APPSEC SOLUTIONS

РОССИЙСКАЯ ЭКОСИСТЕМА DEVSECOPS И AI SECURITY

Безопасность ПО и искусственного интеллекта на каждом шаге разработки



2026 appsec.global

КОНТЕКСТ

Среда разработки изменилась — цепочка поставок ПО стала еще шире

ЧТО НУЖНО

01
Знать состав ПО
SBOM и AI-BOM: транзитивные зависимости и происхождение артефактов

02
Учитывать модели и внешние ИИ-сервисы
ИИ стал частью продукта — и частью поверхности атаки

03
Контролировать код от ИИ-ассистентов
Сгенерированный код и «галлюцинированные» пакеты проверяются как любой другой

04
Защищать обращения к LLM в рантайме
Промпт-инъекции и утечки данных блокируются до модели

05
Строить процесс РБПО по ГОСТ Р 56939-2024
Измеримые метрики и отчетность для регулятора

06
Использовать решения из реестра российского ПО
On-premise
в закрытом контуре

МАСШТАБ ПРОБЛЕМЫ

Нельзя управлять тем, чего не видишь

19 500

вредоносных open-source пакетов к концу 2025 года, +37% за год

«Лаборатория Касперского», 2026

77%

российских разработок используют готовые компоненты; в Java — до 90% чужого кода

АРПП «Отечественный софт»

>80%

организаций применяют ИИ для разработки кода

АРПП «Отечественный софт» и AppSec Solutions, 2026

ЧТО ОСТАЕТСЯ НЕВИДИМЫМ БЕЗ ИНСТРУМЕНТОВ

- Состав ПО
- Транзитивные зависимости
- Происхождение артефактов
- ИИ-компоненты и модели
- Связь уязвимости с работающей системой

ПОДХОД К БЕЗОПАСНОЙ РАЗРАБОТКЕ

Периодических проверок недостаточно — нужен единый контур управления безопасной разработкой

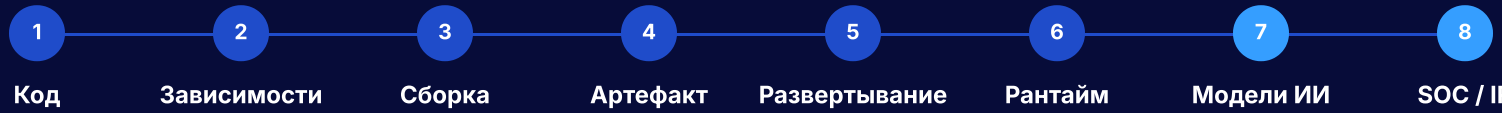
AppSec- и DevSecOps-контроли

Дают постоянную прослеживаемость и предотвращают эксплуатацию критических уязвимостей в продакшене.

Уязвимость видна от кода до работающей системы

От исходного кода и зависимости — до артефакта, работающей системы и рантайм-окружения.

ЖИЗНЕННЫЙ ЦИКЛ СОВРЕМЕННОЙ БЕЗОПАСНОЙ РАЗРАБОТКИ



Не отдельный контур безопасности, а сквозные контроли внутри производственного процесса: результаты возвращаются в код, пайплайн и трекеры задач.

ТРАНСФОРМАЦИЯ ПРОЦЕССОВ

От последовательного PDLC — к AI PDLC с человеком и ИИ-агентами в одном цикле

AS IS
PDLC

DESIGN → DEV → OPS

- Последовательные этапы
- Люди принимают почти все решения
- Автоматизируются отдельные операции этапов PDLC
- Разработка ориентирована на выполнение требований
- Изменения происходят после анализа человеком
- Основной актив – программный код

→ ТРАНСФОРМАЦИЯ

TO BE
AI PDLC

Сотрудник ⇄ ИИ

- Непрерывный параллельный цикл работы мультиагентной системы (человек + ИИ)
- Значительная часть работ и решений осуществляется ИИ-агентами
- Автоматизируются целые процессы
- Разработка ориентирована на достижение бизнес-результата
- ИИ сам обнаруживает проблемы и инициирует изменения
- Основной актив – знания, модели, данные, ИИ-агенты

АРХИТЕКТУРА ПОРТФЕЛЯ

Безопасность встраивается в каждый этап производственного процесса

DISCOVERY

Что создаем и зачем

Требования, архитектура и ИИ-сценарии, политики контроля

APPSEC.GENAI

DEV

Как создаем и проверяем

Код, зависимости, сборка, security gates в CI/CD и IDE

APPSEC.WAVE

APPSEC.TRACK

APPSEC.CODE

APPSEC.REGISTRY

APPSEC.STING

OPS

Как доставляем и защищаем

Артефакты, развертывание, рантайм, мониторинг сторов и LLM

APPSEC.CODE

APPSEC.REGISTRY

APPSEC.STING

APPSEC.CRYPTEX

APPSEC.AIGATE

APPSEC.HUB | Контроль возникает там, где создается объект риска и остается прослеживаемым до работающей системы.

ЗАДАЧИ БИЗНЕСА

Три заказчика — три критерия успеха

Каждый получает измеримый результат

CISO

Управляет риском

- Единая картина защищенности ПО
- Метрики РБПО для регулятора
- Уязвимости не доходят до продакшена
- Риски ИИ под контролем: модели и обращения к LLM защищены
- Анализ AppSec-процессов быстрее благодаря MCP

AppSec

Политиками и security gates

- Приоритизация по эксплуатируемости
- Меньше ложных срабатываний
- Блокировка сборок по политикам
- Проверка ИИ-моделей на устойчивость к атакам до продакшена
- ИИ-агенты через MCP запускают сканы и разбирают результаты

DevSecOps

Наблюдаемостью и обратной связью

- Проверки в CI/CD и IDE без задержек
- Результаты — в код и трекеры задач
- Один вендор на весь конвейер
- Защита обращений к LLM в рантайме без изменения кода
- MCP-коннект: проверка кода прямо в IDE

ПОЧЕМУ APPSEC SOLUTIONS

Собственная разработка с 2018 года: девять продуктов, каждый закрывает свою задачу

9

продуктов собственной разработки — не переупакованный open source

100%

экосистемы в реестре отечественного ПО

Каждый продукт решает свою задачу

SAST, SCA/OSA, MAST, AI Red Teaming, ASPM, Secure Git, Artifactory, App Shielding, AI Firewall.

Начните с одного модуля — остальные подключают по мере развития ваших практик безопасной разработки.

Поддержка в РФ

Вендорская поддержка, экспертиза внедрения, программы обучения команд.

ПРИЗНАНИЕ РЫНКА

Лидер AI Security
TAdviser 2026

ТОП-41 ИИ-рынка
CNews 2025

«Приоритет.Цифра»
2026



ПОЧЕМУ СЕЙЧАС — 2026

Регулятор уже требует безопасную разработку, а бездействие стоит дорого

КАКИЕ РЕГУЛЯТОРНЫЕ ТРЕБОВАНИЯ ВЛИЯЮТ НА ОРГАНИЗАЦИИ

ГОСТ Р 56939-2024 — процессы РБПО и отчет по ОУД 4 для финансовых организаций

Приказ ФСТЭК № 117 — безопасная разработка (п. 50) и контроль систем ИИ (п. 60–61)

Указ № 166 и импортозамещение — только ПО из реестра на объектах КИИ

Цифровой рубль и ПС «Мир» — требования к защите мобильных приложений

90,3% приложений в сторах содержат критические и высокие уязвимости

77% кода приложения — чужой open-source; атаки идут через цепочку поставок

81–88% сырых срабатываний сканеров — ложные; без корреляции команда ИБ тонет в шуме

ИИ В ЭКОСИСТЕМЕ

Сила ИИ в продуктах AppSec Solutions

APPSEC.WAVE	**MCP-коннект для LLM-редакторов** MCP Claude Code, Cursor и аналоги проверяют сгенерированный код
APPSEC.TRACK	**Track.AI — ИИ-помощник для оценки сканов** ИИ MCP Сам исследует каждую CVE по коду, доказывает вывод цитатами кода и ставит VEX-статусы; чат, Fix Advisor и MCP по данным Track
APPSEC.STING	**MCP и агентный режим** MCP ИИ-агент получает данные о сборке, запускает скан мобильного приложения и разбирает результаты
APPSEC.HUB	**ИИ-приоритизация с точностью 96%** ИИ Дедупликация и корреляция находок из разных сканеров, авторазметка ложных срабатываний
APPSEC.GENAI	**Проверка ИИ-моделей на устойчивость к атакам** ИИ 90+ атак на языковые модели, классификаторы изображений и распознавание речи — до вывода в продакшен
APPSEC.AIGATE	**Защита обращений к LLM в рантайме** ИИ Блокирует промпт-инъекции и джейлбрейки, маскирует ПДн и секреты в запросе и в ответе модели

ЧТО ДАЕТ MCP ПО РОЛЯМ

CISO

Код от ИИ-ассистентов проходит проверку безопасности до попадания в репозиторий

AppSec

ИИ-агент сам запускает сканы и разбирает находки — меньше ручного триажа, быстрее анализ

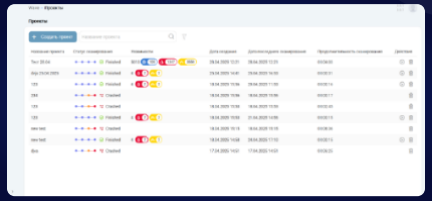
DevSecOps

Проверки и результаты доступны прямо в IDE и чате — без переключения между инструментами

НАЙТИ И УСТРАНИТЬ · SAST

APPSEC.WAVE

Статический анализатор исходного кода с минимумом ложных срабатываний — в закрытом контуре.



ПОМОГАЕТ СОБЛЮДАТЬ ТРЕБОВАНИЯ РЕГУЛЯТОРОВ

- **ГОСТ Р 56939-2024, п. 5.10** — статический анализ и регистрация предупреждений
- **Приказ ФСТЭК № 117, п. 50** — меры РБПО по ГОСТ Р 56939
- **Профиль защиты Банка России, п. 7.4.2.2** — обязательный статический анализ
- **Репозиторий доверенных решений** Ассоциации ФинТех — № АФТ1224

Реестр отечественного ПО **№ 29442**

1. **5 000 правил для 28 языков**
   Готовые правила для Java, 1C, C/C++, Python, JS, Go, PHP и других языков

2. **Кастомизация правил и отчетов**
   Свои правила по шаблону без ожидания релиза вендора, отчеты под требования заказчика

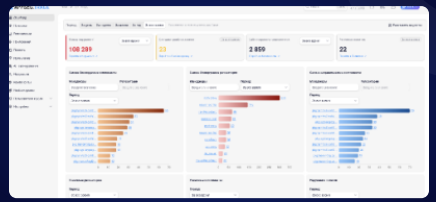
3. **Не тормозит релизы**
   4 минуты на 100 000 строк Java (8 CPU, 32 ГБ RAM), развертывание за 20 минут

4. **MCP-коннект для LLM-редакторов**
   Сгенерированный ИИ код не уходит в репозиторий без проверки: Claude Code, Cursor и аналоги через MCP сами запускают анализ и исправляют уязвимости

5. **Межфайловый taint-анализ**
   Поток данных между файлами: Java, Python, JS/TS, C/C++, Go — шаг к требованиям ГОСТ Р 71207-2024

НАЙТИ И УСТРАНИТЬ · SCA / OSA

APPSEC.TRACK



ПОМОГАЕТ СОБЛЮДАТЬ ТРЕБОВАНИЯ РЕГУЛЯТОРОВ

- **ГОСТ Р 56939-2024, п. 5.15–5.17** — секреты, зависимости, вредоносное ПО в цепочке поставок
- **Приказ ФСТЭК № 117, п. 50;** Приказы № 21, № 239; Указ № 166
- **Профиль защиты Банка России, п. 7.4.2.2** — композиционный анализ
- **Репозиторий доверенных решений** Ассоциации ФинТех — № АФТ0292

Реестр отечественного ПО **№ 20552**

1 **Track.Feed — собственная база**

2,7 млн уязвимостей из 20+ источников: NVD, БДУ ФСТЭК, CISA KEV, VulnCheck, GHSA, OSV; привязка к PURL

2 **OSA Firewall на входе в контур**

Блокировка malware, protestware, typosquatting и dependency confusion до попадания к разработчику

3 **SBOM под требования регулятора**

Формирование и анализ SBOM: полный состав ПО с транзитивными зависимостями и лицензиями

4 **Приоритизация по эксплуатируемости**

По CISA KEV, VulnCheck KEV и EPSS; встроенный SAST-модуль подтверждает достижимость в коде

5 **Track.AI — ИИ-помощник для оценки ваших сканов**

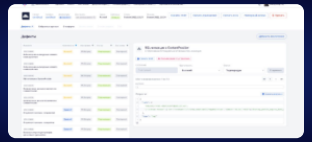
✓ Сам исследует каждую CVE по коду приложения и библиотеки
✓ Доказывает вывод цитатами кода и сам ставит VEX-статусы
✓ Бэклог SCA разбирается за ночь — без ручного триажа
✓ Чат и MCP по данным Track; ваши модели, закрытый контур

НАЙТИ И УСТРАНИТЬ · MAST

APPSEC.STING

Мобильная безопасность для команд и ИИ-агентов

Проверка Android и iOS без исходного кода. AppSec.Sting объединяет методы MAST и сопоставляет результаты; MCP позволяет ИИ-агенту запускать анализ и разбирать проблемы.



ПОМОГАЕТ СОБЛЮДАТЬ ТРЕБОВАНИЯ РЕГУЛЯТОРОВ

- **Приказ ФСТЭК № 117, п. 50** — РБПО для мобильных приложений
- **Профиль защиты Банка России, п. 7.4.2.2** — динамический анализ
- **Положение ЦБ РФ № 820-П и № 833-П** — требования платформы цифрового рубля
- **OWASP MASVS и Mobile Top 10**

Реестр отечественного ПО **№ 7699**

1. **MCP и агентный режим**
   Человек задает задачу и границы, ИИ-агент через MCP получает данные о сборке, запускает скан, работает с экраном и разбирает результаты

2. **Динамический анализ на Android и iOS**
   Android и Android TV — в эмуляторе, iOS 26 — на виртуальном iPhone: проходим сценарии пользователя, исследуем поведение и сетевое взаимодействие

3. **Полный набор методов MAST**
   SAST/BCA, DAST, IAST, SCA и тестирование API в одном процессе: сборка, поведение в работе, внутренние вызовы, компоненты, бэкенд

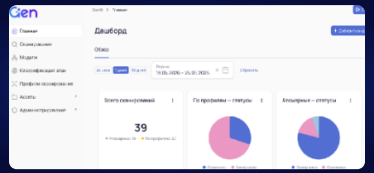
4. **Кросс-корреляция результатов**
   Находки в сборке, наблюдения в рантайме и сетевые данные связаны в одну проблему с доказательствами: откуда вывод и что исправлять

5. **Встраивание в процесс команды**
   Ручная работа и автоматизация сценариев, API/CLI и CI/CD, проверка новых сборок и отчеты

НАЙТИ И УСТРАНИТЬ · AI RED TEAMING

APPSEC.GENAI

Поиск уязвимостей и анализ устойчивости ИИ-моделей к атакам до вывода в продакшен.



АКТУАЛЬНОЕ РЕГУЛИРОВАНИЕ

- **Приказ ФСТЭК № 117, п. 61 б)** — допустимые тематики запросов
- **Приказ ФСТЭК № 117, п. 61 в)** — критерии недостоверных ответов
- **OWASP Top 10 для LLM 2025**
- **Скоро:** ФСТЭК, MITRE ATLAS, OWASP ML Top 10
- **Репозиторий доверенных решений** Ассоциации ФинТех — № АФТ1250

Реестр отечественного ПО **№ 30056**

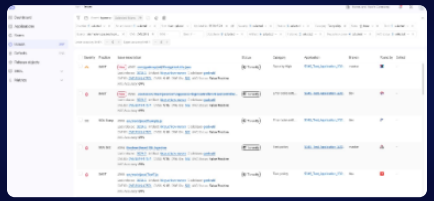
1. **90+ атак на модели**
   64 атаки на языковые модели в едином дереве техник, 19 на классификаторы изображений, 6 на распознавание речи, проверка генераторов изображений и файлов моделей на закладки
2. **Любая модель с HTTP API**
   6 шаблонов провайдеров (OpenAI, Anthropic Claude, DeepSeek, GigaChat, YandexGPT, HuggingFace) и свой контракт; локальные модели для CV и ASR
3. **Проверка как этап конвейера**
   REST API и консольная утилита genai-cli, остановка сборки при уязвимостях, повторные прогоны после каждого обновления модели
4. **Проверка на утечку системных инструкций и обход ограничений**
   Многоходовые атаки, собственные датасеты, модель-судья с категорией ответа и обоснованием
5. **Отчеты и дашборды**
   HTML-отчет с покрытием OWASP, выгрузка в CSV, JSON, XLSX, дашборд с метриками и собственными виджетами

УПРАВЛЯТЬ И ВИДЕТЬ · ASPM

APPSEC.HUB



Оркестрация сканеров, корреляция находок и метрики DevSecOps — в едином окне.



ПОМОГАЕТ СОБЛЮДАТЬ ТРЕБОВАНИЯ РЕГУЛЯТОРОВ

- **ГОСТ Р 56939-2024, п. 5.23** — автоматизация реагирования на уязвимости
- **ГОСТ Р 56939-2024, п. 5.24** — регулярный поиск уязвимостей при эксплуатации
- **Приказ ФСТЭК № 117, п. 50;** метрики РБПО и отчет по ОУД 4

Реестр отечественного ПО **№ 8953**

1. **Единое окно интеграций**
   40+ нативных интеграций SAST/DAST/SCA/MAST любых вендоров; еще 15 — через конвертеры, остальное — через API

2. **ИИ-приоритизация с точностью 96%**
   На CWE Top 25; дедупликация и корреляция находок из разных сканеров, авторазметка ложных срабатываний

3. **Quality Gates в конвейере**
   Блокировка сборок по правилам безопасности на любом этапе CI/CD; запуск сканирований через REST API и CLI

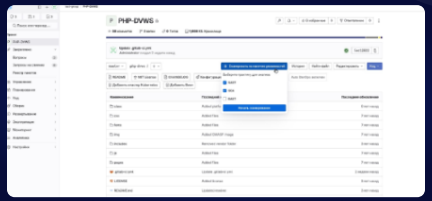
4. **Контроль исправлений в трекерах**
   Автопостановка задач в Jira, YouTrack, Яга с двусторонней синхронизацией статусов

5. **200+ метрик и промышленный масштаб**
   Дашборды и аналитика по ролям и отчеты регуляторам; более 5 000 сканирований в сутки, 5 млн уязвимостей в базе

УПРАВЛЯТЬ И ВИДЕТЬ ·
SECURE GIT / VCS

APPSEC.CODE

Безопасная Git-платформа с полным DevSecOps-циклом — от планирования до релизов.



ПОМОГАЕТ СОБЛЮДАТЬ ТРЕБОВАНИЯ РЕГУЛЯТОРОВ

- **ГОСТ Р 56939-2024, п. 5.12–5.13** — безопасная система и среда сборки
- **ГОСТ Р 56939-2024, п. 5.14** — управление доступом и контроль целостности кода
- **Приказ ФСТЭК № 117, п. 50;** образы на отечественных ОС
- **Репозиторий доверенных решений** Ассоциации ФинТех — № АФТ0291

Реестр отечественного ПО **№ 23202**

1 **Переход с GitLab быстро и легко**
Нативно исполняет .gitlab-ci.yml, импорт проектов с историей, MR, задачами и wiki – команде не нужно переучиваться

2 **Корпоративные функции в базовой лицензии**
Очереди слияния, правила согласования, CODEOWNERS, защищенные окружения, эпики, DORA

3 **Безопасность в запросе на слияние**
Статический анализ (SAST) и поиск секретов из коробки, правила отправки и согласования безопасности; встроенные коннекторы AppSec.Wave, AppSec.Track и AppSec.Hub

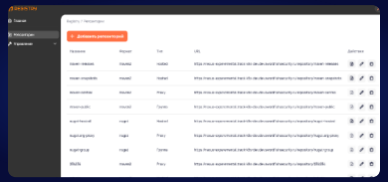
4 **HA и Geo для промышленной нагрузки**
Эталонные архитектуры до 25 000 пользователей, обновление без простоя, Astra Linux, РЕД ОС, ALT, работа без интернета

5 **Контроль качества кода из коробки**
Code smells, дубликаты, сложность, рейтинг разработчиков; политики качества на проект и группу блокируют MR

УПРАВЛЯТЬ И ВИДЕТЬ
· ARTIFACTORY

APPSEC.REGISTRY

Доверенное хранилище артефактов: образы, пакеты, чарты и модели под контролем.



ПОМОГАЕТ СОБЛЮДАТЬ ТРЕБОВАНИЯ РЕГУЛЯТОРОВ

- **ГОСТ Р 56939-2024, п. 5.13.2.5 / 5.13.2.7** — выделенное хранилище и ролевой доступ
- **ГОСТ Р 56939-2024, п. 5.17.2.4** — контроль предсобранных компонентов поставщиков
- **Указ № 166 и ПП № 1236** — импортозамещение и закрытый контур
- **Репозиторий доверенных решений** Ассоциации ФинТех — № АФТ1500

Реестр отечественного ПО **№ 31437**

1. **Единый источник истины для артефактов**
   Зависимости, сборки и образы в одном месте; поиск по версии, тегу и хеш-суммам, журнал всех операций с артефактами

2. **Миграция с Nexus без потерь**
   Та же модель Hosted / Proxy / Group; клиенты Maven, npm, Docker работают штатно — меняется только URL

3. **25 форматов, включая OCI и ML-модели**
   Docker и OCI с подписями, Maven, npm, PyPI, Helm, Go, Alpine, Pub, Terraform, Hugging Face и другие

4. **Корпоративные функции в базовой поставке**
   HA-кластер, обновление без простоя, репликация между площадками, тестовая среда и продвижение, экспорт / импорт — все, чего нет в Nexus CE

5. **Работа в закрытом контуре**
   Astra Linux и «Базальт», режим без прав root, установка без интернета; вендорская поддержка в РФ на русском языке

ЗАЩИТИТЬ В РАНТАЙМЕ · APP SHIELDING

APPSEC.CRYPTEX

Протектор мобильных приложений: реверс, модификация и клонирование становятся дорогими и бессмысленными.



ПОМОГАЕТ СОБЛЮДАТЬ ТРЕБОВАНИЯ РЕГУЛЯТОРОВ

- Требования **платежной системы «Мир»** к защите мобильных приложений
- Защита от внедрения **недекларированных возможностей (НДВ)**
- **Репозиторий доверенных решений** Ассоциации ФинТех — № АФТ1338

Реестр отечественного ПО **№ 29936**

1. **Защита без исходного кода**
   Обрабатываются готовые apk / aab — доступ к репозиторию и переписывание приложения не нужны

2. **Шифрование и обфускация кода**
   Исполняемый код закрыт от декомпиляции; логика и структура приложения нечитаемы для злоумышленника

3. **Anti-tamper: переупаковка и клоны**
   Контроль целостности сборки, защита от подмены и поддельных версий вашего приложения

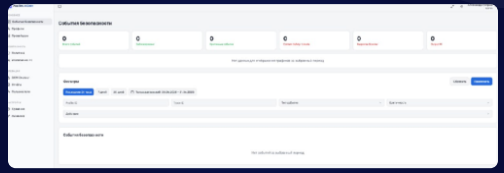
4. **Защита алгоритмов и ML-моделей**
   Уникальная бизнес-логика и модели в сборке скрыты от извлечения и копирования конкурентами

5. **ПС «Мир», защита от НДВ, CI/CD**
   Соответствие требованиям платежной системы; on-premise или SaaS, Docker / K8s, автозащита в конвейере

ЗАЩИТИТЬ В РАНТАЙМЕ · AI FIREWALL

APPSEC.AIGATE

Прокси-шлюз между приложениями и LLM: блокирует атаки и утечки, ведет аудит запросов к ИИ.



ПОМОГАЕТ СОБЛЮДАТЬ ТРЕБОВАНИЯ РЕГУЛЯТОРОВ

- **Приказ ФСТЭК № 117, п. 60** — исключение воздействия на данные и модели ИИ
- **Приказ ФСТЭК № 117, п. 61 а), б)** — шаблоны и допустимые тематики запросов
- **БДУ ФСТЭК, раздел ИИ (СП.1–СП.7);** OWASP Top 10 для LLM
- **Репозиторий доверенных решений** Ассоциации ФинТех — № АФТ1413

Реестр отечественного ПО **№ 34280**

1 **Блокировка джейлбрейков**
Открытые бенчмарки AdvBench и JailbreakBench; 7 датасетов, 30 000+ промптов; защита от Unicode-обфускации

2 **Маскирование ПДн и секретов**
RegEx + NER + валидация; конфиденциальные данные не покидают контур — в запросе и в ответе модели

3 **Внедрение без изменения кода**
Меняется только конечная точка; OpenAI, Anthropic, YandexGPT, ГигаЧат и локальные LLM; конфигурация за 1–2 дня

4 **Кастомные детекторы и политики**
Собственные детекторы без участия вендора; черные / белые списки, квоты токенов на профиль

СЦЕНАРИЙ РЕАЛИЗАЦИИ

01

Диагностика

Определяем текущий SDLC, инструменты безопасности и регуляторные требования.

02

Пилот

Берем 1–2 приоритетные задачи и запускаем их на реальном коде, пайплайне или ИИ-контуре.

03

Масштабирование

Фиксируем эффект и подключаем соседние продукты без замены платформы и повторного внедрения.

LAND → EXPAND | Каждый новый модуль повышает ценность уже созданного контура и снижает стоимость следующего шага.

О ВЕНДОРЕ

AppSec Solutions — российский разработчик экосистемы для защиты ПО и ИИ

2018
год начала собственной разработки

9
продуктов в экосистеме: от SAST до AI Firewall

100%
экосистемы в реестре отечественного ПО

7
продуктов в репозитории доверенных решений Ассоциации ФинТех

ПРИЗНАНИЕ РЫНКА

Лидер AI Security — TAdviser 2026

ТОП-41 ИИ-рынка — CNews 2025

«Приоритет.Цифра» — 2026

ЭКСПЕРТИЗА И СООБЩЕСТВО

Член АРПП «Отечественный софт»
с 2026 года

Ежегодное исследование уязвимостей мобильных приложений
на платформе AppSec.Sting

APPSEC SOLUTIONS

Спасибо за внимание

Покажем AppSec Solutions на вашем коде, в вашем контуре — и соберем состав пилота под ваши задачи.



Запросить демо | **appsec.global**

+7 (495) 620-63-36 inbox@appsec.global 121087, Москва, Береговой пр-д, 5к1, БЦ «Волна»