



## Bezpieczeństwo baz danych

### Kontrola i ochrona kluczowych baz danych

*Najlepsze w swojej klasie produkty bezpieczeństwa baz danych  
Imperva SecureSphere:*

- » Kontrola dostępu do poufnych danych
- » Sygnalizowanie i blokowanie w czasie rzeczywistym ataków i nieautoryzowanych działań, których celem są bazy danych
- » Wykrywanie słabych punktów w architekturze baz danych i system wirtualnych poprawek
- » Identyfikowanie użytkowników posiadających zbyt duże uprawnienia oraz użytkowników nieaktywnych, jak również udostępnianie pełnego przeglądu praw dostępu
- » Przyspieszenie procesów reagowania na incydenty naruszenia bezpieczeństwa oraz procesów śledczych dzięki zastosowaniu zaawansowanych technik analitycznych



## Produkty

**SecureSphere Database Activity Monitoring**

**SecureSphere Database Firewall**

**SecureSphere Discovery and Assessment Server**

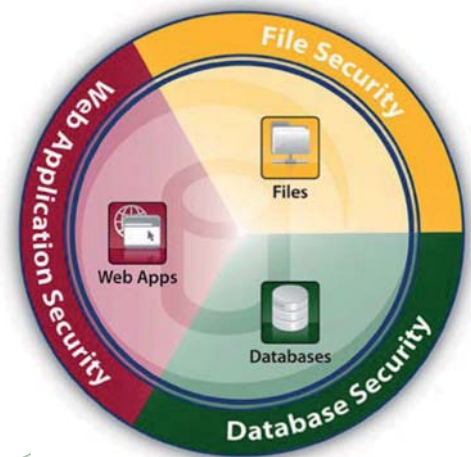
**User Rights Management for Databases**

**ADC Insights**

# Najlepsze w swojej klasie mechanizmy kontroli i ochrony

W bazach danych przechowywane są niezwykle cenne, poufne dane. Zwiększająca się liczba wytycznych dotyczących zgodności z regulacjami bezpieczeństwa zmusza organizacje do wprowadzania procesów kontroli dostępu do tych poufnych danych oraz do ochrony ich przed atakami i nadużyciami.

Wielokrotnie nagradzane produkty bezpieczeństwa baz danych Imperva SecureSphere automatyzują procesy kontroli baz danych i natychmiastowo identyfikują ataki, działania niepożądane oraz nadużycia. W połączeniu z produktami bezpieczeństwa aplikacji webowych oraz produktami bezpieczeństwa plików firmy Imperva, pakiet SecureSphere jest naturalnym wyborem w zabezpieczaniu poufnych danych biznesowych.



## Ciągła kontrola sposobów wykorzystania poufnych danych

SecureSphere 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” wykorzystuje. SecureSphere kontroluje użytkowników uprzywilejowanych, którzy uzyskują dostęp do serwera w sposób bezpośredni, jak również użytkowników nieuprzywilejowanych łączących się z serwerem za pośrednictwem różnych aplikacji. SecureSphere monitoruje również odpowiedzi baz danych w kontekście wycieku poufnych informacji oraz naruszeń bezpieczeństwa.

## Procesy analityczne w badaniu incydentów naruszenia bezpieczeństwa oraz analizie śledczej

SecureSphere zapewnia kompleksowy wgląd w działania dzięki zastosowaniu interaktywnych procesów analitycznych. Za pomocą intuicyjnego interfejsu użytkownika SecureSphere pozwala zespołom zajmującym się bezpieczeństwem oraz administratorom baz danych szybko przeglądać, analizować i korelować aktywność baz danych z praktycznie każdej perspektywy, bez potrzeby stosowania skryptów SQL. Interaktywne procesy analityczne upraszczają analizę śledczą i umożliwiają identyfikowanie trendów i wzorców mogących być oznakami istniejących zagrożeń.

## Wykrywanie nieautoryzowanego dostępu i nadużyć

SecureSphere identyfikuje standardowe modele uzyskiwania dostępu do danych przez użytkowników za pomocą oczekującej na opatentowanie technologii Dynamic Profiling. Ustala ona linię bazową wszelkiej aktywności użytkownika, w tym DML, DDL, DCL, aktywności read-only (SELECT) oraz wykorzystania procedur składowanych. SecureSphere wykrywa rozbieżności ze standardowym modelem pojawiające się w momencie wysyłania przez użytkowników nieoczekiwanych zapytań, a następnie sygnalizuje lub blokuje użytkowników naruszających politykę kontrolującą dostęp. Użytkownicy dokonujący nieautoryzowanych żądań SQL mogą ponadto zostać poddani kwarantannie do momentu, gdy posiadane przez nich prawa dostępu przejdą ponowną ocenę i uzyskają autoryzację.

## Blokowanie w czasie rzeczywistym ataków typu SQL Injection, DoS i innych

Selektywnie kontrolując dostęp do danych wrażliwych, SecureSphere monitoruje również w czasie rzeczywistym aktywność na bazach danych w celu wykrycia wycieku danych, nieautoryzowanych operacji SQL oraz ataków wykorzystujących podatności protokołów i systemów operacyjnych. SecureSphere może sygnalizować oraz opcjonalnie blokować złośliwe ataki, bez względu na to czy zapoczątkowane zostały one przez aplikację czy też uprzywilejowanego użytkownika, w sieci czy też na serwerze bazy danych.

## Egzekwowanie polityki, uproszczone mechanizmy raportowania zgodności z normami

SecureSphere zawiera kompletny zestaw predefiniowanych, edytowalnych reguł polityki bezpieczeństwa i kontroli. Dostępne „z pudełka” funkcje kontrolujące takie aplikacje biznesowe jak: SAP, Oracle EBS oraz PeopleSoft, jak również mechanizmy zapewniające zgodność z regulacjami SOX, PCI DSS oraz HIPAA, pozwalają zaoszczędzić czas przeznaczony na wdrożenie i spełnienie wymagań norm i regulacji. Alarmy bezpieczeństwa mogą być wysyłane do systemów SIEM, systemów ticketowych oraz rozwiązań firm trzecich, upraszczając w ten sposób procesy biznesowe.



## Spełnianie wymogów zgodności

SecureSphere pomaga organizacjom w wypełnieniu różnorodnych wymogów zgodności z regulacjami takimi jak: PCI DSS, SOX oraz HIPAA.

- » Spełnia 8 z 12 wymogów PCI, w tym sekcje 10, 7 oraz 8.5
- » Spełnia wymogi zgodności dotyczące nadzoru finansowego, w tym sekcje 302 i 404 regulacji SOX
- » Egzekwuje podział obowiązków
- » Zapewnia spójność danych dotyczących nadzoru
- » Wykrywa nieautoryzowany dostęp do danych finansowych oraz informacji o posiadaczach kart płatniczych
- » Udostępnia predefiniowane raporty upraszczające procesy spełniania norm zgodności

## Klasyfikowanie kontrolowanych danych w celu zapewnienia ochrony oraz zgodności z normami

Dzięki zastosowaniu automatycznych mechanizmów wykrywania i klasyfikacji poufnych danych SecureSphere wykrywa wszystkie systemy baz danych objęte projektami bezpieczeństwa i zgodności z normami. Połączenie mechanizmów wykrywania i klasyfikacji z oceną słabych punktów umożliwia organizacjom zwiększanie priorytetu działań mających na celu ich likwidowanie.

## Ocena słabych punktów i system wirtualnych poprawek w architekturze baz danych

Wykorzystując ponad tysiąc gotowych analiz słabych punktów w konfiguracji, bazach danych oraz platformie, SecureSphere pomaga organizacjom w ich identyfikacji i eliminacji. System wirtualnych poprawek SecureSphere może blokować próby wykorzystania wykrytych słabych punktów, zapewniając tym samym natychmiastową ochronę. 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 baz danych.

## Efektywne zarządzania prawami użytkowników dla wszystkich baz danych

SecureSphere automatycznie gromadzi informacje na temat praw użytkowników dla heterogenicznych baz danych. Dzięki systemowi zarządzania prawami użytkowników, organizacje mogą korzystać z automatycznego procesu ich przeglądania, identyfikacji użytkowników posiadających zbyt duże uprawnienia oraz wykazywania zgodności z regulacjami takimi jak: SOX, PCI 7 oraz PCI 8.5.

## Kontrola lokalna i ochrona baz danych z wykorzystaniem aplikacji agentów

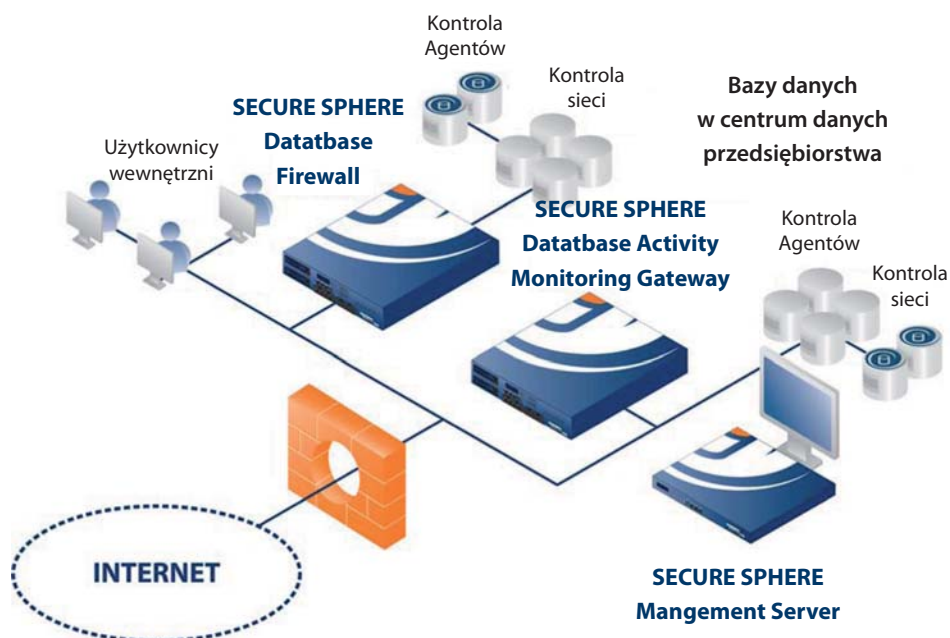
Aby zapewnić kompletną widoczność oraz kontrolę wszelkiej aktywności użytkownika SecureSphere rozszerza swoje funkcje monitorujące, nadzorujące i egzekwujące o serwery hosta. Aplikacje agentów SecureSphere nadzorują aktywność baz danych i zabezpieczają poufne dane przy minimalnym wpływie na wydajność serwera.

# Nieźródne standardy bezpieczeństwa danych oraz zgodności z normami

Dzięki zastosowaniu wiodących rozwiązań kontrolowania baz danych oraz zapewniania ochrony w czasie rzeczywistym SecureSphere obejmuje wszystkie aspekty bezpieczeństwa baz danych oraz zgodności z normami bez negatywnego wpływu na ich wydajność lub dostępność. Dzięki wielowarstwowej architekturze SecureSphere stanowi skalowalne rozwiązanie, które może zostać dostosowane do najbardziej skomplikowanych systemów baz danych. Biorąc pod uwagę zautomatyzowane procesy bezpieczeństwa i zgodności z normami, nie jest niespodzianką, że tysiące organizacji wybiera Imperva SecureSphere, aby chronić swoje najcenniejsze zasoby.

## Wdrożenie

- » **Monitorowanie sieci w trybie non-inline:** Monitorowanie aktywności bez wpływu na wydajność i dostępność bazy danych
- » **Przejrzysta ochrona w trybie inline:** Wdrożenie typu drop-in oraz wysokie parametry wydajność
- » **Monitorowanie za pośrednictwem agenta:** Lekki agent w postaci oprogramowania monitorującego bezpośrednio uprzywilejowaną aktywność oraz ruch sieciowy
- » **Gromadzenie logów:** Wykorzystanie plików z logami baz danych firm trzecich dla zastosowania heterogenicznych procesów analitycznych, ostrzeżeń oraz mechanizmów raportowania
- » **Obsługiwane platformy baz danych:** Oracle, Microsoft SQL, IBM DB2 (w tym DB2 dla z/OS i DB2/400), Informix, Sybase, MySQL, Teradata, oraz Netezza

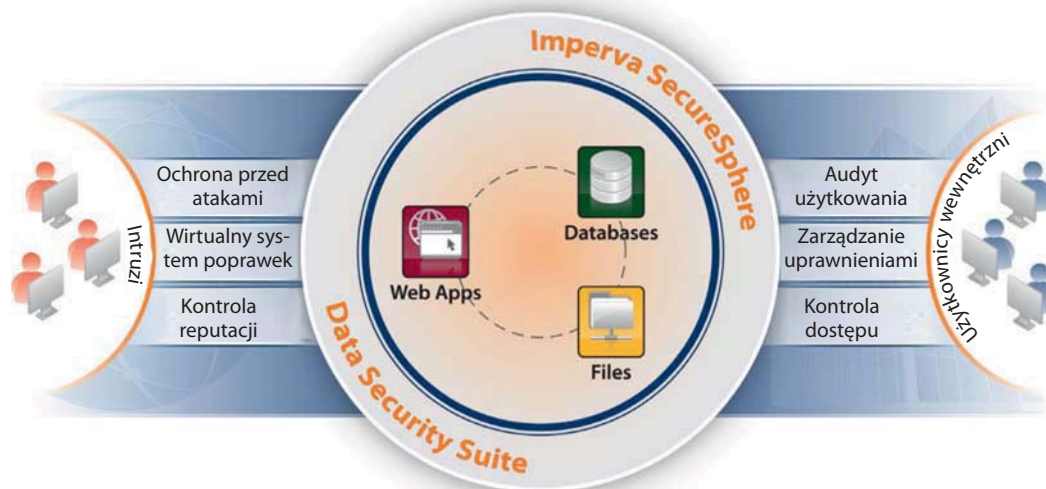


## Nieinwazyjne wdrożenie i ultra wysoka wydajność



- » **Urządzenia fizyczne:** Zapewniają wielogigabitową wydajność i opóźnienia poniżej jednej milisekundy
- » **Urządzenia wirtualne:** Zapewniają adaptacyjny, niezawodny i prosty w obsłudze system bezpieczeństwa

## 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 hakerskimi 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.*

SAP<sup>®</sup> Certified Integration



### 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

