Начальное представление о платформе RSA enVision™

RSA®
The Security Division of EMC

Что это такое?

Аналитики, включая Gartner Group, соглашаются с тем, что платформа RSA enVision™ является лидирующим решением на рынке продуктов управления информационной безопасностью (Security Information and Event Management - SIEM). Продукт представляет собой аппаратно-программное решение с функционалом «три в одном», который:

- Собирает и обрабатывает журнальные файлы со всех сетевых устройств, включая серверы и устройства хранения
- Упрощает соблюдение отраслевых нормативных требований за счет автоматизации мониторинга, аудита и отчетности
- Повышает безопасность и снижает риски за счет оповещения об инцидентах в реальном времени и возможности проведения их дальнейшего расследования.

Назначение

Платформа RSA enVision™ обеспечивает сбор всех журнальных файлов со всех IP-устройств вашей сети: межсетевых экранов, маршрутизаторов, серверов, систем хранения данных и т.п.
Она обрабатывает эту информацию в режиме реального времени, предупреждает администратора о случаях аномального поведения пользователей или устройств, и при этом постоянно архивирует всю собранную информацию для последующего использования.
Администраторы через интуитивно понятную инструментальную панель могут делать запросы ко всему объему сохраненных данных, чтобы всегда иметь представление о том, «Кто в сети делал Что, Когда, Откуда, Где с Чем». Развитое аналитическое программное обеспечение преобразует совокупную массу неструктурированных исходных данных в структурированную информацию, формализуя происходящее с целью помочь администраторам в трех главных областях:
Управление журнальными файлами. Для администратора журнальные файлы- лучший источник информации о сетевой производительности и безопасности. Современные сетевые устройства вырабатывают их тысячами в самых разнообразных форматах, что делает ручную обработку крайне затруднительной. Другие решения по управлению журнальными файлами требуют установки и обслуживания специального программного обеспечения (агентов) на каждом сетевом устройстве. Платформа RSA enVision™ позволяет извлекать журнальные файлы одновременно из десятков тысяч устройств, включая Windows-серверы, межсетевые экраны Checkpoint и маршрутизаторы Cisco без установки на них агентов, что гарантирует непрерывность и полноту сбора данных. В то же время набор функциональных возможностей по мониторингу базовых уровней, тенденций, а также генераторы отчетов предоставляют администраторам ретроспективные (в том числе графические) обзоры касательно событий сетевой производительности и безопасности, чем достигается двойной эффект - улучшается эффективность планирования и при этом снижается трудоемкость данного процесса.
Упрощение соблюдения отраслевых нормативов. При помощи платформы RSA enVision™ можно собирать данные о сети, файле, приложении и активности пользователя, что может помочь в подтверждении соответствия отраслевым нормативным требованиям. Для выполнения этих требований, enVision уже имеет более 850 встроенных отчетов. Более того, данное решение упрощает достижение соответствия новым требованиям законодательства, т.к. сохраняет полный объем данных журнальных файлов без какой-либо их фильтрации и нормализации, защищая их от искажения и предоставляя таким образом для обработки достоверный источник архивированных данных.
Усиление безопасности. Оповещение об инцидентах в реальном времени, мониторинг и возможность проведения детализированного расследования дают администраторам ясное представление о происходящем в сети. Благодаря возможности видеть и понимать, каким рискам и угрозам подвергаются пользователи, данные, сетевые ресурсы и бизнес операции они могут предпринимать более эффективные действия по снижению этих рисков.

Как это работает?

Вы можете развернуть платформу RSA enVision™ либо как автономное «plug-and play» решение, либо как часть масштабируемой отказоустойчивой распределенной архитектуры для того, чтобы соответствовать требованиям крупной корпоративной сети. Вне зависимости от выбранного решения, оно будет включать в себя все необходимое программное обеспечение без каких-либо дополнительных затрат. Администрирование через Web-интерфейс и наличие Event Explorer, нашего весьма развитого аналитического инструмента, обеспечивают функционал для интуитивного контроля и расширенного, тщательно детализированного расследования инцидентов.
При развертывании в качестве автономного решения (серия ES), один функционально полный и защищенный аппаратно-программный комплекс (АПК) делает все, включая сбор, обработку, анализ и хранение данных.
При развертывании в рамках распределенной архитектуры (серия LS), в требуемых местах устанавливаются специализированные АПК, каждый из которых выполняет свою ключевую задачу: локальные и удаленные сборщики осуществляют сбор данных, серверы данных управляют собранными данными, а прикладные серверы проводят анализ данных и генерацию отчетов. Сами данные могут храниться с использованием разнообразных решений из широкого набора систем хранения от RSA и EMC.

Какие опции возможны?

Доступные в рамках серий ES и LX варианты моделей базируются на единой аппаратной платформе, но лицензируются так, чтобы соответствовать сформулированным Вами требованиям. Для того чтобы выбрать наиболее подходящий вам вариант, оцените количество сетевых устройств, которые вы должны контролировать и количество событий в секунду, которое вам потребуется обрабатывать. Какой бы выбор вы не сделали, платформа RSA enVision™ масштабируема, надежна, проста в развертывании и обеспечивает видимый возврат вложенных в нее средств.

Серия ES		ES 560	ES 1060	ES 2560	ES 5060	ES 7560
Описание		Автономный SIEM АПК	Автономный SIEM АПК	Автономный SIEM АПК	Автономный SIEM АПК	Автономный SIEM АПК
Непрерывный поток (событий/сек.)		500	1,000	2,500	5,000	7,500
Макс. кол-во контролируемых устройств		100	200	400	750	1,250
Одновременное кол-во пользователей		6	8	10	12	14
Одновременное кол-во пользователей EventExplorer вкл./макс.		1/5	2/5	3/5	4/5	5/5
Система хранения		300 Gb внутренняя	300 Gb внутренняя	300 Gb внутренняя	Требуется внешняя	Требуется внешняя
Серия LX	LS A60	LS D60	LC L605	LS L610	LS R601	LS R602
Описание	Сервер приложений	Сервер БД	Локальный сборщик	Локальный сборщик	Удаленный сборщик	Удаленный сборщик
Непрерывный поток (событий/сек.)	-	30,000	5,000	10,000	1,000	2,000
Макс. кол-во контролируемых устройств	-	3,072	1,500	2,048	512	1.024
Одновременное кол-во пользователей	16	-	-	-	-	-
Одновременное кол-во пользователей EventExplorer вкл./макс.	5/15	-	-	-	-	-
Система хранения	Платформа RSA enVision NAS3500					

Спецификация продукта

Операционная среда

Защищенный, интегрированный Microsoft Windows 2003 Server Standard.

Аппаратное дублирование

ES: ECC RAM
LS: 8GB буферизованная RAM
ES/LS: резервные/с горячей заменой вентиляторы, источники питания и диски в конфигурации RAID-1

Мониторинг и управление аппаратурой

Интерфейс Интеллектуального Управления Платформой - IPMI 2.0

Подключение к сети

ES: 2 порта 10/100/1000TX Eth изначально, возможно расширение до 6
LS: 6 10/100/1000TX Eth портов

Стандартные опции системы хранения

iSCSI: 2.75Tb DAS2000
NAS: 3,5Tb NAS3500

Подтвержденные соответствия нормативам

ISO9002, UL1950, CSA22.2 no 950, EN 60950, FCCPart15-Class A, ISEC-003 EIN55022:1998, EN50082-1, VCCI V-3/2000.4, AS/NZS3548

Прикладное программное обеспечение

Платформа RSA enVision с LogSmart IPDB; встроенный механизм корреляции событий с автоматической пометкой угроз;
UDS - средство описания еще неизвестных платформе форматов журнальных файлов; более 800 готовых отчетов и инструментарий для их создания;
инструмент для визуализации данных и проведения разбора инцидентов Event Explorer; средства управления жизненным циклом информации (ILM) платформы RSA enVision включая защиту, управление политикой хранения и поддержку систем хранения.

Источник питания

С резервированием и распределением нагрузки, 400Вт, автоподстройка 120/240В

Размеры и Вес

2U, 74,4x44,5x8,6 (ГхШхВ), 24,5 кг, монтажные салазки в стойку прилагаются

Гарантия

90 дней на аппаратуру с расширением до 5 лет при наличии действующего контракта технической поддержки.