ADC analizuje słabe punkty zgłaszane przez Bugtraq, CVE, Snort, a także przez „podziemne fora”. Prowadzi również bezpośrednie badania w celu zapewnienia najaktualniejszej i najbardziej kompleksowej dostępnej ochrony przed atakami.

### Ochrona adaptacyjna przed zautomatyzowanymi atakami na dużą skalę

ThreatRadar, pionierska na rynku usługa bezpieczeństwa webowego opartego na reputacji, stanowi opcjonalny dodatek do firewalla WAF Secure Sphere. ThreatRadar przeciwdziała zautomatyzowanym atakom na dużą skalę poprzez integrację wiarygodnych informacji na temat znanych źródeł ataków z systemami ochrony SecureSphere. ThreatRadar jest w stanie szybko i skutecznie zatrzymać ruch sieciowy z potencjalnie groźnych źródeł, zanim jeszcze atak może zostać zainicjowany.

### System wirtualnych poprawek zintegrowany ze skanerem słabych punktów

Aby natychmiastowo instalować poprawki w słabych punktach aplikacji, SecureSphere jest w stanie importować wyniki analizy z WhiteHat, IBM, Cenizic, NT OBJECTives, Qualys i innych źródeł, a następnie tworzyć nowe reguły polityk przystosowane specjalnie do blokowania znanych słabych punktów. System wirtualnych poprawek redukuje skalę potencjalnego wystawienia na zagrożenia, jak również koszty doraźnych napraw i cykli testowych.

### Ochrona przed atakami ukierunkowanymi na sieć i platformy usługowe

SecureSphere chroni aplikacje webowe i związaną z nimi infrastrukturę poprzez wykrywanie aplikacji, usług webowych, serwerów i ataków sieciowych. Posiadając stale aktualizowane przez ośrodek Imperva ADC informacje na temat ponad 6500 sygnatur, SecureSphere umacnia zabezpieczenia wszystkich warstw aplikacji przed zagrożeniami płynącym z sieci.



### Spełnianie wymogów normy PCI 6.6

Zapora SecureSphere Web Application Firewall pomaga tysiącom przedsiębiorstw spełniać wymogi normy PCI 6.6

- » Zapewnia stałą zautomatyzowaną ochronę
- » Oferuje opcje predefiniowanego i konfigurowalnego raportowania, co służy spełnianiu wymogów norm
- » Stosuje system wirtualnych poprawek w celu zapewnienia kompleksowej ochrony
- » Spełnia wymogi normy PCI dotyczące audytowania i kontroli dostępu użytkownika dzięki opcjonalnej zaporce Database Firewall

## Ochrona protokołów HTTP i usług sieciowych XML

SecureSphere egzekwuje zgodność ze standardami HTTP w celu zapobiegania nadużyciom z wykorzystaniem tego protokołu i technikom omijania zabezpieczeń. Szczegółowe polityki pozwalają administratorom zachowywać ścisłą zgodność ze standardami RFC, bądź też zezwalać na niewielkie od nich odchylenia. Elastyczne, błyskawicznie aktualizowane systemy bezpieczeństwa pozwalają SecureSphere chronić aplikacje Web 2.0, XML i SOAP bez konieczności wprowadzania jakichkolwiek zmian w aplikacji.

## Szczegółowe polityki korelacji redukują przypadki fałszywych trafień

SecureSphere potrafi odróżniać ataki od niekonwencjonalnych, ale autoryzowanych zachowań poprzez korelację żądań dostępu do danego środowiska Web w czasie i pomiędzy warstwami. Taka skorelowana analiza ataku (Correlated Attack Validation) bada różnorakie atrybuty, takie jak zgodność z protokołem HTTP, naruszenia zbudowanego profilu, sygnatury, znaki specjalne czy reputacja użytkownika, w celu efektywnego ostrzeżenia przed atakami bądź całkowitego ich blokowania, przy zachowaniu najniższej w branży liczby fałszywych trafień.

## Konfigurowalne raportowanie służące zapewnieniu zgodności z normami i regulacjami, a także analizie śledczej

Bogate możliwości graficznego raportowania SecureSphere umożliwiają klientom łatwe zrozumienie statusu bezpieczeństwa i spełnienie wymogów norm i regulacji prawnych. SecureSphere zawiera funkcje zarówno predefiniowanego, jak i w pełni konfigurowalnego raportowania. Raporty dostępne są do wglądu na żądanie, bądź też wysyłane pocztą elektroniczną codziennie, raz w tygodniu lub raz w miesiącu.

## Monitoring służący kompleksowej analizie ataków

Ostrzeżenia mogą być w prosty sposób wyszukiwane, szeregowane i korelowane bezpośrednio z adekwatnymi regułami bezpieczeństwa. Funkcje monitorowania i raportowania SecureSphere zapewniają natychmiastowy wgląd w kwestie bezpieczeństwa, zgodności i udostępniania zawartości. Aktualizowana w czasie rzeczywistym baza gwarantuje wysoki poziom wglądu w status systemu i podejmowane działania dotyczące bezpieczeństwa.

## Wiodący na rynku system ochrony aplikacji webowych

Spośród wszystkich dostawców usług związanych z bezpieczeństwem kluczowych aplikacji webowych, to Imperva znalazła największe uznanie wśród różnorodnych przedsiębiorstw. Ze swoimi możliwościami wdrożenia typu drop-in i niewielkimi wymogami w kwestii nakładów na administrację systemem, SecureSphere zapewnia praktyczne i wysoce bezpieczne rozwiązanie, chroniące aplikacje webowe przed wszelakimi atakami sieciowymi.

## Dostępne opcje wdrożenia:

- » **Transparentne wdrożenie w warstwie drugiej:** wdrożenie typu drop-in i najlepsza w branży wydajność
- » **Reverse proxy i transparentne proxy:** modyfikacja zawartości poprzez przypisywanie plików cookie i przepisywanie URLów
- » **Monitorowanie w trybie non-inline:** monitoring i analiza śledcza o zerowym poziomie ryzyka
- » **Wysoka dostępność:** IMPVHA, VRRP, interfejsy fail-open, dostępne opcje redundancji, wdrożenie w trybie non-inline

## ThreatRadar:

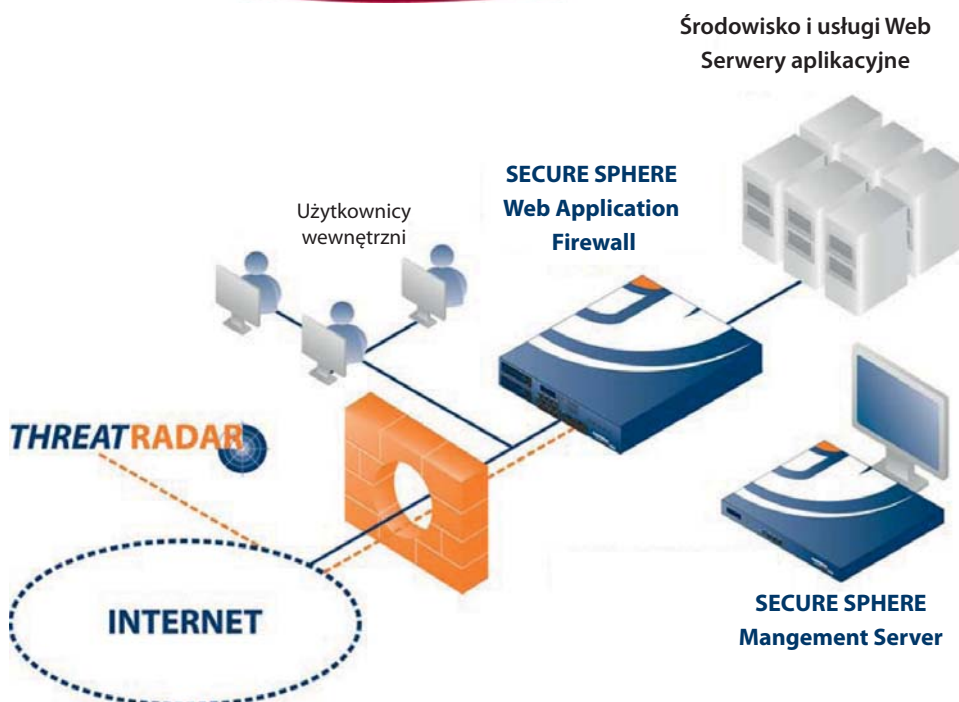
### Ochrona oparta na reputacji

- » Integracja informacji o wiarygodnych źródłach ataku z systemem bezpieczeństwa WAF
- » Zatrzymywanie intruzów zanim jeszcze zdążą zainicjować atak

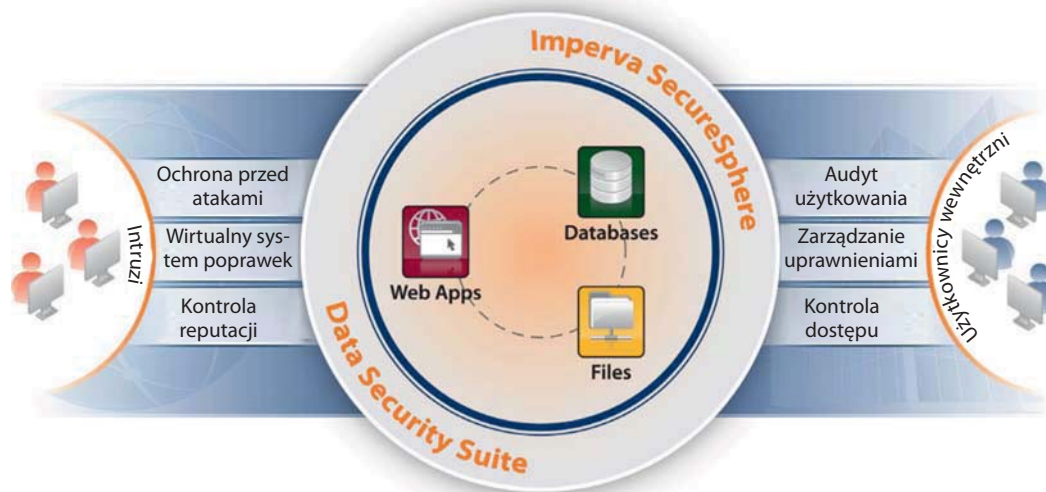
### Nieinwazyjne wdrożenie i najwyższy poziom wydajności



- » Urządzenia fizyczne: zapewniają wielogigabitową przepustowość przy opóźnieniach poniżej jednej milisekundy
- » Urządzenia wirtualne: zapewniają adaptowalny, niezawodny, prosty w obsłudze system bezpieczeństwa, rozwijający się wraz z Twoim biznesem



## Pakiet Imperva SecureSphere Security



Pakiet SecureSphere Data Security Suite jest wiodącym na rynku rozwiązaniem zapewniającym ochronę danych i zgodność z normami oraz regulacjami prawnymi. SecureSphere zabezpiecza kluczowe dane przed atakami i wewnętrznymi nadużyciami, zapewnia szybką i ekonomiczną drogę do pełnej zgodności z regulacjami i wdraża powtarzalny proces zarządzania ryzykiem.

### Rodzina Produkt SecureSphere

<b>Baza danych</b>	<p><b>Database Activity Monitoring</b> Pełna kontrola i wgląd w użytkowanie baz danych</p> <p><b>Database Firewall</b> Monitoring aktywności i ochrona w czasie rzeczywistym dla kluczowych baz danych</p> <p><b>Discovery and Assessment Server</b> Ocena słabych punktów, zarządzanie konfiguracją i klasyfikacja danych dla baz</p> <p><b>User Rights Management for Databases</b> Przegląd i zarządzanie prawami dostępu użytkownika do kluczowych baz danych</p> <p><b>ADC Insights</b> Predefiniowane opcje raportowania i reguły dla zgodności oraz bezpieczeństwa aplikacji SAP, Oracle EBS i PeopleSoft</p>
<b>Plik</b>	<p><b>File Activity Monitoring</b> Pełna kontrola i wgląd w użytkowanie danych z plików</p> <p><b>File Firewall</b> Monitoring aktywności i ochrona dla kluczowych plików</p> <p><b>User Rights Management for Files</b> Przegląd i zarządzanie prawami dostępu użytkownika do kluczowych plików</p>
<b>Środowisko Web</b>	<p><b>Web Application Firewall</b> Skuteczna, zautomatyzowana ochrona przeciwko zagrożeniom płynącym z sieci</p> <p><b>ThreatRadar</b> Pionierska w branży ochrona aplikacji webowych oparta na systemie reputacji</p>

## Imperva jest światowym liderem na rynku bezpieczeństwa danych

*Tysiące wiodących przedsiębiorstw, organizacji rządowych i usługodawców polegają na rozwiązaniach firmy Imperva zapobiegających nadużyciom danych, pomagających spełnić wymogi norm i regulacji prawnych, a także zarządzać ryzykiem.*



### Dystrybucja w Polsce:



CLICO Sp. z o.o.  
Budynek CC Oleandry  
30-063 Kraków  
ul. Oleandry 2  
tel. 12 378-37-00  
tel. 12 632-51-66  
tel. 12 292-75-22... 24  
fax 12 632-36-98  
e-mail: sales@clico.pl  
www.clico.pl

CLICO Oddział Katowice  
40-568 Katowice  
ul. Ligocka 103  
tel. 32 444-65-11  
tel. 32 203-92-35  
tel. 32 609-80-50...51  
fax 32 203-97-93  
e-mail: katowice@clico.pl

CLICO Oddział Warszawa  
Budynek Centrum Milenium  
03-738 Warszawa  
ul. Kijowska 1  
tel. 22 201-06-88  
tel. 22 518-02-70...75  
fax 22 518-02-73  
e-mail: warszawa@clico.pl

