

Каждый путь важен

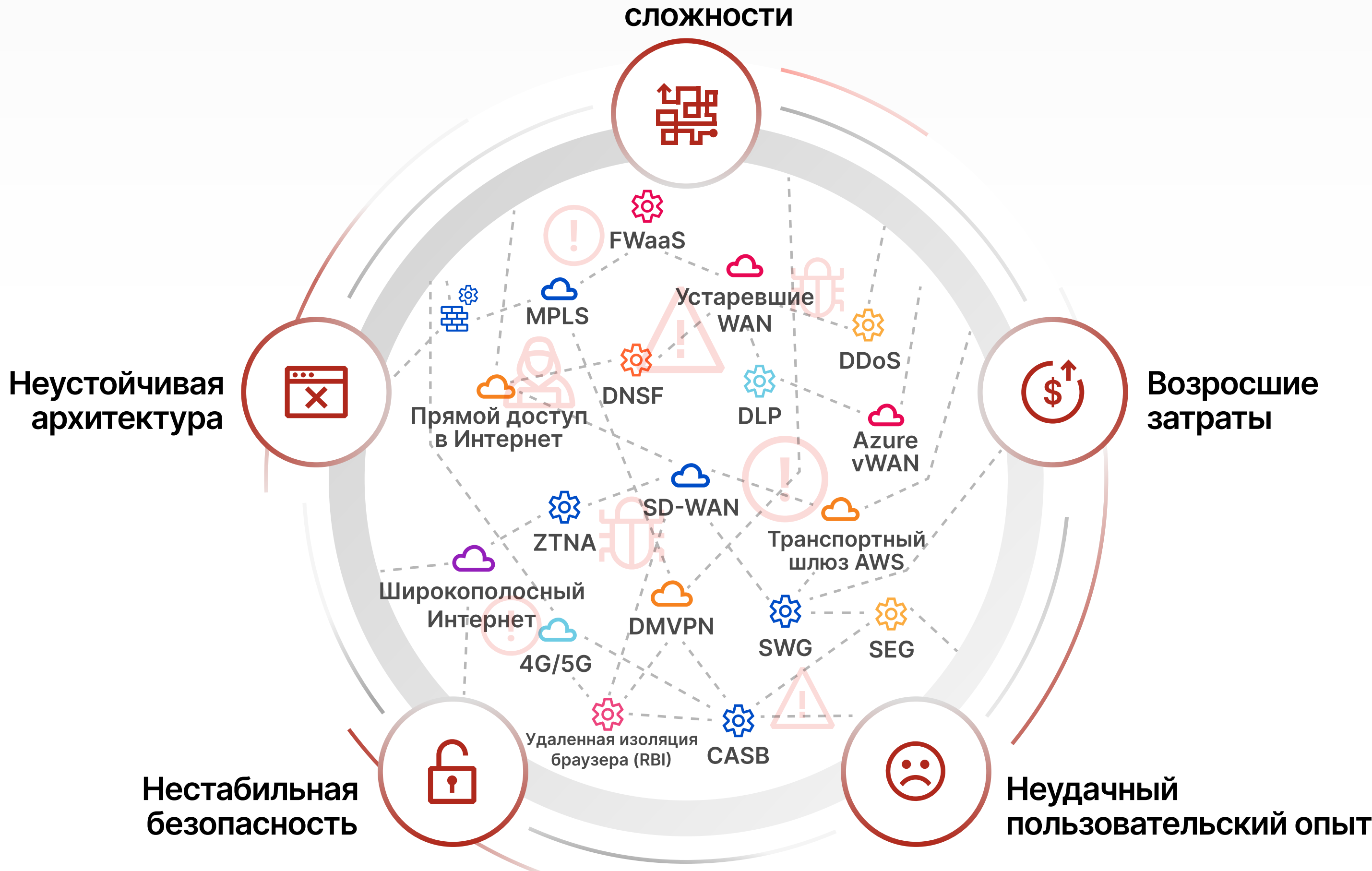
Не пора ли перенаправить потоки сетевого трафика?



Устаревшие корпоративные сети были сосредоточены только на внутренней связи и безопасности. Однако гибридная работа, облачные приложения и быстрые инвестиции в цифровую модернизацию коренным образом изменили место и способ передачи сетевых потоков.

Что произойдет, если сетевая инфраструктура не готова к современным требованиям бизнеса?

В устаревших корпоративных сетях часто возникают следующие проблемы:



52 %

52 % руководителей заявляют, что **чрезмерная усложненность инфраструктуры** является **самым большим препятствием** для обеспечения безопасности¹

70 %

70 % генеральных директоров по всему миру утверждают, что **недостаточный уровень зрелости их сетевой инфраструктуры негативно сказывается** на эффективности ведения бизнеса²

101 %

101 % — это **средняя рентабельность инвестиций для платформенных организаций**, по сравнению с 28 % у тех, кто не перешел на платформенную модель¹

В традиционных архитектурах **использование десятков различных решений для покрытия четырех потоков сетевого трафика** также добавляет сложности

Поток трафика

Необходимые продукты

Проблемы

Входящий трафик из Интернета

Традиционно защищается локальными межсетевыми экранами, VPN, DMZ-инфраструктурой, фильтрацией интернет-провайдеров

- DoS- и DDoS-атаки
- Эксплойты нулевого дня (zero-day)
- Фишинг
- Вредоносное ПО

Исходящий трафик в Интернет и в облачные приложения

Традиционно защищаются локальными межсетевыми экранами и прокси-серверами

- Боковое перемещение (внутри сети)
- Подверженность данных рискам
- Распространение программ-шантажистов
- Участие в ботнете

Сетевое подключение WAN в кампусах и филиалах

Традиционно покрываются физическими/виртуализированными сетями, SD-WAN, частными межсетевыми соединениями, MPLS

- Более высокие капитальные и оперативные расходы
- Задержка сети
- Ограничения пропускной способности
- Неудачный пользовательский опыт

Мультиоблако для приложений в нескольких облаках

Традиционно покрывается продуктами «Сделай сам»

- Проблемы с возможностью мониторинга и применением политик
- Сложность нормативно-правового регулирования

Что нужно изменить?

Традиционные сети

VS

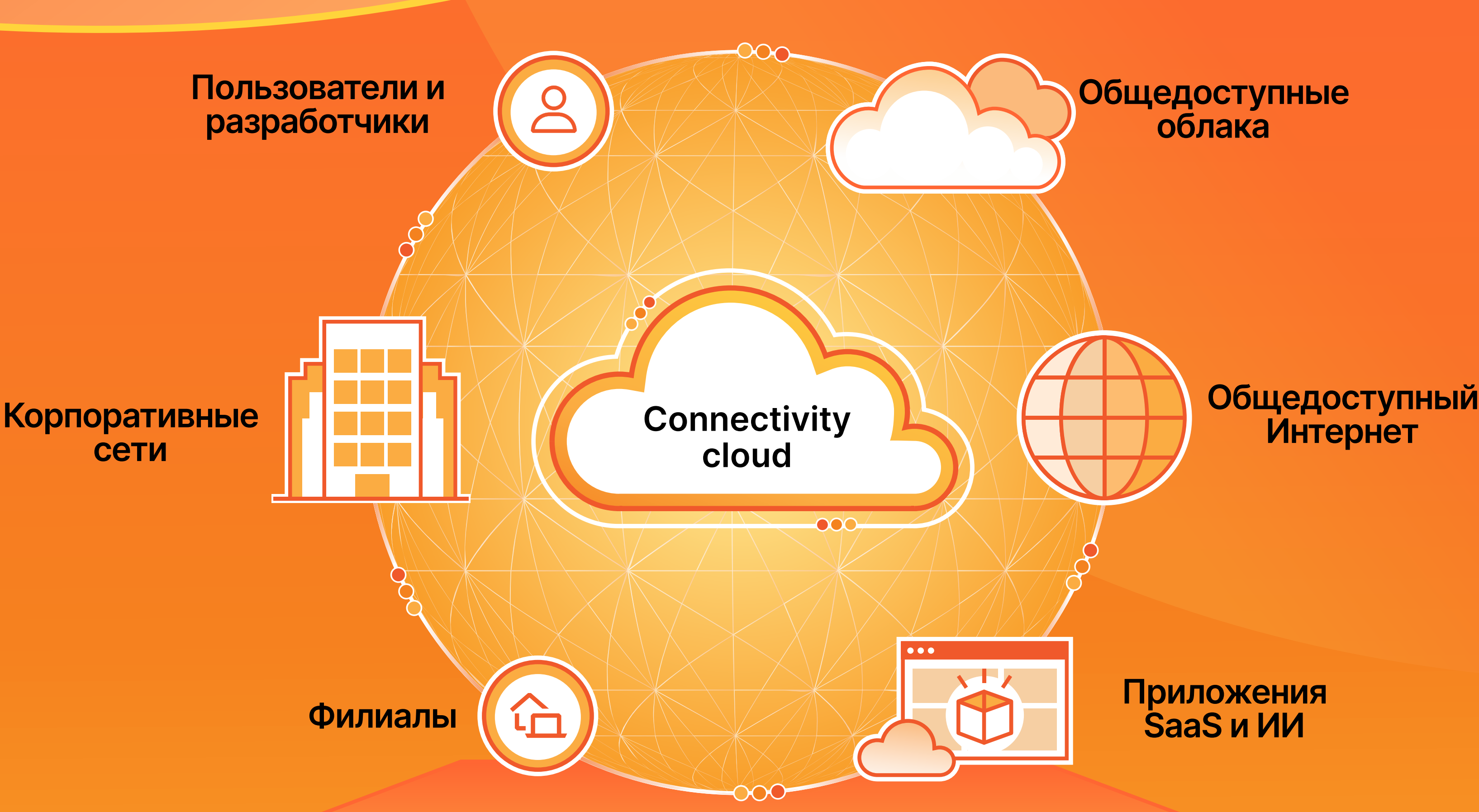
Современные сети

- Внедренные устройства для добавления новых функций или географических регионов требует простоя и перерывов в обслуживании
- Защищенные пользователи и филиалы подключенные к приложениям, размещенным в центре обработки данных
- Неявно «доверенный» трафик внутри периметра
- Оптимизированы для поддержки офисных сотрудников

- Развертывают компонентные сервисы вместо аппаратных решений, снижая сложность и риск сбоев
- Должны поддерживать облачные приложения, SaaS и частные облачные приложения повсюду
- Должны предполагать, что все объекты, включая распределенных пользователей, устройства, приложения и данные, являются «недоверенными».
- Не могут определять местонахождение пользователя и должны поддерживать пользователей, работающих из любого места

Как соответствовать современным требованиям, и при этом обеспечить обслуживание всех потоков трафика?

Вместо использования разрозненных решений для каждого маршрута трафика, **connectivity cloud** решает задачи модернизации сети комплексно.



Входящий трафик

Защитите сеть и приложения от DDoS-атак и других интернет-угроз

Исходящий трафик

Защитите пользователей и офисы от угроз, обеспечьте соблюдение согласованных политик и контролируйте данные в приложениях.

WAN

Подключайте и обеспечивайте безопасность офисов, пользователей, устройств, центров обработки данных и инфраструктуры

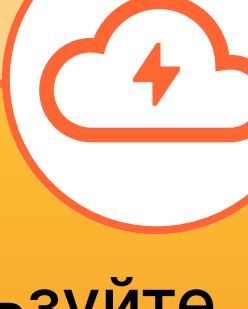
Многооблачный трафик

Обеспечьте сетевые соединения для приложений, защиты и создания приложений в средах общедоступного/гибридного облака.

Connectivity cloud от Cloudflare использует модульную программируемую архитектуру для предоставления сетевых услуг и сервисов безопасности вашим пользователям, а также облачной бизнес-инфраструктуре и приложениям.



Избавьтесь от необходимости расширять или увеличивать частные центры обработки данных



Используйте облачные сетевые услуги и сервисы безопасности, а не аппаратные средства



Сократите чрезмерное «доверие» в сети с помощью Zero Trust

Узнайте больше об использовании Cloudflare для упрощения и ускорения модернизации сети

[Подробнее](#)

1. Али, Мохамад и Дженин, Б.Дж. «Получение дивидендов от кибербезопасности». IBM, <https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/unified-cybersecurity-platform>. Дата обращения: 26 июня 2023 г.

2. «70 % генеральных директоров заявляют, что их сеть замедляет рост бизнеса, согласно новому исследованию NTT». Business Wire, 20 октября 2022 г., <https://www.businesswire.com/news/home/202210200005120/en/70-Of-CEOs-Say-Their-Network-Is-Slowing-Business-Growth-New-NTT-Study-Finds>. Пресс-релиз.