Ростелеком
Солар

Как выбрать свою DLP-систему

На что следует обращать внимание при выборе DLP-системы прежде всего? Предлагаем вам изучить небольшой чек-лист для компаний из разных отраслей с основными критериями современной DLP-системы, составленный исходя из 20-ти летнего опыта разработки продукта Solar Dozor.

solar@rt-solar.ru

+7 (499) 755-07-70

www.rt-solar.ru

Оцените свои потребности

Перехват информации

- [ ] Облачные хранилища
- [ ] Локальные хранилища
- [ ] При записи на USB-носители любого типа
- [ ] Отправка документов на печать
- [ ] Мессенджеры
- [ ] Веб-ресурсы
- [ ] Скопированный текст
- [ ] Нажатия клавиш на ПК сотрудников
- [ ] Сообщения корпоративной почты

Контроль информации

- [ ] «Карантин» для конфиденциальных документов в файловых хранилищах
- [ ] Подмена или изменение содержания электронных писем
- [ ] Установка «в разрыв» для полной блокировки трафика в случае утечки
- [ ] Ведение архива коммуникаций сотрудников

Анализ информации

- [ ] Предиктивная аналитика (UBA) для профилактики инцидентов
- [ ] Сбор данных о рабочем дне сотрудника для проведения расследований
- [ ] Перефильтрация архива электронной почты после обновления политик
- [ ] Поддержка любых форматов файлов
- [ ] Анализ и блокирование передачи графических объектов
- [ ] Поиск паролей для архивов и их распаковка
- [ ] Подключение внешних модулей для анализа информации

Enterprise-возможности

- [ ] Объединение территориально распределенных инсталляций системы
- [ ] Общая панель управления с доступом ко всем сотрудникам
- [ ] Проведение сквозных расследований по всем филиалам
- [ ] Кастомизация политики безопасности в зависимости от филиалов
- [ ] Поддержка очень больших архивов для хранения данных (1 000+ ТБ)

Оцените поставщика решения

- [ ] Время работы на рынке
- [ ] Масштаб бизнеса и его финансовая устойчивость
- [ ] Активные публичные коммуникации и хорошая репутация
- [ ] Подтвержденные кейсы в вашей отрасли
- [ ] Наличие акций или скидок при условии конкурентного перехода
- [ ] Высокое качество сервиса:
  - [ ] Скорость и полнота ответов технической поддержки
  - [ ] Дата последнего обновления системы (позже — лучше)
  - [ ] Возможность прикрепить персонального менеджера
  - [ ] Круглосуточная поддержка

Оцените решение

- [ ] Оцените наличие всех необходимых функций из п. 1
- [ ] Оцените возможности для расследования инцидентов и отчетности:
  - [ ] Высокая скорость «быстрого» поиска
  - [ ] Наличие расширенного поиска с поддержкой логических операторов
  - [ ] Возможность трансляции рабочего стола сотрудника
  - [ ] Возможность записи звука с рабочего ПК сотрудника
  - [ ] Возможность кастомизации отчетов
  - [ ] Доступ к истории работы с инцидентом

Оцените удобство профилактики инцидентов

- [ ] Разделение понятий «рабочая станция» и «пользователь»
- [ ] Высокий уровень визуализации информации: графы, тепловые карты
- [ ] Вывод информации о сотрудниках на отдельную вкладку
- [ ] Поиск уникальных контактов
- [ ] Возможность объединять сотрудников в группы риска
- [ ] Доступ к показателям уровня угрозы и риска утечки со стороны конкретного сотрудника

Оцените удобство внедрения и настройки

- [ ] Интеграция с Active Directory
- [ ] Наличие агента для macOS
- [ ] Наличие агента для Windows
- [ ] Наличие агента для Linux
- [ ] Возможность установки на виртуальные рабочие места

Ростелеком Солар

Оцените масштабируемость и отказоустойчивость

- [ ] Максимальное количество работающих агентов
- [ ] Максимальный объем обрабатываемой информации
- [ ] Максимальный объем хранимой информации
- [ ] Возможность балансировки трафика

Оцените гибкость управления политиками фильтрации и инцидентами

- [ ] Простота настроек политик с помощью графического интерфейса
- [ ] Действие политик для всех модулей системы
- [ ] Наличие встроенных шаблонов политик
- [ ] Разделение понятий «событие» и «инцидент»
- [ ] Инцидент-менеджмент по ГОСТ 15408 «Менеджмент ИБ» (ISO/IEC 27035-1:2016)

Оцените возможности администрирования и управления

- [ ] Запуск диагностики рабочей станции
- [ ] Подключение/отключение модулей системы по надобности
- [ ] Адаптивный веб-интерфейс с поддержкой 4K-мониторов
- [ ] Поддержка Zabbix для мониторинга здоровья системы

Оцените защищенность данных и безопасность

- [ ] Журналирование действий пользователя (офицера безопасности)
- [ ] Ролевая модель доступа в систему
- [ ] Оперативная деактивация агентов

Ростелеком Солар

Оцените возможности по обеспечению импортозамещения

- [ ] Регистрация в Едином реестре отечественного ПО
- [ ] Работа на агентов на ПК с ОС на базе Linux
- [ ] Работа на сервере с ОС на базе Linux
- [ ] Наличие сертификата ФСТЭК России

solar@rt-solar.ru
+7 (499) 755-07-70
https://rt-solar.ru

Ростелеком Солар