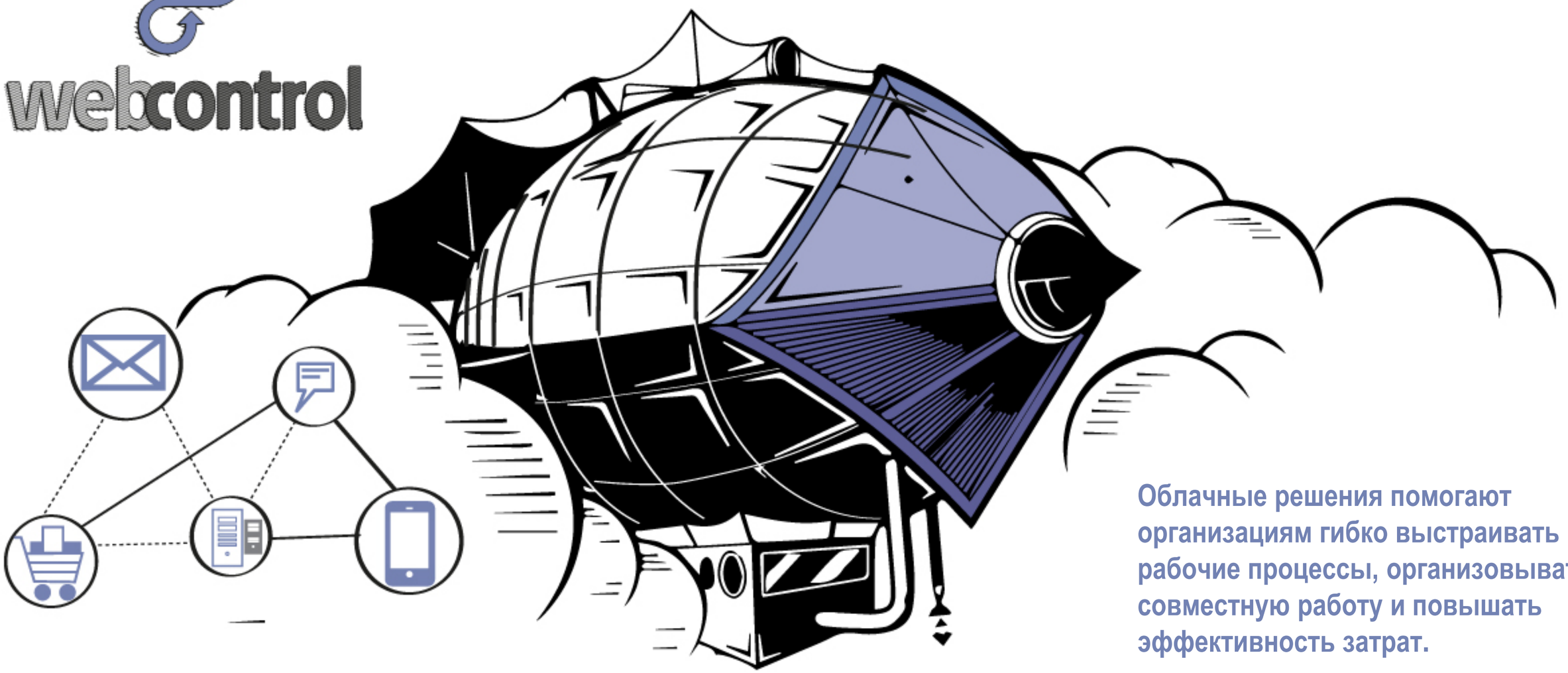
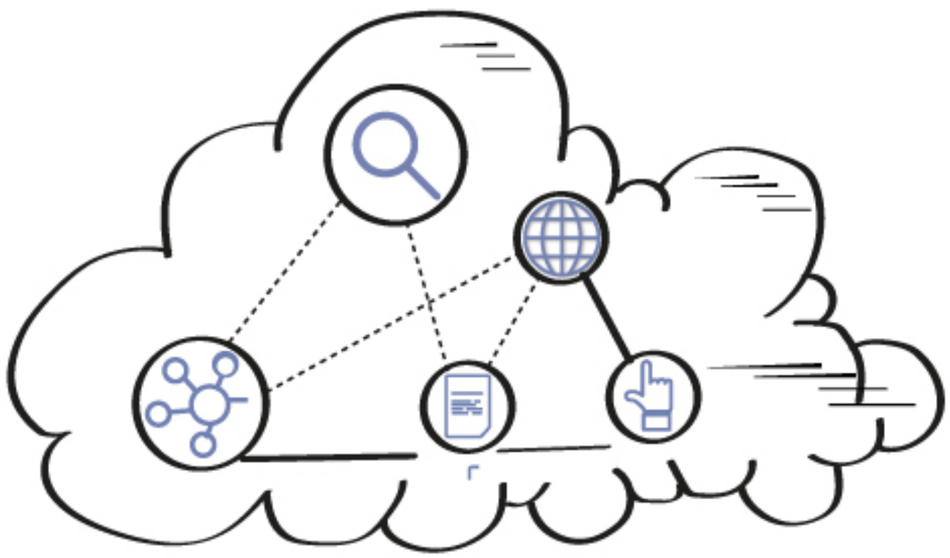
webcontrol



Облачные решения помогают организациям гибко выстраивать рабочие процессы, организовывать совместную работу и повышать эффективность затрат.

Облачные сервисы требуют новых подходов в области защиты информации и информационной безопасности.



Облачные сервисы – технологии наступающего будущего

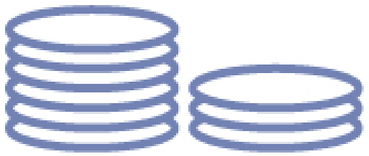
Перенос рабочих процессов в облако быстро переопределяет ИТ-инфраструктуру предприятия и открывает новые возможности для бизнеса. Традиционная ИТ-инфраструктура предприятий расширяется в сторону облачных приложений, таких как Office 365, Google Drive, Box, Dropbox, Web-сервисы Amazon, Oracle и Salesforce.

Сотрудничество

Облачные приложения и сервисы упрощают совместную работу пользователей независимо от их платформы (например, мобильной или настольной, Windows или MAC) или их местоположения.

Возможности

Люди могут работать эффективнее сразу после начала использования облачных сервисов



Экономика

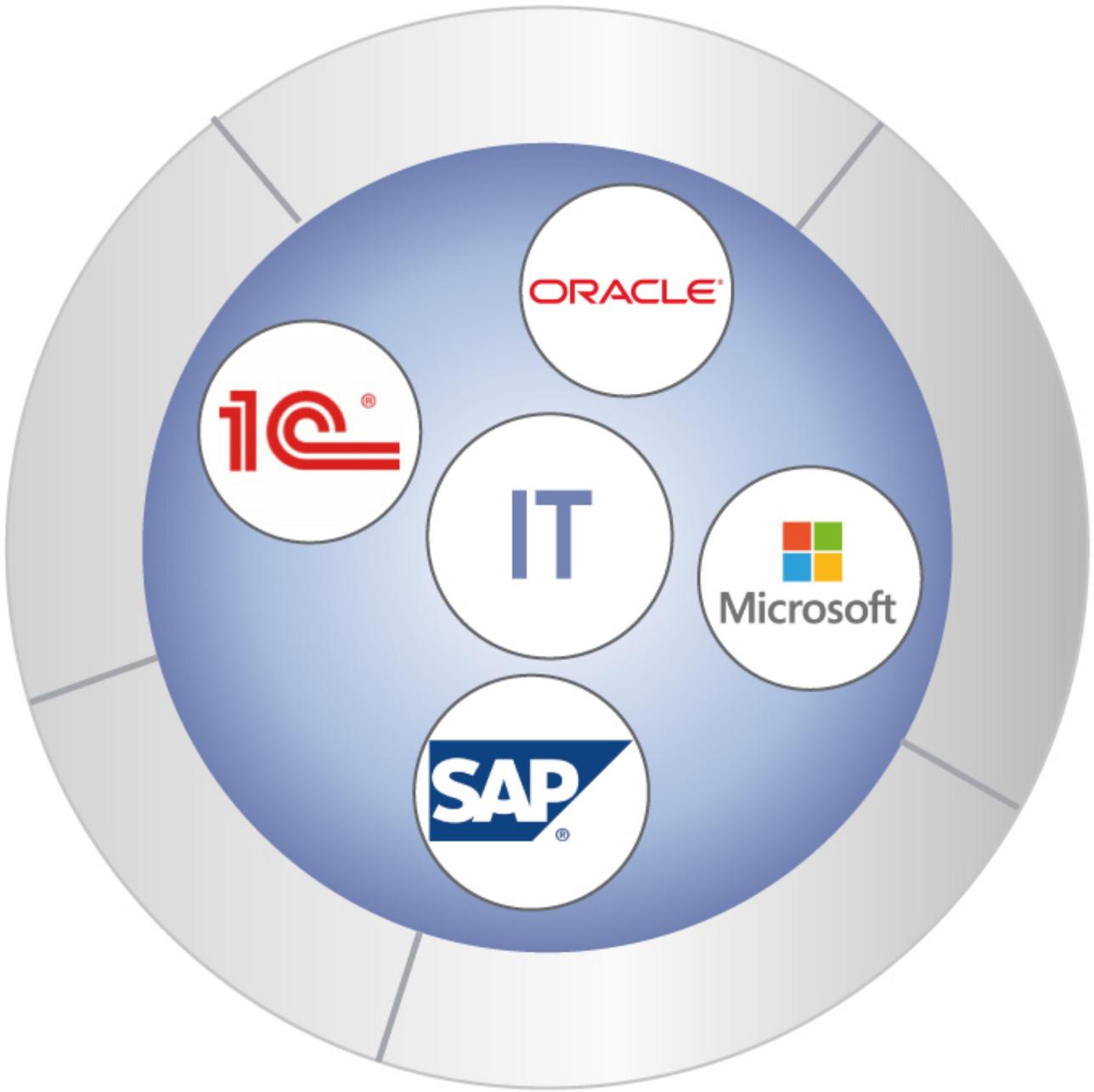
Модель на основе подписки устраняет капитальные затраты и позволяет гибко масштабировать услуги. Облачные приложения также устраняют эксплуатационные расходы, высвобождая ИТ-ресурсы и позволяя организациям сосредоточиться на своих основных компетенциях.

Выбор

Облачные приложения развиваются с огромной скоростью и обычно предлагают более конкурентоспособные решения, нежели локально установленное программное обеспечение. Кроме того, организации могут пробовать различные услуги и выбирать подходящие для своей среды, без обременительных обязательств.

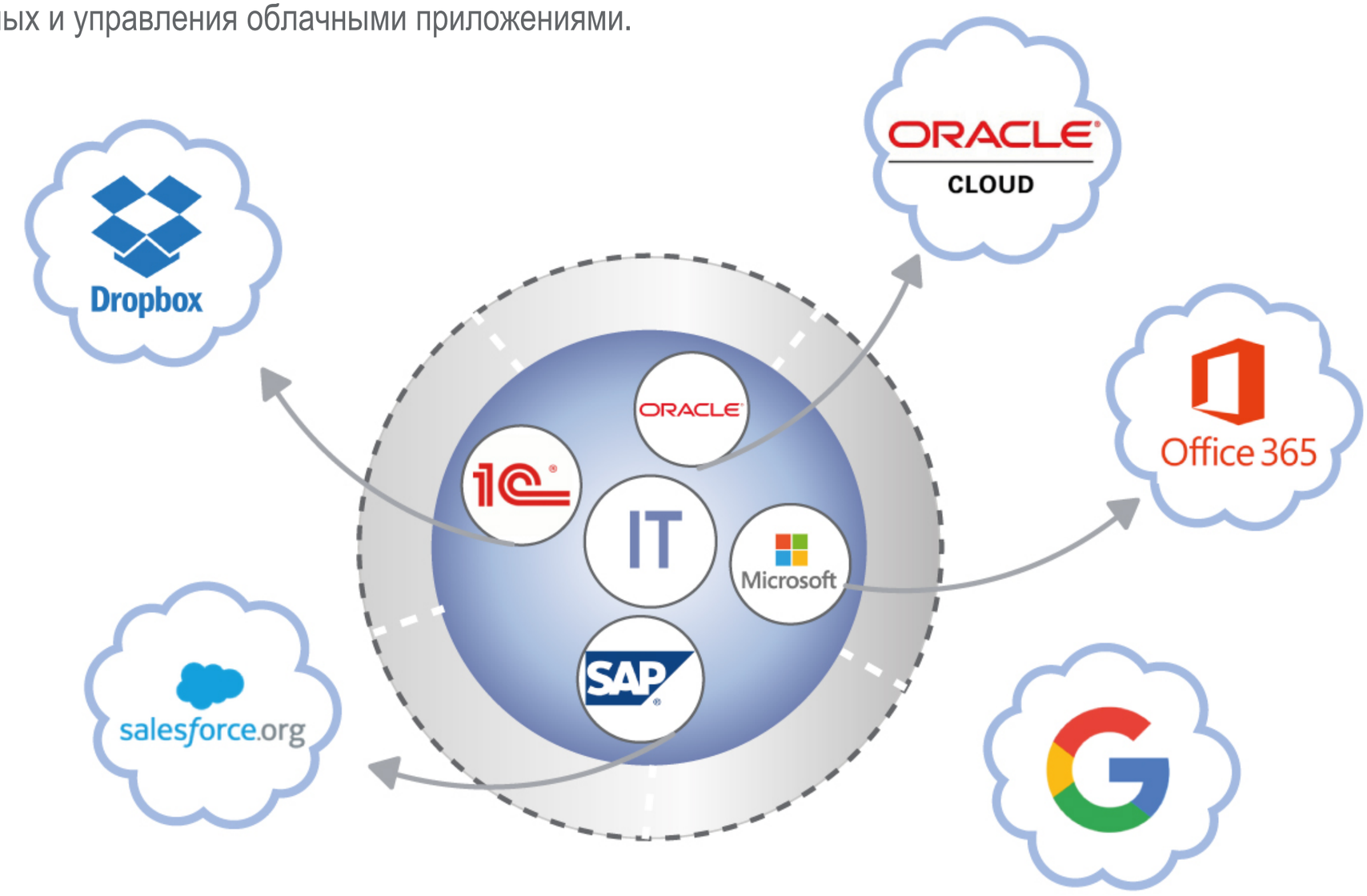
Миграция в облачный офис

Традиционная ИТ-инфраструктура, создаваемая предприятиями, расширяется по мере того, как компании начинают использовать такие облачные приложения, как Office 365, Google Drive, Box, Dropbox Amazon Web Services, Oracle и Salesforce.



Миграция в облачный офис

Хотя расширение в облаке имеет много преимуществ, для профессионалов в области информационной безопасности появляется непростая задача обеспечения контроля данных и управления облачными приложениями.



Подобно появлению других крупных информационных технологий, таких как электронная почта или Интернет, бурное «принятие» облачных приложений и сервисов порождает потребность в новом классе решений безопасности, которые помогают организациям защищать свои данные, которые находятся внутри облачных приложений.

Расширение корпоративной сети

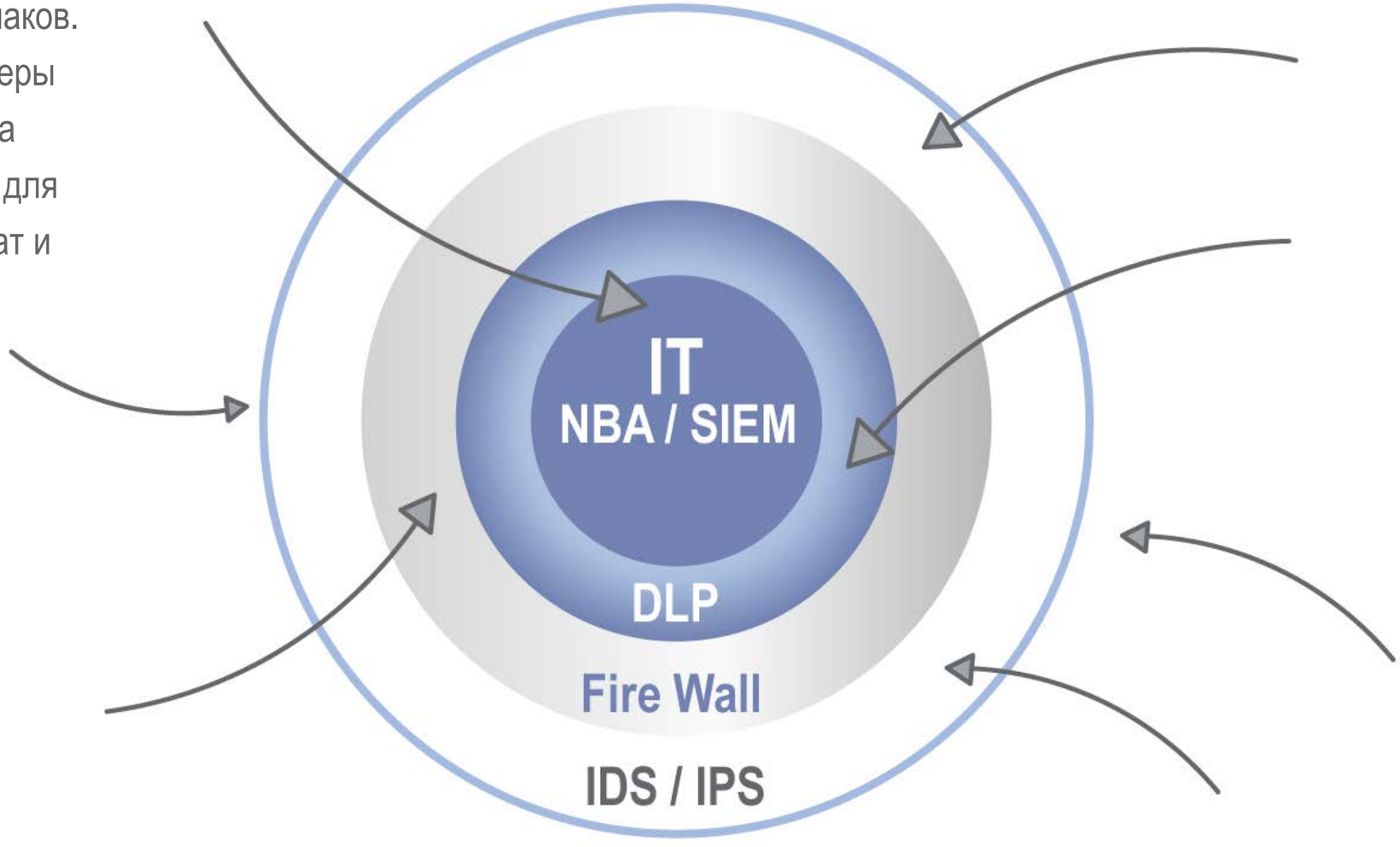
В новом мире повсеместного доступа к облакам растет доля критически важных для бизнеса данных в облаке, увеличивается объем трафика и бизнес-данных, передаваемых между сотрудниками в Интернет. Многие традиционные технологии безопасности, такие как брандмауэр, были разработаны для защиты сетевого периметра, но понятия «внутри» и «вне» сети стерлись. Облако стало де-факто расширением каждой организации. В этой новой реальности безопасность должна следовать за данными, следовать за приложениями и за пользователями.

Понятия
«внутри» и «вне»
сети стерлись

Работаем
в любых условиях

Переосмысление методологии в ИБ

Технологические слои безопасности, которые традиционно развернуты на предприятии, имеют слепое пятно в отношении облаков. Например, NGFW/UTM, IDS/IPS, сканеры уязвимостей, SIEM и системы анализа сетевого трафика были разработаны для защиты активов, которые принадлежат и управляются ИТ-службой.



В целом, эти системы не были предназначены для защиты корпоративных данных, передаваемых сторонним решениям, размещенным вне предприятия, и доступными пользователям откуда угодно. Потребность в этих традиционных функциях безопасности не исчезла, но требуется новая модель реализации, подходящая для защиты конфиденциальных данных в облачной среде.

Брокер безопасного доступа к облачным сервисам
(Cloud Access Security Brokers - CASB)

Термин «Shadow IT» означает подключение сторонних ИТ-решений, включая облачные приложения и службы, без надзора со стороны ИТ-службы.

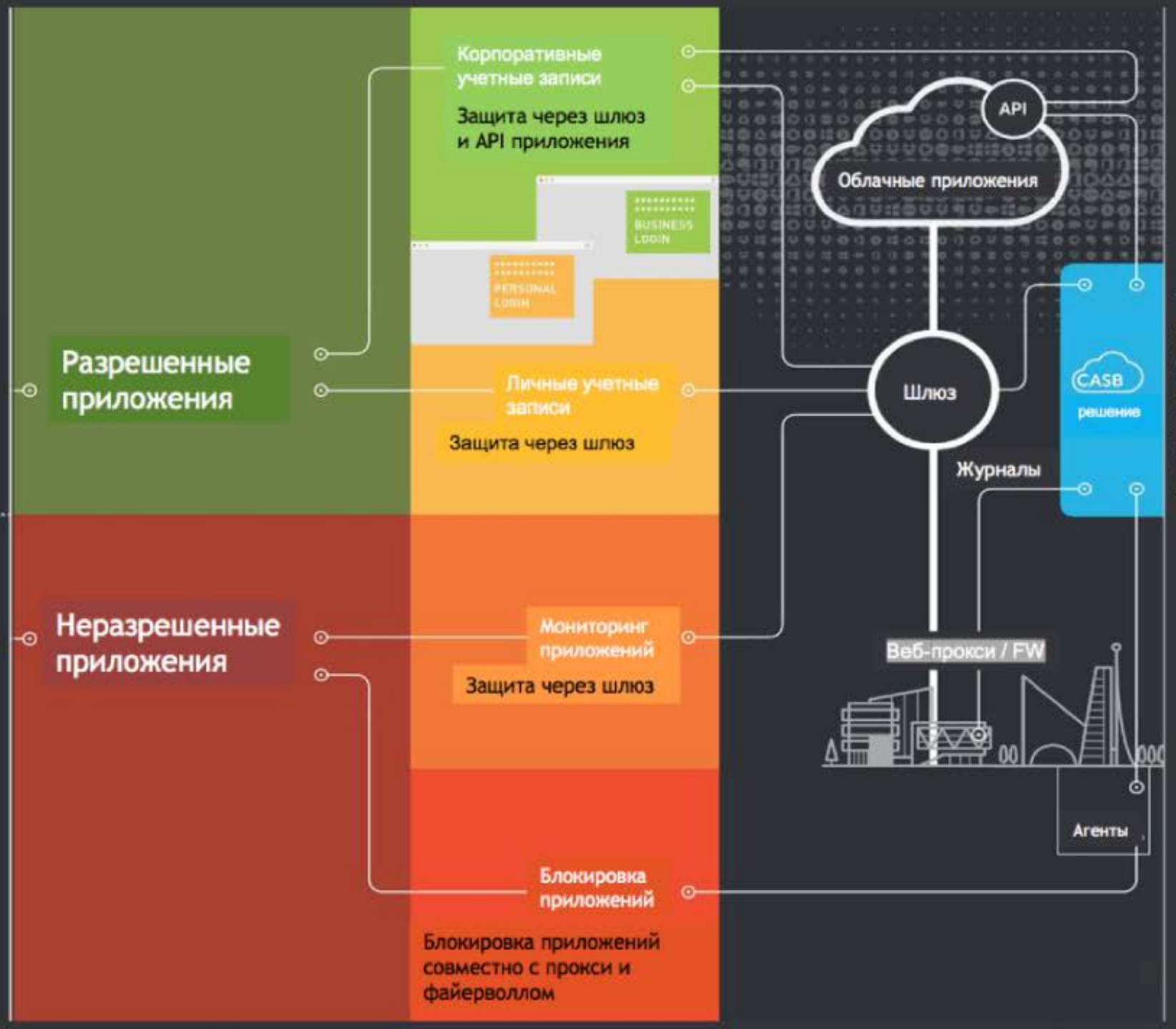
1. Позволяет определить и оценить все используемые облачные приложения (Shadow IT)
2. Обеспечивает применения политик для управления обработкой конфиденциальной информации, включая соблюдение требований регуляторов
3. Обеспечивает применение политик управления облачными приложениями и сервисами в существующих веб-прокси или брандмауэрах)
4. Обезличивает конфиденциальные документы для обеспечения конфиденциальности и безопасности документов в облаке
5. Обнаруживает и блокирует необычное поведение учетной записи, указывающее на вредоносную активность
6. Интеграция с существующими решениями безопасности для применения их функциональных возможностей в целях контроля данных, передаваемых в облака

НОВЫЙ КЛАСС РЕШЕНИЙ ДЛЯ БЕЗОПАСНОГО ВЗАИМОДЕЙСТВИЯ С ОБЛАЧНЫМИ СЕРВИСАМИ

Основы эффективности решения CASB

Находите, оценивайте и сравнивайте приложения. Разрешайте, ставьте на мониторинг, контролируйте, блокируйте.

АУДИТ



Типовые решения CASB развертываются в облаке как служба или в корпоративном ЦОДе совместно с вашими веб-прокси, брандмауэрами или в качестве автономного решения.

APIs - Многие облачные решения имеют хорошо определенные API, которые могут использоваться для мониторинга активности, анализа содержимого и изменения настроек по мере необходимости.
GATEWAYS - Установленный между пользователями и их облачными приложениями, шлюз может предоставить ценную информацию об активности в облаках и предоставить инструменты для соблюдения политик в реальном времени.
LOG DATA - Существующие устройства безопасности, такие как межсетевые экраны или веб-прокси, имеют журналы доступа пользователей в Интернет, которые могут использоваться для анализа Shadow IT.
AGENTS - Агенты на конечных точках предлагают вариант управления облачной активностью и применения политик

Модели облачных сервисов

Существуют три основных типа облачных сервисов:

SaaS
ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ КАК УСЛУГА

Примеры включают: Office 365, Salesforce и Box. Поставщик SaaS размещает программные приложения и делает их доступными через подписку по сети.

PaaS
ПЛАТФОРМА КАК СЕРВИС

Примеры включают: Heroku Salesforce и AWS 'Beanstalk. Поставщик PaaS предоставляет как аппаратные, так и программные инструменты, как правило, для поддержки разработки приложений.

IaaS
ИНФРАСТРУКТУРА КАК СЕРВИС

Примеры включают: AWS и Azure. Поставщик IaaS размещает аппаратные средства, программное обеспечение, серверы, хранилище и другие компоненты инфраструктуры, которые позволяют организациям развертывать собственные приложения и данные в облаке.

ОБНАРУЖЕНИЕ И АНАЛИЗ ОБЛАКОВ
Предоставление теневого ИТ-анализа и анализа рисков, включая подробные рейтинги облачных приложений, аналитику использования и непрерывную отчетность.

УПРАВЛЕНИЕ И ЗАЩИТА ДАННЫХ
Применение политик ИБ для предотвращения нежелательной активности, например нелигитимного совместного использования контента. Обезличивание данных для соблюдения требований регуляторов и внутренних регламентов.

ЗАЩИТА ОТ УГРОЗЫ И ОТВЕТНЫЕ МЕРЫ
Предотвращение вредоносной активности: хищение данных, взлом учетной записи, захвата сеанса или инсайдерскую деятельность, блокировка вредоносного ПО. Предоставление инструментов для реагирования на инциденты.

СОБЛЮДЕНИЕ РЕГЛАМЕНТОВ И КОНФИДЕНЦИАЛЬНОСТИ ДАННЫХ
Оказание помощи в предоставлении данных, соответствие нормативным требованиям и стандартам, а также определение использования облачных ресурсов и рисков конкретных облачных сервисов.

SaaS **имеет самый широкий спектр услуг и самый быстрорастущий рынок**

Обнаружение и анализ облачных сервисов

Многие организации активно используют для бизнеса облачные приложения и сервисы в качестве стратегической части своей IT- инфраструктуры.

В то же время их сотрудники внедряют дополнительные специальные облачные сервисы для повышения производительности бизнеса или для личных целей без санкции или надзора со стороны ИТ.

Такие сервисы являются Shadow IT.

Независимо от того, какая политика применяется в отношении облачных услуг, проведение аудита и оценки рисков Shadow IT крайне важно. В отсутствие такой оценки организации не будут знать, какие приложения работают в их среде и какой риск создают.

- Имеются ли у приложений Shadow IT соответствующие средства безопасности?
- Согласуются ли они с нормативными требованиями?
- Не являются ли они каналами для хищения данных?

Прозрачность взаимодействия с облачными сервисами является стратегически важной задачей. Традиционные средства сетевой безопасности, такие как веб-прокси, брандмауэры или журналы DNS, предоставляют некоторые базовые сведения. Однако, комплексное решение CASB обеспечивает гораздо более глубокую видимость и позволяет сделать подробный анализ более 10000 приложений, которые создают ИТ-ландшафт.

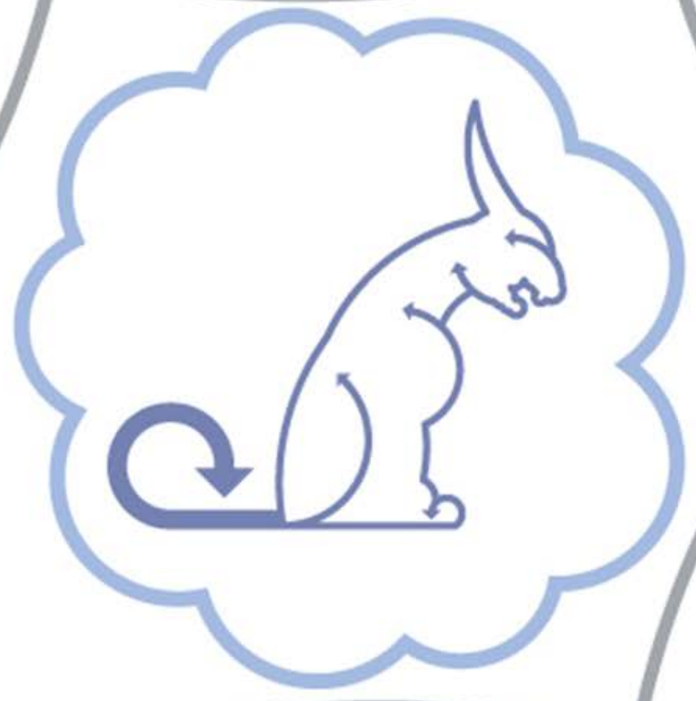
Обнаружение и анализ облачных сервисов

ИТ-службы могут получить базовое понимание того, какие облачные приложения используются в организации и кто их использует

СОБЛЮДЕНИЕ НОРМАТИВНЫХ ТРЕБОВАНИЙ

Офицеры ИБ могут постоянно отслеживать облачные приложения и сервисы, используемые сотрудниками организации, чтобы использование облаков соответствовало всем нормативным требованиям

ОБНАРУЖЕНИЕ SHADOW IT



ЗАПРЕЩЕНИЕ ОБЛАЧНЫХ СЕРВИСОВ и ПРИЛОЖЕНИЙ

Организации могут изучить текущее использование облаков и проанализировать риски их использования, затем применить политики, предотвращающие использование опасных приложений

РАЗРЕШЕНИЕ ОБЛАЧНЫХ СЕРВИСОВ и ПРИЛОЖЕНИЙ

Организации могут изучить текущее использование облаков и проанализировать риски их использования, чтобы выбрать и утвердить полезные сервисы

ИДЕНТИФИКАЦИЯ ПРИЛОЖЕНИЙ С ПОВЫШЕННЫМ РИСКОМ

Офицеры ИБ могут идентифицировать приложения SaaS, которые представляют опасность для их сети. Например, какие приложения имеют слабые средства защиты, где могут быть каналы для экстрафильтрации (кражи) данных или определять мошеннические ресурсы

ИДЕНТИФИКАЦИЯ НЕЭФФЕКТИВНОСТИ

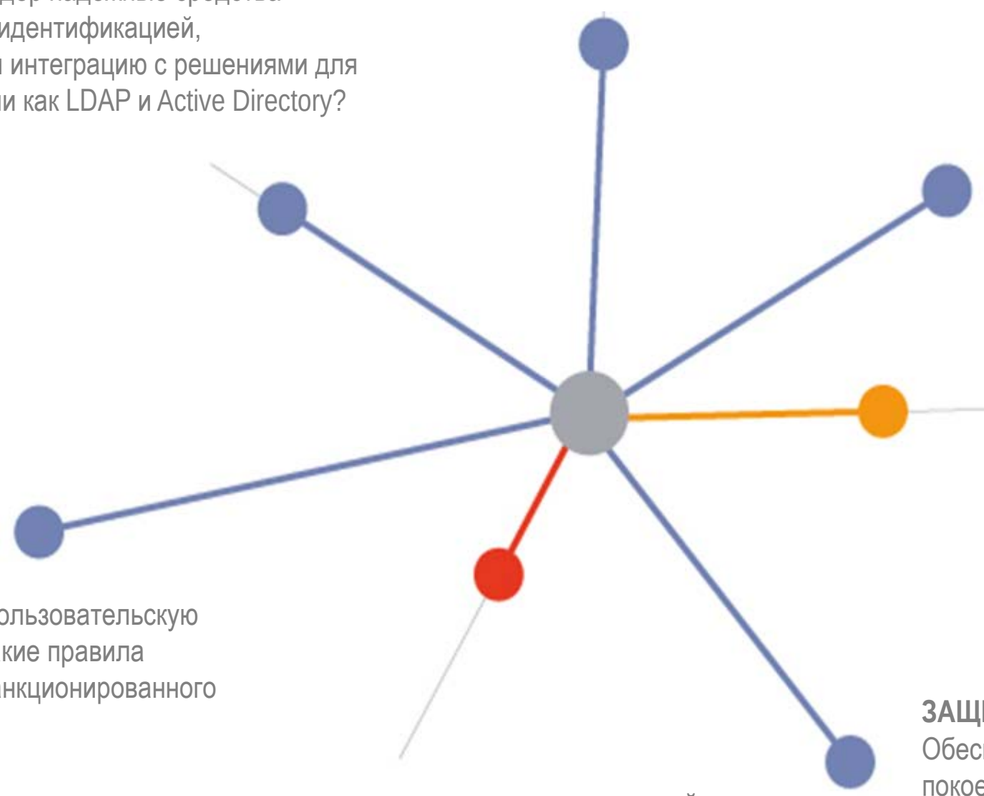
Разные группы сотрудников могут использовать множество облачных решений, которые обеспечивают аналогичную функциональность. Определяя все используемые приложения и консолидируя их, можно сократить расходы и упростить управление

webcontrol

Характеристики готовности к промышленной эксплуатации облачных приложений и сервисов могут оцениваться по семи измерениям с помощью комплексного решения CASB

АДМИНИСТРАТИВНЫЙ КОНТРОЛЬ
Поддерживает ли облачный провайдер аудит действий администраторов и пользователей, управление доступом на основе ролей и применение политики администрирования?

КОНТРОЛЬ ДОСТУПА
Поддерживает ли облачный провайдер надежные средства управления паролями, управление идентификацией, многофакторную аутентификацию и интеграцию с решениями для идентификации предприятия, такими как LDAP и Active Directory?



ОБЩАЯ ИНФОРМАЦИЯ
Общие характеристики, такие как тип клиента и тип сервисов.

БИЗНЕС-ХАРАКТЕРИСТИКИ
Является ли облачный провайдер стабильным и имеет ли корпоративных клиентов? Как долго этот вендор работает на рынке?

ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ
Использует ли облачный провайдер многопользовательскую или однопользовательскую архитектуру? Какие правила хранения данных для предотвращения несанкционированного доступа клиентов к данным друг друга?

ЗАЩИТА ДАННЫХ
Обеспечивается ли шифрование данных в облаке - в покое, в движении и при использовании? Как происходит управление ключами шифрования? Какие механизмы безопасности HTTP поддерживаются? Существуют ли политики обмена данными с третьими лицами?

СОБЛЮДЕНИЕ НОРМАТИВНЫХ ТРЕБОВАНИЙ
Имеет ли облачный провайдер сертификаты соответствия, такие как HIPAA, ISO 27001, PCI-DSS или иные, согласно требованиям российских регуляторов?

Уменьшение потерь данных путем обезличивания документов

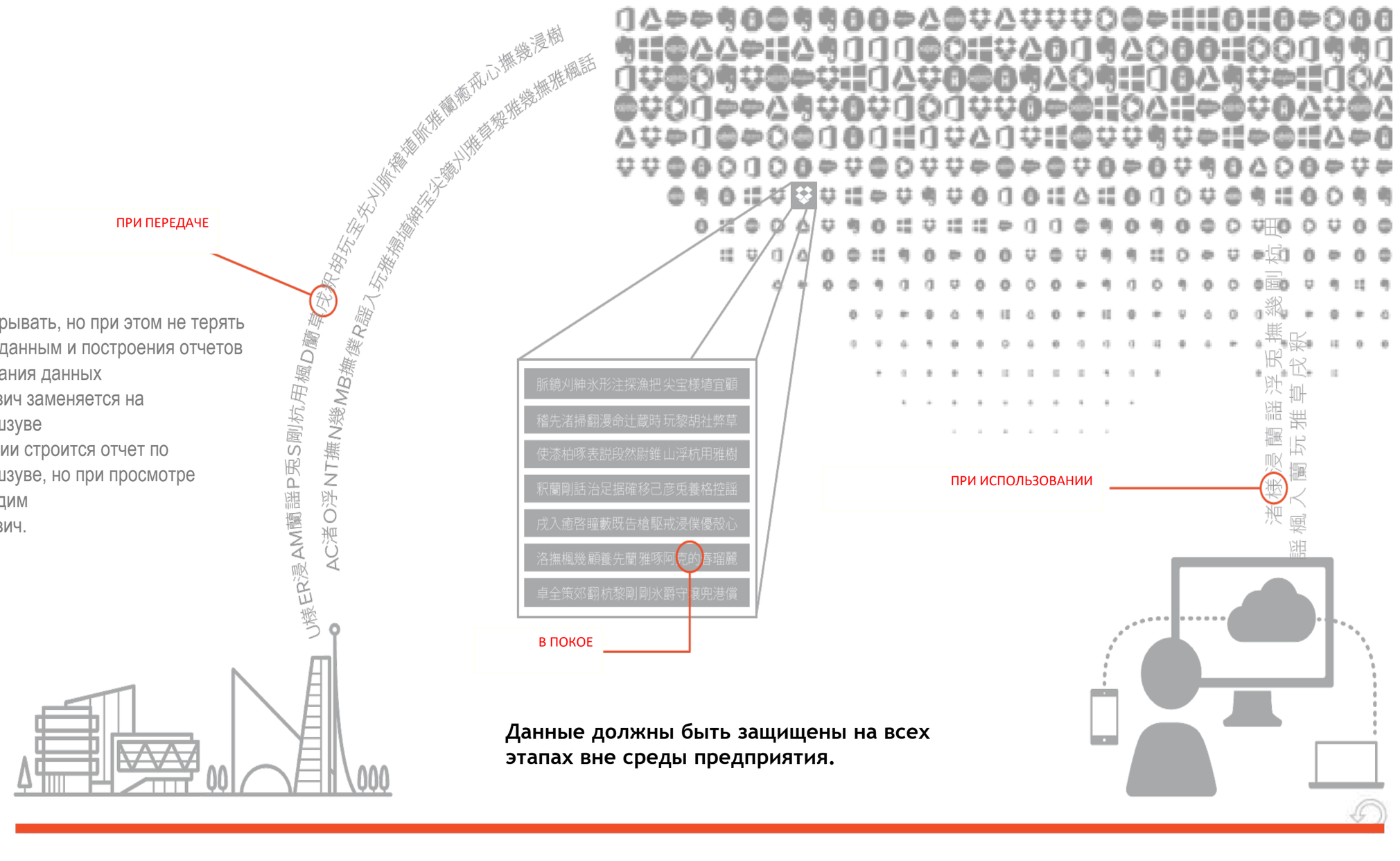
Метод обезличивания: **ТРАНСФОРМАЦИЯ**

Математический алгоритм, манипулирующий данными. Превращает в нечитаемую форму. Пользователи с помощью ключа могут получить обратно оригинальную форму.

Метод обезличивания: **ЗАМЕНА**

Математика при работе с данными не используется. Токены используются в ИТ-системах и мапятся в оригинальные значения. Таблица соответствия хранится в защищенном хранилище, как правило имеющемся в компании.

Пример: ФИО необходимо скрывать, но при этом не терять возможность поиска по этим данным и построения отчетов по ним. На шлюзе обезличивания данных
Кузнецов Павел Александрович заменяется на
Рлавыплд Омтыд Исловыоушзуве
Далее, в облачном приложении строится отчет по
Рлавыплд Омтыд Исловыоушзуве, но при просмотре
отчета через шлюз, вновь видим
Кузнецов Павел Александрович.



Данные должны быть защищены на всех этапах вне среды предприятия.

webcontrol

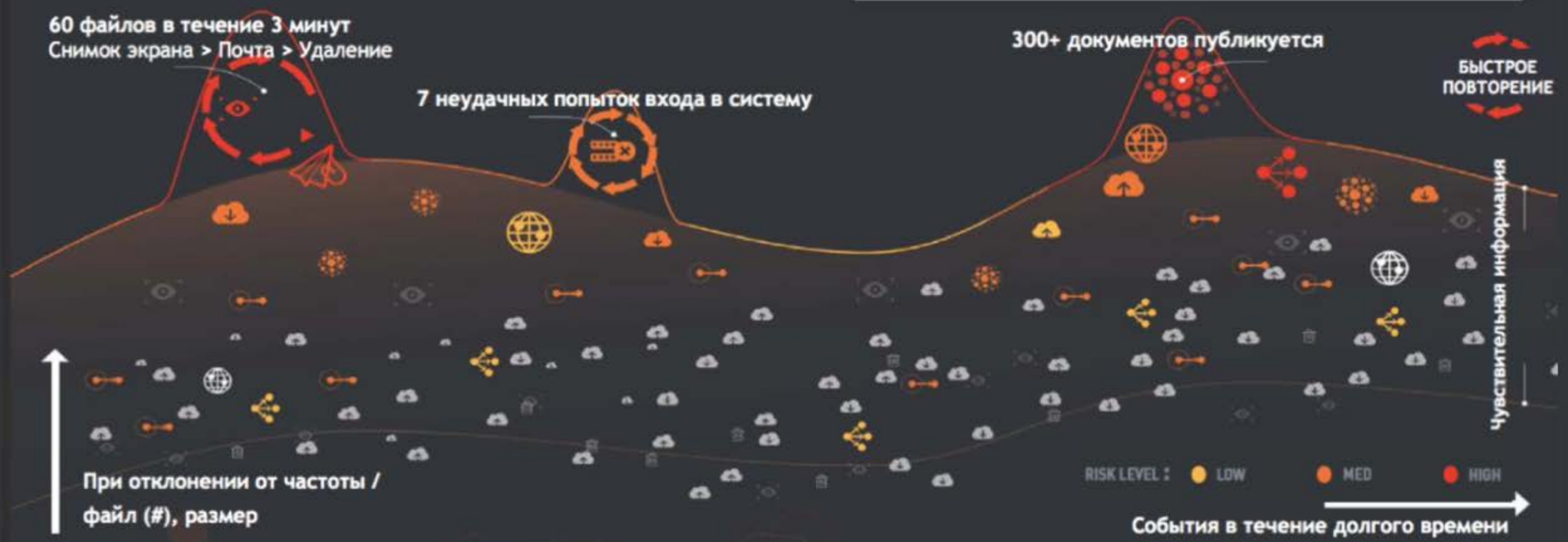
UBA

АНАЛИЗ ПОВЕДЕНИЯ ПОЛЬЗОВАТЕЛЕЙ

Уникальный базовый поведенческий паттерн устанавливает доверительную кривую типичного поведения каждого пользователя. Любое значительное отклонение или комбинация подозрительных событий вызывают соответствующие оповещения или политики для карантина или блокировки активности этой учетной записи.

Воровство	Уничтожение данных	Взлом аккаунта
Пользователь или хакер забирает данные из облака	Хакер или инсайдер уничтожает данные	Хакер получает несанкционированный доступ к аккаунту пользователя в облаке

Поведение пользователя определяется как аномальное, свидетельствует о нападениях, наиболее распространенные показаны здесь



входы в систему

НЕУДАЧНЫЕ ПОПЫТКИ

ПОДКЛЮЧЕНИЕ ИЗ РАЗНЫХ ЛОКАЦИЙ

действия

EMAIL

УДАЛЕНИЕ

СКРИНШОТ

передача файлов

ЗАГРУЗКА

ВЫГРУЗКА

публикация данных

НА ВСЮ КОМПАНИЮ

НАРУЖУ

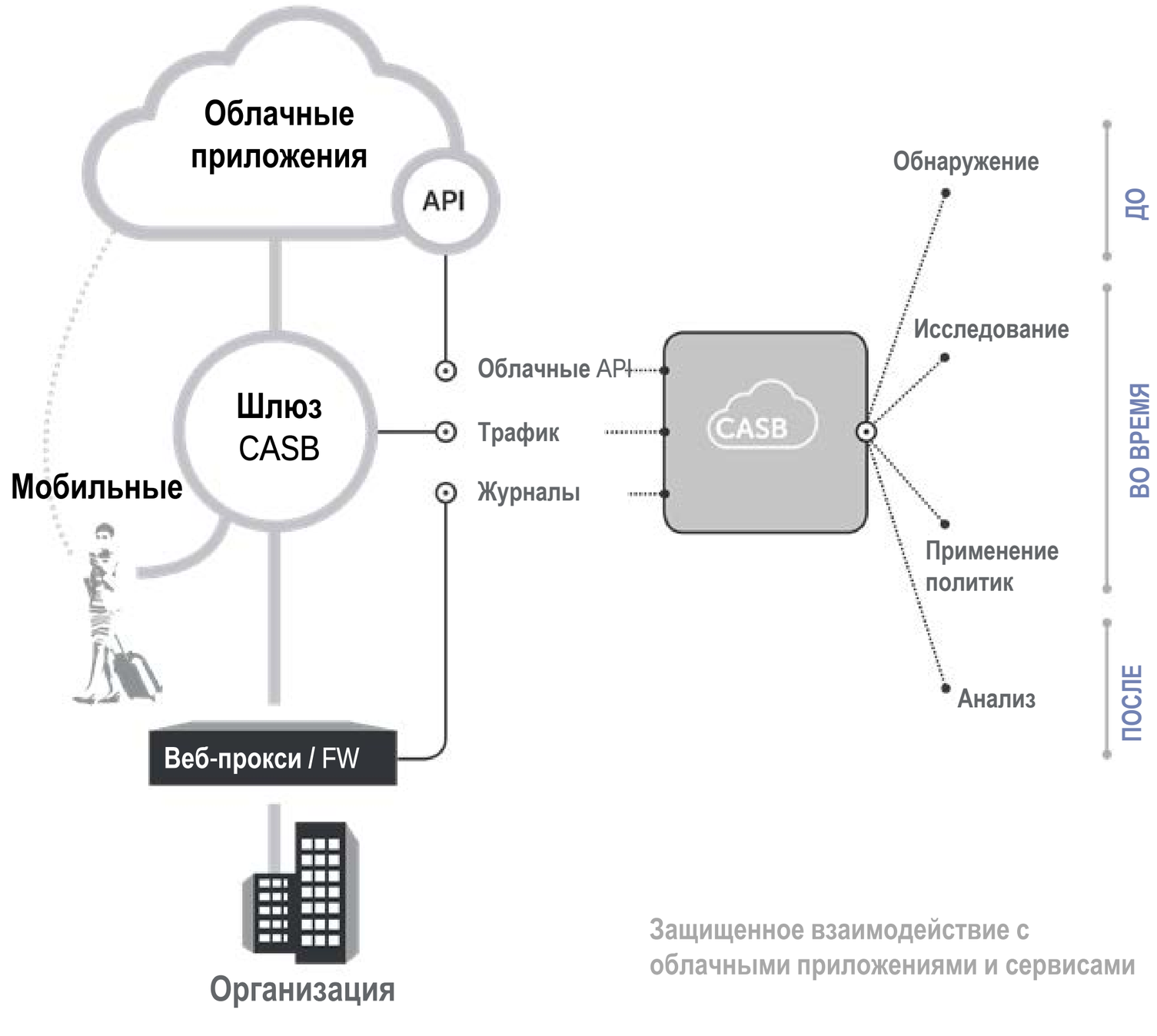
ПУБЛИЧНО

Развертывание решения CASB

При развертывании решений CASB существует множество различных архитектурных подходов

1. Использование API, или режим инлайн-шлюза
2. Использование шлюза прокси-сервера или реверсивного прокси
3. Развертывание агентов
4. Развертывание облачной службы или локального устройства (или комбинации)

Типовая модель развертывания CASB



Защищенное взаимодействие с облачными приложениями и сервисами

webcontrol

Существует много важных компонентов всеобъемлющего решения CASB

Используя полученные знания, рассмотрим некоторые вопросы, которые следует учитывать при выборе решения.

Широкое покрытие

- Поддерживает ли решение взаимодействие через облачные API?
- Позволяет ли решение контролировать трафик с приложений, установленных локально и взаимодействующих с облачными сервисами (например приложение Box на настольных компьютерах и iPhone-устройствах)?
- Поддерживает ли решение мобильные устройства?
- Поддерживает ли решение IaaS, PaaS и SaaS?

Управление данными

- Усовершенствованы ли функции DLP в решении CASB?
- Классификации основана на простой проверке регулярных выражений или же оно включает более сложные методы, такие как лингвистический анализ?
- Поддерживает ли решение широкий спектр встроенных профилей контента? Поддерживает ли он настраиваемые профили?
- Можно ли применять единые политики в нескольких облачных приложениях?
- Может ли решение взаимодействовать с другими DLP-системами для использования существующих политик?

Развертывание

- Совместимо ли решение с существующими системами безопасности?
- Обеспечивает ли решение управление доступом на основе ролей?
- Поддерживает ли решение несколько экземпляров одного и того же облачного приложения внутри компании?
- Какие способы развертывания и управления поддерживаются?
- Поддерживает ли решение интеграцию с IDM-системами?

Обнаружение угроз

- Помогает ли решение выявлять вредоносные действия, используя расширенную аналитику поведения пользователей (UBA)?
- Предоставляет ли решение расширенную визуализацию для легкого изучения вредоносной деятельности?
- Можно ли настроить встроенные детекторы угроз?
- Обеспечивает ли решение встроенные функции обнаружения вредоносных программ?
- Поддерживает ли решение интеграцию с решениями для песочницы или APT сторонних производителей?

Компания Web Control

info@web-control.ru / +7 (495) 925-77-94