



Bezpieczeństwo plików

Kontrola i ochrona kluczowych plików

Najnowocześniejsze produkty bezpieczeństwa plików Imperva SecureSphere:

- » Kontrola dostępu do plików zapewniająca bezpieczeństwo, zgodność z normami oraz efektywność procesów IT
- » Identyfikowanie użytkowników posiadających zbyt duże uprawnienia oraz udostępnianie kompleksowego przeglądu praw dostępu do plików
- » Sygnalizowanie lub blokowanie żądań dostępu naruszających politykę korporacyjną dotyczącą bezpieczeństwa plików
- » Mapowanie plików do właścicieli danych
- » Zgodność z normami i reagowanie na incydenty bezpieczeństwa oraz zaawansowane narzędzia analityczne i raportowania

Produkty

SecureSphere File Activity Monitoring

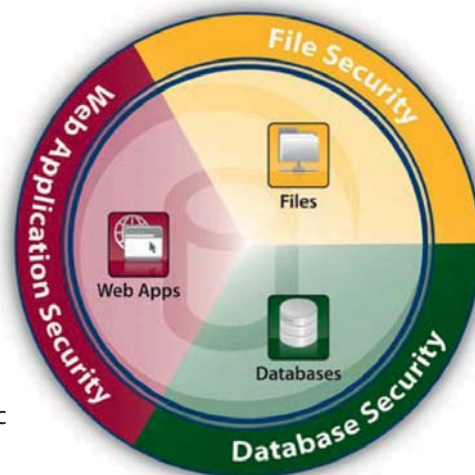
SecureSphere File Firewall

User Rights Management for Files

Wiodące mechanizmy kontroli i ochrony plików

Konwencjonalne podejście do kontroli plików i zarządzania prawami dostępu nie spełnia oczekiwań większości organizacji. Narzędzia administracyjne firm trzecich i inne powszechnie wykorzystywane rozwiązania, takie jak grupy usług katalogowych oraz mechanizmy nadzorowania plików wbudowane w systemy operacyjne, nie nadążają za zmianami organizacyjnymi lub nie są w stanie poradzić sobie z objętością i przyrostem niestrukturalnych danych.

Produkty bezpieczeństwa plików Imperva SecureSphere zapewniają mechanizmy monitorowania i kontrolowania plików, procesy bezpieczeństwa oraz zarządzania prawami użytkowników dla plików przechowywanych na serwerach oraz sieciowych pamięciach masowych (NAS). SecureSphere kontroluje wszystkie ścieżki dostępu do plików w celu ustalenia, kto jest ich właścicielem i kto z nich korzysta. Zabezpiecza poufne pliki danych, sygnalizując lub opcjonalnie blokując nieautoryzowany dostęp. Przyspiesza procesy śledcze poprzez zastosowanie przejrzystych i adekwatnych mechanizmów raportujących i analitycznych. Co więcej, w przeciwieństwie do wbudowanych rozwiązań kontrolujących, SecureSphere nadzoruje dostęp do plików, nie wpływając przy tym na wydajność serwera plików.



Kontrola dostępu do plików bez negatywnego wpływu na kluczowe systemy

SecureSphere nieustannie monitoruje i kontroluje w czasie rzeczywistym wszystkie operacje wykonywane na plikach, nie ograniczając przy tym wydajności i dostępności serwera plików. SecureSphere udostępnia szczegółowe informacje dotyczące nazwy użytkownika, pliku do którego uzyskiwany jest dostęp, folderu macierzystego, czasu dostępu, operacji wykonanej i innych. Aby zapewnić podział obowiązków informacje te przechowywane są w zewnętrznym, zabezpieczonym repozytorium i udostępniane poprzez widok „tylko do odczytu” na podstawie opartego na rolach mechanizmu dostępowego.

Kontrola praw dostępu użytkownika do poufnych plików

SecureSphere identyfikuje prawa dostępu użytkownika i ułatwia kompleksową ich ocenę w celu upewnienia się, że dostęp uzyskiwany do poufnych plików posiada podstawę biznesową. Upraszcza kontrolę konsolidując i raportując prawa dostępowe użytkowników dla wszystkich serwerów plików i urządzeń NAS. SecureSphere przyspiesza cykl oceny praw dostępu poprzez:

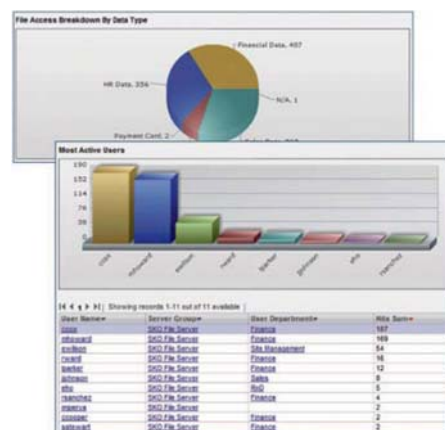
- » Identyfikowanie użytkowników posiadających dostęp do poufnych danych objętych podwyższonym ryzykiem
- » Oznaczanie użytkowników posiadających zbyt duże uprawnienia dostępowe
- » Wykrywanie użytkowników nieaktywnych i niewykorzystywanych praw dostępu
- » Zapewnienie narzędzi organizujących przegląd praw dostępu

Sygnalizowanie lub blokowanie w czasie rzeczywistym aktywności odbiegającej od przyjętego modelu

SecureSphere File Firewall zapewnia ochronę plików poprzez blokowanie lub sygnalizowanie dostępu, który odbiega od polityki korporacyjnej. Bazując na regułach polityki, mechanizmy blokujące umożliwiają administratorom przeciwdziałanie błędom pojawiającym się na poziomie list kontroli dostępu. Elastyczny szablon tworzenia reguł umożliwia ich definiowanie, biorąc pod uwagę szereg kryteriów, takich jak metadane plików, kontekst organizacyjny, aktywność dostępową oraz klasyfikację danych, a następnie podejmują działania, gdy zaobserwowane zostaną niepożądane zachowania.

Identyfikowanie właścicieli danych przy zarządzaniu polityką

SecureSphere identyfikuje właścicieli danych poprzez analizę wykorzystania plików i folderów. Identyfikowanie właścicieli danych ma kluczowe znaczenie dla zgodności z normami bezpieczeństwa oraz procesów IT, ponieważ znają oni znaczenie swoich danych dla procesów biznesowych oraz wiedzą jak powinny być one zarządzane i chronione.



Zgodność z normami PCI, SOX oraz HIPAA

SecureSphere pomaga organizacjom w wypełnieniu różnorodnych wymogów zgodności z regulacjami, w tym 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
- » Spełnia wymogi sekcji 160.103 oraz 164.312(b) normy HIPAA
- » Egzekwuje podział obowiązków
- » Zapewnia spójność danych dotyczących kontroli
- » Wykrywa nieautoryzowany dostęp do danych finansowych oraz informacji dotyczących posiadaczy kart płatniczych
- » Udostępnia predefiniowane raporty upraszczające procesy spełniania norm

Reagowanie na incydenty naruszające bezpieczeństwo i ich analiza

SecureSphere zapewnia interaktywne mechanizmy analityczne, które za pomocą kilku kliknięć pozwalają zobrazować aktywność na plikach danych oraz prawa dostępowe użytkowników. Personel odpowiedzialny za bezpieczeństwo, zgodność z normami oraz nadzór może wykorzystać powyższe narzędzia analityczne w celu identyfikowania trendów, wzorców oraz ryzyka związanego z aktywnością na plikach oraz prawami użytkowników. Interaktywne narzędzia analityczne pozwalają uprościć procesy śledcze i precyzyjnie wskazać incydenty naruszające bezpieczeństwo.

Szybkie i efektywne udokumentowanie zgodności z normami za pomocą raportów graficznych

SecureSphere udostępnia bogate funkcje graficznego raportowania umożliwiające firmom ocenę ryzyka oraz udokumentowanie zgodności z normami, takimi jak: SOX, PCI, HIPAA oraz innymi prawami dotyczącymi ochrony danych. Raporty mogą być udostępniane na żądanie lub planowane i rozpowszechniane w regularnych odstępach czasu.

Interfejs udostępniający dane w czasie rzeczywistym zapewnia kompleksowy wgląd w zdarzenia naruszające bezpieczeństwo. Platforma raportująca SecureSphere w natychmiastowy sposób obrazuje dane istotne z punktu widzenia bezpieczeństwa, zgodności z normami oraz zarządzania prawami dostępu.

Wzrost efektywności procesów IT

SecureSphere pozwala na wydajniejszą pracę administratorom zajmującym się systemem Windows, przechowywaniem danych oraz usługami katalogowymi. Monitorowanie aktywności plików umożliwia:

- » Udzielanie praw dostępu przy wykorzystaniu aktualnego i precyzyjnego przeglądu właścicieli danych oraz udzielonych pozwoleń
- » Identyfikowanie plików, które od dłuższego czasu nie były wykorzystywane
- » Przyspieszanie migracji danych oraz konsolidacji domen usług katalogowych w oparciu o informacje dotyczące właścicieli danych, kont nieaktywnych oraz niewykorzystywanych danych
- » Upraszczenie przeglądu praw użytkowników podczas migracji i konsolidacji projektów

Zaufaj liderowi w dziedzinie bezpieczeństwa danych

SecureSphere oferuje najlepsze w swojej klasie standardy kontroli plików i zarządzania prawami użytkowników, które poprawiają zgodność z normami, ulepszają system bezpieczeństwa oraz upraszczają procesy operacyjne w sferze IT. Wykorzystując potężną, scentralizowaną platformę zarządzania i raportowania, SecureSphere może sprostać wymaganiom jakiegokolwiek środowiska – od małej organizacji wykorzystującej pojedynczy serwer plików, po duże przedsiębiorstwo posiadające centra danych w różnych lokalizacjach geograficznych. SecureSphere zapewnia niezrównane bezpieczeństwo danych, chroniąc aplikacje webowe, bazy danych oraz pliki.

Elastyczne tryby wdrożenia inline oraz non-inline umożliwiają prostą instalację bez potrzeby wprowadzania zmian w serwerach plików, systemach NAS, aplikacjach oraz w sieci

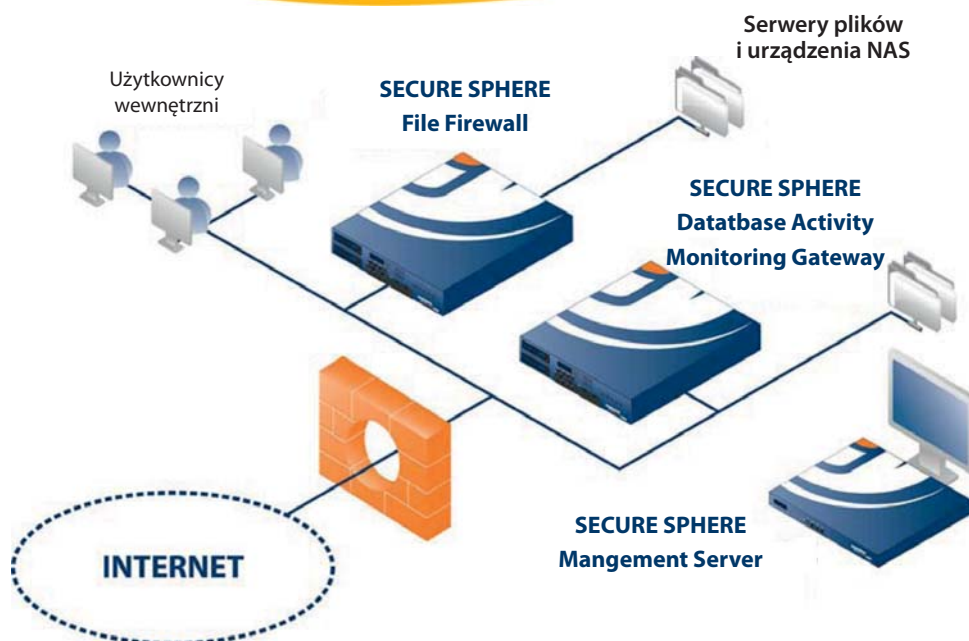
Wdrożenie

- » **Monitorowanie sieci w trybie non-inline:** Monitorowanie aktywności bez wpływu na wydajność i dostępność bazy danych
- » **Przejrzysta ochrona inline:** Wdrożenie typu drop-in oraz wysokie parametry wydajności

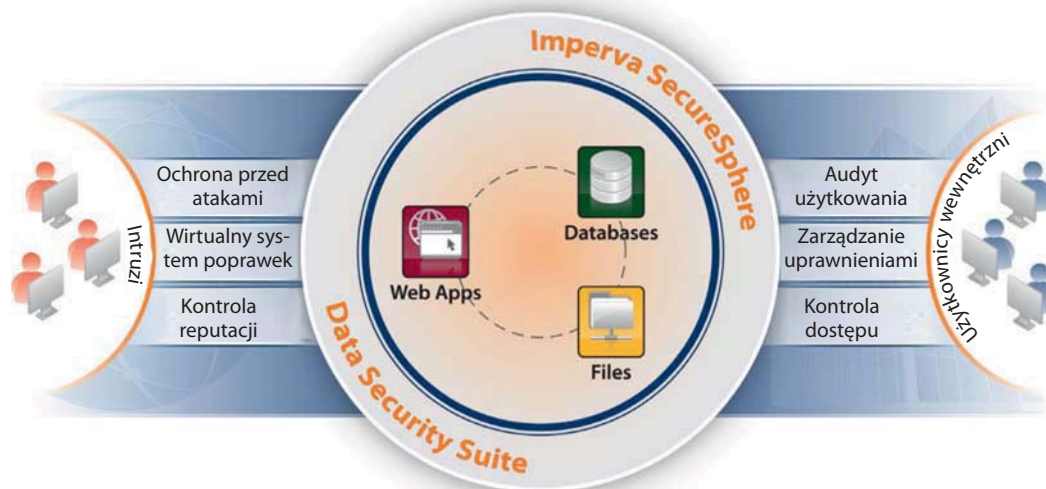
Nieinwazyjne wdrożenie i wysoka wydajność



- » **Urządzenia fizyczne:** Zapewniają wielogigabitową wydajność i obsługę tysięcy użytkowników
- » **Urządzenia wirtualne:** Zapewniają adaptacyjny, niezawodny i 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

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

