CHECK POINT™

Кибербезопасность в эпоху Искусственного Интеллекта

Эльнар Батталов | Менеджер по развитию бизнеса

21.05.2026

ebattalov@monttech.kz

+7 701 908 56 65

MONT TECH

We Secure Your
AI TRANSFORMATION

Что мы узнали о...

Технологический стек

- AWS Agent Core
- LiteLLM
- 5 клиентоориентированных агентов

Область интереса

- Обнаружение всех агентов в инфраструктуре
- Предотвращение утечки финансовых данных со стороны агентов

Nike, Inc. – американская корпорация по производству спортивной обуви и одежды со штаб-квартирой недалеко от Бивертона, штат Орегон. Это крупнейший в мире поставщик спортивной обуви и одежды, а также крупный производитель спортивного оборудования, с выручкой, превышающей 46 миллиардов долларов США в 2022 финансовом году.

Компания была основана 25 января 1964 года как «Blue Ribbon Sports» Биллом Боуэрманом и Филом Найтом и официально стала Nike, Inc. 30 мая 1971 года. Компания получила свое название от Ники, греческой богини победы.

Контакты

Адам Сили

Глобальный CISO

Агенты появляются везде!

БЕЗ согласования с ИБ

БЕЗ видимости

БЕЗ контроля

Ноутбуки сотрудников

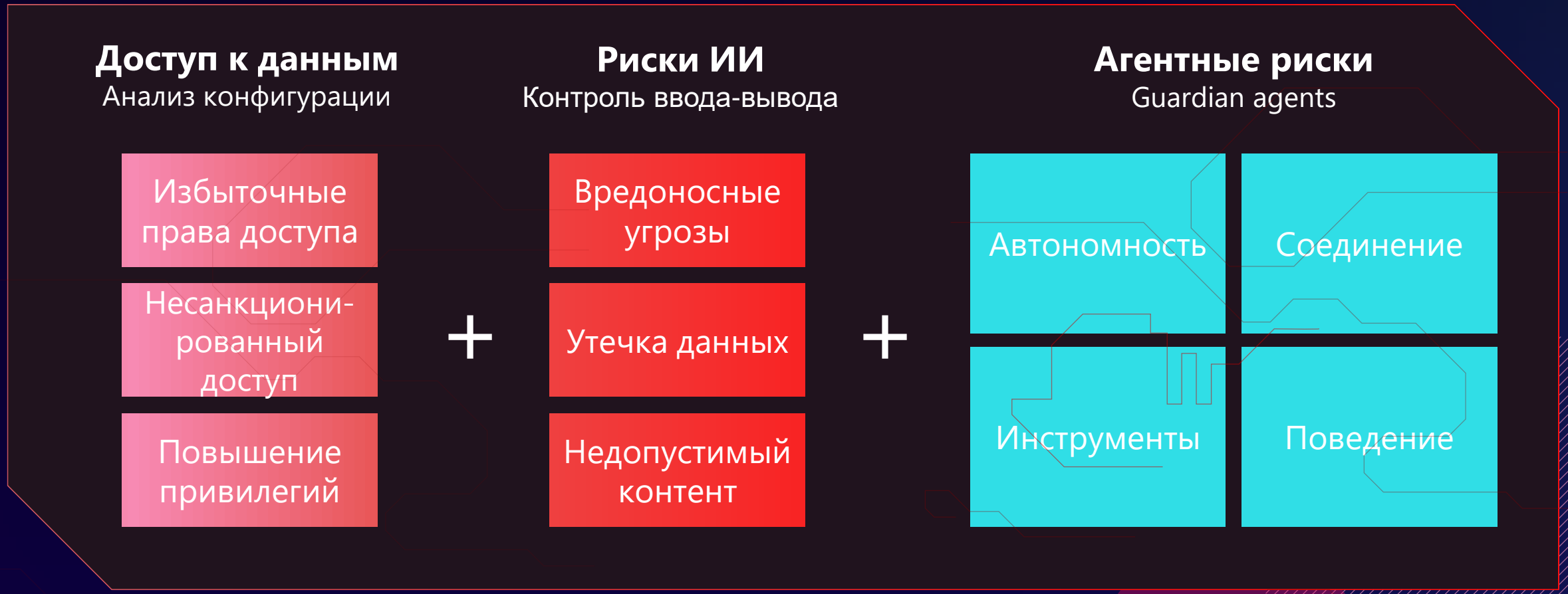
Сторонние SAAS-сервисы

Клиентские и Внешние

Корпоративные приложения и Инфраструктура

Новые риски – новый подход

Автономность и использование инструментов требуют ***контекста*** для понимания и обеспечения безопасности

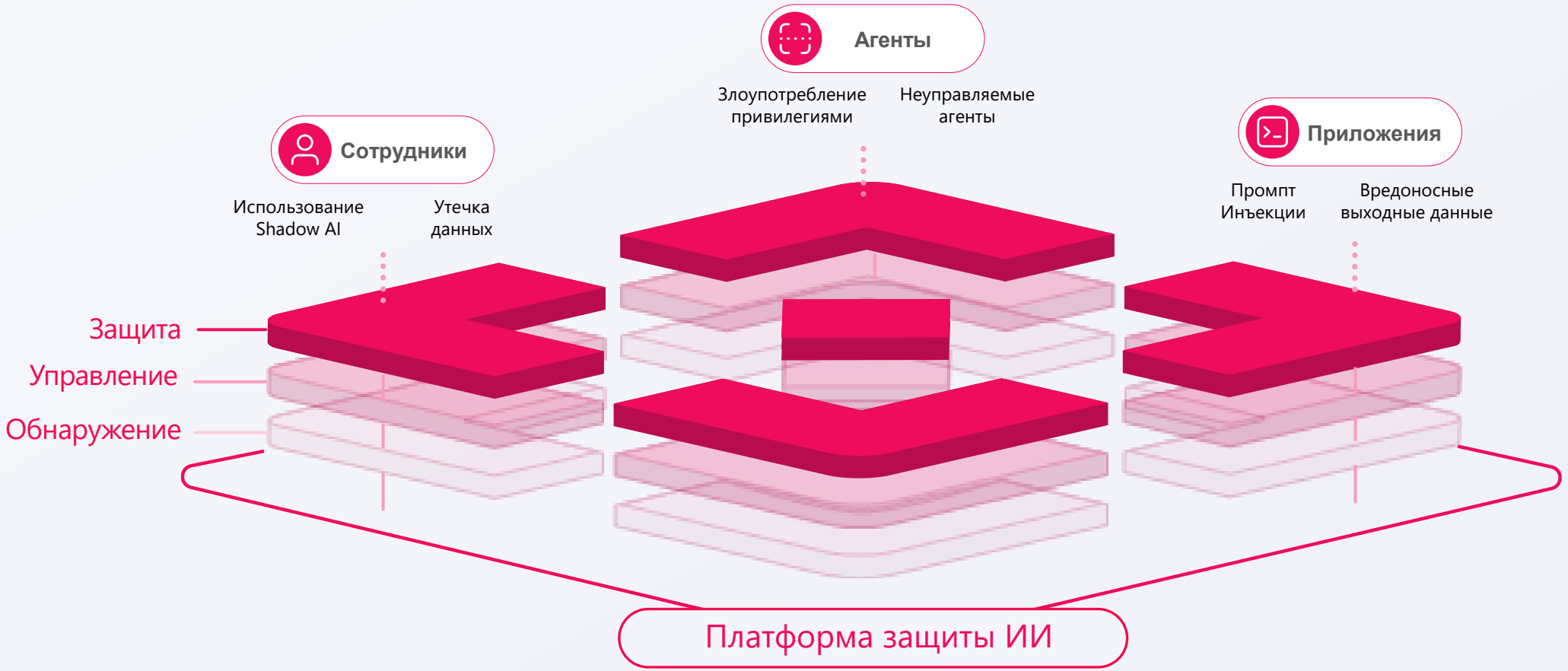


Контроль прав доступа и шаблонный анализ не могут ответить на вопрос:

"Следует ли ИИ агенту удалить эти файлы на основании только что прочитанного письма?"

Платформа защита ИИ

Единая модель безопасности обеспечивающая контроль в реальном времени за действиями сотрудников, агентов и приложений



Одна платформа. Один взгляд. От сотрудников – к приложениям и агентам.

Платформа защита ИИ

Единая модель безопасности обеспечивающая контроль в реальном времени за действиями сотрудников, агентов и приложений

Workforce AI Security

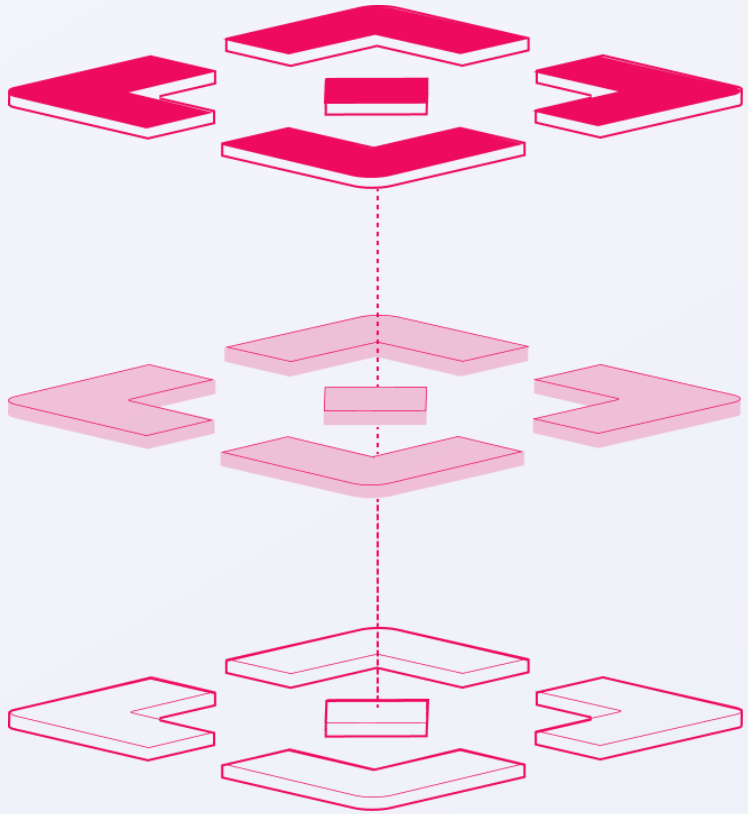
Обнаружение, управление и защита при использовании ИИ сотрудниками

AI Agent Security

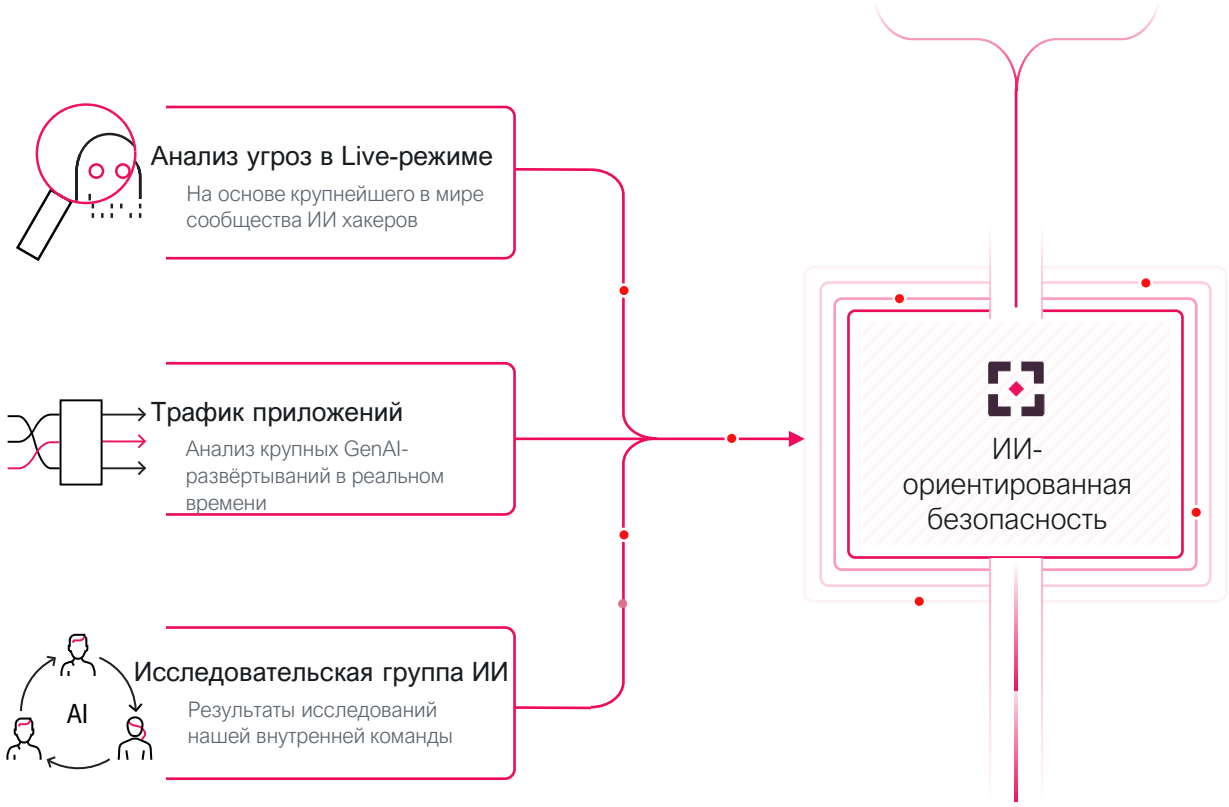
Обнаружение, управление и защита пользовательских приложений и ИИ-агентов

AI Red Teaming

Проактивная оценка угроз на основе рисков



ИИ-ориентированная безопасность



Собственные постоянно обновляемые данные об угрозах:

85M+
Паттерны атак

30+ лет
AI Red Teaming

100+
Языков используются для атак

Защищенность, доступ и идентификация агентов

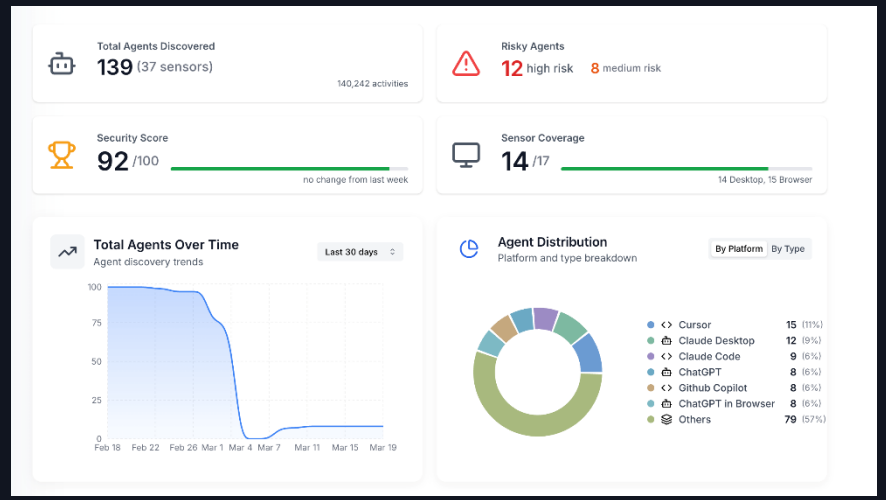
Расширение обнаружения и контроля агентов: в SaaS, на хостах и в экосистемах агентов

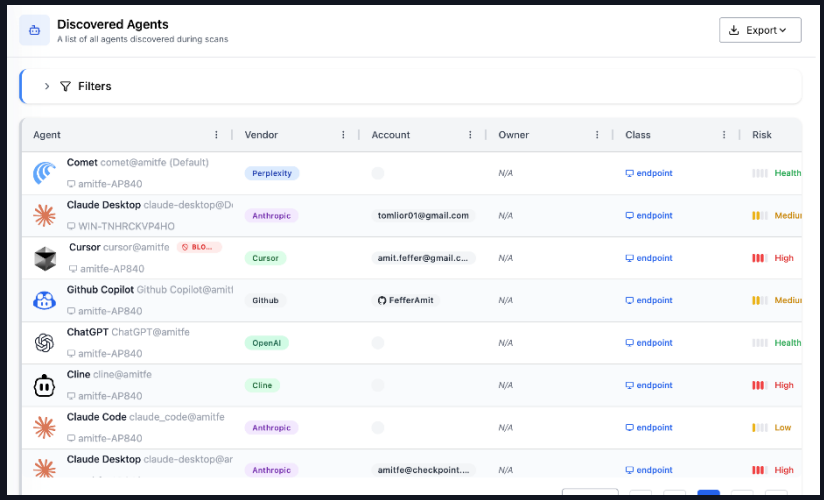
НОВЫЕ ВОЗМОЖНОСТИ

- Обнаружение и контроль доступа агентов ИИ на хостах и в SaaS
- Оценка рисков агентов в различных средах
- Контроль использования AgentCore и MCP
- Выявление теневых/неуправляемых агентов
- Непрерывный мониторинг агентов

Интеграция с корпоративными SaaS и экосистемами ИИ

139 Agents Discovered | 12 High Risk | Score: 92/100





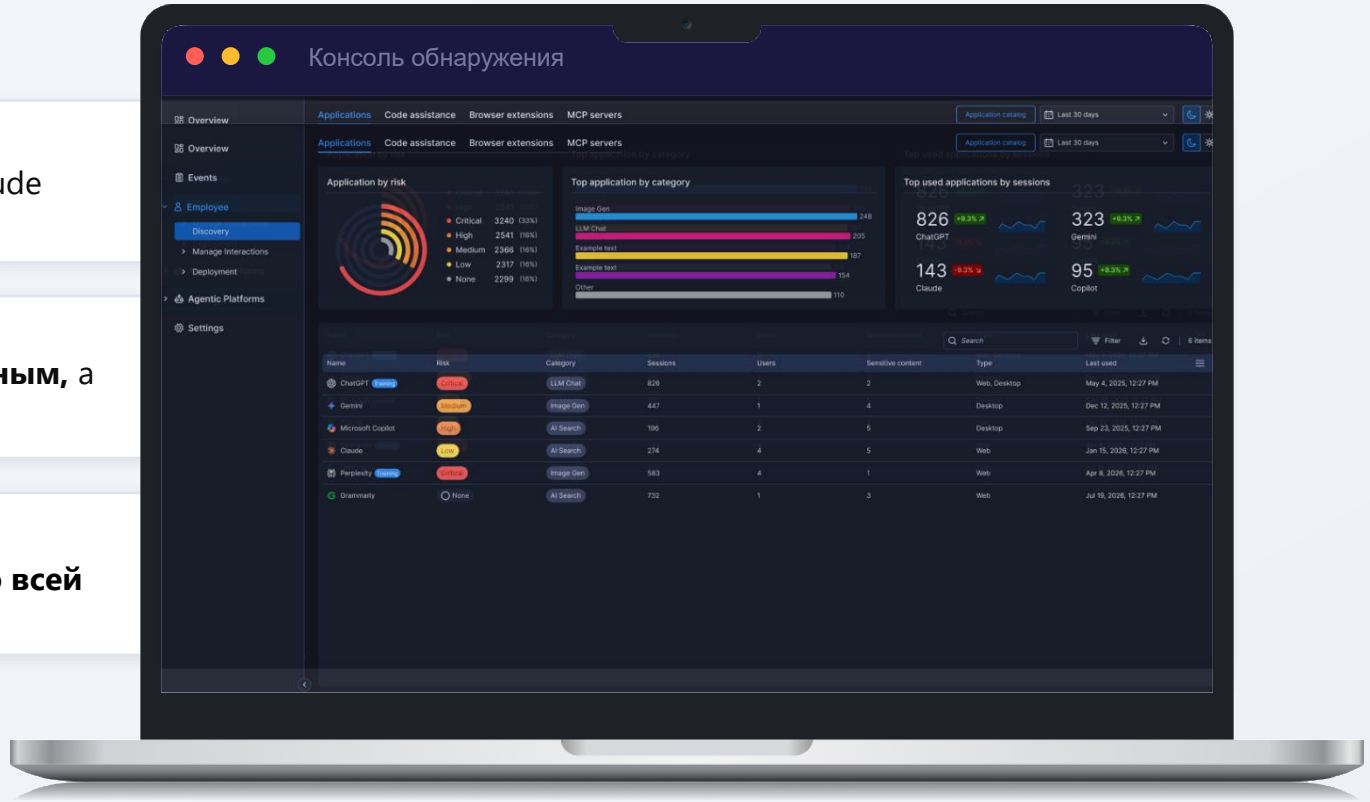
↑ *Обнаружение агентов и оценка рисков в режиме реального времени*

Workforce AI Security: защита ИИ-агентов для всей инфраструктуры

Использование ИИ **РАЗРЕШИТЬ!**
Защита без ущерба для продуктивности

Что это дает Заказчику?

- ✓ **Защита агентов ИИ на конечных точках** (Cursor, Claude Code, VSCode и др.)
- ✓ **Управление поведением агентов и доступом к данным,** а не только промптами
- ✓ **Безопасное использование ИИ для сотрудников во всей организации**



Развёртывание с агентом и без агента в масштабах предприятия

Начало работы с Workforce AI Security

Три шага для полного контроля над агентами

1

Создание политик

Определение агентов, пользователей и данных для мониторинга

2

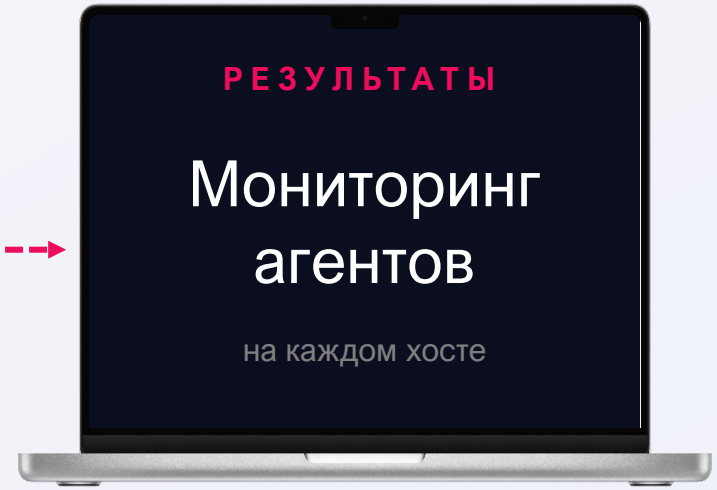
Загрузка установщика

Один клик в Infinity Portal — установщик готов

3

Развертывание агента

Распространение через MDM или SCCM на хосты с Windows и macOS



Опционально — интеграция с IdP для SSO

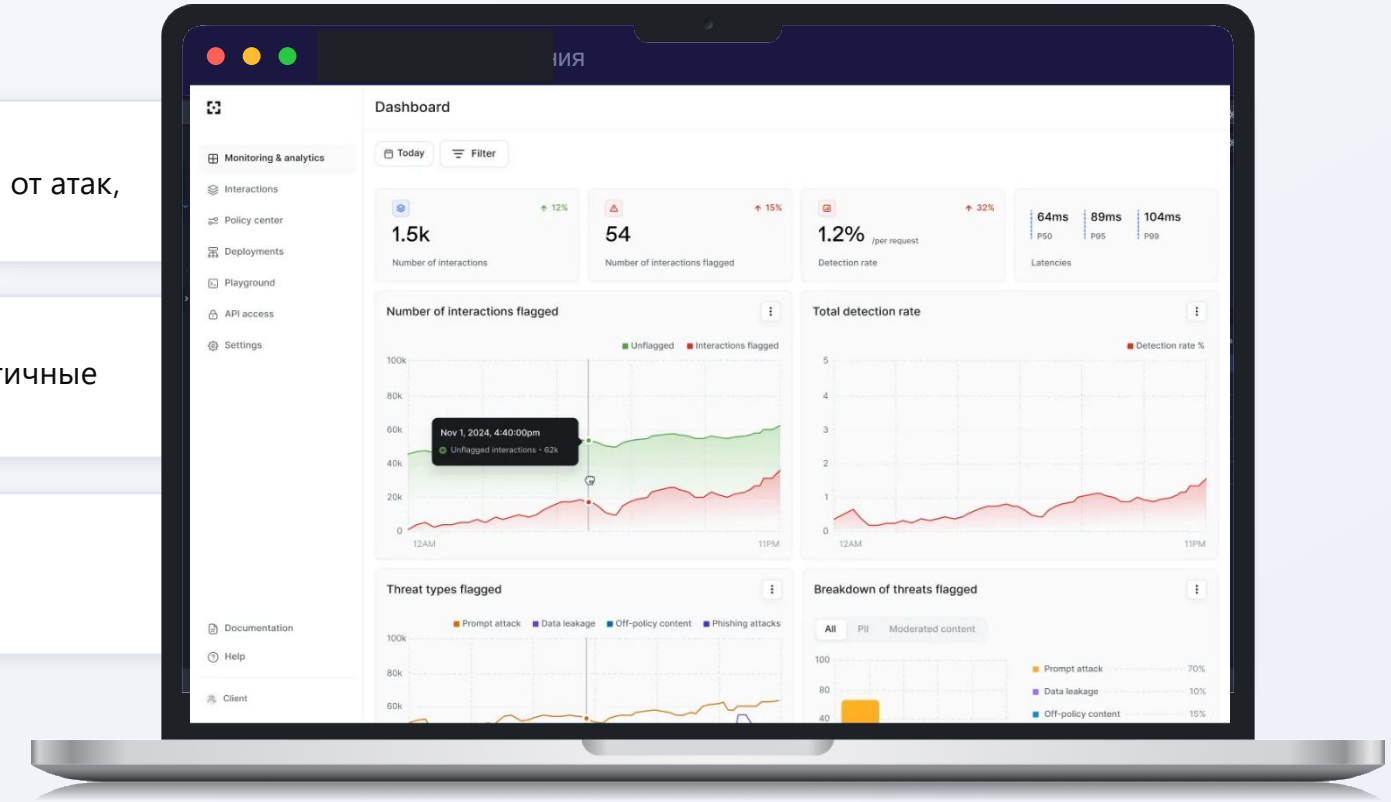
AI Agent Security: Непрерывная защита ИИ-систем в продуктивной среде

Предотвращение внедрения промптов, утечки данных и небезопасного поведения в агентах и приложениях ИИ — без замедления их работы.

Что это дает Заказчику?

- ✓ **Детерминированная защита в реальном времени** от атак, специфичных для ИИ
- ✓ **Применение политик с учётом контекста,** а не статичные правила
- ✓ **Встроенная защита** без необходимости пересмотра архитектуры

Inline защита с задержкой менее 50 мс



Начало работы с AI Agent Security

Три шага для защиты агентов в режиме реального времени

1

Подключение источников обнаружения

Copilot Studio, AWS Bedrock и др.

2

Интеграция с трафиком LLM

Подключение к LLM-шлюзу или MCP-серверу

3

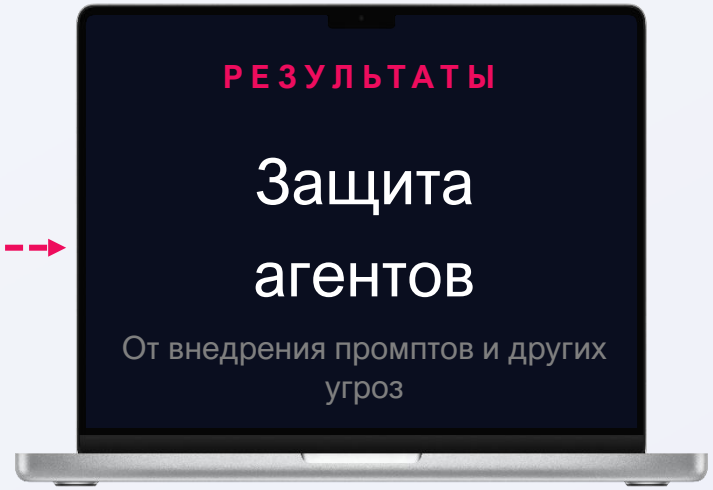
Определение политики применения

Блокировать

Редактировать

Помечать

Логировать



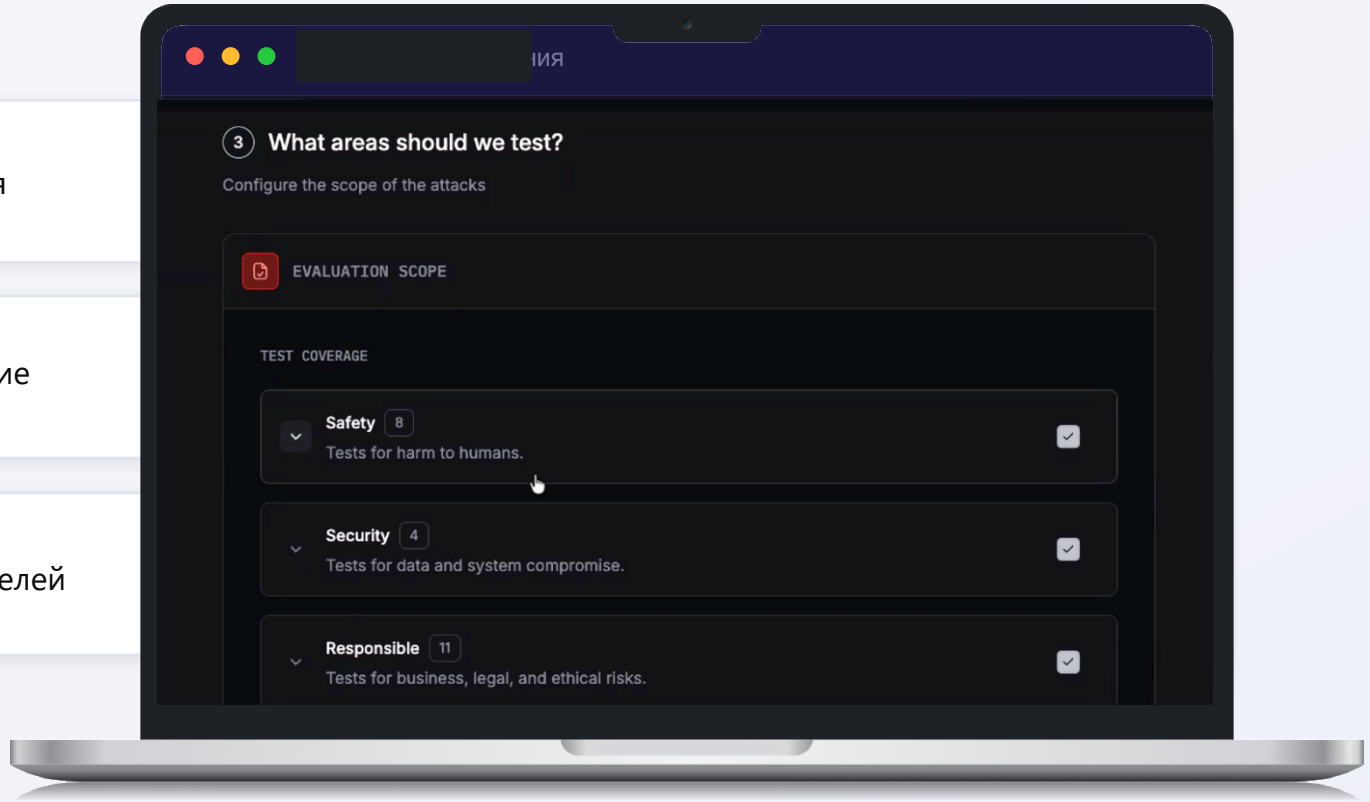
AI Red Teaming: тестирование систем ИИ на устойчивость к атакам

Моделирование реальных атак на ИИ для выявления уязвимостей в агентах и приложениях до выхода в продакшн

Что это дает Заказчику?

- ✓ **Адаптивная симуляция атак,** имитирующая действия реального злоумышленника
- ✓ **Непрерывно пополняемая база атак,** а не устаревшие тестовые наборы
- ✓ **Тестирование реальных систем ИИ,** а не только моделей или промптов

Обнаружьте уязвимости вашего ИИ раньше, чем это сделают злоумышленники



Начало работы с AI Red Teaming

Три шага для полноценного тестирования на устойчивость ИИ систем к атакам перед запуском

1

Конфигурация цели

Подключение модели, приложения или API

2

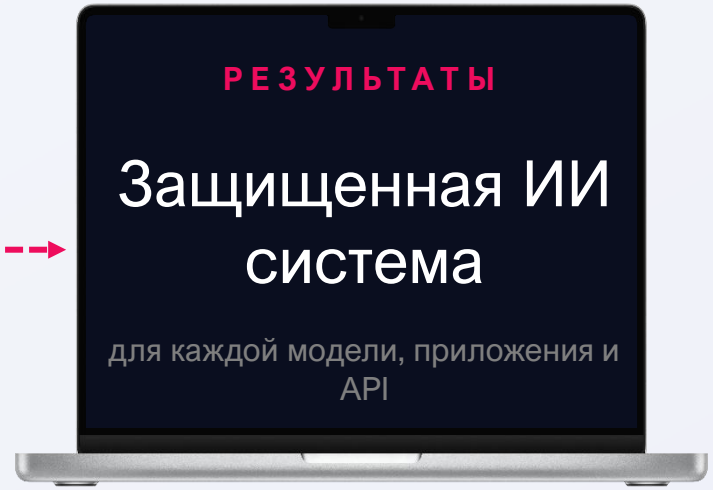
Симуляция атак

Создание и выполнение сценариев атак на ИИ систему

3

Оценка рисков

Изучение уязвимостей, их критичность и то, что и как необходимо исправить



Интеграции с экосистемой ИИ

От платформ ИИ до корпоративной инфраструктуры - полностью интегрировано в фабрику безопасности Check Point

НА ВЕДУЩИХ ПЛАТФОРМАХ ИИ И ОБЛАЧНЫХ СЕРВИСАХ

AWS Azure GCP NVIDIA

ВСТРОЕНО В ПЛАТФОРМУ CHECK POINT

Check Point Platform

CloudGuard WAF | Quantum NGFW | AI Factory FW | Harmony SASE | Harmony Endpoint

ПРИМЕРЫ ПРИМЕНЕНИЯ

- Расширение интеграций с **Copilot Studio и Glean**
- Соответствие **стандартам безопасности OWASP AI** и **нормативным требованиям**
- Ожидается: интеграция Red Teaming + **Exposure Management**

CHECK POINT™

Благодарю за внимание!

MONT TECH

We Secure Your
AI TRANSFORMATION