

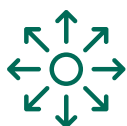
Next-Gen DLP

Платформа защиты данных Enterprise-уровня

Fortra's Digital Guardian — обеспечьте целостность информации и ее защиту от внутренних и внешних угроз.

- › Точное обнаружение конфиденциальных данных любого типа и формата на основе контентной, контекстной и пользовательской классификаций
- › Защита структурированных и неструктурированных данных, контроль приложений и действий пользователей на уровне процессов ОС
- › Уменьшение рисков информационной безопасности с помощью интегрированных механизмов уведомления и обучения пользователей

КЛЮЧЕВЫЕ ОСОБЕННОСТИ:



Облачный\On-premise DLP

Fortra's Digital Guardian на базе AWS обеспечивает легкое развертывание и гибкую масштабируемость, повышая окупаемость затрат на безопасность. При этом данную DLP можно развернуть в вашей инфраструктуре



Кроссплатформенность

Поддержка платформ Windows, macOS, Linux или виртуальных сред VMware\Citrix на уровне ядра системы



Гибкое управление

Гранулированная и гибкая настройка политик безопасности по логированию, мониторингу и блокировке



Широкий обзор

Возможность увидеть все процессы перемещения конфиденциальных данных на рабочей станции и сервере



Предустановленные политики

Работа DLP из коробки без необходимости написания сложных политик



Комплексная классификация

Только Fortra's Digital Guardian обеспечивает анализ и классификацию данных по контенту, контексту и пользователю

DLP Fortra's Digital Guardian: сценарии применения



КОНТРОЛЬ ДОСТУПА К ДОКУМЕНТАМ:

уведомления в случае открытия файлов с меткой «совершенно секретно» и отчет по пользователям, открывавшим такие документы.

ЗАПРЕТ НА ОТКРЫТИЕ ФАЙЛОВ:

пользователь с обычными правами не сможет открыть документ с меткой «конфиденциально».

КОНТРОЛЬ ЗАПУЩЕННЫХ ПРИЛОЖЕНИЙ:

при работающей бухгалтерской программе пользователь не сможет запустить мессенджер для передачи конфиденциальных данных или трансляции экрана.

НАСЛЕДОВАНИЕ МЕТКИ ЧЕРЕЗ БУФЕР ОБМЕНА:

часть текста из документа с меткой «конфиденциально» (даже не имеющая контролируемых ключевых слов) при вставке в новый документ автоматически применит к нему тот же статус – «служебная информация».

ИНТЕЛЛЕКТУАЛЬНЫЙ БУФЕР ОБМЕНА:

часть текста документа с меткой «абсолютно секретно» (даже не имеющую контролируемых ключевых слов) можно вставить в новый текстовый документ, но нельзя отправить через мессенджер.

КОНТРОЛЬ АРХИВОВ С ПАРОЛЕМ:

метка «ДСП (для служебного пользования)», примененная к файлу, сохраняется, и при помещении этого файла в архив, в т. ч. с парольной защитой, почтовая система не пропустит такое вложение