

Эволюция DDoS-защиты: роль ИИ в 2026–2027 гг.



Павел Акифьев

Руководитель пресейл-направления Servicepipe



О компании



Компания основана
в 2015 году
ведущими экспертами
из крупных российских
зарубежных
ИТ-компаний

120+

Технических
экспертов
в команде, включая
специалистов
highload и big data



Собственная
геораспределенная
отказоустойчивая
платформа
фильтрации
с узлами в России
и Германии

500+

Клиентов, включая
ведущие компании
в различных
секторах: банки,
маркетплейсы, СМИ,
телеком и другие



Резидент
ИНТЦ МГУ



Продукты в реестре
отечественного ПО



Минцифры
России



О чём поговорим

1. Трансформация DDoS и что нас ждёт в будущем
2. Почему классические методы защиты скоро перестанут работать
3. Как реализованы интеллектуальные решения от Servicepipe
4. Следующие этапы развития систем защиты

Как угрозы эволюционируют в 2026-2027 гг. и почему ИИ скоро станет стандартом борьбы с DDoS

Фундаментальная трансформация киберугроз через ИИ

Изменение парадигмы атак:

От человека-оператора к ИИ-исполнителю:

Раньше злоумышленники использовали инструменты; теперь ИИ сам выполняет сложные операции.

Демократизация сложных атак:

Операторы без технических навыков теперь могут проводить атаки уровня АРТ-групп. Северокорейские «работники» не умели писать код, но успешно удерживали позиции разработчиков в компаниях из Fortune 500.

Масштабирование без увеличения ресурсов:

Один оператор GTG-2002 скомпрометировал 17 организаций за месяц — работа, требующая целой команды специалистов.

Вывод: Эффективность атак стала выше с использованием ИИ

Почему ИИ скоро станет стандартом для эффективной борьбы с DDoS

Старые подходы не выдерживают темпа

- Ещё недавно инженеру хватало 5–10 минут, чтобы изучить трафик и создать фильтры вручную.
- Сегодня на это есть не больше нескольких секунд – иначе атака уже сменила вектор.
- Классические системы, основанные на статических правилах и ручных плейбуках, просто не успевают адаптироваться.

Скорость реакции стала таким же важным параметром, как пропускная способность канала

2015 – реакция 10 мин.

2020 – 1 мин.

2025–2026 – секунды

Почему классическая DDoS-защита больше не справляется

TTM → секунды

Время выработки контрмер стремительно сокращается; окно на реакцию — секунды, не минуты/часы.

Мультивекторы сквозь L3/L4/L7

В одном рейде смешиваются UDP/TCP/TLS/HTTP; «раздельные» фильтры не вывозят.

Реактив не успевает

Ранее выписанные правила «застаиваются», не покрывают свежие комбинации/ковры по подсетям.

История сети = контекст

Без исторических данных защита слепнет: нет «нормы» трафика, и система путает всплеск спроса с атакой.

Шифрование ломает DPI

На L7 остаются поведенческие признаки (JA3/JA4/тайминги/последовательности), а не полезная нагрузка.

Цена ошибки — бизнес

Ошибка в сторону FP = падение SLA; нужны «мягкие» точечные меры по умолчанию.

Что нас ждёт в 2026–2027 гг.

В ближайшие время роль человека в DDoS-сценариях постепенно начнет переходить к ИИ — и в атаке, и в защите.

Современные DDoS — это цепочка фаз: сканирование, атака на каналы, затем на приложения.

Векторы переключаются мгновенно, подстраиваясь под реакцию защиты.

Такой тип атак называют «гибридными» или «многослойными», и они требуют синхронного ответа на всех уровнях OSI.

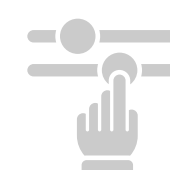
Любая задержка между эшелонами защиты превращается в уязвимость.



Победят те, кто встроит машинное обучение и ИИ не как надстройку, а как ядро своей архитектуры.



Реакция будет происходить на уровне миллисекунд, без ручного участия.

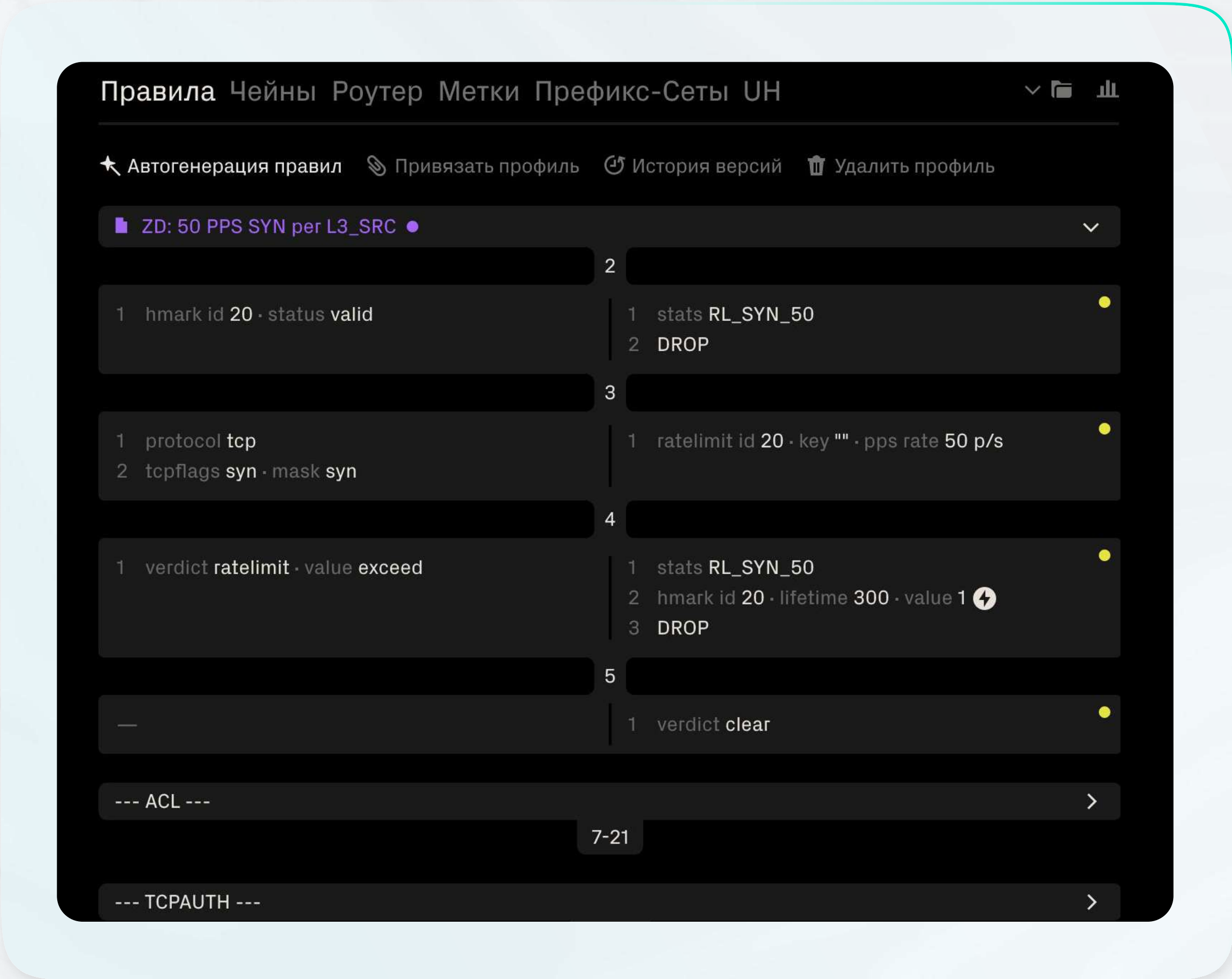


Главный вызов — сделать ИИ в кибербезопасности прозрачным и управляемым, чтобы человек сохранял контроль.

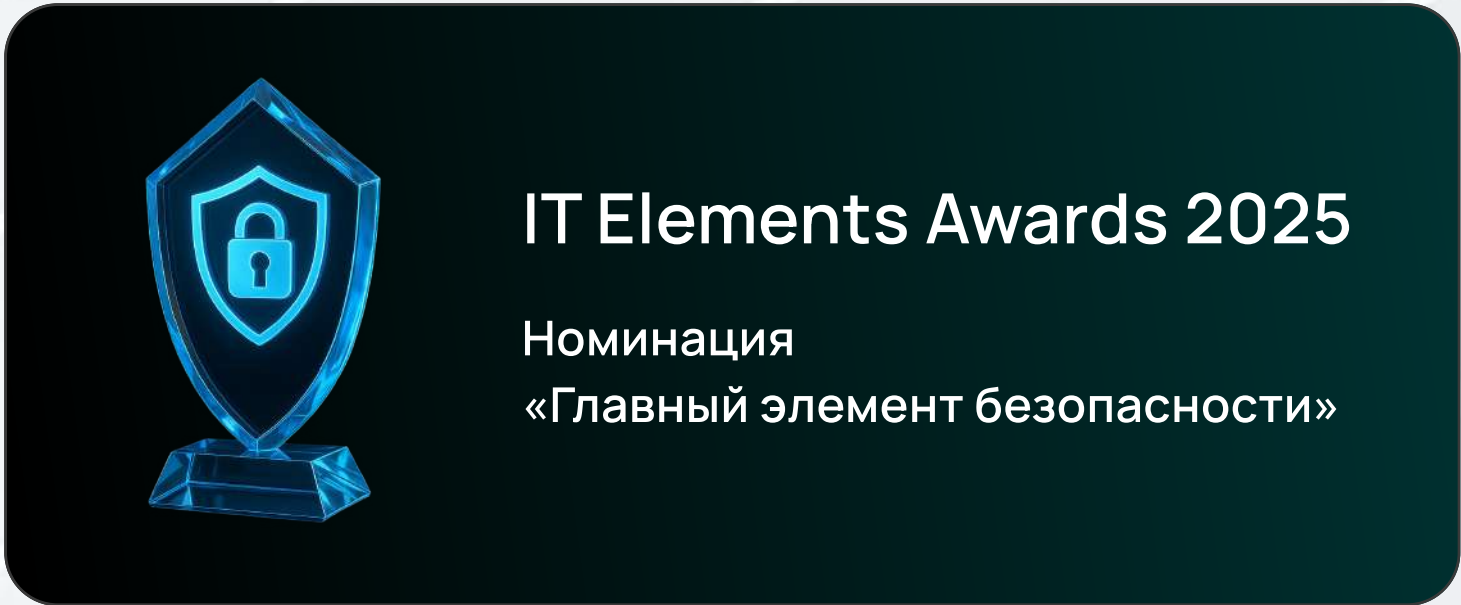


Как реализованы интеллектуальные решения от Servicepipe

DosGate Autopilot



Интеллектуальный модуль внутри Servicerpipe DosGate, автоматически создающий правила фильтрации в ответ на сетевые аномалии на основе анализа трафика атаки в реальном времени и без участия инженера.



DosGate Autopilot

На базе сигнатур, поведенческого анализа и rate-limit-метрик модуль Autopilot создаёт необходимое количество взаимосвязанных правил, не требуя ручной настройки:

- блокирует ботнеты, флуды и все типы амплификаций;
- активирует проверки, встроенные в DosGate, если это требуется для отражения атаки (например, TCP-аутентификацию);
- противодействует широкому спектру DDoS-угроз, включая сложные многовекторные атаки;
- следит за оптимальным порядком размещения правил для мгновенного эффекта.

The image displays three sequential screenshots of the DosGate Autopilot web interface, illustrating the automated rule generation process.

Скриншот 1: Показывает панель управления правилами. В меню слева выбран пункт "Правила". В центре экрана активирована опция "Автогенерация правил" (выделена красным прямоугольником). В выпадающем меню выбрана настройка "ZD: 50 PPS SYN per L3_SRC".

Скриншот 2: Показывает процесс генерации правил. На экране отображается сообщение: "Генерируем правила для очистки трафика, это займет до 2 минут. Сгенерированные правила добавим в список контроллеров." В центре экрана находится значок "Отменить".

Скриншот 3: Показывает редактирование правил. В заголовке отображается информация о профиле: "profile123, 13:57:01, Jun 29 2025". В центре экрана отображается таблица правил, включающая правила для TCP Auth with RST method, hmark, verdict tcpauth и stats TCP_AUTH.

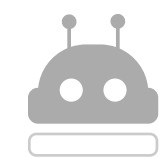
Cybert

Система тонкой фильтрации трафика для высокоточной защиты веб-ресурсов от любой нежелательной автоматизации без потери пользователей



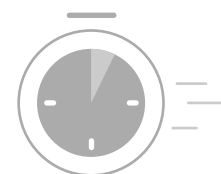
Realtime-анализ 100+ параметров каждого запроса

Статистика — не основа для принятия решений



Защита от любых автоматизированных угроз

Сигнатуры не являются статической частью конфигурации, а генерируются автоматически на лету



Моментальное реагирование, вердикт < 1 мс

Полностью автоматический real-time анализ



Высокоточная фильтрация, < 0,01% false positive

Полностью автоматический real-time анализ

Трафик запросов

Первичный анализ

Мониторинг всплесков трафика и деградаций параметра response time

Сигнатурный анализ

Сопоставление технических параметров запроса с уже известными сигнатурами

Репутационный анализ

Оценка характеристики профилю трафика ресурса

Поведенческий анализ

Выборочная допроверка в пограничных случаях



Команда аналитиков

Обновление алгоритмов для повышения точности фильтрации

Нелегитимные боты

Полезные боты

Пользователи

Следующие этапы развития систем защиты

Стандартная схема эшелонированной защиты

Атаки по модели OSI

L3-L4 (Сетевой и транспортный уровни)

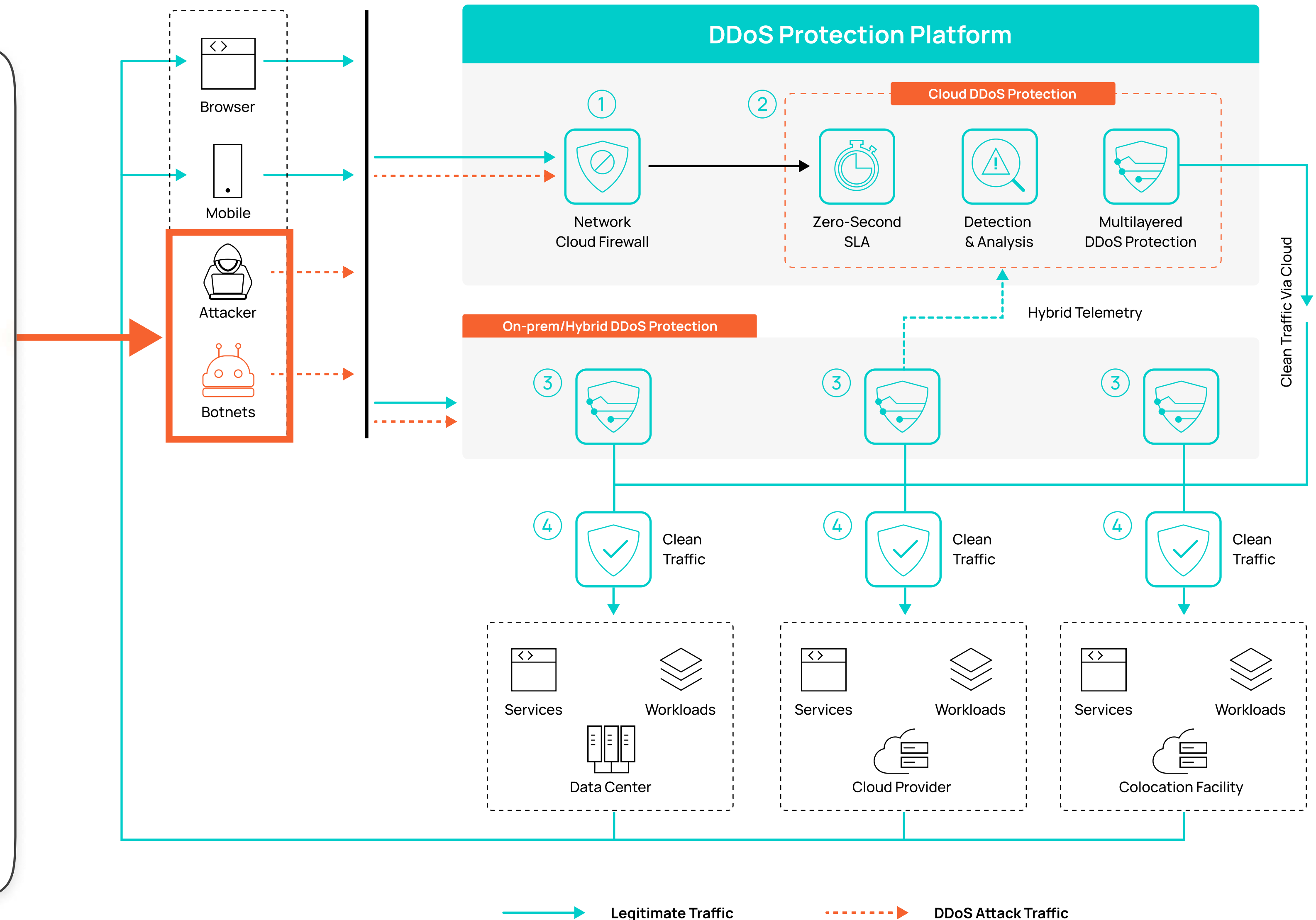
Типичные атаки:

- UDP flood, ICMP flood
- TCP SYN flood, ACK flood, RST flood
- Amplification-атаки (DNS, NTP, Memcached и др.)
- Reflection-атаки
- Volumetric (залив канала трафиком)

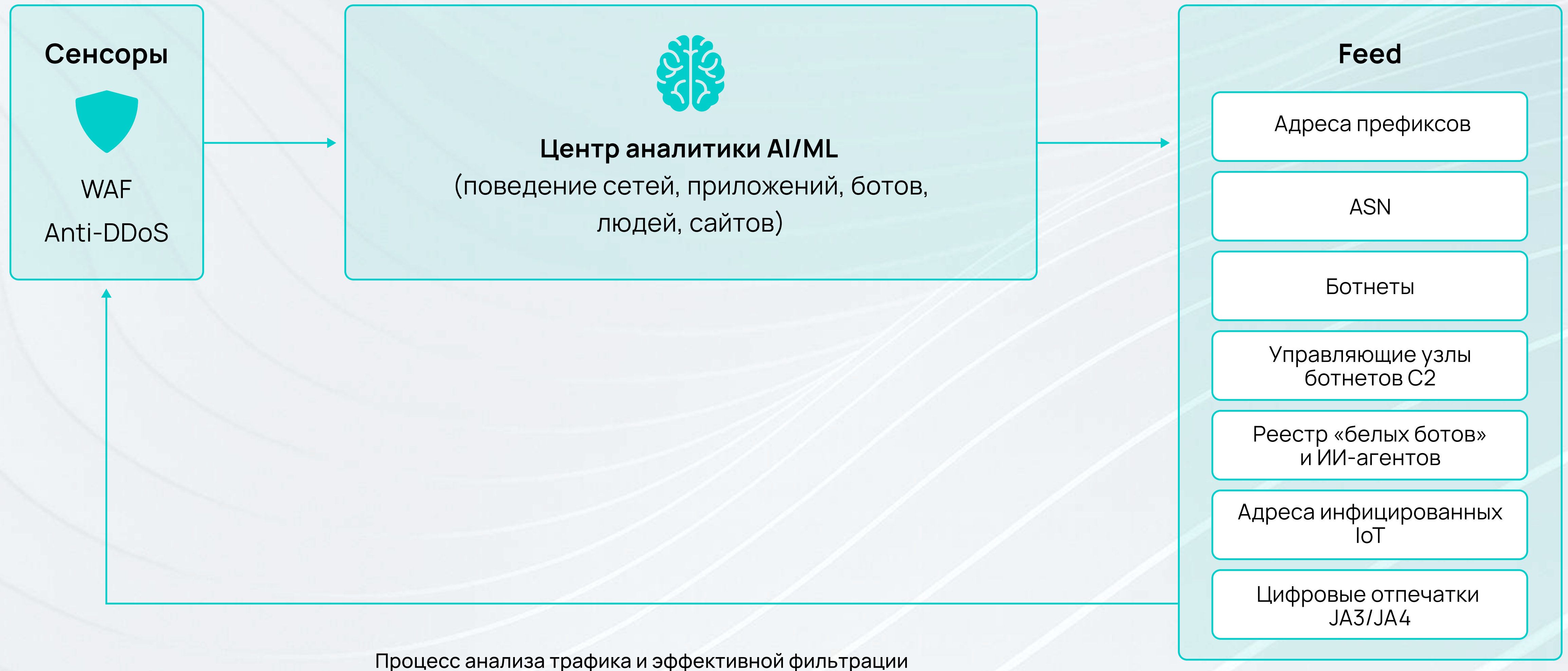
L7 (Прикладной уровень)

Типичные атаки:

- HTTP flood (GET/POST)
- Slowloris, Slow POST
- Атаки на API (например, массовые запросы)
- Атаки на авторизацию/сессии (login brute, session exhaustion)
- Бот-активность (парсеры, скрипты, credential stuffing, фрод)



Платформа аналитики ИИ – ядро системы



Архитектура с ML в решениях Anti-DDoS



Данные — новый капитал киберзащиты

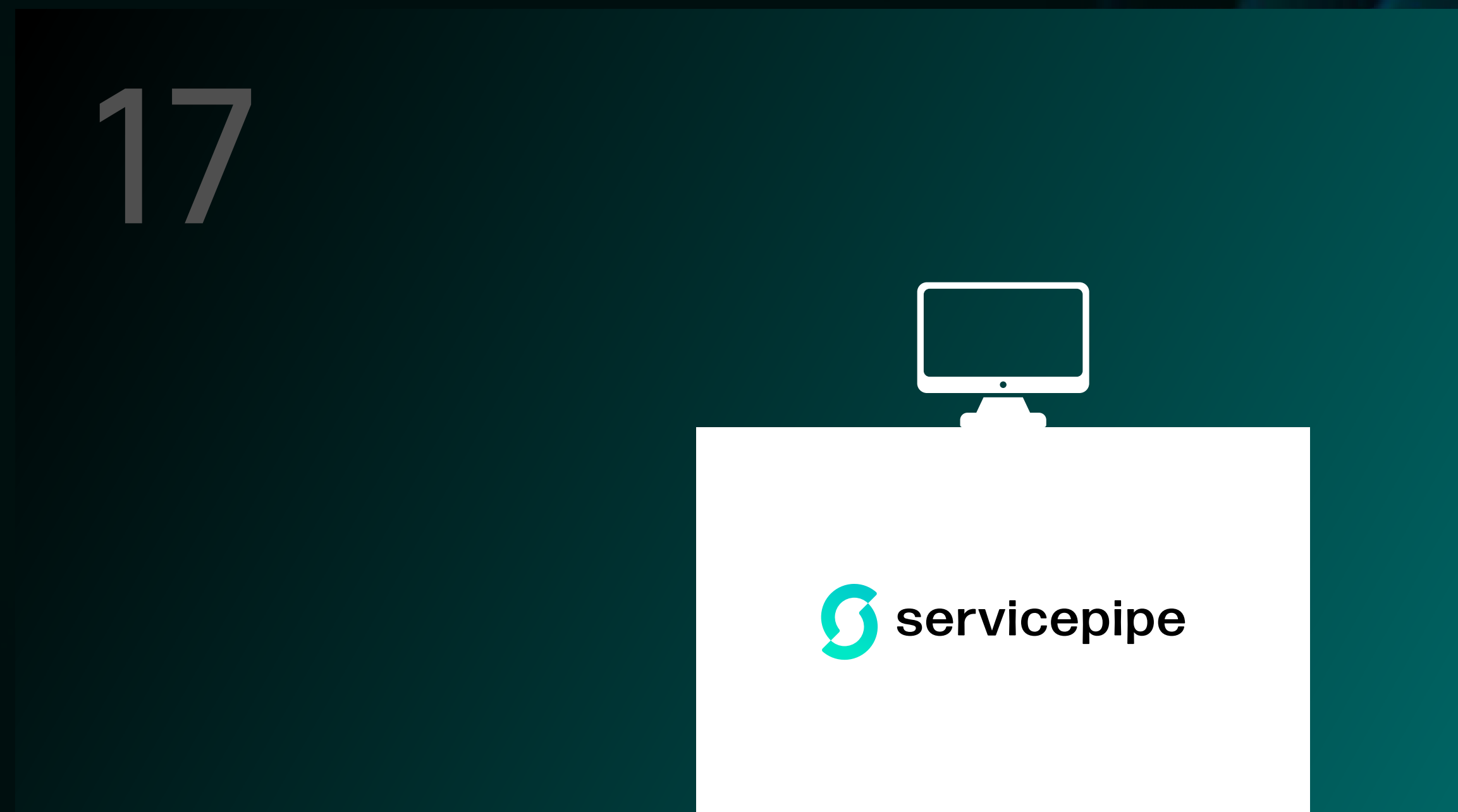
- Эффективность ИИ-защиты напрямую зависит от объёма и разнообразия данных, на которых обучаются модели.
- Только те вендоры, у которых есть доступ к живому трафику смогут создать по-настоящему точные модели.
- Чем больше атак, клиентов и сетевых сценариев проходит через систему, тем умнее и адаптивнее становится защита.

Победят те, кто обучает модели на больших объёмах реального трафика.

Servicepipe обладает уникальным преимуществом — наши сервисные продукты защиты формируют непрерывный поток реальных данных, который ежедневно используется для обучения моделей и обновления паттернов угроз.



Записывайтесь
на демо



Ждем вас на стенде №17