WHITEPAPER

PERIMETRIX SAFESPACE™

КОМПЛЕКСНАЯ ЗАЩИТА КОНФИДЕНЦИАЛЬНОСТИ И ЦЕЛОСТНОСТИ ДАННЫХ

KEEPING SECRETS SAFE

PERIMETRIX

1. ВВОДНЫЕ

При помощи Perimetrix SafeSpace™ организация любого масштаба сможет построить простую, надежную и удобную систему защиты от внутренних нарушителей.

Сегодня уже никто не сомневается, что каждая организация должна защищать свои корпоративные секреты: конфиденциальную информацию, интеллектуальную собственность, персональные данные служащих и клиентов. Причем защищать не только от внешних злоумышленников, но еще и от внутренних нарушителей.

Руководители отчетливо понимают, что утечка корпоративных секретов подрывает конкурентоспособность организации, осложняет отношения с клиентами, партнерами и инвесторами, а также привлекает внимание государства и регулирующих органов, которые принимают соответствующие законы, стандарты, директивы и кодексы.

Однако далеко не все компании и госструктуры сегодня используют системы защиты от утечек. Виной тому низкая эффективность представленных на рынке решений, которые либо способны предотвратить только случайные утечки, либо настолько сложны и бюрократичны, что парализуют работу служащих.

Кроме того, предлагаемые продукты не позволяют решить проблему утечек в комплексе. Вместо этого они концентрируются на каком-то одном вопросе, например, блокируют порты рабочей станции или фильтруют исходящий сетевой трафик. Все остальное поставщики оставляют на откуп самой организации, специалисты которой должны решить самостоятельно, как защититься от кражи и потери ноутбуков и мобильных носителей с конфиденциальной информацией или предотвратить утечку через принтеры.

В результате компании просто боятся инвестировать средства в систему защиты от утечек. Во-первых, не понятно, за что платить, ведь потребность в безопасности корпоративных секретов все равно не удовлетворена. Во-вторых, даже то, за что заплачено, завтра может легко устареть. Такова неминуемая судьба любого неэффективного решения.

Руководители компаний ясно видят, что все перечисленные проблемы обусловлены незрелостью технологий защиты от утечек. Топ-менеджмент ждет, пока на горизонте появится не только эффективное решение, но еще и такое, которое адресует всю проблему в комплексе, а не по кускам.

PERIMETRIX

Данный документ посвящен именно такому продукту. Решение Perimetrix SafeSpace™ позволяет обойти ограничения стандартных технологий в том виде, в котором они существовали до сегодняшнего дня. В основе продукта лежит уникальная технология Secret Documents Lifecycle™. С ее помощью разработчики смогли перенести в электронную среду те принципы секретного документооборота, которые десятилетиями использовались в режимных организациях и доказали свою эффективность на деле.

При помощи Perimetrix SafeSpace™ организация любого масштаба сможет построить простую, надежную и удобную систему защиты от внутренних нарушителей, решить проблему защиты конфиденциальности и целостности данных раз и навсегда.

2. УСТАРЕВШИЕ ПОДХОДЫ К ЗАЩИТЕ ДАННЫХ

Компания Gartner считает, что доступные на рынке продукты не позволяют создать надежной защиты.

Почему все предлагавшиеся до сегодняшнего дня решения по большому счету так и не нашли своего покупателя? Ответ на этот вопрос дает научно-исследовательская компания Gartner. В своем последнем исследовании «Hype Cycle for Information Security, 2007» аналитики четко дают понять, что технологии предотвращения утечек еще не достигли своей зрелости. По мнению Gartner, это произойдет в срок от 2 до 5 лет, а сейчас внедрение предлагаемых решений сулит лишь «умеренные» преимущества для бизнеса.

Хотя технологию защиты от утечек обычно рассматривают в качестве эффективного средства защиты интеллектуальной собственности, эксперты Gartner указывают, что на практике применяемые технологии оказываются гораздо более полезными в выявлении ошибочных бизнес-процессов и лишь случайных утечек. Несмотря на то, что на долю непреднамеренных утечек, искажения и уничтожения данных приходится львиная доля инцидентов, предлагаемые технологии не в состоянии остановить мотивированного внутреннего нарушителя.

Таким образом, Gartner указывает, что доступные на рынке продукты не позволяют создать надежной защиты. Более того, их эффективность достигает лишь 80%, так что о полноценном решении проблемы даже говорить не приходится.

2.1. ПРИЧИНЫ НЕУДАЧ

Ключевой недостаток существующих на сегодняшний день решений состоит в самой постановке задачи. Хотя разработчики совершенно справедливо считают, что утечка происходит только тогда, когда конфиденциальная информация покидает корпоративный периметр, они совершенно необоснованно сужают область защиты только теми каналами, по которым данные могут попасть наружу. Это электронная почта, Интернет, мобильные носители и принтеры.

В результате многие аспекты проблемы остаются нерешенными. Например, ничто не мешает служащему скопировать данные на ноутбук, а потом симулировать его кражу. Кроме того, защита от утечек на рабочих станциях работает обычно по принципу «разрешить/запретить», никак не учитывая уровень конфиденциальности того контента, который копируется, скажем, на USB-носитель. Таким образом, сотрудник, имеющий легальный доступ к секретным данным, выпадает из сферы контроля и может злоупотребить своими правами в корыстных целях.

PERIMETRIX

Между тем все эти проблемы выглядят лишь легким недомоганием на фоне той раковой опухоли, которую представляет собой крайне низкая эффективность предлагаемых продуктов.

Эффективность лингвистической фильтрации в самом лучшем случае достигает лишь 80%.

2.2. ВЧЕРАШНИЙ ДЕНЬ НЕЗРЕЛЫХ ТЕХНОЛОГИЙ

Низкая эффективность используемых технологий обусловлена, прежде всего, их незрелостью. Хотя методы распознавания конфиденциальной информации прошли уже две ступени эволюции, они по-прежнему ограничены сверху в своей эффективности.

Первое поколение технологий – различные виды вероятностного анализа. В том числе, лингвистический и сигнатурный анализ, технология цифровых отпечатков (Digital Fingerprints). Те 80%, на которые указывает в своем исследовании Gartner, это самое лучшее, что могут предложить перечисленные методы, использующиеся для фильтрации исходящего трафика, чтобы отличить конфиденциальный документ от публичного. Даже с учетом контекста найденных ключевых слов, даже при использовании базы контентной фильтрации, учитывающей специфику конкретного заказчика, эффективность вероятностного анализа ниже 80%.

Отметим, что если вместо лингвистического анализа для выявления конфиденциального контента используются цифровые отпечатки, это никак не меняет ситуацию. Например, цифровые отпечатки легко обмануть - злоумышленнику ничто не мешает воспользоваться стеганографией или хоть немного закодировать свое послание (используя различные кодировки, заменяя буквы цифрами и т.д.).

Второе поколение технологий – детерминистские методы или специальная разметка всех конфиденциальных документов. Это позволяет со 100% эффективностью защитить все секретные файлы, которые были признаны таковыми на этапе классификации данных. Однако здесь возникает целый ряд дополнительных препятствий: непонятно, что делать с новыми документами, которые пользователи создают после того, как система внедрена. Проблема в том, что продукт не справляется с задачей поддержания актуальности классификации документов.

Более того, такие решения обычно очень сложно внедрять, а на выходе получается система лишенная всякой гибкости. Ее использование приводит к разрастанию бюрократии в организации, что в конечном итоге провоцирует конфликты между службой информационной безопасности и другими департаментами[1] .

2.3. ВЫВОДЫ

Таким образом, знакомство с технологиями, которые были единственными на рынке до сегодняшнего дня, действительно отбивает всякое желание инвестировать в систему защиты корпоративных секретов. Однако новое поколение систем защиты конфиденциальности и целостности данных Perimetrix SafeSpace™, реализующее революционную концепцию Secret Documents Lifecycle™, позволяет избежать всех описанных выше ограничений, защитить инвестиции, создать гибкую и эффективную систему внутренней информационной безопасности.

1 Подробнее об эволюции технологий защиты от утечек см. документ «Secret Documents Lifecycle™ – новое поколение технологий для защиты корпоративных секретов»

3. ЗАЩИТА ДАННЫХ С ПОМОЩЬЮ PERIMETRIX SAFESPACE™

Компания Perimetrix реализовала работу с данными в том виде, в котором она десятилетиями используется на режимных объектах для защиты гостайны.

Вместо того чтобы концентрироваться на каналах утечки и попадать в ловушку предыдущего поколения, компания Perimetrix реализовала работу с данными в том виде, в котором она десятилетиями используется на режимных объектах для защиты государственной тайны. В результате появилось новое поколение технологий, защищающих секретные документы на всех этапах жизненного цикла – Secret Documents Lifecycle™ (далее SDL).

3.1. ЗАЩИТА ДАННЫХ НА ВСЕХ ЭТАПАХ ЖИЗНЕННОГО ЦИКЛА

Ключевая идея концепции SDL состоит в том, чтобы создать безопасное пространство, в котором пользователи могут работать с секретными документами под контролем системы защиты. Действительно, в каждой режимной организации есть секретная часть (специальный отдел), куда приходит человек, желающий получить доступ к секретному документу.

Прежде всего, он расписывается в журнале, где указывается, кто, когда, с какой целью и какой документ получил на руки. Далее другой служащий – хранитель архива секретных документов и своего рода библиотекарь – отыскивает нужный документ и выдает его на руки. Получив документ на руки, служащий никуда не уходит. Он может работать с секретными бумагами только в специально отведенном для этого месте – в том самом безопасном пространстве. То есть в распоряжении сотрудника есть читальный зал при секретной части, где можно сесть и ознакомиться с документом.

В то же время вся работа с документом протоколируется. Служащий не может исказить полученные секретные сведения, т.е. внести изменения в оригинал, уничтожить документ или каким-то образом скопировать. Конечно, если у сотрудника есть определенный уровень допуска, то он может модифицировать секретный документ, но в этом случае в отдельном журнале остаются записи о том, кто, когда, какие изменения и в какой документ внес. Так что в случае разбирательства всегда можно вычислить внутреннего нарушителя.

Отметим, что при таком подходе к работе с документом обеспечивается как аудит целостности секретного документа, так и защита его конфиденциальности от самых различных инцидентов, связанных с несанкционированным доступом. Например, сотрудник не может выйти из отведенного помещения с секретным документом, а потом его потерять или стать жертвой преступников, которые документ выкрадут. Все дело в том, что пространство, в котором используется и хранится секретный документ, находится под полным контролем, а потому абсолютно безопасно.

Конечно, только что описанный порядок работы с документом связан с большим количеством формальных процедур и высоким уровнем бюрократии. Однако все эти недостатки легко устранить, перенеся все операции и журналы событий в электронную среду: система защиты сама будет вести файл-отчет, отслеживать все изменения в документе, сохранять различные копии в архиве.

Однако технология SDL позволяет контролировать не только использование секретных документов. Она покрывает и все остальные этапы жизненного цикла документа: создание, хранение, архивирование, удаление, а также такие специфические вещи, как понижение уровня конфиденциальности документа и перенос его в другое хранилище[1].

Таким образом, технология SDL позволяет создать безопасное пространство, в котором документы хранятся, используются, передвигаются, в конечном счете, живут и умирают. Реализация этого безопасного пространства нашла свое место в комплексном решении Perimetrix SafeSpace™.

1 Подробнее о технологии Secret Documents Lifecycle™ см. отдельный документ «Secret Documents Lifecycle™ – новое поколение технологий для защиты корпоративных секретов»

PERIMETRIX

Любой из трех продуктов Perimetrix доступен для заказчиков в виде отдельного решения, однако синергия от использования сразу трех решений налицо.

3.2. СОСТАВ КОМПЛЕКСНОГО РЕШЕНИЯ PERIMETRIX SAFESPACE™

Perimetrix SafeSpace™ состоит из трех основных компонентов, каждый из которых доступен в виде отдельного продукта (см. рис. 1):

- **Perimetrix SafeStore™** – система первичной классификации документов с учетом многомерной модели конфиденциальности, а затем размещения секретных документов в распределенном хранилище SafeHouse™. Данный продукт обеспечивает защиту конфиденциальных данных во время хранения.
- **Perimetrix SafeUse™** – система контроля над использованием классифицированных секретных документов авторизованными сотрудниками. Продукт обеспечивает защиту информации при использовании, автоматическую классификацию новых документов, аудит целостности секретных документов и ретроспективный анализ с помощью центрального архива ShadowCore™.
- **Perimetrix SafeEdge™** – система мониторинга в режиме реального времени всех документов, покидающих сеть (SMTP, HTTP, Printer, IM, FTP, P2P), и автоматической классификации входящих документов. Продукт обеспечивает защиту данных в движении.

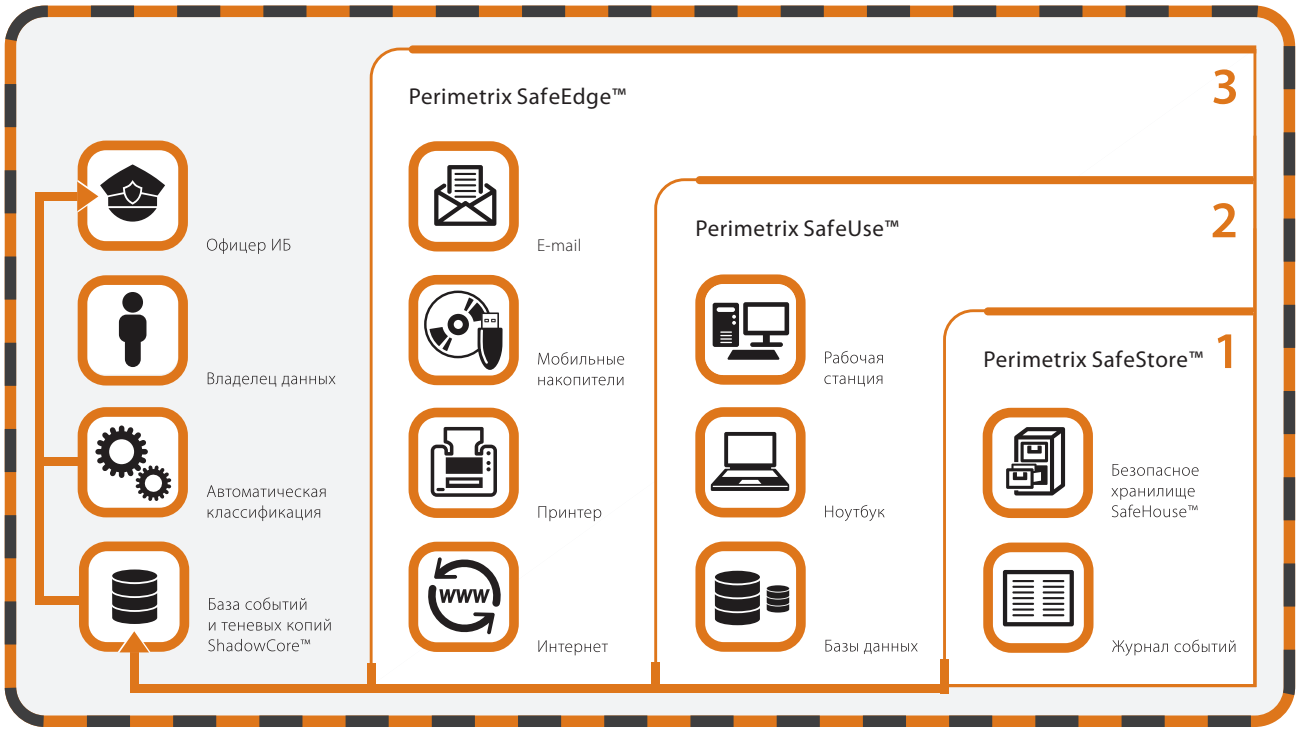

Рисунок 1. Схема работы Perimetrix SafeSpace™

PERIMETRIX

Хотя любой из трех продуктов Perimetrix доступен для заказчиков в виде отдельного решения, синергия от использования сразу трех компонентов налицо: организация может создать полноценную систему предотвращения утечек, которая покроет защиту данных при хранении (data-at-rest), использовании (data-in-use) и в движении (data-in-motion), а также обеспечит аудит целостности.

Интегрированная технология Perimetrix ReadyCompliance™ позволяет в считанные часы распределить секретные данные по категориям.

3.3. PERIMETRIX SAFESTORE™

Очевидно, что на момент создания системы защиты конфиденциальности и целостности данных в организации уже существует огромное количество документов. Поэтому первым этапом внедрения системы является классификация и категоризация всей информации. Этот процесс максимально упрощен по сравнению с продуктами предыдущих поколений. Интегрированная технология Perimetrix ReadyCompliance™ позволяет в считанные часы распределить секретные данные по категориям.

Когда стало понятно, насколько конфиденциален тот или иной документ, система Perimetrix SafeStore™ помечает каждый документ в соответствии с его классом секретности и уровнем доступа. При этом сама метка инкапсулируется в документ так, что она ни в коей мере не видна пользователям и не доступна для модификаций или удаления.

Встраиваемая метка содержит информацию о владельце и классе документа. Благодаря многомерной модели конфиденциальности класс может быть многомерной величиной. Например, класс может отражать:

- природу (категорию) информации в документе (финансовые, персональные данные, интеллектуальная собственность и т.д.);
- принадлежность к определенному департаменту (финансы, маркетинг, производство и др.);
- уровень конфиденциальности (для служебного пользования, секретно, совершенно секретно и пр.).

После того, как Perimetrix SafeStore™ пометит все классифицированные документы, продукт отправляет их в специальное хранилище Perimetrix SafeHouse™, где они хранятся только в зашифрованном виде.

PERIMETRIX

С точки зрения реализации, это хранилище может быть, как централизованным, так и распределенным. В последнем случае документы по-прежнему находятся на рабочих станциях пользователей, но уже в зашифрованном виде и с инкапсулированными метками. Таким образом, реализуется то самое защищенное хранилище, которое даже при краже вычислительной техники, потере ноутбука и любой другой атаке надежно защитит конфиденциальность и целостность секретных документов.

Защищенному хранилищу все равно, в каком виде и формате хранятся данные. Это могут быть текстовые документы, таблицы, рисунки, мультимедиа и даже базы данных. Например, в случае базы данных, сама база не помещается хранилище, но пользователи работают только с безопасным хранилищем, а данные из базы перед тем, как попасть к пользователю, проходят хранилище.

В заключение отметим, что Perimetrix SafeStore™ обеспечивает защиту секретных документов на ноутбуках и мобильных носителях. Ведь если служащий потеряет мобильное устройство, то документ все равно останется зашифрованным и будет абсолютно бесполезен для тех, в чьи руки попадет.

Perimetrix SafeUse™ всегда заранее и точно знает класс конфиденциальности документа, а потому принимает решение со 100% эффективностью и надежностью.

3.4. PERIMETRIX SAFEUSE™

После того, как все документы оказались в Perimetrix SafeHouse™, начинается рабочий процесс. Пользователи работают с документами, которые уже классифицированы, а также создают абсолютно новые документы. При этом все операции контролируются Perimetrix SafeUse™.

Работа с классифицированными и уже помеченными документами осуществляется в соответствии с заданными политиками. Это значит, что служащие не смогут осуществлять определенные операции с заданными классами информации, если у них нет соответствующих привилегий. Например, политика может полностью запретить копирование хотя бы части совершенно секретного документа всем служащим, кроме небольшой группы. В этом случае сотрудники без привилегий не смогут распечатать, скопировать на USB-носитель, отослать по почте или Интернету совершенно секретный документ. Более того, они даже не смогут пронести через буфер обмена даже несколько слов из текста этого документа. Хотя в случае попытки совершения запрещенных действий, офицер безопасности получит соответствующее уведомление.

PERIMETRIX

В процессе работы служащие используют не только уже классифицированные документы, а также создают новые документы. В этом случае, если сотрудники используют для создания нового документа предопределенный шаблон или информацию из уже существующих файлов, то происходит «заражение» нового документа метками конфиденциальности тех документов, которые использовались для его наполнения. Таким образом, все новые документы классифицируются автоматически (за исключением тех, которые создаются с нуля, без использования каких-либо существующих документов и заданных шаблонов).

Таким образом, Perimetrix SafeUse™ не гадает, является ли документ секретным и можно ли его выпустить за пределы корпоративной среды. Продукт всегда заранее и точно знает класс конфиденциальности документа, а потому принимает решение со 100% эффективностью и надежностью.

Отметим, что Perimetrix SafeUse™ столь же эффективно работает на мобильных компьютерах за пределами корпоративной сети. Выше уже говорилось, что Perimetrix SafeStore™ защищает секретные документы от несанкционированного доступа в случае кражи или потери мобильного устройства. Однако Perimetrix SafeUse™ существенно поднимает этот уровень защиты, позволяя обеспечить контроль над действиями сотрудников с помощью нескольких политик работы с классифицированными документами вне офиса. Рассмотрим пример реализации этих политик в зависимости от класса документа (приведенный ниже перечень может быть дополнен или изменен в зависимости от настроек и положений политики).

- **Для служебного пользования (ДСП).** В этом случае мобильный сотрудник может получить доступ к документам с использованием личного ключа, например, воспользовавшись сильной аутентификацией или авторизовавшись с помощью пароля. При данном уровне доступа контроль над тем, как служащий использует документ, не осуществляется.
- **Секретно.** Этот уровень доступа предполагает аутентификацию и последующий контроль использования секретных документов, который осуществляется точно так же, как и контроль внутри корпоративной сети. При этом, естественно, реализуется полный документооборот, посредством которого можно провести аудит целостности. При последующем подключении мобильного компьютера к корпоративной сети, все журналы событий и базы аудита передаются в центральный архив.

- **Совершенно секретно.** В этом случае для получения доступа к документу необходимо пройти аутентификацию и установить VPN-соединение с корпоративной сетью. После этого можно работать с совершенно секретным документом. Естественно, все действия контролируются и записываются для последующего аудита. Кроме того, обеспечивается нотификация о любых нарушениях в режиме реального времени. В результате в случае необходимости офицер безопасности может удаленно лишить мобильного сотрудника прав доступа к совершенно секретному документу.

Ранее уже упоминался центральный архив Perimetrix ShadowCore™ – это ключевой компонент продукта Perimetrix SafeUse™, который позволяет эффективно решить задачу аудита целостности секретных документов.

В центральную базу данных Perimetrix ShadowCore™ записываются как все события (кто, когда, какую операцию произвел и с каким документом), так и теневые копии самих документов (циркулирующие внутри сети, покидающие ее пределы). Таким образом, создается мощная основа для ретроспективного анализа и расследования инцидентов. Используя эту базу данных, офицеры безопасности могут собирать и анализировать статистику, строить графики и отчеты. На основании этих сведений можно определить, насколько эффективно используются информационные ресурсы организации, сбалансировать и оптимизировать потоки данных и внутренние коммуникационные процессы.

Важно, что Perimetrix SafeUse™ содержит встроенную единую систему идентификации пользователей. Это означает, что при помощи центральной базы всегда можно точно выяснить личность служащего, совершившего те или иные действия. Тем самым удается обойти ключевое ограничение лоскутных систем защиты, которые состоят из нескольких не интегрированных компонентов. Такие лоскутные системы позволяют отслеживать действия с каналом Интернета, идентифицируя пользователей только в виде обезличенных IP-адресов (которые могут быть динамическими), с email – по почтовым адресам (которые легко фальсифицируются), со съемными носителями – по именам учетных записей.

Анализируя центральную базу и расследуя уже случившийся инцидент, можно выявить цепочку событий, которая предшествовала попытке утечки или другим нарушениям. При накоплении такой информации становится возможной проактивная защита от внутренних угроз информационной безопасности, когда защитные меры принимаются еще до того, как нарушитель успеет подготовиться к реальным действиям.

Отметим, что аудит целостности является ключевым требованием целого ряда нормативных актов, стандартов и директив. В частности аудиту целостности финансовых документов особое внимание уделяет закон SOX, ставший стандартом де-факто в сфере корпоративного управления. Кроме того, аудит целостности секретных документов является краеугольным камнем любого стандарта по информационной безопасности, управлению рисками и т.д.

Аудит целостности предполагает, что каждый чувствительный документ должен быть защищен от искажения (вплоть до полного уничтожения). Для этого создаются средства внутреннего контроля, которые в общем виде не могут помешать модификации важных документов теми служащими, у которых есть на это соответствующие права. Однако средства внутреннего контроля всегда позволяют выявить кто, какие изменения и в какой документ внес, а также восстановить важные файлы в оригинальном виде (даже после уничтожения).

Продукт Perimetrix SafeUse™ и модуль ShadowCore™ в полной мере адресуют задачу аудита целостности и защиты от искажения и уничтожения документов. Центральный архив содержит в себе все необходимые сведения для аудита: различные версии документов, а также указания, кто, когда, как и что изменил. В случае необходимости легко поднять историю любого документа и последить весь его жизненный цикл. Найти тот момент, когда внутренний нарушитель исказил отчет. Узнать, когда и как он это сделал, а потом откатить изменения, просто восстановив оригинальную версию документа.

В основе Perimetrix SafeEdge™ лежат сразу три вероятностных метода выявления конфиденциальной информации: цифровые отпечатки, лингвистический (эвристический) и сигнатурный анализ.

3.5. PERIMETRIX SAFEEDGE™

Продукт Perimetrix SafeUse™ позволяет со 100% эффективностью защитить уже классифицированные документы. Однако если пользователь создает новый документ, не используя для этого существующие документы и предопределенные шаблоны, то новый документ не будет классифицирован автоматически.

Исследование компании Perimetrix показало, что служащие очень редко создают и наполняют новые документы без использования каких-либо уже существующих. Обычно доля таких документов не превышает 0,5% от общей массы создаваемых документов. Так что автоматической классификации не подвергается лишь малая часть вновь создаваемых в компании документов. Тем не менее, их тоже следует защищать – в этом и состоит главная задача Perimetrix SafeEdge™.

В основе Perimetrix SafeEdge™ лежат сразу три вероятностных метода выявления конфиденциальной информации: цифровые отпечатки, лингвистический (эвристический) и сигнатурный анализ. Как говорилось выше, эффективность всех этих методов ограничена 80%, но в данном случае не следует забывать, что на долю неклассифицированных документов приходится лишь 0,5% всего трафика.

Таким образом, доля ложных срабатываний или пропущенных секретных документов по теории вероятности составляет 0,005 x 0,8 = 0,004. Другими словами, эффективность технологии равна 99,6%, что вполне подходит для оценки рисков и моделирования угроз. Говорить о ложных срабатываниях здесь вообще не приходится.

При этом обеспечивается защита неклассифицированных документов, даже если они покидают сеть не через сетевой шлюз (почта, Интернет, принтер), а через порты рабочей станции. Например, если файлы копируются на USB-носитель. В этом случае файл все равно отправляется на сервер фильтрации для классификации в режиме реального времени. Это не создает дополнительной нагрузки на рабочую станцию, сеть организации и специалистов по информационной безопасности, так как число таких неклассифицированных документов крайне низко.

PERIMETRIX

Конечно, неклассифицированные документы могут храниться и накапливаться на рабочих станциях пользователей, если те не высылают их за пределы сети, что приводит к автоматической классификации документов. Однако в этом случае подключается продукт Perimetrix SafeStore™, который по определенному расписанию (ночью раз в сутки или на выходных еженедельно – в зависимости от размера организации) будет сам производить инвентаризацию и классификацию документов. Все новые документы будут автоматически классифицированы и помещены в хранилище SafeHouse™.

В заключение заметим, что Perimetrix SafeEdge™ осуществляет защиту данных в движении. Если секретный документ покидает корпоративную сеть и направляется, например, к партнеру, то шифрование исходящего трафика может производиться автоматически в соответствии с политикой и абсолютно прозрачно.

3.6. ПУБЛИКАЦИЯ СЕКРЕТНЫХ ДОКУМЕНТОВ

При использовании отдельных продуктов или всего комплексного решения Perimetrix SafeSpace™ может возникнуть ситуация, когда секретный документ необходимо передать в небезопасную среду в незащищенном виде. Для этих целей предусмотрена процедура понижения уровня конфиденциальности документа.

Очевидно, что, копируя данные из секретного документа, служащий может создать публичный файл, предназначенный для дальнейшего использования или пересылки за пределы организации. В этом случае сотрудник может инициировать процедуру понижения уровня секретности, что потребует участия еще одного или двух других сотрудников, в зависимости от действующей политики безопасности. Например, офицера безопасности, непосредственного руководителя или уполномоченного лица.

Для пользователей, которые часто создают публичные документы, предусмотрены определенные шаблоны документов, которые позволяют сразу же создавать несекретные файлы. Однако во время этого процесса служащие не смогут работать с конфиденциальной информацией в других документах, что вполне логично.

Высокая производительность Perimetrix SafeSpace™ обеспечивается с помощью уникальных балансировщиков нагрузки.

3.7. ПРОИЗВОДИТЕЛЬНОСТЬ И МАСШТАБИРУЕМОСТЬ

Продукт Perimetrix SafeSpace™ создавался для защиты секретных документов в крупных организациях, в которых более 500 рабочих станций. Основным требованием таких заказчиков являются высокая производительность и легкая масштабируемость.

Высокая производительность Perimetrix SafeSpace™ обеспечивается с помощью уникальных балансировщиков нагрузки, которые найдут самый быстрый способ обработать задание и перераспределят нагрузку в случае выхода из строя одного или нескольких из элементов.

Высокая масштабируемость основана на кластерной структуре решения, которая позволяет легко добавлять новые элементы. В Perimetrix SafeSpace™ практически нет таких модулей, которые не приспособлены для работы в кластере. Поэтому любое узкое место легко превращается в кластер, а добавление еще одного узла в этот кластер решает проблему производительности.

Также заметим, что компоненты Perimetrix SafeSpace™ являются полностью независимыми от платформы: они могут работать на Windows, Linux или Unix.

3.8. ВЫВОДЫ

В отличие от стандартных и уже устаревших продуктов, концентрирующихся на отдельных каналах утечки, Perimetrix SafeSpace™ позволяет обеспечить крайне высокий уровень безопасности (с эффективностью более 99%), защитить данные при хранении и использовании, а также в движении. Ключевым преимуществом решения является то, что данный подход решает проблему комплексно и целиком. Вне зависимости от того, потеряют служащие организации ноутбук с секретными документами или попытаются скопировать конфиденциальную информацию на USB-носитель, утечки не произойдет. Таким образом, SafeSpace™ позволяет раз и навсегда решить проблему защиты конфиденциальности и целостности данных.

PERIMETRIX

4. О КОМПАНИИ PERIMETRIX

Компания Perimetrix разрабатывает системы защиты корпоративных секретов третьего поколения. Благодаря реализации революционной концепции Secret Documents Lifecycle™ наши решения обеспечивают гарантированную 100% защиту секретных документов, полный контроль над каналами коммуникаций и полноценный аудит электронных операций.

В отличие от конкурентов Perimetrix концентрирует весь свой потенциал, инновационный подход и уникальный опыт на решении важнейшей задачи заказчиков – сохранении корпоративных секретов для повышения конкурентоспособности, установления плодотворных отношений с инвесторами и партнерами, соответствия государственным требованиям.

Компания основана в 2007 году инновационной командой профессионалов, стоявших у истоков создания современных систем защиты от внутренних IT-угроз. Perimetrix входит в группу компаний «КомпьюЛинк» – лидирующий альянс на российском рынке информационных технологий. Устойчивое финансовое положение группы, ее уникальный опыт и знания, внушительная база заказчиков служат надежным фундаментом развития Perimetrix. Благодаря мощной поддержке «КомпьюЛинка» компания имеет возможность выполнять комплексные проекты по внутренней IT-безопасности, выйти в лидеры российского рынка и создать основу для международной экспансии.

PERIMETRIX

Штаб-квартира Perimetrix

Российская федерация,
119607, Москва,
Мичуринский проспект, д. 45

Телефон: +7 495 737 99 91
Факс: +7 495 737 99 92

info@perimetrix.com
www.perimetrix.com

KEEPING SECRETS SAFE

PERIMETRIX