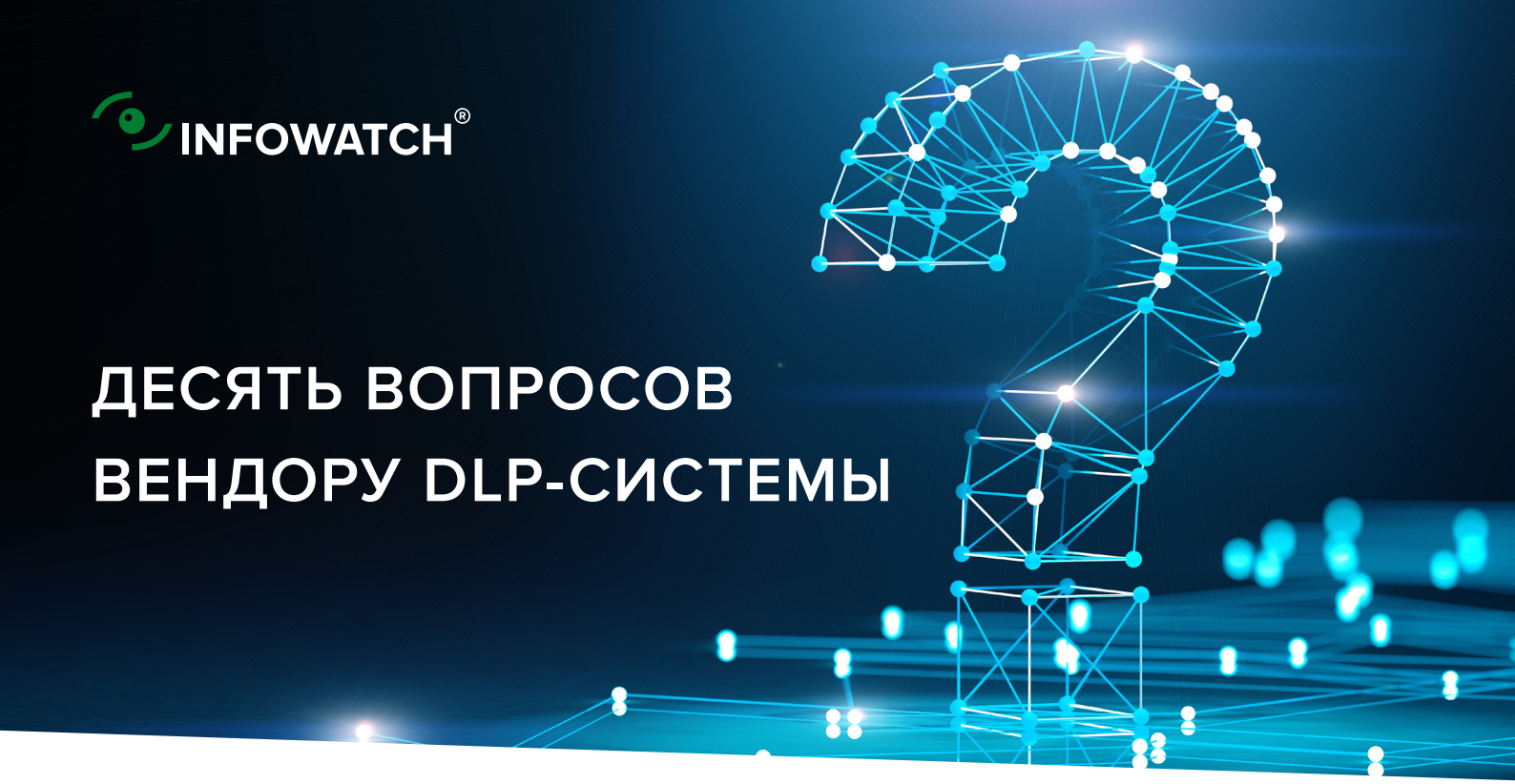
INFOWATCH®



ДЕСЯТЬ ВОПРОСОВ ВЕНДОРУ DLP-СИСТЕМЫ

1. Какие технологии анализа использует вендор?

Технологии лингвистического анализа — самая важная часть DLP системы. От точности «понимания» содержимого зависит количество ошибок, которые совершит система. То есть, в каком количестве случаев она пропустит чувствительную информацию, и сколько будет ложных срабатываний, когда система ошибочно сочтет отправку той или иной информации нарушением. Количество ложных срабатываний – один из самых критических показателей работы DLP, поскольку ложные срабатывания способны радикально увеличивать трудозатраты сотрудников ИБ службы, а в случае работы в режиме блокировки — мешать нормальному ходу бизнес-процессов.

К базовым технологиям, которые есть у всех вендоров, относится категоризация текстовых документов с использованием ключевых слов. Конечно же, система должна учитывать морфологию (словоформы), опечатки и транслитерацию.

Уточните, поддерживает ли вендор необходимые вам языки помимо русского.

Следующее — это отраслевые и тематические словари. Сколько таких словарей есть у вендора по вашей тематике и можно ли их пополнять самостоятельно? Чем больше, тем лучше.

Еще одна базовая технология — копирайтный анализ. Имея эталонный документ, система создает его текстовый или бинарный отпечаток и может детектировать его фрагменты или весь документ целиком. Далеко не все поддерживают технологию работы с растровыми отпечатками: при изменении разрешения картинки или формата файла картинка не может быть обнаружена при помощи бинарных отпечатков!

Использует ли ваш вендор верифицирующие функции для точной идентификации текстовых объектов, представляющих собой регулярные выражения, например, корректность номера кредитной карты проверяется с помощью алгоритма Луна?

Защита выгрузок из баз данных. (Не путаем с контролем доступа к БД! Технический специалист может иметь совершенно легитимный доступ к базе. А что происходит с данными после того, как они выгружены?) Это технология, которая позволяет защищать списки клиентов или мноменклатуру, персональные данные, другие именованные сущности, которые очень плохо защищаются с помощью регулярных выражений, потому что, во-первых, защищать нужно не абстрактные данные, которые могут перемещаться по компании в рамках рабочих процессов, а совершенно конкретные записи, хранящиеся в определенной базе, и автоматически поддерживать актуальной защиту при изменении этих данных, во-вторых, если у вас прайс-лист на 1000 позиций, вряд ли вы захотите создавать 1000 правил и обновлять их по мере обновления прайс-листа. Кроме того, часто конфиденциальным является сочетание нескольких полей, а не одно отдельно взятое поле, например ФИО+адрес.

Детектор бланков — технология, которая позволяет выявлять пересылку заполненных (в том числе, от руки!) или не заполненных бланков. Бланк предъявляется системе, после чего она должна идентифицировать изображения таких бланков, но заполненных.

Технологии детектирования графических объектов включают в себя:

- Распознавание текста файлов в графическом формате с помощью OCR.
- Детектирование документов с печатью, причем, с конкретной, и вне зависимости от того, стоит ли она поверх текста документа или подписи, как она повернута, отмасштабирована и хорошо ли пропечатана.
- Детектирование фотографий (а не только сканов!) документов. Фото отличается от скана большим количеством оптических искажений, что кратно усложняет задачу распознавания таких объектов. Вспомните, как выглядит кредитная карта, сфотографированная под углом, или паспорт — с не полностью раскрытыми страницами или с изгибами.
- Графический классификатор, который позволяет классифицировать разнообразные изображения: топографические карты (например, карты геологоразведки), картографические схемы, технические чертежи, формулы химических реагентов.
- Векторный копирайтный анализ позволяет защитить векторные изображения, например, чертежей: фрагмент чертежа может быть идентифицирован, даже если он вставлен в другой чертеж, модифицирован или отмасштабирован.

И наконец, возможность распознавать сложные документы. Например, поинтересуйтесь у вендора, сможет ли его система распознать скан товарно-транспортной накладной с определенной номенклатурой? Тут задействованы сразу три технологии: детектор бланков, защита выгрузки из БД и детектирование печатей.

Учтите, что при количестве сотрудников в компании более 5000, отсутствие продвинутых технологий анализа в DLP системе приводит к такому количеству ложных срабатываний, что делает ее попросту бесполезной.

2. По каким каналам DLP система анализирует трафик?

Конечно же, чем больше каналов умеет перехватывать система, тем лучше. Все вендоры примерно одинаковы с этой точки зрения и поддерживают мониторинг почты, основных мессенджеров, печати, копирования на съемные носители и в облако, облачные почтовые системы, и так далее.

Стоит уточнить у вендора, есть ли у него открытый API в случае, если у вас есть какие-то проприетарные приложения, например, для обмена мгновенными сообщениями, или если вы используете корпоративное облако: наличие API позволит вам и вашему интегратору поддержать и такие каналы передачи информации, адаптировав решение под ваши потребности и задачи. Важно не только перехватывать трафик, нужно уметь формировать политики, которые учитывают специфику тех приложений, с которыми выполняется интеграция, скорее всего, для этого потребуется передать из внешней системы в DLP какие-то специфические атрибуты событий, и DLP система должна позволять их обрабатывать наравне со стандартными.

3. Может ли DLP система устанавливаться в разрыв и блокировать распространение конфиденциальной информации?

Большинство систем на рынке умеют работать исключительно в режиме мониторинга, то есть, анализировать перенаправленную в них копию трафика. Если система используется в режиме мониторинга, то вы, конечно, сможете впоследствии понять, кто виноват, но предотвратить утечку не получится. Только если система установлена в разрыв, она сможет заблокировать передачу той информации, которая не должна уйти за пределы организации.

Дополнительно нужно уточнить, по каким каналам возможна блокировка, желательно, чтобы это была не только корпоративная электронная почта, блокироваться должна запись информации на съемные носители, загрузка на FTP и в облачные хранилища, отправка через веб-почту.

Решение о блокировке должно приниматься на основе полноценного контентного и лингвистического анализа текста, включая применение отраслевых и тематических словарей. Это необходимо для того, чтобы избежать ошибок первого и второго рода: если мы ошибочно детектируем информацию как конфиденциальную и блокируем, то это приводит к нарушению бизнес-процессов, а если пропускаем — налицо утечка.

Кроме того, решение должно приниматься достаточно быстро, чтобы сделать работу системы незаметной и не вызывающей раздражения у пользователя: если задержка копирования файлов на съемный носитель или в облако составляет минуты, а работа ПК ощутимо замедляется, вряд ли пользователям это понравится.

Таким образом, работа в разрыв накладывает серьезные технологические требования на DLP систему и требует продвинутого контентного анализа, а со стороны агента — стабильности, высокой производительности, нетребовательности к ресурсам и совместимости с множеством других приложений, в частности, с антивирусом.

Уточните у DLP вендора, есть ли у него проекты, где DLP используется в режиме блокировки.

4. Примеры реальных проектов, в которых система устанавливалась на большом количестве рабочих мест?

Большое — это сотни тысяч. Провести тестирование системы в «лабораторных» условиях на таком объеме живого, а не синтетического трафика практически невозможно. Если вы — первый крупный клиент у вендора, есть вероятность, что полноценное нагрузочное тестирование вендор проведет как раз на вас). Нужно ли вам это? А в том случае, если у вас относительно немного рабочих мест (по сравнению с названными выше цифрами), факт того, что система установлена и работает на больших проектах, будет для вас гарантией запаса производительности и надежности. Что будет делать система в случае, если ей не хватает производительности? Правильно, система будет либо вносить задержку в отправку сообщений и копирование файлов, которая не понравится вашим пользователям, либо проверять сообщения выборочно. То есть, не все. Очевидно, речи о полноценной защите в этом случае идти не может.

5. Как проверить удобство работы с системой, в частности, ее конфигурирование и обработку инцидентов.

Если разработчик системы думал о реальных сценариях использования, то он позаботился о том, чтобы пользователь тратил как можно меньше времени на выполнение своих регулярных задач. Настройки системы должны быть достаточно гибкими и позволять определять сложные объекты защиты, мы приводили выше пример такого объекта. Спросите у вендора, а можно ли потом отфильтровать список инцидентов по объекту защиты, представляющему из себя сложный документ?

Попробуйте оценить во время пилотного проекта, сколько времени у вас уйдет на то, чтобы понять, почему в конкретном случае было создано событие: какие фрагменты документа система сочла нарушением, какая политика сработала и на какой объект защиты. Продуманная зрелая система поможет вам сделать это быстро с помощью визуальных инструментов. А ведь эту вам придется выполнять многократно, когда вы будете дорабатывать свои политики, например, при переходе в режим блокировки.

6. Гибкость и скорость работы инструментов анализа данных и построения отчетности.

- Только ленивый вендор не имеет сейчас в своем арсенале графа связей. Попробуйте уточнить, это инструмент, который помогает проводить расследования, или же просто красивая визуализация для отчета?
- Может ли граф отразить коммуникации в масштабе всей компании, в которых была нарушена конкретная политика, причем, по неформальным каналам, например мессенджерам?
- Может ли граф связей быть перестроен «на лету» при изменении параметров фильтрации, или вы успеете выпить пару чашек кофе, пока картинка на вашем мониторе обновится?

7. Умеет ли система поддерживать политики безопасности в актуальном состоянии?

Наиболее интересные и чувствительные данные обычно создаются и хранятся в бизнес-приложениях. Если DLP-система не интегрирована с бизнес-приложениями, она всегда будет защищать устаревшие данные, потому что они постоянно

изменяются. Например, если ваша компания живет в SAP, то отсутствие интеграции с ним обернется для вас утратой контроля. Интеграция с бизнес-системами, возможность автоматического обновления базы эталонных документов обеспечивает актуальность политик безопасности.

Узнайте у своего вендора, с какими бизнес-системами есть интеграции у его DLP.

8. Может ли система отдавать данные во внешние приложения, например, SIEM, IRM?

Зрелые компании стремятся к централизации и унификации обработки инцидентов ИБ, часто они используют SIEM или IRM системы, куда собираются данные из множества других систем. Предполагается, что офицер безопасности работает в этой централизованной системе.

Для поддержки такого сценария работы DLP-система должна уметь отдавать свои события во внешнюю систему, а вердикт по событию, вынесенный офицером безопасности при работе в централизованной системе, нужно уметь передавать обратно в DLP систему.

9. Оказывает ли вендор дополнительные услуги по обеспечению правильного с юридической точки зрения внедрения DLP системы и расширенной технической поддержке?

Внедрение DLP системы подразумевает необходимость аккуратного выполнения целого ряда юридических действий, благодаря которым компания, с одной стороны, может обезопасить себя от необоснованных претензий, с другой стороны, иметь возможность использовать результаты работы системы для защиты своих интересов, в том числе, в судебном порядке. Поможет ли вам ваш вендор в процессе введения режима коммерческой тайны?

Еще один нюанс состоит в том, что в погоне за функционалом некоторые вендоры добавляют в свои решения такой функционал, который прямо нарушает законодательство и не может быть легализован никакими юридическими процедурами.

Ну и, наконец, есть ли возможность заключить контракт на техническую поддержку в соответствии с правилами и требованиями вашей компании? Далеко не все вендоры могут поддержать вас в режиме 24x7, обеспечив стандартное время реакции и решения инцидента.

10. Посмотрите, что и как говорит вендор о себе и о своих конкурентах.

Если вы задумались о защите своих данных, вы, конечно, осознаете их ценность для вашей организации.

Готовы ли вы сотрудничать и доверять чувствительную информацию «специалистам», не слишком разборчивым в средствах достижения цели? Конечно, любой вендор подписывает с вами соглашение о неразглашении конфиденциальной информации, однако, помимо соглашений есть еще понятия о бизнес этике. При найме сотрудников стало распространенной практикой просматривать их профили в соцсетях. Так почему бы не перенести эту практику на партнерские отношения и посмотреть, какие подходы и какую риторику используют руководители и сотрудники вендора, представляя свою компанию. Это раскроет принципы и ценности вашего потенциального партнера и даст вам ответ, можете ли вы на него положиться.

Остались вопросы? Свяжитесь с нами:

sales@infowatch.ru +7 495 22-900-22 infowatch.ru