



Opis produktu

Najważniejsze informacje o platformie RSA enVision™

Zintegrowane rozwiązanie typu „3 w 1” do zarządzania dziennikami

Wprowadzenie

Analitycy – w tym specjaliści z firmy Gartner – są zgodni co do tego, że platforma RSA enVision™ jest najlepszym na rynku rozwiązaniem do zarządzania informacjami i zdarzeniami związanymi z bezpieczeństwem (ang. Security Information and Event Management – SIEM). Zintegrowany system zarządzania dziennikami – łączący w sobie funkcje trzech odrębnych produktów – upraszcza realizację wymogów ustawowych, a także podnosi poziom bezpieczeństwa i zmniejsza ryzyko. Ponadto zastosowane w nim mechanizmy automatyzujące gromadzenie, analizę, kontrolę i bezpieczne zapisywanie wszystkich dzienników oraz ostrzeganie i raportowanie na ich podstawie pozwalają zoptymalizować działanie systemów informatycznych i sieci.

Zastosowanie

Platforma RSA enVision umożliwia gromadzenie wszystkich dzienników zdarzeń generowanych przez urządzenia IP w sieci użytkownika, trwałe archiwizowanie kopii danych, przetwarzanie dzienników w czasie rzeczywistym oraz generowanie ostrzeżeń w przypadku wykrycia podejrzanych wzorców zachowań. Korzystając z intuicyjnego panelu kontrolnego, administratorzy mogą badać wszystkie przechowywane dane, a zaawansowane oprogramowanie analityczne pozwala przekształcić złożoną, nieusystematyzowaną masę nieprzetworzonych danych w czytelne informacje. W ten sposób produkt dostarcza administratorom praktycznych wskazówek, które można wykorzystać w trzech podstawowych obszarach opisanych poniżej.

Uproszczenie realizacji wymogów ustawowych. Administratorzy mogą automatycznie gromadzić zawarte w dziennikach dane dotyczące aktywności sieci, plików, aplikacji oraz użytkowników, co znacznie upraszcza spełnianie wymogów ustawowych. Dostępnych jest przy tym ponad 1100 raportów dostosowanych do wymagań konkretnych, aktualnie obowiązujących przepisów. Oprócz tego opisywane rozwiązanie ułatwia przestrzeganie wymagań ustaw, które zostaną uchwalone w przyszłości, ponieważ pozwala przechowywać wszystkie dane z dzienników bez filtrowania bądź normalizacji, a także chroni je przed manipulacją – zapewniając w ten sposób weryfikowalne, rzetelne źródło danych archiwalnych.

Podnoszenie poziomu bezpieczeństwa i zmniejszanie ryzyka. Platforma umożliwia przekazywanie w czasie rzeczywistym ostrzeżeń o zdarzeniach związanych z bezpieczeństwem, a także oferuje funkcje monitorowania i szczegółowej analizy danych zapewniające przejrzysty dostęp do ważnych informacji. Widząc i rozumiejąc występujące zagrożenia i czynniki ryzyka, administratorzy mogą następnie podejmować skuteczniejsze działania zaradcze.

Optymalizacja działania systemów informatycznych i sieci.

Dane zawarte w dziennikach, które są objęte zarządzaniem, stanowią najlepsze źródło informacji o wydajności działania infrastruktury oraz zachowaniach użytkowników. Informatycy odpowiedzialni za pomoc techniczną mogą wykorzystać platformę RSA enVision do obserwowania dzienników dotyczących aktywności serwerów, urządzeń sieciowych i platform pamięci masowej oraz zarządzania nimi, a także do monitorowania zasobów sieciowych oraz dostępności i statusu osób, urządzeń i aplikacji w firmie. Ponadto platforma oferuje inteligentne narzędzia analityczne pozwalające rozwiązywać problemy z infrastrukturą i chronić jej zasoby, ułatwia kierownikom działów informatycznych wykonywanie obowiązków związanych z pomocą techniczną oraz zapewnia precyzyjny wgląd w określone zachowania użytkowników.

Sposób działania

Platforma RSA enVision umożliwia jednocześnie pobieranie dzienników z dziesiątek tysięcy urządzeń – w tym serwerów z systemem Windows®, zapór Check Point® i routerów Cisco® – bez konieczności instalowania agentów programowych działających po stronie klienta. Dzięki temu przez cały czas gromadzone są wszystkie dane – zgodnie z modelem All the Data™. Korzystając z funkcji ustalania punktów odniesienia, analizy tendencji oraz raportowania, administratorzy systemów informatycznych i sieci mogą tworzyć długoterminowe, graficzne odwzorowania zdarzeń związanych z wydajnością i bezpieczeństwem, co pozwala usprawnić planowanie i zmniejszyć nakłady pracy. Platformę można wdrożyć jako autonomiczne, gotowe do natychmiastowego użytku rozwiązanie lub w ramach skalowalnej architektury rozproszonej o dużej dostępności, która jest w stanie sprostać wymaganiom nawet największych sieci korporacyjnych. Bez względu na wybrany wariant wszelkie niezbędne oprogramowanie jest dostarczane bez dodatkowych opłat.

Internetowe mechanizmy zarządzania oraz wysoce inteligentne narzędzie analityczne RSA enVision Event Explorer™ umożliwiają intuicyjne sterowanie systemem oraz wykonywanie rozszerzonych, szczegółowych i dogłębnych analiz na potrzeby prowadzonych dochodzeń. W przypadku wdrożenia wariantu autonomicznego (przy użyciu produktów z serii ES) jedno samodzielne urządzenie jednofunkcyjne o podwyższonym poziomie bezpieczeństwa wykonuje wszystkie niezbędne operacje, takie jak gromadzenie, analiza i przechowywanie danych oraz zarządzanie nimi. Z kolei w wariantcie architektury rozproszonej (seria LS) instaluje się – zależnie od potrzeb – wiele wyspecjalizowanych urządzeń jednofunkcyjnych służących do realizacji kluczowych zadań. W takim przypadku do gromadzenia danych wykorzystuje się lokalne i zdalne kolektory, do zarządzania danymi stosuje się serwery danych, a do wykonywania analiz i raportowania – serwery aplikacji. Same dane można przechowywać przy użyciu urządzeń pamięci masowej podłączanych bezpośrednio, dostępnych w czasie rzeczywistym lub zbliżonym do rzeczywistego lub w trybie bez połączenia dostępnych w ofercie firmy EMC.



The Security Division of EMC

Dostępne opcje

Dostępna jest cała gama urządzeń jednofunkcyjnych z serii ES i LS. Wszystkie te urządzenia są oparte na tej samej platformie, a opcje licencjonowania są dostosowane do indywidualnych potrzeb przedsiębiorstw. Aby wybrać najbardziej odpowiedni produkt, należy kierować się liczbą urządzeń sieciowych wymagających monitorowania oraz liczbą zdarzeń przetwarzanych w ciągu sekundy.

Seria ES		ES 560	ES 1060	ES 2560	ES 5060	ES 7560
Opis		Autonomiczne urządzenie SIEM	Autonomiczne urządzenie SIEM	Autonomiczne urządzenie SIEM	Autonomiczne urządzenie SIEM	Autonomiczne urządzenie SIEM
Liczba zdarzeń na sekundę (długotrwała)		500 zdarzeń na sekundę	1000 zdarzeń na sekundę	2500 zdarzeń na sekundę	5000 zdarzeń na sekundę	7500 zdarzeń na sekundę
Maksymalna liczba obsługiwanych urządzeń		100	200	400	750	1250
Liczba jednocześnie pracujących użytkowników platformy RSA enVision		6	8	10	12	14
Liczba jednocześnie pracujących użytkowników narzędzia Event Explorer (w pakiecie/maksymalna)		1/5	2/5	3/5	4/5	5/5
Pamięć masowa		Wewnętrzna, 300 GB	Wewnętrzna, 300 GB	Wewnętrzna, 300 GB	Wymagana zewnętrzna pamięć masowa	Wymagana zewnętrzna pamięć masowa
Seria LS	LS A60	LS D60	LS L605	LS L610	LS R601	LS R602
Opis	Urządzenie jednofunkcyjne – serwer aplikacji	Urządzenie jednofunkcyjne – serwer bazy danych	Urządzenie jednofunkcyjne – kolektor lokalny	Urządzenie jednofunkcyjne – kolektor lokalny	Urządzenie jednofunkcyjne – kolektor zdalny	Urządzenie jednofunkcyjne – kolektor zdalny
Liczba zdarzeń na sekundę (długotrwała)	Nie dotyczy	30 000 zdarzeń na sekundę	5000 zdarzeń na sekundę	10 000 zdarzeń na sekundę	1000 zdarzeń na sekundę	2000 zdarzeń na sekundę
Maksymalna liczba obsługiwanych urządzeń	Nie dotyczy	3072/6144*	1500	2048	512	1024
Liczba jednocześnie pracujących użytkowników platformy RSA enVision	16	Nie dotyczy	Nie dotyczy	Nie dotyczy	Nie dotyczy	Nie dotyczy
Liczba jednocześnie pracujących użytkowników narzędzia Event Explorer (w pakiecie/maksymalna)	5/15	Nie dotyczy	Nie dotyczy	Nie dotyczy	Nie dotyczy	Nie dotyczy
Pamięć masowa	RSA enVision NAS3500					

Dane techniczne produktu

ŚRODOWISKO PRACY

Wbudowany system Microsoft Windows 2003 Server o podwyższonym poziomie bezpieczeństwa (standard)

Nadmiarowe podzespoły sprzętowe

ES: pamięć RAM z funkcją ECC

LS: 8 GB pamięci RAM z pełnym buforowaniem

ES/LS: nadmiarowe wentylatory, zasilacze i dyski w macierzy RAID-1 wymieniane podczas pracy

MONITOROWANIE WARUNKÓW PRACY, ZARZĄDZANIE

Zarządzanie pozapasmowe zgodnie ze standardem IPMI 2.0, 100-procentowe zdalne zarządzanie urządzeniami jednofunkcyjnymi w trybie „headless” (bez obsługi urządzeń peryferyjnych)

SIĘĆ

ES: 2 porty Ethernet 10/100/1000TX w pakiecie, maksymalnie 6 portów przy użyciu dodatkowych kart sieciowych

LS: 6 portów Ethernet 10/100/1000TX

OPCJE PAMIĘCI MASOWEJ

Pamięć podłączana bezpośrednio o użytecznej pojemności 2,75 TB (patrz dane urządzenia RSA enVision DAS2000)

Pamięć sieciowa o użytecznej pojemności od 3,5 do 7 TB (patrz dane urządzenia RSA enVision NAS3500)

ATESTY I ŚWIADECTWA ZGODNOŚCI

Certyfikat ISO9002, UL1950, CSA22.2 nr 950, EN 60950, FCC część 15 (klasa A), ICES-003 EN55024:1998, EIN55022:1998, EN50082-1, VCCI V-3/2000.4, AS/NZS3548

OPROGRAMOWANIE APLIKACYJNE

Platforma RSA enVision z bazą danych RSA enVision LogSmart™ IPDB; szeregowa korelacja w czasie rzeczywistym z automatyczną oceną zagrożeń; uniwersalna obsługa urządzeń; ponad 1100 standardowych raportów i pełny kreator raportów; zaawansowane narzędzie do wizualizacji i analizy dochodzeniowej Event Explorer; ochrona informacji przez cały cykl życia; zarządzanie regułami przechowywania danych; obsługa wielowarstwowej pamięci masowej

OPCJE ZASILANIA

Nadmiarowe zasilacze o mocy 400 W z wyrównywaniem obciążenia, automatyczne wykrywanie napięcia 120/240 V

WYMIARY

744 x 445 x 86 mm (dł. x szer. x wys.)

Dołączone prowadnice do instalacji w szelaku (wymagany szelak na 4 podporach)

Waga: 24,5 kg

GWARANCJA

90-dniowa gwarancja na sprzęt z możliwością przedłużenia do 5 lat w ramach umowy serwisowej



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

The Security Division of EMC

©2008 RSA Security Inc. Wszelkie prawa zastrzeżone. Nazwy RSA i enVision, hasło „All the Data”, nazwa Event Explorer i logo RSA są znakami towarowymi lub zastrzeżonymi znakami towarowymi firmy RSA Security Inc. w Stanach Zjednoczonych i/lub innych krajach. Nazwa EMC jest zastrzeżonym znakiem towarowym firmy EMC Corporation. Wszelkie pozostałe nazwy produktów i usług wymienione w niniejszym dokumencie są znakami towarowymi odpowiednich podmiotów.