Решение Cisco Security Agent для предотвращения утечки данных

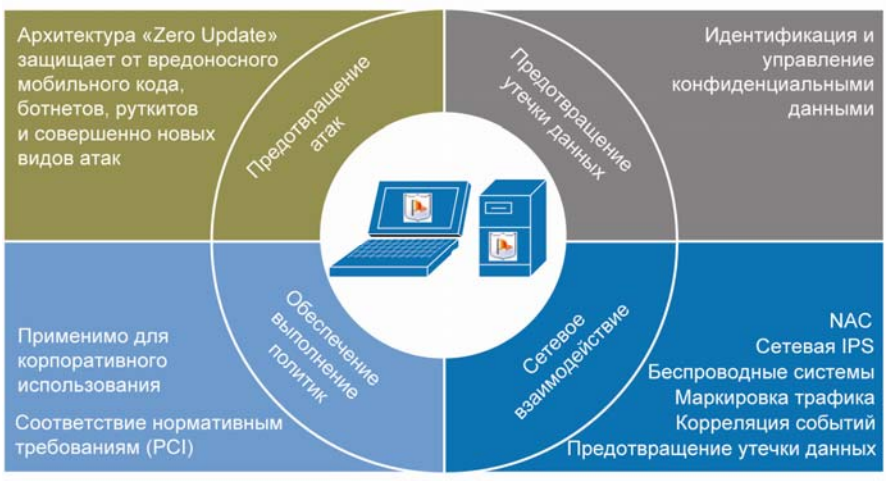
Утечка данных — серьезная проблема для бизнеса. В условиях распространения атак и вредоносного ПО, целью которых является получение прибыли, компании должны принять меры по обеспечению безопасности для защиты конфиденциальной информации и соблюдения регулятивных и внутренних корпоративных требований. Во избежание развертывания сложного, трудно управляемого отдельного решения, предназначенного для защиты только от одной проблемы, необходимо сделать обдуманный выбор. Требуется решение, которое будет защищать не только важные данные, но и целостность самого оконечного устройства, а также решать и многие другие задачи защиты.

Cisco® Security Agent предоставляет полностью интегрированное решение по защите рабочих станций и ноутбуков, сочетающее возможности предотвращения утечек данных на основе политик и архитектуру «Zero Update» (не требует обновления «сигнатур») для обнаружения и предотвращения вирусных атак — все это в рамках одного агента и одной консоли управления. С помощью этого уникального набора возможностей Cisco Security Agent защищает оконечные устройства от утечек данных, происходящих в результате как действий вредоносных программ, так и пользователей, и обеспечивает соблюдение политик допустимого использования и соответствия нормативным требованиям в рамках унифицированной инфраструктуры управления. Возможности Cisco Security Agent по предотвращению утечек данных объединены с функциями предотвращения атак «zero-update» для защиты оконечных устройств от целевых атак, вредоносного мобильного кода, руткитов (вредоносного ПО для скрытого удаленного управления), червей и совершенно новых атак. Cisco Security Agent защищает важные данные и обеспечивает защиту от вредоносного ПО в едином интегрированном агенте.

Cisco Security Agent

Комплексная постоянная защита оконечного устройства

Рисунок 1. Общие сведения о Cisco Security Agent

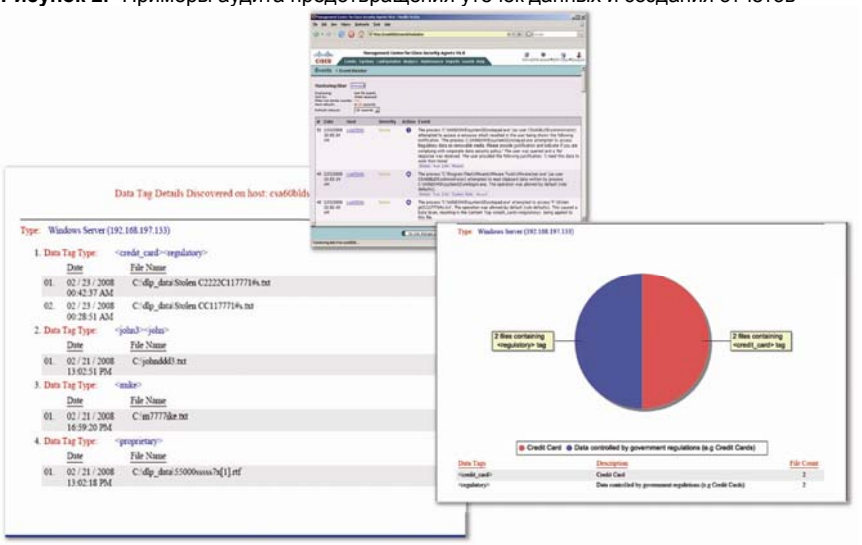


Интеграция агента и системы управления

Предотвращение утечки данных

Cisco Security Agent обеспечивает контроль конфиденциальных данных и управление ими на всех оконечных устройствах, защищая от утечки данных, связанной как с действиями пользователей, так и целенаправленного вредоносного ПО. С помощью недавно введенных функций сканирования содержимого Cisco Security Agent может находить в локальных файлах номера кредитных карт, номера карт социального страхования, а также определенные заказчиком конфиденциальные данные. Для предотвращения злонамеренного копирования данных на съемное устройство (через порт USB) или с помощью небезопасного сетевого приложения можно при необходимости использовать аудит доступа к конфиденциальной информации и средства управления политиками. Доступ к конфиденциальной информации может быть предоставлен только авторизованным пользователям, все другие попытки доступа будут блокироваться и регистрироваться. В целях проведения аудита и соответствия нормативным требованиям целостность конфиденциальных файлов и журналов может быть защищена путем блокировки и регистрации попыток каких-либо изменений. Средства контроля местоположения позволяют обеспечить соблюдение политик доступа к важным данным или запретить печать документов вне офиса. Cisco Security Agent позволяет запрашивать конечного пользователя о причине выполняемых им действий с конфиденциальной информацией. Ответы пользователя попадают в журнал аудита, не оказывая негативное воздействие на производительность труда сотрудника и своевременный доступ к важным данным. Кроме того, пользовательский интерфейс переведен на 11 языков (включая русский), что облегчает развертывание в разных языковых средах.

Рисунок 2. Примеры аудита предотвращения утечек данных и создания отчетов



Решение Cisco Security Agent для предотвращения утечки данных

Управление предопределенными и настраиваемыми политиками осуществляется централизованно с помощью средства Management Center для агентов Cisco Security Agent, которое обеспечивает эффективное предоставление отчетности и проведение аудита для всех действий, связанных с утечкой данных. Management Center имеет административный интерфейс, позволяющий изменять конфигурации решения по предотвращению утечек данных, выполнять анализ событий, создавать детализированные политики и генерировать отчеты. Журналы и отчеты по предотвращению утечек данных образуют единое консолидированное хранилище всех связанных событий. Сведения о доступе пользователя к конфиденциальным данным записываются в журнал для обеспечения соответствия нормативным требованиям и возможности проведения аудита.

Уникальное сетевое взаимодействие

Функции по предотвращению утечек данных Cisco Security Agent являются частью большего решения Cisco для защиты критически важных сетевых сегментов. Cisco Security Agent выполняет сканирование содержимого узла, которое дополняет возможности сканирования и защиты периметра сети Cisco IronPort Appliance. При работе пользователей вне офиса Cisco Security Agent может принудительно использовать доступ в корпоративную виртуальную частную сеть (VPN) для предотвращения обхода сервисов защиты Cisco IronPort для электронной почты и работы в Интернете.

Функции Cisco Security Agent по предотвращению утечек данных работают вместе с системой управления доступом к сети Cisco (NAC), улучшая контроль конфиденциальных данных и управление ими. Система Cisco NAC Appliance содержит предварительно настроенные проверки присутствия и состояния Cisco Security Agent на узле. В дополнение к отчетности по информационной безопасности Cisco Security Agent может сообщать Cisco NAC Appliance о наличии конфиденциальных данных, что позволяет Cisco NAC Appliance при необходимости изолировать подозрительный или зараженный компьютер.

Рисунок 3. Интегрированные сетевые решения CSA с NAC, DLP и IronPort

Рассмотрим следующий пример. Cisco Security Agent сообщает Cisco NAC Appliance, что на компьютере находится файл с электронной таблицей, содержащей большое количество номеров кредитных карт. Этот компьютер входит в группу продаж. Данный момент является нарушением корпоративной политики, поскольку доступ к персональным данным (PII) должны иметь только сотрудники отдела кадров. Cisco Security Agent обеспечивает уникальную связь между оконечным устройством и механизмами сетевой безопасности, таким образом, компьютер изолируется и пользователь получает уведомление о нарушении политики. При этом создается и регистрируется предупреждение для немедленного исправления.

Постоянная защита оконечного устройства

Cisco Security Agent версии 6.0 является первым решением для защиты оконечных устройств, которое объединяет в рамках одного агента функции защиты от атак, предотвращения утечек данных на основе политик и обнаружения вирусов как на основе сигнатур, так и на основе профилей несанкционированных действий. Этот уникальное сочетание возможностей обеспечивает защиту серверов, настольных систем и ноутбуков от совершенно новых атак и обеспечивает соблюдение политик допустимого использования и соответствия нормативным требованиям в рамках простой инфраструктуры управления.