"DLP уже не та"

Как меняется функционал и формат работы с системой

Рынок DLP-систем, каким его помнят старожилы, выглядел совсем не так, как сегодня. Программы были громоздкими и имели скромные возможности. Внедрение занимало около полугода, для настройки требовалось привлекать лингвистов. А за тестирование еще надо было платить. То есть DLP на старте – это такой "космический корабль" (долго, дорого, с непонятным эффектом), который был доступен только крупному бизнесу. Системы изменились, их применение стало более массовой практикой. Но порог вхождения в "клуб" пользователей DLP продолжает снижаться и сегодня, благодаря новым форматам работы с программой.

Что за "зверь" такой – DLP-система в 2020 году

Период, когда вендоры могли диктовать заказчикам, какой должна быть DLP-система, был непродолжительным и канул в Лету. С тех пор ситуацией владеют клиенты, а разработчики развивают продукты под их пристальным вниманием.

Это пошло рынку на пользу. Современные DLP-системы не сравнить с ранними версиями. Теперь программы умеют выполнять даже смежные функции: eDiscovery, Time Tracking, Risk Management, криптозащиты информации, аудита ИТ-инфраструктуры, контроля привилегированных пользователей и др.

С помощью программы заказчик может:

1. Проводить мониторинг перемещения информации по всем каналам, в том числе в облачных хранилищах, мессенджерах с шифрованием End-to-End (Telegram, WhatsApp, Viber), программах удаленного соединения (TeamViewer и аналоги).

2. Анализировать полученную в ходе мониторинга информацию. Система должна "вылавливать" любые нарушения даже самых специфических политик безопасности. В продвинутых DLP реализованы всевозможные варианты поиска, которые можно использовать по отдельности и в любой комбинации. Система должна уметь анализировать все популярные типы файлов, на любом языке.

3. Проводить подробные расследования, в том числе ретроспективные. Большинство корпоративных преступлений совершаются в электронном виде и оставляют цифровые следы. DLP-системы должны уметь находить причины, участников, последствия инцидентов. Поэтому нужно, чтобы программа делала теневое копирование, создавала архивы, позволяла поднимать информацию об активности пользователей в программах и процессах.

Мы в "СёрчИнформ" тоже ориентируемся на потребности практиков. Переработали архитектуру, что повысило производительность на 30%, и заказчикам приходится тратиться на "железо" меньше. Постоянно делаем доработки, чтобы не перегружать базу перехвата (например, применяя дедупликацию, кодеки для сжимания аудио, запись видео с экранов пользователей в выбранном качестве, в процентах от оригинала), вводим настройки и работаем над распределением нагрузки, чтобы не тормозили ПК пользователей.

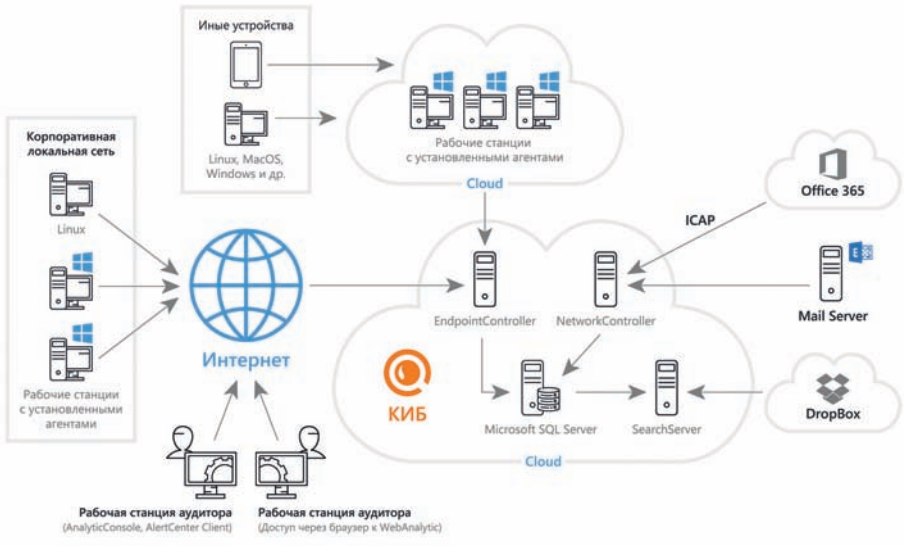

Рис.1. Схема работы "СёрчИнформ КИБ" в облаке

Сейчас DLP-системы – функционально зрелые продукты, и вендоры все больше внимания уделяют оптимизации и экономичности софта.

Эти изменения программ сейчас особенно востребованы, потому что бизнесы стремятся урезать любые лишние траты. Но все же главные изменения касаются форматов работы с DLP-системами: они позволяют заказчикам еще серьезнее оптимизировать бюджеты на внутреннюю безопасность.

DLP в облачном формате

Это хоть и не новый формат, но до последнего времени не широко распространенный. Сейчас его стали применять чаще. Не только по экономическим соображениям, но и потому что рынок предлагает более защищенные технологии. Крупные облачные провайдеры подчиняются жестким нормативам, используют механизмы защиты, которые недоступны среднему бизнесу, гораздо устойчивее к DDoS-атакам. Клиенты тоже стали доверять облакам больше.

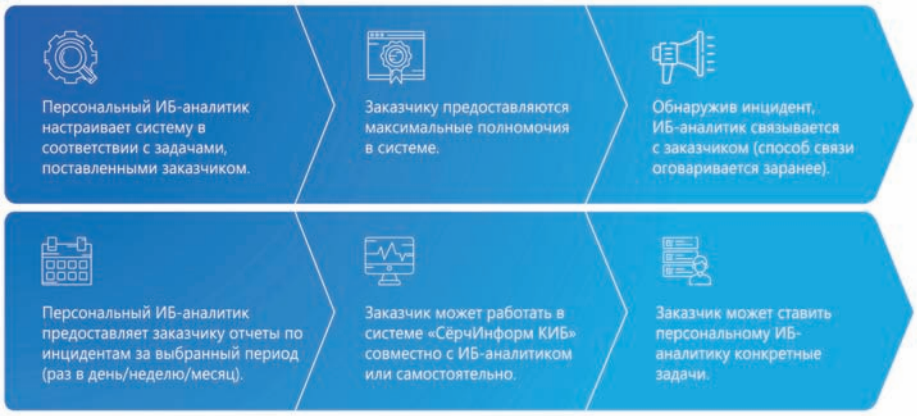

Рис.2. Модель взаимодействия с заказчиком при ИБ-аутсорсинге от "СёрчИнформ"

Сейчас DLP-системы – функционально зрелые продукты. Программы умеют выполнять даже смежные функции: eDiscovery, Time Tracking, Risk Management, криптозащиты информации, аудита ИТ-инфраструктуры, контроля привилегированных пользователей и др. Разработчики теперь все больше внимания уделяют оптимизации и экономичности софта. Но все же главные изменения касаются форматов работы с DLP-системами, что позволяет еще радикальнее снизить вложения в инфраструктуру и кадры.

По данным KPMG и Oracle, 75% ИБ-директоров считают публичные облака более безопасными, чем собственные ЦОД.

Мы, например, долгое время не предлагали разворачивать свою DLP в облаке, пока не убедились, что это можно сделать безопасно. Все данные с корпоративных ПК передаются в дата-центр по защищенным каналам, а доступ к "ядру" системы имеет только заказчик. Он платит за услугу помесячно, и ему не нужно приобретать, настраивать и обслуживать "железо".

Облачный формат очень востребован, так как многие компании намеренно отказываются от парка собственного оборудования. Формат подходит и когда бизнес растет, расширяет филиальную сеть. В этот период компании наращивают ИТ-инфраструктуру под основные бизнес-процессы, все остальные траты оказываются не в приоритете. Облачное исполнение становится выходом и когда нужно контролировать компьютеры большого штата сотрудников, работающих на удаленке.

Аутсорсинг внутренней информационной безопасности

Как решение экономической и кадровой проблемы возник и другой формат – ИБ-аутсорсинг. Заказчик получает DLP + специалиста-аналитика. Он выявляет инциденты, разбирает и докладывает о них клиенту. При этом DLP-система может быть как в полной собственности у заказчика, так и в аренде (в том числе и в описанном выше облачном формате).

Вдолгую ИБ-аутсорсинг обходится компаниям дороже, чем покупка лицензий. Но распределенная финансовая нагрузка в короткой перспективе оказывается оправданной. Аутсорсинг подходит тем компаниям, которые не могли оценить, оправданно ли покупать лицензии, "железо", искать ИБ-специалиста. Последнее особенно важно, потому рынок испытывает острый дефицит кадров. Не в любой даже крупной компании штат укомплектован полностью, что говорить об остальных.

Таким образом, сервис делает DLP демократичным инструментом, который становится доступен и малому бизнесу.

От "космических кораблей" до легких "гибридных автомобилей"!

Давайте на минуту вернемся к началу статьи и оценим, какой внушительный путь прошли системы.

Конечно, ситуация от вендора к вендору различается. Свою DLP "СёрчИнформ КИБ" мы развиваем в рамках описанного выше подхода. Она доступна и в традиционном формате, когда у заказчика есть своя ИБ-служба и лицензии в вечной собственности. Но возможна и в рассмотренных форматах, которые не требуют от клиента больших вложений в собственные кадры и инфраструктуру. При этом в нашем понимании система должна быть не просто "легким гибридом", но и трансформером – бесшовно интегрироваться с другими решениями по мере развития потребностей бизнеса. Это тоже дает оптимизацию бюджета при долгосрочном планировании.

Все продукты "СёрчИнформ" можно тестировать бесплатно в полном функционале в течение месяца. Запросите информацию на сайте searchinform.ru.

Ваше мнение и вопросы присылайте по адресу is@groteck.ru