Система предотвращения утечек данных RSA DLP

Обеспечивая защиту бизнеса, ИБ-специалистам приходится постоянно отслеживать появление, перемещение и удаление конфиденциальных документов в корпоративных сетях. Цена утечки данных в современном мире может быть очень высока. В условиях постоянного роста объемов и форм представления информации контроль за движением конфиденциальных данных становится проблематичным.

«Классические» средства защиты, не поддерживающие функции анализа содержимого электронных документов, абсолютно беспомощны при решении задач предотвращения утечек конфиденциальной информации.

Для их решения нужны современные технические средства, такие как система предотвращения утечек данных RSA DLP.

Возможности системы

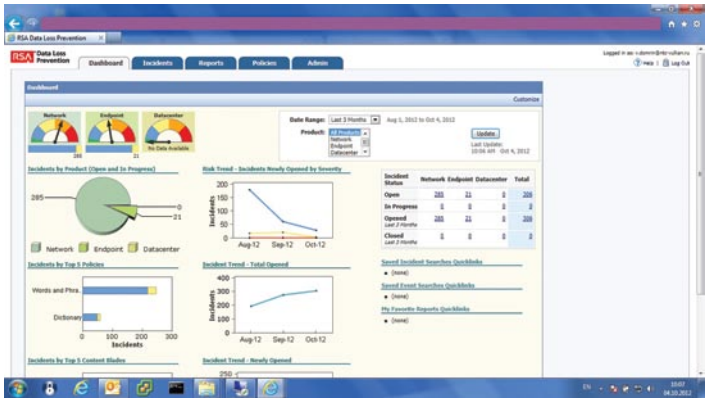
Решая задачи борьбы с утечками данных, система RSA DLP осуществляет:

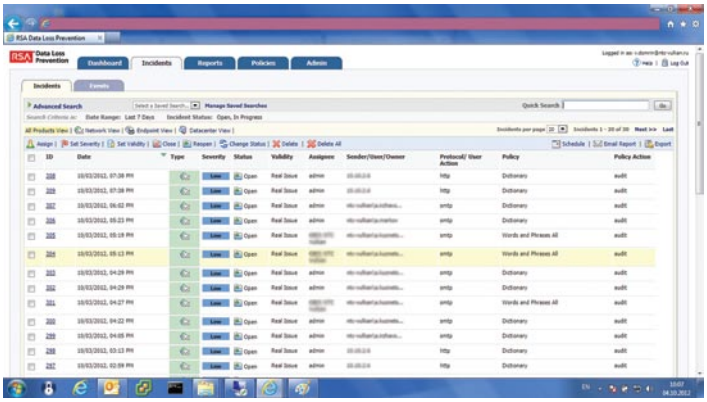
- выявление конфиденциальной информации путем сканирования каталогов общего доступа, баз данных, сайтов SharePoint, информационных систем;
- мониторинг сетевого трафика и предотвращение несанкционированной передачи конфиденциальной информации по сети;
- контроль корпоративной электронной почты;
- активную блокировку несанкционированных попыток копирования конфиденциальных данных на съемные носители, CD и DVD, внешние файловые и веб-ресурсы;
- активную блокировку печати на локальные и сетевые принтеры;
- централизованный и унифицированный контроль различных каналов утечек защищаемой информации.

Система RSA DLP поддерживает все наиболее распространенные технологии организации данных:

- форматы Office-документов (DOC, DOCX, TXT, DOCM, DOT, DOTM, DOTX, HTM, MHT, PDF, RTF, XML, XPS, ODT, WPS, XML, HTML, ODT, OTT, STW, SXW, RTF, XLS, XSLM, ODS, XLSX, XLTX, ODP, POT, POTM, POTX, PPS, PPSM, PPSX, PPTM, THMX, PPTX, EMF, WMF);
- все основные форматы схем и чертежей (DWG, DXF, DWF, CAT, VSD);
- базы данных MS SQL, Oracle и DB2;
- почтовые базыMS Exchange и Lotus Notes;
- файлы в форматах HTML, PDF, DjVu, fb2, epub.

Реакция системы RSA DLP на обнаружение нарушений установленных правил варьируется в зависимости от настроенных политик.

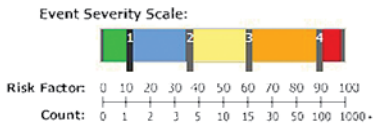


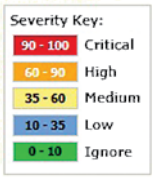


Сценарии поведения RSA DLP могут включать:

- «прозрачную» для пользователя регистрацию действий с электронными документами, в том числе создание «теневых» копий;
- Уведомление пользователя или запрос подтверждения на выполнение определенного действия с электронным документом;
- уведомление администратора безопасности;
- блокирование запрещенных действий;
- перенаправление данных, попадающих под политики, в защищенное хранилище — «карантин».

За счет использования в системе RSA DLP шкал оценок рисковых факторов возможна автоматическая оценка рисков в случае возникновения инцидентов информационной безопасности.





НТЦ ВУЛКАН

RSA
The Security Division of EMC

Архитектура и масштабирование

Система RSA DLP состоит из трех компонентов, интегрирующихся в «защищенный сайт» RSA DLP Suite.

RSA DLP Datacenter обеспечивает контроль за файловыми ресурсами на уровне ЦОД, выявление конфиденциальной информации и применение политик, в том числе с использованием механизмов безопасности других систем защиты информации.

RSA DLP Network предотвращает утечки информации при ее передаче по сети средствами корпоративной электронной почты (SMTP), веб-почты или других веб-приложений (HTTP или HTTPS), систем мгновенного обмена сообщениями, FTP-серверов.

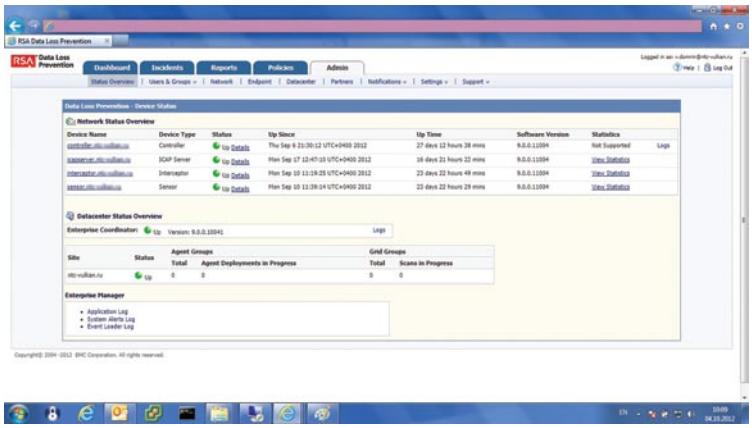
RSA DLP Endpoint обеспечивает защиту от утечек информации на уровне ПК и ноутбуков под управлением ОС Microsoft Windows. Осуществляется периодическое сканирование локальных данных и активная блокировка несанкционированных попыток перемещения информации за пределы АРМ.

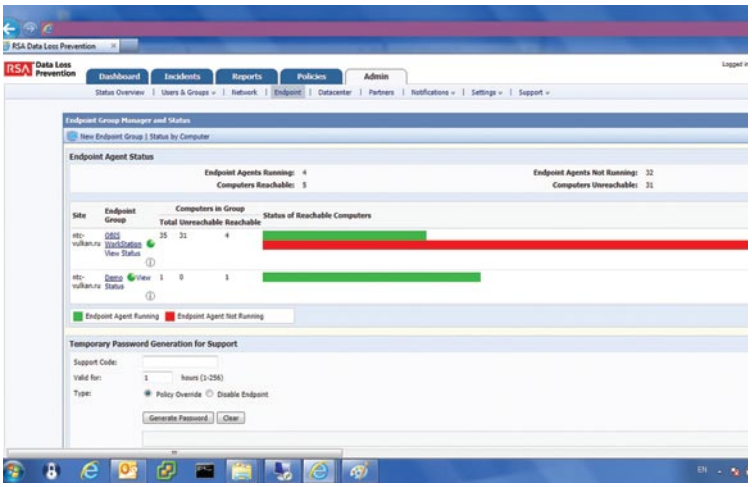
Модельный ряд RSA DLP позволяет системе расти вместе с организацией как горизонтально, так и вертикально, а возможность развертывания ее компонентов в виртуальной инфраструктуре VMware обеспечивает применение современных подходов к оптимизации ИТ-ресурсов.

Безопасность на практике

Ключевой результат применения системы RSA DLP— повышение уровня «реальной ИБ», а именно:

- проактивная защита от утечек конфиденциальной информации — противодействие инсайдерам;
- снижение рисков потери важных данных в результате ошибок пользователей;
- оптимизация работы ИБ-персонала за счет упрощения мониторинга различных каналов утечки информации;
- снижение затрат на управление данными и оптимизация бизнес-процессов;
- регулярная многоуровневая отчетность с возможностью дальнейшей обработки в системах BI и GRC.





Целевая аудитория

Система RSA DLP представляет интерес для широкого круга организаций:

- банки и кредитно-финансовые учреждения (не только «техническая» потребность, но и необходимость соблюдения требований международных и государственных регуляторов);
- конструкторские и научно-производственные учреждения, осуществляющие разработку инновационных образцов продукции;
- аудиторские и консалтинговые организации, аккумулирующие «чувствительную» информацию о своих клиентах;
- медицинские учреждения, обрабатывающие информацию о состоянии здоровья пациентов;
- государственные учреждения и правоохранительные органы.

Профессиональный сервис

НТЦ «Вулкан», авторизованный партнер RSA, The Security Division of EMC, предлагает:

- демонстрацию возможностей системы RSA DLP и проведение пилотных проектов;
- разработку инженерно-технических решений по применению RSA DLP для решения задач заказчика;
- разработку технической и эксплуатационной документации на русском языке;
- подбор (sizing), поставку и внедрение RSA DLP Suite;
- создание систем управления ИБ-инцидентами, связанными с утечкой конфиденциальной информации;
- интеграцию с другими системами защиты и анализа информации (DRM, SIEM, eGRC);
- техническую поддержку на русском языке, в том числе выездную.

НТЦ «Вулкан»
105318 г. Москва, ул. Ибрагимова, д. 31
тел./факс +7 (495) 663-9516
info@ntc-vulkan.ru
www.ntc-vulkan.ru