

# Все Сервисы ИБ Yandex Cloud

**Марат Вахитов**

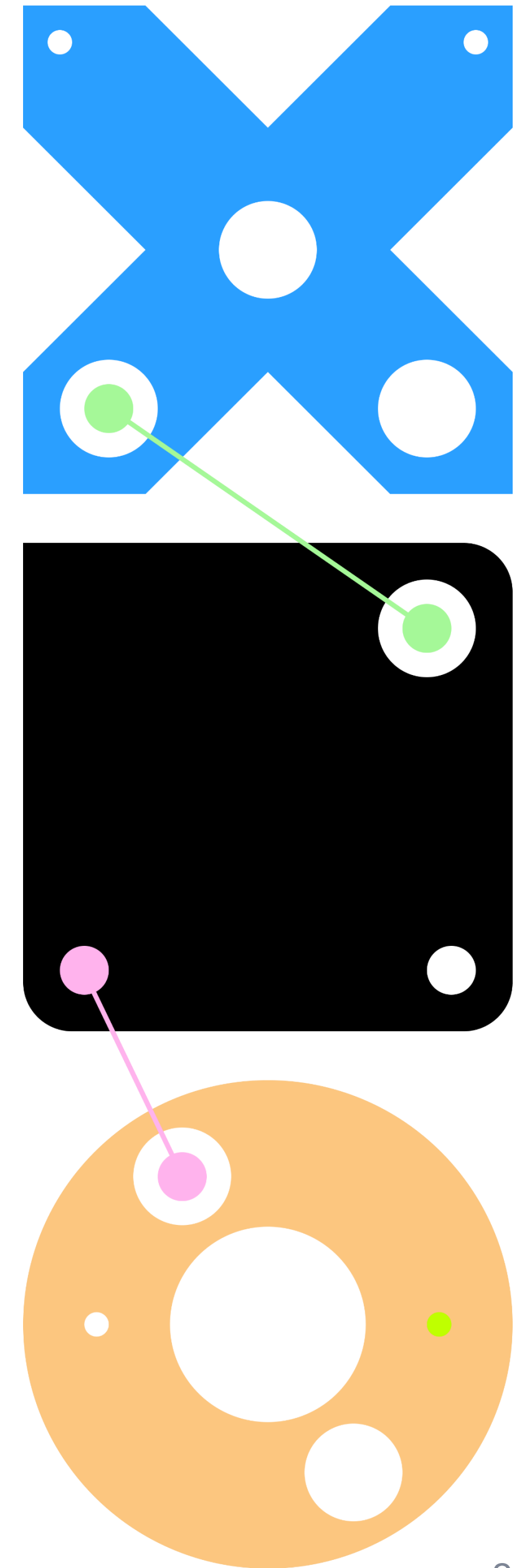
Security Solution Sales,  
Yandex Cloud

**Алексей Чупринин**

Руководитель направления защиты  
приложений, «Софтлайн Решения»

# О чём поговорим?

1. Продукты безопасности  
Yandex Cloud
2. Компетенции «Софтлайн Решений»
3. Q&A  
Ответы на вопросы



# Продукты безопасности Yandex Cloud

## Yandex Smart Web Security

Сервис для защиты сайтов и приложений от DDoS-, веб-атак и ботов

## AI Security Gateway

Шлюз для защиты ИИ-приложений

## Yandex Identity Hub

Централизованное управление учётными записями и доступ к корпоративным ресурсам (SSO)

## Yandex Cloud Detection and Response (YCDR)

SOC-сервис для мониторинга и реагирования на инциденты

## Yandex SIEM

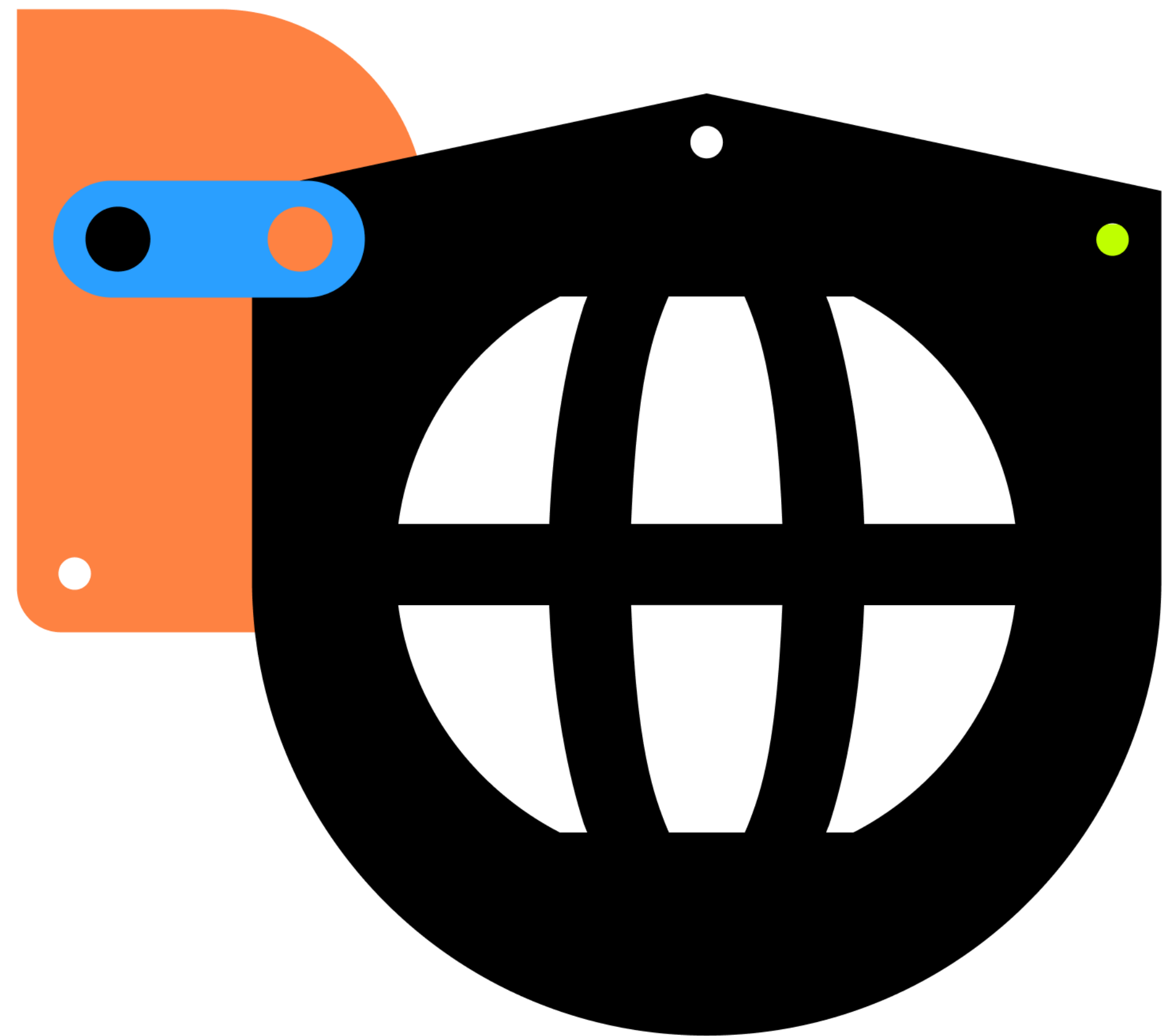
Система мониторинга событий безопасности и обнаружения угроз

## Security Deck

Платформа для контроля безопасности облачных ресурсов

# Yandex Smart Web Security

Платформа для защиты сайтов  
и приложений от DDoS-, веб-атак и ботов



# Возможности по защите

## Защита от DDoS-атак уровней L3, L4 и L7

L3 и L4 DDoS — атаки на TCP и UDP

L7 DDoS — атаки на уровне приложений

## Защита от эксплуатации уязвимостей веб-приложений

Защита от основных классов веб-угроз, включая OWASP® Top 10

Защита от атак на бизнес-логику приложения

Защита от атак на механизмы идентификации и авторизации

Защита API

Защита корпоративных сервисов (SAP®, Oracle®, 1C)

## Защита от ботов и парсеров

Парсеры

Скраперы

Поведенческие атаки (брутфорс, СМС-бомбинг)

Фродеры

Скликиватели и другие сложные роботы

# Преимущества **Smart Web Security**

Сервис для защиты веб-приложений

## **Защищаем как себя**

Мы давно знакомы с ландшафтом угроз из каждой сферы бизнеса и используем в своих продуктах те же технологии защиты, которые предлагаем рынку

## **Обучаем защиту на трафике Рунета**

Используем собственные ML-технологии для защиты приложений, которые обучаем на трафике всего Рунета. Это обеспечивает минимальный вклад в задержки и возможность предотвращать ранее неизвестные типы атак

## **Минимальный вклад в задержки**

Решение разработано специально для высоконагруженных сервисов, обладает высокой производительностью и вносит минимальный вклад в отсрочки

# Преимущества **Smart Web Security**

Сервис для защиты веб-приложений

## **SolidWall WAF в составе Smart Web Security**

Усиливает защиту при помощи анализа бизнес-логики приложения, защиты конечных точек приложения (API), возможности работы по позитивной модели и выявления сложных ботов

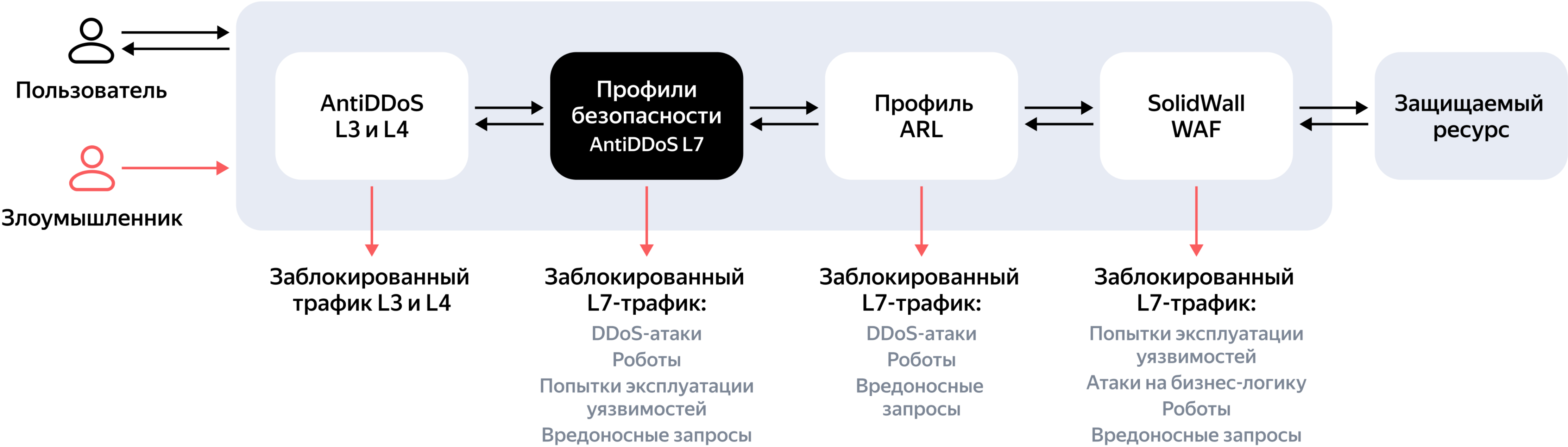
## **Широкий инструментарий по борьбе с ботами**

Выявление роботов на основе поведенческой модели, возможность отправки ботов на challenge, управление трафиком роботов при помощи списков верифицированных ботов и TLS-отпечатков, а также нативная интеграция с сервисом Smart Captcha

## **Гибкая настройка политик и правил фильтрации**

Настраивайте правила фильтрации трафика для каждого модуля и управляйте их приоритетом. В сервисе можно гибко настраивать политики фильтрации для разных частей приложения, эндпоинтов API, параметров и источников запроса

# Архитектура решения



# AntiDDoS L3 и L4 от Яндекса

Preview

Автоматическая фильтрация трафика на сетевом и транспортном уровнях (L3 и L4) от атак:

TCP SYN flood

TCP ACK flood

TCP fragment flood

TCP connection flood

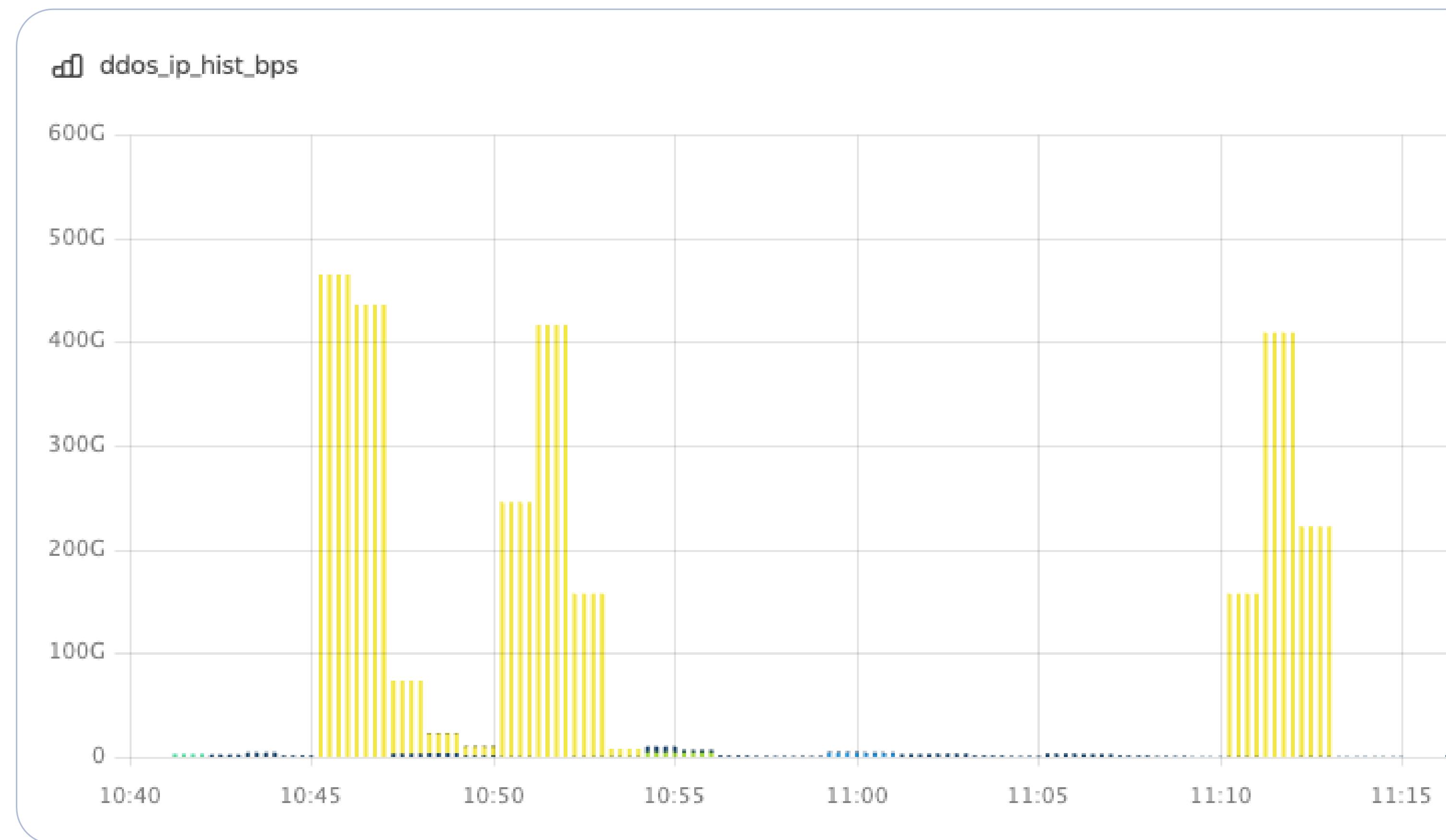
UDP flood

Стойки фильтрации в точках присутствия Yandex Cloud

Треть клиентов SWS уже защищены

Защищаем высоконагруженные сервисы — до 8K RPS

Отбили атаку 500 Гбит/с



# AntiDDoS L7. Smart Protection

**Анализирует трафик  
с помощью алгоритмов  
машинного обучения  
и поведенческого анализа**

Блокирует атаки, аномальные  
и нелегитимные запросы

Подозрительные запросы отправляет  
в сервис SmartCaptcha

**Построен на собственной технологии  
Яндекса «Антиробот»**

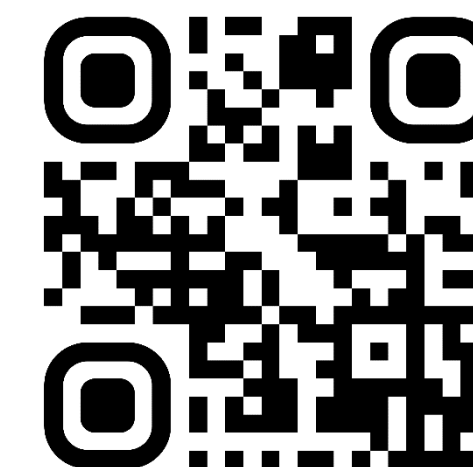
Защищает уже более 100 сервисов, включая:



Подробнее о технологии:



[clck.ru/  
3SrnDM](https://clck.ru/3SrnDM)



[clck.ru/  
3SrnR9](https://clck.ru/3SrnR9)

# Yandex Smart Web Security WAF

**Yandex Ruleset:** широкое покрытие сигнатур и сканеров. Теперь совместно с командой SolidWall WAF

**ML WAF (Yandex Malicious Score):** для обнаружения атак, которые не детектируются сигнатурным методом, и покрытия 0-day-уязвимостей

**OWASP® Core Ruleset** — набор правил от сообщества OWASP®

arch yc yc-sws Object Storage / Бакеты / app-bucket

### Создание профиля WAF

Имя\*

Описание

Метки

#### Наборы правил

Выберите один или несколько наборов правил, которые будут применяться для анализа и действий с запросами. Настроить выбранные наборы можно после создания профиля WAF.

Набор / Вендор	Версия	Количество правил <sup>?</sup>	Описание	Выбран
Yandex Ruleset <small>PREVIEW</small> Yandex	0.1.0	167	Набор разработан сообществом инженеров и аналитиков информационной безопасности Яндекса и состоит из ... тестируется на реальном трафике сервисов Yandex.	<input checked="" type="checkbox"/>
Yandex Malicious Score <small>PREVIEW</small> Yandex	latest	6	Набор разработан инженерами и аналитиками Яндекса для выявления вредоносных запросов с помощью технологий машинного обучения. Это позволяет выявлять неизвестные угрозы и оперативно адаптироваться к новым типам атак, обеспечивая защиту в реальном времени. Набор проходит тестирование и показывает высокую эффективность при низком уровне ложных срабатываний.	<input type="checkbox"/>
OWASP Core Ruleset OWASP	4.8.0 <sup>▼</sup>	264	Набор разработан открытым сообществом OWASP и состоит из правил, которые предназначены для обнаружения вредоносных действий, включая загрузку вредоносных файлов, потенциальные атаки SQL Injection, попытки отказа в обслуживании, попытки инъекции кода и многое другое.	<input type="checkbox"/>

# SolidWall WAF

Preview

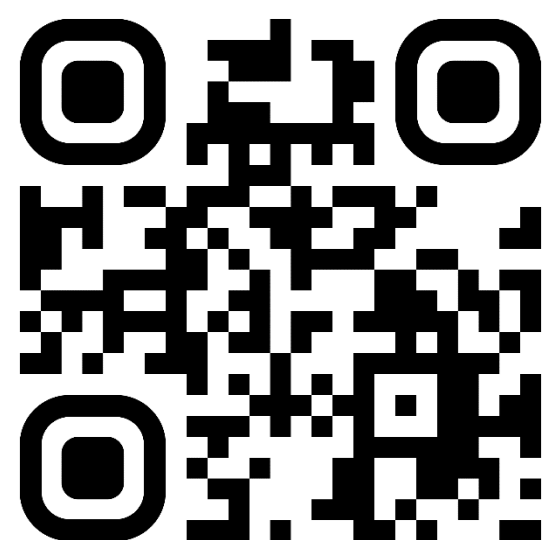
Теперь часть Yandex Smart Web Security

Сочетает негативную  
и позитивную модели защиты

Анализ поведения пользователей  
для выявления продвинутых ботов

Инвентаризация API

Подключается в несколько кликов



Запросить  
доступ:  
[clck.ru/3T84fo](https://clck.ru/3T84fo)

The screenshot shows the management interface for a SolidWall WAF profile. The breadcrumb navigation at the top reads: arch / yc yc-vpc / Smart Web Security / Защита доменов / Профили SolidWall WAF / solidwall-waf-main / Обзор. The main header is "solidwall-waf-main" with the subtitle "Профиль SolidWall WAF". A left sidebar contains three menu items: "Обзор" (Overview), "Операции" (Operations), and "Панель управления" (Control Panel). The "Обзор" section displays the following details:

- Имя: solidwall-waf-main
- Идентификатор: esqsjbg18eoh0ceg1geh
- Описание: —
- Статус: Active


Below this, the "Подключенные домены" (Connected domains) section shows "Нет доменов" (No domains) with the instruction "Создайте или выберите домен, который собираетесь защищать." (Create or select a domain you intend to protect.) and a "Подключить домен" (Connect domain) button.

At the bottom, a "Документация" (Documentation) section lists links for "Все сервисы Yandex Cloud", "Начало работы с сервисами", "Практические руководства", "Описание технической поддержки", and "Вся документация".

# AntiBot

- Поведенческий анализ для определения уровня автоматизации запроса
- Капча
- TLS-отпечатки JA3/JA4
- Защита от ИИ-краулеров
- Списки верифицированных ботов
- JS Challenge Coming soon
- Cookie Challenge Coming soon

**Я не робот**  
Нажмите, чтобы продолжить  
SmartCaptcha by Yandex Cloud ?



Введите текст с картинки

↻ 🔊 ℹ️ Отправить

SmartCaptcha by Yandex Cloud ?

# Референсные клиенты

 ZENDESK

КОФЕМАНИЯ

 ProgressMe

 МИР  
ИНСТРУМЕНТА

 *Капуста*

 циан

# Ценообразование

## Подписки

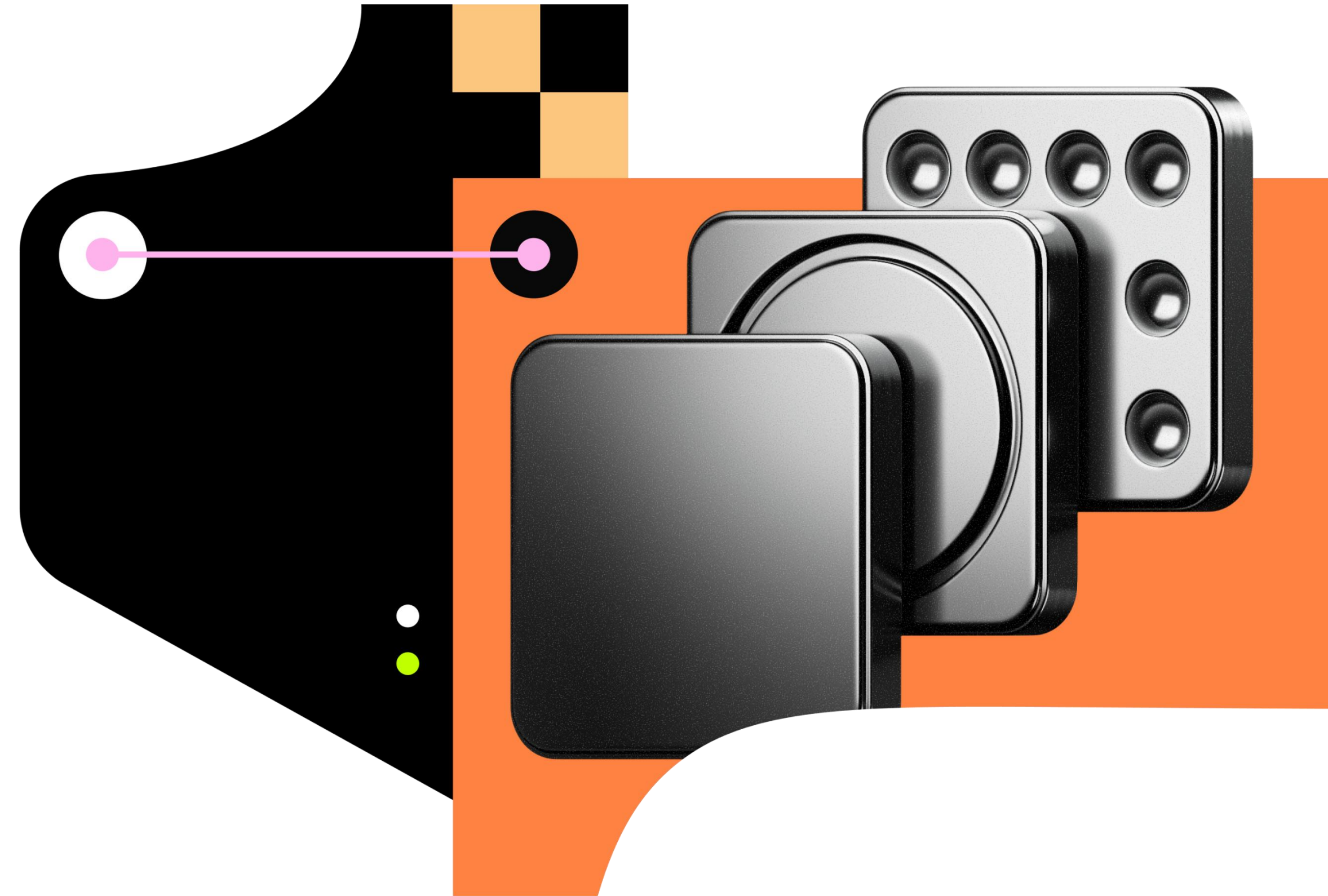
	Start, вкл. НДС	Pro, вкл. НДС	Business, вкл. НДС	Enterprise
Количество легитимных запросов в месяц, включенных в абонентскую плату, в миллионах	100	500	1 000	Рассчитывается индивидуально
Абонентская плата за пакет AntiDDoS, ежемесячно. Пакет включает обработку запросов правилами <a href="#">профиля безопасности</a> : <ul style="list-style-type: none"><li>• базовыми</li><li>• Smart Protection</li></ul>	50 833 ₽	160 633 ₽	259 250 ₽	Рассчитывается индивидуально
Абонентская плата за пакет WAF, ежемесячно. Пакет включает анализ запросов <a href="#">правилами WAF</a>	40 667 ₽	76 250 ₽	152 500 ₽	Рассчитывается индивидуально

## PAYG

The screenshot shows the Yandex Cloud pricing calculator for Smart Web Security 1. The interface includes a header with the Yandex Cloud logo, navigation links (Сервисы, Решения, Почему Yandex Cloud, Ресурсы, Цены, Кейсы, Документация, Блог), a search bar, and a button to contact an expert. The main heading is "Рассчитать свою стоимость" (Calculate your cost), with a subtext "Узнайте стоимость вашей конфигурации, задав параметры в калькуляторе" (Find out the cost of your configuration by setting parameters in the calculator). The configuration is titled "Конфигурация 1" and is set for the "Россия" region. It shows a single instance of Smart Web Security 1. The configuration details include: AntiDDoS and AntiBot (1,000,000 requests/month, free up to 10,000), WAF (1,000,000 requests/month, free up to 10,000), and RPS translation (0 requests). The total cost is 54,351.00 RUB per month. A note at the bottom states that the price of several services will change on May 1, 2026.

Smart Web Security 1	54 351,00 ₽
Smart Web Security 1	54 351,00 ₽
<b>Итого</b> в месяц	<b>54 351,00 ₽</b>

# **SolidWall AI Security Gateway**



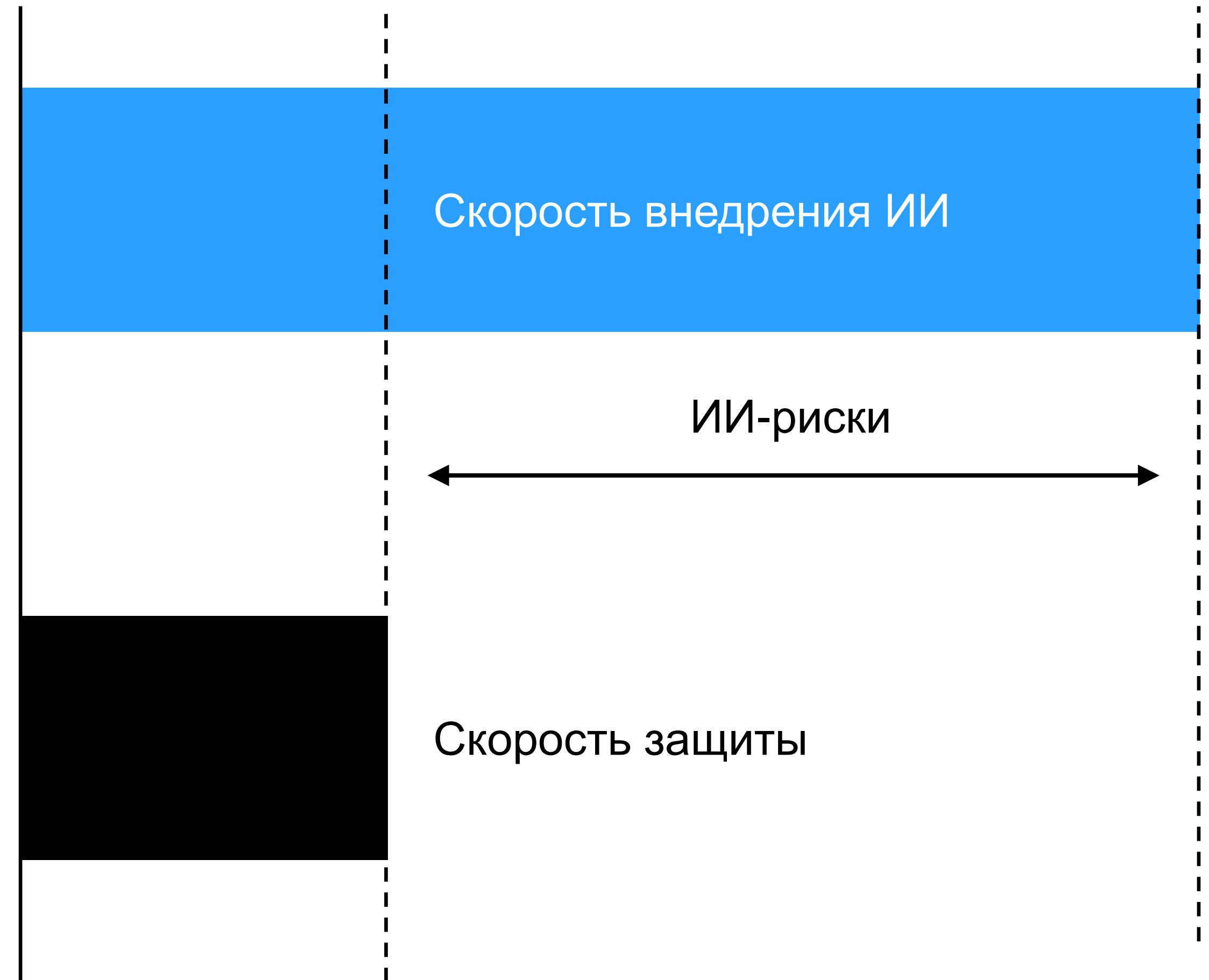
# Разрыв безопасности

**60% ИИ**

не имеют формализованной  
политики

**65% ИИ**

используют GenAI

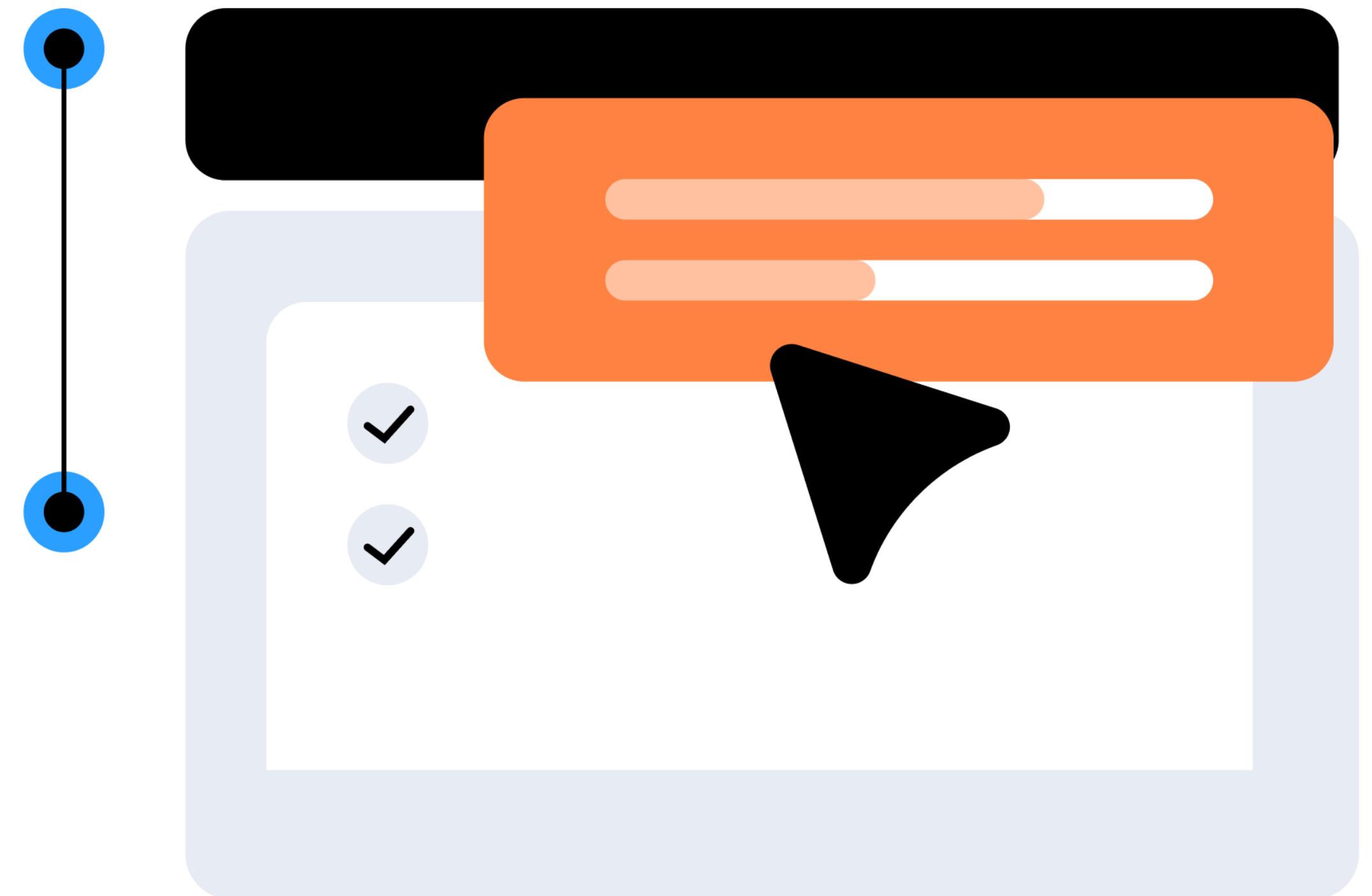


# Рекомендации по безопасной работе с ИИ-агентами

AI Secure Agentic Framework  
Essentials (AI-SAFE)

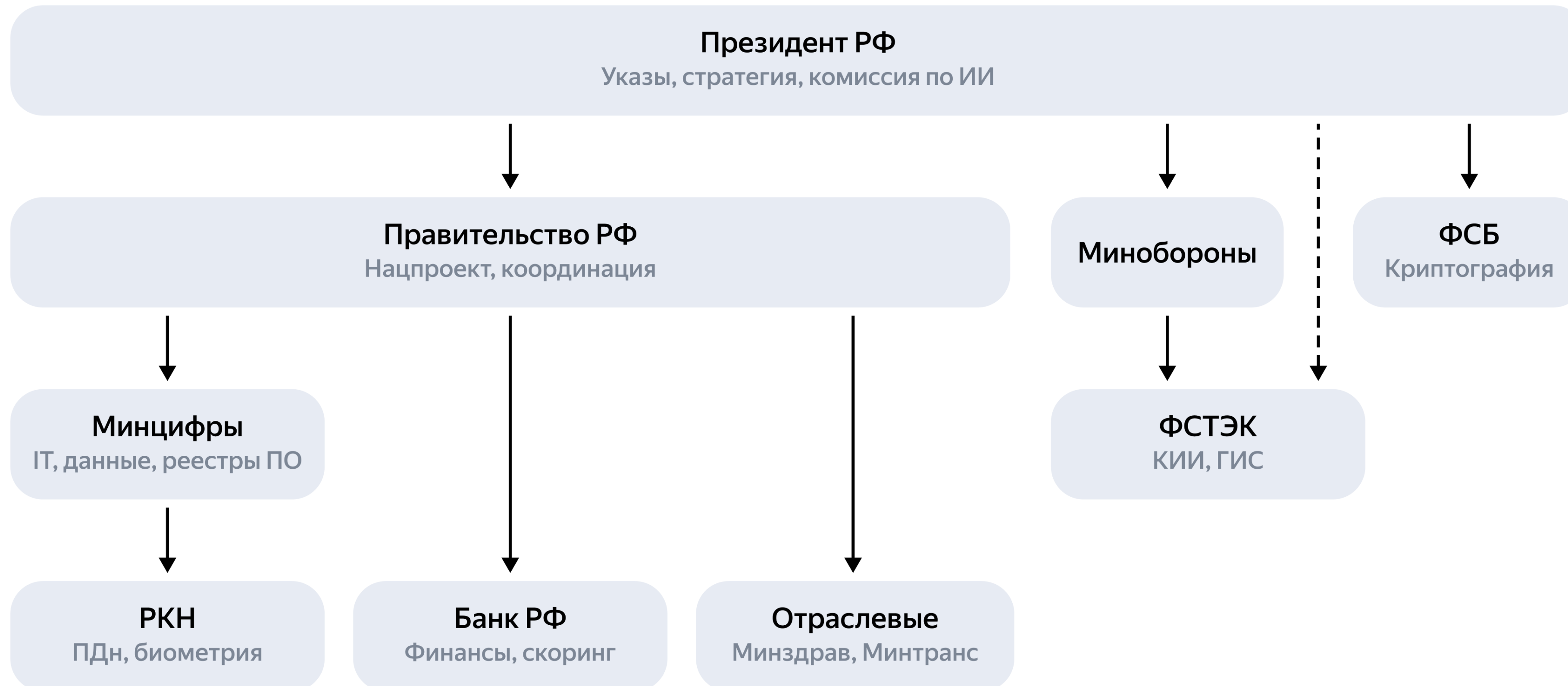


[yandex.cloud/ru/security/ai-safe](https://yandex.cloud/ru/security/ai-safe)



# Кто регулирует ИИ в России в 2026 году

С 26 февраля 2026 года действует Комиссия при Президенте РФ по вопросам развития технологий ИИ, координирующая взаимодействие федеральных органов власти, Банка России, регионов и иных участников



# Timeline-регулирования

2019

Указ № 490  
Стратегия

2020

258-ФЗ ЭПР  
Песочницы  
123-ФЗ: Москва  
258-ФЗ: общий ЭПР

2021

Кодекс  
этики ИИ  
Soft law

2024

Указ № 124  
Нацпроект  
«Экономика  
данных»

2025–2026

Приказ  
ФСТЭК № 117  
Ужесточение  
обязательных  
требований/  
ПДн, ГИС/КИИ,  
рост штрафов

2027

Рамочный  
закон  
Полноценный  
закон об ИИ

Soft law

Hard law

# AI Security Gateway

## 20+

типов атак, специфичных для ИИ-агентов и моделей, такие как:

инъекции промпта

обход бизнес-ограничений

избыточные привилегии агентов

чрезмерное потребление ресурсов

The screenshot displays the SolidWall AI Security Gateway interface. At the top, it shows the logo and statistics: "Всего приложений: 1" and "Активных правил: 56".

**Приложения (Applications):**

- Фильтр (Filter)
- Все (All): 62
- Общие (General): 62
- SolidSmart Bank

**Категории атак (Attack Categories):**

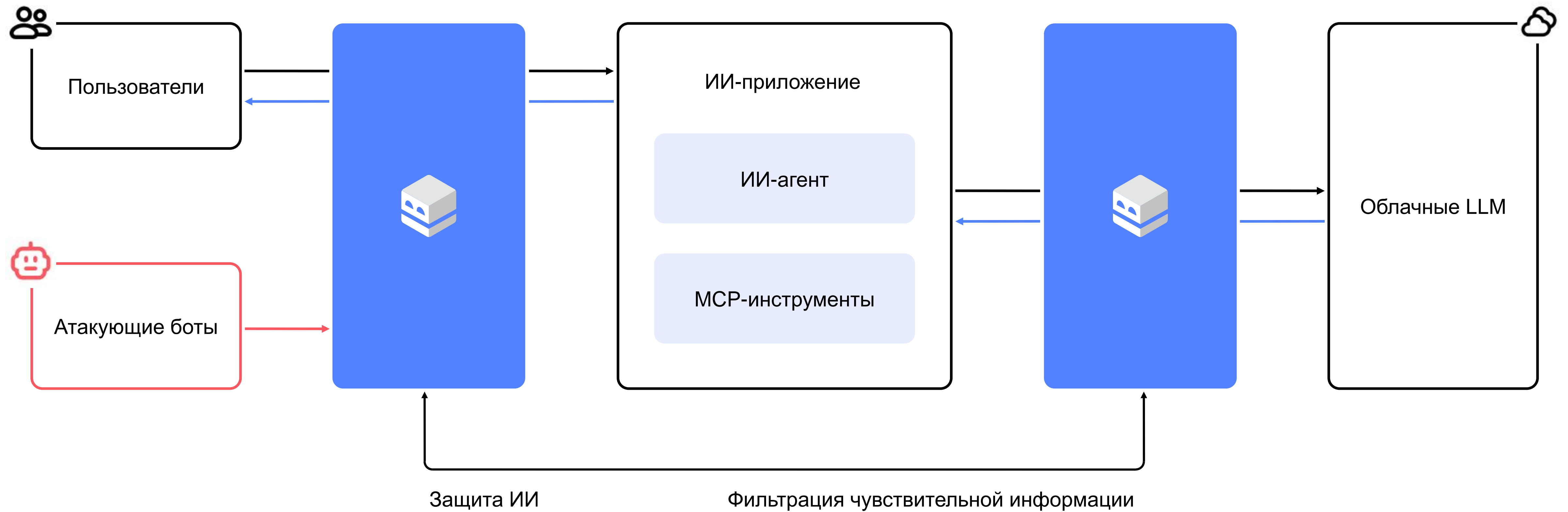
- протокол: 14
- сигнатура: 31
- управление данн...: 1
- черный список: 3
- финансы: 1
- синтаксис: 24
- инъекция: 6
- бизнес-логика: 4
- стандарт: 62
- модель приложе...: 13
- утечка данных: 7
- юридический: 1
- AI: 13
- мошенничество: 1
- модерация конте...: 1
- соответствие тр...: 6
- здравоохранение: 1
- корреляция: 1
- сессия: 7
- пользователи: 1
- анализ ответов: 10

**Выбраны теги (Selected Tags):** AI, соответствие требованиям, модерация к...

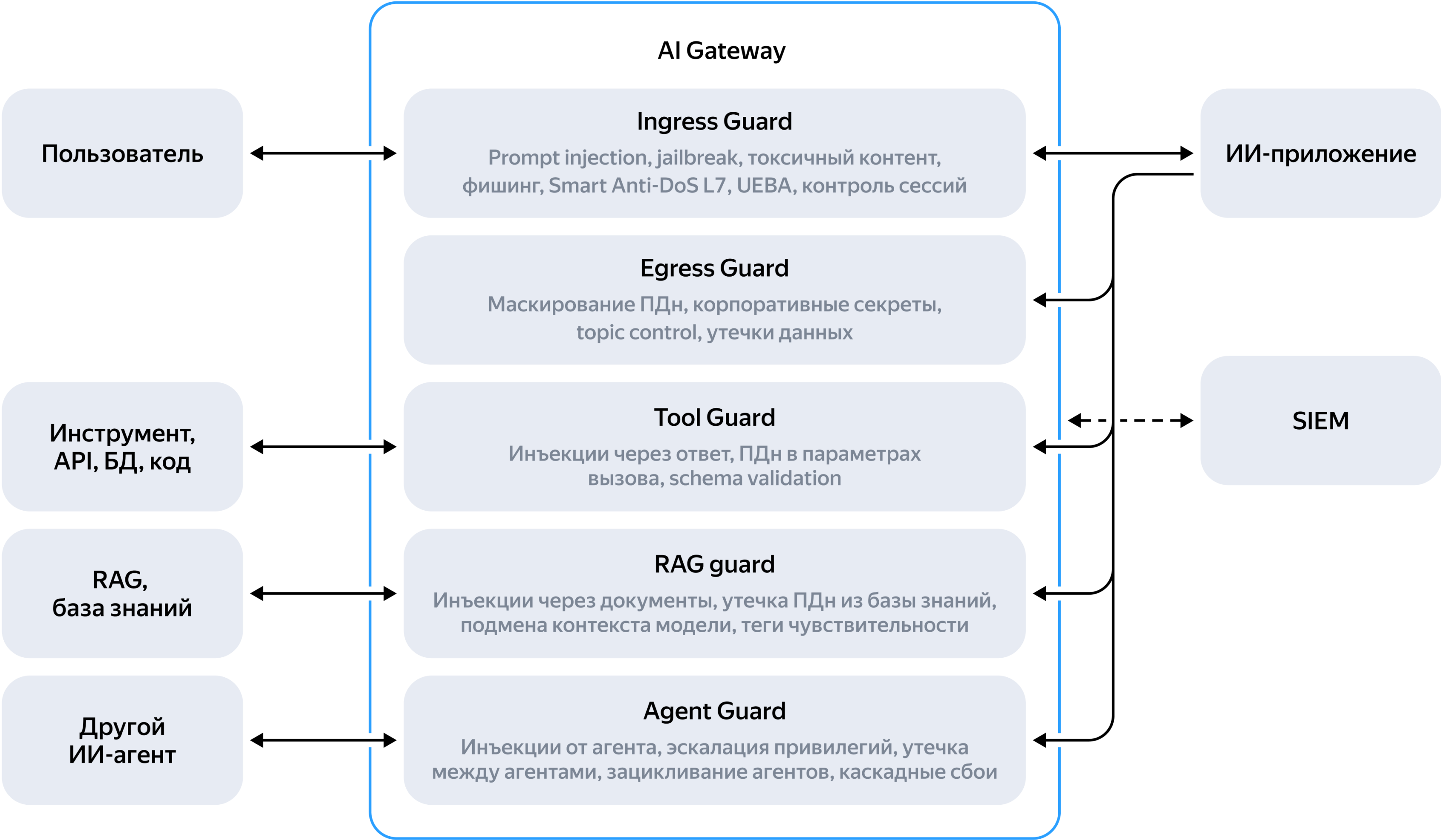
**Выбор правил (Rule Selection):**

- Выберите правила (Select rules) | Отметить все (Mark all)
- AI, соответствие требованиям, здравоохранение
- Нарушение медицинского регулирования (LLM)
- AI, мошенничество
- Подозрение на финансовое мошенничество (LLM)
- AI, модерация контента
- Запрещённый или оскорбительный контент (LLM)
- AI, соответствие требованиям
- Нарушение внутренней политики компании (LLM)
- Нарушение финансовых нормативов (LLM)
- Нарушение юридических требований (LLM)
- Нарушение политики ИТ-безопасности (LLM)

# Архитектура решения



# Как работает SolidWall AI Security Gateway



# Функции AI Gateway

## Filtering

Injection detect,  
jailbreak detect

## PII masking

Маскирование PII  
перед отправкой

## Цепочки действий

Обнаружение  
многоступенчатых атак

## Rate limiting

По запросам,  
по времени ответа

## Умный DoS (DoW)

Контроль ресурсоёмкости  
запросов к LLM

## Адаптивные фейковые ответы

Затрудняют автоматизацию  
атак через LLM

## Logging

Полная трассировка

## Отказоустойчивость

Active/active-  
и active/passive-кластеры,  
режим bypass

## Стандарты и соответствие

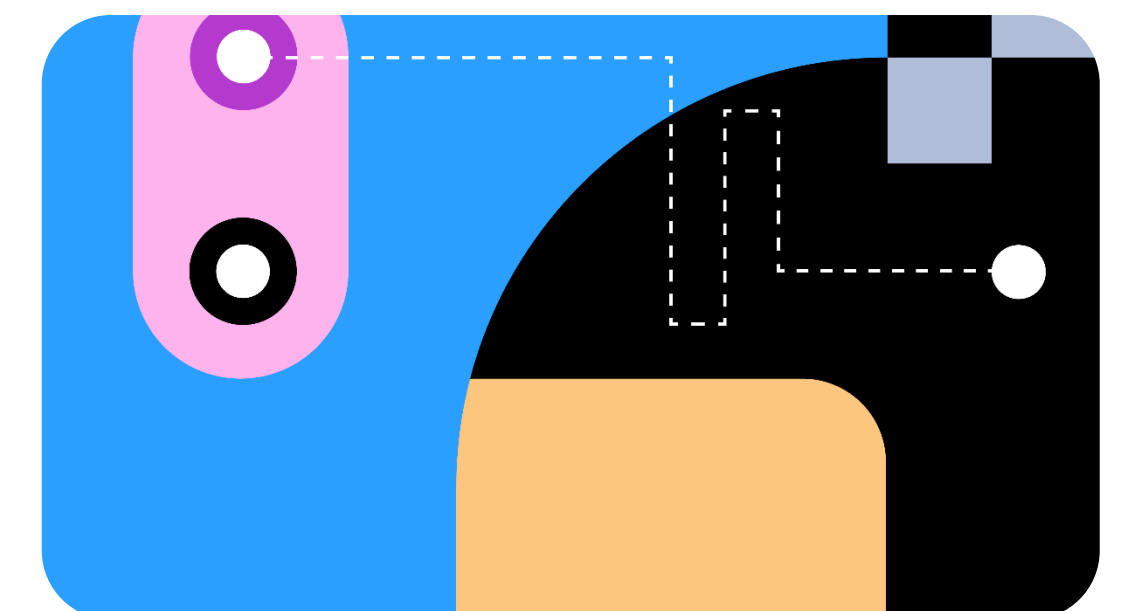
OWASP® Top 1,  
Yandex AI-SAFE

## Интеграции

SIEM/SOAR, Zabbix,  
Prometheus®

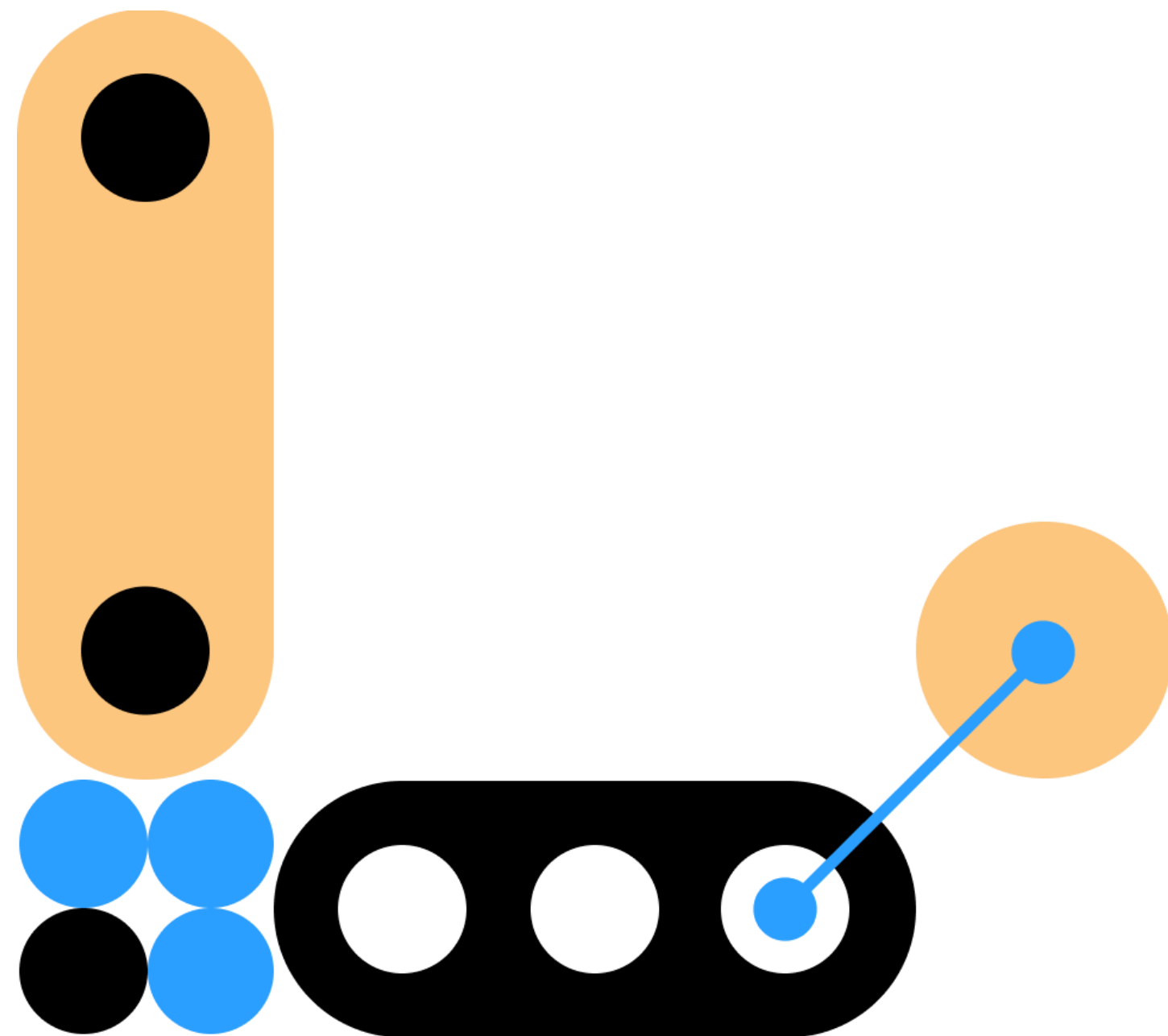
## Интерпретируемость

Гранулярные классы,  
интерпретируемые  
модели



# Итог

Зачем это нужно  
именно сейчас



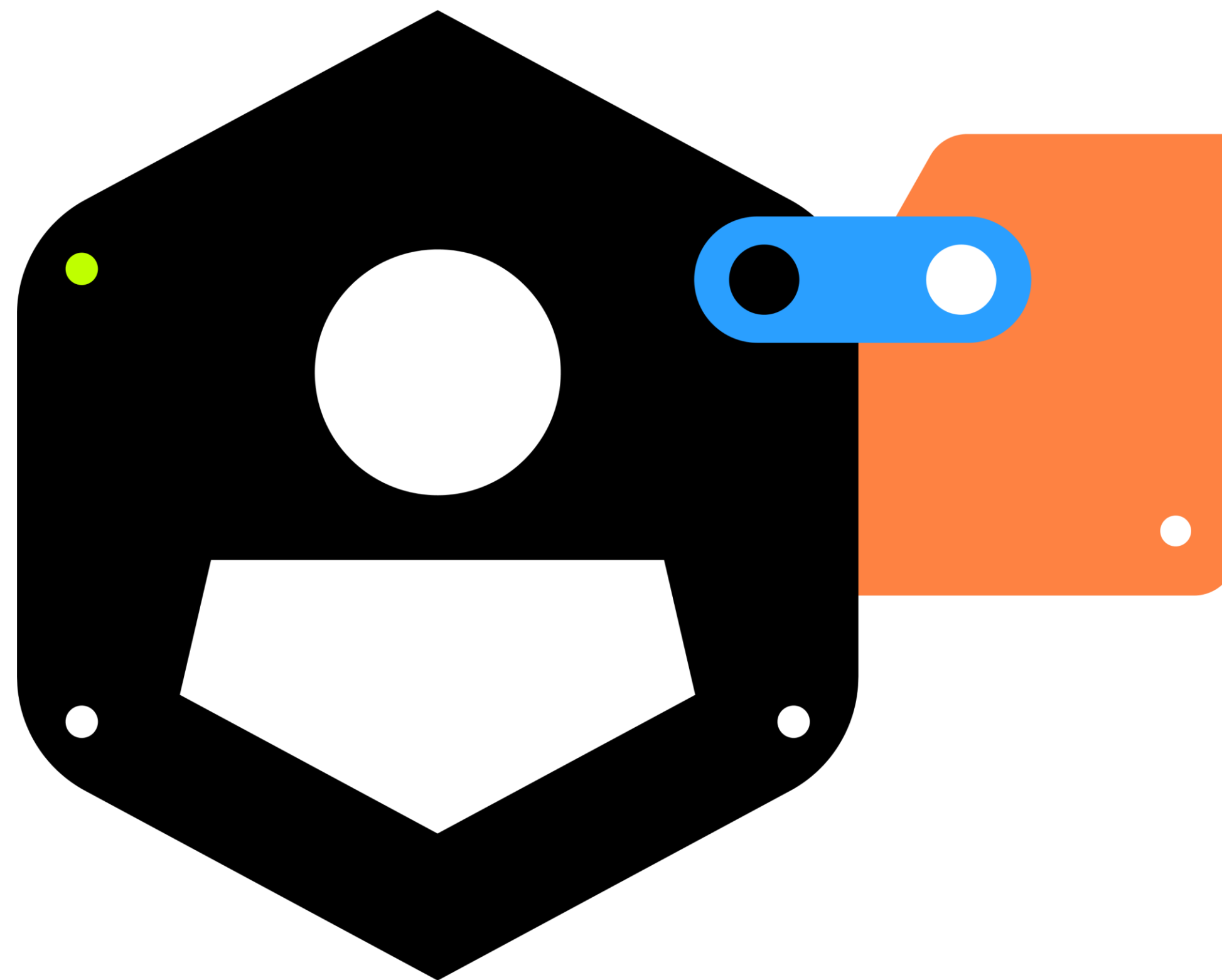
Каждый корпоративный чат-бот,  
RAG-система или ИИ-агент —  
это новая поверхность атаки

Регуляторы начинают требовать  
контроль ИИ (Yandex Cloud AI  
SAFE, OWASP<sup>®</sup>, NIST AI RMF)

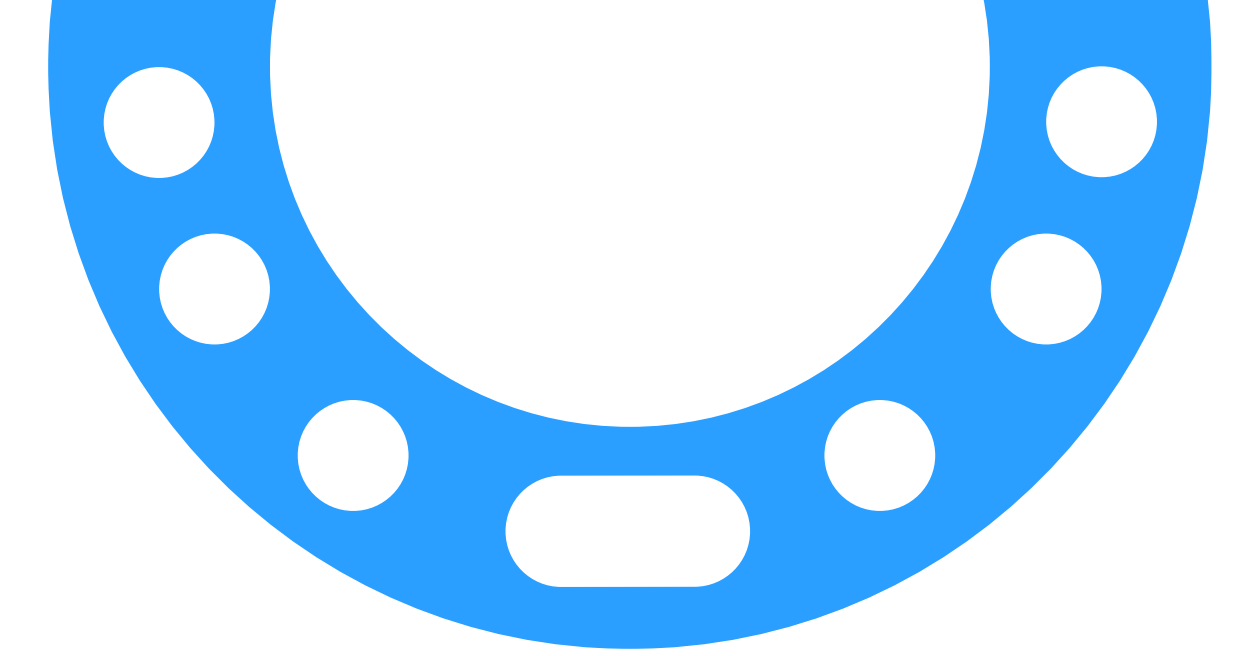
SolidWall AI Security Gateway  
закрывает разрыв между  
скоростью внедрения  
ИИ и зрелостью его защиты

# Yandex Identity Hub

IdP-сервис на базе SaaS-модели  
для централизованного управления  
пользователями и единого входа (SSO)  
в бизнес-приложения со встроенной MFA



# Аутентификация под прицелом атакующих



# 55%

атак на облачные и гибридные инфраструктуры в 2025 году связаны с компрометацией и манипуляцией учётными записями

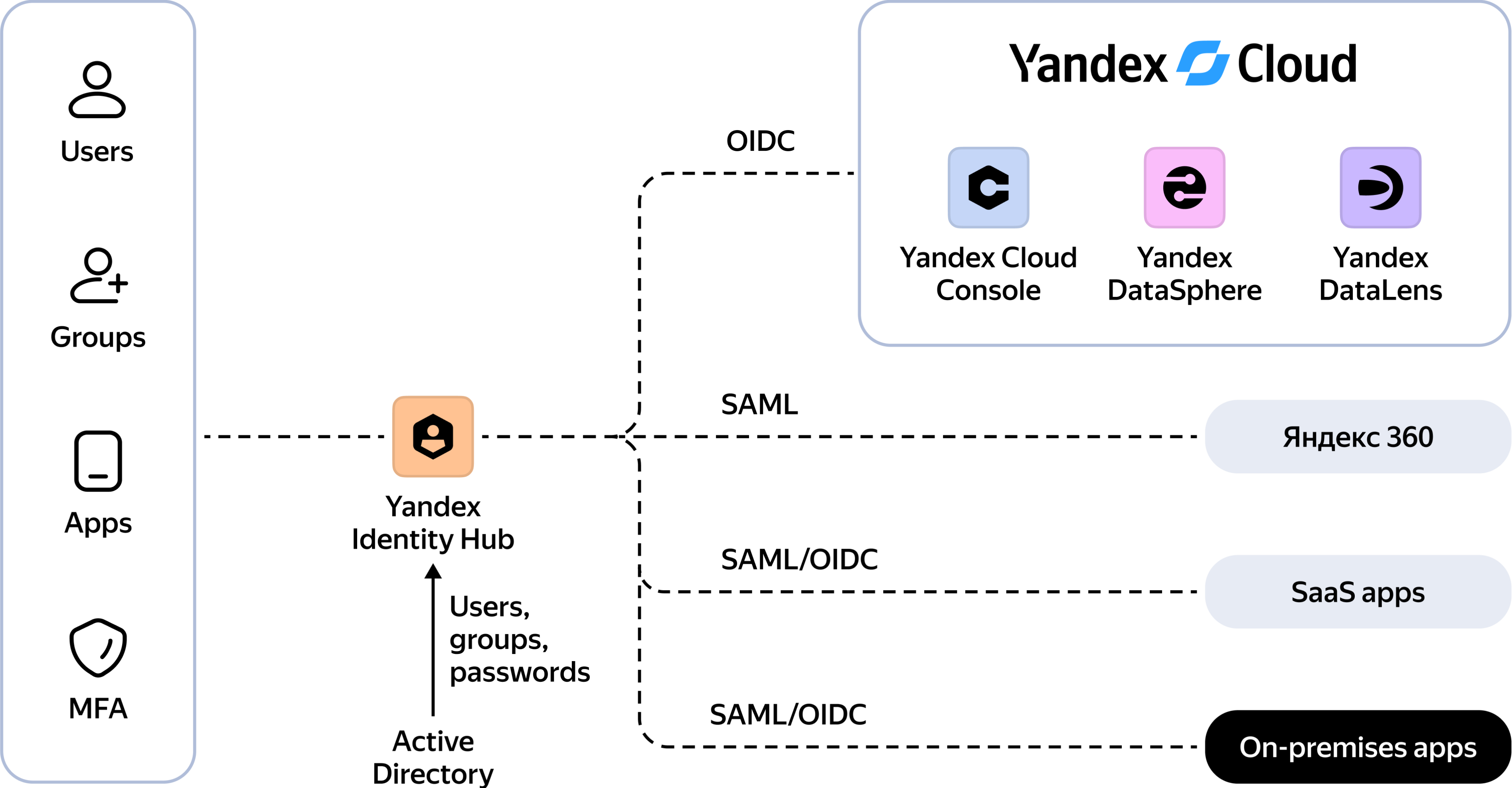
«Анализ киберугроз в облачных и гибридных инфраструктурах за второе полугодие 2025»,  
Yandex Cloud

# 77%

утечек данных связаны с использованием скомпрометированных или слабых учётных данных (Credentials)

Verizon's Data Breach Investigations Report (2024)

# Архитектура сервиса



# Возможности

## Хранение учётных данных пользователей

Управление пользователями и их атрибутами

Пулы пользователей / tip-userpool

Обзор Пользователи

Поиск по имени, идентификатору или электронной почте

Все домены Все статусы

Пользователь	Имя пользователя	Статус	Идентификатор	
	roman.korovin	Active	roman.korovin@tip-userpool	...
	anna.petrova	Active	anna.petrova@tip-userpool	...
	ivan.sidorov	Inactive	ivan.sidorov@tip-userpool	...
	maria.kuznetsova	Active	maria.kuznetsova@tip-userpool	...



### Пользователи / Roman Korovin

Active

Обзор Группы Профили OS Login SSH-ключи

Имя пользователя ..... roman.korovin

Электронная почта ..... roman.korovin@tip-userpool

Пул пользователей ..... tip-userpool

Дата создания ..... 30.06.2025, 18:11

Дата последней аутентификации ..... —

#### Персональная информация

Имя ..... Roman

Фамилия ..... Korovin

Номер телефона ..... +7 916 123 4567

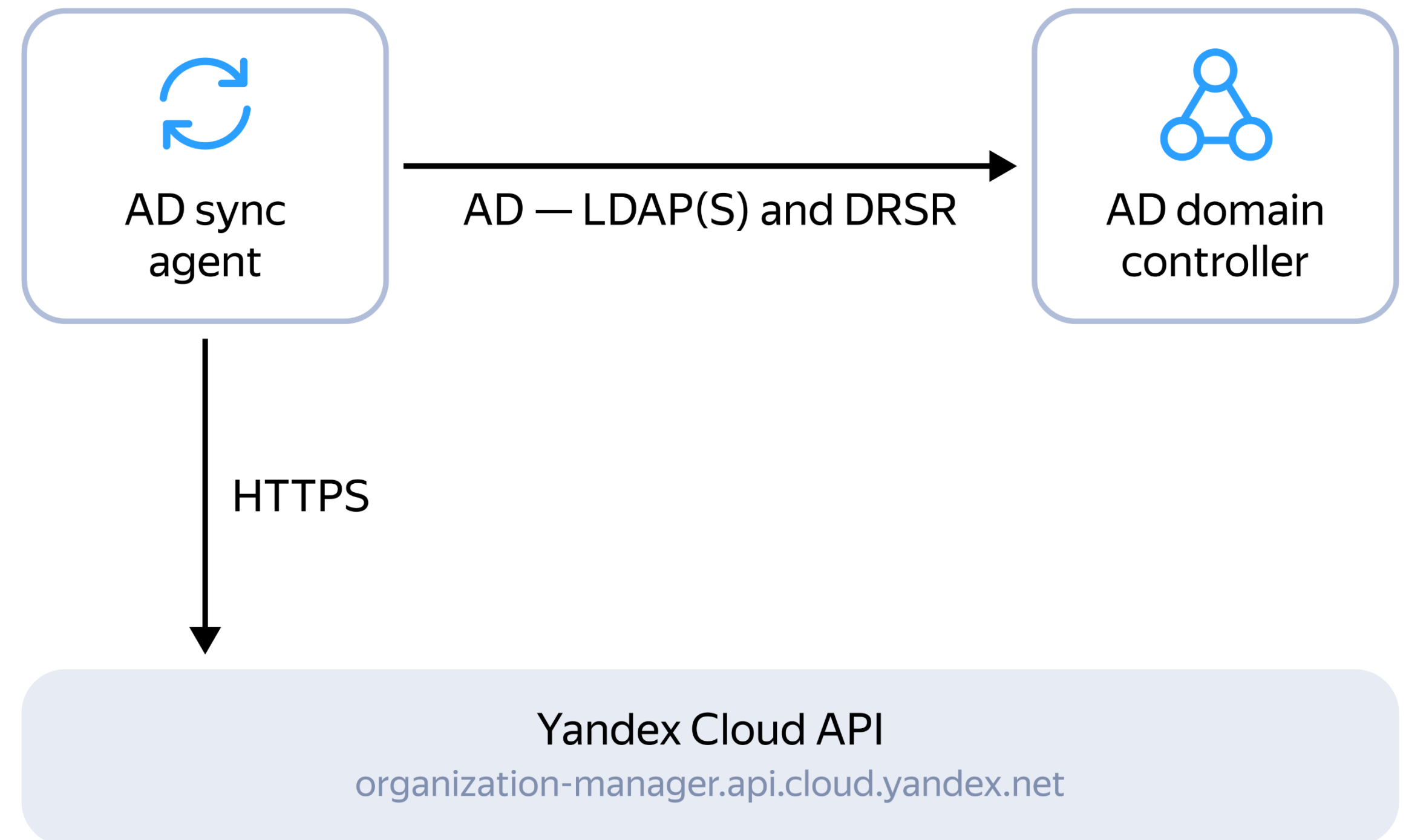
#### Права доступа пользователя

Запустите диагностику доступа, чтобы показать права пользователя на доступ к ресурсам Yandex Cloud.

Диагностика доступа

# Синхронизация с Active Directory

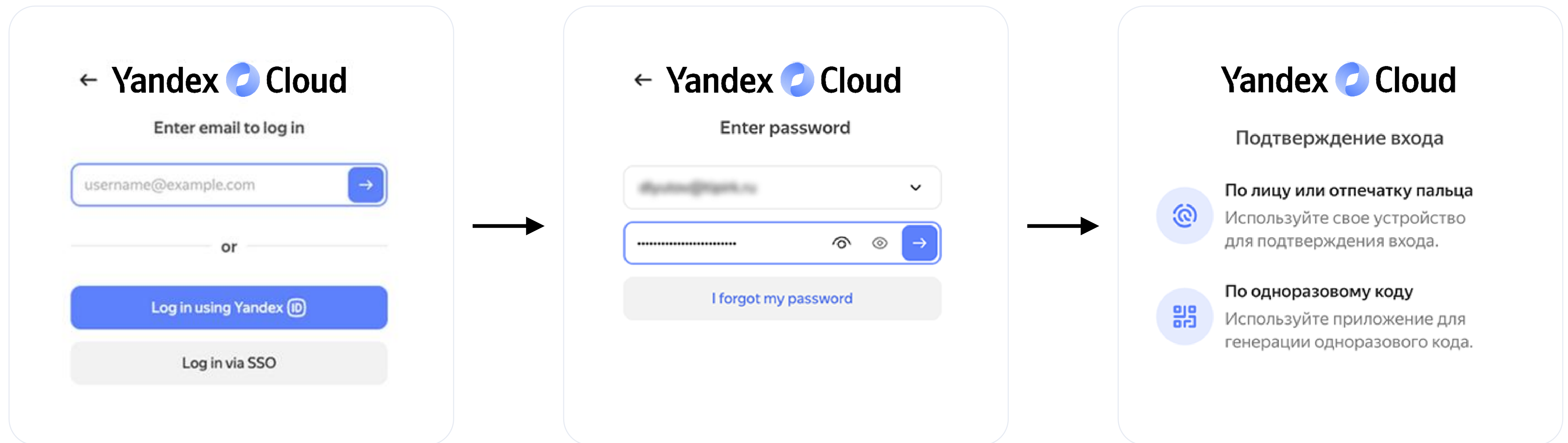
- Синхронизация пользователей и их атрибутов
- Синхронизация групп и членства пользователей в них
- Единый пароль с Active Directory  
Password hash synchronization
- Настройка области и периодичности синхронизации



# Возможности

## Аутентификация

Проверка личности пользователя с помощью связки «логин — пароль», двухфакторной аутентификации, TOTP, WebAuthn/FIDO2



# Возможности

## Интеграция с сервисами

Единый вход (Single sign-on) в корпоративные приложения без повторного ввода пароля по протоколам SAML и OpenID Connect

Тесная интеграция с облачными и другими сервисами экосистемы: Яндекс 360 и Яндекс Браузер для организаций

Приложения / zabbix-saml

Обзор Атрибуты Пользователи и группы

Имя \_\_\_\_\_

Описание \_\_\_\_\_

Статус \_\_\_\_\_ Active

Дата создания \_\_\_\_\_ 19.06.2025, 09:30

Конфигурация поставщика удостоверений (IdP)

Issuer / IdP EntityID \_\_\_\_\_

Login URL \_\_\_\_\_

Logout URL \_\_\_\_\_

Metadata URL \_\_\_\_\_

Скачать файл с метаданными

Конфигурация поставщика услуг (SP)

Метод единого входа \_\_\_\_\_ SAML

SP EntityID \_\_\_\_\_ https://zb.tipirk.ru/

ACS URL \_\_\_\_\_ https://zb.tipirk.ru/index\_sso.php?acs

Режим подписи \_\_\_\_\_ Assertion

Сертификат приложения

Добавьте сертификат в настройках приложения на стороне поставщика услуг.

Цифровой отпечаток (fingerprint) \_\_\_\_\_ 1E946ADA626923FB49483FCFF747F65D0B75D5B1

Срок действия сертификата \_\_\_\_\_ 18.06.2030, 09:30

Скачать сертификат Управление сертификатами

Приложения / test-datalens-application

Обзор Пользователи и группы

Имя \_\_\_\_\_ test-datalens-application

Описание \_\_\_\_\_

Каталог \_\_\_\_\_ test - tip-cloud

Статус \_\_\_\_\_ Active

Дата создания \_\_\_\_\_ 24.04.2025, 09:22

Конфигурация поставщика удостоверений (IdP)

ClientID \_\_\_\_\_ aje8tksjgm2mr1me3jq5

OpenID Configuration \_\_\_\_\_ https://auth.yandex.cloud/.well-known/openid-configuration

Дополнительные атрибуты

Конфигурация поставщика услуг (SP)

Метод единого входа \_\_\_\_\_ OIDC

Redirect URI \_\_\_\_\_ https://dl.tipirk.ru/auth/callback/oidc

Scopes

Атрибуты пользователей \_\_\_\_\_ email groups openid profile

Секреты приложения

Добавьте секрет в настройках приложения на стороне поставщика услуг.

Дата создания	Описание	Данные секрета
30.06.2025, 09:24	datalens	

Добавить секрет

# Возможности

## Аудит пользовательской активности

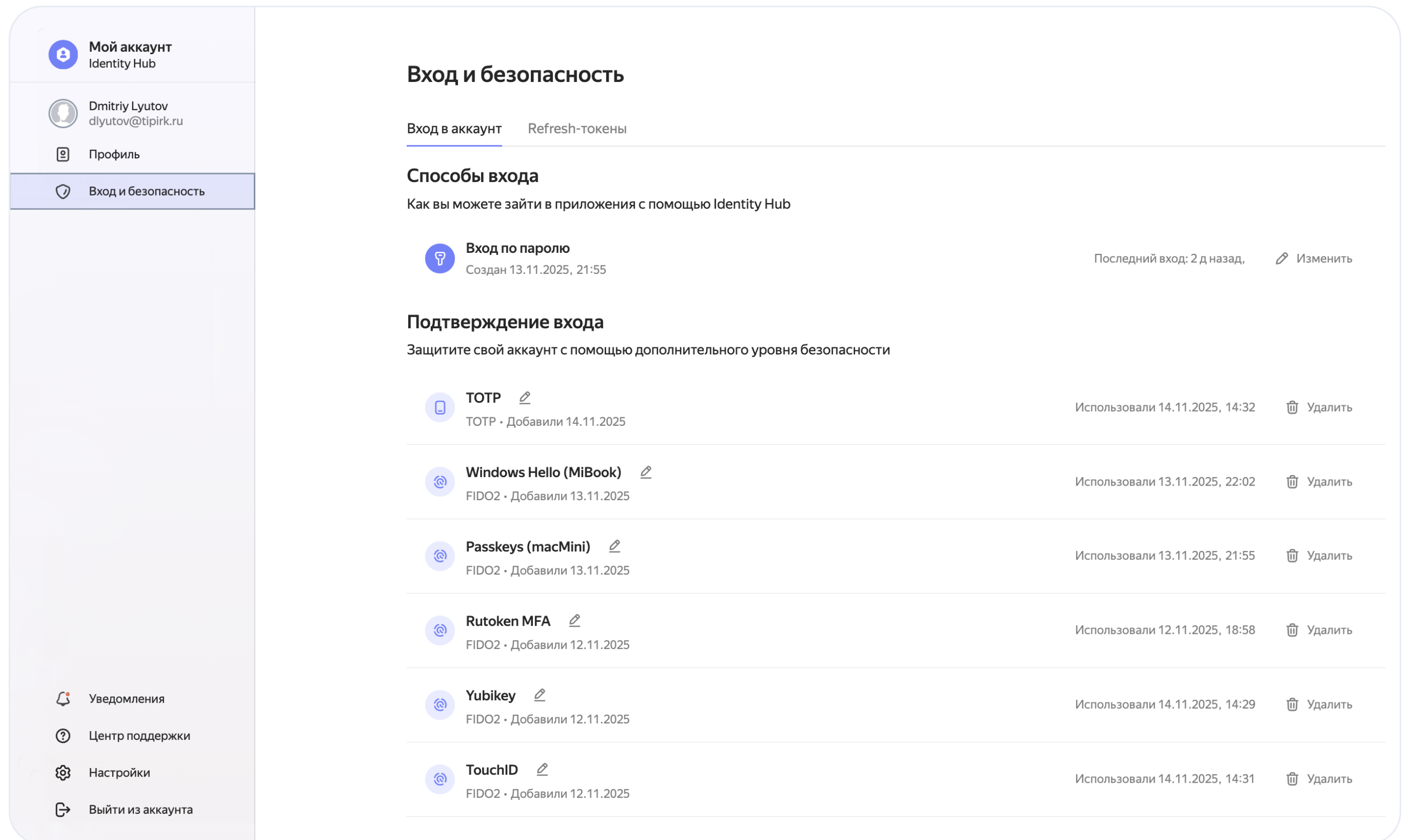
Широкие возможности  
по аудиту аутентификации  
пользователей в UI и поставка  
событий в SIEM-системы

The screenshot shows the 'Пользователи / Дмитрий Егоров' (Users / Dmitry Egorov) page in the Cloud Center interface. The user is active. The 'Аудитный лог' (Audit log) tab is selected, showing a list of operations performed by the user and other users. The log includes columns for Status, Date, Operation, User, IP Address, and Identifier. The operations listed include 'Update user info', 'Add MFA factor', 'Add SSH key', 'Delete SSH key', 'Create OS Login profile', 'Reset password (by admin)', and 'Create user'. The status of each operation is indicated by a green 'Успешно' (Successful) or a red 'Неуспешно' (Unsuccessful) label.

Статус	Дата	Операция	Пользователь	Адрес IP	Идентификатор
Успешно	05.10.2024, 13:40:04	Update user info	michael.mike@example.com	116.72.144.185	c8r87145pp94k1rvg88a
Успешно	05.10.2024, 22:52:38	Add MFA factor	willa.jennings@example.com	58.77.159.25	dg5883p48ms1rr12364k
Успешно	05.10.2024, 13:40:04	Add SSH key	jessica.hanson@example.com	221.122.108.252	c8r99u2vc4661j4p4815
Успешно	05.10.2024, 13:40:04	Delete SSH key	nathan.roberts@example.com	46.31.79.186	c8rv71rj4f8u37u1x12b
Успешно	05.10.2024, 13:40:04	Add SSH key	michelle.harris@example.com	156.219.185.228	a71811x2183q1p1538p1
Успешно	05.10.2024, 13:40:04	Create OS Login profile	george.young@example.com	85.96.141.157	c8r8u1jvpxm2nd38u1f
Успешно	05.10.2024, 13:40:04	Reset password (by admin)	heather.simmons@example.com	103.163.220.183	c8rj6v381362vnd4p1s
Неуспешно	05.10.2024, 13:40:04	Reset password (by admin)	curtis.walker@example.com	36.79.219.86	c8rLah8qpt1vb1ar18d
Успешно	05.10.2024, 13:40:04	Update user info	felicia.west@example.com	34.75.155.72	c8r85ubj466v714r1xg1
Успешно	03.07.2024, 10:47:10	Create user	bill.sanders@example.com	2a02:6b8:b081:7326::1:3b	c8r3apq6vc48v1jxh48

# Портал Мой аккаунт

- Персональное пространство пользователя
- Просмотр и редактирование собственных атрибутов
- Самостоятельная смена пароля
- Управление собственными MFA-факторами
- Просмотр своих групп **Soon**
- Просмотр событий аудита и входа **Soon**



# Брендинг

Страницы аутентификации и ошибок, приложения, подсказки в строке авторизации и приветствие можно оформлять в соответствии с корпоративными брендбуками

**Брендинг** PREVIEW

**Цвета и изображения**  
Настройте внешний вид страниц аутентификации в разных темах для соответствия вашему фирменному стилю.

Светлая тема  Тёмная тема

**Фоновое изображение**  
До 3840×2160 px  
До 4 МБ

**Логотип**  
от 1920×1920 px  
До 512 КБ

**Фавиконка**  
До 512×512 px  
До 512 КБ

**Основной цвет**  
 #47abe5

**Форма входа**  
Настройте форму под ваши сценарии аутентификации

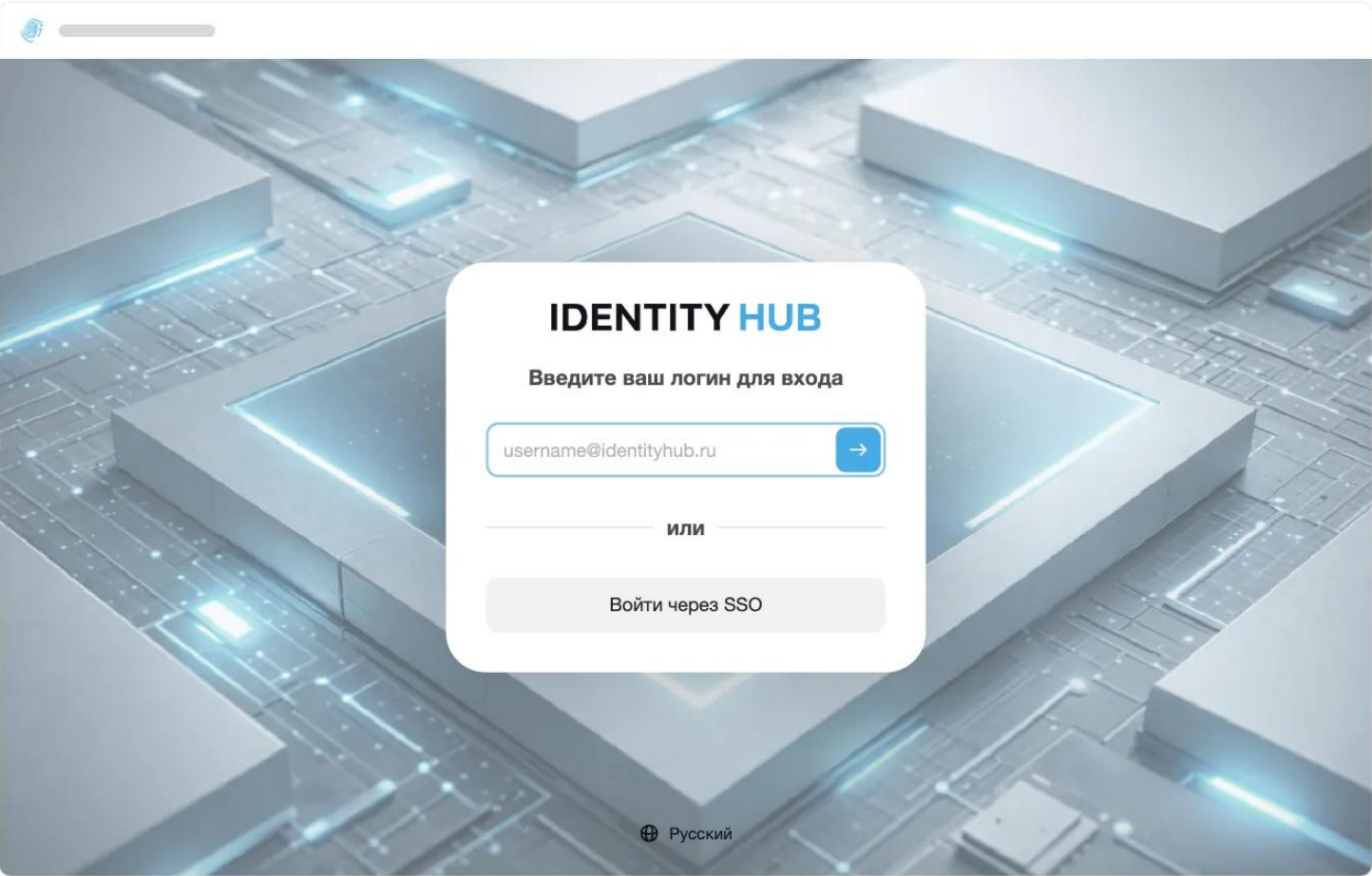
**Приветствие**  
Введите ваш логин для входа

**Подсказка в поле для входа**  
username@identityhub.ru

**Альтернативные способы входа**

Яндекс ID ⓘ  
 Single-Sign On ⓘ

**Предварительный просмотр**



Введите ваш логин для входа

username@identityhub.ru

или

Войти через SSO

Русский

# Как рассчитывается стоимость

Количество пользователей	Стоимость за пользователя в месяц, вкл. НДС, руб.
--------------------------	---

< 15	Не тарифицируется
------	-------------------

16–100	530
--------	-----

101–500	490
---------	-----

501–1000	440
----------	-----

1001–3000	350
-----------	-----

3001–5000	270
-----------	-----

5001–10 000	210
-------------	-----

> 10 000	180
----------	-----

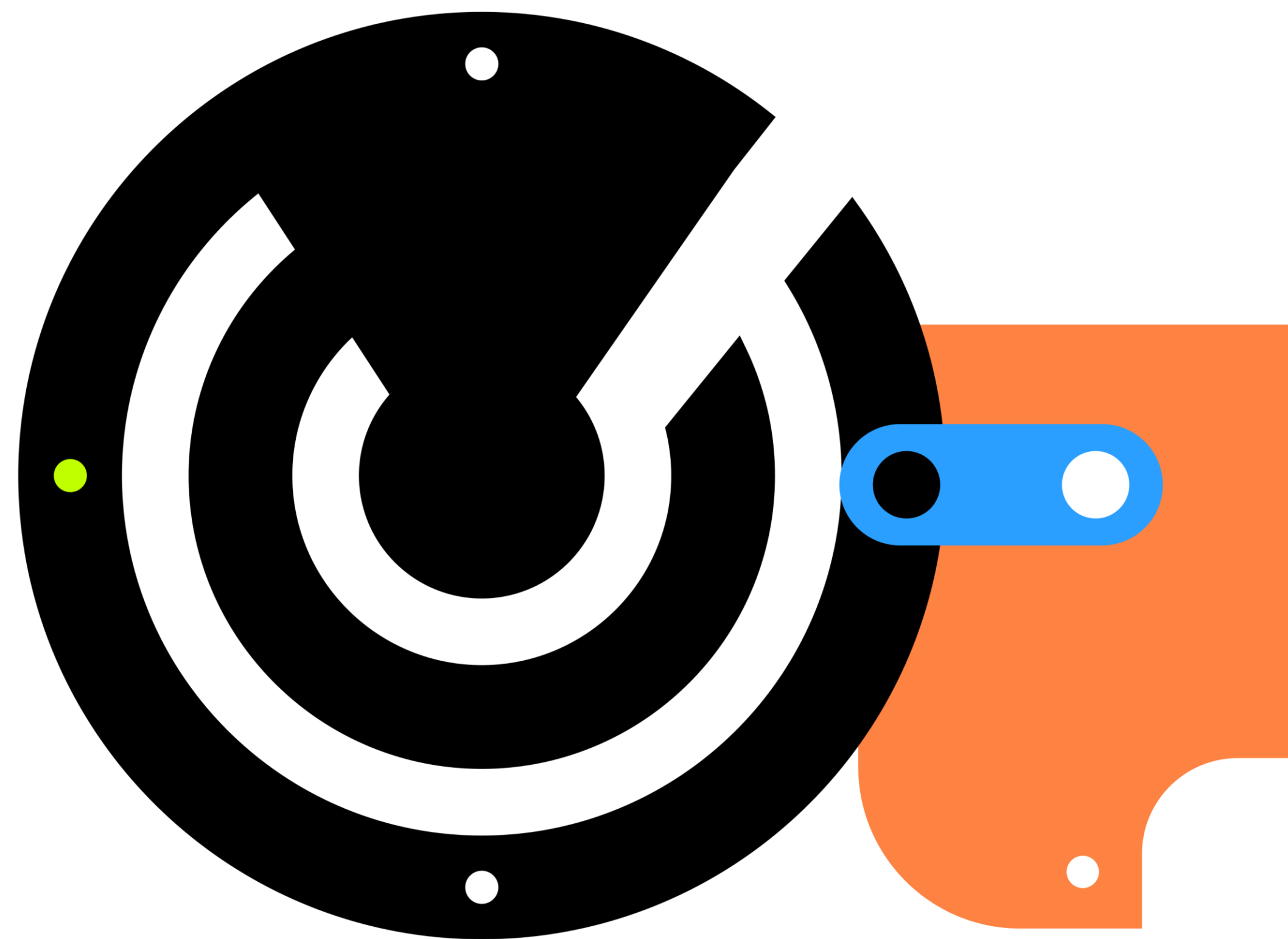
Стоимость использования сервиса Yandex Identity Hub входит в стоимость оплачиваемых сервисов

Дополнительно тарифицируется только подключение к сторонним приложениям

Цена рассчитывается исходя из количества пользователей в месяц

# YCDR

Yandex Cloud Detection and Response –  
управляемый сервис по сбору событий,  
проактивному мониторингу и реагированию  
на инциденты (SOCaaS)



# Yandex Cloud Detection and Response

Сбор и анализ событий из внешних сервисов и кастомных источников

Выявление ошибок конфигураций и подозрительной активности с их последующим устранением

Реагирование на потенциальные угрозы и инциденты для обеспечения непрерывной защиты

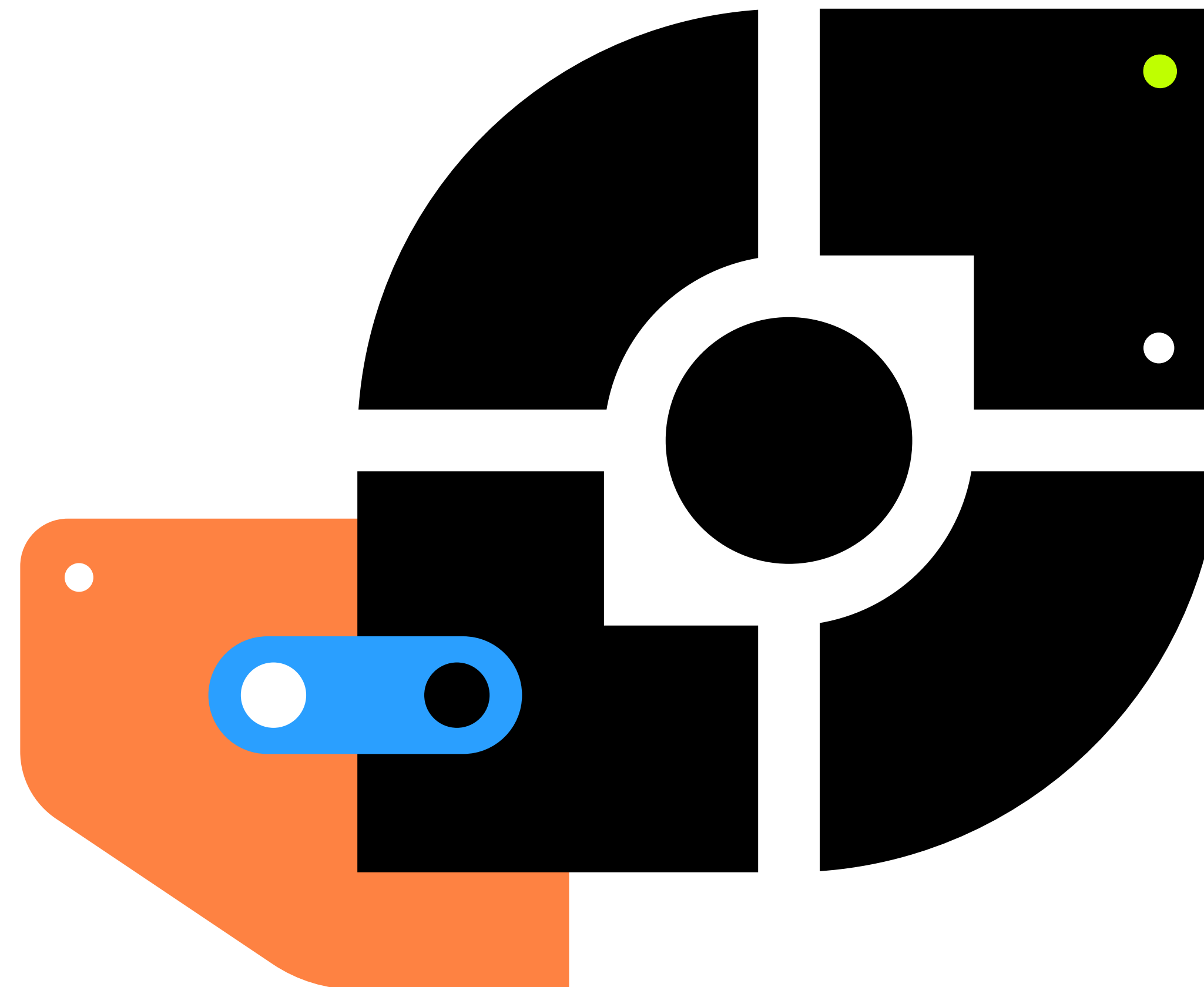
# Ценообразование

Опция	Cloud	Hybrid
Анализ поступающих событий ИБ в круглосуточном режиме 7 дней в неделю	✓	✓
Первичная обработка инцидентов ИБ, проверка ложного срабатывания, регистрацию и последующее сопровождение инцидентов ИБ	✓	✓
Адаптация правил корреляции	✗	✓ 4 в мес.
Добавление исключений в правила корреляции	✓	✓
Количество расследований DFIR (расследование инцидента с отчётом)	✗	✓
Стандартный — до 10 затронутых облачных ресурсов		1 стандартный инцидент
Сложный — от 10 до 30 затронутых ресурсов		

Объём, EPS	Ед. изм.	Платёж до скидки, с НДС
100	руб./мес	26 800
200	руб./мес	53 600
300	руб./мес	80 400
400	руб./мес	107 200
500	руб./мес	134 000
600	руб./мес	160 800
700	руб./мес	187 600
800	руб./мес	214 400
900	руб./мес	241 200
1 000	руб./мес	268 000
2 000	руб./мес	536 000
3 000	руб./мес	804 000
4 000	руб./мес	1 072 000
5 000	руб./мес	1 340 000

# Yandex SIEM

Собственная SIEM-система на базе технологий Яндекс



# Рынок SIEM

Зрелый рынок,  
но проблемы не исчезли

Ограничивают сбор логов  
из-за стоимости  
и инфраструктуры

56%

Хранят логи  
менее 6 месяцев

53%

Рост объёма событий —  
основной фактор нагрузки

37%

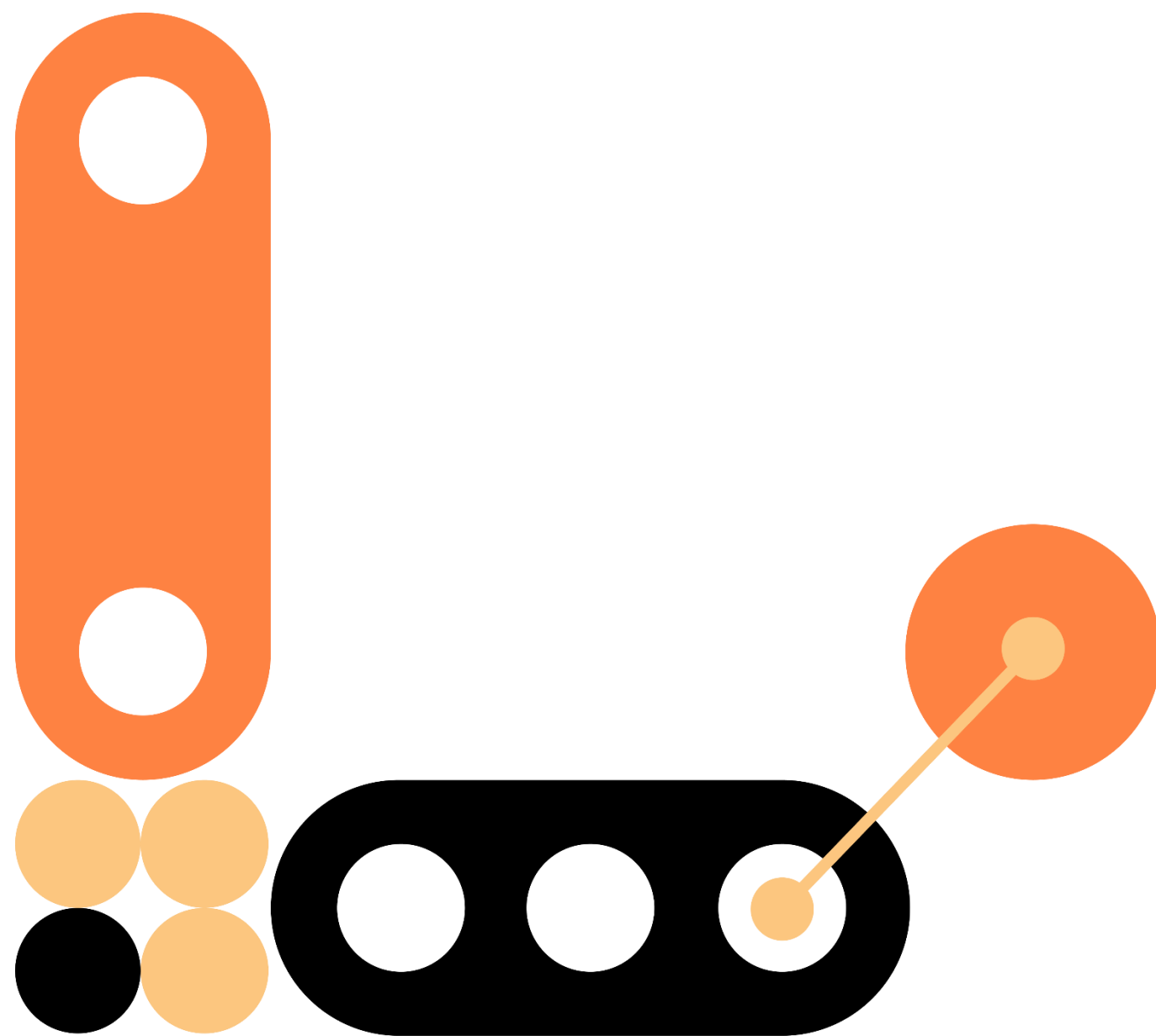
Высокая стоимость  
владения SIEM

29%

Необходимость постоянного  
масштабирования инфраструктуры

27%

# Что даёт Yandex SIEM



## Полноценная SaaS-SIEM-система без необходимости управлять собственной инфраструктурой

- **Полная видимость вашего контура.**  
Собирает и нормализует события из всех источников в единую модель, обеспечивая централизованный мониторинг и анализ.
- **Обнаружение угроз в реальном времени**  
Выявляет атаки за счёт потоковой корреляции, готовых сценариев и гибких правил детектирования.
- **Масштабируемость и устойчивость**  
Обработывает миллионы событий в секунду благодаря cloud-native архитектуре и технологиям Яндекс по обработке больших данных.
- **Снижение нагрузки на SOC и интеграция в экосистему сервисов безопасности**  
Автоматизирует рутину, обогащает алерты и интегрируется с сервисами YCDR, Security Deck и его модулями.

# Ключевые преимущества

## Быстрый запуск

Внедрение за несколько дней  
без проектирования инфраструктуры

## Без эксплуатации инфраструктуры

Нет необходимости управлять железом  
и разворачивать инфраструктуру

## Масштабируемость под реальные нагрузки

Обработка миллионов  
событий и стабильная работа  
в высоконагруженных сценариях

## Прозрачная экономика

Подписка без капитальных затрат  
и скрытых расходов

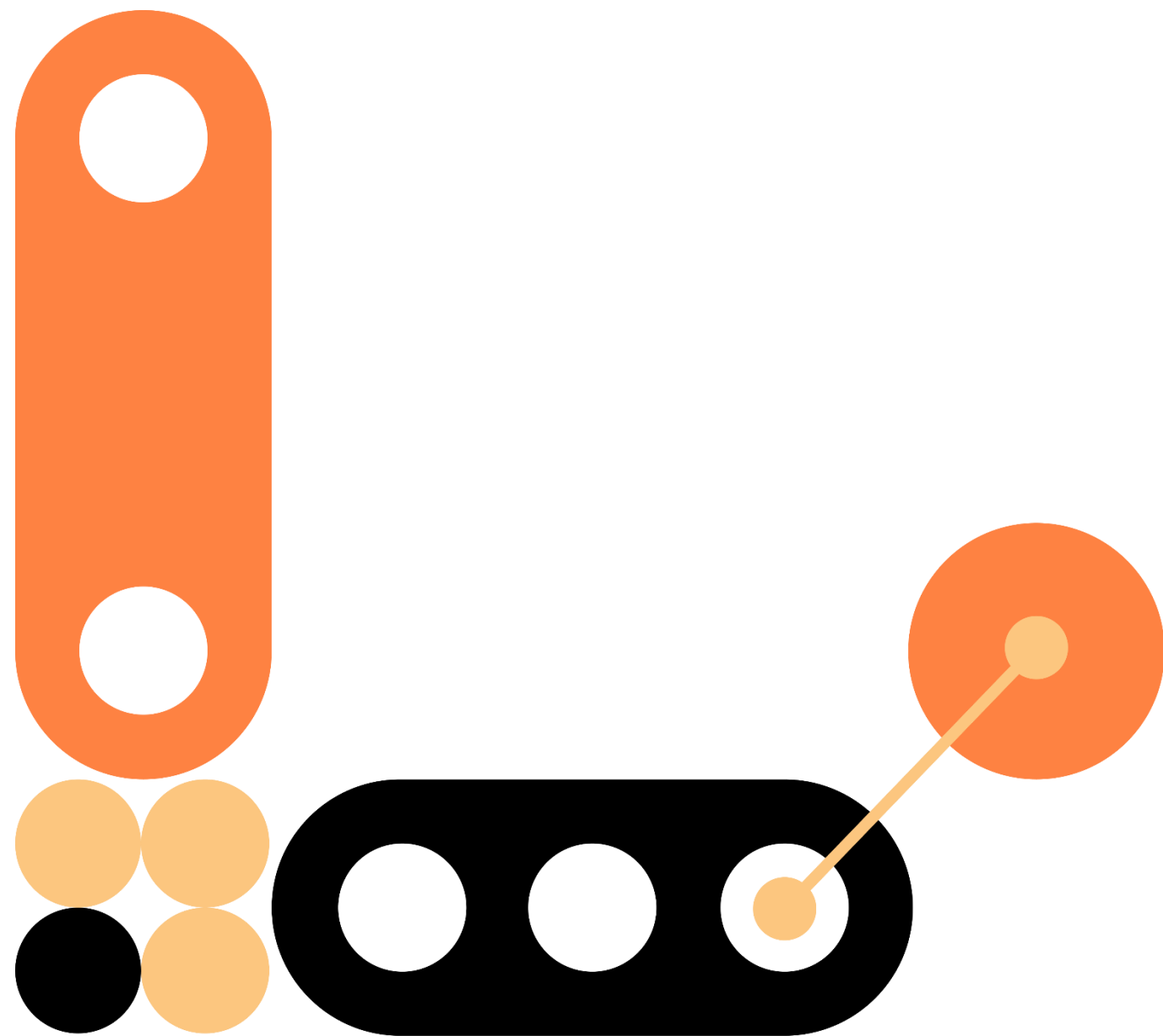
# Тарификация

Принципы тарификации и калькулятор

## Подписочная модель

Тариф на 500 EPS	448 350 руб. без НДС/мес.
Тариф на 1000 EPS	541 800 руб. без НДС/мес.
Тариф на 2000 EPS	728 700 руб. без НДС/мес.
Тариф на 3500 EPS	1 009 050 руб. без НДС/мес.
Тариф на 5000 EPS	1 289 400 руб. без НДС/мес.
Тариф на 7000 EPS	1 782 000 руб. без НДС/мес.
Тариф на 10000 EPS	2 647 500 руб. без НДС/мес.

# Сценарии использования



- Сбор событий из облачной и on-premises инфраструктуры
- Поточковая корреляция и детектирование угроз в реальном времени
- Поиск по сырым событиям и нормализованной телеметрии
- Тriage и приоритизация сработок с учётом контекста
- Расследование инцидентов и реагирование из единого окна
- ИИ-помощник для анализа алертов и рекомендаций
- Интеграция с экосистемой безопасности Yandex Cloud (Security Deck и его модули)

# Возможности

## Правила корреляции: потокосые и по расписанию

**Режим анализа событий**  
Выберите, когда и какие события будет проверять правило.

Потокосый (в реальном времени)  
Правило проверяет события сразу при их поступлении для оперативного обнаружения угроз.

По базе (ретроспективно)  
Правило ищет совпадения в сохранённых данных для обнаружения скрытых атак.

**Действия при срабатывании**  
Выберите действия со срабатываниями, которые не были проигнорированы.

Создавать алерт

Имя алерта \*

Тип алерта

**Параметры правила**  
Придумайте уникальное название и опишите суть правила.

Имя \*

Описание



**Правила корреляции / Редактирование правила корреляции**

**Условие корреляции \***  
Напишите запрос с условием выполнения правила.

Шаблоны | Схема | Датасеты

```
1 Events
2 | where event_class in ("ATS3UpdateBucket", "ATS3CreateBucket") and at_event_status == "DONE"
3 | and (
4 |   ['s3_bucket_setting_read_access@object'] == "true"
5 |   or ['s3_bucket_list_access@object'] == "true"
6 |   or ['s3_bucket_object_access@object'] == "true"
7 | )
8 | extend organization_id = tostring(resource_metadata_org.resource_id),
9 |   cloud_id = tostring(resource_metadata_cloud.resource_id),
10 |   folder_id = tostring(resource_metadata_folder.resource_id),
11 |   authentication_context = authentication
12 | extend bucket_name = tostring(bucket_id@object),
13 |   settings_read_access = tostring(s3_bucket_setting_read_access@object),
14 |   list_access = tostring(s3_bucket_list_access@object),
15 |   objects_access = tostring(s3_bucket_object_access@object)
16 | extend event_class = "BucketWithPublicAccess",
17 |   severity = "HIGH"
```

# Возможности

## Расследования инцидентов

12.04.2026 23:00:00 — 🗑 Шаблоны 🗑 Схема 🗑 Датасеты ?

1 | `ATS3CreatePresignURL`  
2 | `where toString(request_metadata.user_agent) contains "Mozilla"`  
3 | `limit 100`

▶ Запустить 🔄 Поделиться 📁 Сохранить

Запуск: 15.04.2026, 11:13:31 · 30 сек · ✅ Завершён 🕒 История

🔍 Все поля 📄 Экспорт ▾ 59 записей · 12.04.2026, 23:00:00 – 13.04.2026, 23:00:00

>	event_class	time	action	action_state	action_status	at_details	at_event_status	at_event_type	authentication	authorized	bur
>	ATS3CreatePresignURL	13.04.2026 04:44:00	create	—	—	—	DONE	yandex.cloud.audit.storage.PresignURLCreate	{impersonator_name: yc-iam-openid-server, ...}		cloi ass
>	ATS3CreatePresignURL	13.04.2026 04:46:13	create	—	—	—	DONE	yandex.cloud.audit.storage.PresignURLCreate	{impersonator_name: yc-iam-openid-server, ...}		cloi ass

# Возможности

## Исключения

The screenshot displays the Azure Security Center interface. On the left is a sidebar with a search bar and a list of correlation rules: 'Имя / Описание', 'iam-detect-leaked-severity', 'test-revert-exception', 'test-exception-1', and 'ttt'. The main area shows the details for the 'iam-detect-leaked-severity' rule, which is an exception to the correlation rule. It is currently in a 'Healthy' state. Action buttons include 'Развернуть', 'Редактировать', and 'Ещё'. Below the main title, there is a section for 'Правило' (Rule) showing 'IAMDetectLeakedCredential' with a 'Высокая критичность' (High severity) warning and a 'Healthy' status. A section for 'Условие' (Condition) shows the value 'high' for the 'severity' field.

ucem-preprod ... m-arefiev

### Security Information and

Расследования Правила корреляции

Имя, описание или правило

- Имя / Описание
- iam-detect-leaked-severity
- test-revert-exception
- test-exception-1
- ttt

### iam-detect-leaked-severity

Исключение правила корреляции · Healthy

Развернуть Редактировать Ещё ▾

Обзор

#### Правило ^

**IAMDetectLeakedCredential**  
Пользовательский · ⚠ Высокая критичность · Healthy

#### Условие ^

severity

high

# Возможности

## Алертинг

## с ИИ-ассистентом

### Для виртуальной машины добавлен публичный IP-адрес



Открыт ▾

⚠ Средняя

· 15.04.2026, 11:00 · al3getka988larpfrtn1

Для виртуальной машины `fv48214a43srdsa0tcoj` был добавлен публичный IP-адрес. Это может привести к увеличению поверхности атаки, несанкционированному доступу или утечке данных.

Пользователь добавивший публичный IP-адрес:

ID: `yc.compute.tf-api-sa`

Имя: `tf-api-sa`

Информация о виртуальной машине:

ID виртуальной машины: `fv48214a43srdsa0tcoj`

AI-ассистент PREVIEW



**i** В этом чате ассистент работает только с алертом  
[Для виртуальной машины добавлен публичный IP-адрес](#)

15 апреля 2026 г.

Разбор алерта «Для виртуальной машины добавлен публичный IP-адрес»

Для виртуальной машины был добавлен публичный IP-адрес, что повышает риски безопасности. Требуется изолировать систему, пересмотреть управление доступом и усилить меры безопасности. Детальный анализ MITRE ATT&CK невозможен без дополнительных данных.

### Сводка

- **Контекст инцидента:** для виртуальной машины `fv48214a43srdsa0tcoj` был добавлен публичный IP-адрес. Это может увеличить поверхность атаки, привести к несанкционированному доступу или утечке данных.
- **Технические детали:** виртуальная машина `fv48214a43srdsa0tcoj`, пользователь, добавивший публичный IP-адрес: `tf-api-sa` (ID:

# Соответствие законодательству и отраслевым стандартам



152-ФЗ  
«О персональных  
данных»



ГОСТ Р 57580



Payment Card  
Industry Data  
Security Standard



Стандарт  
по защите облачной  
инфраструктуры

# «Софтлайн Решения»

Преимущества сотрудничества  
с компанией «Софтлайн Решения»:

## Сильная команда

400+

Сотрудников  
в Управлении ИБ

300

Из них технические  
специалисты

1000+

Проектов по ИБ  
ежегодно



Поддержка отраслевой  
экспертизы

## Заказчик в центре внимания

- Фокус на долгосрочное сотрудничество и эффективное решение задач
- Реализация требований ИБ в комплексных проектах с другими направлениями
- Регулярный мониторинг качества реализуемых проектов и улучшение связанных с этим процессов

Топ-2

cnews

Топ-100 российских ИТ-поставщиков  
решений для защиты информации

## Финансовые инструменты

- Гибкие финансовые условия с применением SL Finance
- Внедрение решений по модели MSSP/SaaS

# Компетенции «Софтлайн Решений»

Полный цикл внедрения решений информационной безопасности

## Экспертиза

Консультант по продуктам, специализирующийся на какой-либо продуктовой группе:

- Защита приложений
- Управление инцидентами
- Управление доступом



## Сопровождение

Комплексная проработка выбранного решения:

- Обученные специалисты по продуктам безопасности Yandex Cloud
- Опытные архитекторы

# Спасибо за внимание!

**Алексей Чупринин**

Руководитель направления защиты приложений,  
«Софтлайн Решения»

[Alexey.Chuprinin@softline.com](mailto:Alexey.Chuprinin@softline.com)



[appsec@softline.com](mailto:appsec@softline.com)