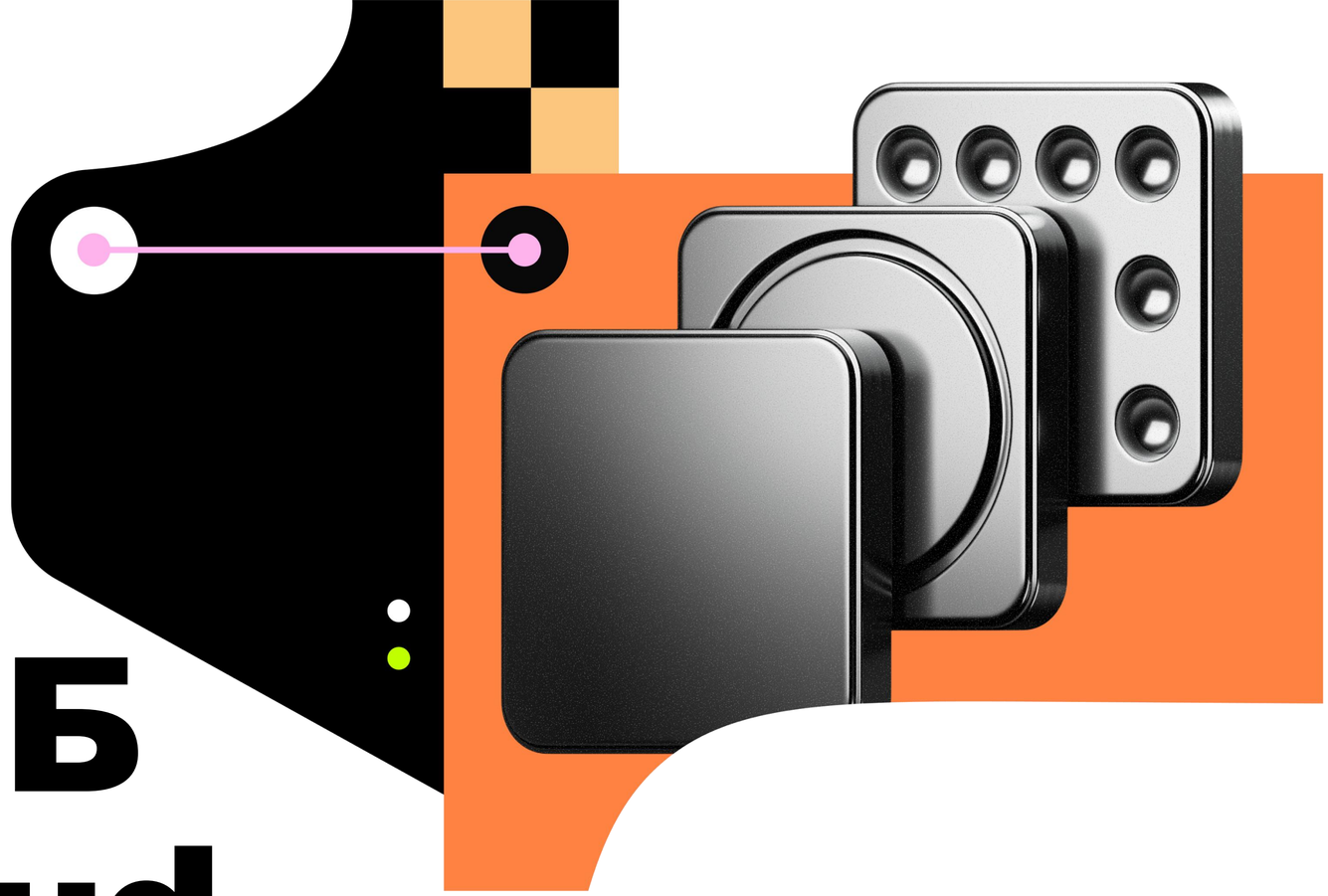
Yandex Cloud



Все Сервисы ИБ Yandex Cloud

Марат Вахитов
Security Solution Sales,
Yandex Cloud

Алексей Чупринин
Руководитель направления защиты
приложений, «Софтлайн Решения»

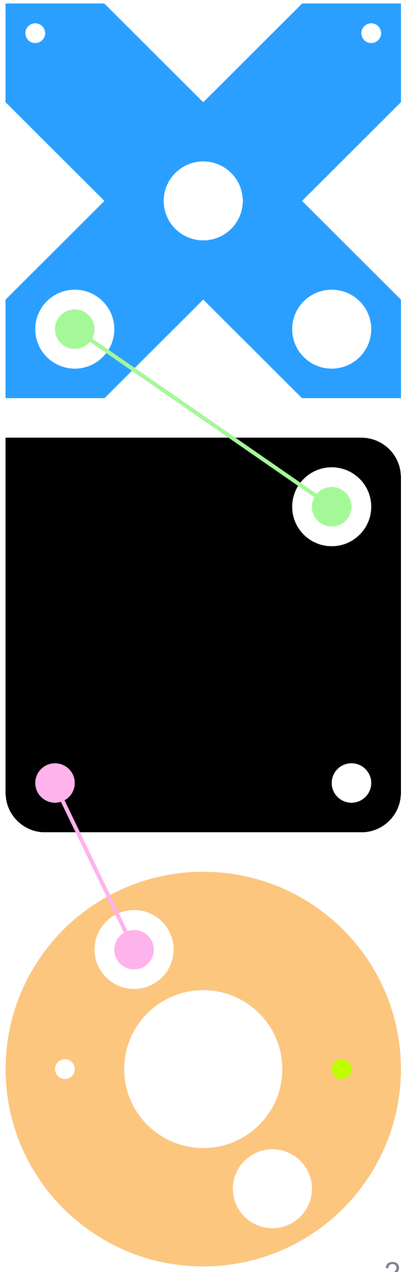
О чём поговорим?

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

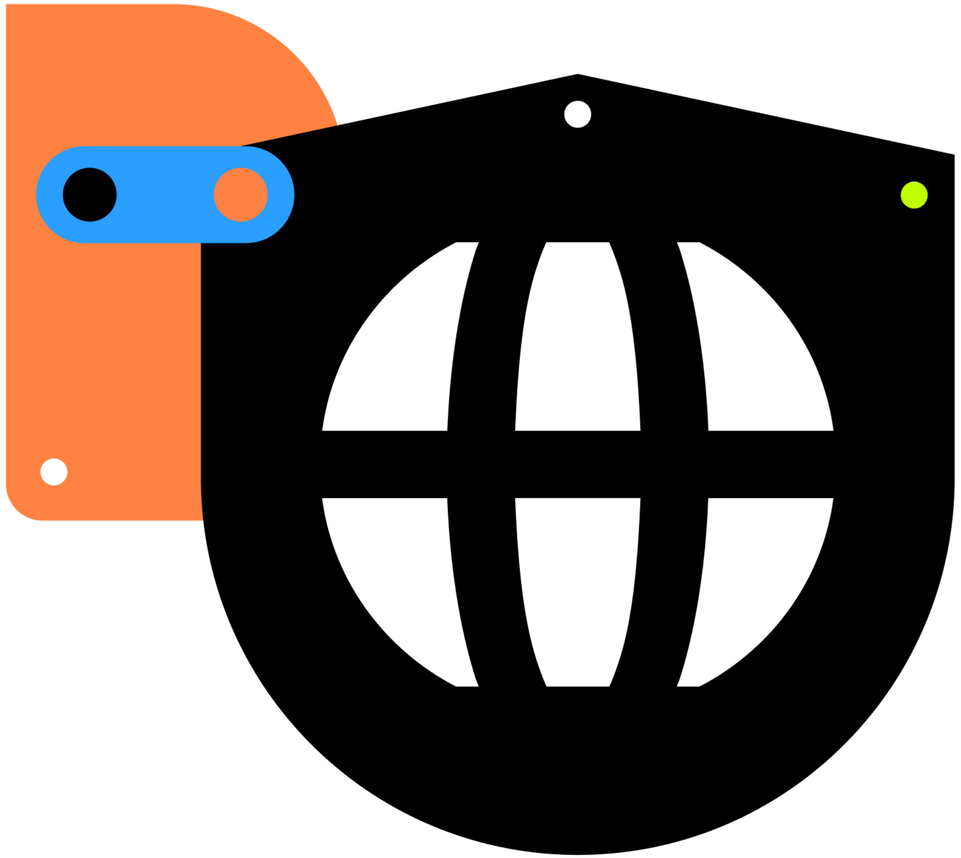
Система мониторинга событий безопасности и обнаружения угроз

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®, 1С)

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 высоко-нагруженных 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

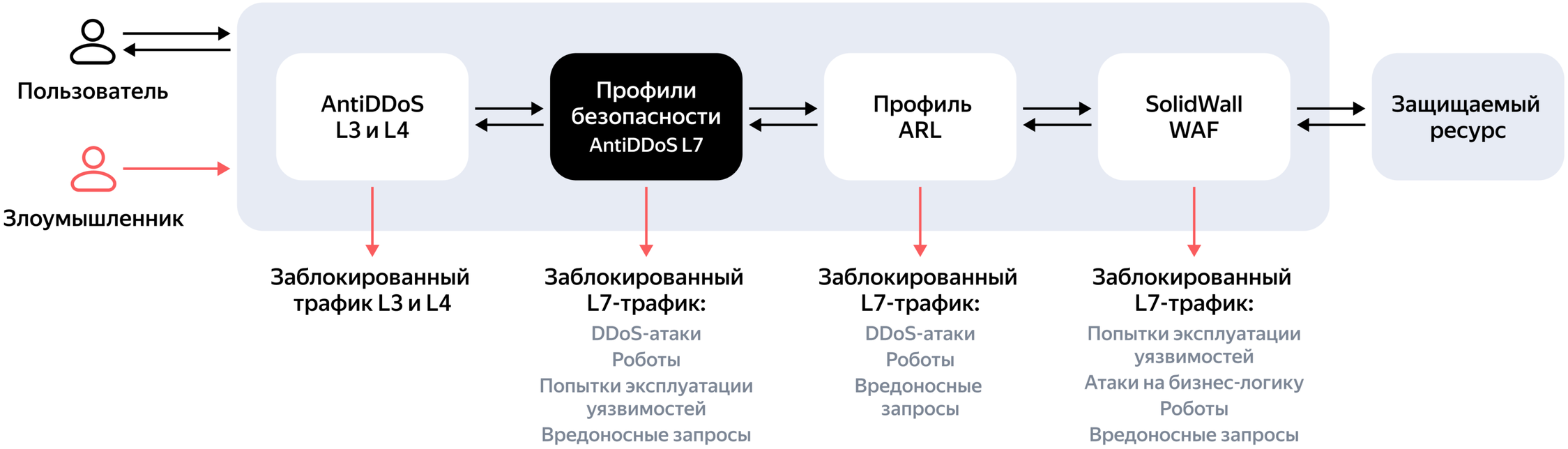
Широкий инструментарий по борьбе с ботами

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

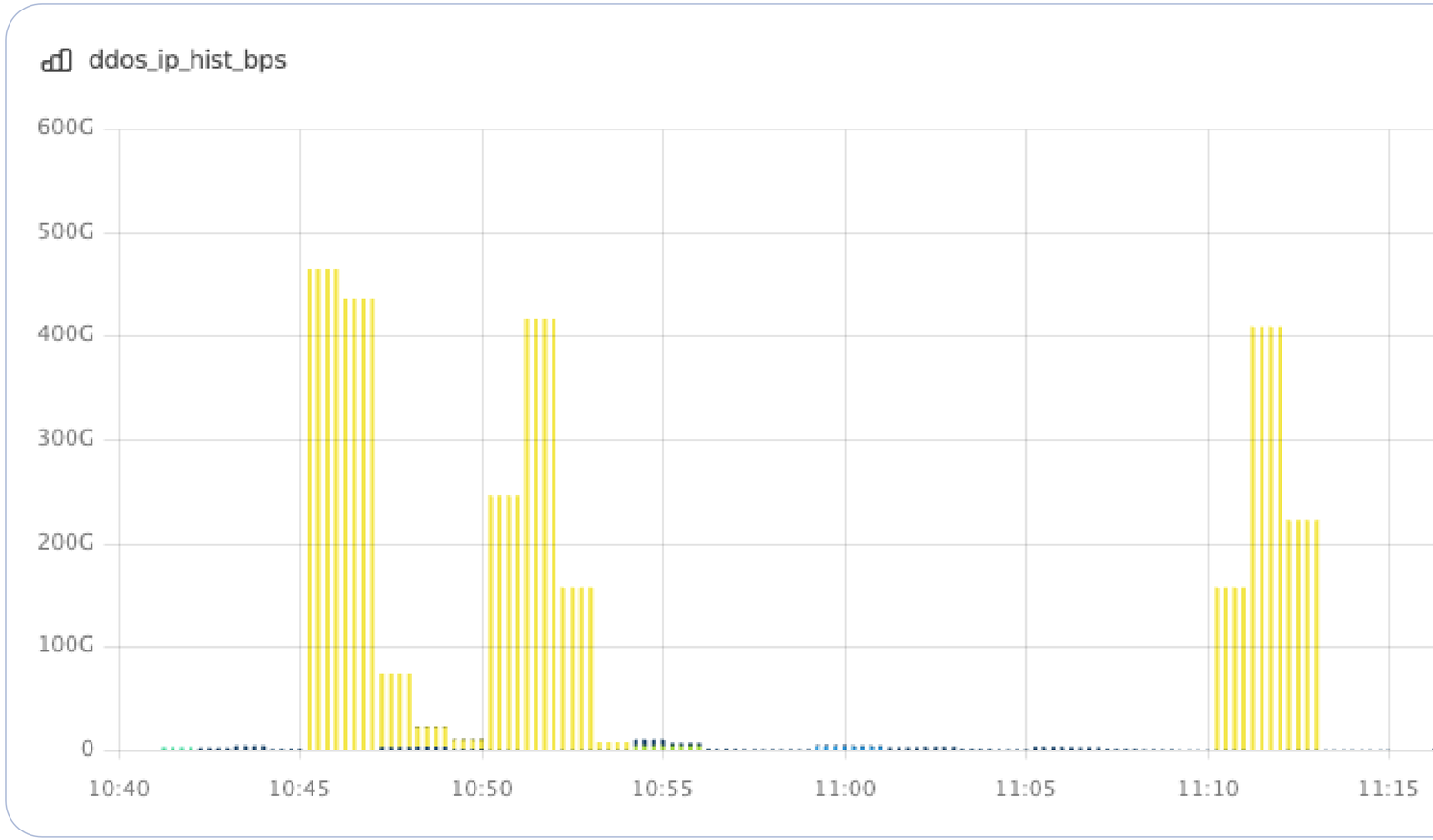
UDP flood

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

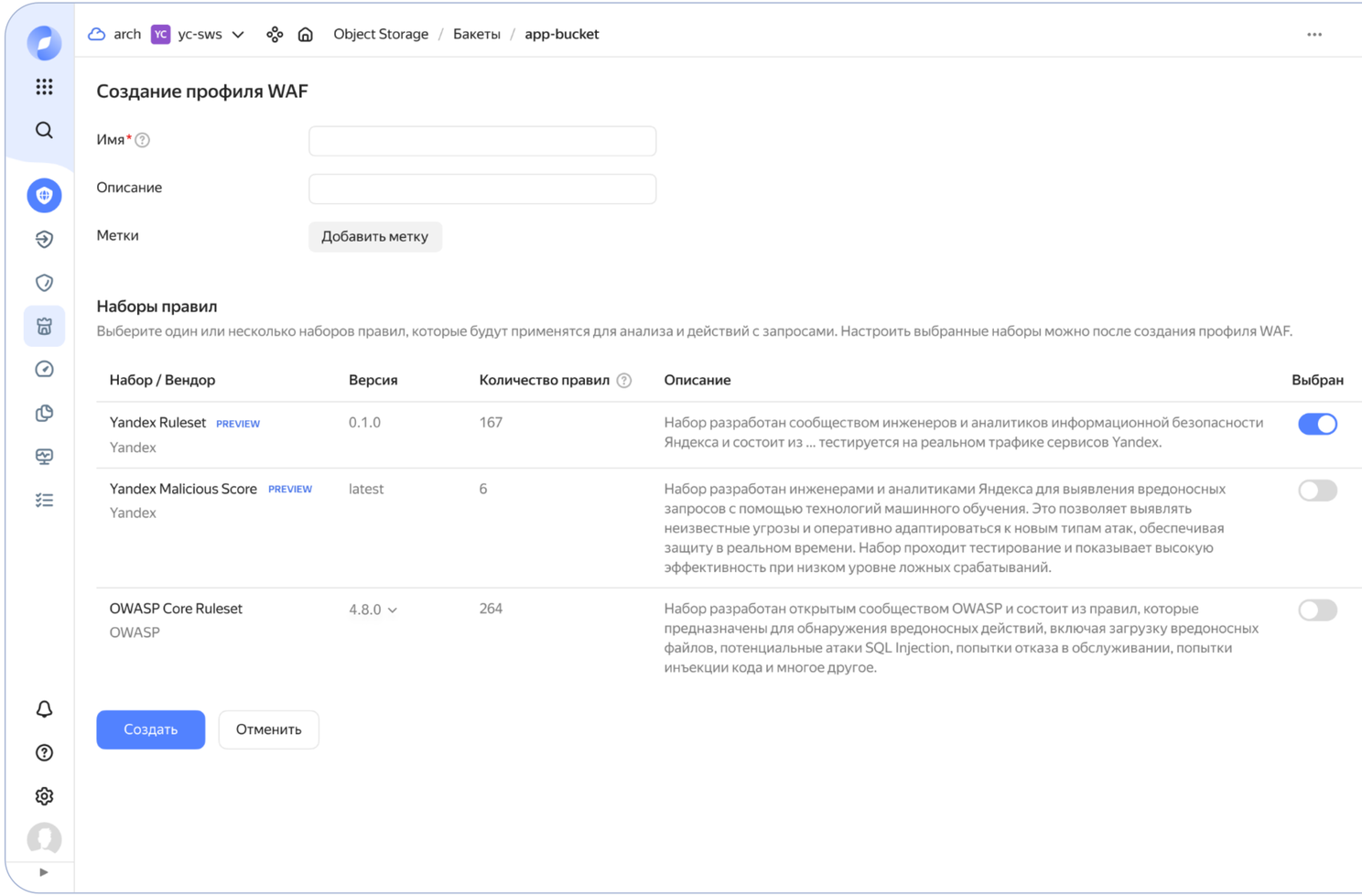
clck.ru/3SrnR9

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®



SolidWall WAF

Preview

Теперь часть Yandex Smart Web Security

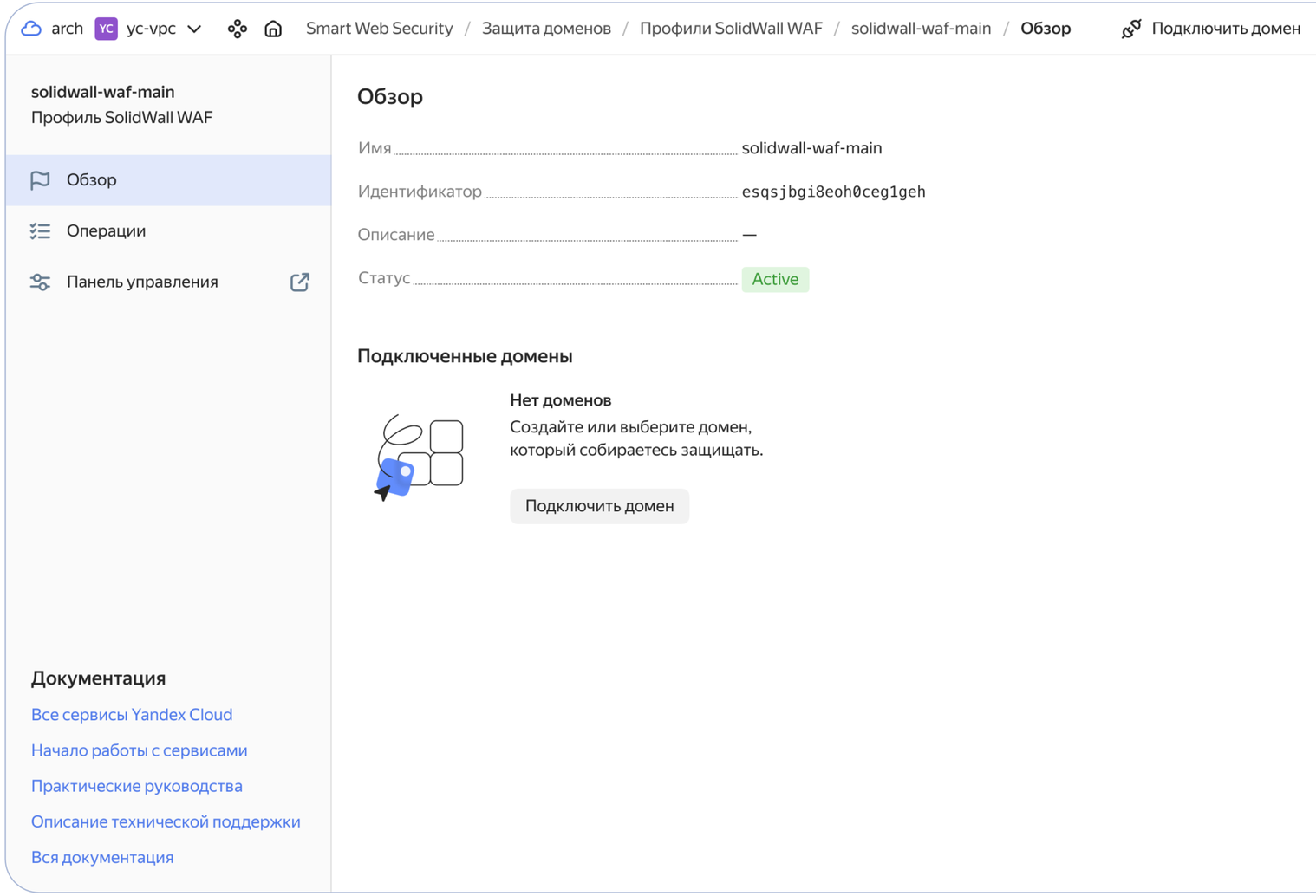
Сочетает негативную
и позитивную модели защиты

Анализ поведения пользователей
для выявления продвинутых ботов

Инвентаризация API

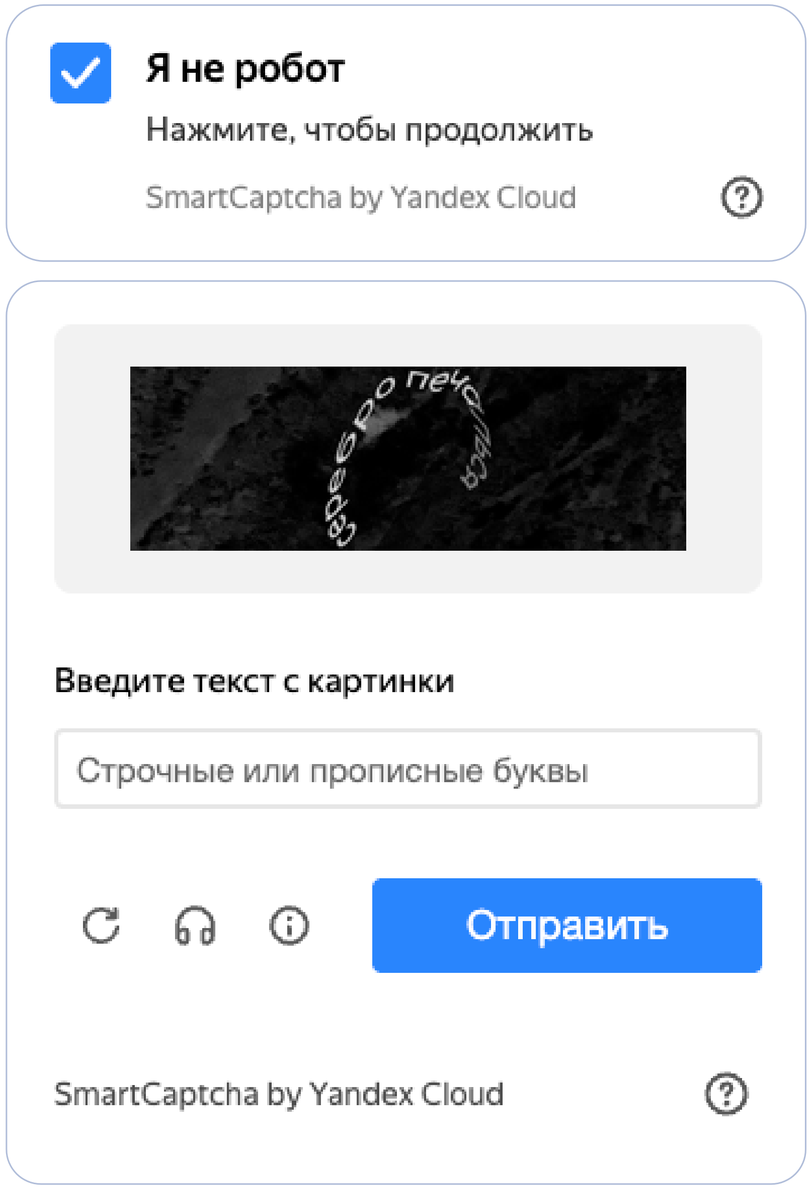
Подключается в несколько кликов

Запросить
доступ:
clck.ru/3T84fo



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



Референсные клиенты

ZENDEN

КОФЕМАНИЯ

ProgressMe

МИР ИНСТРУМЕНТА

екапуста

циан

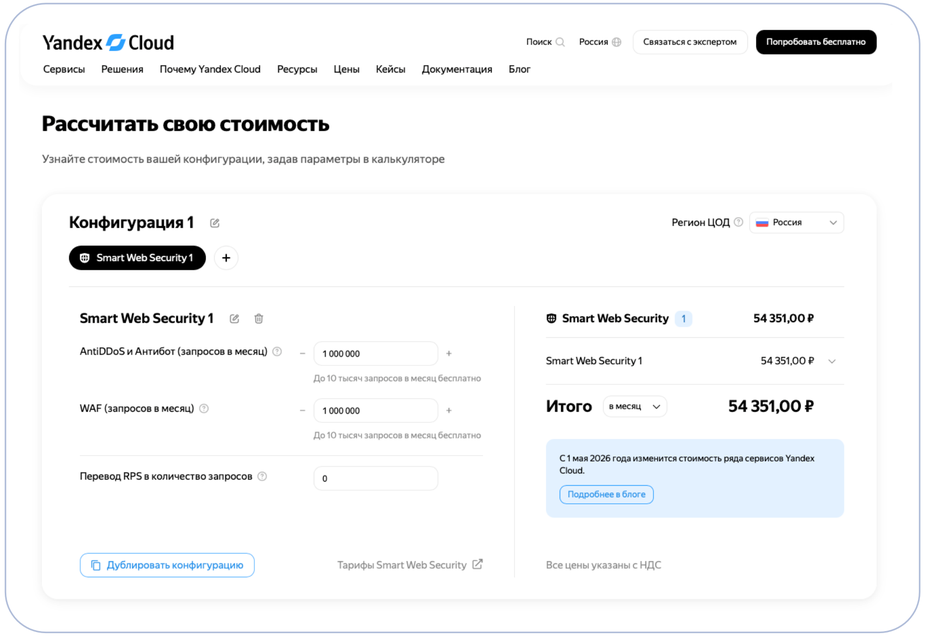
Ценообразование

Подписки

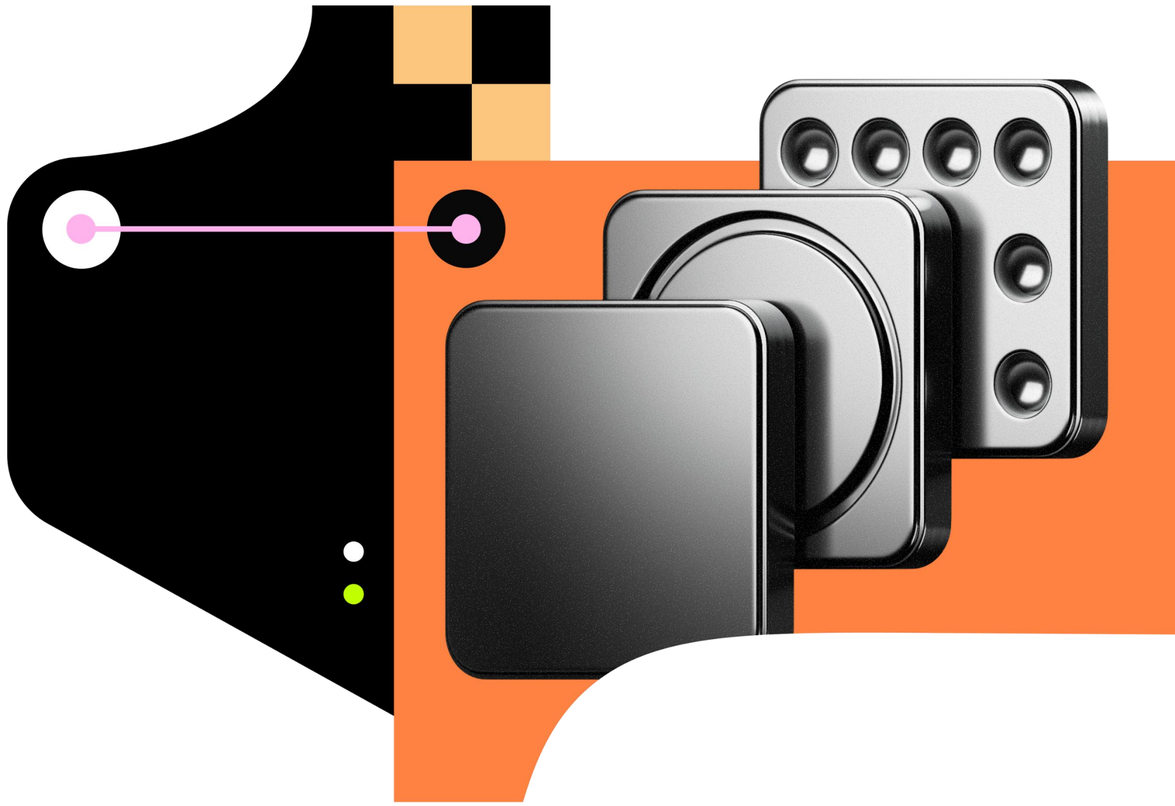
Цены в рублях | Цены в тенге

	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 профиля безопасности: • базовыми • Smart Protection	50 833 ₽	160 633 ₽	259 250 ₽	Рассчитывается индивидуально
Абонентская плата за пакет WAF, ежемесячно. Пакет включает анализ запросов правилами WAF	40 667 ₽	76 250 ₽	152 500 ₽	Рассчитывается индивидуально

PAYG



SolidWall AI Security Gateway



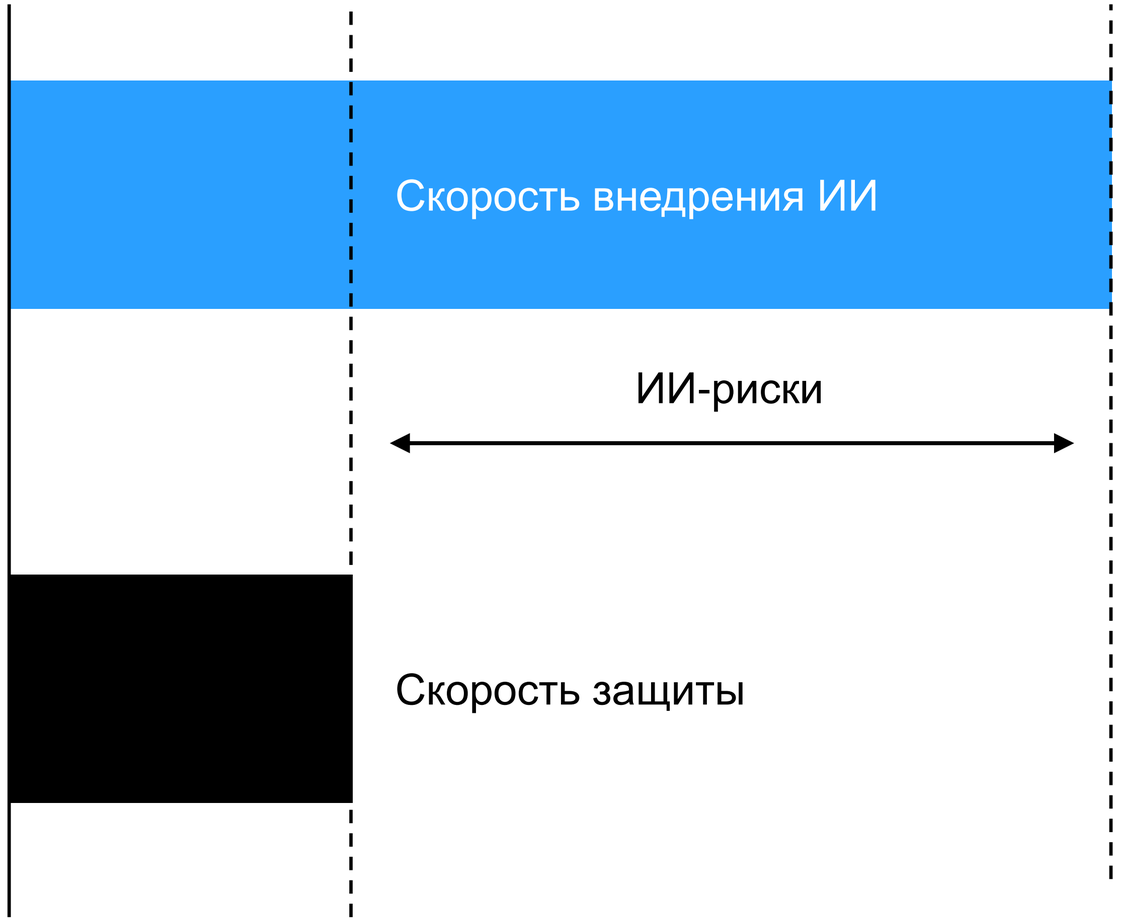
Разрыв безопасности

60% ИИ

не имеют формализованной политики

65% ИИ

используют GenAI

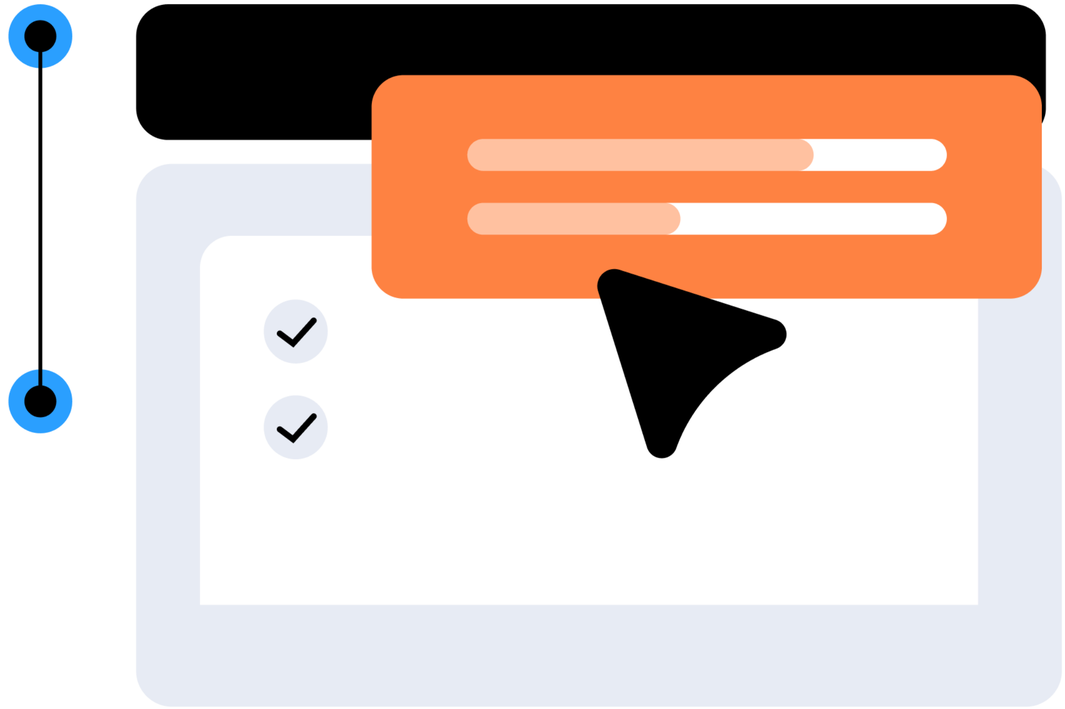


mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai-2024, rt-solar.ru/events/news/6366/

Рекомендации по безопасной работе с ИИ-агентами

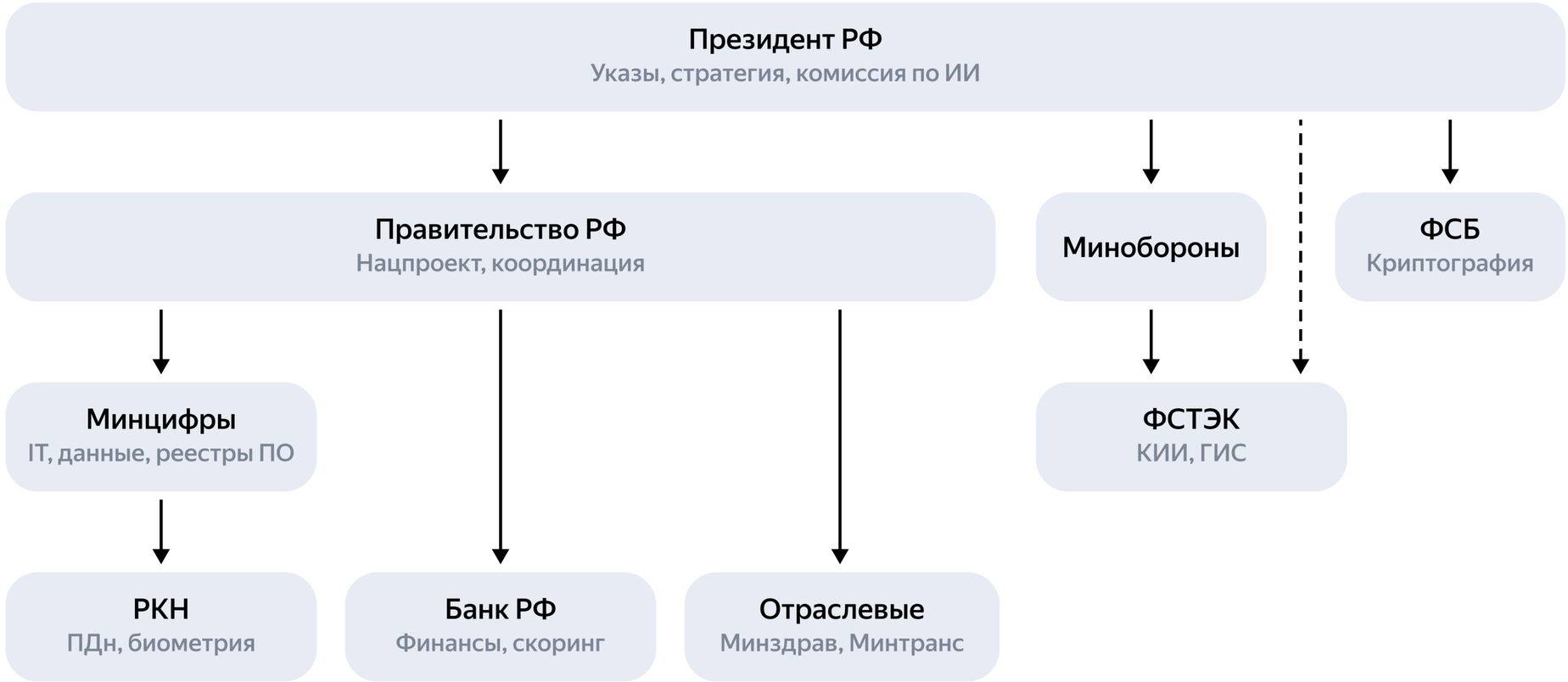
AI Secure Agentic Framework Essentials (AI-SAFE)

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	2020	2021	2024	2025–2026	2027
Указ № 490 Стратегия	**258-ФЗ ЭПР** Песочницы 123-ФЗ: Москва 258-ФЗ: общий ЭПР	**Кодекс этики ИИ** Soft law	**Указ № 124** Нацпроект «Экономика данных»	**Приказ ФСТЭК № 117** Ужесточение обязательных требований/ ПДн, ГИС/КИИ, рост штрафов	**Рамочный закон** Полноценный закон об ИИ

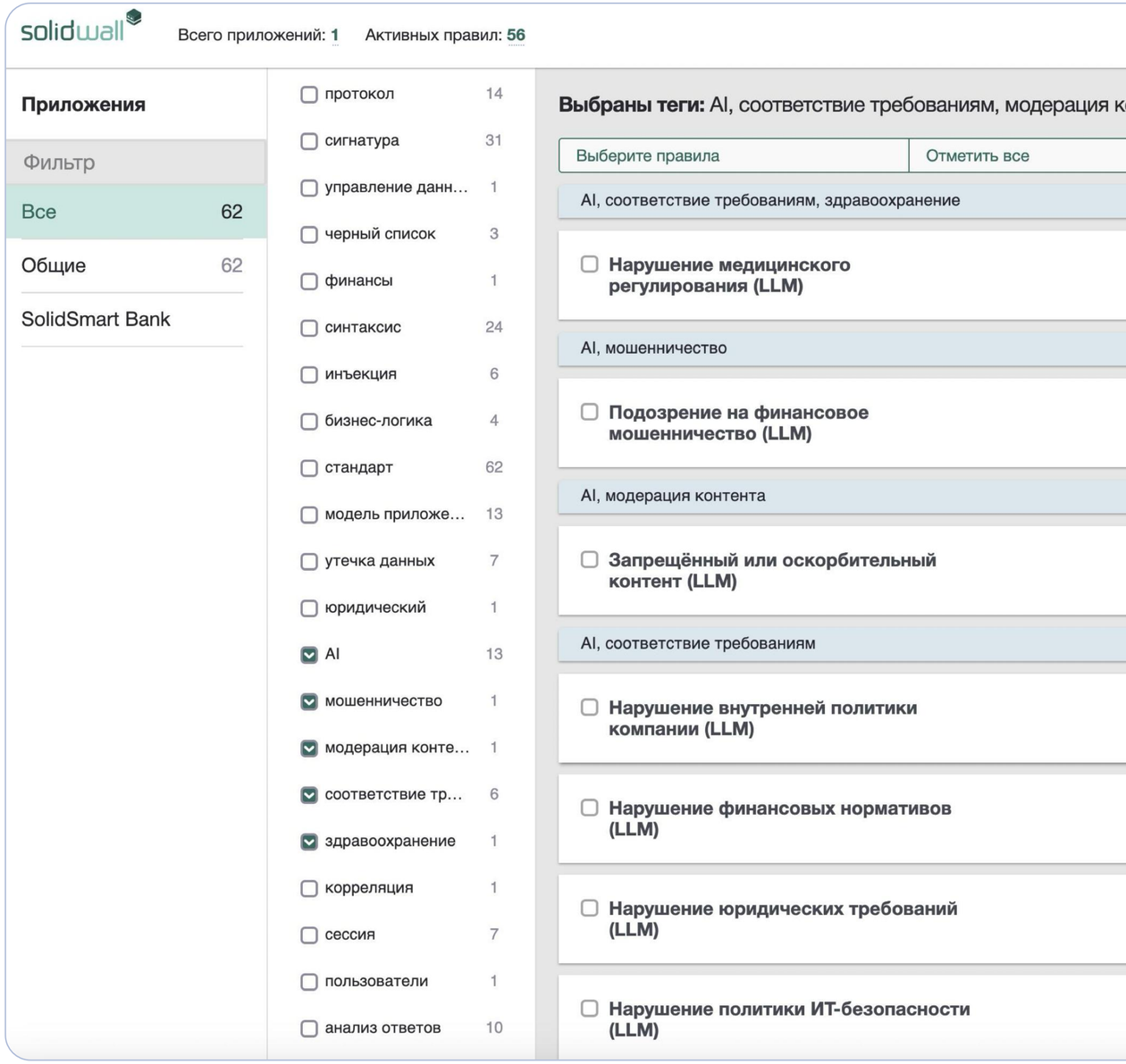
Soft law — Hard law

AI Security Gateway

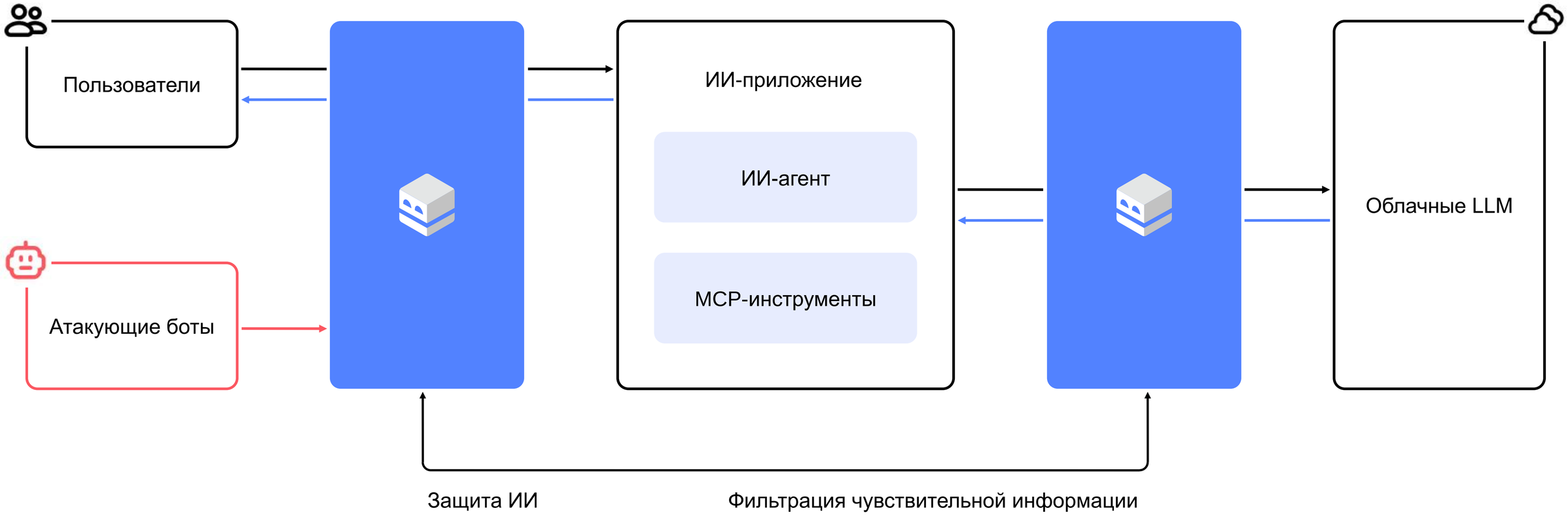
20+

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

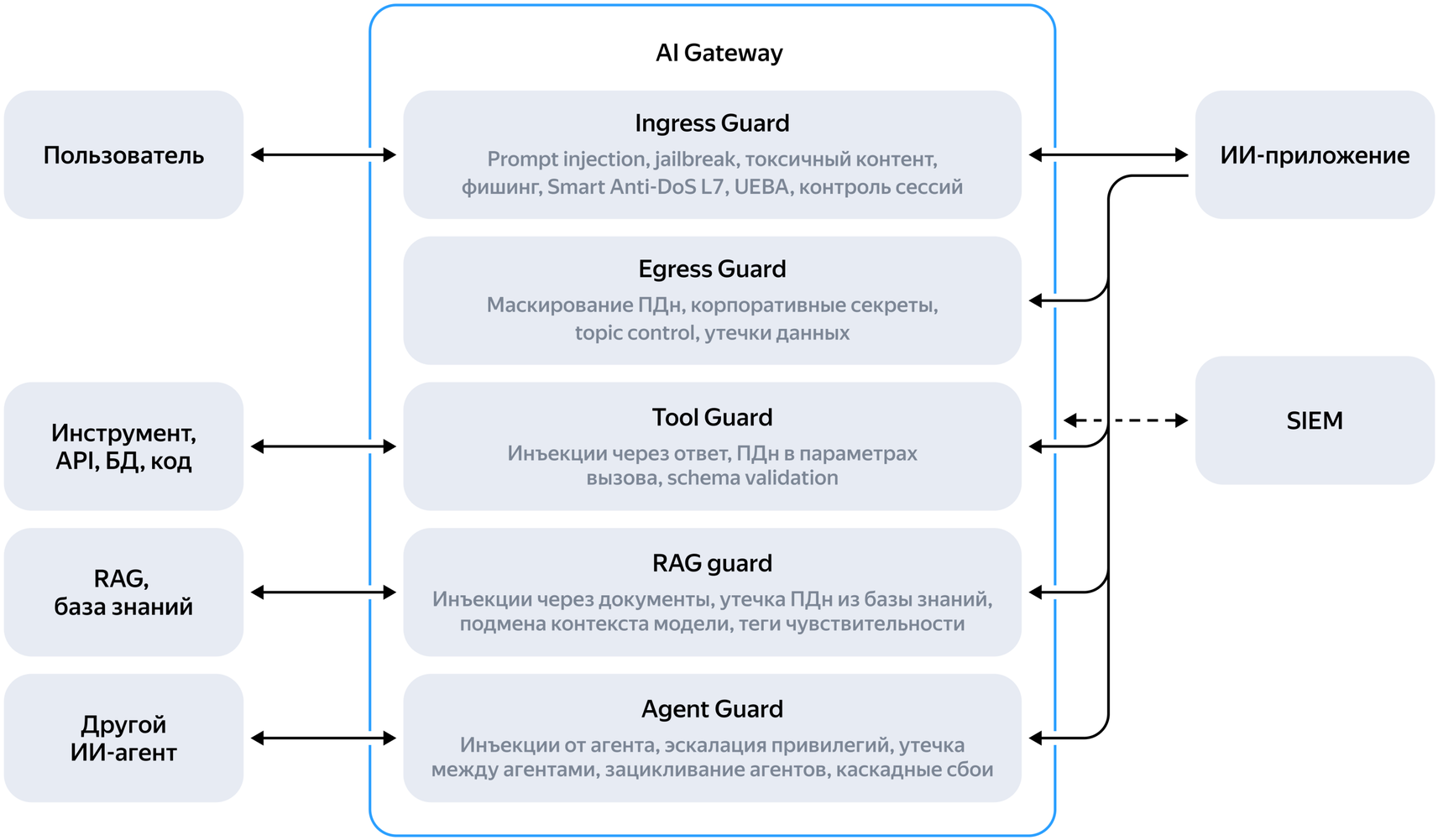
- инъекции промпта
- обход бизнес-ограничений
- избыточные привилегии агентов
- чрезмерное потребление ресурсов



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

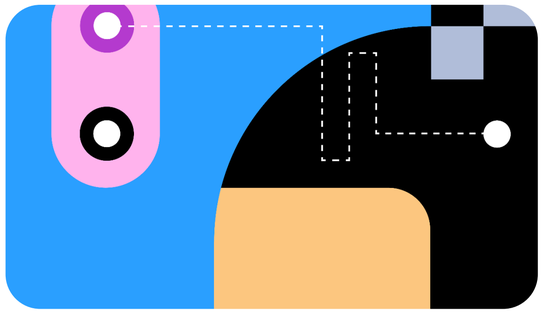
OWASP® Top 1,
Yandex AI-SAFE

Интеграции

SIEM/SOAR, Zabbix,
Prometheus®

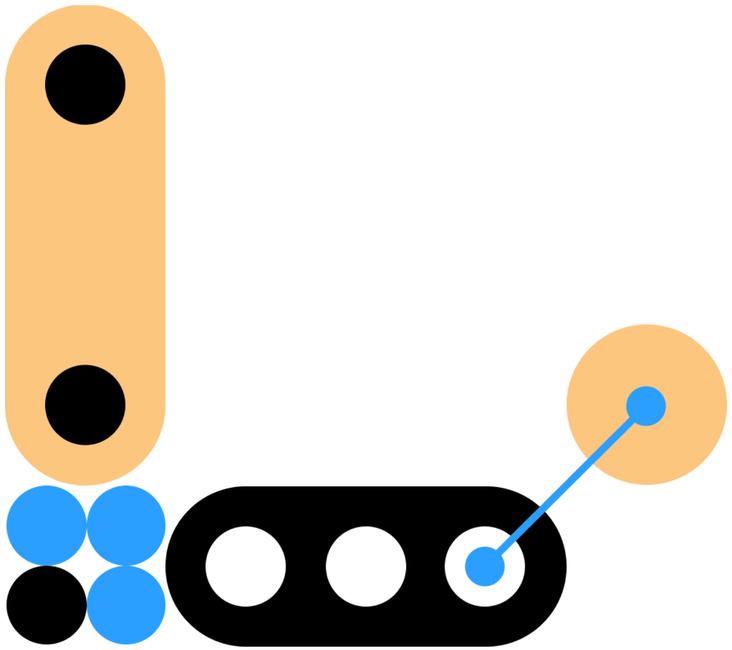
Интерпретируемость

Гранулярные классы,
интерпретируемые
модели



Итог

Зачем это нужно
именно сейчас



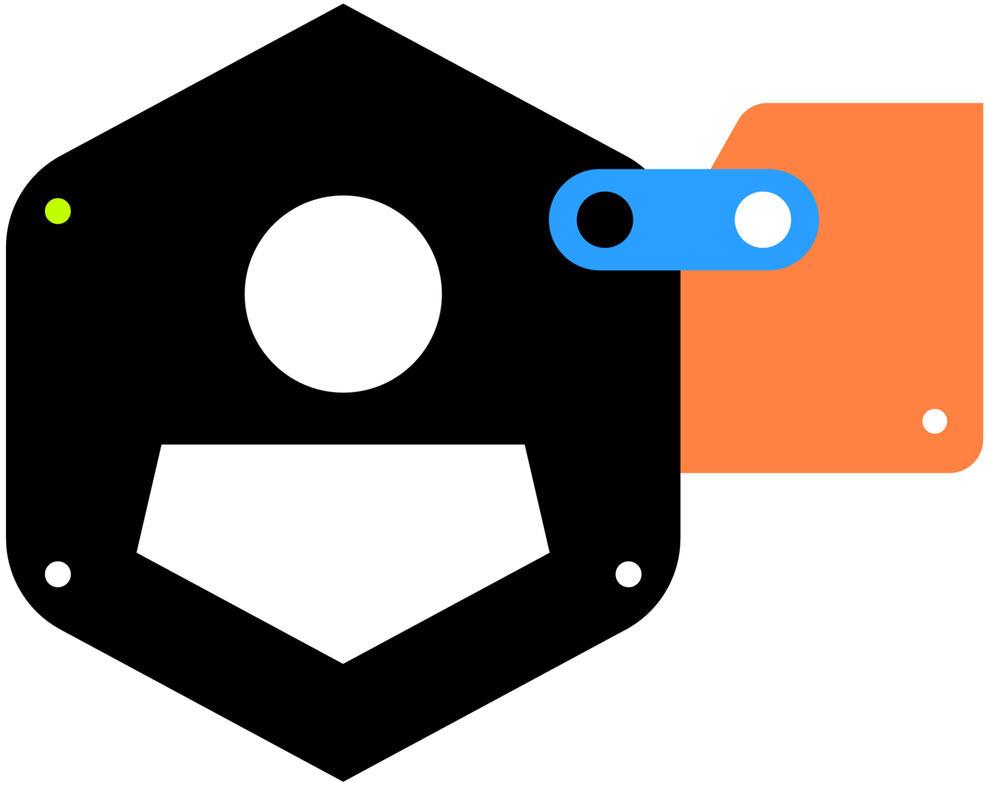
Каждый корпоративный чат-бот, RAG-система или ИИ-агент — это новая поверхность атаки

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

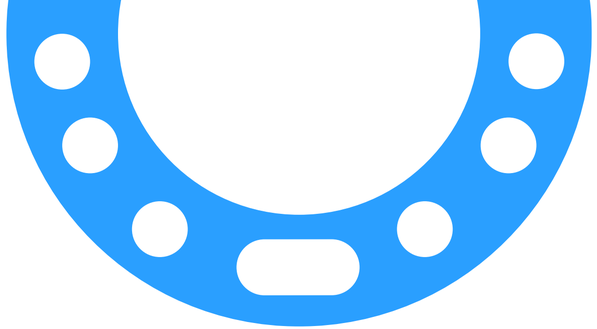
SolidWall AI Security Gateway закрывает разрыв между скоростью внедрения ИИ и зрелостью его защиты

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

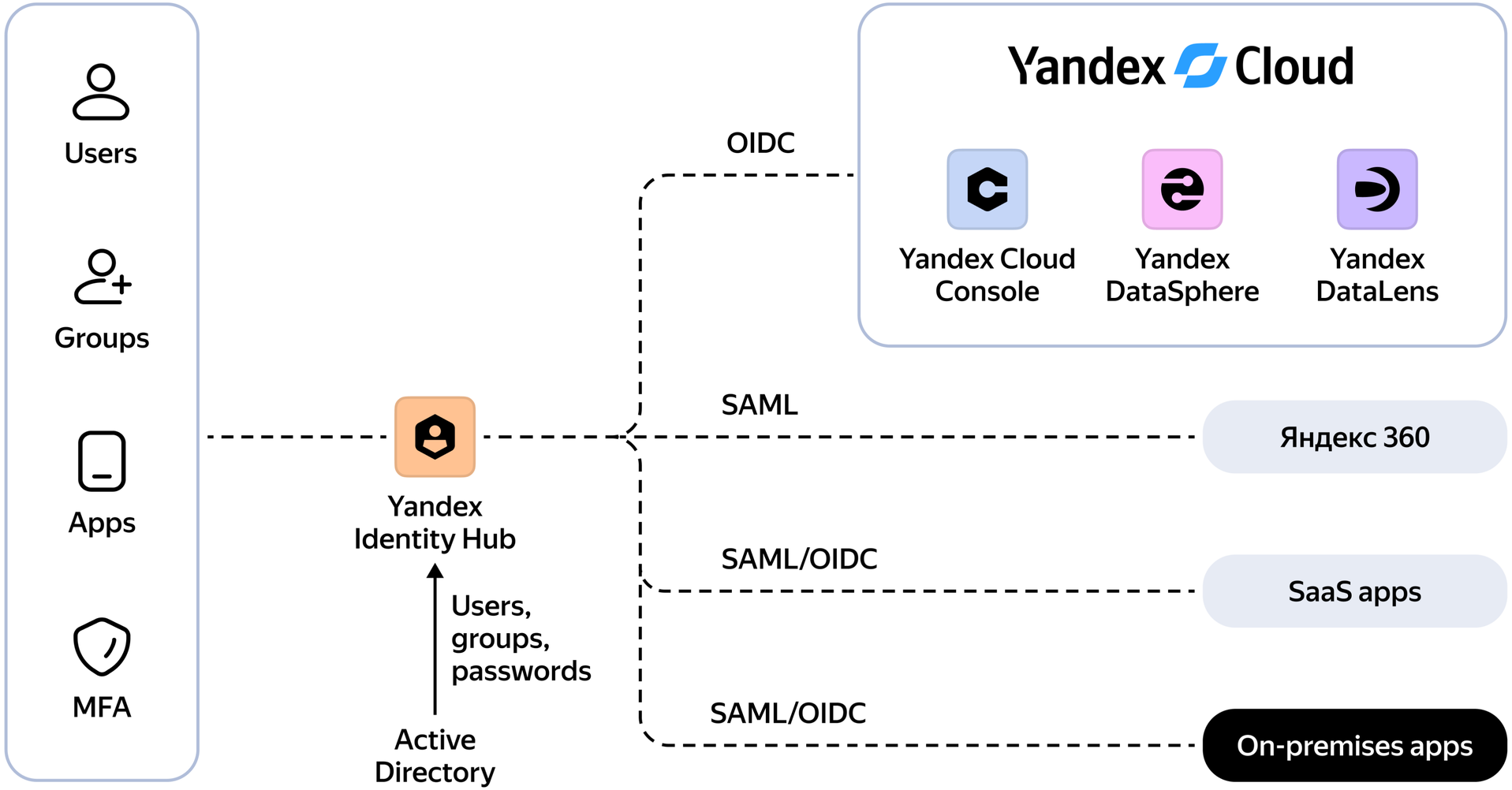
«Анализ киберугроз в облачных и гибридных инфраструктурах за второе полугодие 2025», Yandex Cloud

77%

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

Verizon’s Data Breach Investigations Report (2024)

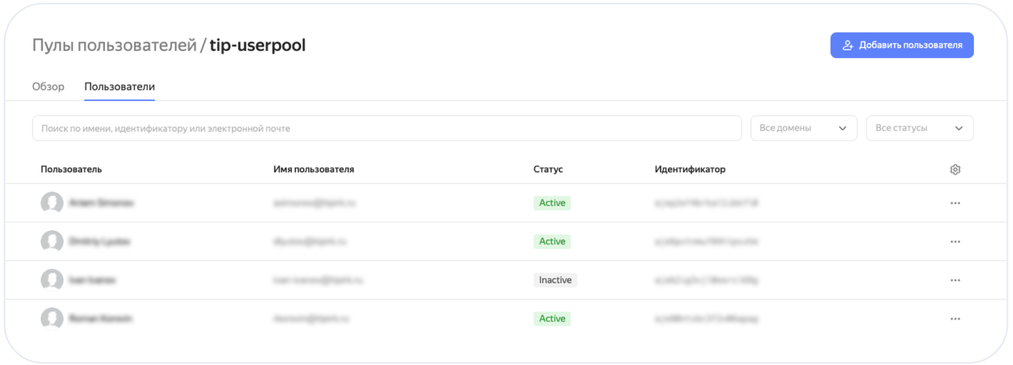
Архитектура сервиса

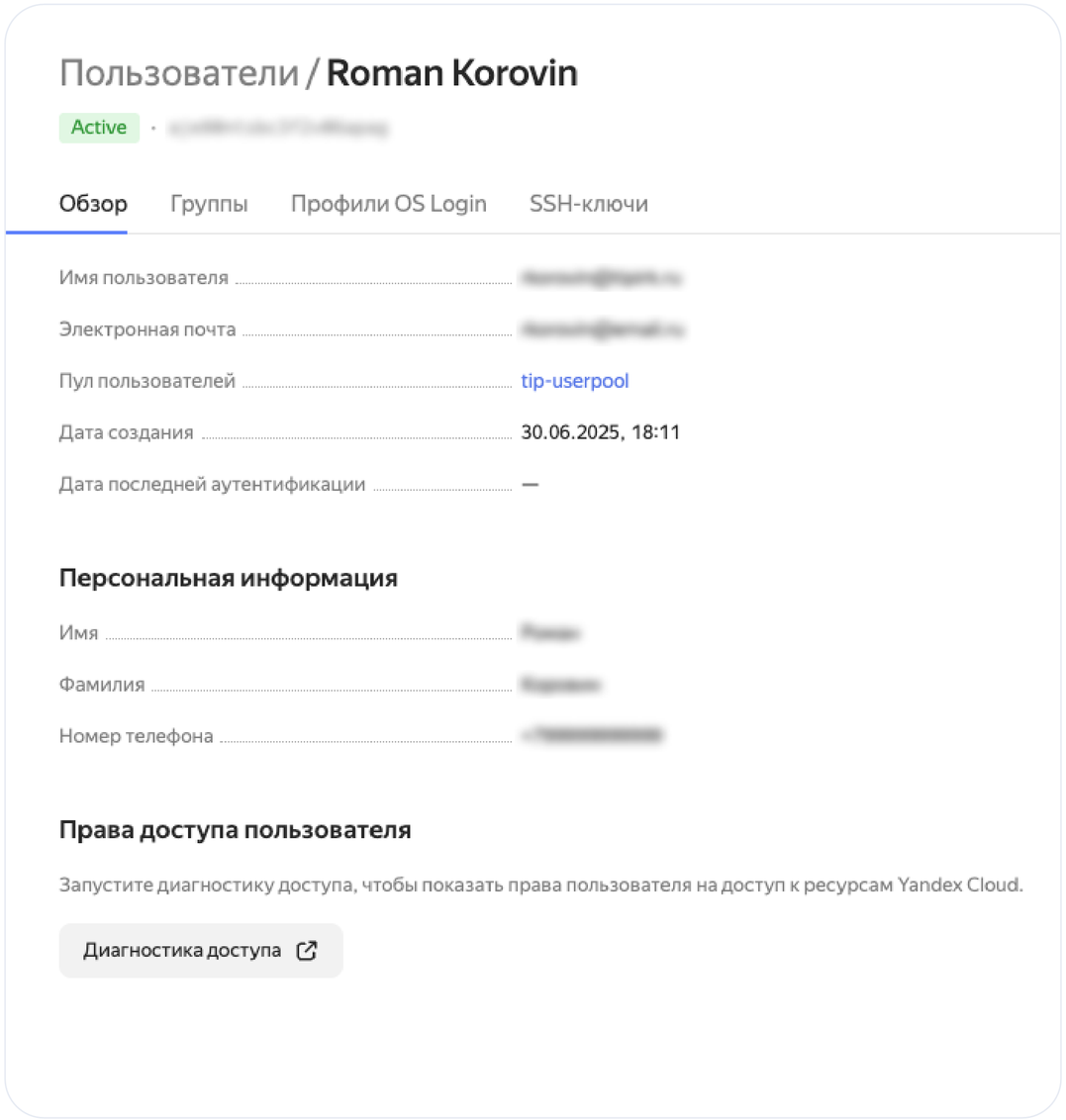


Возможности

Хранение учётных данных пользователей

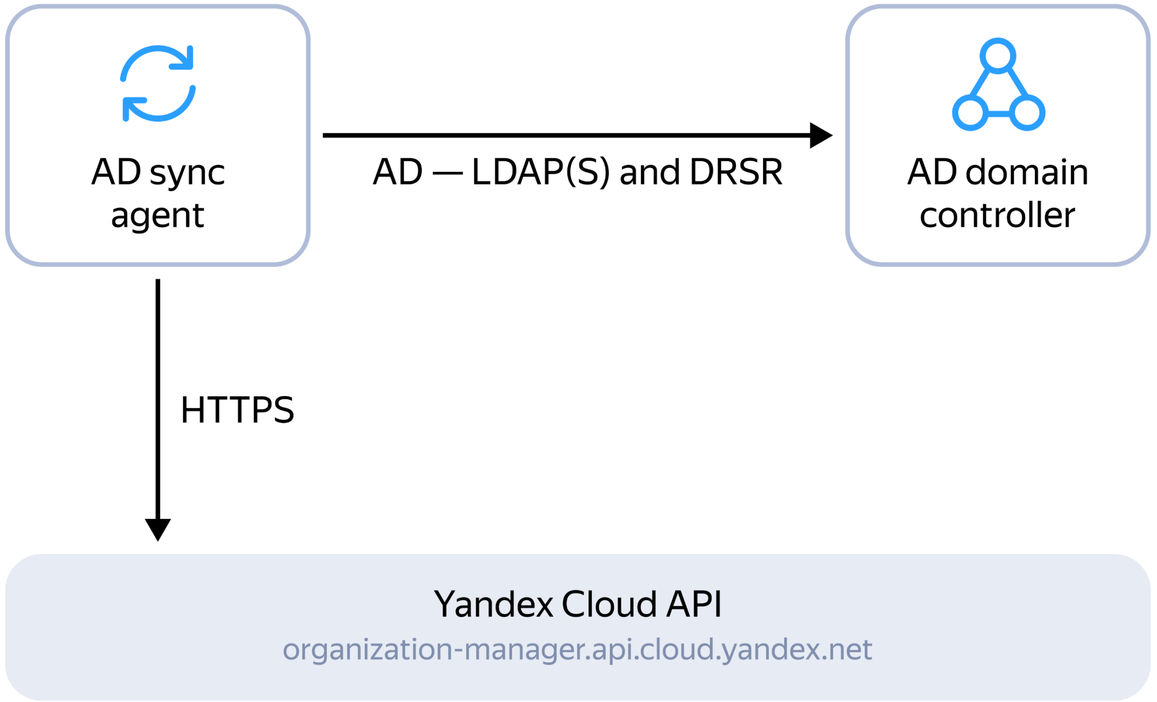
Управление пользователями
и их атрибутами





Синхронизация с Active Directory

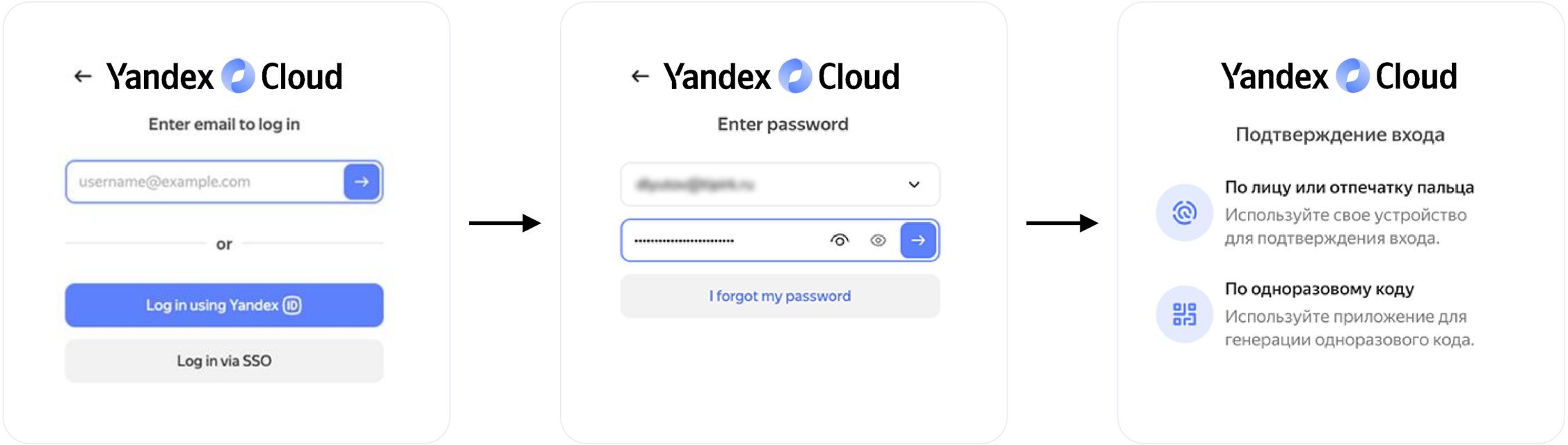
- Синхронизация пользователей и их атрибутов
- Синхронизация групп и членства пользователей в них
- Единый пароль с Active Directory
  Password hash synchronization
- Настройка области и периодичности синхронизации



Возможности

Аутентификация

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

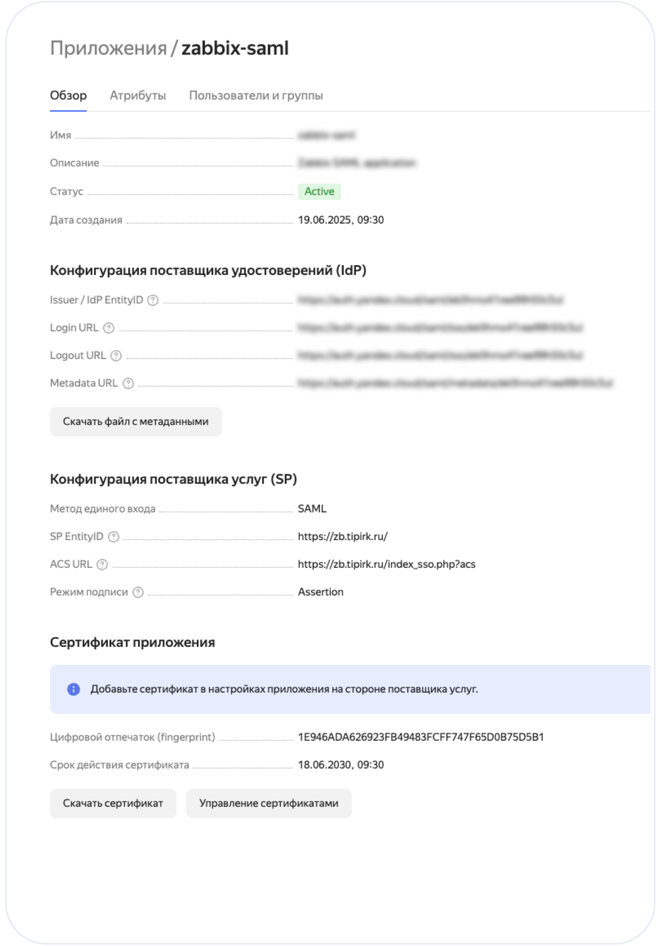


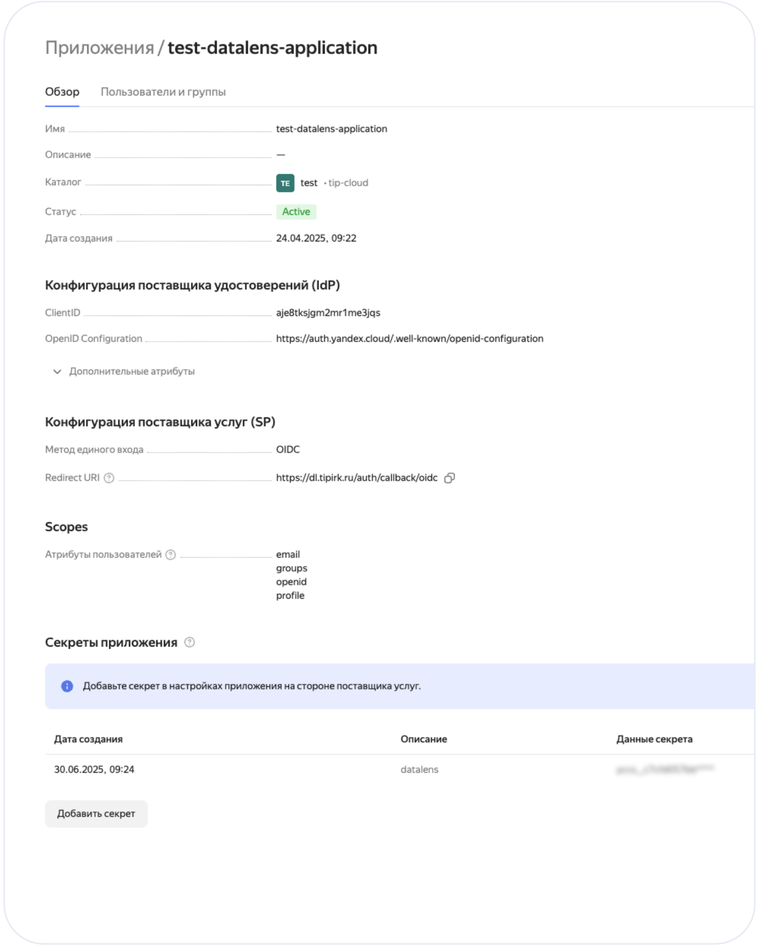
Возможности

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

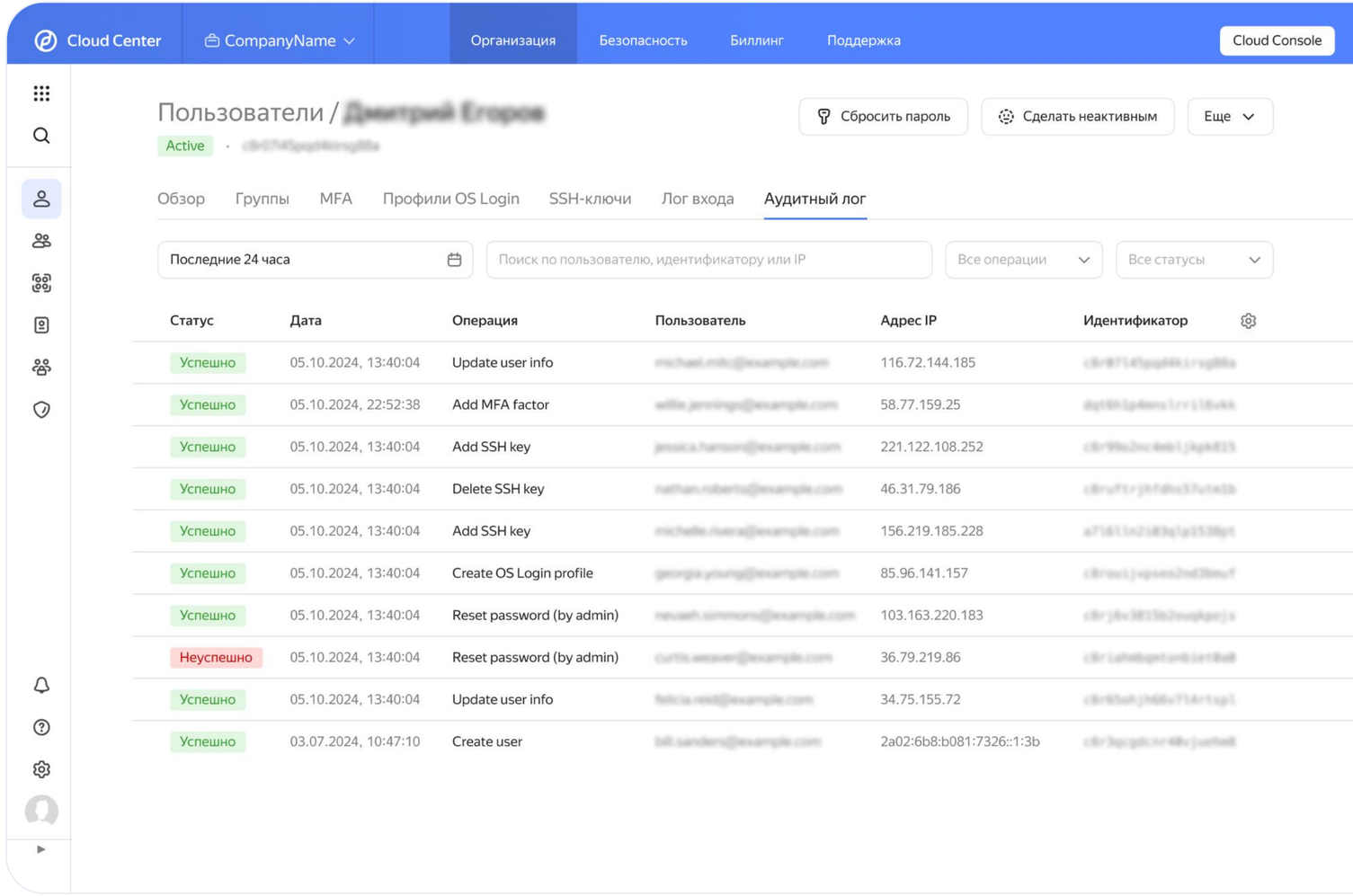




Возможности

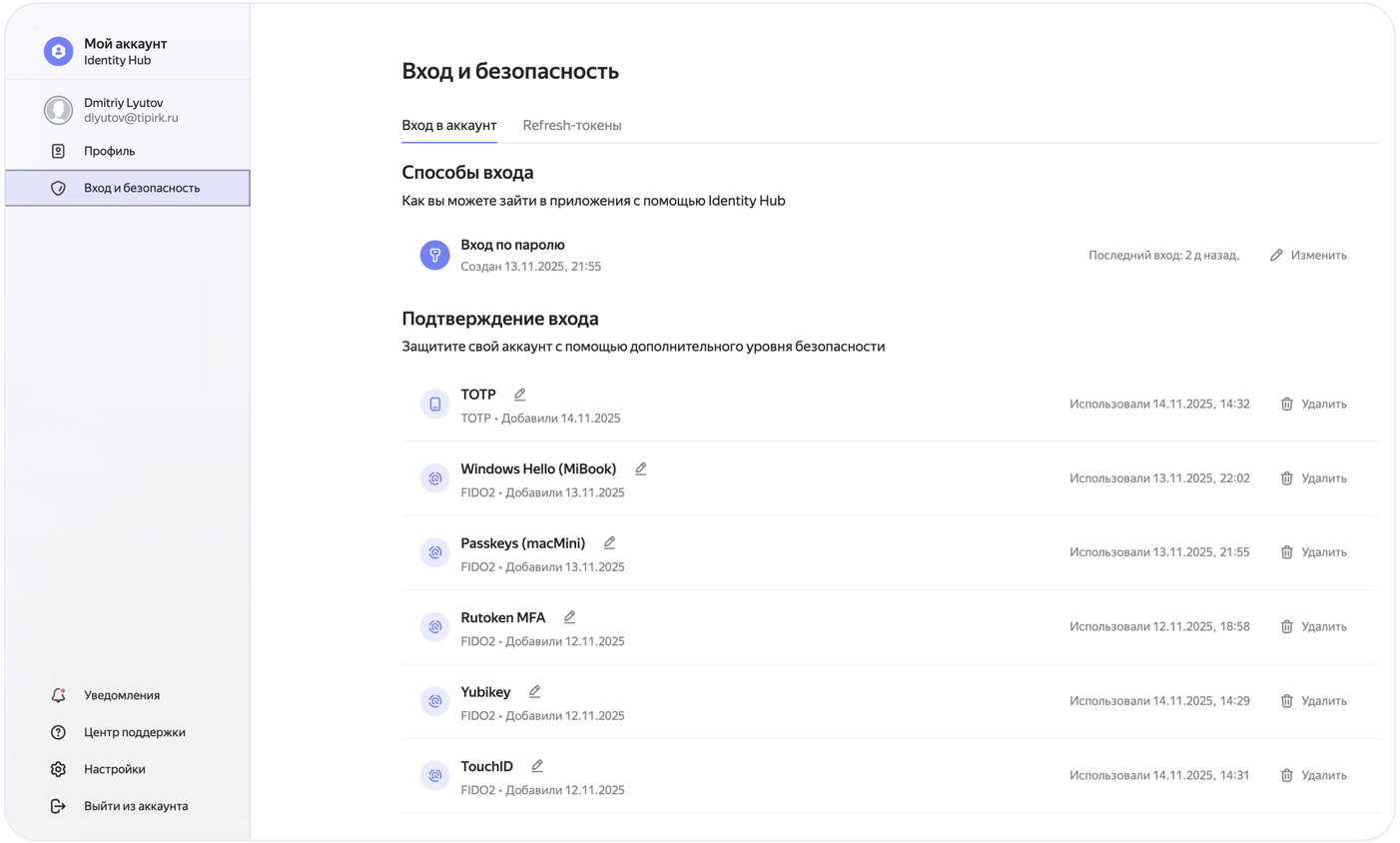
Аудит пользовательской активности

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



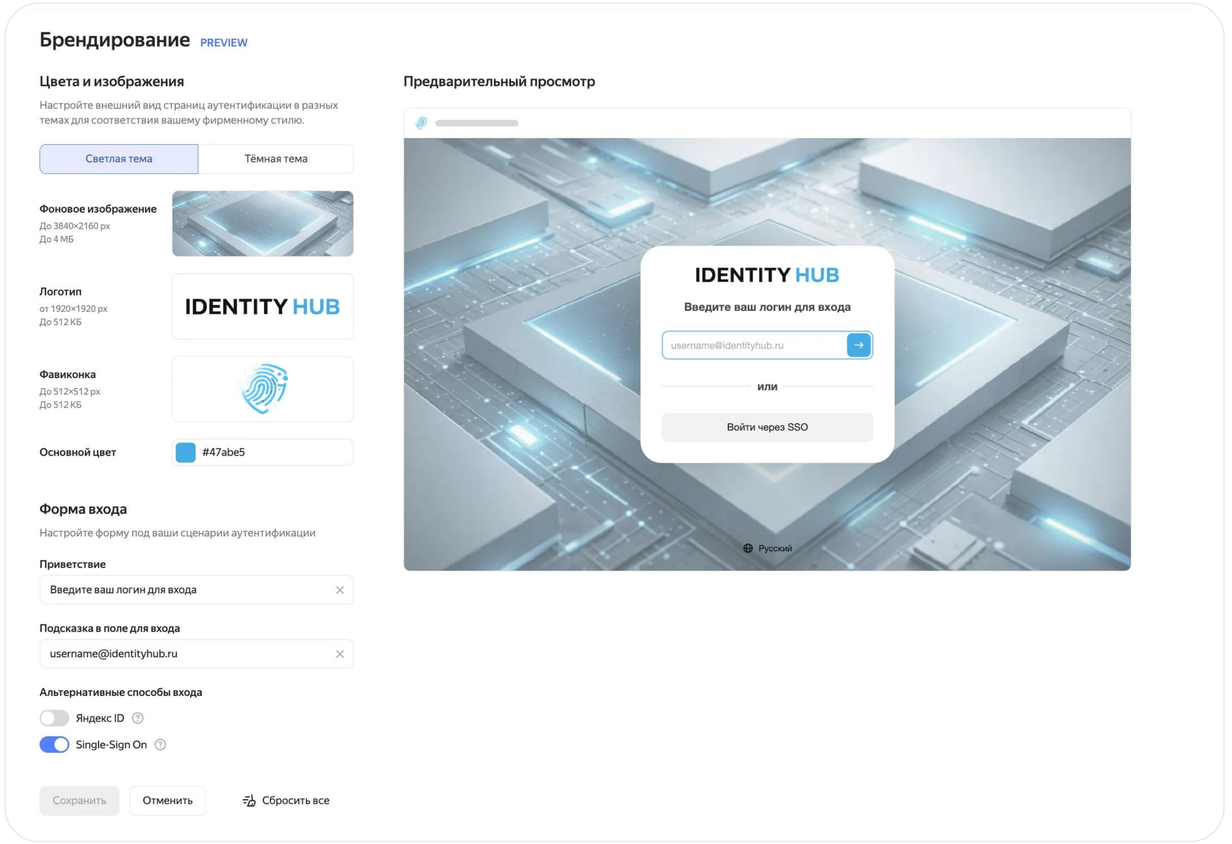
Портал
Мой аккаунт

- 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



Брендирование

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



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

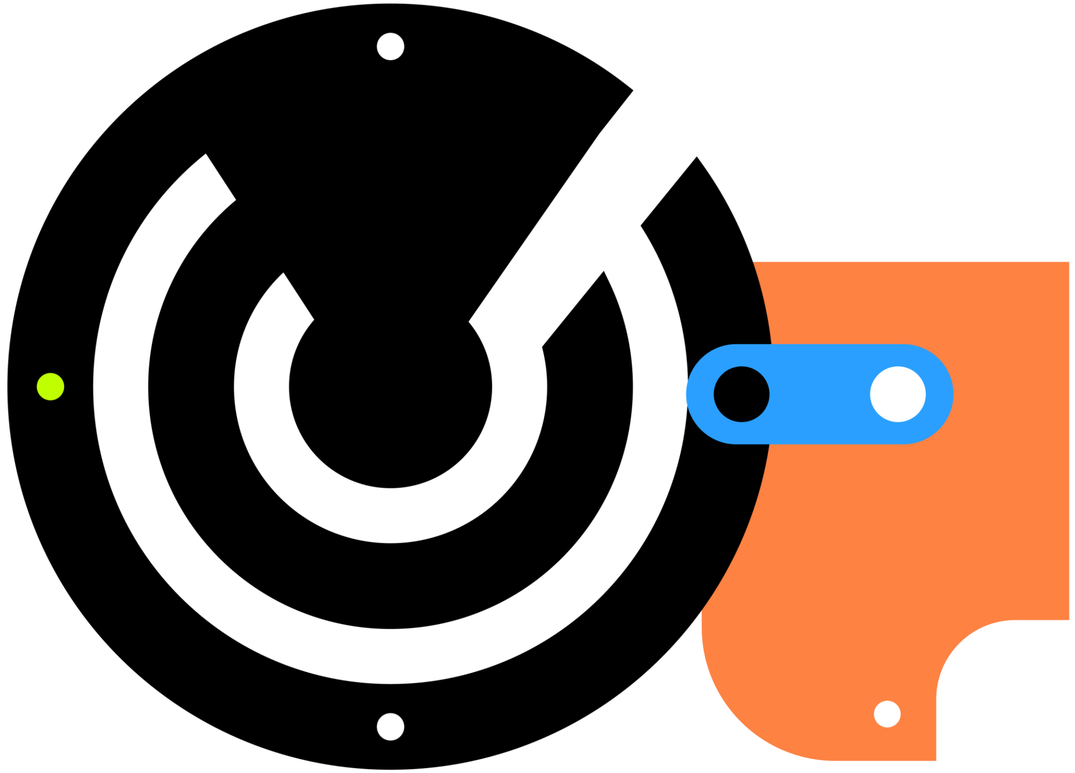
Стоимость использования сервиса Yandex Identity Hub входит в стоимость оплачиваемых сервисов

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

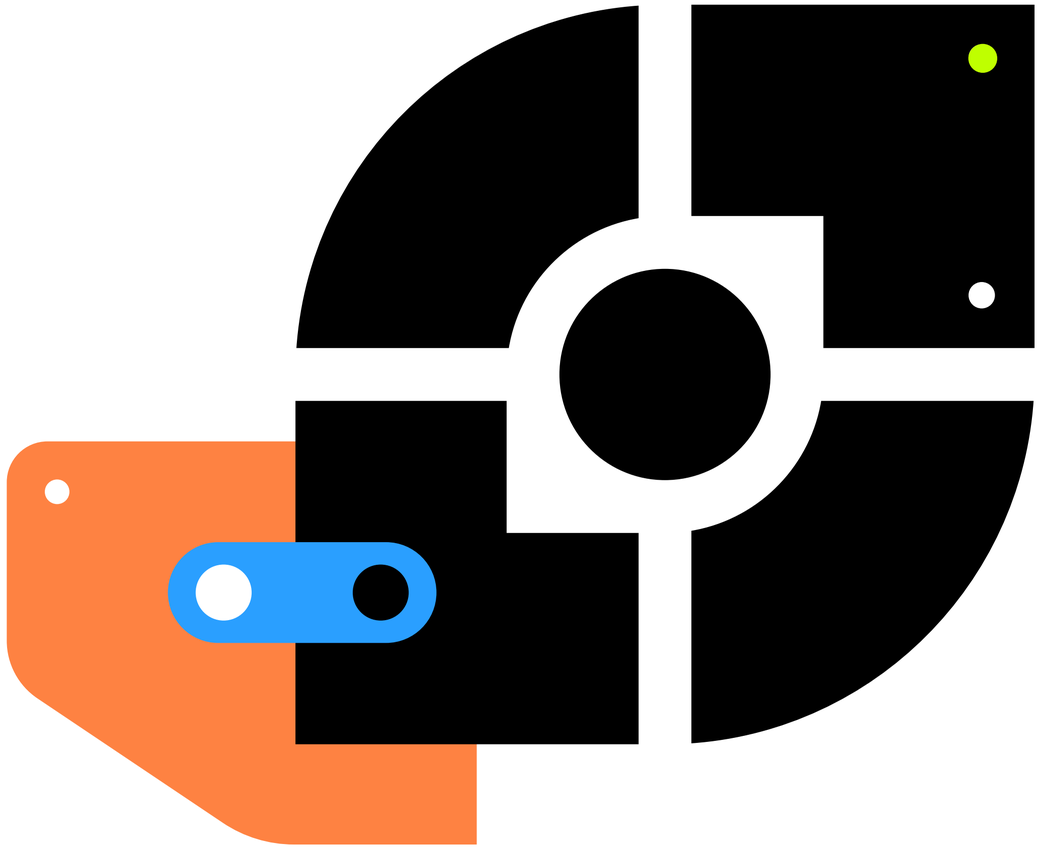
Ценообразование

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

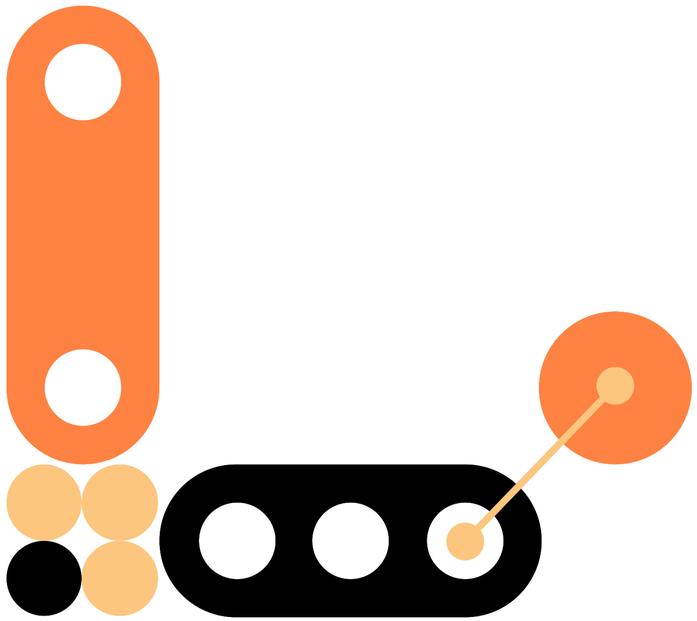
Собственная SIEM-система на базе технологий Яндекс



Рынок SIEM

Зрелый рынок,
но проблемы не исчезли

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**
  Обрабатывает 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

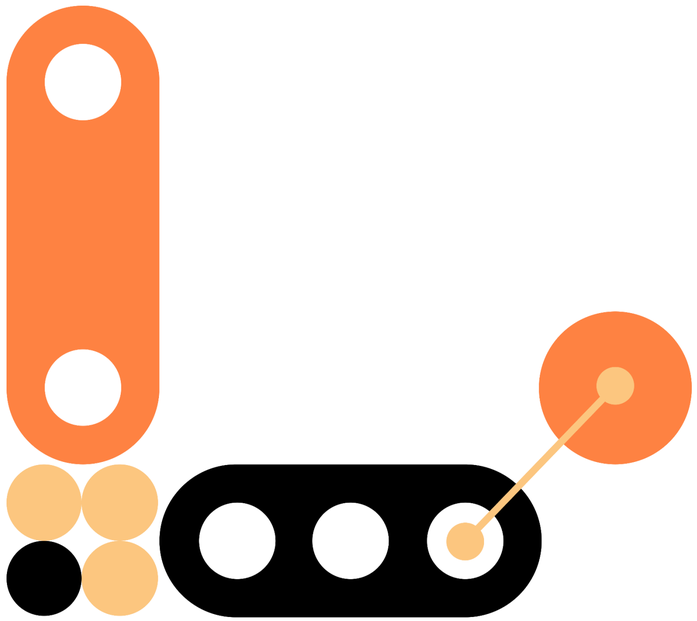
Тарификация

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.

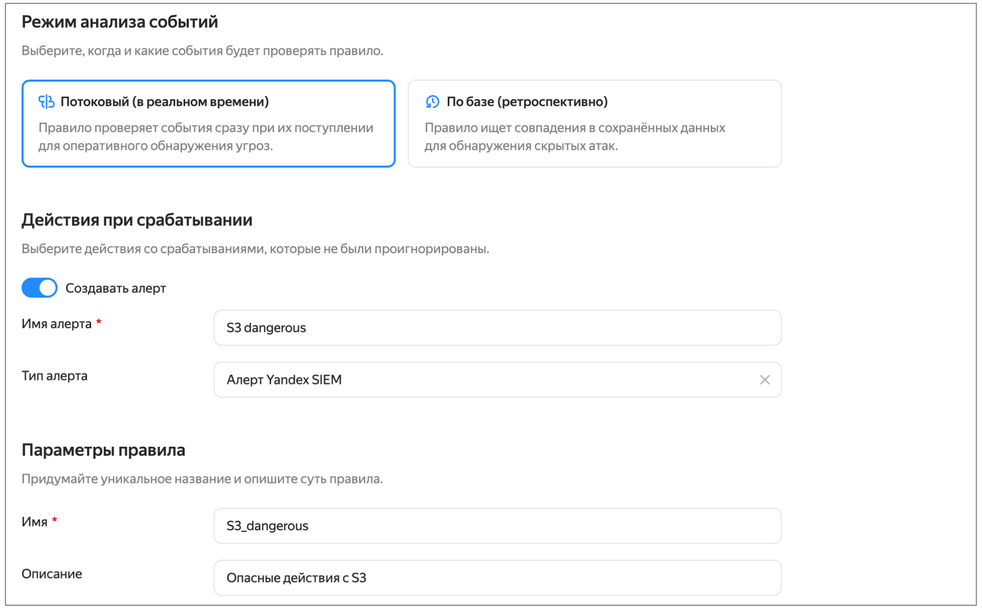
Сценарии использования

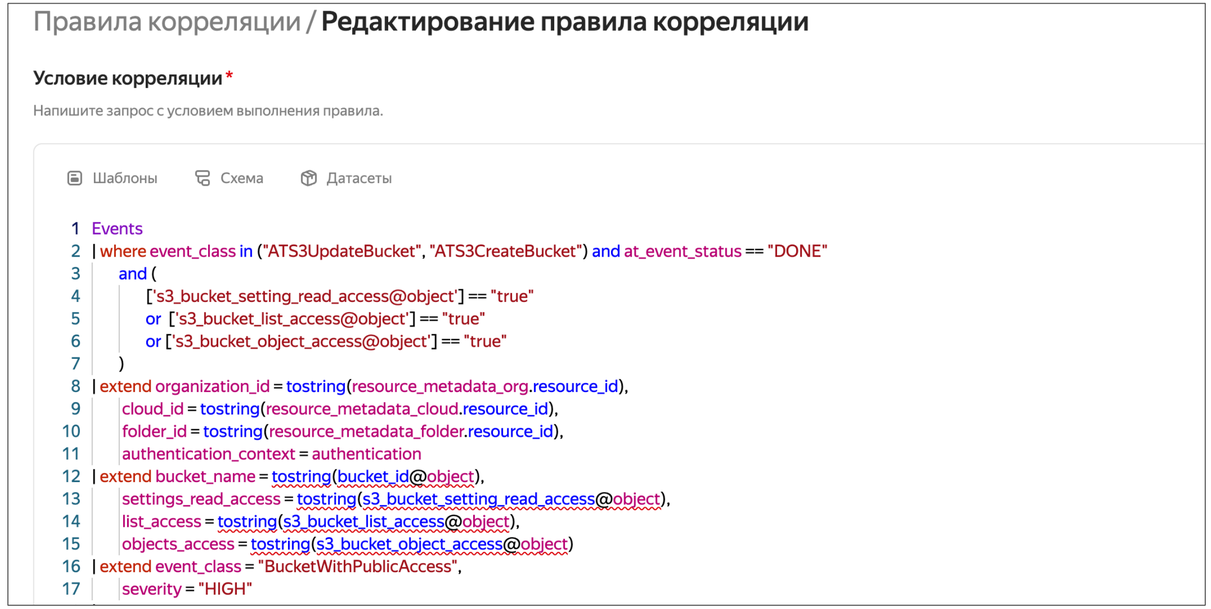


- Сбор событий из облачной и on-premises инфраструктуры
- Потоковая корреляция и детектирование угроз в реальном времени
- Поиск по сырым событиям и нормализованной телеметрии
- Триаж и приоритизация сработок с учётом контекста
- Расследование инцидентов и реагирование из единого окна
- ИИ-помощник для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

Возможности

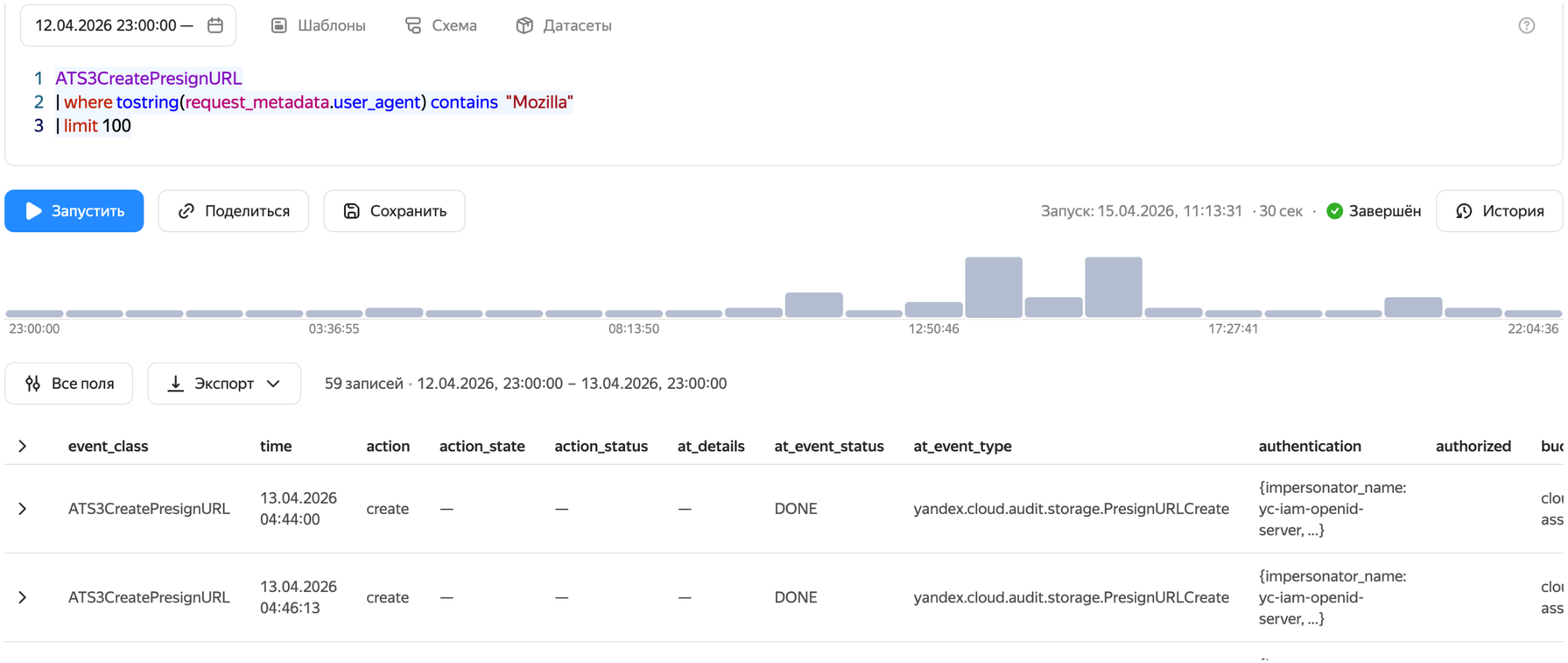
Правила корреляции: потоковые и по расписанию





Возможности

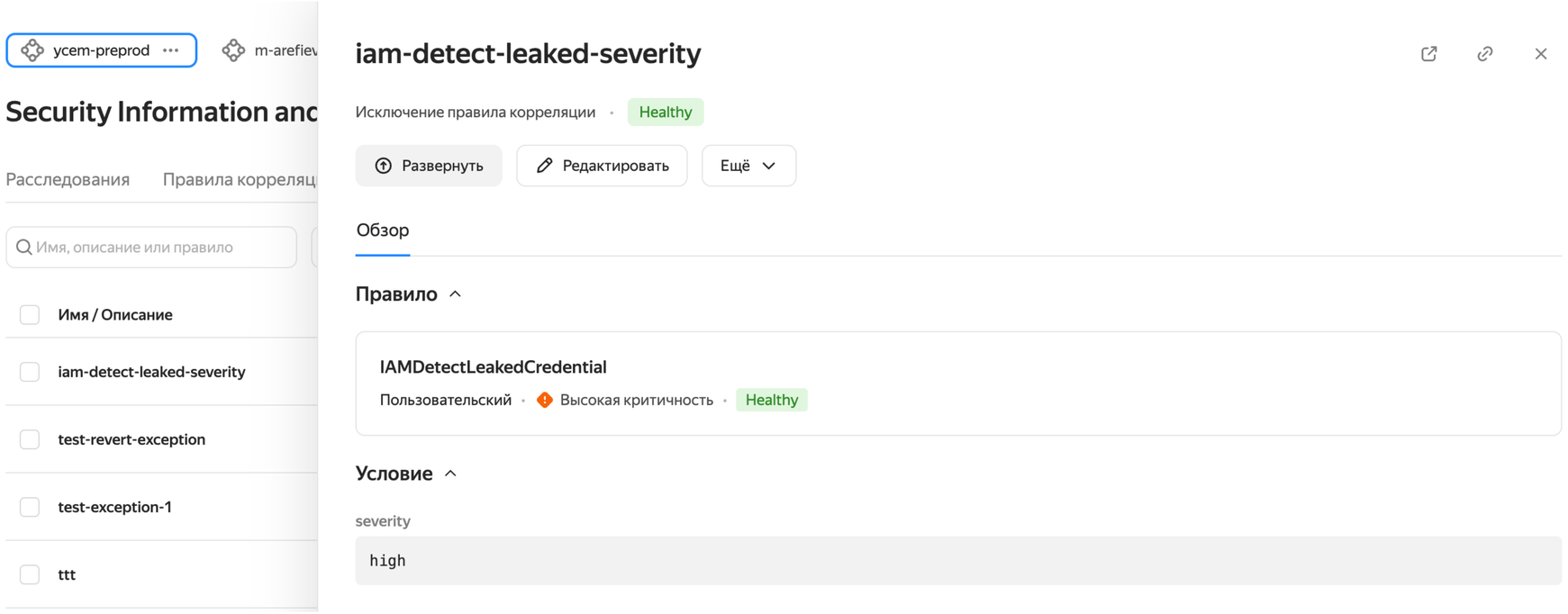
Расследования инцидентов



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

Возможности

Исключения



Возможности

Алертинг

с ИИ-ассистентом

Для виртуальной машины добавлен публичный IP-адрес

Открыт · Средняя · 15.04.2026, 11:00 · al3getka988larpfrtn1

Для виртуальной машины `fv482l4a43srdsa0tcoj` 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: `fv482l4a43srdsa0tcoj`

AI-ассистент PREVIEW

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 fv482l4a43srdsa0tcoj был добавлен публичный IP-адрес. Это может увеличить поверхность атаки, привести к несанкционированному доступу или утечке данных.
- **Технические детали:** виртуальная машина fv482l4a43srdsa0tcoj, 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»

Сильная команда

400+
Сотрудников в Управлении ИБ

300
Из них технические специалисты

1000+
Проектов по ИБ ежегодно

Поддержка отраслевой экспертизы

Топ-2

Топ-100 российских ИТ-поставщиков решений для защиты информации

Преимущества сотрудничества с компанией «Софтлайн Решения»:

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

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

appsec@softline.com