



The Security Division of EMC

Przegląd rozwiązania firmy RSA

RSA® Data Loss Prevention Suite

Ustalenie ryzyka, utworzenie kontroli

Streszczenie dla kadry zarządzającej

RSA Data Loss Prevention (DLP), rozwiązanie firmy RSA, służące do zapobiegania utracie danych, pomaga w określeniu ryzyka biznesowego związanego z utratą kluczowych danych oraz dynamicznie zmniejsza to zagrożenie przy pomocy środków zaradczych bazujących na odpowiedniej polityce zabezpieczeń i wdrażaniu elementów kontrolnych. Rozwiązanie pozwala zredukować ryzyko niezależnie od tego, czy dane znajdują się w ośrodku przetwarzania danych, są przesyłane sieciami komputerowymi lub przetwarzane przez użytkownika w punkcie końcowym. Rozwiązanie DLP korzysta ze scentralizowanego zarządzania politykami bezpieczeństwa, obejmującego wszystkie trzy produkty: DLP Datacenter, DLP Network oraz DLP Endpoint. Upraszcza to wdrażanie i zapewnia spójność zarządzania wszystkimi kluczowymi danymi firmy.

Zmiana w zarządzaniu ryzykiem firmy

Zakres i rodzaj informacji ulegają zmianie. W ciągu ostatnich kilku lat nastąpiła wyraźna zmiana priorytetów w rozwoju infrastruktury informatycznej: od zabezpieczania sieci, poprzez ochronę systemów w sieci, do zabezpieczania samych danych. Istnieje kilka czynników odpowiadających za zmianę sposobu, w jaki firmy chronią swoje kluczowe dane i zmniejszają ryzyko ich utraty:

- stale rosnące zagrożenie utraty danych w wyniku działań osób wewnątrz organizacji;
- firmy przechowują więcej kluczowych danych; zwiększa się potrzeba udostępniania danych partnerom oraz wewnątrz firmy;
- powstają nowe rynki dla skradzionych danych; liczba przepisów wzrasta, a same przepisy stają się coraz bardziej skomplikowane.

Biorąc pod uwagę powyższe fakty, tradycyjne technologie zabezpieczające, które koncentrują się na intruzach i ochronie sieci na jej granicach, nie pozwalają na istotną redukcję ryzyka wewnętrznego. Należy ponownie zdefiniować obszary zainteresowań, aby uwzględnić zagrożenia tworzone przez własnych użytkowników o złych intencjach lub osoby, które nieświadomie narażają dane na ryzyko w wyniku źle zdefiniowanych procesów biznesowych i zabezpieczających. Z czasem ryzyko dotyczące utraty danych wrażliwych prowadzi do zwiększenia wydatków z tytułu likwidacji skutków naruszenia prawa, kosztów dostosowawczych, zmniejszenia się liczby klientów oraz osłabienie pozytywnego odbioru znaku towarowego.

Najważniejsze informacje o pakiecie DLP firmy RSA

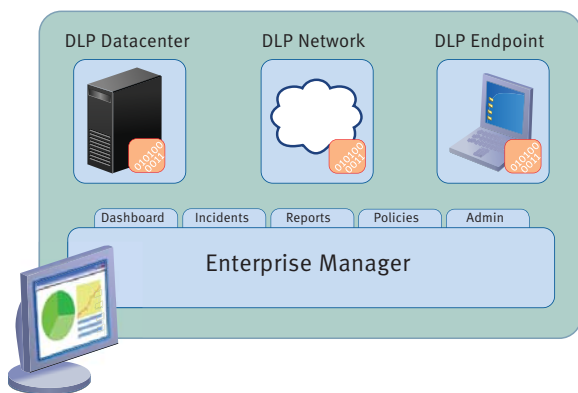
- Wykrycie i zredukowanie ryzyka utraty danych wrażliwych: znajdujących się w ośrodku przetwarzania danych, przesyłanych sieciami komputerowymi oraz używanych w punktach końcowych.
- Uzyskanie skalowalności przy pomocy architektury rozproszonej oraz pojedynczej podstawy budowania polityk ochrony danych wrażliwych, obowiązujących w całej infrastrukturze.
- Wcześniejsza realizacja wartości poprzez szybsze skanowanie oraz wbudowane, gotowe do natychmiastowego zastosowania, polityki bezpieczeństwa.
- Redukcja całkowitego kosztu posiadania rozwiązania, w wyniku większej precyzji i grupowania logicznego, a także przepływu zadań w przypadku naruszenia polityk.rmy.

„Rozwiązanie DLP firmy RSA zawiera wszechstronne opcje dotyczące sieci komputerowych, punktów końcowych i procesu wykrywania, obejmujące wszystkie elementy DLP wymagane przez wielu klientów we wszystkich sektorach”.

*Raport Magic Quadrant firmy Gartner, dotyczący monitorowania i filtrowania treści oraz zapobiegania przed utratą danych.
Czerwiec 2008 r.*

Rozwiązanie DLP firmy RSA – proaktywna propozycja opracowywania strategii bezpieczeństwa danych

Pakiet DLP firmy RSA zawiera zintegrowane produkty oferujące proaktywną koncepcję zarządzania ryzykiem biznesowym związanym z utratą danych firmy. Pakiet ten składa się z trzech produktów: RSA DLP Datacenter (do analizy i ochrony danych w centrach danych), RSA DLP Network (do ochrony danych przesyłanych przez sieć) oraz RSA DLP Endpoint (do ochrony danych na stacjach końcowych użytkowników), które można kupić osobno lub jako zestaw, zależnie od wymagań klienta. Koncepcja



Współczesne problemy dotyczące utraty danych

Ryzyko związane z utratą danych wrażliwych objawia się zarówno w obszarach uwzględniających regulacje prawne, jak i tych, które im nie podlegają. Aby zmniejszyć skutki tego typu ryzyka, organizacje muszą zastosować

rozwiazania nastepnej generacji, takie jak pakiet DLP firmy RSA, który koncentruje się na zabezpieczeniu samych danych, niezależnie od ich lokalizacji (ośrodek przetwarzania danych, sieć lub stacja końcowa).

cja pakietu przewiduje scentralizowane zarządzanie politykami bezpieczeństwa przy pomocy programu Enterprise Manager, co pozwala na ochronę danych wrażliwych niezależnie od ich lokalizacji. Ta nowatorska koncepcja pozwala firmom na wyszczególnianie i priorytetyzowanie ryzyka, a następnie likwidowanie go w podobny sposób, jak w przypadku strategii bezpieczeństwa dotyczącej konkretnych danych.

Zwykle klienci zaczynają od opracowania polityki bezpieczeństwa danych, a następnie – przy pomocy pakietu DLP firmy RSA – identyfikują dane wrażliwe u źródła, przy pomocy dokładnych technik wykrywania i klasyfikacji. Po identyfikacji danych wrażliwych, pakiet DLP pomaga w utworzeniu kontroli poprzez wdrożenie właściwych mechanizmów, w oparciu o jeden lub więcej konkretnych modułów przedstawionych w tabeli poniżej. Skomplikowane mechanizmy – przepływu zadań, powiadamiania, kontroli i raportowania – działają wspólnie, aby wykrywać i definiować źle zdefiniowane procesy biznesowe, stanowiące często główną przyczynę naruszenia danych. Zawarte w rozwiązaniu DLP mechanizmy powiadamiania i wdrażania są wystarczająco elastyczne, aby zaspokoić konkretne potrzeby różnych branż, działu prawnego i ds. zgodności lub innych zainteresowanych jednostek (np. kadr).

Ryzyko biznesowe	Potrzeba biznesowa	Dane, których dotyczy ryzyko (przykłady)	Skutki naruszenia danych
Obszar regulacji prawnych	Utrzymanie zgodności z regulacjami	Informacje finansowe: specyficzne dane dotyczące przepisów międzynarodowych i obowiązujących w USA (ustawy: SOX, GLBA)	Utrata wartości marki, grzywny i opłaty prawne; koszty wynikające z naruszenia / ujawnienia danych oraz zastosowania środków zaradczych; utrata zaufania klientów.
Obszar bez regulacji prawnych	Ochrona strategii biznesowej oraz informacje o operacjach Ochrona własności intelektualnej	Dane osobowe (PII): dane pracownika i klienta związane z przepisami (standard PCI oraz ustawy HIPAA i California SB 1386).	Utrata konkurencyjności, potencjalnego dochodu; niskie morale pracowników.
		Informacje dotyczące: ustalenia cen, fuzji i przejęć (M&A), sprzedaży oraz marketingu. Kod źródłowy, patent, kopie lub dokumenty techniczne.	

W porównaniu z innymi użytkownikami, klienci rozwiązania DLP mają znacznie niższy profil ryzyka odnośnie utraty danych, co pozwala na skuteczniejsze zabezpieczenie danych i zapewnia lepsze perspektywy biznesowe. Możliwość utrzymania zgodności prawnej oraz ograniczenia stopnia ryzyka w przypadku własności intelektualnej, strategii i narażenia na utratę danych operacyjnych, przekłada się na zwiększenie zaufania klientów, ograniczenie rotacji klientów, zmniejszenie ilości grzywien i kar, a także zapewnienie lepszej ochrony całkowitej firmy. Pakiet DLP firmy RSA pozwala na wykrywanie ryzyka oraz utworzenie kontroli najbardziej wrażliwych informacji, poprzez opracowanie i wdrożenie polityk bezpieczeństwa.

Podstawowe zalety pakietu DLP

Pewne zarządzanie politykami bezpieczeństwa i klasyfikowanie danych

Scentralizowane zarządzanie politykami bezpieczeństwa oraz wbudowane polityki dotyczące danych wrażliwych znajdujących się w dowolnej lokalizacji (ośrodki przetwarzania danych, sieci komputerowe, punkty końcowe) – gwarantuje spójne wykrywanie, klasyfikowanie, stosowanie środków zaradczych oraz kontrolę, w zależności od ryzyka biznesowego i potrzeby biznesowej.

Wydajność i skalowalność rozwiązań

Architektura rozproszona na poziomie firmy zapewnia najszybsze skanowanie punktów końcowych i ośrodka przetwarzania danych, w celu wykrywania i analizowania danych wrażliwych.

Najwyższy poziom precyzji

Najwyższy na rynku poziom dokładności identyfikowania danych wrażliwych osiągnięto poprzez wdrożenie wyrafinowanych algorytmów wykrywania danych oraz szablonów polityk, dzięki którym informacje wrażliwe można wykrywać zarówno w oparciu o analizę treści, jak i kontekstowe umieszczanie w plikach słów kluczowych.

Polityki i reakcje systemu uwzględniające tożsamość

Polityki oraz reakcje systemu uwzględniają tożsamość właścicieli danych wrażliwych, poprzez unikatową integrację z usługą katalogową Windows Active Directory®. Pozwala to na uściślenie polityki bezpieczeństwa, przy ograniczeniu do minimum zakłóceń w firmie i wyeliminowaniu fałszywych alarmów.

Elastyczny przepływ zadań; audyt i raportowanie

Wyrafinowany i elastyczny przepływ zadań oraz mechanizmy powiadamiania, audytu i raportowania działają wspólnie, aby wykrywać i definiować źle zdefiniowane procesy biznesowe, stanowiące często główną przyczynę naruszenia danych.

Pojedyncza podstawa budowania polityk dla infrastruktury

Wspólna polityka obejmuje wszystkie komponenty, w tym integrację z rozwiązaniami opracowanymi przez głównych dostawców infrastruktury – m.in. usługami Microsoft® Right Management Services, rozwiązaniami dotyczącymi punktów końcowych (Cisco) oraz rozwiązaniami firmy EMC przeznaczonymi do przechowywania i zarządzania treścią.

Moduł DLP Datacenter

Wykrywanie i ochrona danych wrażliwych u źródeł zagrożeń

Głównym celem modułu DLP Datacenter jest uruchamianie i obsługa aplikacji stosowanych przez grupy biznesowe w ramach organizacji, z uwagi na dużą ilość danych przechowywanych w ośrodkach przetwarzania danych. Część z tych danych ma charakter wrażliwy i właśnie te dane są zwykle rozproszone w systemach plików, bazach danych, systemach poczty elektronicznej, systemach zarządzania treścią lub dużych systemach SAN / NAS.

Moduł DLP Datacenter wykrywa dane wrażliwe w centrum przetwarzania danych, niezależnie od ich konkretnej lokalizacji.



Źródło danych

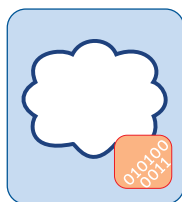
Serwer plików
NAS / SAN
Pliki baz danych
Strony SharePoint
Systemy zarządzania treścią

Zadania

kwarantanna
kasowanie
powiadomienie
przesunięcie danych do zabezpieczonej lokalizacji
zastosowanie polityk eDRM (przy pomocy usługi RMS firmy Microsoft)

Jest to często główna przyczyna utraty danych, ponieważ systemy te mają dużą liczbę użytkowników, przy czym niektórzy z nich nie wymagają do wykonania swoich zadań wszystkich aktualnych praw dostępu. Niepotrzebny dostęp stanowi ryzyko bezpieczeństwa wewnętrznego firmy. Moduł DLP Datacenter wykrywa dane wrażliwe na podstawie szczegółowej analizy treści i oferuje przegląd ryzyka odnośnie danych wrażliwych znajdujących się w ośrodku przetwarzania danych. Na przykład, użytkownicy mogą przypadkowo lub umyślnie pobrać plik wrażliwy z systemu plików lub bazy danych i udostępnić go innym nieupoważnionym użytkownikom znajdującym się poza firmą. Taka utrata danych wrażliwych stanowi ryzyko biznesowe. Moduł DLP Datacenter zmniejsza to ryzyko u źródła, poprzez szybkie i precyzyjne wykrycie wszystkich danych wrażliwych znajdujących się w ośrodku przetwarzania danych. Moduł może wyeliminować to ryzyko poprzez zastosowanie np. kwarantanny i skasowanie danych wrażliwych lub przesunięcie ich do systemu zabezpieczonego.

W wyniku nowej integracji z usługą RMS firmy Microsoft, moduł DLP Datacenter może również automatycznie zastosować w przypadku plików wrażliwych polityki zarządzania prawami i zapewnić dostęp do plików tylko właściwym osobom.



Moduł DLP Network wykrywa i monitoruje dane wrażliwe przesyłane sieciami komputerowymi oraz wymusza wykonanie określonych działań (np. zablokowanie).

Obsługiwane transmisje	Wykonywane działania
Poczta elektroniczna (SMTP, IMAP...)	zezwolenie
IM / chat	blokowanie
http / https	szyfrowanie
FTP	powiadomienie
dowolny protokół TCP	

Co więcej, dane wrażliwe przesyłane w taki sposób mogą być przechwycone "w locie", mimowolnie przesłane pod niewłaściwy adres lub po prostu mogą być niezgodne z obowiązującymi wytycznymi. Każdy z tych przypadków nieupoważnionych transmisji, może narazić firmę na ryzyko.

Moduł DLP Network umożliwia wyeliminowanie tego ryzyka poprzez szybkie i precyzyjne wykrycie / przeanalizowanie danych wychodzących z sieci firmy oraz wymuszenie zastosowania polityki bezpieczeństwa danych, na podstawie rodzaju firmy i potrzeby biznesowej.

Moduł DLP Network może zapobiegać przed utratą danych na dwa sposoby. Najpierw można wykonać monitorowanie pasywne, pomagające w zrozumieniu konkretnych rodzajów ryzyka oraz w wykryciu źle zdefiniowanych procesów biznesowych. W trybie tym moduł przesyła stosownym stronom powiadomienia i alarmy, które ułatwiają przeprowadzanie audytu i szkolenie pracowników odnośnie ryzykownych transmisji i praktyk biznesowych. Moduł oferuje również możliwość pracy w trybie aktywnym, pozwalającym na wdrażanie dodatkowych mechanizmów, np. wbudowanego blokowania wiadomości e-mail lub szyfrowania przez partnerów. Niezależnie od tego, która metoda bardziej pasuje do profilu ryzyka firmy, moduł DLP Network zmniejsza prawdopodobieństwo, że transmisje wrażliwe wpłyną na działalność i zyski firmy.

Moduł DLP Network

Monitorowanie danych wrażliwych opuszczających sieć danej firmy i wymuszanie wykonania określonych działań

Współpraca zarówno wewnętrzna, jak i zewnętrzna, ma krytyczne znaczenie dla sukcesu każdej firmy. Współpraca w panujących obecnie warunkach gospodarczych, wymaga przepływu informacji pocztą elektroniczną, wiadomości rozprawdzanych za pomocą komunikatorów lub innych form łączności sieciowej. Przepływ danych jest układem krwionośnym firm, wpływającym bezpośrednio na prężność i wydajność każdej firmy. Wadą tego układu jest to, że dane wrażliwe mogą wydostać się na zewnątrz i trafić do firm / osób niepowołanych.

Niezależnie od tego, czy użytkownik działa przypadkowo, czy umyślnie, plik wrażliwy może zostać przesłany pocztą elektroniczną jako załącznik, lub na przykład tajemnica handlowa może być przesłana przy pomocy usługi FTP.

Korzyści stosowania modułu

- Pasywne monitorowanie danych wrażliwych wychodzących z sieci firmy.
- Aktywne blokowanie i zabezpieczanie przesyłanych danych, na podstawie polityk.
- Przesyłanie powiadomień alarmowych w ramach przepływu zadań oraz wykonywanie audytów lub raportów dotyczących przypadków naruszeń bezpieczeństwa danych.

Moduł DLP Endpoint

Wykrywanie i kontrola danych wrażliwych w punktach końcowych

Punkty końcowe, takie jak komputery przenośne lub stacjonarne, zrewolucjonizowały sposób prowadzenia działalności biznesowej. Większość codziennych czynności jest wykonywana w punktach końcowych, w związku z tym stanowią one krytyczny komponent pomyślnej działalności, mającej na celu wspieranie mobilności i zapewnianie wydajności procesu zarządzania. Ponieważ większość osób pracuje głównie na tego typu sprzęcie, łatwo można sobie wyobrazić ogromną ilość wrażliwych informacji przechowywanych w komputerach stacjonarnych i przenośnych. Dane statystyczne dowodzą, że we współczesnych środowiskach IT, ponad 50% danych jest traconych w wyniku transmisji do urządzeń przenośnych.

Dane wrażliwe mogą znaleźć się w sprzęcie przenośnym poprzez pobranie pliku z systemu plików lub bazy danych, jako pozostałość zarchiwizowanej wiadomości e-mail, a nawet wpis utworzony ręcznie na stacji roboczej i zapisany na dysku. Jedynym sposobem zabezpieczenia danych wrażliwych w urządzeniach przenośnych, jest szybkie i precyzyjne wykrycie oraz przeanalizowanie miejsca przechowywania danych, monitorowanie ruchu danych, a także wymuszenie podjęcia działań takich, jak blokowanie, aby nie dopuścić do nieuprawnionego użycia danych.

Moduł DLP Endpoint wyposażony jest w dwie różne opcje, które działając wspólnie zmniejszają ryzyko utraty danych wrażliwych w komputerach stacjonarnych i przenośnych. Po pierwsze, w oparciu o scentralizowane polityki, moduł DLP Endpoint wykrywa i analizuje dane wrażliwe znajdujące się w komputerach stacjonarnych i przenośnych. Po drugie, moduł zwiększa bezpieczeństwo poprzez blokowanie transmisji danych wrażliwych do urządzeń przenośnych (pamięci USB, płyt CD/DVD) oraz zapewnienie dodatkowych możliwości kontroli plików w przypadku drukowania.

Korzyści stosowania modułu

- Wykrywanie, monitorowanie i analizowanie danych wrażliwych w sprzęcie typu punkt końcowy.
- Kontrola i zapobieganie przed nieuprawnionymi transmisjami danych ze stacji roboczych firmy; oraz ograniczenie innych działań użytkowników – na podstawie polityk.
- W przypadku kradzieży komputera przenośnego, opracowywany jest raport zawierający wszystkie szczegóły na temat przechowywanych w komputerze danych wrażliwych (zgodnie z przepisami).



Moduł DLP Endpoint wykrywa i monitoruje dane wrażliwe w sprzęcie końcowym (komputery stacjonarne / przenośne) oraz wymusza wykonanie określonych działań.

Moduł obsługuje działania przewidziane w polityce, w oparciu o stan połączenia sieciowego.

Obsługiwane punkty końcowe	Wykonywane działania (zezwolenie lub zablokowanie)
Komputery przenośne i stacjonarne drukowanie z systemem w wersji Windows 2000 SP4 lub wyższej	drukowanie opcja: zapisz / zapisz jako nagrywanie na płytach CD / DVD
(ograniczone wsparcie eksportowanie danych do pamięci USB w przypadku systemu zastosowanie strategii eDRM	eksportowanie danych do pamięci USB zastosowanie strategii eDRM (przy pomocy usługi RMS firmy Microsoft)

Zrób kolejny krok Oceń ryzyko już dziś

Usługa oceny ryzyka (DLP RiskAdvisor) umożliwia – przy pomocy pakietu RSA DLP Suite – profesjonalną zmianę poziomu ochrony danych, z formy reaktywnej do proaktywnej. Poprzez zdefiniowanie danych wrażliwych i określenie ich lokalizacji, usługa oferuje podstawę do identyfikacji źle określonych procesów biznesowych i pomaga firmom w opracowaniu strategii zapobiegania przed utratą danych. Usługa dostarcza szczegółowy raport ryzyka, wraz z zaleceniami dotyczącymi poprawienia procesu i lepszego zarządzania obszarami zarówno objętymi regulacjami prawnymi, jak i bez regulacji.

Usługa DLP RiskAdvisor obejmuje:

- szczegółowy spis danych wrażliwych;
- skanowanie komputerów stacjonarnych i przenośnych;
- skanowanie plików udostępnianych;
- raport dla kierownictwa (streszczenie) na temat aktualnego profilu ryzyka, wraz z zaleceniami.

„Pakiet DLP (Tablus Content Sentinel) firmy RSA, pomaga w identyfikowaniu luk w bezpieczeństwie danych, poprzez sprawdzaniu treści znajdujących się w komputerach stacjonarnych, przenośnych i serwerach. Po dokonaniu oceny, można zastosować właściwe środki w celu ochrony informacji, zanim zostaną ujawnione lub przesunięte do innej lokalizacji. Już tylko ta jedna właściwość przekona audytorów, że dana firma stosuje proaktywne środki bezpieczeństwa. Podobnie, ochrona danych poufnych zmniejsza ryzyko zdobycia tych danych przez firmy konkurencyjne. Rozwiązanie to odgrywa zasadniczą rolę w całej strategii, aby zapewnić zgodność ze strategiami korporacyjnymi i obowiązującymi przepisami”.

Infoworld

Szybkie wykrywanie treści wrażliwych



Firma RSA jest partnerem godnym zaufania

RSA, oddział firmy EMC zajmujący się bezpieczeństwem, specjalizuje się w ochronie informacji w całym cyklu ich istnienia. Firma oferuje klientom rozwiązania pozwalające na opłacalne zabezpieczenie informacji krytycznych oraz tożsamości wykorzystywanych w transakcjach internetowych, na każdym etapie i niezależnie od lokalizacji, a także zarządzanie informacjami i zdarzeniami dotyczącymi bezpieczeństwa, aby zredukować problemy dotyczące zgodności z przepisami.

Firma RSA oferuje najlepsze na rynku rozwiązania w dziedzinie ochrony tożsamości i kontroli dostępu, szyfrowania i zarządzania kluczami, zarządzania informacjami dotyczącymi zgodności i bezpieczeństwa, a także ochrony przed oszustwami. Rozwiązania te zapewniają ochronę tożsamości milionów użytkowników, wykonywanych przez nich transakcji oraz generowanych danych. Więcej informacji na ten temat można znaleźć na stronach: www.RSA.com oraz www.EMC.com.

© 2007 r. RSA Security Inc. Wszystkie prawa zastrzeżone. Nazwy: RSA, RSA Security, FraudAction, eFraudNetwork oraz logo RSA, są znakami towarowymi lub zarejestrowanymi znakami towarowymi firmy RSA Security Inc. w USA i/ lub innych krajach. EMC jest zarejestrowanym znakiem towarowym firmy EMC Corporation. Wszystkie pozostałe produkty i usługi wymienione w niniejszym dokumencie, są znakami towarowymi poszczególnych firm.



RSA Security Inc.
RSA Security Ireland Limited
www.rsa.com

The Security Division of EMC