Описание продукта RSA

RSA® Data Loss Prevention Network

Комплексная система предотвращения утечки важной информации в процессе передачи данных

Краткий обзор

- Оценка риска выхода значимых данных за пределы предприятия
- Мониторинг, аудит, шифрование или блокирование несанкционированной передачи значимых данных в реальном времени
- Высокий уровень точности, позволяющий снизить риски и ССВ благодаря применению расширенной библиотеки политик и классификаций, обеспечивающей защиту значимых данных
- Использование преимуществ централизованного управления политиками для упрощения внедрения и текущего администрирования решения

Общий обзор

Работа современного предприятия в значительной степени зависит от координации действий с партнерами, заказчиками и т.п., а также сопровождается пересылкой больших объемов цифровой информации по электронной почте, через системы мгновенной доставки сообщений и другие внутренние и внешние сетевые приложения. Значительная часть этих данных может иметь конфиденциальный характер, и их раскрытие посторонним лицам влечет за собой определенный коммерческий риск. Для предотвращения утечки информации и обеспечения защищенного обмена коммерческой информацией необходимо контролировать и блокировать как случайные, так и злонамеренные попытки несанкционированной передачи данных.

RSA®
The Security Division of EMC

Система RSA Data Loss Prevention (DLP) Network входит в состав RSA DLP Suite и представляет собой комплексное решение по предотвращению утечки данных, передаваемых по вычислительной сети средствами корпоративной электронной почты (SMTP), Веб-почты или других веб-приложений (HTTP или HTTPS), системы мгновенных сообщений, FTP-серверов, а также любых универсальных протоколов на базе TCP/IP. Система не только распознает важную информацию путем анализа передаваемого контента, но и помогает предотвратить ее утечку с помощью блокирования или шифрования данных в соответствии с установленной политикой безопасности.

Высокий уровень точности

Важные данные, подпадающая под нарушение установленной политики, должны расцениваться как угроза безопасности и подвергаться корректировке. Традиционные решения, не обладающие высоким уровнем точности, имеют высокий уровень ложных срабатываний (например, путают случайное пятнадцатизначное число с номером кредитной карты). Такое неточное профилирование риска не только увеличивает совокупную стоимость владения, но и со временем снижает доверие к подобным решениям. Ложные тревоги вызывают необходимость проведения мероприятий по устранению несуществующих рисков, что в итоге приводит к чрезмерному росту расходов на обеспечение безопасности и средства ИТ.

Система RSA Data Loss Prevention Network обеспечивает исключительно высокую точность распознавания следующих важных данных: персональные данные (PII), данные индустрии платежных карт (PCI) и данные об интеллектуальной собственности. Высокий уровень точности достигается за счет применения предопределенных шаблонов классификации, контрольных сумм (отпечатков), или комбинацией обоих методов. Сложные алгоритмы обнаружения используют четкие правила выявления важных данных по предварительно определенным шаблонам. Эти правила используются не только для анализа ключевых слов и образцов, но и для исследования контекстного размещения ключевых слов в файле. Позволяется как использовать предопределенные шаб-

Предотвращение утечки данных в вычислительной сети

Система RSA Data Loss Prevention Network осуществляет мониторинг и упреждающую блокировку передачи важных данных в реальном времени и на основе политики безопасности.

лоны политик (для данных PCI, PII, HIPAA, GLBA, SOX, исходного кода и др.), так и создавать собственные правила, для обеспечения высокого уровня точности распознавания важных данных и, в итоге, для предотвращения утечки информации. В тех случаях, когда важность данных предварительно определена, организация может использовать технологию отпечатков, - создание сигнатур и их регистрация в DLP-системе, - для создания классификационных политик. Система DLP может снимать отпечатки с файлов в папках или с данных БД и отслеживать их полное или частичное совпадение при сканировании центра хранения и обработки.

Производительность и централизованное управление

Традиционные системы, осуществляющие мониторинг передаваемых по сети важных данных часто просто не рассчитаны на информационные нагрузки предприятия. Применение большинства современных систем контроля влечет замедление сетевого трафикаи представляет собой серьезную проблему. Система RSA DLP Network рассчитана на обеспечение высокоскоростного контроля и анализа данных без ущерба для точности идостоверности их распознавания. Она основана на архитектуре резервирования с высокой отказоустойчивостью, использующей преимущества рассредоточенного развертывания на выходных точках сети. Это гарантирует бесперебойный контроль, коррекцию и регистрацию всех случаев нарушения политики безопасности для всех выходящих за пределы сети значимых данных.

Централизованное управле-ние политиками облегчает развертывание и администрирование системынезависимо от географического расположения локальных сетей. Администраторы могут из единого центра настраивать шаблоны политик, запускать блокирование или другие механизмы управления, снижая затраты времени на внедрение и совокупную стоимость владения.

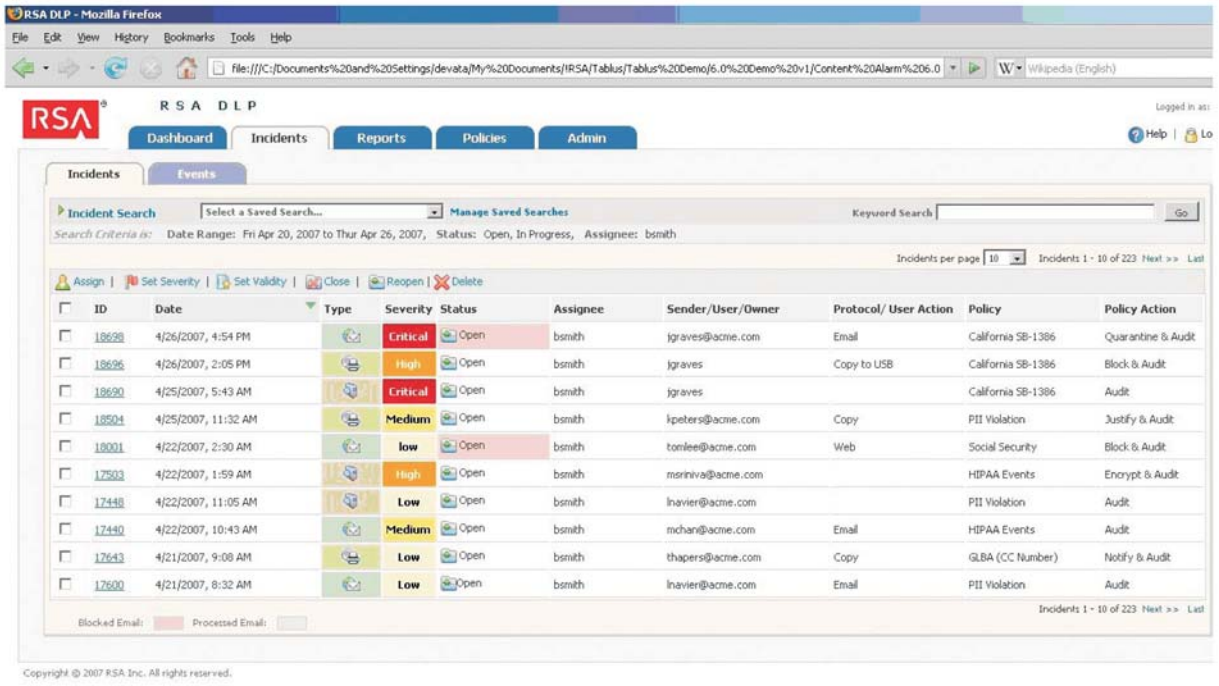
Мониторинг, блокирование и защита от несанкционированной передачи важных данных

Для снижения риска утечки важных данных традиционные методы защиты предусматривают простое блокирование всей передачи данных с помощью протоколов FTP, IM или IMAP. Подобный подход снижает эффективность работы предприятия и не обеспечивает защиты данных, передаваемых разрешенными способами, например, через корпоративную электронную почту.

Система RSA DLP Network контролирует сетевой трафик даже самой загруженной корпоративной сети в реальном времени, выявляя относительную важность данных и анализируя уровень риска. Благодаря всесторонней поддержке популярных протоколов сетевой передачи данных (SMTP, HTTP, FTP и др.) система RSA DLP Network может использоваться как в режиме простого контроля, так и в режиме контроля с противодействием. В режиме простого контроля она анализирует передаваемые по сети данные, выявляет среди них важные и сообщает об этом специалистам по безопасности. В режиме контроля с противодействием система не только выявляет важные данные, но и на основе политик безопасности осуществляет определенные действия (например, блокирование или помещение на карантин). В целях дальнейшего повышения степени защиты систему можно объединить со средствами шифрования электронной почты, что позволяет шифровать важные данные перед их отправкой за пределы корпоративной сети.

"63% респондентов сообщили о том, что они хотя бы иногда отправляют рабочие документы на свои личные адреса электронной почты, чтобы работать с ними из дома".

Уличный опрос на тему внутренних угроз.
RSA, The Security Division of EMC.



Контроль происшествий и отчетность

После выявления значимых данных система запускает процесс отслеживания событий для контроля и регистрации передаваемых данных, относящихся к группе риска. Она ведет контрольные записи событий и может автоматически рассылать по электронной почте предупреждения определенному кругу заинтересованных лиц. Кроме того, события системы DLP могут быть переправлены платформе RSA enVision® для упрощения процессов идентификации рисков по всей информационной инфраструктуре за счет использования операционной консоли безопасности платформы RSA enVision. Такие средства управления, как блокирование, шифрование, помещение на карантин или аудит могут применяться к передаваемым важным данным автоматически в соответствии с корпоративной политикой.

Описание	Поддерживаемые системы	Преимущества
Средства и протоколы передачи данных	– Вся корпоративная электронная почта (SMTP) – Вся интернет-почта (POP, IMAP и т.д.) – FTP и IM/Chat – Универсальные протоколы TCP/IP, в т.ч. HTTP и HTTPS	– Снижение риска за счет поддержки большего числа источников данных
Поддерживаемые действия	– Контроль, аудит/регистрация – Блокирование – Шифрование	– Усиление контроля за передачей значимой информации – Предотвращение несанкционированной передачи важных данных
Поддерживаемые нормативные данные (более 150 предопределенных шаблонов политик)	– Данные индустрии платежных карт (PCI) – Персональные данные (PII) – Закон о передаче и защите данных учреждений здравоохранения (HIPAA) – Закон Грэма-Лича-Блайли (GLBA) – Закон Сарбейнса-Оксли (SOX) – Стандарты калькуляции себестоимости CASB 1386, CA AB-1298 – Североамериканский Совет по надежности электротехники (NERC) – Международный номер банковского счета (IBAN) – Около 50 прочих нормативных документов для Северной Америки, Европы, Австралии и Азии	– Помощь в соответствии нормативным требованиям – Снижение риска судебных штрафов – Защита конфиденциальной информации клиентов – Снижение затрат, связанных с утечкой данных
Прочие поддерживаемые данные	– Интеллектуальная собственность: исходный код, копии чертежей и т.п. – Бизнес-стратегия и операционные данные: цены, конкурентный анализ, информация о слияниях и поглощениях – Проектная документация в формате CATIA	– Помощь в предотвращении групповых исков – Снижение риска потери конкурентного преимущества – Помощь в предотвращении потери доходов – Защита ценности бренда – Защита корпоративной интеллектуальной собственности

Комплексная система предотвращения утечки данных

Пакет RSA Data Loss Prevention Suite (модули Network, Datacenter и Endpoint) представляет собой комплексное решение по предотвращению утечки данных и позволяет осуществлять выявление, мониторинг и защиту значимых данных от утечки или несанкционированного использования как в центре обработки данных, так и в сети или на рабочем месте.

О компании RSA

Компания RSA, входящая в состав корпорации EMC, является ведущим разработчиком систем безопасности для повышения эффективности бизнеса и оказывает помощь лидерам глобального рынка в решении сложнейших задач в сфере обеспечения безопасности. Решения RSA обеспечивают целостность и конфиденциальность информации на протяжении всего ее жизненного цикла независимо от того, где она находится, кто с ней работает или каким образом она используется.

Компания RSA предлагает ведущие отраслевые решения по идентификации и контролю доступа, управлению шифрами и ключами защиты, обеспечению соответствия стандартам и управлению информацией по вопросам безопасности, а также решения по защите от мошенничества. Эти решения применяются для защиты персональных данных миллионов пользователей, сведений о выполняемых ими операциях и данных, создаваемых в результате этих операций. Дополнительная информация приведена на сайтах www.RSA.com и www.EMC.com.

RSA®
The Security Division of EMC

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

DLPNET DS0409