



Charakterystyka produktu

RSA enVision® Mid Market

Kompleksowe rozwiązanie do zarządzania dziennikami zdarzeń dla sektora średnich przedsiębiorstw

Wprowadzenie

Platforma RSA enVision® Mid Market jest rozwiązaniem przeznaczonym na rynki Europy Wschodniej w dziedzinie zarządzania informacjami związanymi z bezpieczeństwem i zdarzeniami (ang. *Security Information and Event Management* – SIEM). Oferuje przedsiębiorstwom zintegrowany system zarządzania dziennikami zdarzeń, który upraszcza realizację wymogów prawnych odnośnie do przechowywania informacji związanej z bezpieczeństwem, a także podnosi poziom bezpieczeństwa i zmniejsza ryzyko. Ponadto zastosowane w rozwiązaniu mechanizmy automatyzujące gromadzenie, analizę, kontrolę i bezpieczne przechowywanie dzienników oraz ostrzeganie i raportowanie na ich podstawie pozwalają zoptymalizować działanie systemów informatycznych i sieci.

Zastosowanie

Przedsiębiorstwa średniej wielkości stają wobec tych samych wyzwań w zakresie bezpieczeństwa, które dotyczą ich większych odpowiedników, jednak często brakuje im odpowiednich zasobów do opracowania skutecznych procesów zapobiegawczych oraz budżetu, aby inwestować w najnowsze technologie. Dodatkowo wiele takich przedsiębiorstw jest zmuszonych do podejmowania olbrzymiego wysiłku związanego ze stałym przestrzeganiem zmieniających się wymagań prawnych, co zmniejsza ilość czasu poświęcanego na rozwijanie przedsięwzięć bezpieczeństwa.

Platforma RSA enVision Mid Market 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 prawnych. Administratorzy mogą automatycznie gromadzić zawarte w dziennikach dane dotyczące aktywności sieci, plików, aplikacji oraz użytkowników, co znacznie upraszcza spełnianie wymogów ustawowych dotyczących przechowywania informacji związanej z bezpieczeństwem. Dostępnych jest przy tym ponad 1100 raportów dostosowanych do wymagań konkretnych, aktualnie obowiązujących przepisów. Rozwiązanie ułatwia również przestrzeganie wymagań ustaw, które zostaną

uchwalone w przyszłości, ponieważ pozwala przechowywać wszystkie dane z dzienników zdarzeń 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 umożliwi 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 podejmować skuteczniejsze działania zaradcze.

Optymalizacja działania systemów informatycznych i sieci. Dane zawarte w zarządzanych dziennikach stanowią najlepsze źródło informacji o wydajności działania infrastruktury oraz zachowaniach użytkowników. Informatycy odpowiedzialni za pomoc techniczną mogą wykorzystać platformę RSA enVision do obserwowania dzienników zdarzeń 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 Mid Market umożliwia jednoczesne pobieranie dzienników z 40 urządzeń – w tym serwerów z systemem Windows®, zapór Check Point® i routerów Cisco® – bez konieczności instalowania agentów oprogramowania działających po stronie klienta. Dzięki temu stale 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.

Webowy interfejs 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. Produkty ES 160 i ES 260 w ramach platformy enVision Mid Market stanowią autonomiczne rozwiązania zapewniające samodzielne urządzenia o podwyższonym poziomie bezpieczeństwa, wykonujące wszystkie niezbędne operacje, takie jak gromadzenie, analiza i przechowywanie danych oraz zarządzanie nimi. Same dane można przechowywać przy użyciu urządzeń pamięci masowej dostępnych w ofercie firmy EMC.



The Security Division of EMC

Produkty o cechach wskazanych poniżej są dostępne wyłącznie w krajach Europy Wschodniej.

Seria ES enVision Mid Market	ES-160-PROMO	ES-260-PROMO
Opis	Autonomiczne urządzenie SIEM	Autonomiczne urządzenie SIEM
Liczba zdarzeń na sekundę (długotrwała)	100	200
Maksymalna liczba obsługiwanych źródeł logów	20	40
Liczba jednocześnie pracujących użytkowników platformy RSA enVision	4	5
Liczba jednocześnie pracujących użytkowników narzędzia Event Explorer (w pakiecie/maksymalna)	5	5
Pamięć masowa	Wewnętrzna, 300 GB	Wewnętrzna, 300 GB

SKU	Opis	Cena katalogowa
ES-160 - PROMO	Urządzenie RSA enVision 160	13,000 \$
ES-260 - PROMO	Urządzenie RSA enVision 260	18,000 \$
U160P-260P-S	Aktualizacja urządzenia RSA enVision 160 na wersję 260	8,000 \$
SSP-160-12M	12-miesięczna konserwacja podstawowa urządzenia RSA enVision ES-160	2,040 \$
SSP-260-12M	12-miesięczna konserwacja podstawowa urządzenia RSA enVision ES-260	2,890 \$
PSP-160-12M	12-miesięczna konserwacja rozszerzona urządzenia RSA enVision ES-160	3,240 \$
PSP-260-12M	12-miesięczna konserwacja rozszerzona urządzenia RSA enVision ES-260	4,590 \$

Dane techniczne produktu

ŚRODOWISKO PRACY

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

Nadmiarowe podzespoły sprzętowe

ES: Chroniona pamięć RAM z funkcją ECC

ES: Nadmiarowe wentylatory, zasilacze i dyski w macierzy RAID-1 podłączane w trakcie pracy

MONITOROWANIE WARUNKÓW PRACY I ZARZĄDZANIE

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

SIEĆ

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

OPCJE PAMIĘCI MASOWEJ

Wewnętrzna, 300 GB

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 kompletny 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

74,4 × 44,5 × 8,6 cm (dł. × szer. × wys.)

Dołączone prowadnice do instalacji w stelażu (wymagany stelaż na czterech podporach).

GWARANCJA

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



ARROW ENTERPRISE COMPUTING SOLUTIONS

Autoryzowany Dystrybutor rozwiązań RSA The Security Division of EMC w Polsce:
Arrow ECS Sp. z o.o.
ul. Stawowa 119, 31-346 Kraków,
www.arrowecs.pl,
tel. +48 12 616 43 00