



# Platforma RSA enVision

## Przegląd zabezpieczeń

### Najważniejsze cechy

- Daje stuprocentowy wgląd we wszystkie zagrożenia bezpieczeństwa mogące wystąpić w całej infrastrukturze informatycznej
- Przechwytuje wszystkie dane (All the Data™) z sieci, mechanizmów zabezpieczających, hostów, warstw aplikacji, urządzeń do zapisu danych zainstalowanych w przedsiębiorstwie
- Umożliwia analizę danych zarówno w czasie rzeczywistym, jak i danych archiwalnych, oraz ich prezentację w formie przeglądów i raportów

### Cel użytkownika

Nawet najlepsze mechanizmy ochrony na styku z internetem nie mogą powstrzymać wszystkich zagrożeń bezpieczeństwa pochodzących z zewnątrz, jakie mogą się pojawić w dzisiejszych czasach, a w przypadku zagrożeń wewnętrznych są one prawie beзуteczne. Aby dobrze zabezpieczyć infrastrukturę informatyczną, użytkownik musi dokładnie wiedzieć, co się dzieje przez cały czas zarówno w obrębie całej sieci, jak i infrastruktury IT.

Platforma enVision™ firmy RSA jest jedynym rozwiązaniem do zarządzania informacją i zdarzeniami bezpieczeństwa, które daje stuprocentowy wgląd we wszystkie zagrożenia bezpieczeństwa mogące wystąpić w obrębie całej infrastruktury informatycznej – począwszy od przełączników i routerów przez urządzenia zabezpieczające, zasoby hostów, aplikacje i serwery, aż po urządzenia do zapisu danych. Platforma zapewnia bezpieczeństwo poprzez agregację i analizę wszystkich danych (All the Data) ze wszystkich elementów infrastruktury sieciowej w czasie rzeczywistym. Wykorzystuje przy tym możliwości bazy danych protokołu internetowego (IPDB) LogSmart. Wykorzystując system uczenia się platformy, użytkownik dokładnie widzi zwyczajne – albo odbiegające od normy – wzorce powstające w sieci, dzięki czemu może zidentyfikować zagrożenia bezpieczeństwa dosłownie w każdym miejscu sieci, nawet w przypadku oddalonych lokalizacji.



The Security Division of EMC

### Platforma RSA enVision®: rozwiązania z zakresu bezpieczeństwa

Złożoność jest wrogiem bezpieczeństwa. W dzisiejszych czasach większość infrastruktury zapewniającej bezpieczeństwo firmy jest niewiarygodnie złożona. Obejmuje ona wiele niekompatybilnych systemów bezpieczeństwa rozproszonych w obrębie całej sieci. Platforma RSA enVision® oferuje rozwiązania zapewniające bezpieczeństwo, które radykalnie upraszczają zarządzanie bezpieczeństwem poprzez konsolidowanie, normalizowanie i analizowanie danych pochodzących ze złożonej infrastruktury. Dla klientów oznacza to znaczne podniesienie skuteczności zabezpieczeń, ponieważ umożliwia szybsze reagowanie na zagrożenia zewnętrzne oraz wykrycie zagrożeń wewnętrznych dzięki uzyskaniu ujednoczonego i kompleksowego wglądu na sieć.

### Baza danych protokołu internetowego RSA enVision

Dzięki wykorzystaniu zaawansowanej architektury LogSmart IPDB stosowanej przez setki przedsiębiorstw na całym świecie, platforma RSA enVision jest w stanie przechwytywać wszystkie dane (All the Data) z sieci, mechanizmów zabezpieczających, hostów, warstw aplikacji i urządzeń do zapisu danych zainstalowanych w obrębie całego przedsiębiorstwa. LogSmart IPDB umożliwia analizę danych zarówno w czasie rzeczywistym, jak i archiwalnych, oraz ich prezentację w formie przeglądów i raportów dostosowanych do różnorodnych potrzeb każdego działu przedsiębiorstwa – np. działu IT, działu bezpieczeństwa, osób odpowiedzialnych za zapewnienie zgodności i zarządzanie ryzykiem czy wreszcie zarządu.

Zalety bazy danych LogSmart IPDB:

- Zaprojektowana w celu przechowywania i zapewnienia efektywnej pracy z wykorzystaniem danych nieusystematyzowanych, bez konieczności ich filtrowania lub normalizowania
- Zapewnia utrzymanie cyfrowego łańcucha ochrony danych, dzięki czemu dane raz wprowadzone do bazy nie mogą zostać zmienione – w odróżnieniu od większości schematów danych wykorzystywanych w rozwiązaniach opartych na RDBMS
- Nie są konieczne programy typu agent
- Rozproszona architektura typu „peer-to-peer” umożliwia dużą skalowalność i wydajność



Platforma RSA enVision – dzięki zastosowaniu architektury LogSmart IPDB – umożliwia klientom gruntowną poprawę poziomu bezpieczeństwa poprzez:

- Wdrożenie kontroli dostępu – możliwość kompleksowego kontrolowania i raportowania w celu wdrożenia zasad kontroli dostępu pozwala klientom na natychmiastowe wykrycie nadużyć i wprowadzenie odpowiedzialności zarówno za uprawniony, jak i nieuprawniony dostęp do sieci, zasobów obliczeniowych i składników na poziomie obiektów.
- Zmniejszenie liczby błędnych klasyfikacji – automatyczna korelacja zgłaszanych ataków z zasobami i danymi podatnymi na uszkodzenia znacznie ogranicza koszty powstałe w wyniku incydentu i umożliwia skoncentrowanie strategicznych zasobów analizy bezpieczeństwa na ważnych zdarzeniach.
- Monitorowanie w czasie rzeczywistym – ujednoczony podgląd wzajemnych zależności pomiędzy zdarzeniami następującymi w obrębie przedsiębiorstwa znacznie usprawnia praktyki klienta zdefiniowane i stworzone na podstawie ciągłego monitorowania sieci w czasie rzeczywistym oraz informacji o systemie i zdarzeniach bezpieczeństwa. Dzięki temu użytkownik może bardzo szybko ustalić, „co się dzieje” w sieci firmowej.
- Wykrywanie nieautoryzowanych usług sieciowych – Wykrywanie niedozwolonych usług wykorzystujących „otwarte ścieżki” w zabezpieczeniach sieci umożliwia klientom zamknięcie dróg dostępu do sieci, które mogłyby umożliwić wypływ informacji, naruszenie prywatności oraz przepływ nielegalnych treści przez sieć przedsiębiorstwa.
- Wdrożenie listy obserwacyjnej – analiza zdarzeń i ostrzeżeń o określonych parametrach umożliwia uzyskanie większej sprawności pracy, a także pozwala klientom na zdefiniowanie ryzyka narażenia na zagrożenia zewnętrzne i wewnętrzne ze strony przestępców identyfikowanych za pomocą adresów

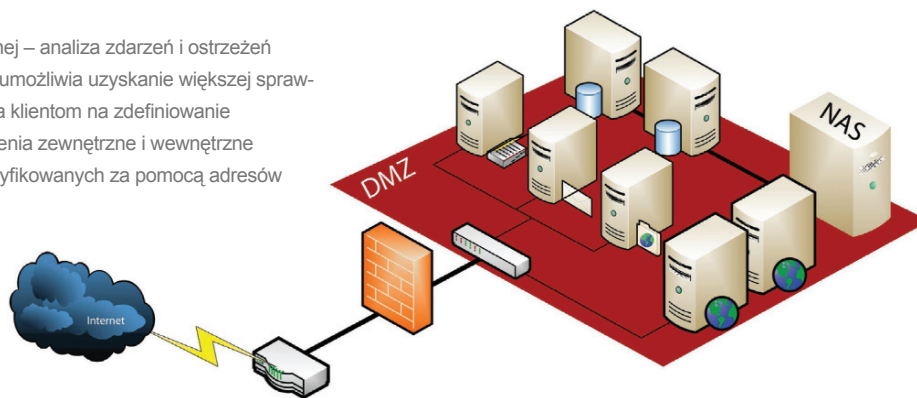
sieciowych i nazw użytkownika, atakujących określoną usługę i systemy w sieci przedsiębiorstwa.

- Skorelowane wykrywanie zagrożeń – cel zapewnienia bezpieczeństwa całej sieci przedsiębiorstwa realizowany jest poprzez zautomatyzowany proces sprawdzania sieci, bezpieczeństwa i zdarzeń systemowych pod kątem słabych punktów oraz oceny ryzyka i zagrożeń we wszystkich lokalizacjach firmy.

## O firmie RSA

RSA, oddział firmy EMC zajmujący się bezpieczeństwem – jest ekspertem w zakresie bezpieczeństwa informacji, dostarczającym rozwiązania umożliwiające ochronę informacji przez cały czas jej istnienia. RSA umożliwia klientom opłacalne zabezpieczenie ważnych zbiorów informacji oraz tożsamości online bez względu na to, gdzie mieszkają i dokąd się przemieszczają, a także zarządzanie informacjami dotyczącymi bezpieczeństwa i zdarzeniami, co ułatwia dostosowanie się do wymogów zgodności.

RSA udostępnia najlepsze w branży rozwiązania z zakresu zabezpieczenia tożsamości i kontroli dostępu, szyfrowania i zarządzania kluczami, zarządzania informacjami dotyczącymi zgodności i bezpieczeństwa oraz zabezpieczenia przed oszustwami. Dzięki tym rozwiązaniom tożsamości milionów użytkowników cieszą się zaufaniem, podobnie jak realizowane przez nich transakcje oraz generowane dane. Więcej informacji znajdą Państwo na stronach: [www.RSA.com](http://www.RSA.com) oraz [www.EMC.com](http://www.EMC.com)



RSA Security Inc.  
RSA Security Ireland Limited  
[www.rsa.com](http://www.rsa.com)

The Security Division of EMC

© 2007 RSA Security Inc. Wszelkie prawa zastrzeżone.  
RSA, RSA Security, enVision i logo RSA są zastrzeżonymi znakami towarowymi lub znakami towarowymi firmy RSA Security Inc. w Stanach Zjednoczonych i/lub innych krajach. EMC jest zastrzeżonym znakiem towarowym EMC Corporation. Wszystkie inne produkty i usługi wymienione w niniejszej publikacji są znakami towarowymi odpowiednich podmiotów.

ENVOV DS 0307