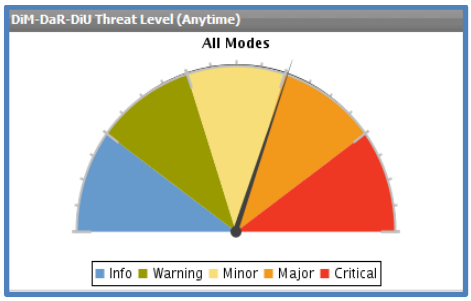
105318 г. Москва, ул. Ибрагимова, д. 31
тел./факс+7 (495) 663-9516
http://www.ntc-vulkan.ru
info@ntc-vulkan.ru

Корпоративная система предотвращения утечек данных на базе DLP-решения McAfee

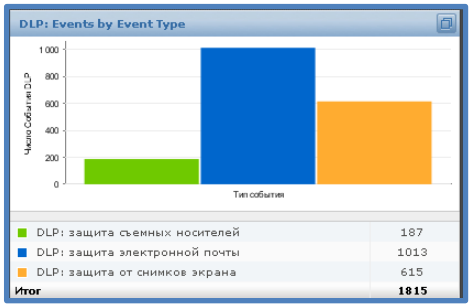
Заказчик: российский банк (ТОП-100), входящий в крупный международный финансовый холдинг.

Назначение проекта: автоматизация контроля над санкционированными действиями и попытками несанкционированной передачи документов в электронной форме или отдельных частей документов, содержащих конфиденциальную информацию, за пределы периметра контролируемой информационно-телекоммуникационной инфраструктуры.



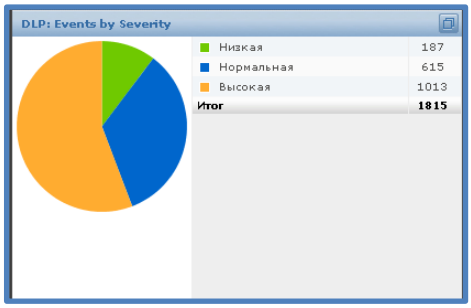
Цели выполнения проекта:

- снижение вероятности потери и/или утечки конфиденциальной информации
- расследование и реагирование на инциденты информационной безопасности[1]
- информационно-аналитическая поддержка операционной деятельности по управлению ИБ в банке



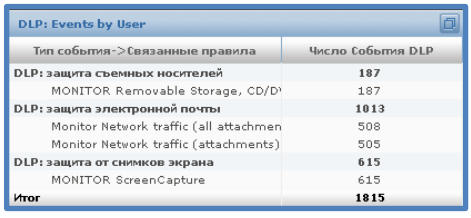
Средства и системы, подлежащие защите от утечек данных:

- пользовательские рабочие станции – 300 шт.
- пользовательские ноутбуки – 50 шт.
- серверы, в том числе виртуальные – 100 шт.



Защищаемые каналы утечки информации:

- съемные носители (CD, USB-flash, …)
- электронная почта
- публикация документов в сети Интернет
- протоколы служб мгновенных сообщений



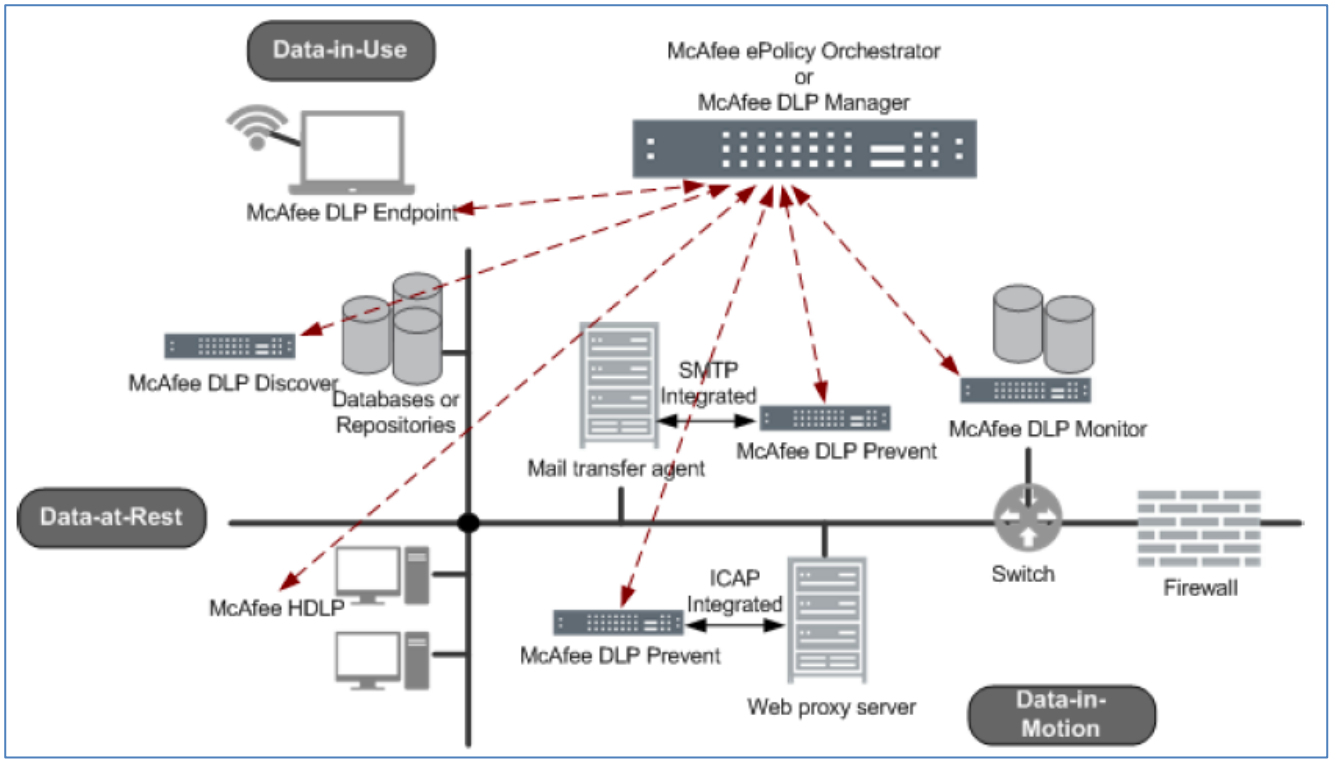
Техническое решение

Построено на компонентах McAfee DLP:

- McAfee Manager DLP
- McAfee Prevent DLP
- McAfee Discover DLP
- McAfee Monitor DLP
- McAfee Host DLP

[1] *Под инцидентом ИБ понимается зафиксированная попытка несанкционированной передачи конфиденциальной информации в электронной форме за пределы периметра контролируемой ИТ-инфраструктуры*

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



В рамках проекта проведены следующие работы:

- локализация конфиденциальной информации в информационных системах и сервисах, идентификация каналов утечки защищаемой информации, разработка технического решения, подготовка проектной и эксплуатационной документации[2]
- развертывание сервера централизованного управления системой предотвращения утечек данных
- развертывание агентов системы на рабочих станциях, ноутбуках и серверах
- настройка автоматического развертывания агентов системы на новые рабочие станции
- развертывание сетевых компонент системы в ИТ-инфраструктуре
- формирование политик защиты
- настройка перечней исключений пользователей
- формирование целевых рабочих областей (Dashboard)
- настройка шаблонов отчетов
- тестирование системы

В результате внедрения системы предотвращения утечек данных заказчик получил:

- повышение уровня информационной безопасности за счет контроля каналов утечки данных (на сетевом уровне и на уровне рабочих станций)
- централизованную консоль управления антивирусными решениями и DLP-системой
- систему централизованного управления инцидентами ИБ, связанными с утечками данных
- профили (статистику) для поведенческого анализа работы пользователей
- гибкую систему отчетности по инцидентам безопасности

[2] *Разработка документации на систему выполнена в соответствии с требованиями ГОСТ «Информационная технология. Комплекс стандартов на автоматизированные системы»*