

Solar Dozor

Предотвращение утечек информации с рабочих станций на базе Linux

Подходит для импортозамещения

В приказе Минкомсвязи России № 96 от 01.04.2015 «Об утверждении плана импортозамещения программного обеспечения» говорится, что к 2025 году доля отечественных операционных систем (ОС) в государственных организациях должна составить не менее 50%. Такие ОС разрабатываются на базе GNU/Linux, и, как правило, их не поддерживают системы предотвращения утечек (системы DLP).

В DLP-системе Solar Dozor реализован специализированный модуль для контроля рабочих станций **Dozor Endpoint Agent**, который работает на ОС Microsoft Windows и на сертифицированных дистрибутивах ОС на базе GNU/Linux. Во втором случае модуль отличается лишь отсутствием возможности перехватывать сообщения и файлы в мессенджерах.

Наличие полнофункционального агента под GNU/Linux позволяет постепенно переводить рабочие станции на другую ОС, поэтапно выполняя план по импортозамещению. Уровень защиты от утечек информации при этом не снижается.

Схема работы






Функциональные возможности







Dozor Endpoint Agent использует системные функции ОС, что позволяет ему отслеживать и при необходимости блокировать действия пользователей и отдельных приложений на рабочей станции. Одной из отличительных особенностей агента является поддержка работы на терминальных серверах под управлением ОС Циркон 36СТ.

Возможности Dozor Endpoint Agent	Версия для Windows	Версия для Linux
Разрешение и блокировка подключения USB-устройств по заданным категориям и экземплярам	+	+
Перехват сетевого трафика по протоколу HTTPS, включая веб-почту и облачные хранилища	+	+
Контроль почтовой переписки по протоколам SMTP, POP3, IMAP, в том числе с шифрованием SSL/TLS	+	+
Снятие снимков экрана	+	+
Трансляция видео с экрана	+	+
Перехват нажатия клавиш (кейлоггер)	+	+
Контроль передачи данных через буфер обмена (текст, изображения, файлы)	+	+
Контроль копирования файлов на USB-устройства и сетевые диски	+	+
Контроль и блокировка печати	+	+
Контроль рабочего времени пользователей (названия сайтов и приложений, время работы с ними, аналитика по сотруднику и отделу)	+	+
Перехват сообщений и файлов в мессенджерах	+	—

Системные требования

 Процессор	1,5 ГГц	 Оперативная память	1 ГБ	 Свободное место на диске	30 ГБ
---	----------------	--	-------------	--	--------------

Поддерживаемые операционные системы

 Astra Linux 1.6 Astra Linux 2.12	 РЕД ОС 7.2 «Муром»	 Гослинукс ИК6	 CentOS 7.x	 Ubuntu 18.04 LTS Ubuntu 20.04 LTS	 Циркон 36СТ
--	---	--	---	---	--

О компании

№1 на рынке сервисов кибербезопасности	900+ экспертов кибербезопасности	70+ клиентов из топ-100 российского бизнеса	24/7 обеспечение кибербезопасности	400+ комплексных и сервисных проектов в год	110+ млрд анализируемых событий ИБ в сутки
--	--	---	--	---	--