ФОРУМ ДОРОЖНЫХ ИНИЦИАТИВ

КОД безопасности

30 МАЯ - 1 ИЮНЯ 2022 IRCFORUM.RU

# Комплексные решения ИБ от Кода Безопасности

Шутенко Александр

КОД безопасности

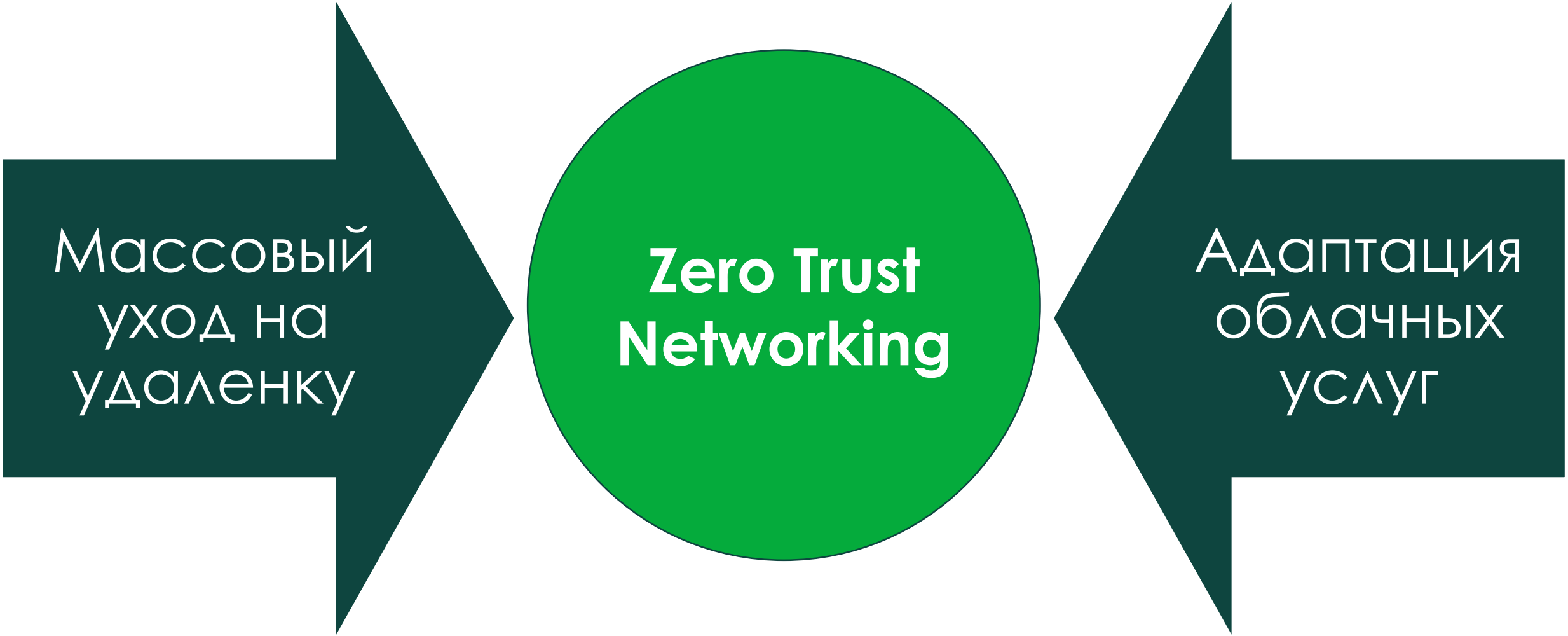
# Началась эта история до пандемии

**Поговорим об использование архитектуры нулевого доверия для защиты инфраструктуры :**

- **На Инфофоруме 2020 мы рассказывали про новую, перспективную тему**
- **Пандемия подтвердила правильность подхода**

КОД безопасности

# Предпосылки новой эпохи

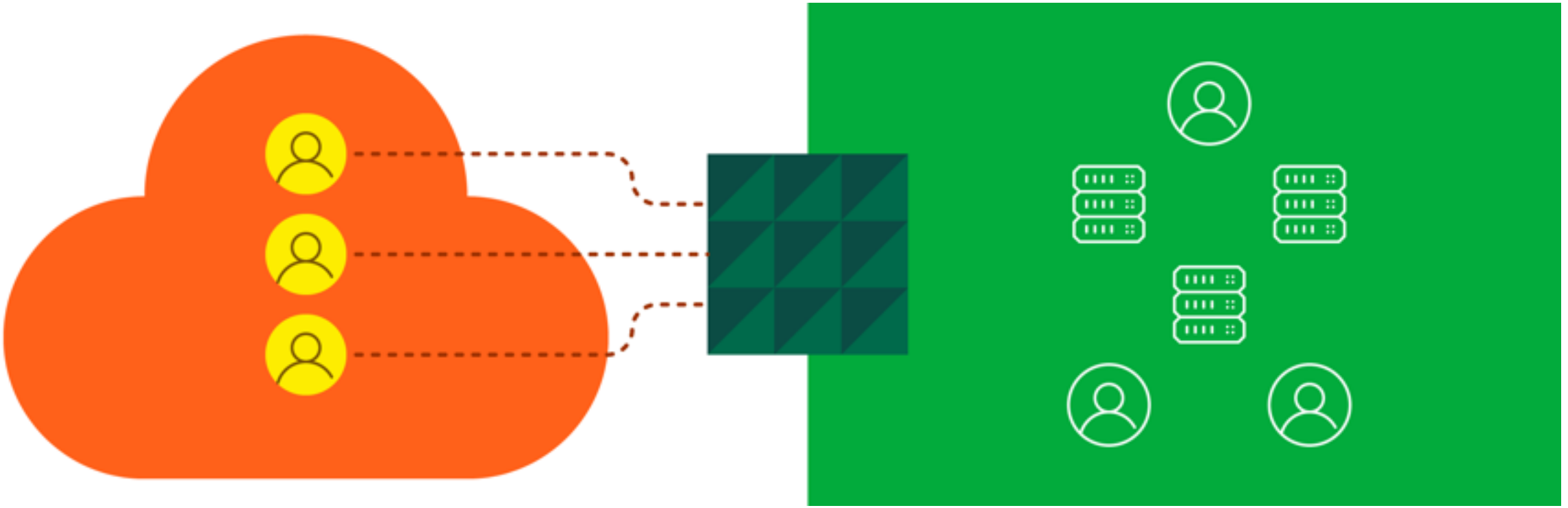


КОД безопасности

# Эволюция

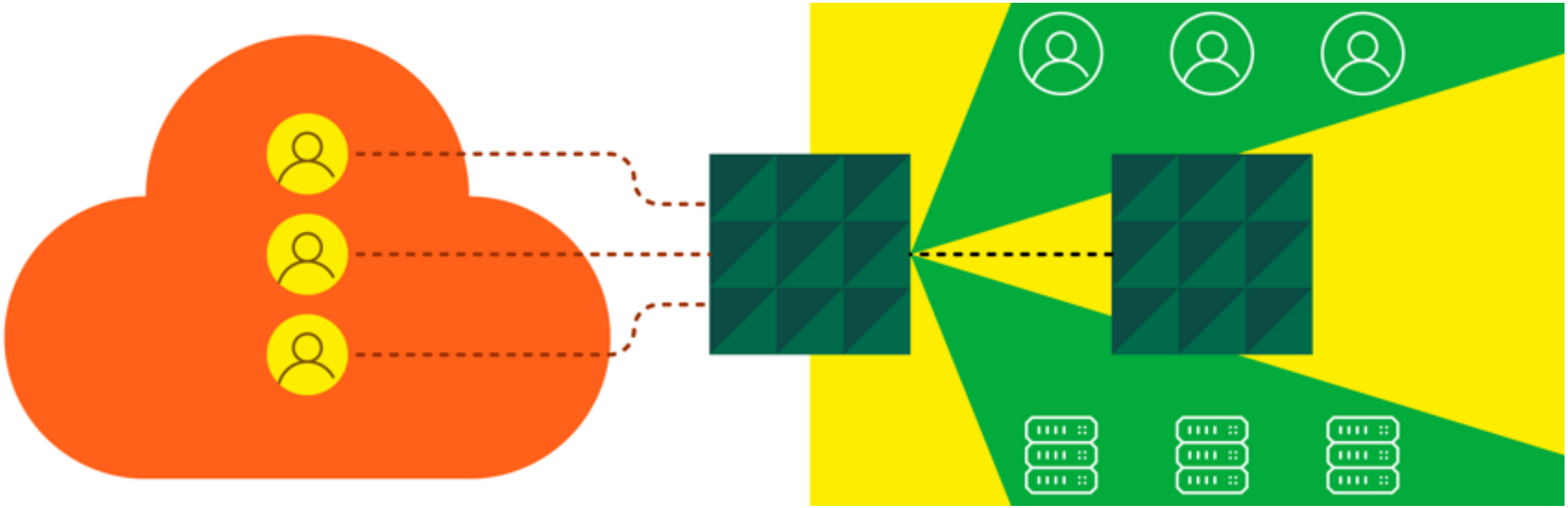
КОД безопасности

# Эволюция



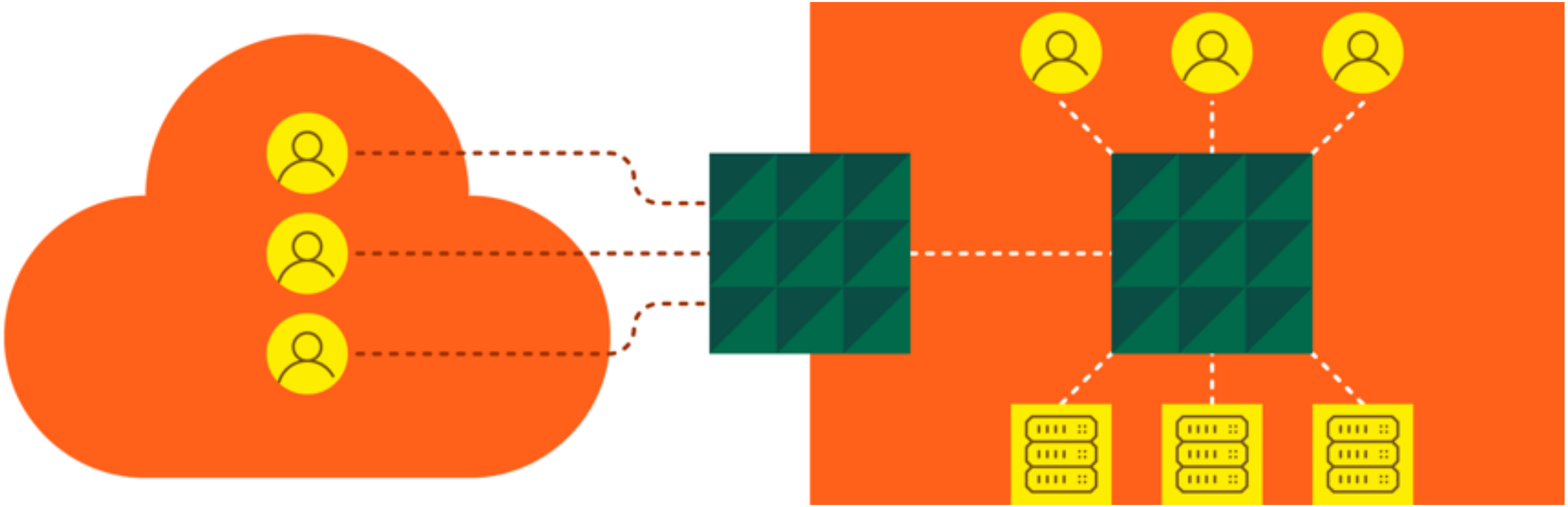
КОД безопасности

# Эволюция



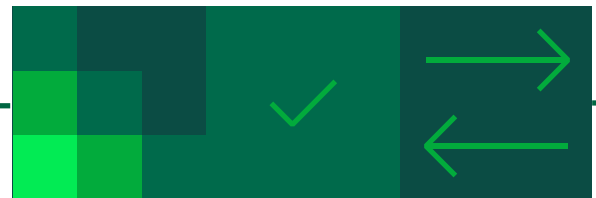
КОД безопасности

# Эволюция



КОД безопасности

# Что говорит нам законодательство РФ по этому поводу?


КОД безопасности

# ФСТЭК России описывает схожий подход в Приказах :

- №17 (ГИС/МИС)
- №21 (ИСПДн)
- №31 (АСУ ТП)
- №239 (КИИ)

КОД безопасности

# В НПА РФ все есть, что же нового в ZTN?

Все пользователи - **удаленные**

Контролируемая зона - **минимальна**

КОД безопасности

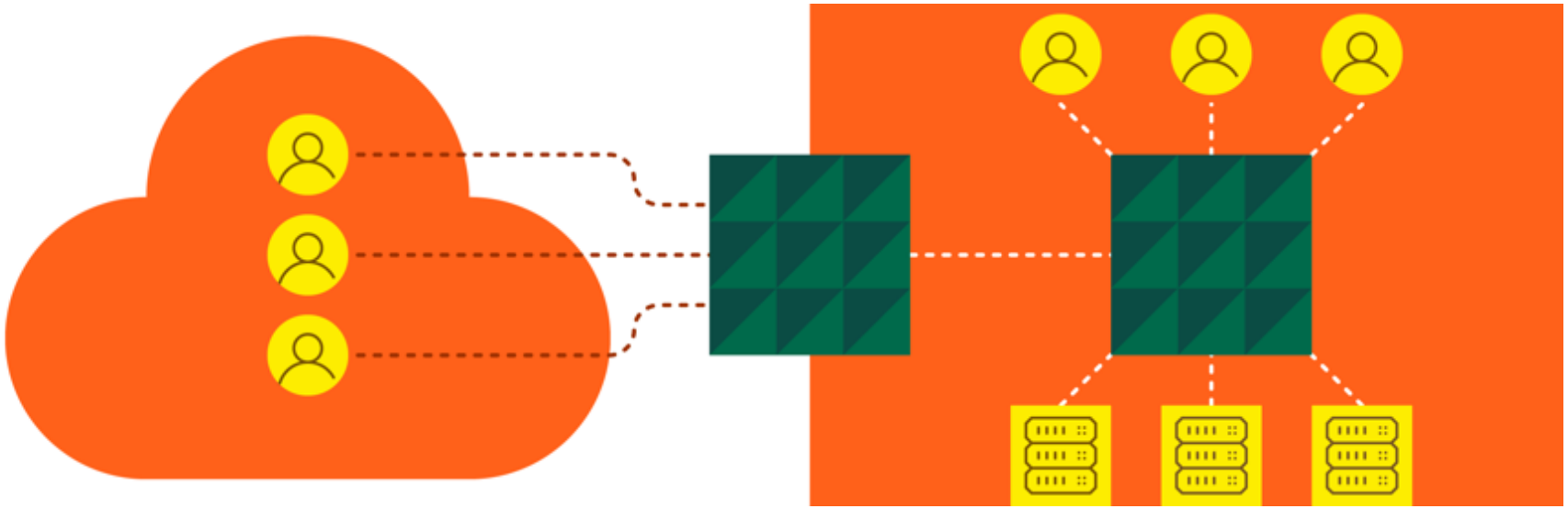
# Ключевые положения Zero Trust Networking

## Не доверяй без предварительной проверки!

Шифруем и аутентифицируем **каждое** подключение

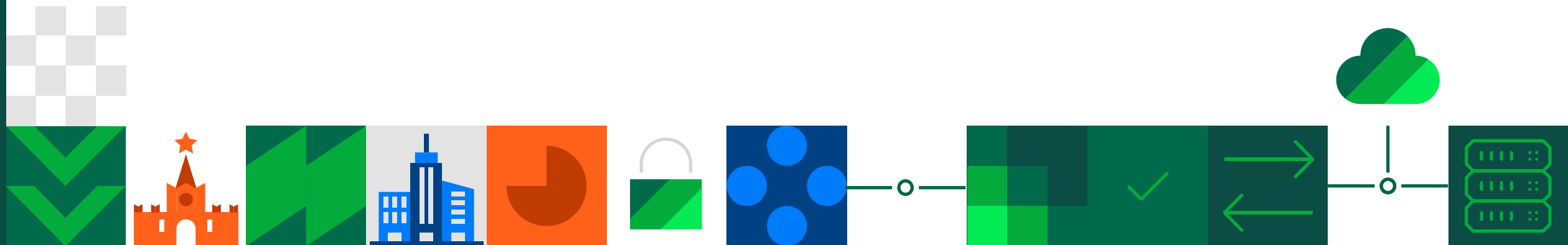
Добавляем дополнительный "фактор" к IP-адресу

Добавляем «ПЦР-тест» при каждом подключении



КОД безопасности

# Что дает Zero Trust Networking?



КОД безопасности

# Что дает Zero Trust Networking?

**Безопасность**

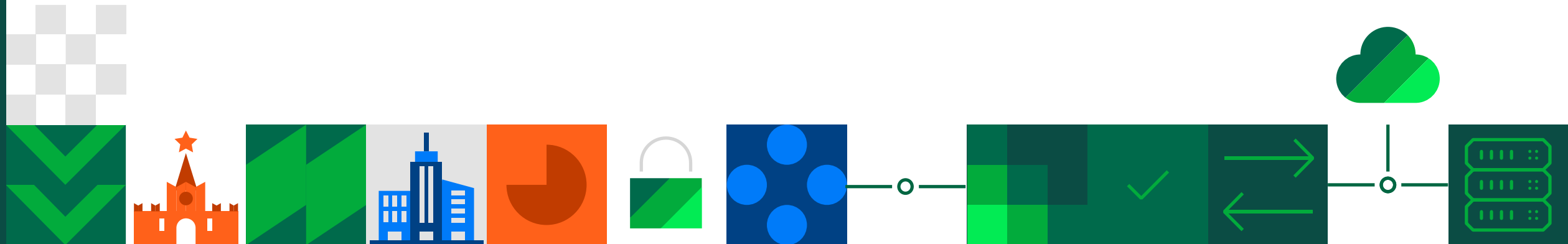
- Безопасный уход на «удаленку»
- Безопасный уход в облако
- Снижение вероятности и тяжести инцидентов ИБ

**Бизнес**

- Увеличение скорости изменений
- Комфортный переход к цифровой модели бизнеса
- Сокращение потерь от инцидентов ИБ и санкций со стороны регуляторов

КОД безопасности

# Нужен алгоритм обеспечения доверия?



КОД безопасности

# Алгоритм обеспечения доверия

## Варианты алгоритма:

- **Степень уверенности**
  - Обязательное выполнение всех требований
  - Скоринговая модель
- **Фактор времени**
  - Учет предыдущих событий
  - Учет только текущих условий

КОД безопасности

# Подходы к архитектуре

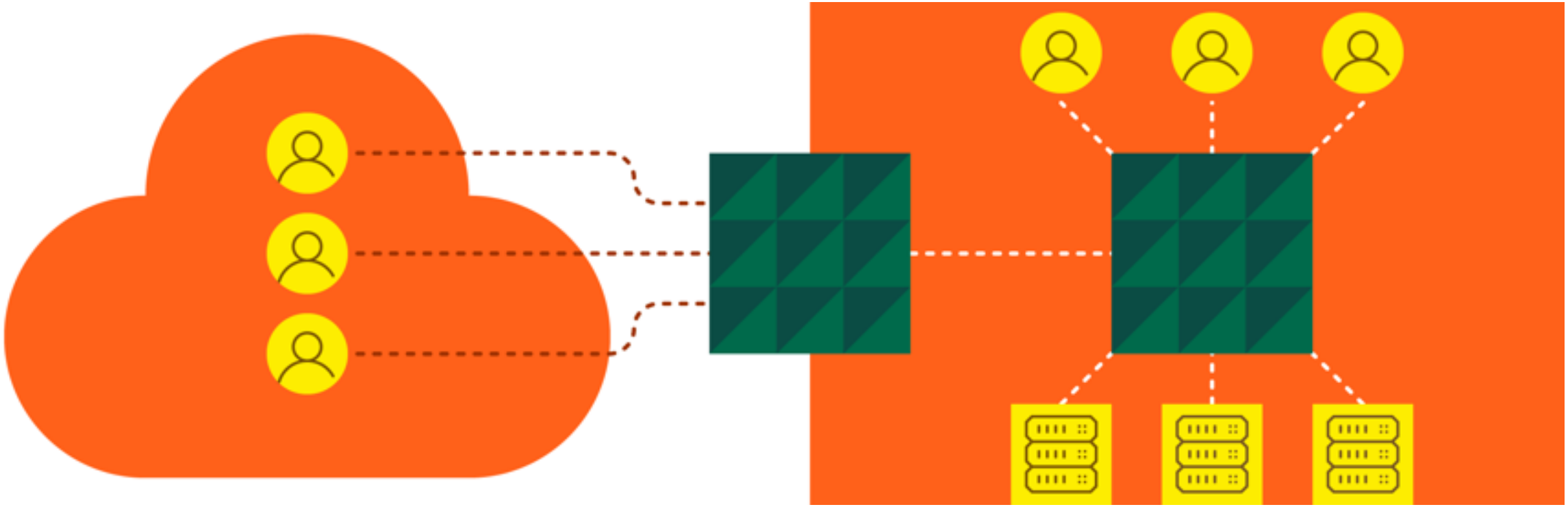
| Подход | Описание | Реализация у нас |
|---|---|---|
| **Расширенная идентификация активов** | Для идентификации должен использоваться устойчивый к фальсификации фактор | • Подключение пользователя к серверу доступа Континент и Континент TLS<br>• Captive portal K4<br>• Контроль жизненного цикла виртуальных машин в vGate<br>• Контроль аутентификации пользователя/компьютера в SNS |
| **Микросегментация** | Сегментация реализуется на уровне сетевой топологии | • Континент 3, 4<br>• Континент TLS |
| **Программный периметр** | Сегментация реализуется «поверх» сетевой топологии | • Межсетевой экран и авторизация сетевых соединений в SNS<br>• Межсетевой экран в vGate |

# Варианты архитектуры

| Варианты архитектуры | Пример реализации |
|---|---|
| Агентская архитектура | • Secret Net Studio |
| Защищенный анклав | • **Шлюзовые компоненты**: Континент 3, Континент 4, Континент TLS server<br>• **Клиентские компоненты**: Континент АП, Континент TLS клиент, Континент ZTN клиент |
| Прозрачный шлюз | • vGate |
| Песочница | • Secret Net Studio (ЗПС+МЭ) |

КОД безопасности

# Вместо резюме

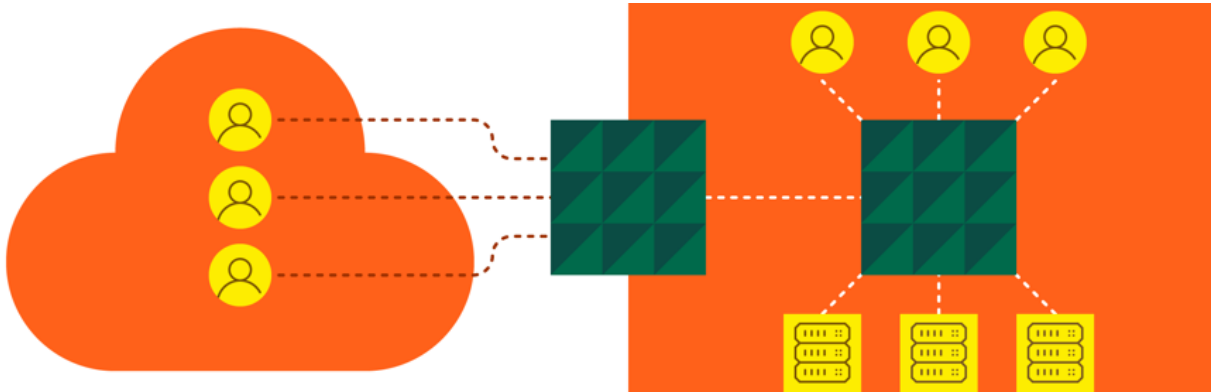


КОД безопасности

# Вместо резюме

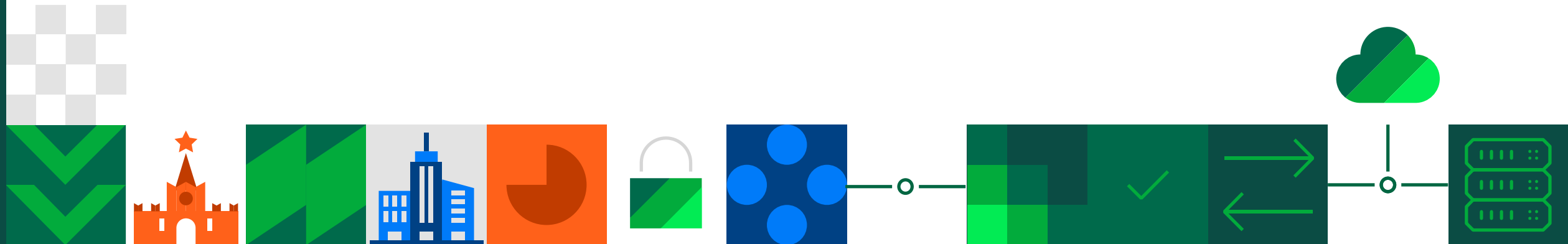
Подумайте над вопросами:

- Знаю ли я обо всех приложениях и о том, какие к каким приложениям должны ходить?
- Можно ли использовать уже имеющиеся продукты для реализации этого подхода?



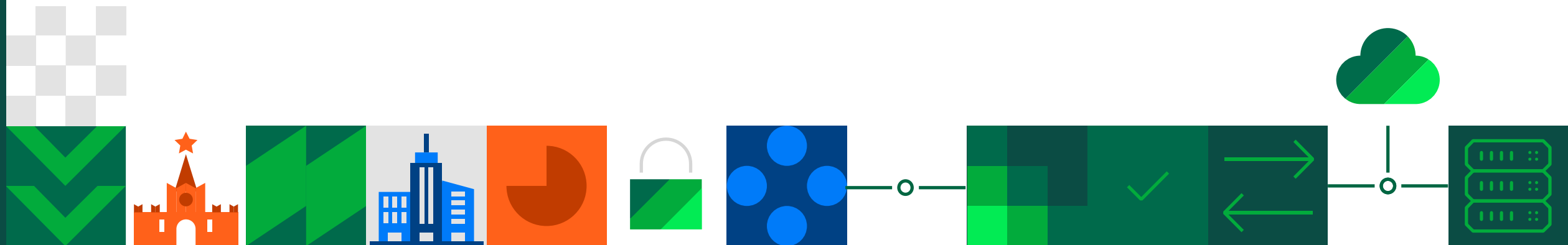
КОД безопасности

# Хочу себе такое, что делать?



КОД безопасности

# Континент 4.1 UTM/NGFW



КОД безопасности

# Консолидация механизмов безопасности в едином устройстве

КШ — Криптошлюз (КШ)

КК — Криптокоммутатор (КК)

Детектор атак (ДА)

Центр управления сетью (ЦУС)

## Узел безопасности


FW | IPS | App control | L2 VPN | L3 VPN | MGMT | Anti bot | Log | URL reputation

КОД безопасности

# Модельный ряд

| Характеристики | IPC-10 | IPC-50M | IPC-500 | IPC-500F | IPC-600 | IPC-800F |
|---|---|---|---|---|---|---|
| |  |  |  |  |  |  |
| **Производительность** | | | | | | |
| **Производительность МЭ**, Мбит/с | до 800 | до 1 700 | до 3 800 | до 3 800 | до 8 000 | до 10 200 |
| **Производительность UTM**, Мбит/с | до 250 | – | до 400 | до 400 | до 2 900 | до 5 600 |
| **Производительность IPS**, Мбит/с | до 100 | – | до 1 750 | до 1 750 | до 1 500 | до 3 000 |
| **Производительность VPN**, Мбит/с | до 150 | до 300 | до 500 | до 500 | до 2 000 | до 2 500 |
| **Максимальное число одновременных сессий МЭ** | 1 000 000 | 1 000 000 | 3 000 000 | 3 000 000 | 3 000 000 | 3 000 000 |

КОД безопасности

# Модельный ряд

| Характеристики | IPC-1000F | IPC-3000F | IPC-3000FC | IPC-1000NF2 | IPC-3000NF2 |
|---|---|---|---|---|---|
| |  |  |  |  |  |
| **Производительность** | | | | | |
| **Производительность МЭ**, Мбит/с | до 22 300 | до 40 000 | – | до 40 000* | до 80 000* |
| **Производительность UTM**, Мбит/с | до 6 000 | до 7 000 | – | до 6 000 | до 7 000 |
| **Производительность IPS**, Мбит/с | до 6 500 | до 10 000 | – | до 6 500 | до 10 000 |
| **Производительность VPN**, Мбит/с | до 4 500 | до 8 000 | до 20 000 | до 4 500 | до 8 000 |
| **Максимальное число одновременных сессий МЭ** | 10 000 000 | 10 000 000 | 10 000 000 | 10 000 000 | 10 000 000 |

КОД безопасности

# Российские платформы Континент

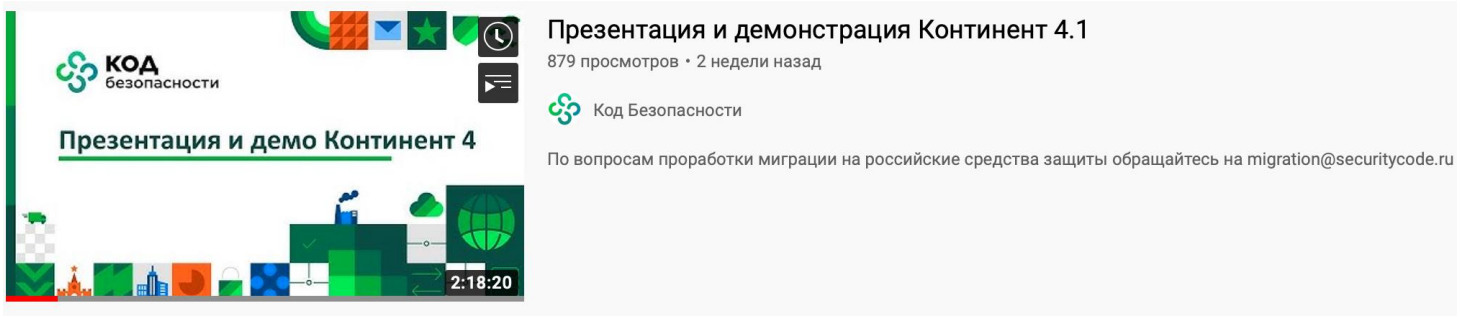

| Платформа | Производи-тельность МЭ, Mbit/s | Производи-тельность UTM, Mbit/s | Производи-тельность VPN, Mbit/s |
|---|---|---|---|
| IPC-R10 | 1300 | 600 | 250 |
| IPC-R50 | 1800 | 1000 | 350 |
| IPC-R300 | 4000 | 1200 | 450 |
| IPC-R550 | 6000 | 2000 | 1000 |

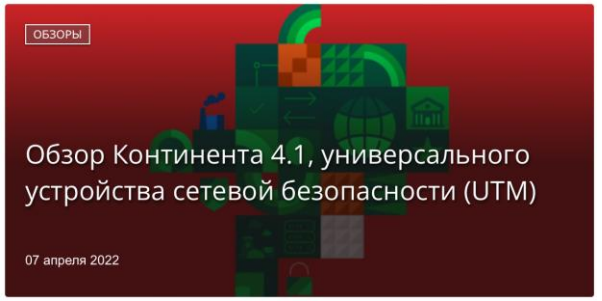
# Что дальше?

Тестирование на виртуальном стенде

Проработка перехода с помощью команды migration@securitycode.ru

Обмен опытом в телеграм-чате @apksh




https://www.youtube.com/watch?v=-j1qUiSAxfY

https://www.anti-malware.ru/reviews/Kontinent-41

КОД безопасности


Шутенко Александр

ООО «Код Безопасности»

Моб.: +7 (904) 482 44 83

E-mail: a.shutenko@securitycode.ru