Краткий обзор продукта

Система RSA® Data Loss Prevention Datacenter

Выявление и активная защита конфиденциальной информации в центрах сбора и хранения данных

Краткий обзор

- Систематизирует риск на основании выявления и анализа конфиденциальных данных в файлах общего доступа, сетевых системах хранения SAN/NAS, в базах данных и иных информационных системах;
- Избирательно точно снижает риски и, как следствие, снижает TCO за счет использования распределенной политики и библиотеки классификации, настроенных на защиту важных данных;
- Легко масштабируется за счет использования распределенной архитектуры, позволяющей быстро сканировать данные с минимальными аппаратными и организационными затратами.
- Управляет конфиденциальными данными с помощью таких действий, как перемещение, помещение на карантин, удаление и присвоение цифровых меток доступа (eDRM);
- Использует централизованное управление политиками для упрощения, как внедрения, так и последующего обслуживания.

Общий обзор

Объем данных в центрах хранения и обработки данных предприятий фактически удваивается каждый год. Эти данные могут включать в себя номера социального страхования клиентов или информацию по кредитным картам, которая регламентируется определенными нормативными актами. Часть этих данных может содержать объекты интеллектуальной собственности и планы запуска продуктов, которые имеют критическое значение для коммерческой деятельности компании. Потому для каждого важно понимать, где следует хранить подобную конфиденциальную информацию и как правильно ей управлять. Однако выявление данных, подпадающих под категорию конфиденциальных, по-прежнему остается достаточно сложной задачей, поскольку объемы таких данных велики, а инструментов, которые позволили бы автоматизировать процессы их обработки с повышенной точностью и классификацией – не хватает.

RSA®
The Security Division of EMC

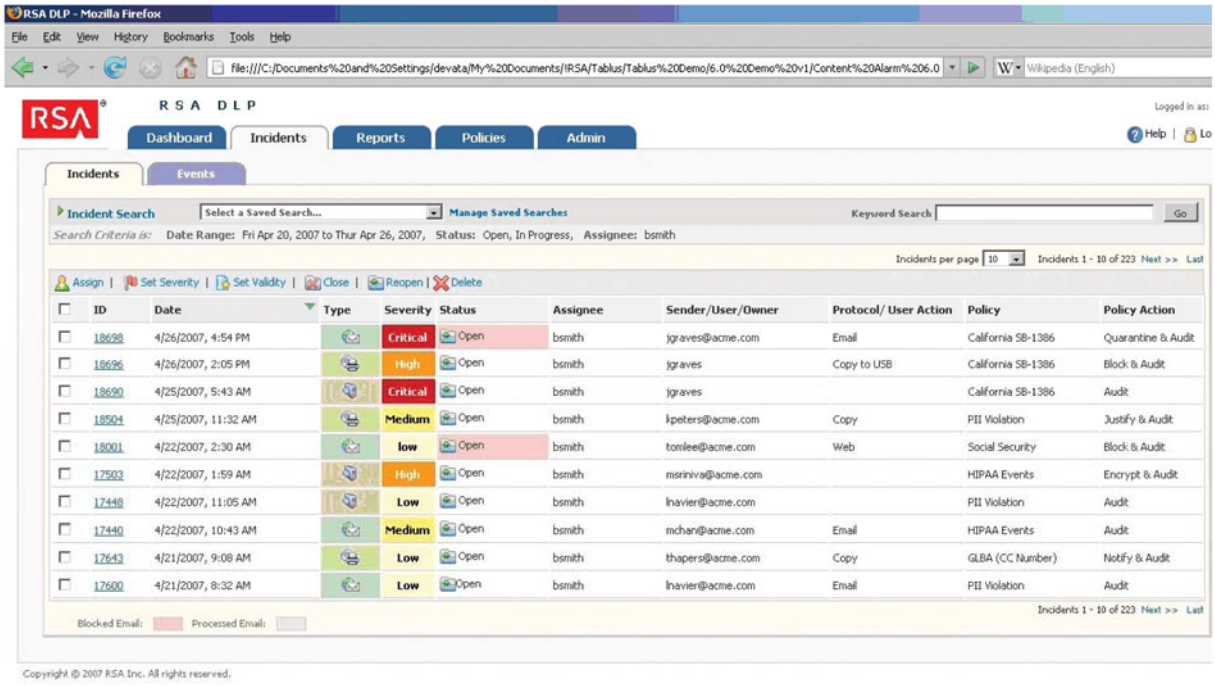
Центр предотвращения утечки информации (RSA® Data Loss Prevention (DLP) Datacenter) является частью комплексной системы RSA DLP Suite и представляет собой решение по защите от утечки информации, хранящейся в общих каталогах, базах данных, на сайтах системы SharePoint® и иных информационных системах. Предлагаемое программное решение позволяет сканировать данные с беспрецедентной скоростью и точностью, и получать готовый профиль риска для данных в точках хранения.

Определение и управление конфиденциальной информацией

Система предотвращения утечки информации RSA Data Loss Prevention Datacenter применяет передовую архитектуру, в основе которой лежит интеграция программного обеспечения в данные, а не наоборот, данных в программное обеспечение. В отличие от стандартных технологий выявления и сбора данных, когда данные из нескольких источников собираются в единый центр хранения и обработки для последующего анализа, в случае применения предлагаемой системы данные сканируются и анализируются по месту расположения. Уникальная распределенная архитектура позволяет предприятиям сканировать всю конфиденциальную информацию, которая храниться в папках общего доступа, базах данных, на сайтах системы SharePoint и в иных информационных системах без значительного повышения сетевого трафика. Более того, не требуются большие аппаратные мощности, поскольку система использует свободные циклы существующих серверов и задействует их для сканирования данных. В результате рабочее время сокращается, поскольку нагрузка сканирования автоматически выравнивается и распределяется по всем серверам, исключая необходимость ее ручного контроля специалистами ИТ. Подобный подход позволяет компании производить параллельное сканирование нескольких источников с большими объемами данных и вместе с тем сократить время сканирования от нескольких месяцев до нескольких часов. Решение изначально поставляется в комплекте с более чем со 150 шаблонами политик, позволяя максимально быстро и точно выявить важные данные.

Реакция и оповещение об инцидентах

После выявления важной информации система запускает рабочий процесс отслеживания происшествий для регистрации и мониторинга данных, подвергающихся риску. Она ведет контрольный журнал происшествий и может извещать предустановленное число лиц о наступлении какого-либо события посредством автоматической почтовой рассылки. События системы DLP так же 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 операции с данными как перемещение, помещение на карантин или цифровая разметка доступа eDRM (через интеграцию со службой Microsoft Active Directory Rights Management Services®) могут быть осуществлены автоматически в соответствии с действующей корпоративной политикой.



Высокий уровень точности

Важная информация, подпадающая под нарушение установленной политики, должна быть расценена как угроза безопасности и закрыта от НСД. Стандартные решения, не обладающие высоким уровнем точности, выявляют большие объемы незначимой информации, однако расценивая ее как значимую (например, путая случайное число из пятнадцати цифр с номером кредитной карты клиента), ведут к ложному срабатыванию системы. Неверное профилирование информации по риску не только увеличивает общую стоимость владения, связанную с покупкой и эксплуатацией дополнительного оборудования, но и со временем снижает надежность подобных решений. Подобные ложные тревоги ведут компанию к дополнительным затратам на устранение несуществующих рисков, и, в итоге, к необоснованным затратам на дополнительные аппаратные мощности, и расходам ресурсов, задействованных в обеспечении безопасности.

Система RSA Data Loss Prevention Datacenter предоставляет исключительную точность в выявлении таких важных данных как персональная информация (PII), данные платежных карт (PCI) и объектов интеллектуальной собственности. Высокий уровень точности достигается за счет применения предопределенных шаблонов классификации, контрольных сумм (отпечатков), или комбинацией обоих методов. Сложные алгоритмы обнаружения в предопределенных шаблонах используют четкие и точные правила для выявления существенной информации. Эти правила не только анализируют файл по ключевым словам и встроенным образцам, но и исследуют их контекстное размещение в файле. Компании могут использовать предустановленные шаблоны политик (в отношении данных, подпадающих под категории PCI, PII, HIPAA, GLBA, SOX, исходный код и т.д.) или создавать собственные правила для обнаружения важной информации и предотвращения ее утечки. В случаях, когда существенная информация уже определена, компании могут использовать технологию идентификации на базе отпечатков (fingerprinting) – в этих случаях данные отмечаются контрольными суммами и регистрируются в системе DLP – для создания классификационных политик информации. Система DLP может снимать отпечатки как с файлов непосредственно в папках, так и с данных из баз данных с возможностью последующего анализа полного или частичного их совпадения при сканировании центром хранения и обработки информации.

Масштабируемость и централизованное управление

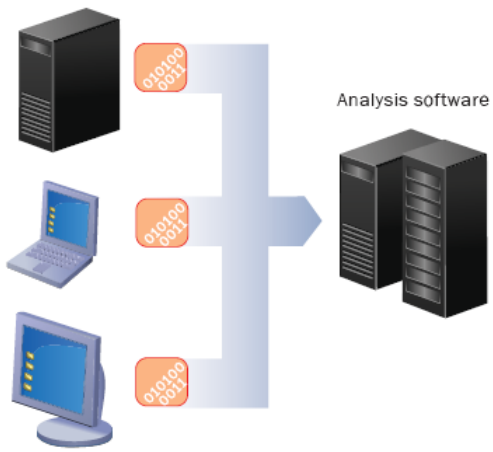
Компаниям, у которых в распоряжении находятся тысячи файловых серверов и информационных хранилищ, требуется эффективная и масштабируемая методика не только для выявления и анализа значимой информации, но и для осуществления мер по защите в отношении ее удаления и помещения на карантин. Решение RSA DLP Datacenter , как часть пакета RSA Data Loss Prevention Suite, обеспечивает унифицированную архитектуру с централизованным управлением, позволяющую упростить процесс ее внедрения и управления независимо от месторасположения данных. Администраторы могут настраивать шаблоны политик и применять политики ко всем источникам данных по всему предприятию из единого центра, облегчая компании внедрение и поддержание данного решения. Для эффективного сканирования больших объемов информации система включает в себя такие инструменты, как распределенное сканирование (Grid Scanning), - функция, которая извлекает максимум из технологии параллельной обработки за счет использования готовых серверов, сконфигурированных в кластер. Этот уникальный подход не только снижает общую стоимость владения (например, необходимость покупки дополнительного оборудования), но и увеличивает скорость сканирования не менее чем в 10 раз.

"Как и в предыдущей версии системы RSA DLP Datacenter (ранее называвшейся Tablus Content Sentinel) идентификация информационного наполнения компании происходит с высокой степенью точности. Предустановленные шаблоны Expert Content Blades выдали минимум ложных вариантов. После регистрации собственных списков клиентов и алгоритма обработки система RSA Datacenter 3.0 обнаружила все наборы важной информации".

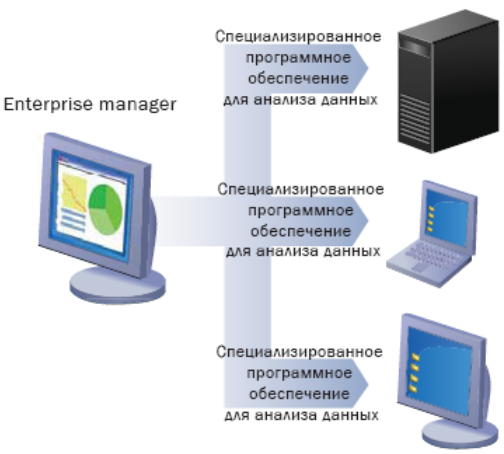
“Быстрое выявление конфиденциальной информации”
InfoWorld

Сканирование и анализ конфиденциальных данных по месту их расположения

Система обеспечивает выявление и анализ существенных данных с исключительно высокой эффективностью благодаря использованию революционной архитектуры распределенного сканирования.



Стандартный метод сканирования с единичной точкой обработки
Все данные перемещаются в одно место для последующего анализа с помощью специализированного ПО.



Метод распределенного сканирования системы RSA DLP Datacenter
Специализированное ПО анализирует данные по месту их расположения.

Система RSA Data Loss Prevention Datacenter: Особенности и преимущества

Описание	Поддерживаемые системы	Преимущества
Выявляемые объекты	- файлы с расширением систем Windows®, AIX®, HP-UX®, Solaris® - файлы систем SharePoint®, Documentum® и иных информационных хранилищ - Системы хранения данных NAS/SAN	- Снижение риска за счет поддержки большего числа источников данных
Поддерживаемые типы баз данных	- Microsoft SQL Server", Microsoft Access" - Oracle" 10g и 11g	- Снижение риска путем защиты данных, хранящихся во всей системе
Выявление официальных нормативных данных (более 150 шаблонов с предустановленными политиками безопасности)	- Индустрия платежных карточек (PCI) - Личная информация (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 регулярных соответствий для Северной Америки, Европы и Азии	- Помощь соответствию нормативным требованиям - Снижение риска судебных штрафов - Сохранение конфиденциальности информации клиентов - снижение затрат, связанных с несанкционированным доступом к данным (НСД)
Выявление неофициальных данных (внутренний конфидент)	- Интеллектуальная собственность: исходный программный код, проект 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 достоинства бренда - Защита интеллектуальной собственности

Комплексное обеспечение защиты данных от утечки

Пакет RSA Data Loss Prevention Suite (модули Network, Datacenter и Endpoint) представляет собой комплексное решение по предотвращению утечки данных и позволяет осуществлять выявление, сбор, мониторинг и защиту конфиденциальной информации от утечки или несанкционированного использования в центре обработки данных, в сети или на оконечных пользовательских системах.

"Распределенная обработка и поэтапное сканирование были особенно важны для компании Microsoft, если учесть, какие объемами информации мы обладаем. Кроме того, система RSA DLP Datacenter (ранее, называвшаяся Content Sentinel) способна определять совпадения с заданными шаблонами с точностью 98% и выше".

Олав Опедал,
Программа безопасности компании Microsoft

О компании RSA

Компания RSA является подразделением компании EMC, специализируется на решениях в сфере обеспечения информационной безопасности и выступает в качестве основного поставщика решений в сфере безопасности для улучшения бизнеса во всем мире, помогая международным компаниям добиться успеха в решении наиболее сложных и важных вопросов обеспечения безопасности и конфиденциальности. Компания RSA при работе с информацией ориентируется в первую очередь на обеспечение безопасности, защиту целостности и конфиденциальности на протяжении всего ее жизненного цикла независимо от того, куда она перемещается, кто имеет к ней доступ или каким образом она используется.

Компания RSA предлагает лучшие решения по идентификации и контролю доступа в данной области; шифрование и управление ключами; совместимость; и управление безопасностью информации и защите от мошенничества. Благодаря этим решениям растет доверие миллионов клиентов, обеспечивается безопасность выполняемых ими транзакций и генерируемых ими данных. Для более детальной информации посетите наш сайт в Интернете www.RSA.com и www.EMC.com.

RSA®
The Security Division of EMC

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

DLPCTR DS 0409