CHECK POINT™

AI-трансформация: как технологии сейчас меняют контуры ИТ и ИБ

Сергей Чекрыгин

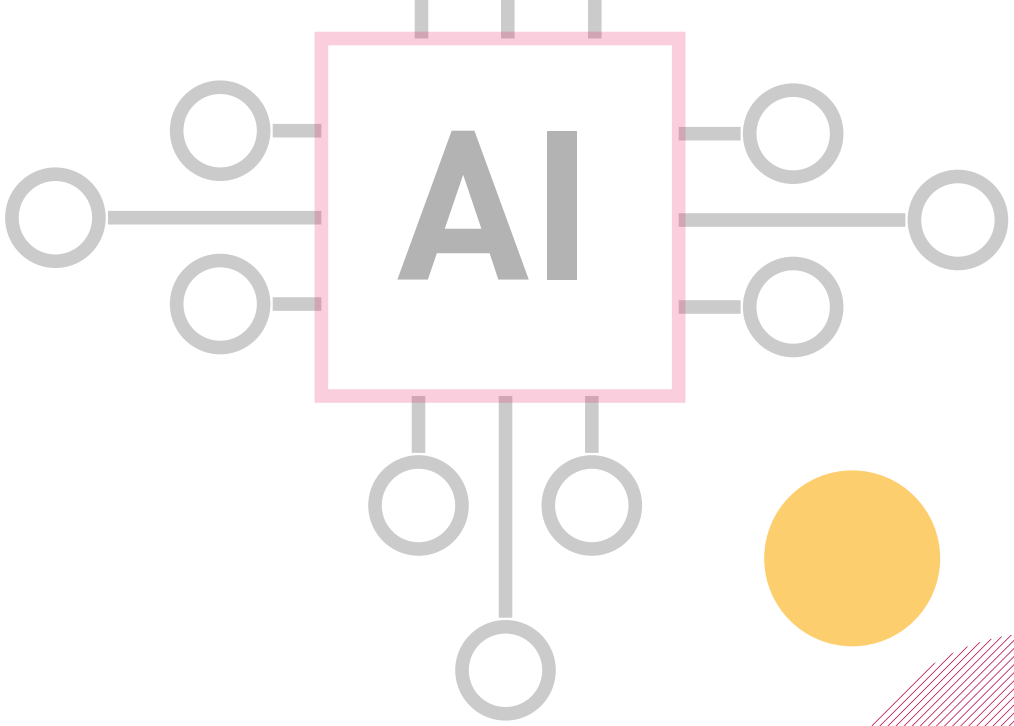
YOU DESERVE THE BEST SECURITY

Миссия Check Point

Мы защищаем вашу ИИ трансформацию

ИИ-трансформация (AI Transformation)

- Комплексное внедрение технологий искусственного интеллекта во все бизнес-процессы, продукты и культуру компании.
- Переход от отдельных IT-инструментов к принятию решений на основе данных, автоматизации рутины и изменению бизнес-модели для роста эффективности.
- Носит стратегический характер: В отличие от простой автоматизации, ИИ трансформирует архитектуру бизнеса.



70%

Сотрудников уже используют ИИ **без согласования.**

- Salesforce Survey 2025

Чат-боты

- Чат-бот – это большая зыковая модель, Large Language Model, LLM
- LLM — это «мозг» (пассивный генератор контента)
- Это часть Generative AI – создающих моделей
- Создающие ИИ используются для:
  - Создания текста
  - Генерации изображений
  - Генерации видео по тексту или оживления изображений
  - Создания кода приложений
  - Автоматизации поддержки и ответов на вопросы
- Содержат в себе знания многих экспертов в различных областях
- Имеют несколько уровней глубины рассуждений

Чем может угрожать чат-бот?

Добро пожаловать в мир агентов

ИИ агенты

Автономная или полуавтономная программа, использующая большие языковые модели (LLM) и алгоритмы для самостоятельного планирования, принятия решений и выполнения сложных задач без постоянного контроля человека

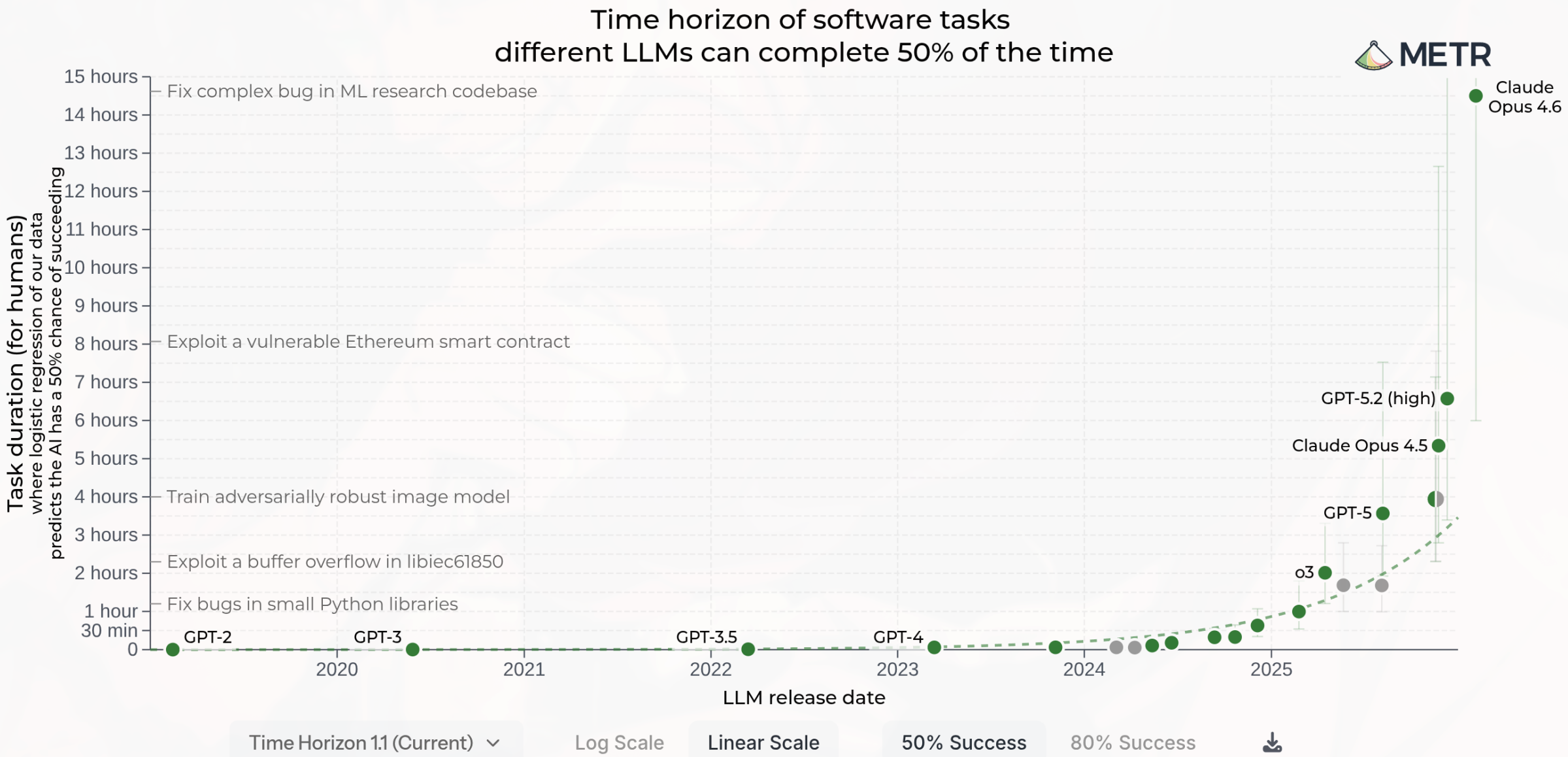
ИИ агент — это «мозг + руки», действующий проактивно

Работают с правами и привелегиями пользователя и знаниями LLM, возможно на компьютере пользователя

Ключевые отличия ИИ-агентов от LLM

	Языковая модель	ИИ агент
Автономность	Ждёт промпта (запроса) и выдают один ответ.	Получает цель, самостоятельно разбивает её на шаги и выполняет их
Действия (Tools):	Ограничена только текстом из обучающей выборки	Умеет пользоваться внешними инструментами: вызывать API, писать файлы, искать в базах данных
Память и контекст	Имеет ограничение контекстного окна	Обладает долгосрочной памятью (через RAG или базы данных), что позволяет помнить предыдущие действия и корректировать стратегию
Работа с обратной связью	Ждёт обратную связь от пользователя	Может оценить промежуточный результат (успешно ли выполнился код/поиск) и, самостоятельно попробовать другой подход

Сложность задач, которые решают агенты



Апокалипс Ко-пилотов

GitHub Copilot
(code generation)

Microsoft Copilot
(system-wide)
- Dynamics 365 Copilot
- Power Platform Copilot

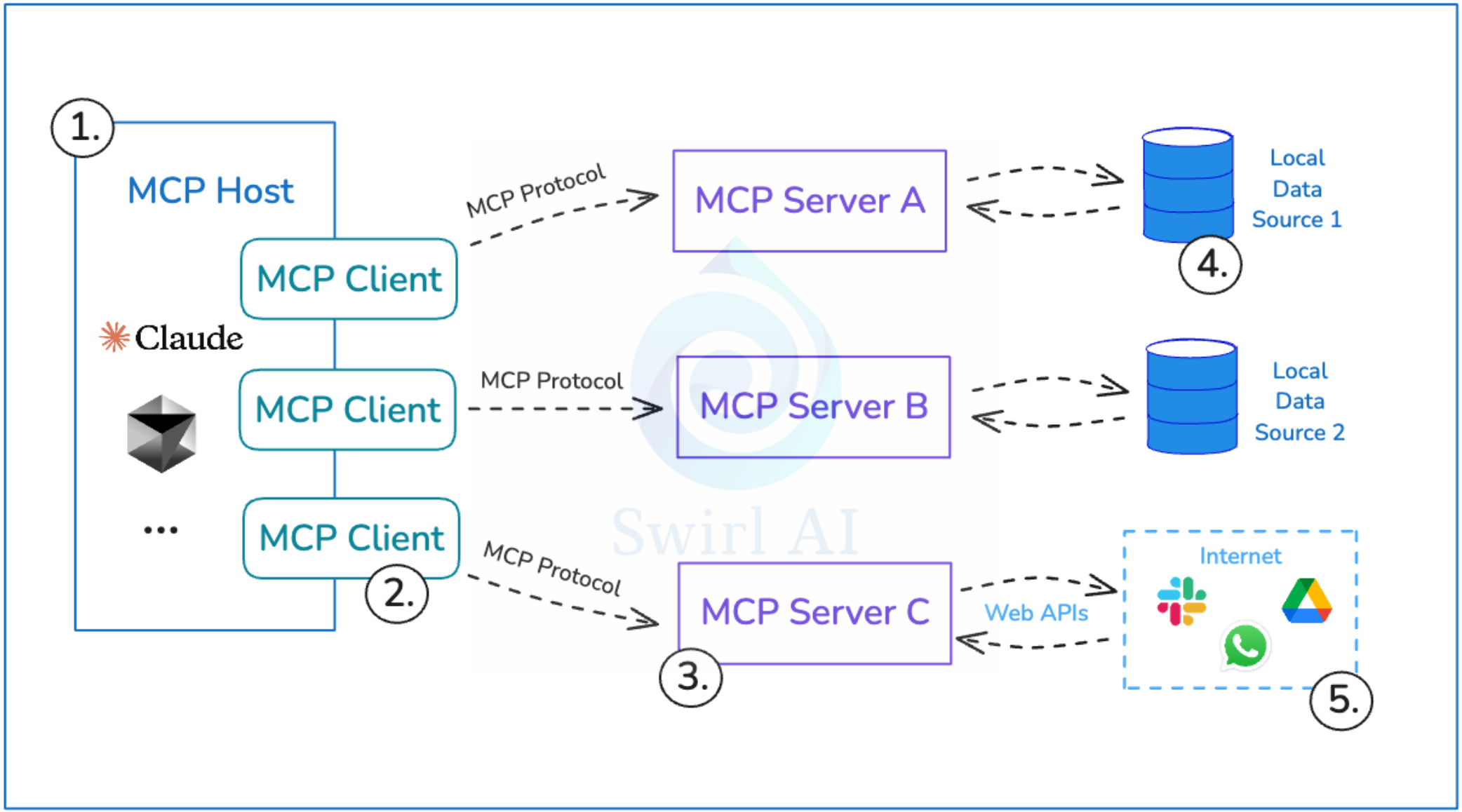
Einstein Copilot
(Salesforce)

Atlassian Intelligence Copilot

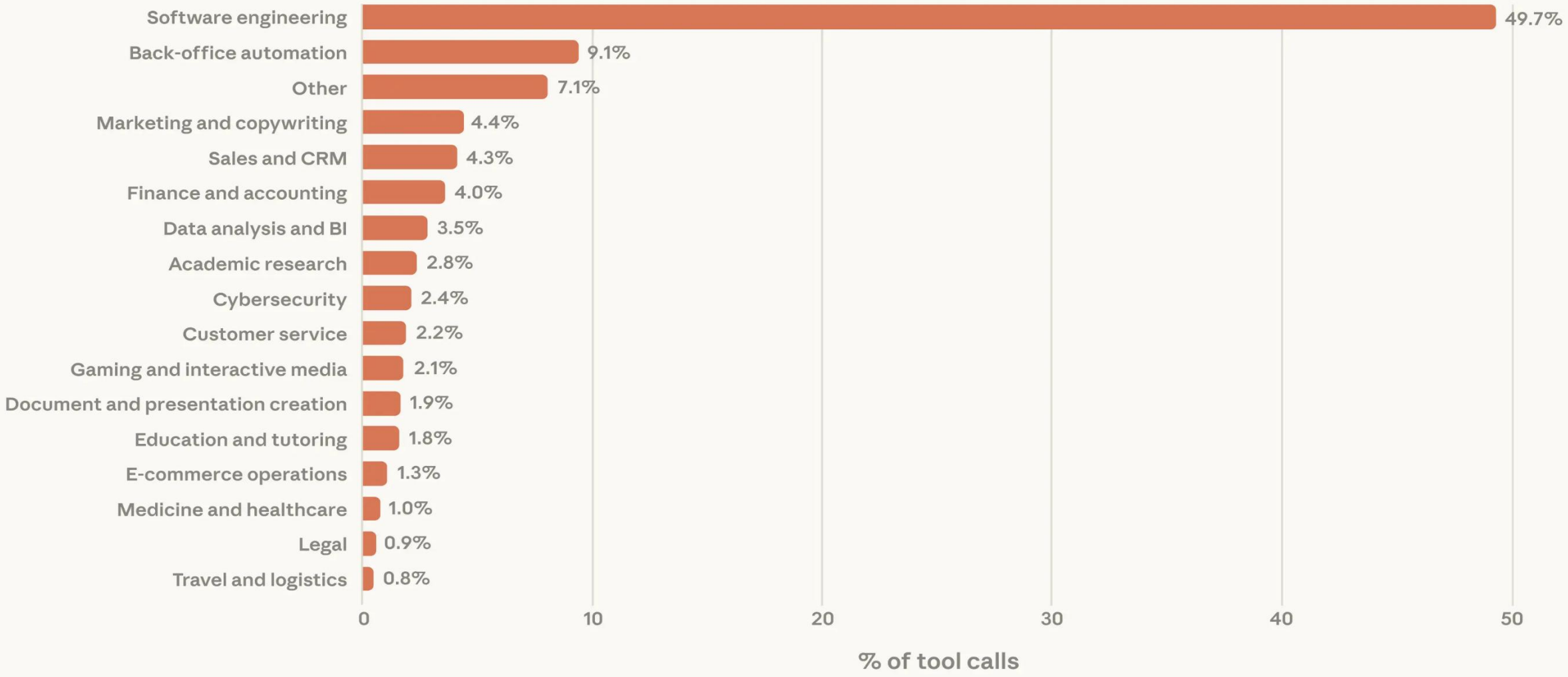
LinkedIn Recruiter Copilot

ServiceNow “Now Assist”

Model context protocol – обмен данными между агентами



Где (не) используются агенты



Корпоративное окружение + ИИ агент = **Новый уровень**

РИСКА

Что нужно ДИБу?

Единая платформа для контроля использования ИИ в организации

Защитить

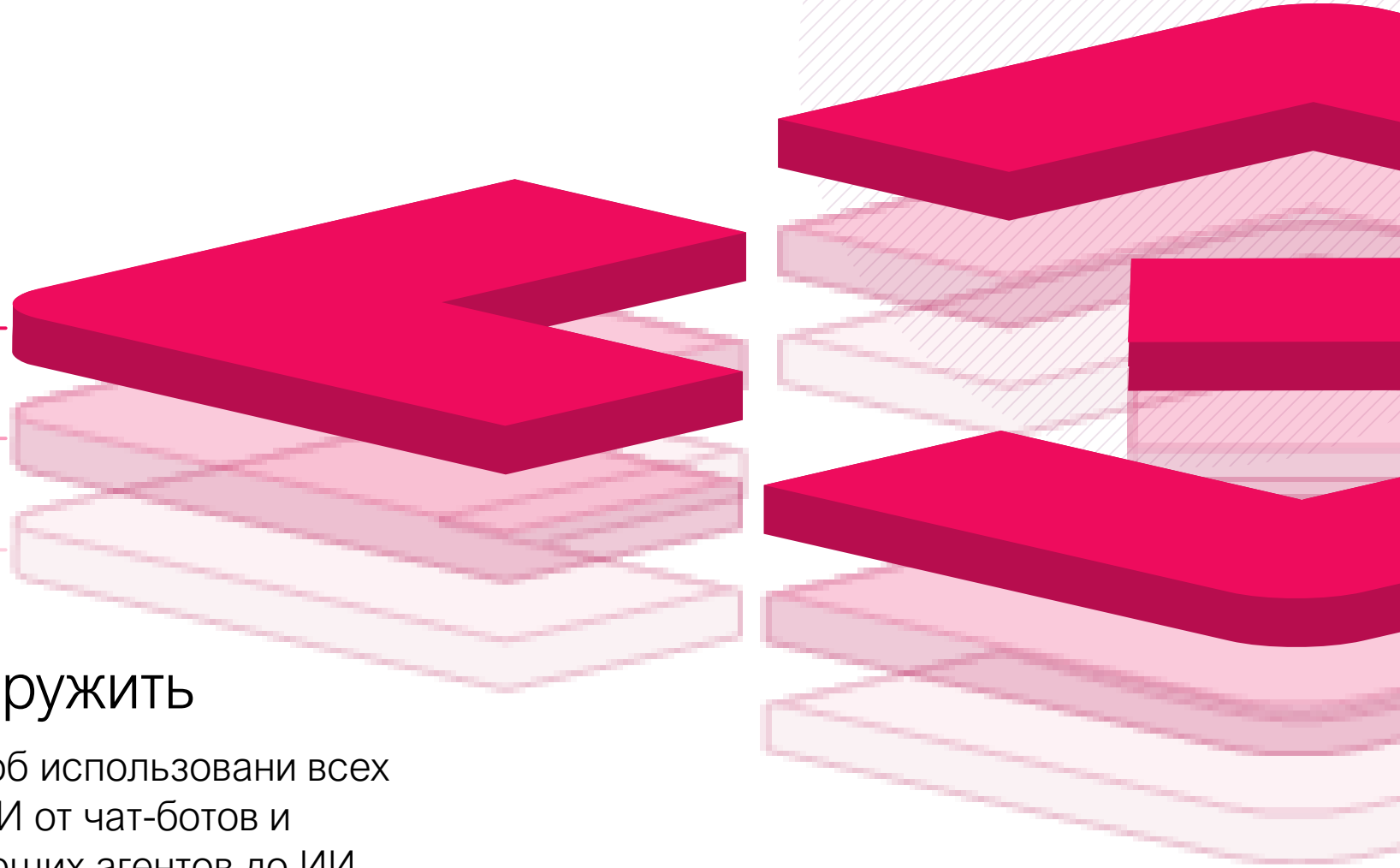
Блокировать небезопасные действия в реальном времени за счет применения ИИ ограничений и DLP

Управлять

Определить и применить правила для контроля риска использования ИИ приложений и действий пользователя

Обнаружить

Узнать об использовани всех типов ИИ от чат-ботов и кодирующих агентов до ИИ агентов



Продукты Check Point для контроля ИИ

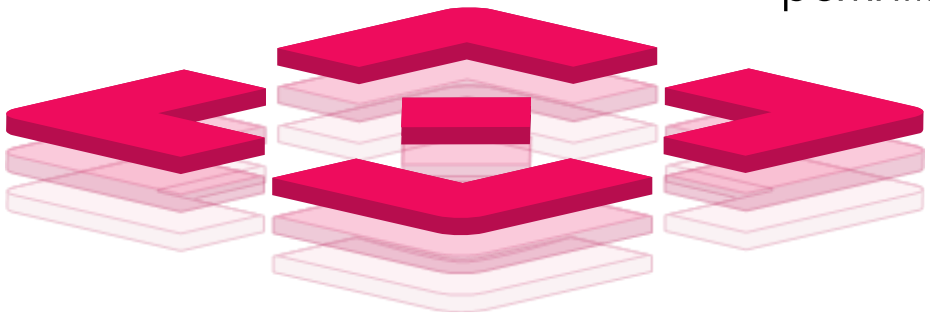
Объединённая модель безопасности для сотрудников, приложений и агентов.

Workforce AI Security

Обнаруживать и контролировать использование ИИ сотрудниками

AI Guardrails

Защита языковых моделей и чат-ботов от потенциально опасных запросов в режиме реального времени



Lakera Red

Автоматический и ручной аудит и проверка AI агентов перед использованием

CHECK POINT™

Спасибо за внимание

We Secure Your
AI TRANSFORMATION