Инполюс
Информационные технологии

inpolus SDDS

Инполюс

Система обнаружения утечек
(Sensitive Data Detection System)

127287, Москва, 2-я Хуторская 38А, стр. 9
+7 (495) 274-01-91 · info@inpolus.ru

www.inpolus.ru

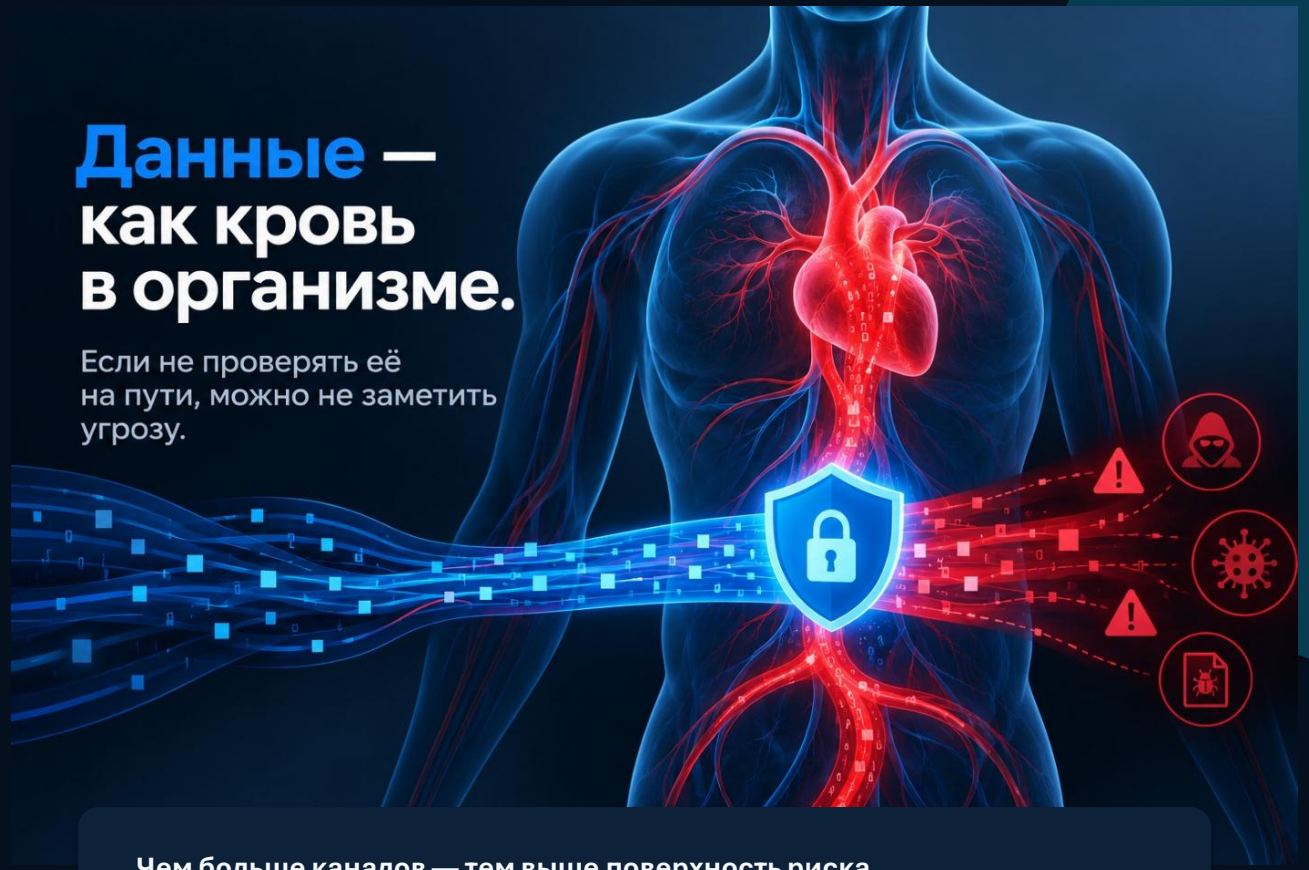
Данные — цифровая нервная система компании

Бизнес работает при непрерывном обмене различными данными.

Информация передаётся между сервисами, API, файлами, облаками, очередями и т.д.

Чем больше каналов, тем выше риск возможных утечек.

Защищать нужно не только хранилища, но и данные в момент передачи в различные каналы.



Чем больше каналов — тем выше поверхность риска.

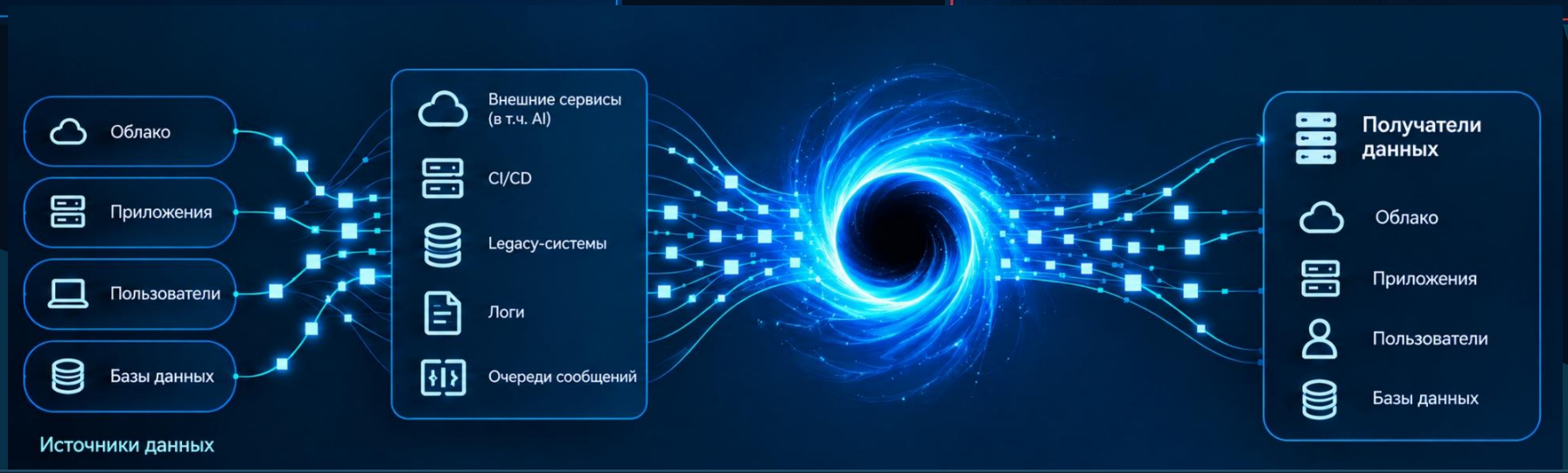
Проблема: утечка может произойти в пути

Чувствительные данные:

ФИО · Паспорта · Карты · Телефоны · ИНН · СНИЛС · API-ключи

Риски:

Внешние AI-сервисы · CI/CD · Legacy-системы · Логи · Очереди сообщений



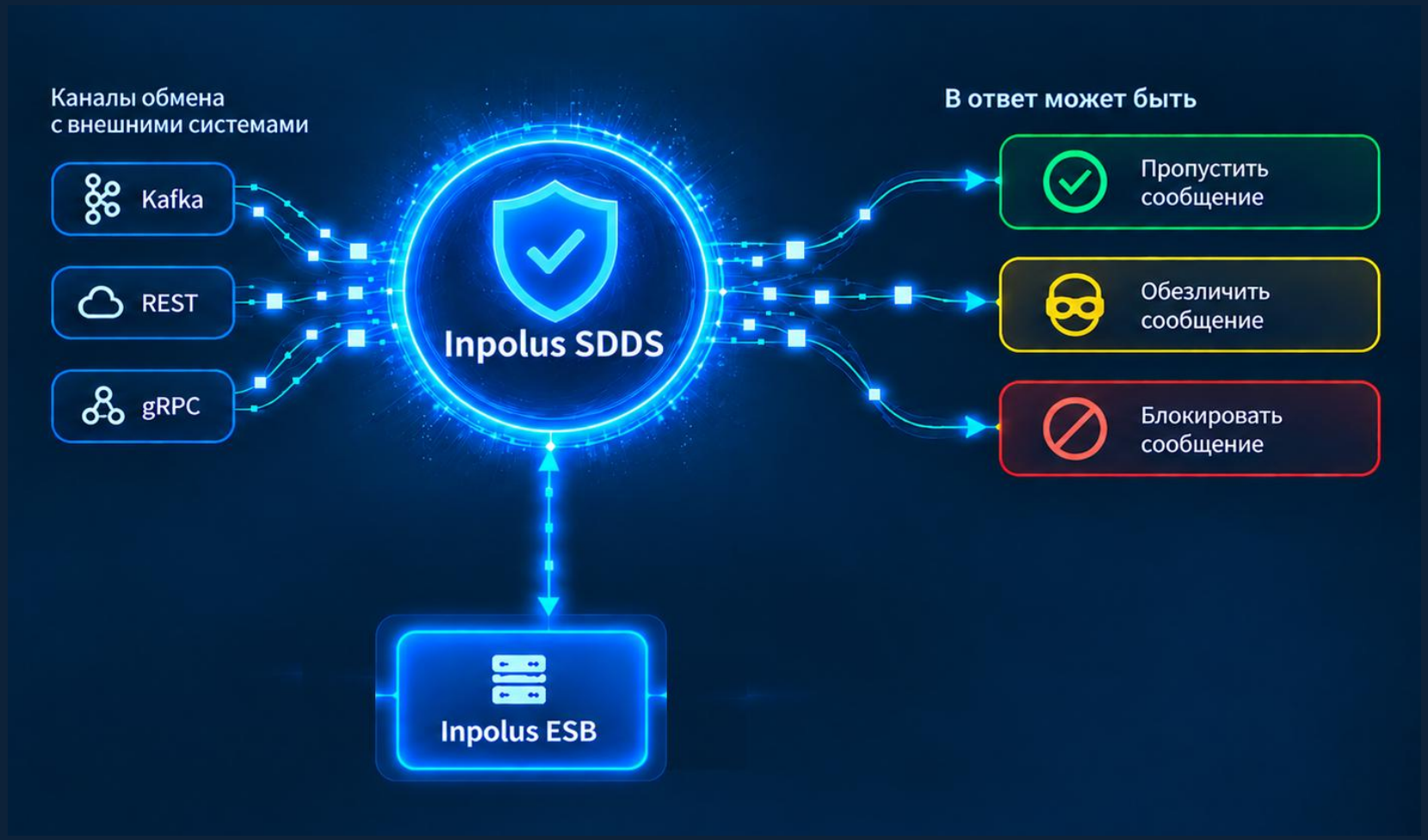
Обычный сканер не видит поток данных в реальном времени. → Нужен «пограничный контроль» внутри каналов обмена.

Решение: Inpolus SDDS

Модуль обнаружения и расследования инцидентов.
Анализирует данные в движении.
Настраиваемые политики: пропускать, обезличивать, блокировать.

Работает через модульные адаптеры — «переходники» к разным источникам. Позволяет подключать различные системы.
Inpolus ESB имеет интеграцию «из-коробки».

Гибкое подключение: входы и выходы

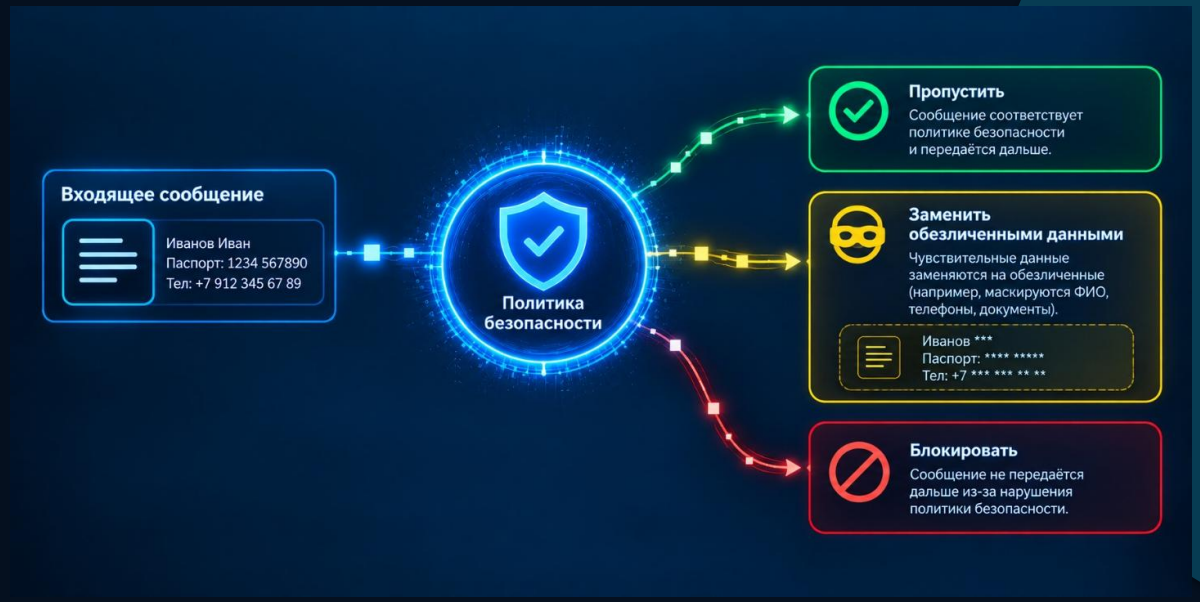


Три режима защиты: от наблюдения к контролю

Данные идут дальше, но фиксируются нарушения.

Персональные данные заменяются масками.

Выдается команда остановить передачу критичного сообщения.



Политики зависят от контекста: источник, канал, время и могут комбинироваться, а также позволяют внедрять систему отслеживания плавно без остановки бизнеса, повышая уровень постепенно.

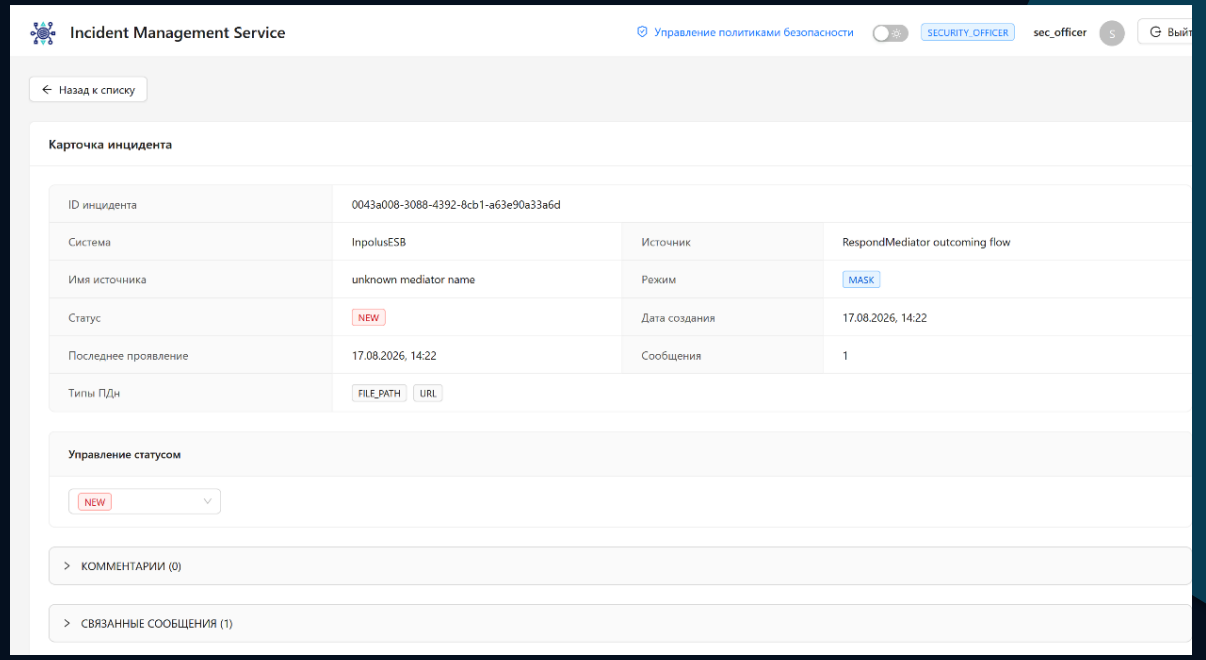
Аудит и работа с инцидентами

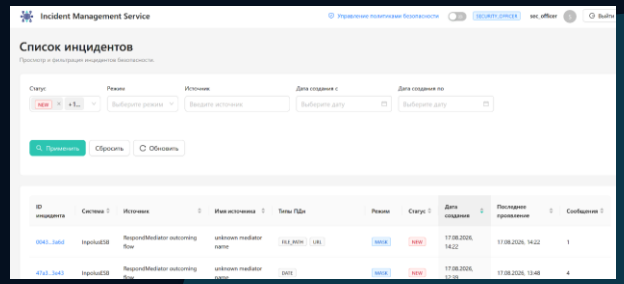
Пользовательский интерфейс администратора политик.

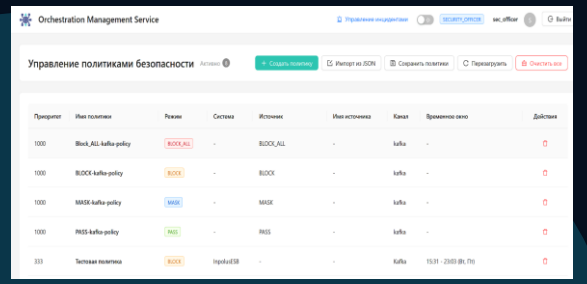
Пользовательский интерфейс офицера безопасности.

По каждому запросу — структурированное событие:

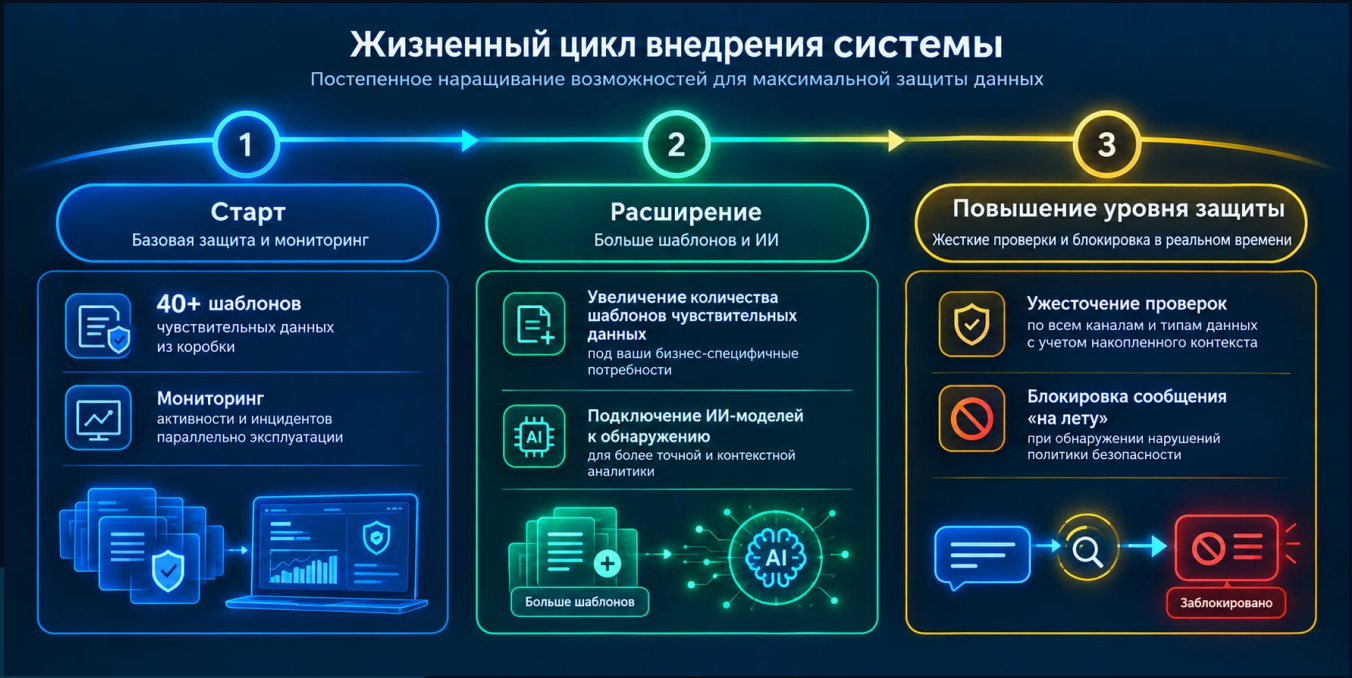
- источник: канал, сервис, окружение;
- хеш сообщения для идентификации;
- категории найденной чувствительной информации;
- действие: пропуск / обезличивание / блокировка;
- связанные сообщения.







Эволюция защиты: от простого к сложному



Старт: 40+ готовых шаблонов (паспорта, карты, телефоны, ИНН, СНИЛС и т.д.).

Расширение:

Возможно расширение количества шаблонов чувствительных данных.
Возможно подключение ИИ-моделей для поиска и детекции, как локальных, так и облачных.

Повышение уровня защиты: от параллельного мониторинга к блокировке потоков.

Что получает бизнес

Вопросы