IMPERVA®

Imperva Skyfence Cloud Gateway

SPECYFIKACJA PRODUKTU

Produkty

- Cloud Discovery Free
- Cloud Discovery & Governance
- Cloud Audit & Protection
- Cloud Security Suite

Imperva Skyfence Cloud Gateway zapewnia widoczność i kontrolę nad wykorzystaniem aplikacji w chmurze. Automatycznie wykrywa użycie aplikacji w chmurze, analizuje ryzyko i wymusza odpowiednie kontrole dla aplikacji SaaS oraz produkcyjnych. Dzięki Skyfence użytkownicy otrzymują aplikacje, które chcą, a personel działu IT zapewnia im ochronę, której potrzebują.

Wstęp

Aplikacje w chmurze pozwalają firmom na zmniejszenie kosztów i elastyczne przydzielanie zasobów, ale wprowadzają zagrożenie dla ich bezpieczeństwa i postawy zgodności. Trend na stosowanie własnych aplikacji w chmurze stworzył martwy punkt, który nie jest uwzględniony w tradycyjnych kontrolach brzegowych i końcowych. Dział IT ma niewielki lub zerowy wgląd w to, które aplikacje są używane, kto ma dostęp do jakich informacji i kto wykonuje uprzywilejowane działania. Nie są w stanie ocenić ryzyka związanego z każdą aplikacją w chmurze i egzekwować niezbędnych polityk i mechanizmów kontroli. Ponadto wiele przedsiębiorstw wdraża poprzez firmy zewnętrzne aplikacje produkcyjne dla swoich klientów i partnerów, którzy coraz częściej stają się ofiarami przejęcia kont z powodu zagrożonych lub wykradzionych danych uwierzytelniających.

Skyfence zapewnia przejrzystość i kontrolę dla wszystkich użytkowników, punktów końcowych oraz aplikacji, tak aby korzystanie z aplikacji w chmurze było bezpieczne i wydajne.

Zalety Skyfence

- Część rodziny systemów cyberbezpieczeństwa firmy Imperva, które obejmują środowisko w siedzibie klienta oraz w chmurze
- Kompleksowe odkrywanie aplikacji, zarządzanie, analiza i ochrona w jednym zintegrowanym rozwiązaniu
- Elastyczność wdrażania przy pomocy urządzeń, urządzeń wirtualnych, usług wykonywanych w oparciu o chmurę lub usług zarządzanych
- Szczegółowe polityki dla urządzeń przenośnych i punktów końcowych umożliwiają kontrolę dostępu i ochronę danych dla zarządzanych i niezarządzanych telefonów komórkowych, tabletów i laptopów
- Wbudowana integracja z katalogami przedsiębiorstw 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

Zmniejszanie ryzyka dla aplikacji w chmurze

Zazwyczaj organizacje wymagają widzialności w dostępie do chmury przed wdrożeniem polityk dla wyeliminowania lub zminimalizowania ryzyka. Dlatego ważne jest, żeby mieć zestaw funkcji w trybie offline, które pomogą Państwu rozpoznać i ocenić swoją postawę ryzyka. Po ustaleniu krajobrazu zagrożenia i stworzeniu wymaganych polityk, możecie Państwo skorzystać ze zgodnych rozwiązań, żeby faktycznie wdrożyć wspomniane polityki. Even Gartner zaleca rozwiązania, które oferują "to co najlepsze z obu światów," np., połączenie proxy i API[1].

Pracownicy firm, użytkownicy telefonów komórkowych i hakerzy

obsługiwane wdrożenia wewnętrzne i w trybie offline

Aplikacje w chmurze

Twoje aplikacje w chmurze — poznane, zrozumiane i chronione.

[1] Gartner, Inc., "Technology Overview for Cloud Access Security Broker," May 19, 2015.

Rozwiązania dla Twojego biznesu

Przedsiębiorstwa

- Odkrywanie aplikacji i ocena ryzyka
- Kontrola urządzeń mobilnych i punktów końcowych
- Zapobieganie wyciekowi danych
- Integracja SIEM w chmurze
- Monitorowanie uprzywilejowanych użytkowników
- Zapobieganie cyber-zagrożeniom i ochrona przed kradzieżą danych dostępu

Produkcyjne aplikacje webowe

- Przejęcia kont
- Audyty aktywności

IMPERVA® SKYFENCE

Wiedz, co tam jest: Cloud Discovery and Governance

Korzystając ze Skyfence Cloud Discovery od samego początku, możecie Państwo automatycznie wykrywać aplikacje działające w chmurze poprzez analizę danych zaimportowanych z plików dziennika, niezależnie od tego czy są one zatwierdzone przez dział IT czy nie. Rozwiązanie to zawiera także skany dostępów użytkowników z serwerów proxy i zapory sieciowej, aby zapewnić globalne i lokalne widoki na to, które aplikacje są używane i jak często. Raport Cloud Discovery zapewnia szczegółowy profil ryzyka dla każdej aplikacji, dzięki czemu możecie Państwo określić odpowiednie dla swojej organizacji polityki.

Skyfence rozszerza tradycyjne informacje o odkrywaniu aplikacji w chmurze poprzez dostarczanie szczegółów na temat czynników ryzyka, które są unikalne dla Państwa organizacji. Przykładowo, Skyfence zapewnia wgląd w nieaktywne konta (np. możecie Państwo płacić za licencje, które nawet nie są używane), porzucone konta (np. byli pracownicy wciąż mają dostęp do Państwa aplikacji w chmurze) i konta zewnętrzne (np. partnerów lub dostawców), które stanowią różne zagrożenia dla bezpieczeństwa.

Dodatkowo Skyfence przetestuje obecne ustawienia dotyczące bezpieczeństwa w Państwa organizacji zgodnie z najwyższymi obowiązującymi obecnie normami, dzięki czemu będziecie mogli łatwiej znaleźć luki w systemach bezpieczeństwa i zgodności oraz podjąć natychmiastowe działania w celu rozwiązania problemów.

Wszystkie funkcjonalności Cloud Discovery & Governance są dostępne poprzez interfejs API dostawcy aplikacji w chmurze, tj. jest to proces w trybie offline, który jest nieinwazyjny i nie wymaga żadnych pośredników, zmian w aplikacji lub wysyłania logów do Skyfence.

Zrób coś z tym: Cloud Audit and Protection

Skyfence Cloud Audit and Protection dostarcza analizę operacyjną i narzędzia, których potrzebujecie Państwo do ochrony swoich danych w chmurze. Skyfence zapewnia krytyczny wgląd i analizę w:

- **Zapobieganie wyciekowi danych:** Kto, co, kiedy i jak często udostępniał, wgrywał, przeglądał i modyfikował
- **Monitorowanie uprzywilejowanych użytkowników:** W tym dostęp do danych, konfigurację i zmiany w uprawnieniach użytkowników
- **Aktywność API:** Dane aplikacji i usług w chmurze dostępne za pośrednictwem interfejsu API

Skyfence posiada wbudowane adaptery, które ułatwiają integrację z katalogami przedsiębiorstw i wiodącymi rozwiązaniami SIEM, w tym ArcSight, Splunk i Q1 Labs.

Skyfence monitoruje i kontroluje wgrywanie, pobieranie i udostępnianie danych wrażliwych na podstawie różnych kryteriów (np. na podstawie miejsca przeznaczenia, użytkownika, aplikacji w chmurze). Skyfence sprawdza pliki i treści w czasie rzeczywistym, aby zapewnić bezpieczeństwo Państwa PII, PCI, HIPAA i innym wrażliwym informacjom. Skyfence oferuje wbudowaną ochronę przed wyciekiem danych (DLP) lub standardową integrację opartą na ICAP z wiodącymi rozwiązaniami DLP takimi jak Websense, aby można było wykorzystać istniejące polityki w zakresie ochrony danych.

Skyfence automatycznie wykrywa i blokuje zagrożenia dla aplikacji w chmurze i egzekwuje polityki ograniczania ryzyka. Innowacyjna technologia Dynamic User and Device Fingerprinting™ szybko ustanawia szczegółowe profile behawioralne oparte na normalnych wzorcach użytkowania dla każdego użytkownika, działu i urządzenia. Każda próba dostępu, która nie przejdzie testu linii papilarnych może zostać tak skonfigurowana, żeby natychmiastowo ostrzegać, blokować lub wymagać dwuskładnikowej identyfikacji w czasie rzeczywistym. Dzięki intuicyjnemu edytorowi polityk możecie Państwo szybko zdefiniować niestandardowe, szczegółowe polityki i egzekwować je w nieograniczonej liczbie aplikacji w chmurze.

Skyfence pozwala zablokować lub ograniczyć użytkowanie aplikacji w chmurze z punktów końcowych, które nie są zarządzane przez platformę Mobile Device Management (MDM). Rozwiązanie to zwiększa udział w MDM i stanowi tańszą alternatywę dla routingu wszystkich zdalnych dostępów do aplikacji w chmurze za pośrednictwem VPN-a.

Imperva Skyfence Cloud Gateway — Porównanie Funkcji Produktu

		PRODUKTY SKYFENCE			
GRUPA FUNKCJI	**OPIS FUNKCJI**	***CLOUD DISCOVERY FREE**	**CLOUD DISCOVERY & GOVERNANCE**	**CLOUD AUDIT & PROTECTION**	**CLOUD SECURITY SUITE**
Widoczność aplikacji i ocena ryzyka (dostępne w trybie offline/ poprzez API)	CLOUD APP DISCOVERY—Wykorzystuje istniejące pliki dziennika do automatycznego odkrywania i kategoryzowania wszystkich aplikacji używanych w chmurze	●	●		●
	CLOUD APP RISK SCORING—Ocenia ogólne ryzyko dla każdej aplikacji w chmurze na podstawie certyfikatów regulacyjnych i branżowych oraz najlepszych praktyk	●	●		●
	CLOUD APP USAGE SUMMARY—Zawiera liczbę użytkowników, aktywności, natężenie ruchu i typowe godziny użytkowania dla każdej aplikacji w chmurze	●	●		●
	ADVANCED RISK METRICS—Szczegółowe wskaźniki postawy ryzyka aplikacji w chmurze z konfigurowalnymi wyważeniami parametrów	●	●		●
	CUSTOMIZABLE RISK METRICS—Szczegółowe wskaźniki postawy ryzyka aplikacji w chmurze i informacje dla każdej aplikacji		●		●
	CONTINUOUS DISCOVERY—Planuje zautomatyzowane skanowanie plików dziennika i okresowo generuje raporty odkrywania		●		●
	CENTRALIZED DISOVERY DASHBOARD—Połączone wyniki odkrywania, obecne użycie wyjściowe wobec wcześniejszej aktywności i tendencji w użytkowaniu		●		●
	SIEM INTEGRATION—Generuje dane odkrywania w formacie Common Event Format do integracji z istniejącymi środowiskami SIEM		●		●
	APP CATALOG & RISK UPDATES—Automatycznie aktualizuje do katalogu aplikacji w chmurze i dokonuje zmian we właściwościach ryzyka, które są dostępne		●		●
	ACTIVITY LOG COLLECTIONS—Zbiera podstawowe dzienniki działań użytkowników i użytkowników uprzywilejowanych za pośrednictwem API dla aplikacji w chmurze		●		●
Zarządzanie aplikacją i użytkownikiem (dostępne w trybie offline/ poprzez API)	USER ENTITLEMENTS REVIEW—identyfikuje uśpione (np. nieaktywne) konta, porzucone konta (np. byłych pracowników) i użytkowników zewnętrznych (np. dostawców) w celu zmniejszenia kosztów operacyjnych i zminimalizowania powiązanych		●		●
	APP SECURITY ASSESSMENT—przeprowadza analizę porównawczą ustawień bezpieczeństwa Państwa aplikacji w chmurze pod kątem zestawu najlepszych praktyk branżowych i wymogów regulacyjnych (np. PCI DSS, NIST, HIPAA, MAS, ISO) w celu rozpoznania luk w systemach bezpieczeństwa i zgodności		●		●
	INTEGRATED REMEDIATION WORKFLOW—Wykorzystuje wbudowany obieg organizacyjny do przydzielania i wykonywania zadań związanych z ograniczeniem ryzyka poprzez Skyfence lub poprzez integrację z systemami biletowymi innych firm		●		●
Zarządzanie aplikacją i użytkownikiem (dostępne w trybie offline/ poprzez API)	ACTIVITY MONITORING & ANALYTICS—Monitorowanie aktywności w czasie rzeczywistym i analiza na podstawie użytkowników, grup, lokalizacji, urządzenia, działania aplikacji i innych			●	●
	PRIVILEGED USER MONITORING—Monitorowanie i raportowanie aktywności uprzywilejowanych użytkowników i administratorów w czasie rzeczywistym			●	●
	ENTERPRISE SIEM INTEGRATION—adaptery do bezpośredniego dostarczania dzienników aktywności do wiodących rozwiązań SIEM, w tym ArcSight, Splunk, i Q1 Labs			●	●
	ENTERPRISE DIRECTORY INTEGRATION—Wykorzystuje istniejącą infrastrukturę AD lub katalogu LDAP dla użytkownika, grupy oraz raportowania organizacyjnego i polityki			●	●
	ROLE-BASED ADMINISTRATION—Określa uprawnienia administracyjne do edycji zasobów, polityk i ustawień systemowych			●	●
	ENTERPRISE REPORTING—Elastyczne opcje raportowania, w tym uprzednio zdefiniowane raporty z możliwością edycji i zapisu niestandardowych raportów			●	●
Kontrola dostępu i ochrona danych (dostępny wewnętrznie/ poprzez proxy)	AUTOMATIC ANOMALY DETECTION—Stale monitoruje zachowanie i wykrywa nietypowe aktywności, w tym poufnych działań wysokiego ryzyka i ataki z zewnątrz			●	●
	REAL-TIME THREAT PREVENTION—Stosuje polityki do profilu, bloku lub wymaga weryfikacji tożsamości dla każdej aplikacji lub konkretnej akcji w ramach aplikacji			●	●
	DATA LEAK PREVENTION—Klasyfikacja danych dla ponad 100 typów plików i setek zdefiniowanych uprzednio typów danych, które spełniają wymagania szeregu regulacji (np. PCI, PII, PHI, HIPAA, SOX)			●	●
	MULTI-FACTOR AUTHENTICATION—Wbudowane funkcje, które mogą być egzekwowane w skali globalnej w oparciu o rodzaj punktu końcowego lub lokalizacji, lub zautomatyzowane w odpowiedzi na naruszenie polityk			●	●
	SINGLE SIGN-ON—Wykorzystuje wbudowane rozwiązania SSO lub innych firm, aby uzyskać dostęp do aplikacji opartych na SAML			●	●
	DYNAMIC ALERTS—W czasie rzeczywistym otrzymuje powiadomienia o wszelkich naruszeniach polityk lub progu aktywności za pośrednictwem SMS-a lub wiadomości e-mail			●	●
	MOBILE & ENDPOINT ACCESS CONTROL—Umożliwia stosowanie unikalnych polityk dla urządzeń zarządzanych i niezarządzanych, czy pochodzących z przeglądarek lub bogatych aplikacji mobilnych			●	●
	LOCATION-BASED ACCESS CONTROLS—Ogranicza dostęp w zależności od lokalizacji użytkownika lub lokalizacji usługi w chmurze			●	●
	MDM INTEGRATION—Wykorzystuje istniejące wdrożenie MDM do zarządzania zapisami punktów końcowych i dostępem do chmury			●	●
	CUSTOM POLICIES—Wizualny edytor polityk umożliwia łatwą konfigurację niestandardowych polityk na podstawie różnych atrybutów			●	●
	PRODUCTION APPLICATION PROTECTION—Zapobiega przejęciu konta i innym zagrożeniom związanym z kontami dla aplikacji zorientowanych na klienta			●	●
Zaawansowana Architektura Chmury	PERFORMANCE OPTIMIZATION—Przyspiesza dostęp do aplikacji w chmurze poprzez techniki inteligentnego ukrywania i optymalizacji zawartości			●	●
	DDOS PROTECTION—Kompleksowa ochrona przed wszystkimi atakami DDoS, opartymi na aplikacjach, sieci lub protokołach			●	●
	GLOBAL CDN—Część światowej klasy sieci dostarczania zawartości, która składa się z ponad 25 centrów danych na całym świecie, zapewniając pełną akcelerację strony			●	●

*Niezależna, lokalnie uruchamiana usługa dla systemów Mac oraz Windows