

Zero Trust на уровне веб-сессий

Как SEB даёт SOC видимость и контроль



Дмитрий Мажарцев

Директор по информационной безопасности

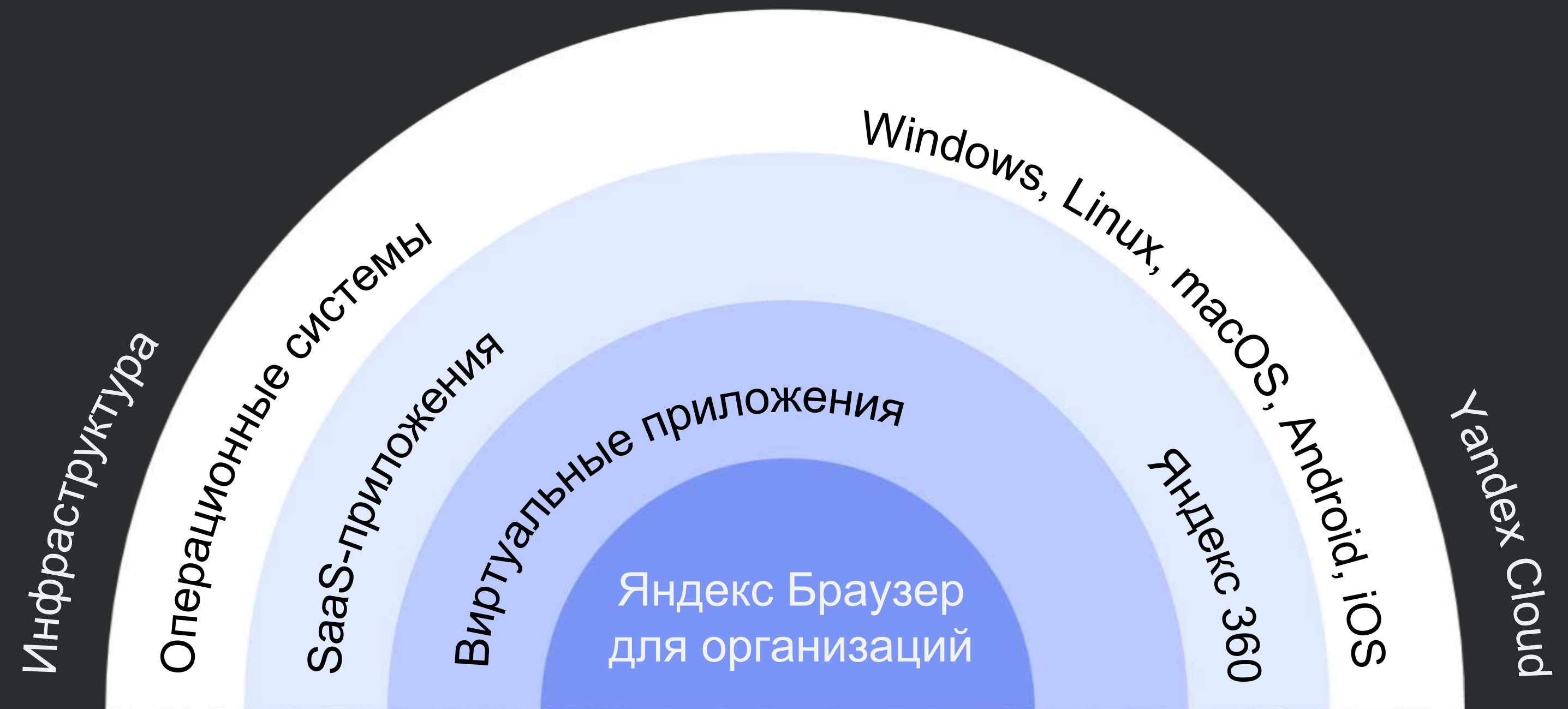
Яндекс Браузер для организаций

Всё стремится в веб

- 1 Всё больше задач выполняется в вебе
- 2 Увеличивается количество SaaS-приложений
- 3 80% бизнес-процессов происходит в браузере
- 4 SOC теряет видимость внутри веб-сессий
- 5 Классические средства защиты не дают детального контекста действий пользователя в браузере



Формат взаимодействия становится
браузероцентричным



Типовые проблемы SOC в веб-сессиях

Ограниченная видимость действий в SaaS

Утечки данных через браузер.

Copy-paste, скриншоты, DevTools, расширения, CDP

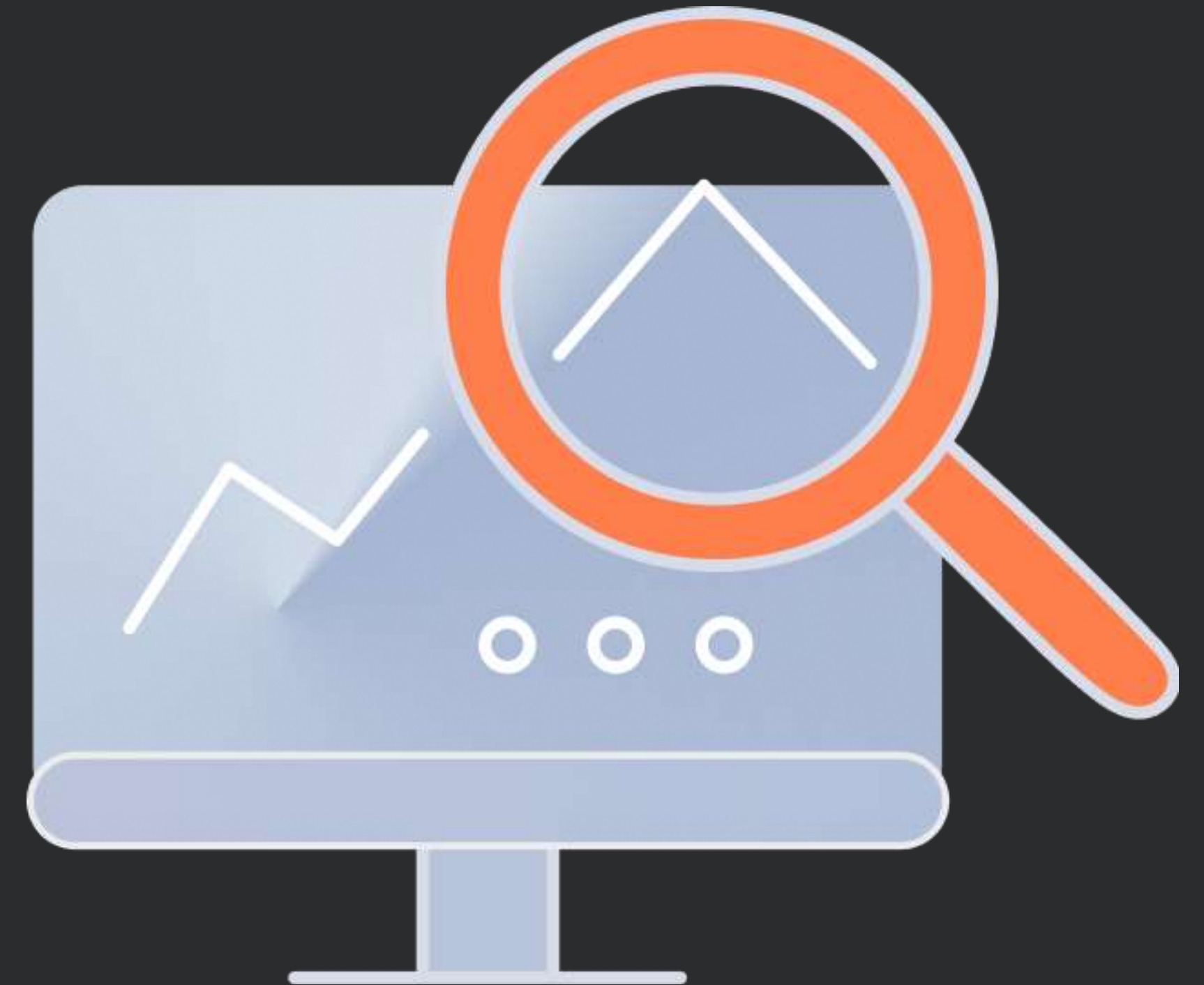
Сложность корреляции событий
между браузером и SIEM

Пользователи работают с чувствительными
данными вне корпоративной
сети и с неуправляемых устройств



Влияние на SOC

- ✓ Реагирование постфактум
- ✓ Увеличение MTTR
- ✓ Отсутствие контекста для расследований
- ✓ Ложные срабатывания
- ✓ Повышенная нагрузка на аналитиков SOC



Zero Trust: переход от периметра к сессии

Эволюция контроля



Раньше

Защита периметра



Потом

Контроль доступа



Теперь

Контроль действий
в веб-сессии



Zero Trust = проверяй
всегда, даже внутри
авторизованных сессий



SEB как точка
внедрения Zero Trust
в реальном времени



Что такое Secure Enterprise Browser

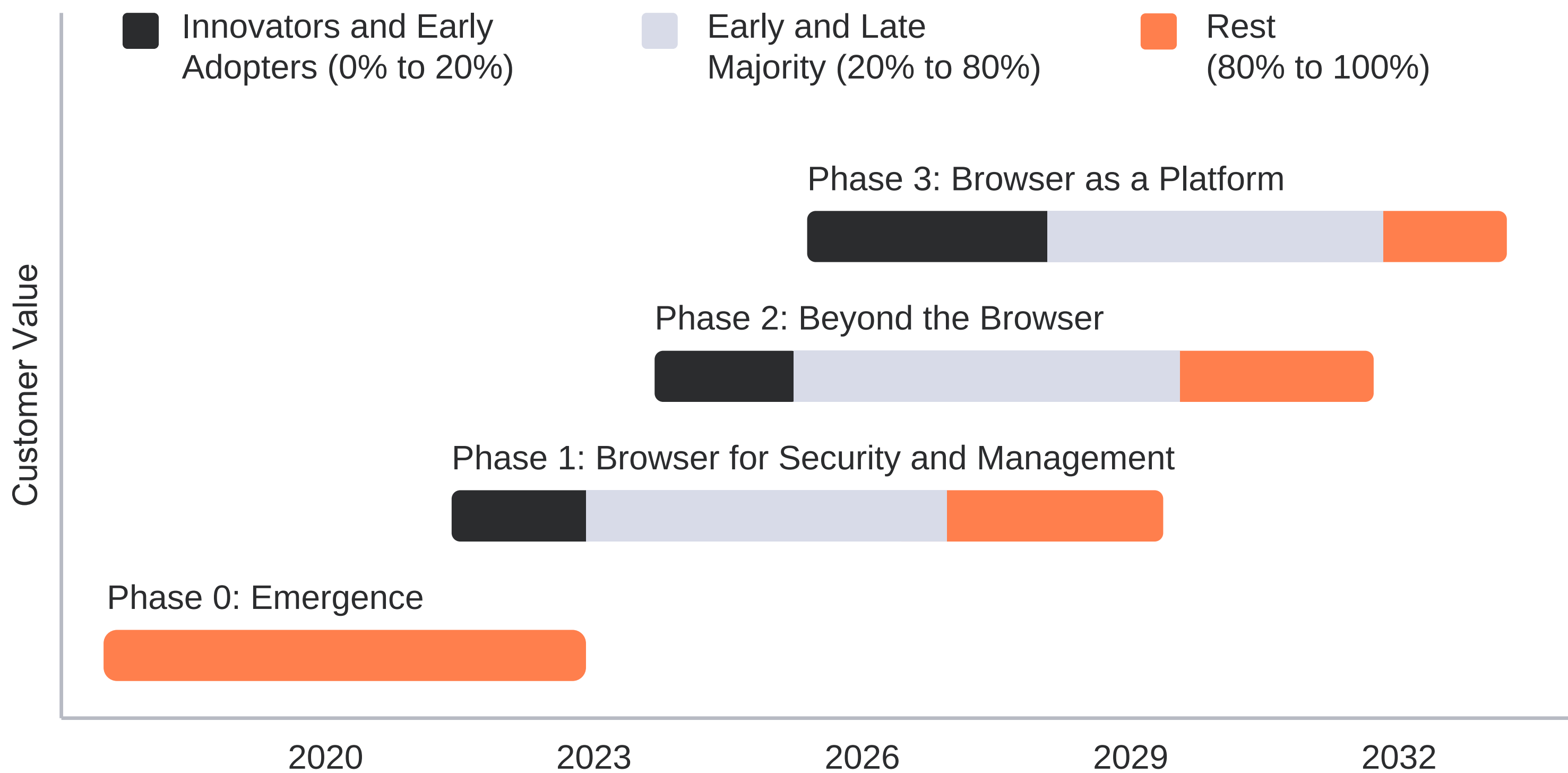
SEB: контроль в точке входа

- 1 SEB = корпоративный браузер со встроенными модулями безопасности
- 2 Встраивается между пользователем и веб-приложением
- 3 Позволяет применять политики Zero Trust на уровне веб-сессий
- 4 Даёт полную телеметрию действий пользователя



От браузера к платформе безопасности

Evolution Spectrum for Secure Enterprise Browsers



Source: Gartner 782989_C

«Браузер — ключевой элемент безопасности компаний»

Gartner®



Яндекс Браузер для организаций

Управляемый и безопасный доступ к веб-ресурсам

17 тыс.

компаний выбрали
корпоративную версию

3,5 млн

сотрудников регулярно
используют браузер



Российский браузер для безопасной работы в вебе
и защиты данных компании, интегрируемый
в ИБ-инфраструктуру, централизованно управляемый

1

Безопасность данных

- ✓ Защита от утечки данных (DLP)
- ✓ Обмен событиями и управление через ИБ-системы (SIEM/SOC)
- ✓ Отслеживание событий активности сотрудников и их экспорт в BI-систему

2

Управление

- ✓ Централизованное управление на десктопах и мобильных устройствах, во внешнем закрытом контуре
- ✓ Синхронизация со структурой организации (LDAP)
- ✓ Конфигурация браузера, состава корп. вкладок и расширений

3

Доступ с любых устройств

- ✓ Поддержка BYOD-сценариев для мобильных сотрудников
- ✓ Совместимость с MDM-системами
- ✓ Форсинг: доступ к рабочим сервисам только из Яндекс Браузера



Инструменты защиты



Защита от утечки данных

- Ограничение действий с данными
- Цифровые водяные знаки



Защита от вредоносных файлов и фишинга

- Защита от вредоносных расширений
- Защита от вредоносных загрузок
- Фильтрация контента
- Защита от фишинга и мошенничества



Защита данных

- Защита от обхода политик безопасности
- Защищённое хранилище (Tech Preview)
- Менеджер паролей
- Защита ПИН-кодом



Улучшение прозрачности и контроля

- События безопасности
- Проверка уровня безопасности устройства



Защита от утечки данных

- ✓ Защита от скриншотов
- ✓ Контроль доступа к буферу обмена
- ✓ Защита от перехвата видео- и аудиопотоков
- ✓ Контроль доступа к печати
- ✓ Контроль выгрузки файлов
- ✓ Контроль сохранения страниц сайтов
- ✓ Цифровые водяные знаки
- ✓ Интеграция с внешними DLP-решениями



События безопасности

Отправка событий безопасности в SIEM

- ✓ События навигации
- ✓ Контроль целостности модулей
- ✓ События процессов браузера
- ✓ Изменения групповых политик
- ✓ Блокировка вредоносного кода в расширениях
- ✓ Защита от вредоносных файлов
- ✓ Телеметрия
- ✓ Защита от фишинга и вредоносных страниц
- ✓ Защита от утечки данных
- ✓ Активность в браузере
- ✓ События рисков, связанных с паролями

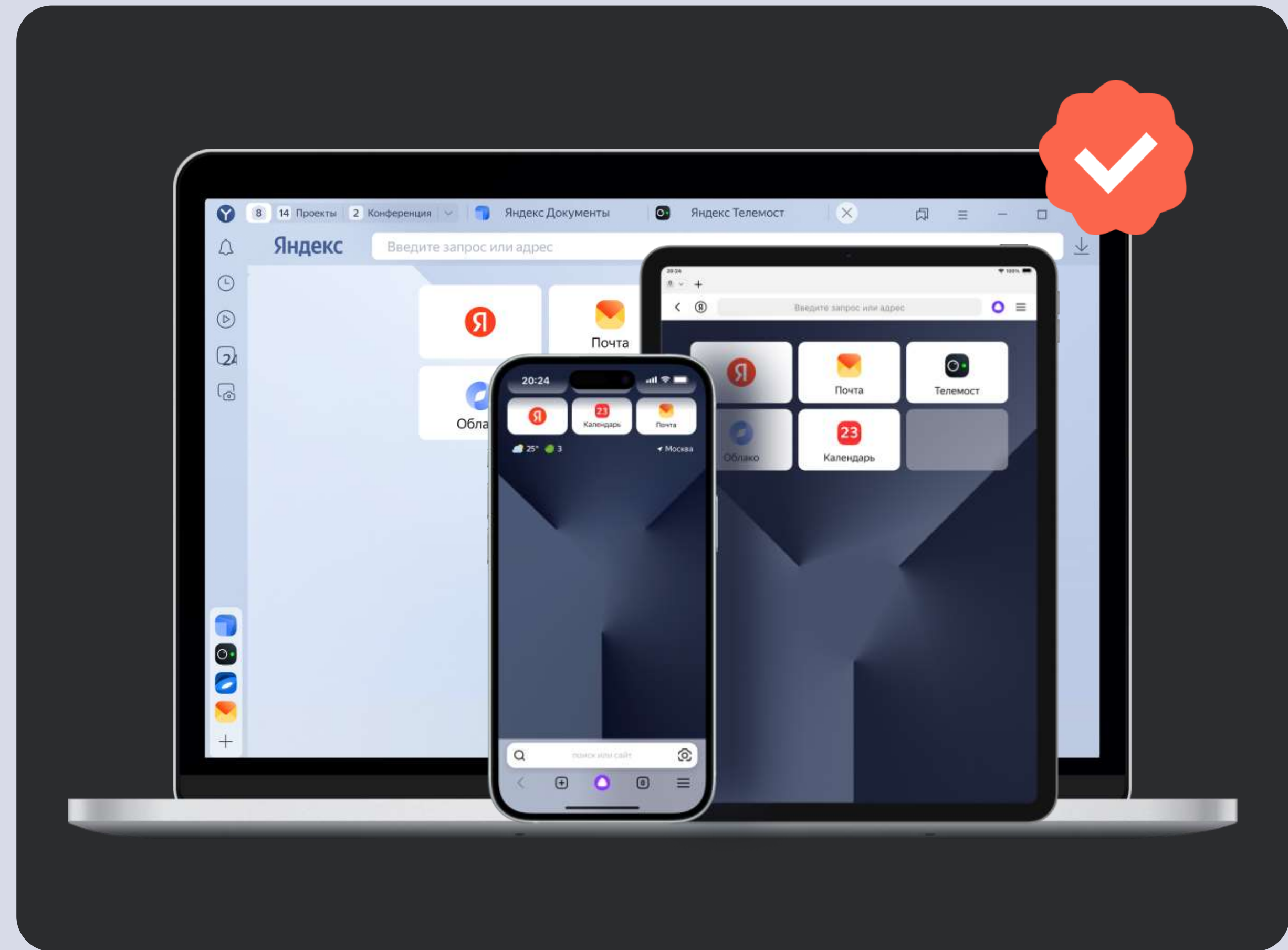


Проверка устройства на соответствие требованиям безопасности

Сбор технических данных
об устройстве пользователя

Проверка соответствия устройства
заданным политикам безопасности

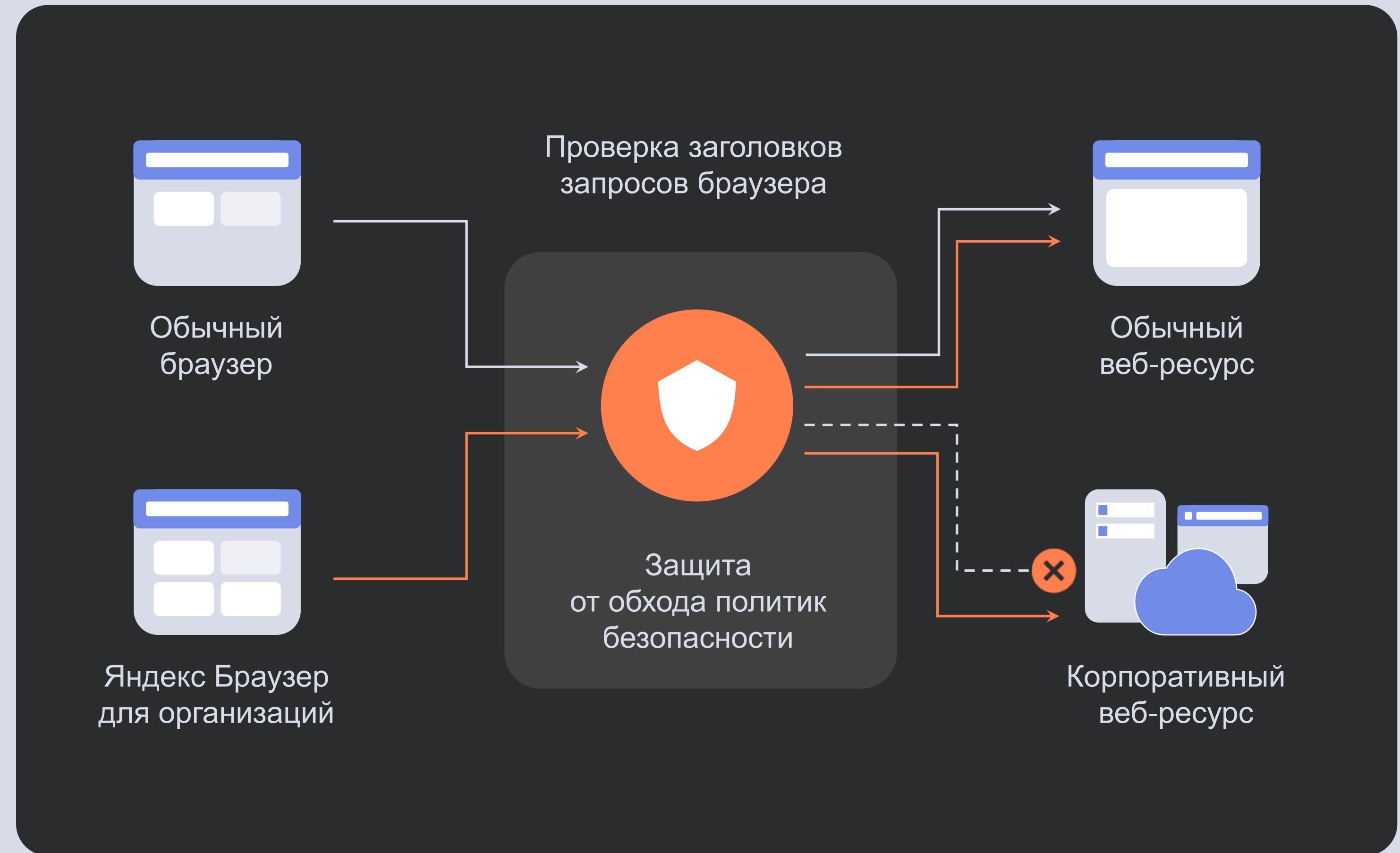
По результатам проверок предоставляет/
ограничивает доступ к ресурсам компании



Защита от обхода политик безопасности



Возможность проверки
подлинности защищённого
браузера в момент доступа
к корпоративным ресурсам



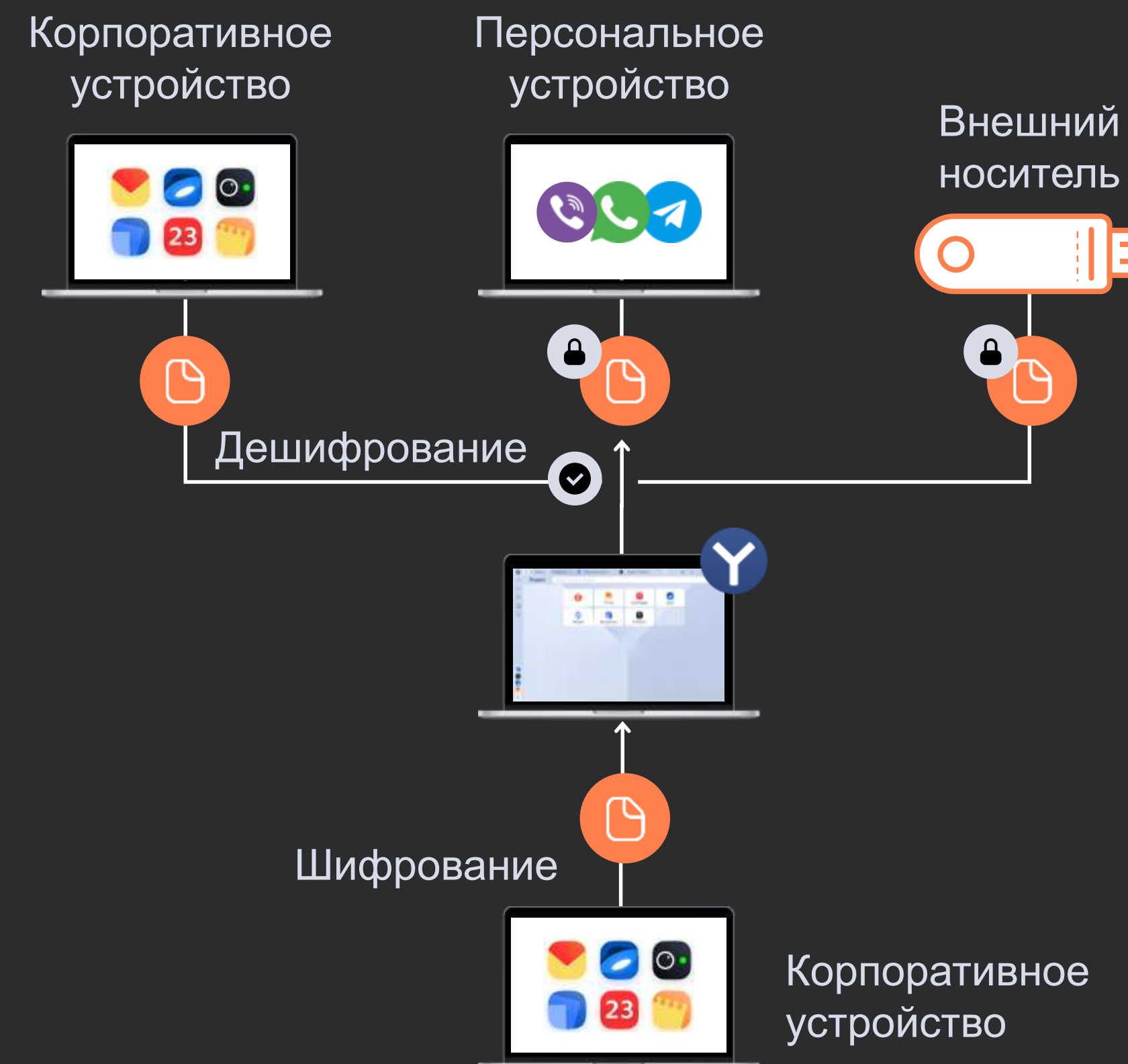
Защищённое хранилище

Tech Preview

Позволяет безопасно хранить конфиденциальные данные в контуре браузера

Данные надёжно зашифрованы

При передаче на незащищаемые ресурсы данные остаются зашифрованными



Централизованное управление

- 

Централизованное управление

Управление расширениями, лицензиями и обновлениями, поддержка API управления
- 

Консоль управления в закрытом контуре

Возможность развёртывания консоли внутри контура, синхронизация с AD, ролевая модель, аудит и другие возможности
- 

Конструктор браузера

Возможность создавать кастомные сборки со своими настройками политик для различных платформ



Яндекс Браузер

Моя компания

Скачать

Купить

Моя компания

Устройства

Браузеры

Профили

Расширения

Что нового?

API-токены

Поддержка

Справка

Попробуйте расширенную версию

Усиленная безопасность и выделенная поддержка

Сравнить версии

Назад

I11667656

Имя устройства

I11667656

Версия ОС

Windows 11 (10.0.22621.3007)

Дата ак

25.06.2

Machine user

LD\mazhartsev

Serial number

C24T3M3

Device

abb2fa7

Применённые политики

8

Последняя активность

12.02.2024, 09:20

Лиценз

До 31 д

Профиль в браузере

Profile 1

Установленные расширения

Расширение	Статус	Версия	Тип установки	id расширения
Google Translate	Активно	2.0.13	Администратор	aapbdbdomjkkjk
Momentum	Активно	4.2.6.0	Самостоятельно	laookkfknppbbbf
Turn Off the Lights	Активно	1.73.0 [1.73.6]	Самостоятельно	bfbmjmiodbnnpl
Volume Master	Активно	1.14.4	Администратор	jghecgabfgfdldn

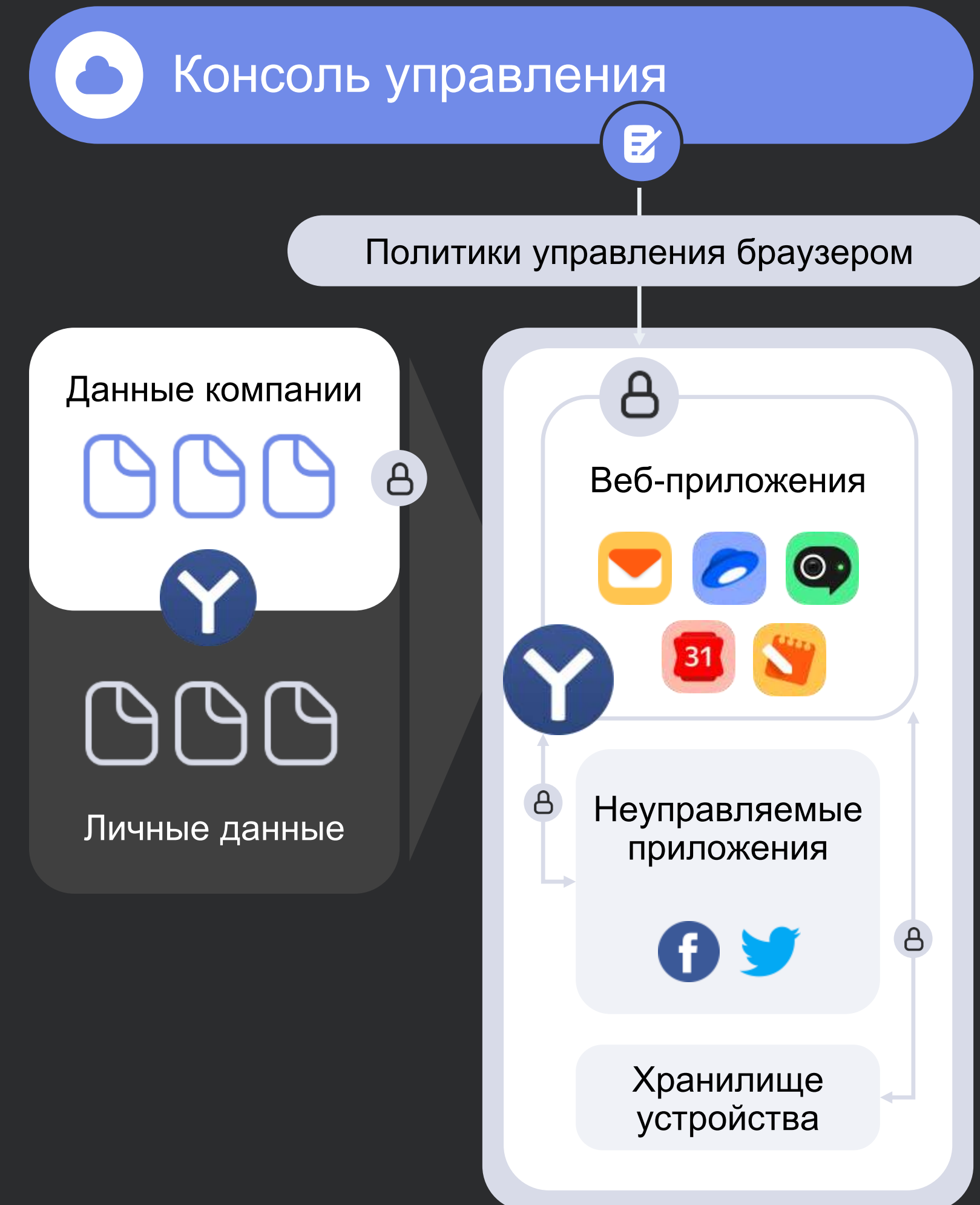
Настроенные политики

Разработчик

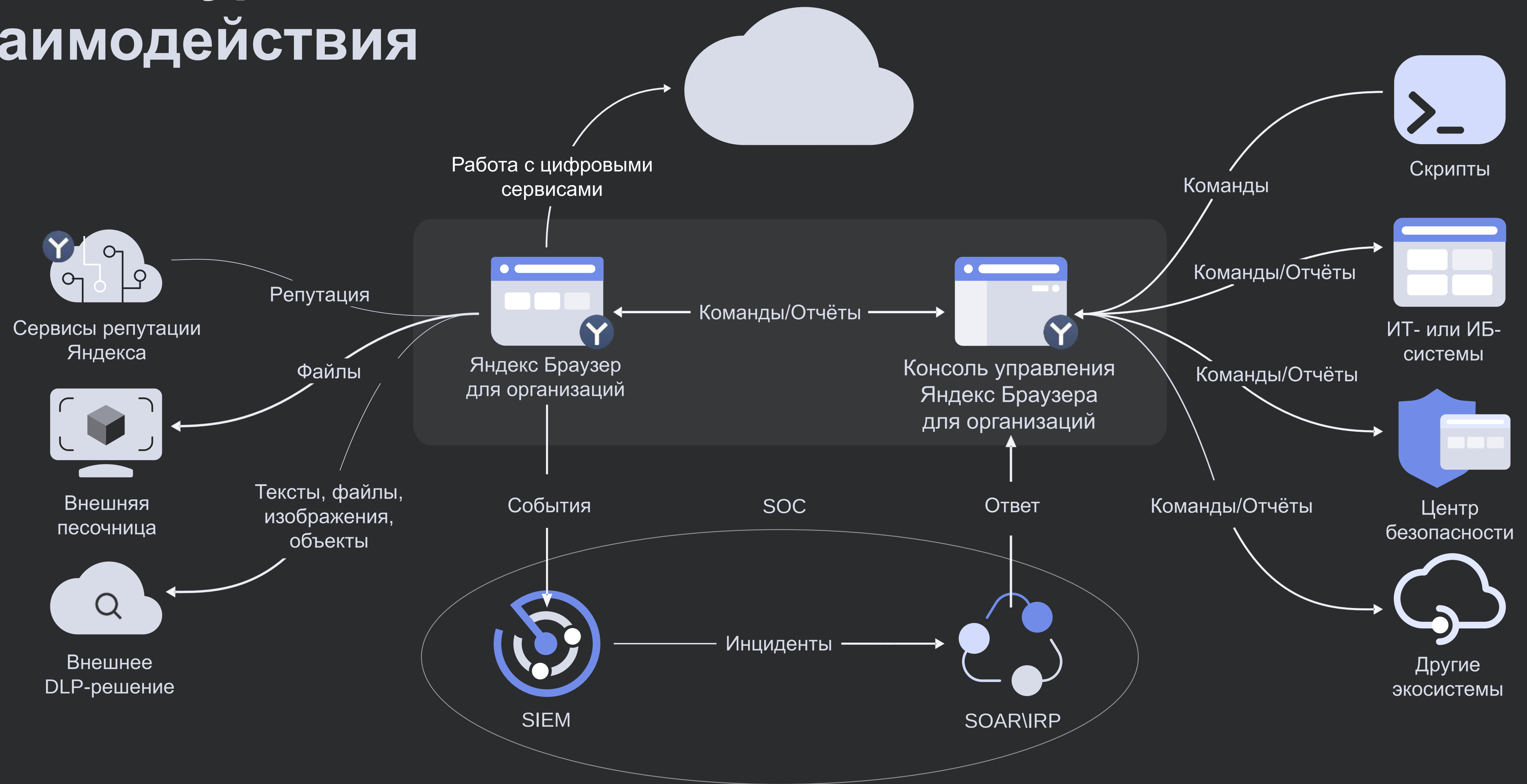
Защита корпоративных данных при BYOD-подходе

Возможность защитить рабочие данные на личных устройствах сотрудников

- ✓ Защита от утечки данных
- ✓ Защита от обхода политик безопасности
- ✓ Проверка уровня безопасности устройств
- ✓ Защищённое хранилище (Tech Preview)
- ✓ Защита браузера паролем
- ✓ События безопасности
- ✓ Централизованное управление



Архитектура взаимодействия



Как SEB помогает SOC

Новая видимость для SOC



События из SEB дают
детальный контекст:
**кто, где, когда и что
делал** в веб-сессии

Примеры

- Выгрузка конфиденциального файла
- Ввод доменного пароля на «левых» сайтах
- Попытка доступа к веб-приложению с устройства, нарушающего compliance
- ...



Привязка
к пользователю
и устройству



События



SIEM



Реакция в реальном времени через API

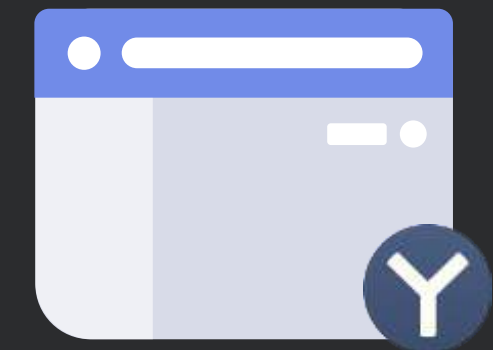


Автоматическое реагирование

- Блокировать действие
- Принудительно завершить сессию
- Ввести MFA

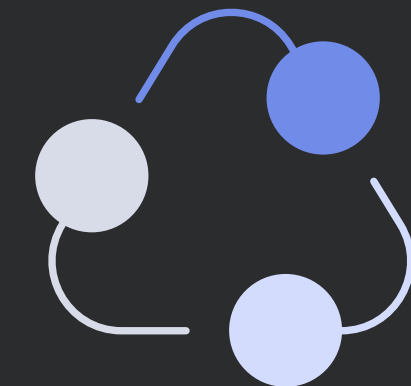


Инциденты фиксируются мгновенно, а не через часы



Консоль управления
Яндекс Браузера для организаций

↑
Ответ



SOAR/IRP



Усиление DLP

SEB как точка контроля данных

- ✓ Контроль последней мили
- ✓ Защита от видео- и аудиозахвата
- ✓ Защита водяными знаками
- ✓ Интеграция с внешними DLP

События DLP → SIEM → Аналитик SOC



Практические сценарии применения



Безопасный доступ с любых устройств

- Защита от обхода политик безопасности
- Инвентаризация устройств
- Проверка уровня безопасности
- Защита загружаемых данных



Защита от кражи учётных записей

- Обнаружение ввода защищаемых паролей на внешних ресурсах
- Обнаружение событий безопасности в SIEM
- Отправка сотрудника на страницу сброса пароля



Защита от утечек данных

- Защищённое хранилище
- Контроль потоков данных в браузере (выгрузка/загрузка, печать, буфер обмена, сохранение данных)
- Защита от скриншотов, захвата экрана браузера (шеринг экрана)
- Защита контента при помощи цифровых водяных знаков
- Интеграция с внешними DPL-решениями



Практические сценарии применения



Защита от вредоносных решений

- Полный контроль за всеми расширениями организации
- Блокировка вредоносных расширений
- Ограничение доступов
- Полная блокировка доступа расширений



Предотвращение «Теневого IT»

- Обнаружение «теневого IT»
- Предотвращение утечек
- Предотвращение доступов



Защита от веб-угроз

- Защита от фишинга
- Защита от загрузки вредоносных файлов
- Защита от недостоверных веб-ресурсов и сертификатов
- Защита от уязвимостей нулевого дня



Централизованное управление

- Консоль управления
- API консоли управления
- On-premises-версия консоли управления



Развитие SOC с SEB

1

Повышение эффективности SOC

- Сокращение MTTR
- Меньше ручных расследований
- Лучше качество данных

2

Поддержка стратегии Zero Trust на прикладном уровне

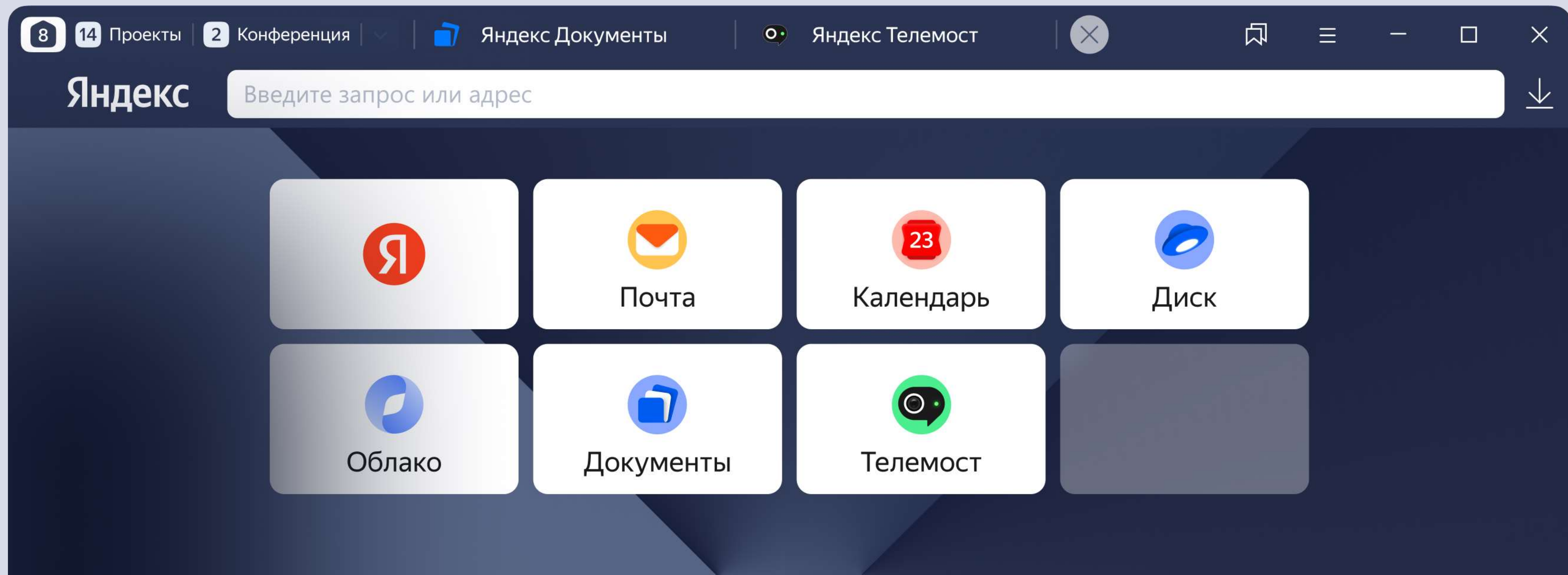
3

Масштабирование без увеличения штата



SEB — новая точка контроля для SOC

Превращает браузер из «чёрного ящика» в управляемую зону Zero Trust.
Укрепление DLP и SIEM. Ускорение реагирования



Спасибо

Будем рады встречным
идеям и предложениям

Подписывайтесь на телеграм-канал
Яндекс Браузера для организаций

