2013

Предотвращение утечки информации

SYMANTEC DATA LOSS PREVENTION 12.0

SYMANTEC RUSSIA

Оглавление

Symantec Data Loss Prevention. Общие данные

Начиная с 2006 года Symantec по оценке Gartner уже 7 раз подряд является абсолютным бессменным лидером и продолжает удерживать свои позиции в области защиты от утечек и потери данных.

2013 Gartner Magic Quadrant for Content-Aware Data Loss Prevention:

Каждая 3-я компания “Fortune 100” использует Symantec DLP, включая:

- 9 из 10 ведущих банков,
- 9 из 10 крупнейших страховых компаний,
- 7 из 10 лидирующих медицинских компаний,
- 4 из 4 крупнейших компаний кредитных карт,

суммарно охватывая при этом более 5 миллионов сотрудников.

В отличие от большинства компаний-производителей DLP-решений постсоветского пространства, решение Symantec базируется не на словоформах и сочетаниях слов, хоть и этот метод не исключается, а на оценке конфиденциальности содержимого документов при помощи нескольких технологий (в различных сочетаниях):

- Describe Content Matching,
- Exact Data Matching,
- Indexed Document Matching,
- Vector Learned Machine.

Уникальные технологии Symantec позволяют оперативно автоматизированно обучать / дообучать / переобучать DLP-решение в соответствии с изменением статуса информации внутри компании, а также интегрировать его с функциональными системами предприятия (ERP, CRM, HR и др).

Таким образом, задача предотвращения утечек сводится к нескольким регулярно выполняемым операциям:

1. Обнаружение конфиденциальной информации на всех корпоративных устройствах, включая мобильные, периодически покидающие корпоративную сеть, и контроль безопасного хранения данных.
2. Контроль и управление доступом и использованием конфиденциальной информации сотрудниками компании.
3. Контроль и обеспечение безопасности жизненного цикла конфиденциальной информации, включая процедуры обработки и хранения.
4. Контроль передачи конфиденциальной информации по любым каналам (Mail, Web, Network, Local Ports and Devices) согласно заданным политикам.
5. Блокирование неправомерных действий, включая печать на сетевых и локальных принтерах, автоматизированное удаление конфиденциальной информации с недоверенных сред, шифрование конфиденциальной информации при отправке наружу или записи на внешние носители, перемещение подозрительных сообщений в карантин, уведомление об инциденте сотрудника-нарушителя и его руководителя.
6. Предоставление отчётности по снижению рисков в рамках задач, решаемых Symantec DLP.
7. Встроенный механизм контроля расследования инцидентов.

Единая среда управления всеми компонентами решения и выполняемыми задачами полноценно поддерживает несколько языковых интерфейсов, включая русский. Решение имеет действующую сертификацию ФСТЭК.

Помимо DLP-функционала обеспечивается интеграция с другими системами обеспечения (СОИБ) и управления (СУИБ) информационной безопасностью:

- Интеграция с PGP/ERM/DRM-продуктами для усиления защиты конфиденциальной информации (КИ) за счёт шифрования в случае их нахождения на небезопасных (недостаточно защищённых) ресурсах;
- Не только контроль прав доступа к КИ, но и автоматическое изменение привилегий пользователей согласно политикам безопасности;
- Построение процессов раздельного хранения и обработки КИ, маркирование объектов КИ для их последующей обработки согласно политикам безопасности;
- Изменять уровня значимости ресурса в случае обнаружения на нём КИ (через создание дополнительных скриптов), и влияние, таким образом, и на вес/приоритет обработки инцидентов ИБ (Symantec SIM), и на актуальный уровень рисков (Symantec CCS Risk Manager);
- Интеграция в системы IT-аналитики (Symantec IT Analytics) для расширения отчётности, контроля ключевых индикаторов эффективности и консолидации информации от различных ИТ и ИБ систем;

- Построение процессов обработки информации согласно требованиям регуляторов, в частности PCI DSS и ФЗ-152, и обеспечение прохождения аудита на соответствие их требованиям.

Технологии распознавания конфиденциальной информации

1. Vector Machine Learning (VML)

Технология VML основана на математическом методе опорных векторов, представляющем собой набор алгоритмов решения задач классификации и регрессионного анализа. Данная технология широко применяется в различных системах – от анти-спам решений до алгоритмов текстового перевода компании Google. В рамках DLP-решения технология VML учится распознавать конфиденциальную информацию (КИ) по предоставленным образцам документов.

Практическая работа с технологией VML в продукте Symantec Data Loss Prevention выглядит следующим образом. Пользователь системы (офицер безопасности), осуществляющий настройку политик, формирует два набора документов – “позитивный” и “негативный”, один из которых состоит из документов, содержащих КИ, а другой – из похожих документов, но не содержащих КИ, а так же задаёт набор слов/терминов, которые система не должна учитывать. После поступления этой информации в систему, VML на основе полученных данных, а так же настроек “порогового значения подобия” и “выделенной памяти” создаёт статистическую модель или профиль. При этом система рассчитывает и отображает пороговые уровни ложноположительных и ложноотрицательных срабатываний. В случае приемлемости полученных значений профиль утверждается и затем реплицируется на остальные модули DLP. Расчёт уровней ложных срабатываний производится на основе процесса, который мы называем k-fold, который проще пояснить на примере: для создания профиля используется 500 документов, из которых 250 “позитивных” и 250 “негативных”. В процессе обучения системы набор документов делится на 10 частей (поднаборов), содержащих "позитивные" и "негативные" типы документов. Система использует 9 поднаборов для создания "профиля" и 1 для его проверки. Данный процесс повторяется для всех 10 поднаборов. В конце система производит финальное обучение, усредняющее результаты для всех поднаборов и создаёт финальную модель профиля.

Точность распознавания КИ повышается с увеличением количества документов, используемых для обучения системы и создания профиля.

2. Described Content Matching (DCM)

DCM включает в себя ряд механизмов:

- Обнаружение в тексте документа ключевых слов.
- Обнаружение в тексте документа пары ключевых слов. При это можно задать максимальное количество слов, которое может оказаться между заданной парой.

- Обнаружение в тесте документа последовательности символов, описанных регулярным выражением.
- Обнаружение в тексте последовательности символов, описанных идентификатором.

Идентификатор работает следующим образом:

a) Захват последовательности символов с помощью упрощённого регулярного выражения (например для определения номера кредитной карты это может быть 16 цифр или 4 набора по 4 цифры в каждом разделённые пробелом или тире и т.д.).

b) Нормализация, то есть исключение из анализа незначащих символов (для номера кредитной карты это могут быть пробелы, тире и т.д.)

c) Валидация, то есть проведение над полученной последовательностью определённых математических действий для подтверждения валидности данного набора символов. Для написания валидаторов применяется специализированной язык программирования, за счёт чего достигается простота написания собственного валидатора (если это необходимо), высокая скорость обработки и низкая нагрузка на целевую систему по сравнению с регулярными выражениями.

3. Exact Data Matching (EDM)

Механизм снятия цифровых отпечатков с документов, имеющих структуру. Характерно его использование для таблиц Excel, баз данных и т.д.

В данном случае каждый элемент структуры (например каждая ячейка) подвергается обработке с помощью математической функции для формирования хэша. Набор этих хэшей система хранит в виде специализированных файлов и если данный набор хэшей используется в правилах – загружает в оперативную память сервера. За счёт этого достигается максимальная скорость взаимодействия и анализа.

При использовании механизма EDM возможно написание правил, где система будет понимать взаимосвязь ячеек. Например, если в одной строке у нас указан номер паспорта и фамилия человека – система поймёт, что именно этот паспорт связан с этим человеком и не будет реагировать на другие номера или фамилии.

Так же возможно задать реагирование системы только на сочетание ключевых полей, то есть реагирование только на номер паспорта и фамилию, но не фамилию и имя и т.д.

4. Indexed Document Matching (IDM)

Механизм снятия отпечатков с документов, для которых характерен большой объем текста, например договоры/контракты, техническая и другая документация и т.д.

Механизм обработки аналогичен EDM, но минимальной единицей «снятия отпечатка» является “чанк”, который в общем случае составляет 25 слов. При этом при снятии отпечатка отбрасываются незначащие символы, такие как пробелы, запятые и т.д.

Так как эти документы не имеют чёткой структуры, то используется порог совпадения, который можно выбирать в правиле (от 10 до 100%).

При анализе отправляемого документа система DLP производит аналогичное действие, то есть с детектируемого документа снимаются цифровые отпечатки и уже они сравниваются с отпечатками, которые изначально были заведены в систему.

Цели, задачи и основные принципы функционирования

Первичной задачей Symantec DLP является выявление конфиденциальной информации (КИ), содержащейся:

1. В файлах различных форматов на всех ресурсах корпоративной сети, включая стационарные и мобильные компьютеры, серверы, хранилища данных и общие сетевые файловые ресурсы,
2. Трафике/сообщениях электронной почты
3. Web-трафике,
4. В сетевом трафике,
5. При записи на сменные носители информации,
6. При отправке документов на печать и
7. В документах, отправляемых через интернет-пейджеры.

Для решения этой задачи Symantec DLP располагает несколькими технологиями обнаружения КИ, применяемыми совместно или по отдельности в зависимости от характера защищаемых данных:

- Described Content Matching (DCM),
- Exact Data Matching (EDM),
- Indexed Document Matching (IDM),
- Vector Machine Learning (VML).

Symantec DLP позволяет проводить автоматизированное обучение на основе документов с конфиденциальной информацией и похожих документов, не содержащих КИ, при этом отображается степень вероятности выявления КИ данного вида. Разумеется, при этом предполагается, что категоризация информации уже проведена, и степень конфиденциальности известна и формализована.

Symantec DLP использует 4 метода обнаружения контента:

- **DCM**, в который входят методы обнаружения по ключевым словам, регулярным выражениям и идентификаторам. Идентификаторы позволяют реализовать такой функционал при проверке, ка контроль валидности номеров кредитных карт по алгоритму Luhn или корректность ИНН, используя механизмы проверки, заложенные в номер и т.д.
- **EDM** или цифровые отпечатки для структурированных данных, по сути таблиц. В данном случае процедура снятия отпечатка применяется на каждой ячейке, что позволяет обнаруживать например паспорт и его владельца и защищать именно это сочетание, основываясь на такой таблице.
- **IDM** или отпечатки для неструктурированных данных предназначены для защиты текстовых данных, например договоров и т.д. Механизм обнаружения позволяет определить похожесть документа до 10%. Данный порог может изменяться при написании правил обнаружения.

- **VML** – собственная разработка Symantec для автоматизации обучения системы. Обучение производится на массивах «позитивных» и «негативных» документов с целью выявления характерных признаков КИ в контролируемых потоках. Чем больше документов будет предложено системе в процессе обучения, тем точнее система будет определять КИ.

Вторая задача Symantec DLP – это оперативное реагирование на события, связанные с обменом, передачей или выявлением КИ на недопустимых ресурсах в соответствии с заданными правилами/политиками: предупреждение, перемещение в карантин, блокировка, изменение прав/списка доступа, перемещение из недоверенной среды на «правильные» ресурсы, шифрование и др. Создание политик – серьёзная и объёмная предварительная работа, но уже с помощью предоставляемого инструментария и множества различных шаблонов, которые можно использовать и в готовом виде (например, под персональные данные) или модернизировать в соответствии с внутренними требованиями.

В случае срабатывания политики – потенциального или реального инцидента ИБ (утечки КИ), Symantec DLP включает механизм уведомления и контроля расследования инцидентов.

Symantec DLP предлагает также средства подготовки аналитической отчётности и визуального представления информации касательно рисков ИБ, динамики, тенденций и количественных характеристик.

Таким образом, основной целью Symantec DLP является предотвращение утечек конфиденциальной информации за счёт использования различных технологий и средств технического контроля, обучения сотрудников правилам обработки КИ и расследования каждого произошедшего инцидента или неправильных действий сотрудника.

Решение Symantec DLP объединяет несколько модулей специализированного функционала, которые могут применяться все вместе или в различных сочетаниях – по необходимости.

Описание модулей

1. **ENFORCE PLATFORM** – интегрирующая и управляющая основа решения Symantec DLP. Управление набором модулей DLP осуществляется через Web-интерфейс и позволяет выполнять следующие операции:

   Снятие цифровых отпечатков с неструктурированных данных. Снятие может производиться из следующих источников: общая сетевая папка, доступная по протоколу SMB, CIFS; локальная папка на сервере Enforce; в виде архива, загружаемого через web-интерфейс, содержащего необходимые документы.

   Снятие цифровых отпечатков со структурированных данных. Снятие производится через файл-выгрузку формата CSV, загружаемый через web-интерфейс.

   Создание профиля с помощью технологии Vector Machine Learning. Создание происходит при обработке достаточно большого массива документов «позитивного» и «негативного» характера. Документы загружаются через web-интерфейс.

   Создание и редактирование идентификаторов, представляющих сочетание регулярных выражений и проверок.

   Создание политик на основе цифровых отпечатков, ключевых слов, профилей VML, регулярных выражений, идентификаторов, аттрибутов файлов, идентификаторов съемных носителей, расположения рабочей станции, протоколов, списков пользователей, доменов, адресов электронной почты и IP-адресов.

   Создание правил реагирования на срабатывание политики.

   Создание целей сетевого сканирования.

   Добавление, переназначение, управление и удаление серверов детектирования.

   Создание групп политик.

   Просмотр и управление уведомлениями о системных событиях.

   Просмотр статистики сетевого трафика.

   Сбор логов модулей системы.

   Просмотр состояния, удаление, изменение конфигурации и создания уведомления о состоянии агентов, устанавливаемых на рабочих станциях.

   Управление функционалом контроля приложений.

   Создание, изменение и удаление идентификаторов съемных устройств.

   Управление основными настройками системы, настройками сетевых протоколов, групп пользователей на основе групп Active Directory, **хранением учетных записей** и **управление интеграцией** с модулями Data Insight и Management Console, создание и изменение атрибутов инцидентов, управление выгрузок данных инцидентов в архив и управление пользователями и ролями.

   Просмотр инцидентов, создание отчётов.

2. **NETWORK MONITOR** – модуль, предназначенный для анализа зеркалированного сетевого трафика который передаётся на анализ с помощью дополнительного сетевого оборудования: коммутаторов или TAP устройств.

   Модуль Network Monitor позволяет на основе сигнатур анализировать протоколы: SMTP, HTTP, NNTP, AOL, MSN, YAHOO. Другие сетевые протоколы анализируются, основываясь на используемых ими сетевых портах.

   Анализ трафика происходит локально. Данные об инциденте передаются на модуль Enforce по шифрованному каналу. Сертификат шифрования может использоваться как встроенный, так и созданный дополнтельно.

3. **NETWORK PREVENT FOR E-MAIL** – модуль, предназначенный для анализа и блокирования электронной почты, передаваемой по протоколам SMTP или ESMTP. Технологически представляет собой (E)SMTP Proxy.

   Предоставляет несколько вариантов интеграции в почтовую инфраструктуру – как в разрыв, так и параллельная обработка.

   Анализ трафика происходит локально. Данные об инциденте передаются на модуль Enforce по шифрованному каналу. Сертификат шифрования может использоваться как встроенный, так и созданный дополнтельно.

4. **NETWORK PREVENT FOR WEB** – модуль, предназначенный для анализа и блокирования трафика, передаваемого на него Proxy-серверами. Возможен анализ протоколов HTTP, HTTPS (при использовании proxy-серверов, имеющих функционал расшифровки SSL-трафика), FTP over HTTP. Интеграция с Proxy-серверами возможна по протоколу ICAP или с помощью дополнительного ПО, устанавливаемого на серверы Microsoft ISA 2004/2006 и TMG.

   Анализ трафика происходит локально. Данные об инциденте передаются на модуль Enforce по шифрованному каналу. Сертификат шифрования может использоваться как встроенный, так и созданный дополнтельно.

5. **NETWORK DISCOVER** – модуль, предназначенный для обнаружения данных на сетевых источниках хранения. Обнаружение возможно на файловых серверах, файловых системах серверов, в базах данных SQL, почтовых серверах и др.

   Сканирование источников осуществляется по расписанию с правами заданного пользователя.

   Анализ трафика происходит локально. Данные об инциденте передаются на модуль Enforce по шифрованному каналу. Сертификат шифрования может использоваться как встроенный, так и созданный дополнтельно.

6. **NETWORK PROTECT** – модуль, являющийся расширением модуля Network Discover, позволяющий производить операции с файлами, такие как перенос или копирование файлов, нарушающих политики. В случае переноса файлов возможно оставлять на их

месте файл-заглушку, имеющий то же название, что и переносимый файл, но с заданным текстом внутри.

7. **ENDPOINT DISCOVER** – модуль, предназначенный для поиска и анализа файлов, расположенных на рабочих станциях. Поиск осуществляется установленным на рабочей станции Endpoint-агентом.

   Анализ файлов происходит локально, за исключение анализа по цифровм отпечаткам, для чего данные передаются на Endpoint-сервер. Данные об инциденте передаются с агента на серверы Endpoint и далее на модуль Enforce по шифрованному каналу. Сертификат шифрования может использоваться как встроенный, так и созданный дополнтельно.

8. **ENDPOINT PREVENT** – модуль, предназначенный для контроля действий пользователей на рабочих станциях. Контроль производится с помощью ПО Endpoint Agent, устанавливаемого на рабочие станции и серверы.

   Агент анализирует данные, передаваемые следующими способами:

   - Запись на USB носитель
   - Запись на локальный диск
   - Запись на SD и CF карты памяти
   - Копирование в буфер обмена
   - Запись на CD/DVD носители
   - Запись на общие сетевые папки
   - Отправка через POST-запросы на web-страницы. Анализу подлежит как HTTP протокол (для всех браузеров), так и HTTPS (для браузеров MS Internet Explorer и Mozilla Firefox)
   - Отправка данных по электронной почте через почтовые клиенты MS Outlook и Lotus Notes
   - Отправка данных через интернет-пейджеры, такие как MSN, Yahoo, и др.
   - Обращение программ к файлам и передача данных по сети (Application Control)

   Анализ файлов происходит локально, за исключением анализа по цифровм отпечаткам, для чего данные передаются на Endpoint-сервер. Данные об инциденте передаются с агента на серверы Endpoint и далее на модуль Enforce по шифрованному каналу. Сертификат шифрования может использоваться как встроенный, так и созданный дополнтельно.

   В случае нарушения политик на рабочей станции с помощью агента может выдаваться диалоговое окно с требованием объяснить необходимость совершаемого действия.

9. **DATA INSIGHT** – модуль, предназначенный для сбора информации о действиях (создание файла, запись, чтение и т.д.), совершаемых с файлами на уровне файловой системы. Данные могут собираться с файловых серверов на платформе Windows, серверов MS Sharepoint, а так же NAS-серверов компания NetApp и EMC. Модуль формирует отчетность по доступу к файлам, а так же по занятому месту на серверах. Так же модуль позволяет контролировать с помощью политик следующие действия пользователей: доступ к файлу,

доступ к файлу пользователей, не находящихся в белых списках. Так же модуль позволяет определять нестандартное поведение пользователей в отношении доступа к данным. Модуль состоит из следующих компонентов:

- **Management** – настройка, управление, хранение данных и предоставление отчетности;
- **Indexer – индексирование и обработка данных, передаваемых с collector;**
- **Collector – сбор данных с серверов-источников.**

Контроль доступа

Доступ к данным внутри Symantec DLP осуществляется только через веб-интерфейс. Ролевая система доступа с гранулированным распределением прав встроена в продукт изначально. Доступ к данным регулируется на основе любых атрибутов системы. Если каких-либо атрибутов не хватает, то их можно создать дополнительно и также использовать для контроля доступа.

Отчётность

Отчётность формируется по большинству атрибутов инцидента. Она бывает трёх типов, отражает различные тренды, в том числе и двухуровневые. Примеры отчетов:

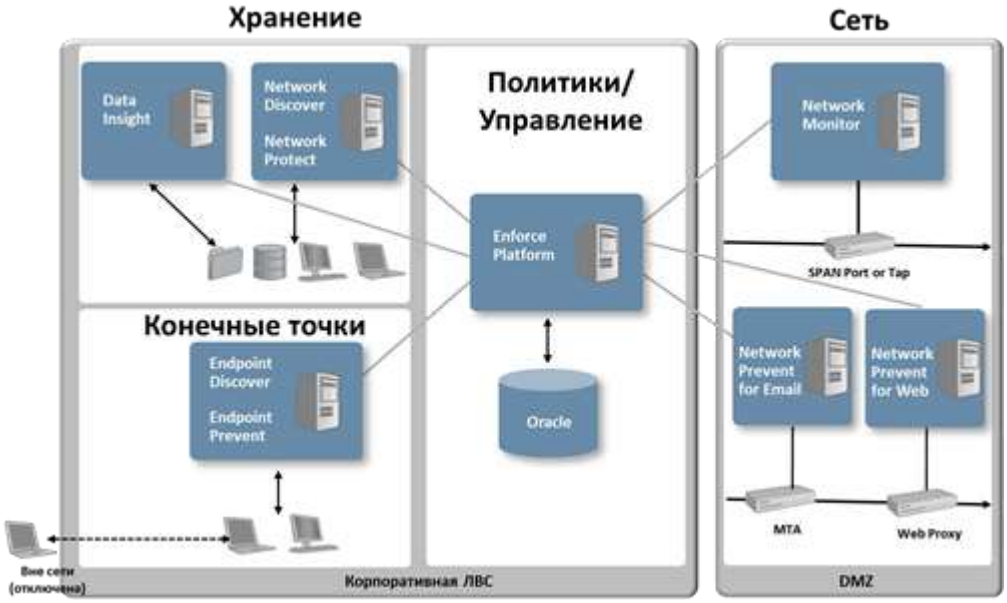
- количество нарушений за месяц,
- количество нарушений со статусом «высокий» за 2 недели,
- 5 пользователей, чаще других нарушающих политики,
- изменение количества инцидентов по неделям,
- распределение серверов по уровню риска. Риск в данным случае зависит от количества пользователей имеющих доступ к информации и её степени критичности.

Так как атрибуты инцидента могут добавляться – то и отчетность может расширяться.

В случае нехватки встроенных средств отчётности можно использовать модуль ИТ-аналитики (Symantec IT Analytics), предоставляемый нашим клиентам бесплатно.

Архитектура решения

На схеме ниже представлена многоуровневая архитектура решения Symantec Data Loss Prevention. Каждый прямоугольник на этой схеме представляет собой отдельный физический (виртуальный) сервер с установленным на нём программным компонентом Symantec DLP. Белым шрифтом на схеме обозначены названия этих программных компонентов.



Важно помнить, что Symantec DLP – это программное обеспечение, а не устройство. Серверное программное обеспечение устанавливается в операционной среде Windows или Linux. Также обратите внимание, что часть компонентов Symantec DLP устанавливается внутри корпоративной сети, а остальные находятся в демилитаризованной зоне (DMZ).

В центре схемы находится Symantec DLP **Enforce Platform**.

Enforce Platform предназначен для управления всеми модулями DLP. Enforce Platform является единственным решением для обеспечения универсального управления политиками DLP по методу «один раз написать, использовать везде» и автоматического их применения. Enforce Platform обеспечивает доставку кросс-платформенных политик, детектирование, автоматизацию, отчетность и аналитику, а также системы управления и безопасности. Модуль обычно находится в защищенной корпоративной сети. Управление осуществляется через Web-интерфейс.

После создания, политики DLP сохраняются в базе данных Enforce (Oracle 10 или 11). Также эти политики DLP незамедлительно отправляются в модули DLP и хранятся в локальной памяти на конечных устройствах, где производится обнаружение конфиденциальной информации. Если политики нарушаются, генерируется соответствующий инцидент. Он отправляется обратно на Enforce, где потом и хранится. Сервер Enforce и базу данных можно установить на отдельный физический сервер, также их можно устанавливать отдельно.

Справа на схеме в демилитаризованной зоне (DMZ) находятся **сетевые модули Symantec DLP**.

Модуль **Network Monitor** просматривает копию сетевого трафика в пассивном режиме. Трафик передается на модуль с помощью дополнительного сетевого оборудования: коммутаторов (SPAN-порт) или TAP устройств. Модуль позволяет на основе сигнатур анализировать протоколы: SMTP, HTTP, HTTPS, NNTP, AOL, MSN, YAHOO, а также другие сетевые протоколы, основываясь на используемых ими сетевых портах.

Анализ трафика происходит локально. Данные об инциденте передаются на модуль Enforce по шифрованному каналу. Сертификат шифрования может использоваться как встроенный, так и созданный дополнительно.

Модули **Network Prevent** позволяют не только отслеживать, но и блокировать утечку данных за пределы сети.

Модуль **Network Prevent for Email** предназначен для анализа и блокирования электронной почты (SMTP/ESMTP), нарушающей политики ИБ. Технологически это (E)SMTP Proxy и предоставляет несколько вариантов интеграции в почтовую инфраструктуру.

Анализ трафика происходит локально. Данные об инциденте передаются на модуль Enforce по шифрованному каналу. Сертификат шифрования может использоваться как встроенный, так и созданный дополнительно.

Модуль **Network Prevent for Web** предназначен для анализа и блокирования трафика, нарушающего политики ИБ. Возможен анализ протоколов HTTP, HTTPS (при использовании proxy-серверов, имеющих функционал расшифровки SSL трафика), FTP over HTTP. Интеграция с Proxy-серверами возможна по протоколу ICAP или с помощью дополнительного ПО, устанавливаемого на сервера Microsoft ISA 2004/2006 или TMG.

Анализ трафика происходит локально. Данные об инциденте передаются на модуль Enforce по шифрованному каналу. Сертификат шифрования может использоваться как встроенный, так и созданный дополнительно.

Слева внизу на схеме корпоративной сети (LAN) находятся модули, предназначенные для работы на рабочих станциях – **Endpoint Discover** и **Endpoint Prevent.** Технически это единый агент с широким функционалом. Политики хранятся локально, контроль производится независимо от подключения пользователя к сети, что обеспечивает защиту от потери данных в любое время, в любом месте.

Модуль **Endpoint Prevent** отслеживает и блокирует попытки копирования конфиденциальных данных на съемные носители (USB, CD/DVD, Firewire), передачу их по сети (по электронной почте, HTTP/S, IM или FTP), копирование и вставку из буфера обмена, а так же напечатать или отправить по факсу.

Агент анализирует данные, передаваемые следующими каналами:

- Запись на USB, CD/DVD носители, карты памяти SD и CF
- Запись на локальный диск
- Копирование в буфер обмена
- Запись на общие сетевые папки

- Отправка через POST-запросы на web-страницы. Анализу подлежит как HTTP протокол (для всех браузеров), так и HTTPS (Для браузеров MS Internet Explorer и Mozilla Firefox)
- Отправка данных по электронной почте с помощью почтовых клиентов MS Outlook и Lotus Notes
- Отправка данных через интернет пейджеры, такие как MSN, Yahoo, AOL
- Обращение любым программ к файлам и передача данных по сети (Application Control)

Анализ файлов происходит локально, за исключение анализа по цифровым отпечаткам, для чего данные передаются на Endpoint сервер. Данные об инциденте передаются с агента на сервера Endpoint и далее на модуль Enforce по шифрованному каналу. Сертификат шифрования может использоваться как встроенный, так и созданный дополнительно.

В случае нарушения политик на рабочей станции с помощью агента может выдаваться диалоговое окно с требованием объяснить необходимость совершаемого действия.

Модуль **Endpoint Discover** предназначен для поиска и анализа файлов, расположенных на рабочих станциях. Модуль сканирует жесткие диски настольных и портативных компьютеров и ищет на них конфиденциальные данные с их последующей инвентаризацией или перемещением в безопасное хранилище. Для поиска стандартных типов конфиденциальных данных, связанных с различными отраслевыми и нормативными положениями, предусмотрено более 60 готовых шаблонов. Первое сканирование конфиденциальных данных выполняется во время бездействия конечных систем. В ходе последующих сканирований проверяются только объекты, измененные со времени последнего сканирования.

Данные об инциденте передаются с агента на сервера Endpoint и далее на модуль Enforce по шифрованному каналу. Сертификат шифрования может использоваться как встроенный, так и созданный дополнительно.

Слева, в верхней части схемы, на схеме корпоративной сети (LAN) находятся **модули для работы с хранилищами данных - Network Discover и Network Protect.** Технически это единый копонент системы с широким функционалом.

Модуль **Network Discover** предназначен для обнаружения конфиденциальной информации на сетевых хранилищах данных (репозитариев), обеспечивая поддержку широкого набора возможных вариантов, предлагая готовые средства для сканирования следующих систем:

- Файловые сервера. Сетевые (CIFS, NFS, DFS и др.) и локальные файловые системы (Windows, Linux, AIX, Solaris)
- Базы данных
- Хранилища электронной почты (Microsoft Exchange, Lotus Notes)
- Системы учета документов и записей (Microsoft SharePoint, Documentum и др.)
- Web сервера.

Анализ трафика происходит локально. Данные об инциденте передаются на модуль Enforce по шифрованному каналу. Сертификат шифрования может использоваться как встроенный, так и созданный дополнительно.

Network Protect - дополнительная лицензия для модуля Network Discover, позволяющая обрабатывать найденную конфиденциальную информацию в хранилищах данных с помощью функций автоматического карантина, перемещения, шифрования и архивирования. Также Network Protect позволяет применять к файлам функцию «карантин» в ручном режиме, с восстановлением файлов, шифрованием на месте и применения политик цифровых прав (right management).

Модуль **Data Insight** собирает информацию о наиболее активных пользователях файлов, а также полную историю доступа к ним, чтобы определить, кто владеет ими. Также обеспечивается визуализация прав доступа. Data Insight интегрируется с компонентом Network Discover для предоставления информации о владельце файла и детали по уровню доступа (что может существенно повысить эффективность расследования).

На следующей схеме показаны каналы передачи данных, которые Symantec DLP может отслеживать и при необходимости блокировать передачу конфиденциальной информации.

Требования к серверному оборудованию и ПО

Требования к серверному оборудованию указаны в таблице 1.

Enforce Server		Detection		Data Insight	
CPU	1x2,4 ГГц 6 ядер	CPU	1x2,4 ГГц 6 ядер	CPU	1x2,4 ГГц 6 ядер
RAM	6-8 ГБ +	RAM	6-8 ГБ +	RAM	12 ГБ +
HDD	500 ГБ Raid 10 или Raid 5	HDD	140 ГБ	HDD	300 ГБ
Сеть	1 NIC 100 Мб / 1 Gb	Сеть	1 NIC 100 Мб / 1 Gb; 2 NIC 100 Мб / 1 Gb для Network Monitor	Сеть	1 NIC 100 Мб / 1 Gb

Требования к операционным системам сервера Enforce и серверов Detection:

- Microsoft Windows Server 2008 R2, Enterprise Edition (64-bit)
- Microsoft Windows Server 2008 R2, Standard Edition (64-bit)
- Microsoft Windows Server 2008 R2 SP1, Enterprise Edition (64-bit)
- Microsoft Windows Server 2008 R2 SP1, Standard Edition (64-bit)
- Red Hat Enterprise Linux 5.6 through 5.9 (64-bit)

Требования к операционной системе сервера Data Insight:

- Windows Server 2003 (32-bit and 64-bit) Standard Edition and Enterprise Edition
- Windows Server 2003 R2 (32-bit and 64-bit) Standard Edition and Enterprise Edition
- Windows Server 2008 (32-bit and 64-bit) Standard Edition and Enterprise Edition
- Windows Server 2008 R2 (32-bit and 64-bit) Standard Edition and Enterprise Edition

Внимание: Все модули DLP поддерживают виртуализацию на VMWare, кроме СУБД Oracle и модуля Network Monitor.