Обзор DLP-систем на мировом и российском рынке

www.anti-malware.ru/analytics/Technology_Analysis/DLP_market_overview_2014

Данный обзор даёт краткие ответы на вопросы: что такое DLP-системы, как они возникли и развиваются, какие они бывают, как они устроены, какие DLP-решения можно купить на российском рынке, какие у них основные преимущества и недостатки.

Введение

Обзор предназначен для всех интересующихся рынком решений в сфере DLP и, в первую очередь, для тех, кто хочет выбрать подходящее для своей компании DLP-решение. В обзоре рассматривается рынок систем DLP в широком понимании этого термина, даётся краткое описание мирового рынка и более подробное — российского сегмента.

Системы защиты ценных данных существовали с момента их появления. В течение веков эти системы развивались и эволюционировали вместе с человечеством. С началом компьютерной эры и переходом цивилизации в постиндустриальную эпоху, информация постепенно стала главной ценностью государств, организаций и даже частных лиц. А основным инструментом её хранения и обработки стали компьютерные системы.

Государства всегда защищали свои секреты, но у государств свои средства и методы, которые, как правило, не оказывали влияния на формирование рынка. В постиндустриальную эпоху частыми жертвами компьютерной утечки ценной информации стали банки и другие кредитно-финансовые организации. Мировая банковская система первой стала нуждаться в законодательной защите своей информации. Необходимость защиты частной жизни осознали и в медицине. В результате, например, в США были приняты Health Insurance Portability and Accountability Act (HIPAA), Sarbanes–Oxley Act (SOX), а Базельский комитет по банковскому надзору выпустил ряд рекомендаций, называемый «Basel Accords». Такие шаги дали мощный толчок развитию рынка систем защиты компьютерной информации. Вслед за растущим спросом стали появляться компании, предлагавшие первые DLP-системы.

Что такое DLP-системы?

Общепринятых расшифровок термина DLP несколько: Data Loss Prevention, Data Leak Prevention или Data Leakage Protection, что можно перевести на русский как «предотвращение потери данных», «предотвращение утечки данных», «защита от утечки данных». Этот термин получил широкое распространение и закрепился на рынке примерно в 2006 году. А первые DLP-системы возникли несколько раньше именно как средство предотвращения утечки ценной информации. Они были предназначены для обнаружения и блокирования сетевой передачи информации, опознаваемой по ключевым словам или выражениям и по заранее созданным цифровым «отпечаткам»

конфиденциальных документов.

Дальнейшее развитие DLP-систем определялось инцидентами, с одной стороны, и законодательными актами государств, с другой. Постепенно, потребности по защите от различных видов угроз привели компании к необходимости создания комплексных систем защиты. В настоящее время, развитые DLP-продукты, кроме непосредственно защиты от утечки данных, обеспечивают защиту от внутренних и даже внешних угроз, учёт рабочего времени сотрудников, контроль всех их действий на рабочих станциях, включая удалённую работу.

При этом, блокирование передачи конфиденциальных данных, каноническая функция DLP-систем, стала отсутствовать в некоторых современных решениях, относимых разработчиками к этому рынку. Такие решения подходят исключительно для мониторинга корпоративной информационной среды, но в результате манипуляции терминологией стали именоваться DLP и относиться в этому рынку в широком понимании.

В настоящее время основной интерес разработчиков DLP-систем сместился в сторону широты охвата потенциальных каналов утечки информации и развитию аналитических инструментов расследования и анализа инцидентов. Новейшие DLP-продукты перехватывают просмотр документов, их печать и копирование на внешние носители, запуск приложений на рабочих станциях и подключение внешних устройств к ним, а современный анализ перехватываемого сетевого трафика позволяет обнаружить утечку даже по некоторым туннелирующим и зашифрованным протоколам.

Помимо развития собственной функциональности, современные DLP-системы предоставляют широкие возможности по интеграции с различными смежными и даже с конкурирующими продуктами. В качестве примеров можно привести распространённую поддержку протокола ICAP, предоставляемого прокси-серверами и интеграцию модуля DeviceSniffer, входящего в «Контур информационной безопасности SearchInform», с Lumension Device Control. Дальнейшее развитие DLP-систем ведет к их интеграции с IDS/IPS-продуктами, SIEM-решениями, системами документооборота и защите рабочих станций.

DLP-системы различают по способу обнаружения утечки данных:

- при использовании (Data-in-Use) — на рабочем месте пользователя;
- при передаче (Data-in-Motion) — в сети компании;
- при хранении (Data-at-Rest) — на серверах и рабочих станциях компании.

DLP-системы могут распознавать критичные документы:

- по формальным признакам — это надёжно, но требует предварительной регистрации документов в системе;
- по анализу содержимого — это может давать ложные срабатывания, но позволяет обнаруживать критичную информацию в составе любых документов.

Со временем, изменились и характер угроз, и состав заказчиков и покупателей DLP-систем. Современный рынок предъявляет к этим системам следующие требования:

- поддержка нескольких способов обнаружения утечки данных (Data in-Use, Data -in-Motion, Data-at-Rest);
- поддержка всех популярных сетевых протоколов передачи данных: HTTP, SMTP, FTP, OSCAR, XMPP, MMP, MSN, YMSG, Skype, различных P2P-протоколов;
- наличие встроенного справочника веб-сайтов и корректная обработка передаваемого на них трафика (веб-почта, социальные сети, форумы, блоги, сайты поиска работы и т.д.);
- желательна поддержка туннелирующих протоколов: VLAN, MPLS, PPPoE, и им подобных;

- прозрачный контроль защищенных SSL/TLS протоколов: HTTPS, FTPS, SMTPS и других;
- поддержка протоколов VoIP-телефонии: SIP, SDP, H.323, T.38, MGCP, SKINNY и других;
- наличие гибридного анализа — поддержки нескольких методов распознавания ценной информации: по формальным признакам, по ключевым словам, по совпадению содержимого с регулярным выражением, на основе морфологического анализа;
- желательна возможность избирательного блокирования передачи критически важной информации по любому контролируемому каналу в режиме реального времени; избирательного блокирования (для отдельных пользователей, групп или устройств);
- желательна возможность контроля действий пользователя над критичными документами: просмотр, печать, копирование на внешние носители;
- желательна возможность контролировать сетевые протоколы работы с почтовыми серверами Microsoft Exchange (MAPI), IBM Lotus Notes, Kerio, Microsoft Lync и т.д. для анализа и блокировки сообщений в реальном времени по протоколам: (MAPI, S/MIME, NNTP, SIP и т.д.);
- желателен перехват, запись и распознавание голосового трафика: Skype, IP-телефония, Microsoft Lync;
- наличие модуля распознавания графики (OCR) и анализа содержимого;
- поддержка анализа документов на нескольких языках;
- ведение подробных архивов и журналов для удобства расследования инцидентов;
- желательно наличие развитых средств анализа событий и их связей;
- возможность построения различной отчётности, включая графические отчеты.

Благодаря новым тенденциям в развитии информационных технологий, становятся востребованными и новые функции DLP-продуктов. С широким распространением виртуализации в корпоративных информационных системах появилась необходимость её поддержки и в DLP-решениях. Повсеместное использование мобильных устройств как инструмента ведения бизнеса послужило стимулом для возникновения мобильного DLP. Создание как корпоративных так и публичных «облаков» потребовало их защиты, в том числе и DLP-системами. И, как логичное продолжение, привело к появлению «облачных» сервисов информационной безопасности (security as a service — SECaaS).

Принцип работы DLP-системы

Современная система защиты от утечки информации, как правило, является распределённым программно-аппаратным комплексом, состоящим из большого числа модулей различного назначения. Часть модулей функционирует на выделенных серверах, часть — на рабочих станциях сотрудников компании, часть — на рабочих местах сотрудников службы безопасности.

Выделенные сервера могут потребоваться для таких модулей как база данных и, иногда, для модулей анализа информации. Эти модули, по сути, являются ядром и без них не обходится ни одна DLP-система.

База данных необходима для хранения информации, начиная от правил контроля и подробной информации об инцидентах и заканчивая всеми документами, попавшими в поле зрения системы за определённый период. В некоторых случаях, система даже может хранить копию всего сетевого трафика компании, перехваченного в течение заданного периода времени.

Модули анализа информации отвечают за анализ текстов, извлечённых другими модулями из различных источников: сетевой трафик, документы на любых устройствах хранения информации в пределах компании. В некоторых системах есть возможность извлечения текста из изображений и распознавание перехваченных голосовых сообщений. Все анализируемые тексты сопоставляются с заранее заданными правилами и отмечаются соответствующим образом при обнаружении совпадения.

Для контроля действий сотрудников на их рабочие станции могут быть установлены специальные агенты. Такой агент должен быть защищён от вмешательства пользователя в свою работу (на практике это не всегда так) и может вести как пассивное наблюдение за его действиями, так и активно препятствовать тем из них, которые пользователю запрещены политикой безопасности компании. Перечень контролируемых действий может ограничиваться входом/выходом пользователя из системы и подключением USB-устройств, а может включать перехват и блокировку сетевых протоколов, теневое копирование документов на любые внешние носители, печать документов на локальные и сетевые принтеры, передачу информации по Wi-Fi и Bluetooth и много другое. Некоторые DLP-системы способны записывать все нажатия на клавиатуре (key-logging) и сохранять копий экрана (screen-shots), но это выходит за рамки общепринятых практик.

Обычно, в составе DLP-системы присутствует модуль управления, предназначенный для мониторинга работы системы и её администрирования. Этот модуль позволяет следить за работоспособностью всех других модулей системы и производить их настройку.

Для удобства работы аналитика службы безопасности в DLP-системе может быть отдельный модуль, позволяющий настраивать политику безопасности компании, отслеживать её нарушения, проводить их детальное расследование и формировать необходимую отчётность. Как ни странно, при прочих равных именно возможности анализа инцидентов, проведения полноценного расследования и отчетность выходят на первый план по важности в современной DLP-системе.

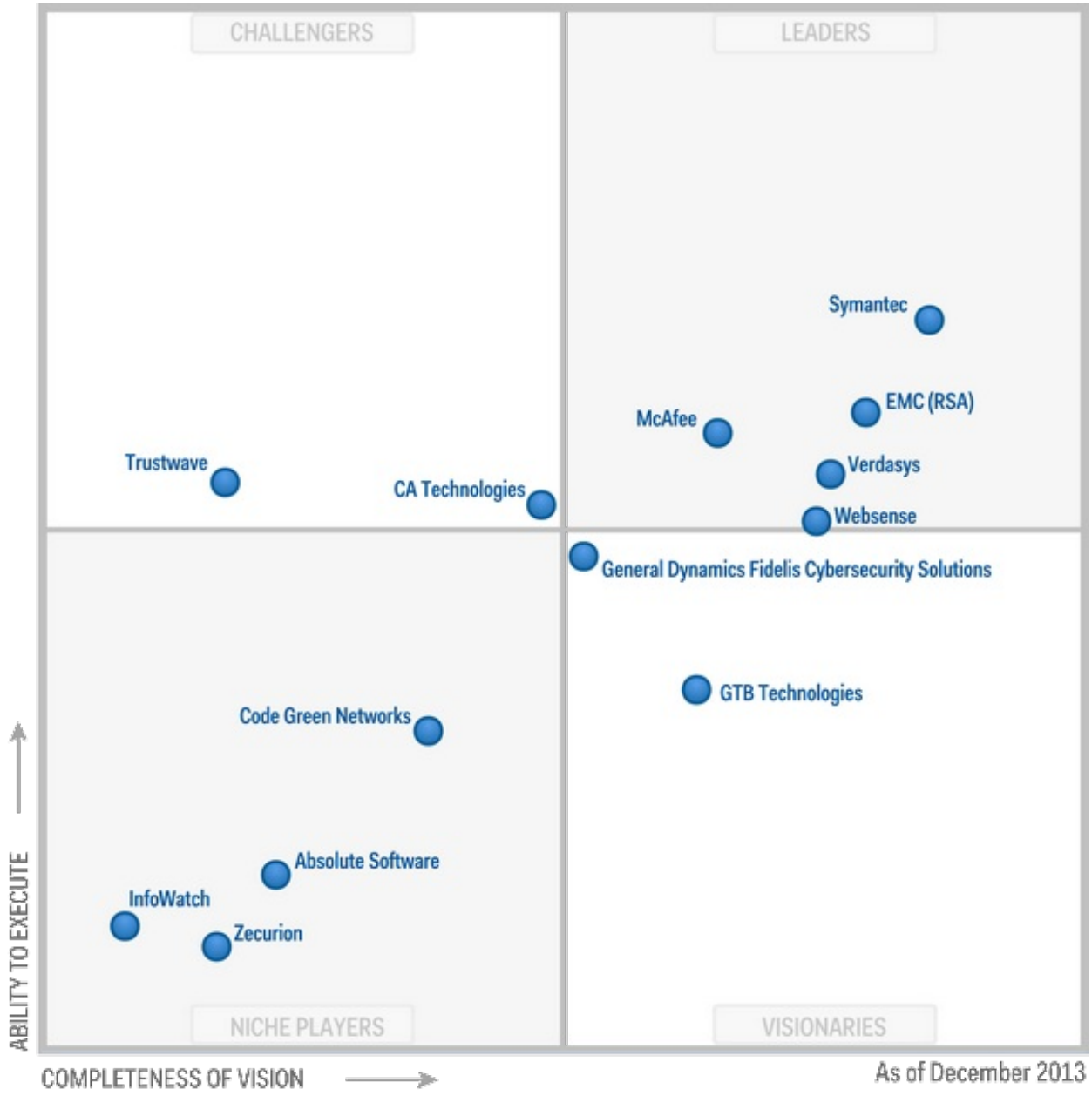
Мировой DLP-рынок

Рынок DLP-систем начал формироваться уже в этом веке. Как было сказано в начале статьи, само понятие «DLP» распространилось примерно в 2006 году. Наибольшее число компаний, создававших DLP-системы, возникло в США. Там был наибольший спрос на эти решения и благоприятная обстановка для создания и развития такого бизнеса.

Почти все компании, начинавшие создание DLP-систем и добившиеся в этом заметных успехов, были куплены или поглощены, а их продукты и технологии интегрированы в более крупные информационные системы. Например, Symantec приобрела компанию Vontu (2007), Websense — компанию PortAuthority Technologies Inc. (2007), EMC Corp. приобрела компанию RSA Security (2006), а McAfee поглотила целый ряд компаний: Onigma (2006), SafeBoot Holding B.V. (2007), Reconnex (2008), TrustDigital (2010), tenCube (2010).

В настоящее время, ведущими мировыми производителями DLP-систем являются: Symantec Corp., RSA (подразделение EMC Corp.), Verdasys Inc, Websense Inc. (в 2013 куплена частной компанией Vista Equity Partners), McAfee (в 2011 куплена компанией Intel). Заметную роль на рынке играют компании Fidelis Cybersecurity Solutions (в 2012 куплена компанией General Dynamics), CA Technologies и GTB Technologies. Наглядной иллюстрацией их позиций на рынке, в одном из разрезов, может служить магический квадрант аналитической компании Gartner на конец 2013 года (рисунок 1).

Рисунок 1. Распределение позиций DLP-систем на мировом рынке по Gartner



Российский DLP-рынок

В России рынок DLP-систем стал формироваться почти одновременно с мировым, но со своими особенностями. Происходило это постепенно, по мере возникновения инцидентов и попыток с ними бороться. Первым в России в 2000 году начала разрабатывать DLP-решение компания «Инфосистемы Джет» (сначала это был почтовый архив). Чуть позже в 2003 году был основан InfoWatch, как дочерняя компания «Лаборатории Касперского». Именно решения этих двух компаний и задали ориентиры для остальных игроков. В их число, чуть позже, вошли компании Perimetrix, SearchInform, DeviceLock, SecureIT (в 2011 переименованная в Zecurion). По мере создания государством законодательных актов, касающихся защиты информации (ГК РФ статья 857 «Банковская тайна», 395-1-ФЗ «О банках и банковской деятельности», 98-ФЗ «О коммерческой тайне», 143-ФЗ «Об актах гражданского состояния», 152-ФЗ «О персональных данных», и другие, всего около 50 видов тайн), возрастала потребность в инструментах защиты и рос спрос на DLP-системы. И через несколько лет на рынок пришла «вторая волна» разработчиков: Falcongaze, «МФИ Софт», Trafica. Стоит отметить, что все эти компании имели наработки в области DLP намного ранее, но стали заменты на рынке относительно недавно. Например, компания «МФИ Софт» начала разработку своего DLP-решения еще в 2005 году, а заявила о себе на

рынке только в 2011 году.

Ещё позже, российский рынок стал интересен и иностранным компаниям. В 2007-2008 годах у нас стали доступны продукты Symantec, Websense и McAfee. Совсем недавно, в 2012, на наш рынок вывела свои решения компания GTB Technologies. Другие лидеры мирового рынка тоже не оставляют попыток прийти на российский рынок, но пока без заметных результатов. В последние годы российский DLP-рынок демонстрирует стабильный рост (свыше 40% ежегодно) в течение нескольких лет, что привлекает новых инвесторов и разработчиков. Как пример, можно назвать компанию Iteranet, с 2008 года разрабатывающую элементы DLP-системы для внутренних целей, потом для корпоративных заказчиков. В в настоящий момент компания предлагает своё решение Business Guardian российским и зарубежным покупателям.

Сейчас российский рынок DLP-систем ещё находится на стадии формирования и далёк от насыщения. Хотя, как было сказано выше, у заказчиков уже возникло понимание их потребностей и сформировался устойчивый список требований к DLP-системам. Рассмотрим игроков российского рынка и их DLP-решения (подробнее — в детальном сравнении).

InfoWatch

Компания отделилась от «Лаборатории Касперского» в 2003 году. По итогам 2012 года InfoWatch занимает более трети российского DLP-рынка. InfoWatch предлагает полный спектр DLP-решений для заказчиков, начиная от среднего бизнеса и заканчивая крупными корпорациями и госструктурами. Наиболее востребовано на рынке решения InfoWatch Traffic Monitor. Основные преимущества их решений: развитый функционал, уникальные запатентованные технологии анализа трафика, гибридный анализ, поддержка множества языков, встроенный справочник веб-ресурсов, масштабируемость, большое количество предустановленных конфигураций и политик для разных отраслей. Отличительными чертами решения InfoWatch являются единая консоль управления, контроль действий сотрудников, находящихся под подозрением, интуитивно понятный интерфейс, формирование политик безопасности без использования булевой алгебры, создание ролей пользователей (офицер безопасности, руководитель компании, HR-директор и т.д.). Недостатки: отсутствие контроля за действиям пользователей на рабочих станциях, тяжеловесность InfoWatch Traffic Monitor для среднего бизнеса, высокая стоимость.

Подробнее об InfoWatch Traffic Monitor Enterprise

Обзор InfoWatch Traffic Monitor Enterprise 5.1. Часть 1 - защита от утечек на шлюзе

Инфосистемы Джет

Компания основана еще в 1991 году, на сегодняшний день является одним из столпов российского DLP-рынка. Изначально компания разрабатывала системы защиты организаций от внешних угроз и ее выход на DLP-рынок − закономерный шаг. Компания «Инфосистемы Джет» − важный игрок российского ИБ-рынка, оказывающий услуги системной интеграции и разрабатывающий собственное ПО. В частности, собственное DLP-решение «Дозор-Джет». Основные его преимущества: масштабируемость, высокая производительность, возможность работы с Big Data, большой набор перехватчиков, встроенный справочник веб-ресурсов, гибридный анализ, оптимизированная система хранения, активный мониторинг, работа «в разрыв», средства быстрого поиска и анализа инцидентов,

развитая техническая поддержка, в том числе в регионах. Также комплекс имеет возможности для интеграции с системами классов SIEM, BI, MDM, Security Intelligence, System and Network Management. Собственное ноу-хау – модуль «Досье», предназначенный для расследования инцидентов. Недостатки: недостаточный функционал агентов для рабочих станций, слабое развитие контроля за действиями пользователей, ориентированность решения только на крупные компании, высокая стоимость.

Подробнее о «Дозор-Джет»

Обзор «Дозор-Джет» 5.0 (актуальная версия 5.02)

Zecurion

Российская компания SecureIT была создана в 2001 год, а в 2012 году стала работать под новым брендом Zecurion. Компания начинала свою деятельность с разработки инструментов защиты хранилищ данных от несанкционированного доступа. Затем расширяла свою продуктовую линейку в сфере информационной безопасности. Комплексная DLP-система Zecurion состоит из трех продуктов: Zgate, Zlock и Zdiscovery. Каждый из них может поставляться как по отдельности, так и в виде единой системы. Основные преимущества: развитый функционал, модульность, встроенный справочник веб-ресурсов, развитые технологии анализа трафика, гибридный анализ, гибкая система отчетности. Недостатки: сложный интерфейс и средства анализа перехваченной информации, недостаточная интеграция между отдельными модулями.

Подробнее о продуктах Zecurion

Обзор новых возможностей Zecurion Zgate 4.0

Обзор новых возможностей Zecurion Zlock 5.0

Обзор Zecurion Zdiscovery 2.0

Websense

Американская компания, начинавшая свой бизнес в 1994 году как производитель ПО по информационной безопасности. В 1996 году представила свою первую собственную разработку «Internet Screening System» для контроля за действиями персонала в сети Интернет. В дальнейшем компания продолжила работу в сфере информационной безопасности, осваивая новые сегменты и расширяя ассортимент продуктов и услуг. В 2007 году компания усилила свои позиции на DLP-рынке, приобретя компанию PortAuthority. В 2008 году Websense пришла на российский рынок. В настоящий момент компания предлагает комплексный продукт Websense Triton для защиты от утечек конфиденциальных данных, а также внешних видов угроз. Основные преимущества: единая архитектура, производительность, масштабируемость, несколько вариантов поставки, предустановленные политики, развитые средства отчетности и анализа событий. Недостатки: нет поддержки ряда IM-протоколов, нет поддержки морфологии русского языка.

Подробнее о Websense Triton

Symantec

Корпорация Symantec является признанным мировым лидером на рынке DLP-решений. Произошло это после покупки в 2007 году компании Vontu, крупного производителя DLP-систем. С 2008 года Symantec DLP официально представлена и на российском рынке. В конце 2010 года, первой из иностранных компаний, Symantec локализовала свой DLP-продукт для нашего рынка. Основными преимуществами этого решения являются: мощный функционал, большое количество методов для анализа, возможность заблокировать утечку по любому контролируемому каналу, встроенный справочник веб-сайтов, возможность масштабирования, развитый агент для анализа событий на уровне рабочих станций, богатый международный опыт внедрения и интеграция с другими продуктами Symantec. К недостаткам системы можно отнести высокую стоимость и отсутствия возможностей контроля некоторых популярных IM-протоколов.

Подробнее о Symantec Data Loss Prevention

Обзор Symantec Data Loss Prevention 12.5

Falcongaze

Эта российская компания была основана в 2007 году как разработчик средств информационной безопасности. Основные преимущества решения Falcongaze SecureTower: простота установки и настройки, удобный интерфейс, контроль большего количества каналов передачи данных, развитые средства анализа информации, возможность мониторинга действий сотрудников на рабочих станциях (включая просмотр скриншотов рабочего стола), граф-анализатор взаимосвязей персонала, масштабируемость, быстрый поиск по перехваченным данным, наглядная система отчетности по различным критериям.

Недостатки: не предусмотрена работа в разрыв на уровне шлюза, ограниченные возможности блокировки передачи конфиденциальных данных (только SMTP, HTTP и HTTPS), отсутствие модуля поиска конфиденциальных данные в сети предприятия.

Подробнее о Falcongaze SecureTower

Обзор Falcongaze SecureTower 5.5

GTB Technologies

Американская компания, основанная в 2005 году. Благодаря собственным наработкам в области информационной безопасности имеет большой потенциал развития. На российский рынок пришла в 2012 и успешно реализовала несколько корпоративных проектов. Преимущества её решений: высокая функциональность, контроль множества протоколов и каналов потенциальной утечки данных, оригинальные патентованные технологии, модульность, интеграция с IRM. Недостатки: частичная русская локализация, нет русской документации, отсутствие морфологического анализа.

Подробнее о GTB Enterprise-Class DLP Suite

Обзор GTB Enterprise-Class DLP Suite

Iteranet

Российская компания, основанная в 1999 году как системный интегратор. В 2013 году реорганизована в холдинг. Одним из направлений деятельности является предоставление широкого спектра услуг и продуктов для защиты информации. Один из продуктов компании — DLP-система Business Guardian собственной разработки.

Преимущества: высокая скорость обработки информации, модульность, территориальная масштабируемость, морфологический анализ на 9 языках, поддержка широкого спектра протоколов туннелирования.

Недостатки: ограниченные возможности блокирования передачи информации (поддерживается только плагинами под MS Exchange, MS ISA/TMG и Squid), ограниченная поддержка шифрованных сетевых протоколов.

Подробнее о Business Guardian

МФИ Софт

«МФИ Софт» – это российская компания-разработчик систем информационной безопасности. Исторически компания специализируется на комплексных решениях для операторов связи, поэтому большое внимание уделяет скорости обработки данных, отказоустойчивости и эффективному хранению. Разработки в области информационной безопасности «МФИ Софт» ведет с 2005 года. Компания предлагает на рынке DLP-систему АПК «Гарда Предприятие», ориентированное на крупные и средние предприятия. Преимущества системы: простота развертывания и настройки, высокая производительность, гибкие настройки правил детектирования (включая возможность записи всего трафика), широкие возможности контроля каналов коммуникации (помимо стандартного набора включающие VoIP-телефонию, P2P и туннелирующие протоколы). Недостатки: отсутствие некоторых видов отчетов, отсутствие возможностей блокировки передачи информации и поиски мест хранения конфиденциальной информации в сети предприятия.

Обзор АПК "Гарда Предприятие" 2.1

SearchInform

Российская компания, основанная в 1995 году, изначально специализировавшаяся на разработке технологий хранения и поиска информации. Позже компания применила свой опыт и наработки в области информационной безопасности, создал DLP-решение под названием «Контур информационной безопасности». Преимущества этого решения: широкие возможности перехвата трафика и анализа событий на рабочих станциях, контроль рабочего времени сотрудников, модульность, масштабируемость, развитые инструменты поиска, скорость обработки поисковых запросов, граф-связи сотрудников, собственный запатентованный поисковый алгоритм «Поиск похожих», собственный учебный центр для обучения аналитиков и технических специалистов клиентов. Недостатки:

ограниченные возможности блокирования передачи информации, отсутствие единой консоли управления.

Подробнее о «Контуре информационной безопасности»

DeviceLock

Российская компания, основанная в 1996 году и специализирующаяся на разработке DLP- и EDPC-решений. В категорию DLP-производителей компания перешла в 2011 году, добавив к своему всемирно известному в категории EDPC решению DeviceLock (контроль устройств и портов на рабочих станциях Windows) компоненты, обеспечивающие контроль сетевых каналов и технологии контентного анализа и фильтрации. Сегодня DeviceLock DLP реализует все способы обнаружения утечки данных (DiM, DiU, DaR). Преимущества: гибкая архитектура и помодульное лицензирование, простота установки и управления DLP-политиками, в т.ч. через групповые политики AD, оригинальные патентованные технологии контроля мобильных устройств, поддержка виртуализованных сред, наличие агентов для Windows и Mac OS, полноценный контроль мобильных сотрудников вне корпоративной сети, резидентный модуль OCR (используемый в том числе при сканировании мест хранения данных). Недостатки: отсутствие DLP-агента для Linux, версия агента для Mac-компьютеров реализует только контекстные методы контроля.

Подробнее о Devicelock DLP Suite

Трафика

Молодая российская компания, специализирующаяся на технологиях глубокого анализа сетевого трафика (Deep Packet Inspection — DPI). На основе этих технологий компания разрабатывает собственную DLP-систему под названием Monitorium. Преимущества системы: простота установки и настройки, удобный пользовательский интерфейс, гибкий и наглядный механизм создания политик, подходит даже для небольших компаний. Недостатки: ограниченные возможности анализа (нет гибридного анализа), ограниченные возможности контроля на уровне рабочих станций, отсутствие возможностей поиска мест хранения несанкционированных копий конфиденциальной информации в корпоративной сети.

Обзор Monitorium 2.0

Выводы

Дальнейшее развитие DLP-продуктов идёт в направлении укрупнения и интеграции с продуктами смежных областей: контроль персонала, защита от внешних угроз, другие сегменты информационной безопасности. При этом, почти все компании работают над созданием облегчённых версий своих продуктов для малого и среднего бизнеса, где простота разворачивания DLP-системы и удобство её использования важнее сложного и мощного функционала. Также, продолжается развитие DLP для мобильных устройств, поддержки технологий виртуализации и SECaaS в «облаках».

С учётом всего сказанного, можно предположить, что бурное развитие мирового, и особенно российского DLP-рынков, привлечёт и новые инвестиции и новые компании. А это, в свою очередь, должно привести к дальнейшему росту количества и качества предлагаемых DLP-продуктов и услуг.