Ochrona danych będących fundamentem działalności firm

IBM Security Guardium pomaga w zapewnieniu kompleksowego bezpieczeństwa danych poprzez analizę, ochronę i gotowość do adaptacji

Najważniejsze informacje

- Umożliwia wdrożenie proaktywnej, holistycznej strategii ochrony newralgicznych danych na wszelkiego typu platformach, w tym w relacyjnych bazach danych, środowiskach Hadoop, NoSQL, w plikach i w chmurze.
- Przyczynia się do obniżenia całkowitych kosztów użytkowania, automatycznie wykrywając dane, które wymagają szczególnej ochrony, proaktywnie ujawniając czynniki ryzyka i podejmując odpowiednie działania.
- Chroni dane wrażliwe przed zagrożeniami wewnętrznymi i zewnętrznymi przy zastosowaniu takich technik, jak szyfrowanie, maskowanie, monitorowanie aktywności, dynamiczne blokowanie, alarmowanie, obejmowanie kwarantanną, identyfikowanie anomalii w zachowaniu użytkwników.
- Automatyzuje egzekwowanie reguł bezpieczeństwa danych i dostarcza właściwe raporty właściwym osobom we właściwym czasie.
- Daje się łatwo dopasować do zmian w otoczeniu informatycznym i wspiera wszystkie aspekty i etapy ochrony danych.

Naruszenia bezpieczeństwa danych zdarzają się dziś częściej niż kiedykolwiek w przeszłości – i niosą ze sobą poważniejsze skutki finansowe. Z badań prowadzonych na całym świecie wynika, że średni koszt naruszenia bezpieczeństwa danych wynosi obecnie 3,8 miliona USD.[1] Co więcej, ujawnienie tajemnic handlowych, projektów produktów lub innych przedmiotów własności intelektualnej może sprowadzić na firmę katastrofę finansową. Ze względu na swoją wartość dane podlegające szczególnej ochronie odgrywają kluczową rolę w działalności gospodarczej, a przez to są także atrakcyjnym celem ataku.

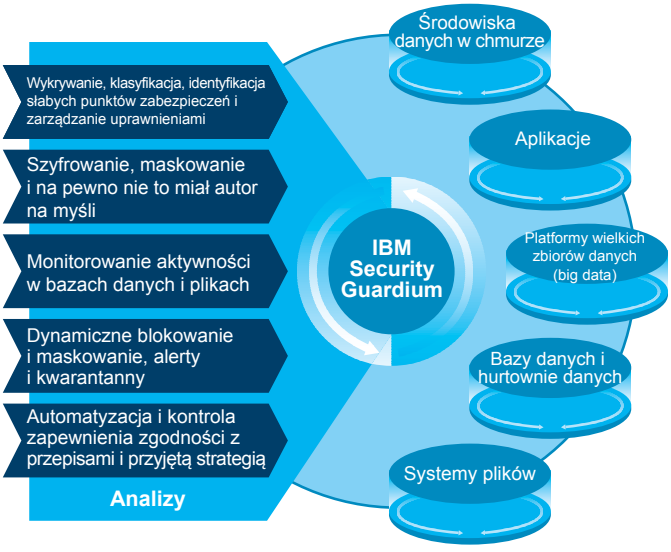
Tradycyjne podejście organizacji do ochrony informacji koncentruje się na zabezpieczeniu w obrębie swojego środowiska IT. Jednak standardowe narzędzia, takie jak programy antywirusowe i firewalle, nie są należycie przygotowane na współczesne zaawansowane zagrożenia. W dodatku dane wciąż się zmieniają, stale są w ruchu i nieustannie ich przybywa, dlatego zabezpieczenia muszą za nimi nadążać. Coraz większa liczba użytkowników, aplikacji i systemów musi mieć natychmiastowy dostęp do różnego rodzaju danych wrażliwych – przechowywanych w bazach danych, hurtowniach danych, plikach, platformach wielkich zbiorów danych (big data), środowiskach w chmurze i nie tylko, a także replikowanych do takich środowisk. Zapewnienie kontroli nad dostępem do tego ogromu dynamicznych, rozproszonych i podzielonych danych oraz nad ich udostępnianiem (by zawsze wiadomo było, kto ma dostęp, kto udostępnia dane i komu) wydaje się zadaniem ponad siły dotychczas stosowanych rozwiązań.

IBM Security Guardium, służy do ochrony danych wrażliwych wszędzie tam, gdzie się one znajdują. Dzięki tej wszechstronnej platformie ochrony danych zespoły odpowiedzialne za bezpieczeństwo informatyczne mogą automatycznie analizować aktywność w środowisku danych, by zminimalizować ryzyko, zabezpieczyć dane przed zagrożeniami wewnętrznymi i zewnętrznymi oraz płynnie adaptować środowisko do zmian wpływających na ich bezpieczeństwo.

Kompleksowa ochrona danych, na którą można liczyć

Guardium działa w oparciu o kompleksową strategię ochrony danych wrażliwych w organizacji – jej „klejnotów koronnych", od których zależy powodzenie biznesowe, a nawet możliwość kontynuowania działalności. Korzystając z wszechstronnego graficznego interfejsu użytkownika, zespoły odpowiedzialne za bezpieczeństwo mogą rozpoznawać i eliminować czynniki ryzyka potencjalnie zagrażające danym w ruchu i w spoczynku. Ta zunifikowana strategia obejmuje również szeroką gamę repozytoriów danych ustrukturyzowanych i nieustrukturyzowanych, w tym bazy danych, hurtownie danych, środowiska Hadoop, NoSQL, systemy operujące na danych w pamięci wewnętrznej, udostępnione pliki (udziały plikowe) itd.

W istocie Guardium oferuje elastyczność potrzebną do ekonomicznego, skalowalnego zaspokajania całego spektrum wymagań w dziedzinie bezpieczeństwa i ochrony danych – od egzekwowania podstawowych zasad po wszechstronną ochronę. To wielowarstwowe rozwiązanie zawiera mechanizmy zautomatyzowanej analizy zagrożeń, dynamicznej ochrony danych i zapewnienia przejrzystości, które pozwalają na adaptację zabezpieczeń do zmian w środowisku danych.



Guardium korzysta z technik analizy i automatyzacji, by chronić newralgiczne dane we współczesnych środowiskach heterogenicznych.

Analiza zagrożeń dla danych wrażliwych

Warunkiem skutecznej ochrony danych jest precyzyjne określenie, które zasoby mają być chronione, a potem wszechstronne ich zabezpieczenie. Guardium umożliwia zespołom odpowiedzialnym za bezpieczeństwo:

- Automatyczne wykrywanie i klasyfikowanie danych wymagających szczególnej ochrony oraz ujawnienie potencjalnych niezgodności z wymaganiami formalno-prawnymi.
- Uzyskiwanie informacji o tym, kto uzyskuje dostęp do danych, wychwytywanie anomalii i zapobieganie utracie danych.
- Szybkie analizowanie schematów wykorzystania zasobów i systemów w celu ujawniania i eliminowania czynników ryzyka.

Guardium pomaga zespołom odpowiedzialnym za bezpieczeństwo w automatycznym wykrywaniu i klasyfikowaniu informacji wymagających ochrony. Odbywa się to za pośrednictwem łatwego w obsłudze graficznego interfejsu użytkownika. Wykonując szereg kroków, personel odpowiedzialny za bezpieczeństwo może wykryć wszystkie źródła danych zawierające informacje podlegające szczególnej ochronie, w tym nieskatalogowane bazy danych, a następnie wykorzystać konfigurowalne etykiety klas i funkcje zarządzania uprawnieniami do zautomatyzowanego egzekwowania strategii bezpieczeństwa. Wykrywanie danych można także zaplanować jako zadanie wykonywane regularnie według harmonogramu, aby identyfikować nowe instancje danych i uniknąć ryzyka nieuprawnionego dostępu do danych wrażliwych.

Aby pomóc w egzekwowaniu strategii i chronić newralgiczne dane, Guardium może nieustannie, w czasie rzeczywistym monitorować dostęp (i próby dostępu) do danych objętych szczególną ochroną. Wychodząc poza tradycyjne techniki monitorowania danych, Guardium oferuje możliwość wykrywania sytuacji nietypowych i inteligentnego analizowania ryzyka na podstawie zmian w zachowaniu. Wykorzystuje zaawansowany algorytm uczenia maszynowego (self-learning machine) do wykrywania działań odbiegających od obserwowanego dotychczas wzorca. Wykrywanie odbywa się na podstawie szczegółowych informacji kontekstowych o dostępie do danych – odpowiadających na pytania „kto, co, gdzie, kiedy i jak". W ramach adaptacyjnego procesu uczenia się Guardium porównuje nowe wzorce typowych zachowań z nowymi działaniami, w miarę jak są one rejestrowane. Intuicyjny interfejs użytkownika ułatwia wykrywanie anomalii, pozwalając administratorom na analizę zstępującą, która doprowadzi do podstawowej przyczyny problemu.

Guardium udostępnia wygodny interfejs graficzny do wykrywania sytuacji nietypowych i reagowania na nie w oparciu o inteligentny algorytm.

Oprócz analizy zstępującej Guardium umożliwia personelowi odpowiedzialnemu za bezpieczeństwo szybkie przeszukiwanie raportów z audytów i innych informacji w interfejsie użytkownika, a także szybkie wyszukiwanie treści danych w środowisku korporacyjnym. Użytkownik nie musi orientować się w topologii, zasadach agregacji i metodach równoważenia obciążenia. Wyszukiwanie może pomóc w wyodrębnieniu wartościowych spostrzeżeń z zapisu aktywności do konkretnych danych, przy czym może być ukierunkowane na konkretne źródła danych, użytkowników lub czas dostępu. Nowy kokpit dochodzeniowy jest przydatny w ujawnianiu wzorców, anomalii i powiązań w danych, ponieważ jego domyślne widoki – opracowane w oparciu o sprawdzone procedury – optymalnie zawężają obszar poszukiwań. Dostępne jest również narzędzie do profilowania połączeń, które zgłasza wszystkie próby nawiązania połączenia z określonym źródłem danych.

Ochrona danych wrażliwych

Rosnący poziom zagrożenia i coraz bardziej rygorystyczne wymagania formalno-prawne skłaniają organizacje do głębszego zastanowienia nad stosowanymi obecnie strategiami bezpieczeństwa. Guardium umożliwia zespołom odpowiedzialnym za bezpieczeństwo:

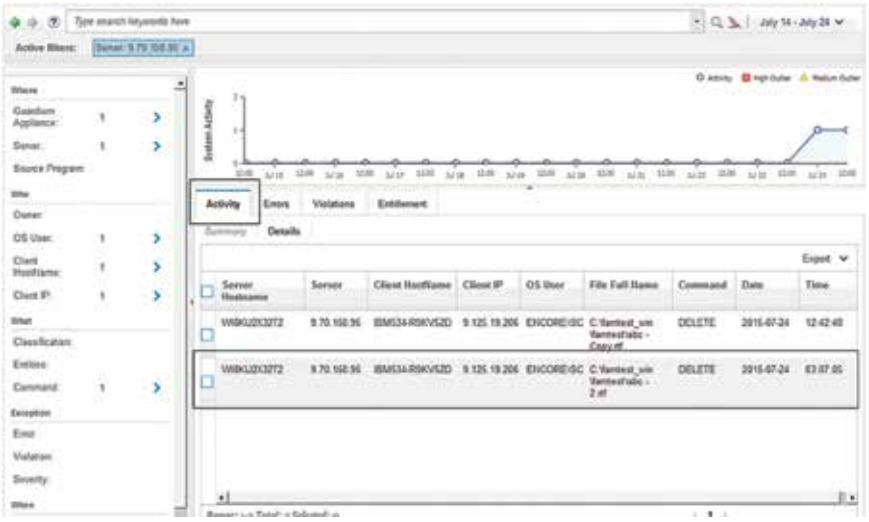
- Zabezpieczenie przedsiębiorstwa przed ryzykiem finansowym dzięki automatyzacji egzekwowania zasad i rozbudowanym funkcjom kontrolnym.
- Ochronę danych wrażliwych poprzez szyfrowanie, maskowanie, dynamiczne blokowanie, alarmowanie i obejmowanie kwarantanną.
- Monitorowanie i blokowanie działań w czasie rzeczywistym w celu uniemożliwienia dostępu do danych i plików osobom nieuprawnionym – zarówno wewnątrz, jak i z zewnątrz organizacji.

Guardium przechwytuje i analizuje cały ruch dotyczący danych krytycznych, w tym dostęp lokalny użytkowników uprzywilejowanych. Zapis kontrolny zebranych w ten sposób danych także jest zabezpieczony przed nieuprawnionym dostępem i manipulacjami. Stanowi w istocie jedno scentralizowane, znormalizowane i ogólnokorporacyjne repozytorium danych audytowych na potrzeby sprawozdawczości formalnej, optymalizacji wydajności, dochodzeń i zbierania dowodów. Organizacje mogą automatyzować cały proces audytu zgodności z wymaganiami w zakresie ochrony danych – w tym rozsyłanie

raportów do zespołów nadzorujących, akceptacje i eskalacje – korzystając ze wstępnie skonfigurowanych raportów zgodnych z wymogami ustawy Sarbanes-Oxley (SOX), standardu Payment Card Industry Data Security Standard (PCI DSS) oraz przepisów o ochronie prywatności.

Co więcej, Guardium umożliwia zespołom odpowiedzialnym za bezpieczeństwo ochronę newralgicznych danych przed zagrożeniami wewnętrznymi i zewnętrznymi przy zastosowaniu szyfrowania plików, statycznego maskowania oraz selektywnego usuwania fragmentów danych. Oferuje także możliwość dynamicznego maskowania i szyfrowania danych w czasie rzeczywistym, a także blokowania, alarmowania i obejmowania podejrzanych użytkowników kwarantanną. Jest w stanie zablokować dostęp szkodliwie działających osób i systemów do newralgicznych danych w większości źródeł, w tym w chmurze, na platformach wielkich zbiorów danych (big data) i w systemach plików.

Guardium wspomaga także egzekwowanie podziału obowiązków między użytkownikami, nieustannie monitorując wszystkie operacje na newralgicznych danych – w tym dostępy do systemu plików. Umożliwia organizacjom wykrywanie, rejestrowanie i blokowanie działań użytkowników uprzywilejowanych, jeśli są one podejrzane lub podejmowane bez autoryzacji. Na przykład Guardium może wykryć masowe kopiowanie newralgicznych plików lub katalogów albo nagłe nasilenie dostępu do plików przez jednego z administratorów, a także alarmować o nieprawidłowych dostępach, blokować dostęp do najściślej chronionych dokumentów i generować konfigurowalne raporty o wszelkich rodzajach aktywności.



Monitorując aktywność podejmowaną w odniesieniu do plików, Guardium umożliwia organizacjom wykrywanie i blokowanie podejrzanych działań – nawet podejmowanych przez użytkowników uprzywilejowanych.

Adaptacja do zmian

Infrastruktury danych nieustannie się zmieniają i rozrastają. W efekcie wciąż powstają nowe i ewoluują znane luki w zabezpieczeniach, a zapewnienie w tych warunkach skutecznej ochrony danych jest bardzo trudne. Guardium umożliwia organizacjom:

- ochronę danych w środowiskach tradycyjnych i zyskujących popularność – takich jak Hadoop, NoSQL i chmura;
- łatwą rozbudowę architektury ochrony danych od minimum wymaganego przepisami aż do wieloaspektowego systemu bezpieczeństwa;
- ograniczenie kosztów i optymalizację wyników w oparciu o jednolitą infrastrukturę ochrony całego środowiska danych zdolną do automatycznego równoważenia obciążenia.

Guardium pomaga organizacjom w adaptacji do zmian w środowisku danych, gdy wymagane jest objęcie ochroną nowych użytkowników, platform i typów informacji. Rozwiązanie uwzględnia szerokie spektrum platform: tradycyjne bazy danych, środowiska chmury, systemy oparte na technologii Hadoop, bazy NoSQL i systemy przetwarzające dane w pamięci wewnętrznej (in-memory). Guardium oferuje elastyczne mechanizmy kontroli i zarządzania, które można dostosować do konkretnych wymagań formalnych i łatwo skalować w ślad za nowymi potrzebami biznesowymi.

W odróżnieniu od rozwiązań punktowych Guardium umożliwia heterogeniczną integrację z innymi czołowymi rozwiązaniami zabezpieczającymi, standardami oceny zabezpieczeń, aplikacjami itd. Guardium zapewnia też najlepszą w swojej klasie integrację z rozwiązaniami IBM z dziedziny bezpieczeństwa, takimi jak system zarządzania informacjami i zdarzeniami związanymi z bezpieczeństwem (SIEM) IBM Security QRadar – z myślą o zapewnieniu proaktywnej ochrony danych. Guardium wysyła informacje o zdarzeniach i wynikach wykrywania/klasyfikacji baz danych do systemu SIEM QRadar, dzięki czemu możliwa jest skuteczniejsza korelacja informacji o zagrożeniach. Ponadto Guardium może odbierać powiadomienia o statusie i alerty z systemu SIEM QRadar, by chronić środowisko przed dostępem z niebezpiecznych adresów IP, działaniami oszustów i wykorzystaniem nowych słabych punktów aplikacji, systemów operacyjnych i źródeł danych. Integracja rozwiązań Guardium i QRadar może pomóc na przykład w ochronie organizacji przed potencjalnymi atakami podejmowanymi za pośrednictwem aplikacji; wykrywaniu ataków na bazy danych (np. wstrzyknięciami kodu SQL) i powstrzymywaniu ich zanim umożliwią pobranie danych; a także w rozpoznawaniu słabych punktów w warstwie aplikacji i stosowaniu wirtualnych poprawek.

Guardium jest wartościowym rozwiązaniem dla organizacji reprezentujących różne branże

- **W dużym towarzystwie ubezpieczeniowym jeden pełnoetatowy pracownik samodzielnie zarządza zabezpieczeniami około 1000 baz danych.**
- **Duże przedsiębiorstwo z sektora usług komunalnych osiągnęło 55 – procentowy zwrot z inwestycji w niecały rok, chroniąc dane 4,5 miliona klientów zgodnie z wymaganiami SOX i PCI.**
- **Bank działający na całym świecie monitoruje ponad 5000 źródeł danych, w tym wielkie zbiory danych transakcyjnych, w czasie rzeczywistym i bez wpływu na wydajność newralgicznych aplikacji.**
- **Międzynarodowe przedsiębiorstwo telekomunikacyjne może teraz centralnie monitorować w czasie rzeczywistym dostępy do tysięcy baz danych rozproszonych w 16 ośrodkach na całym świecie.**
- **Producent z branży motoryzacyjnej monitoruje i kontroluje 500 produkcyjnych baz danych, osiągając wyższy poziom bezpieczeństwa, a angażuje do tego o 90 procent mniej pracowników niż dotychczas.**

Dlaczego IBM?

Rozwiązania IBM z dziedziny bezpieczeństwa cieszą się zaufaniem organizacji na całym świecie. Te sprawdzone rozwiązania techniczne umożliwiają im zapewnienie ochrony kluczowych zasobów przed najnowszymi zagrożeniami. W obliczu coraz to nowych niebezpieczeństw IBM pomaga organizacjom we wzmacnianiu infrastruktury bezpieczeństwa, oferując im pełną gamę produktów, usług, a także rozwiązania opracowane przez partnerów handlowych.

IBM ma doświadczenie w realizacji usług dla branż ściśle regulowanych, w tym dla administracji publicznej, służby zdrowia i sektora usług finansowych. Jako partner strategiczny IBM zapewnia organizacjom środki potrzebne do minimalizacji narażenia i zarządzania ryzykiem nawet w najbardziej skomplikowanych środowiskach informatycznych.

Więcej informacji

Aby uzyskać dodatkowe informacje o rozwiązaniu IBM Security Guardium, należy skontaktować się z przedstawicielem IBM lub Partnerem Handlowym IBM bądź odwiedzić serwis: **ibm.com**/guardium

Rozwiązania IBM z dziedziny bezpieczeństwa

Oferta produktów i usług IBM w dziedzinie bezpieczeństwa należy do najbardziej zaawansowanych i zintegrowanych propozycji dostępnych dziś na rynku. Zaplecze merytoryczne i informacyjne, jakie zapewnia renomowany zespół badawczo-rozwojowy IBM X-Force, pomaga organizacjom w holistycznej ochronie osób, infrastruktury, danych i aplikacji przy wykorzystaniu rozwiązań do zarządzania tożsamością i dostępem, zabezpieczania baz danych, tworzenia bezpiecznych aplikacji, zarządzania ryzykiem, zarządzania punktami końcowymi, zabezpieczania sieci i szeregu innych pokrewnych zastosowań. Rozwiązania te umożliwiają efektywne zarządzanie ryzykiem i implementację zintegrowanych zabezpieczeń platform mobilnych, chmury, mediów społecznościowych i innych korporacyjnych architektur biznesowo-informacyjnych. IBM utrzymuje jedną z największych na świecie organizacji zajmujących się badaniami, rozwojem i realizacją rozwiązań w dziedzinie bezpieczeństwa. Każdego dnia w ponad 130 krajach IBM monitoruje 15 miliardów zdarzeń istotnych dla bezpieczeństwa i posiada ponad 3000 patentów w tej dziedzinie.

IBM Polska Sp. z o.o.
1 Sierpnia 8
02-134 Warszawa
Polska

[1] „2015 Cost of Data Breach Study: Global Analysis," Ponemon Institute, maj 2015 r. **ibm.com**/security/data-breach/

Papier należy przetworzyć wtórnie

WGS03063-PLPL-00