Платформа RSA enVision®

Обзор возможностей обеспечения безопасности

Кратко

- Позволяет видеть все угрозы безопасности по всей корпоративной сетевой информационной инфраструктуре.
- Фиксирует события информационной безопасности - на уровне сетевых устройств, систем защиты, серверных комплексов, приложений и систем хранения данных.
- Анализирует данные как в реальном времени, так и уже сохраненные в базе и предоставляет информацию в виде срезов данных и отчетов.

Назначение

Даже лучшие средства защиты периметра сети не могут предотвратить все современные внешние угрозы безопасности сети, а против внутренних угроз они практически бесполезны. Для того, чтобы действительно защитить вашу информационную инфраструктуру, Вам необходимо непрерывно и точно знать, что происходит в пределах всей вашей сети и IT-инфраструктуры.

Платформа RSA enVision® (ранее - Network Intelligence) предоставляет единственное решение по управлению информационной безопасностью (SIEM), которое позволяет видеть 100% всех угроз безопасности рамках вашей информационной инфраструктуры - от коммутаторов и маршрутизаторов до средств защиты, вычислительных ресурсов, серверов, сетевых хранилищ и приложений. Это достигается благодаря сбору ***ВСЕХ данных от всех элементов сети*** в специализированную базу данных - LogSmart Internet protocol database (IPDB) с возможностью анализа этих данных в реальном масштабе времени. Самообучаемая система анализа событий покажет Вам какие закономерности формируются в Вашей сети - соблюдается ли штатный режим или происходит что-то необычное, что позволит Вам распознавать угрозы безопасности буквально повсюду, включая удаленные площадки.

RSA®
The Security Division of EMC

Платформа RSA envision: решения по безопасности

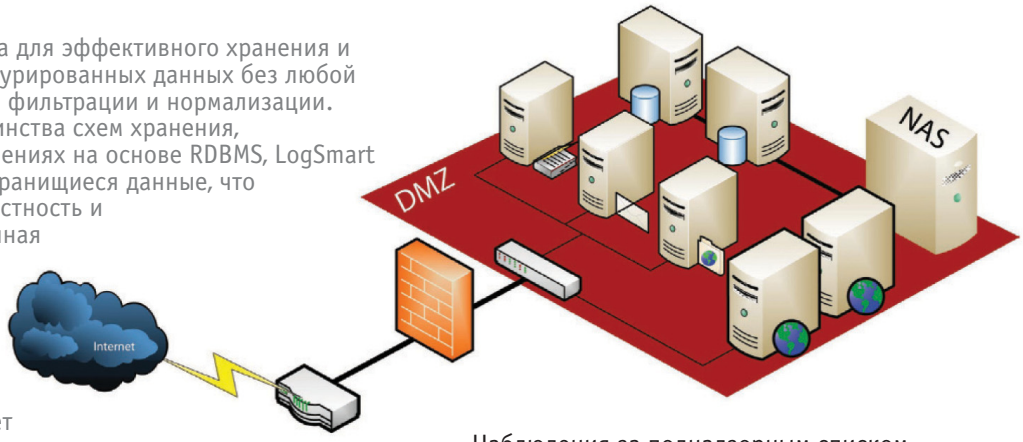
Сложность - враг безопасности. Однако сегодня большинство инфраструктур корпоративной безопасности чрезвычайно сложны и имеют в своем составе многочисленные несвязанные между собой и распределенные по сети системы ее обеспечения. Платформа RSA enVision - это именно то решение, которое позволяет в корне упростить процедуру управления безопасностью за счет консолидации, нормализации и анализа данных из этой комплексной инфраструктуры. С точки зрения администраторов и владельцев информации, это существенно улучшает эффективность обеспечения безопасности, так как они могут быстрее реагировать на внешние угрозы и раскрывать внутренние за счет получения средства унифицированного и всестороннего наблюдения за своими сетями.

RSA enVision Internet Protocol Database - IPDB

Используя собственную передовую разработку - архитектуру IPDB, уже применяемую в сотнях организациях по всему миру, RSA enVision способен собирать все данные на всех уровнях информационной инфраструктуры - от сетевых устройств до приложений. Подсистема анализа LogSmart IPDB анализирует как поступающие в реальном времени, так и уже сохраненные данные и предоставляет информацию в виде срезов данных и отчетов, сделанных с учетом того, чтобы удовлетворять широкий диапазон потребностей каждого заинтересованного лица в вашей организации - от IT-департамента до департамента безопасности, от контроля соответствия политик и анализа рисков, до руководства компании.

Особенности подсистемы LogSmart IPDB состоят в том, что она не использует приложения третьих производителей, что и определяет беспрецедентное ее быстродействие, что крайне важно в сетях сложной и разветвленной архитектуры:

— Система разработана для эффективного хранения и обработки неструктурированных данных без любой их предварительной фильтрации и нормализации.
— В отличие от большинства схем хранения, используемых в решениях на основе RDBMS, LogSmart IPBD подписывает хранящиеся данные, что гарантирует их целостность и неизменность. (Полная замена этого пункта)
— Не требует установки агентов.
— Распределенная архитектура peer-to-peer обеспечивает высокую масштабируемость и производительность.



Посредством LogSmart IPDB платформа RSA enVision позволяет потребителям в корне улучшить состояние безопасности за счет:

— Усиления контроля доступа - Комплексная система ведения контроля и средства отчетности, предназначенные для реализации политик управления доступом, позволяют обеспечить незамедлительное обнаружение моментов злоупотреблений и осуществляют возможность эффективного отслеживания доступа ко всем контролируемым компонентам сетевой инфраструктуры.
— Подавления ложных срабатываний - Автоматическая корреляция обнаруженных атак на ресурсы сети с информацией об имеющихся уязвимостях значительно снижает стоимость обслуживания инцидентов и дает возможность сконцентрировать основные ресурсы анализа безопасности на действительно значимых событиях.
— Мониторинга реального времени - Унифицированное представление взаимосвязи событий, обнаруживаемых в рамках корпоративной сети, значительно расширяет оперативную деятельность в отношении непрерывного мониторинга в реальном времени сетевой и системной информации, а также информации относящейся к вопросам обеспечения безопасности. Пользователи системы получают реальную возможность незамедлительно определять, что в действительности происходит в пределах их корпоративной сети.
— Обнаружения неавторизованных сетевых служб - Обнаружение незарегистрированных сервисов, которые используют "открытые ходы" через сетевую защиту, предоставляет пользователям системы возможность закрыть тот сетевой доступ, который в противном случае привел бы к утечке информации, нарушению конфиденциальности и передаче нежелательного контента за пределы корпоративной сети.
— Наблюдения за поднадзорным списком - параметризованный анализ событий и сигналов предупреждения об угрозах обеспечивает высокую оперативную результативность и позволяет пользователям системы оценивать свои риски по отношению к злоумышленникам, которые идентифицируются сетевыми адресами и именами пользователей, явно нацеленным на определенные сервисы и системы корпоративной сети.
— Коррелированного обнаружения угрозы - задачей обеспечения всеобъемющей корпоративной безопасности становится понимание состояния защищенности с точки зрения уязвимостей, угроз и рисков, которое формируется в результате автоматизированного сбора информации о процессах, происходящих в сети, событиях безопасности и системных событиях во всех сегментах корпоративной сети.

Об RSA

RSA, подразделение Информационной Безопасности корпорации EMC, являеется одной из ведущих организаций в области разработки систем обеспечения безопасности информации на протяжении всего ее жизненного цикла. Продукция RSA предназначена для эффективной защиты ценных данных и идентификационной информации пользователей, где бы они ни были, на каждом этапе взаимодействия с информационной системой.
RSA предлагает самые передовые в отрасли решения по аутентификации и контролю доступа, шифрованию и управлению ключами, соответствию отраслевым стандартам и управлению безопасностью, а также защите от мошенничества. Эти решения создают платформу доверия для миллионов пользователей, позволяют осуществлять безопасные транзакции и обеспечивают сохранность данных.
Дополнительную информацию Вы сможете найти на сайтах www.RSA.com и www.EMC.com

В России - представительство Корпорации EMC:
5-й этаж, БЦ "Северное Сияние",
ул. Правды, 26, Москва
Тел.:+7 495 648-9595
Факс:+7 495 648-9597
Website: http://russia.emc.com/

RSA®
The Security Division of EMC