

# Kaspersky IoT Secure Gateway



Кибериммунные шлюзы для подключения  
**ПРОМЫШЛЕННОГО ОБОРУДОВАНИЯ**  
к облакам и бизнес-системам

## Сценарий №1

Шлюз как программный дата-диод  
(однаправленная передача данных)



- **Безопасный и надежный транспорт** ранее недоступных для бизнеса данных;
- **Доверенные данные со шлюза** помогают строить цифровые сервисы по аналитике, прогнозированию работы оборудования;
- **Мониторинг работы станков ЧПУ**;
- **Мониторинг работы спецтранспорта** (карьерная техника, грузовые автомобили);
- **Анализ производственных цепочек**, включая отслеживание логистики (RFID).

## Сценарий №2

# Шлюз как роутер (двунаправленная передача данных)



- Использование шлюзов на объектах КИИ в режиме FW по сертификации ФСТЭК;
- Отправка событий безопасности по протоколу Syslog;
- Безопасный и надежный двунаправленный транспорт ранее недоступных для бизнеса данных;
- Обнаружение вторжений IDS/IPS для защиты от внешних угроз;
- Контроль и управление промышленным оборудованием (станки ЧПУ, ПЛК, принтеры, роботы), мониторинг работы удаленных площадок;
- Защита периметра предприятия, защита уровня ТСПД, создание сегмента ДМЗ;
- Мониторинг локальной сети с целью обнаружения новых подключенных устройств;
- Защита интеллектуальных систем видеонаблюдения;
- Шлюз как элемент построения систем M2M;
- Анализ производственных цепочек, включая отслеживание логистики (RFID).

### Дополнительно:

- Создание экосистемы из продуктов «Лаборатории Касперского»: KISG+KUMA+KSRW+KICS+KSC для обеспечения комплексной безопасности на объекте и дальнейшей защищенной передачи данных в систему «ГосСОПКА»;
- Централизованное управление продуктами «Лаборатории Касперского» через Kaspersky Security Center.