КОД безопасности

Верить в наше время нельзя никому, порою даже самому себе.

Код Безопасности и Zero Trust Networking

КОД безопасности

Что такое Zero Trust?

Zero Trust обозначает полное отсутствие доверия кому-либо – даже пользователям внутри периметра. Модель подразумевает, что каждый пользователь или устройство должны подтверждать свои данные каждый раз, когда они запрашивают доступ к какому-либо ресурсу внутри или за пределами сети.

КОД безопасности

Проблема избыточного доверия

Подключение к хосту происходит здесь

Данные	Прикладной доступ к сетевым службам
Данные	Представления представление и кодирование данных
Данные	Сеансовый Управление сеансом связи
Блоки	Транспортный безопасное и надёжное соединие точка-точка
Пакеты	Сетевой Определение пути и IP (логическая адресация)
Кадры	Канальный MAC и LLC (Физическая адресация)
Биты	Физический кабель, сигналы, бинарная передача данных

КОД безопасности

Проблема избыточного доверия

Подключение к хосту происходит здесь

Данные	Прикладной доступ к сетевым службам
Данные	Представления представление и кодирование данных
Данные	Сеансовый Управление сеансом связи
Блоки	Транспортный безопасное и надёжное соединие точка-точка
Пакеты	Сетевой Определение пути и IP (логическая адресация)
Кадры	Канальный MAC и LLC (Физическая адресация)
Биты	Физический кабель, сигналы, бинарная передача данных

Аутентификация и шифрование реализованы здесь

КОД безопасности

Проблема избыточного доверия

Данные	Прикладной доступ к сетевым службам
Данные	Представления представление и кодирование данных
Данные	Сеансовый Управление сеансом связи
Блоки	Транспортный безопасное и надёжное соединие точка-точка
Пакеты	Сетевой Определение пути и IP (логическая адресация)
Кадры	Канальный MAC и LLC (Физическая адресация)
Биты	Физический кабель, сигналы, бинарная передача данных

Аутентификация и шифрование реализованы здесь

Подключение к хосту происходит здесь

А что, если код, обрабатывающий это подключение уязвим?

КОД безопасности

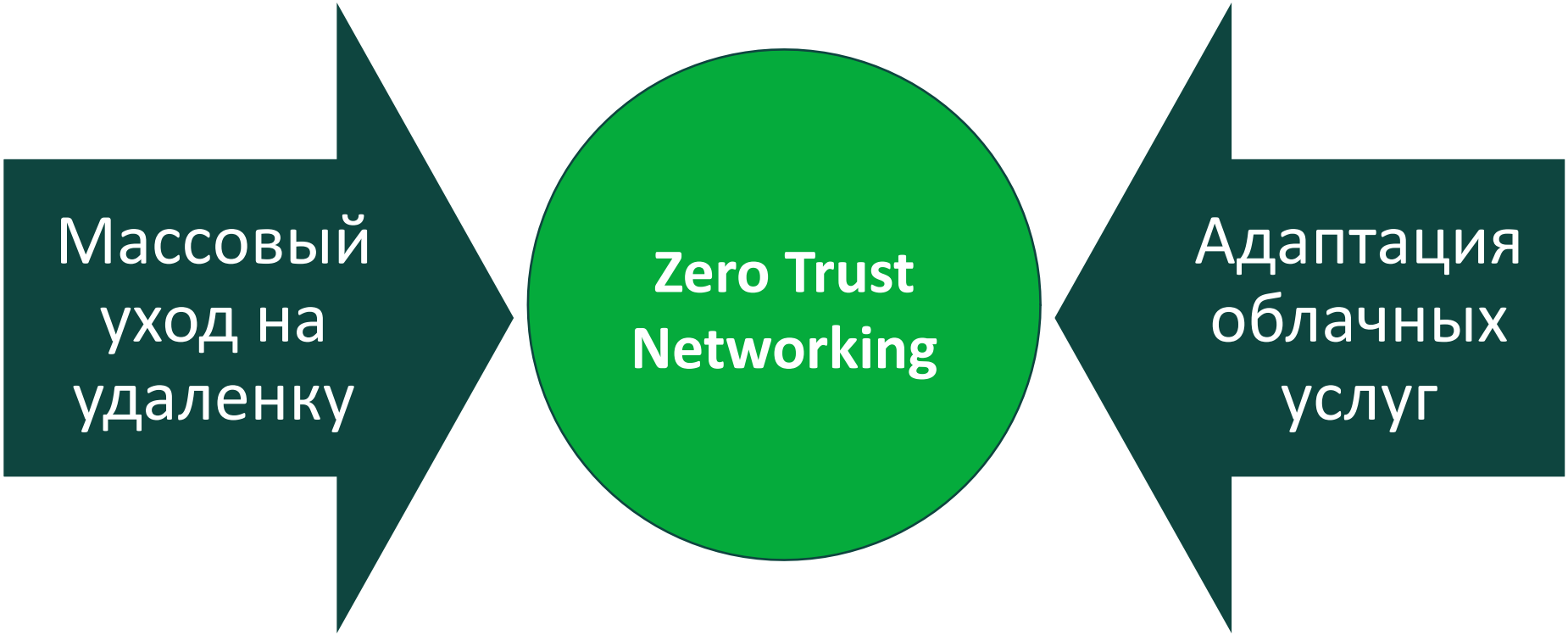
Необходимость в новом подходе

- Стек TCP/IP разрабатывался во времена, когда доверие удаленному хосту можно было допустить
- Сейчас это допущение ведет к повышенному уровню риска
- В этом контексте IP-адреса – плохие идентификаторы

Старая модель: Сначала подключаем, потом аутентифицируем
Новая модель: Сначала аутентифицируем, потом подключаем

КОД безопасности

Предпосылки новой эпохи



КОД безопасности

Ключевые положения Zero Trust Networking

Не доверяй без предварительной проверки!

КОД безопасности

Ключевые положения Zero Trust Networking

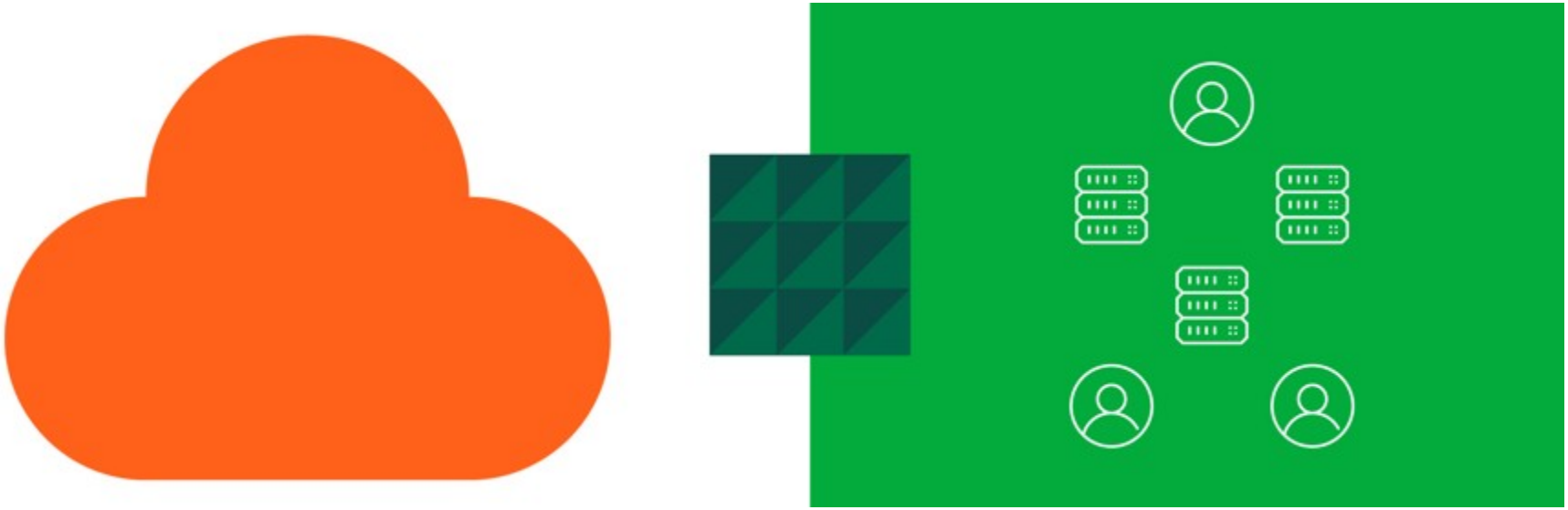
Не доверяй без предварительной проверки!

Компрометация произошла	Сеть, даже внутренняя, недоверенна	Все коммуникации должны быть зашифрованы	Местонахождение не влияет на уровень доступа
Требуется идентификация пользователя/ПК для создания доверия	Максимум проверок в точке подключения	Риск-ориентированный подход и принцип минимальных прав	Обнаружение аномалий и избыточного риска

КОД безопасности

Эволюция

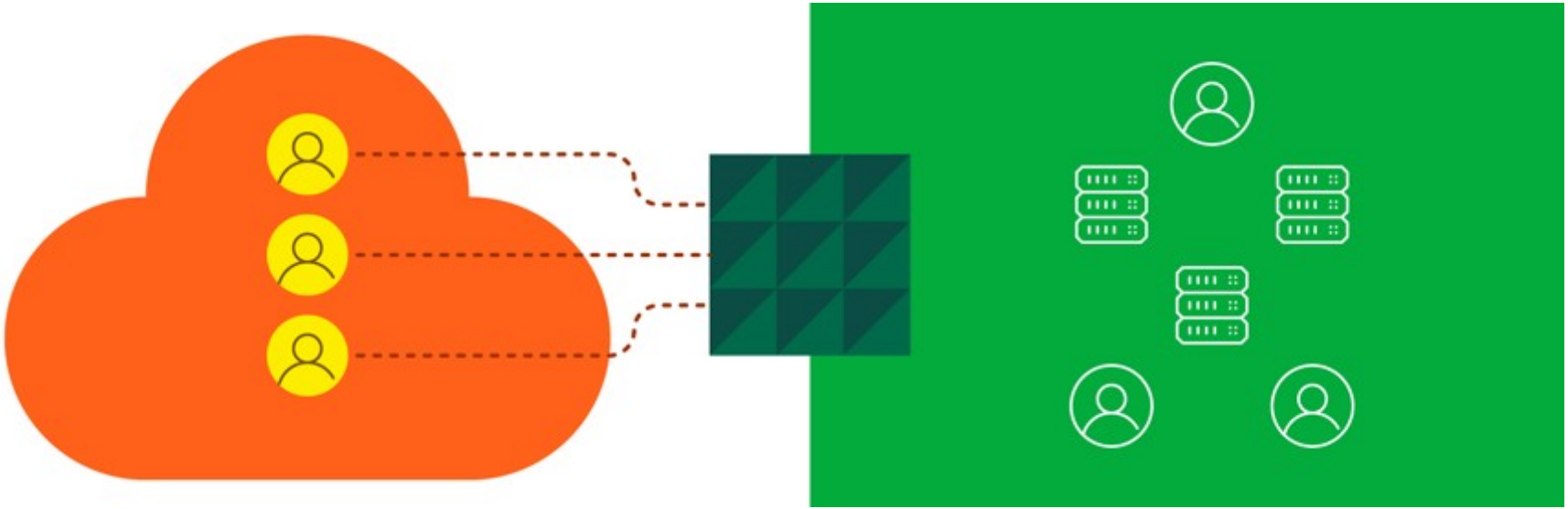
Все пользователи внутри сети



КОД безопасности

Эволюция

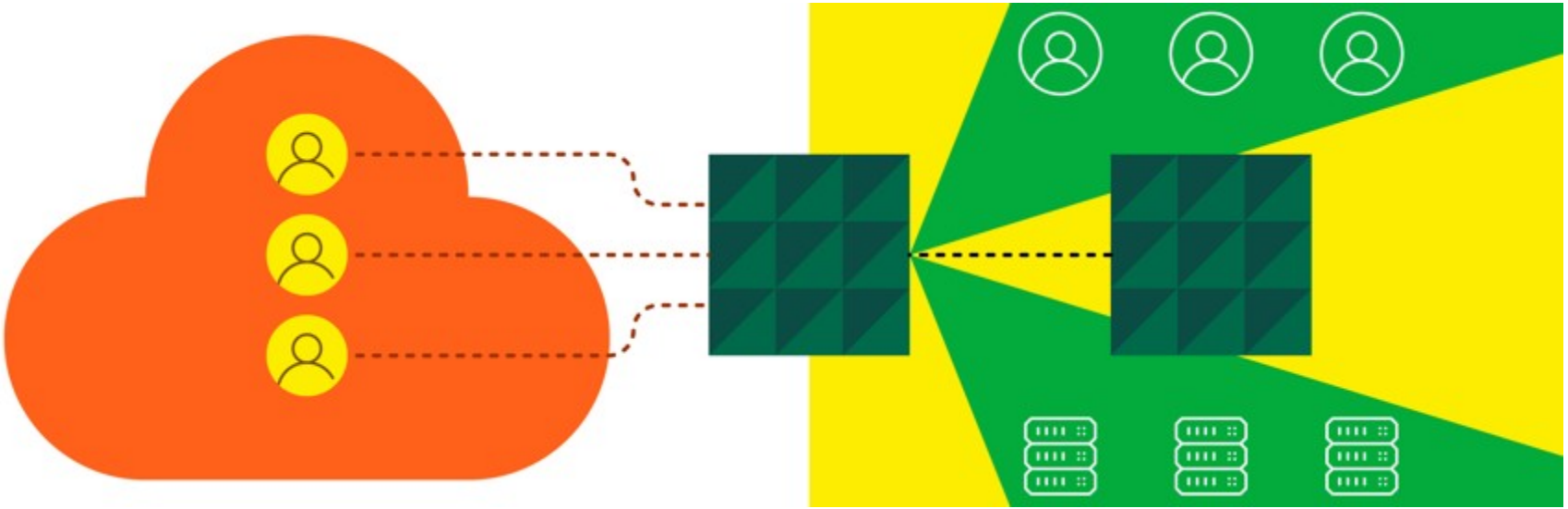
Появляются удаленные пользователи



КОД безопасности

Эволюция

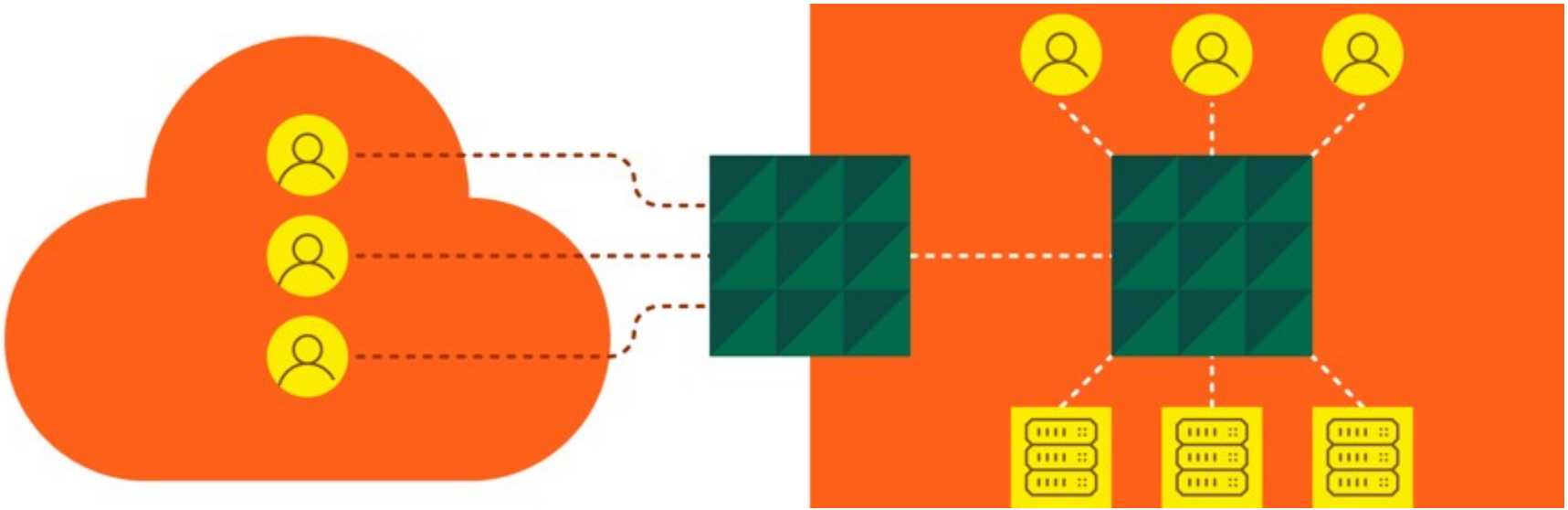
Появляются облака



КОД безопасности

Эволюция

Удаленные пользователи в облаках

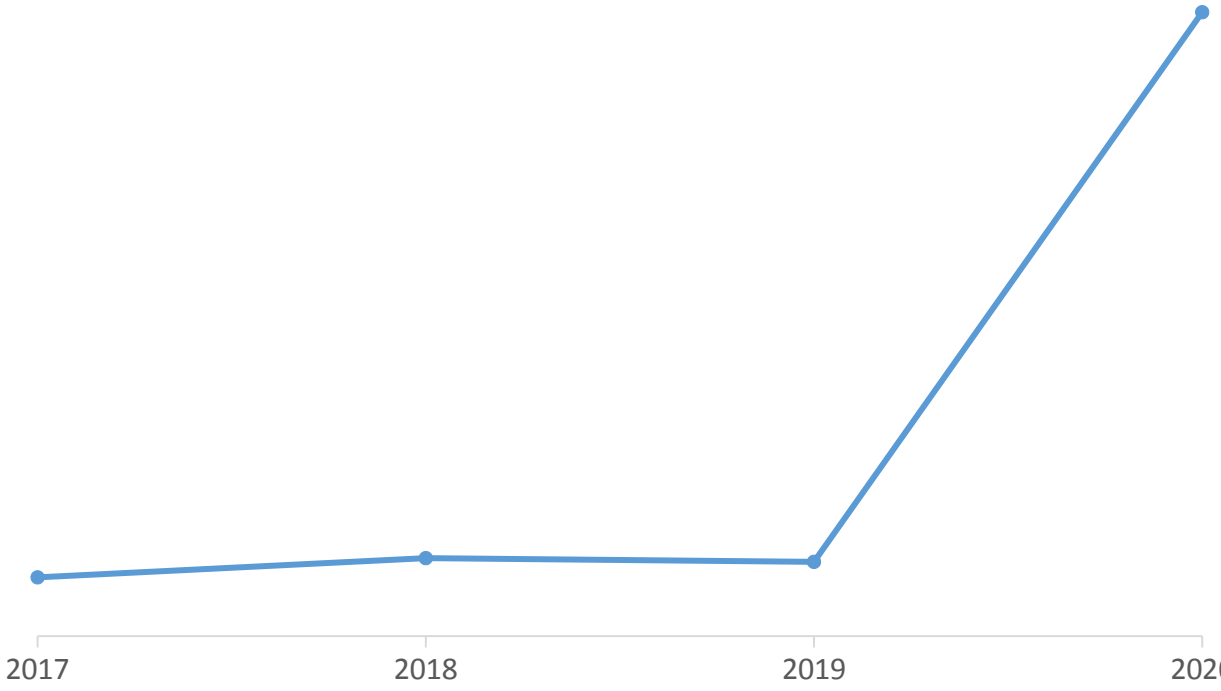


Remote Workers by Country

Source: Gartner (August 2020)
Note: See forecast methodology in Note 1 for information on base data.
727672

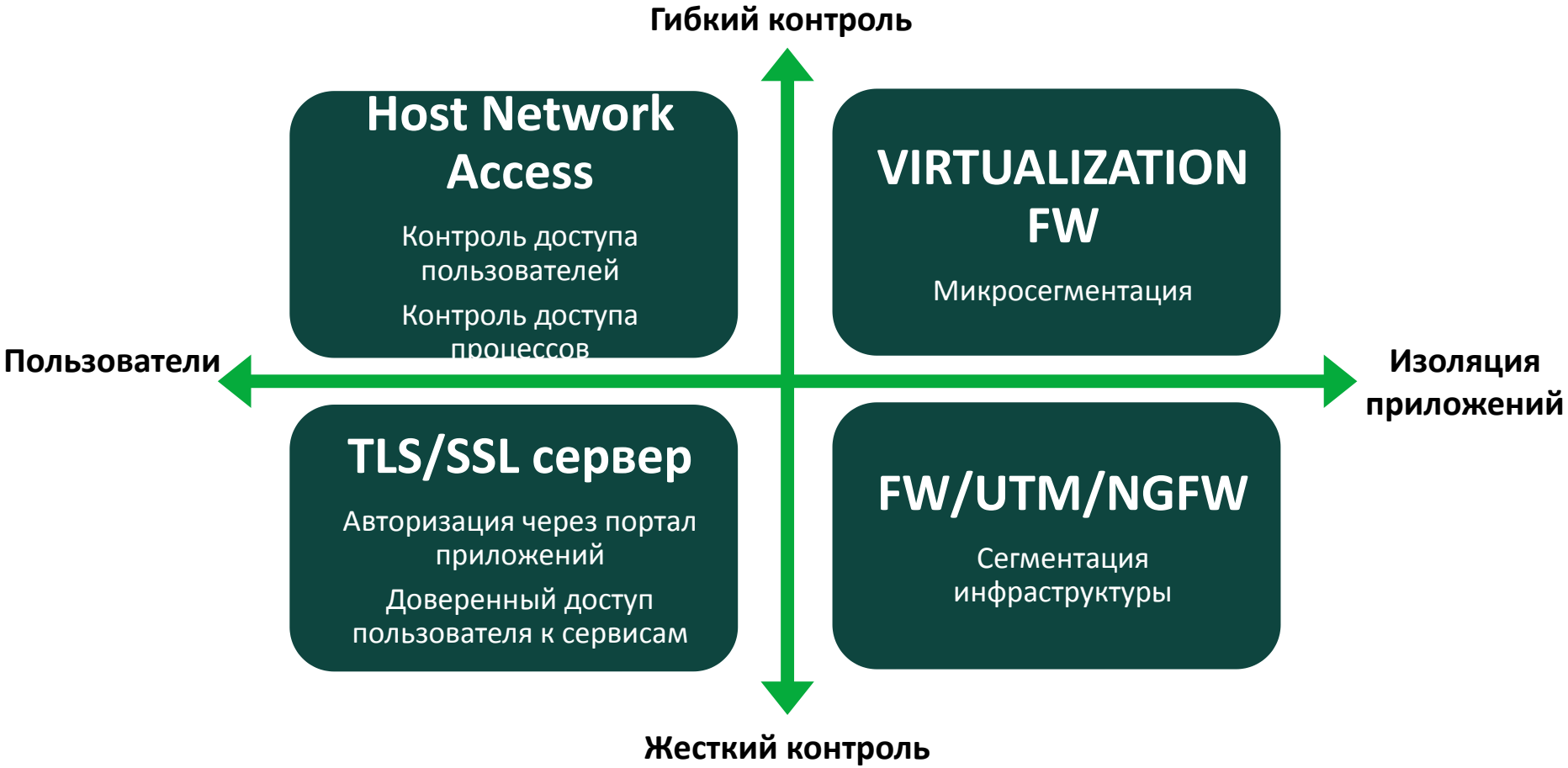
Gartner

Количество удаленных пользователей



Рост в 9 раз

Компоненты сети нулевого доверия



КОД безопасности

Резюме

Всё усложнилось. Опять.

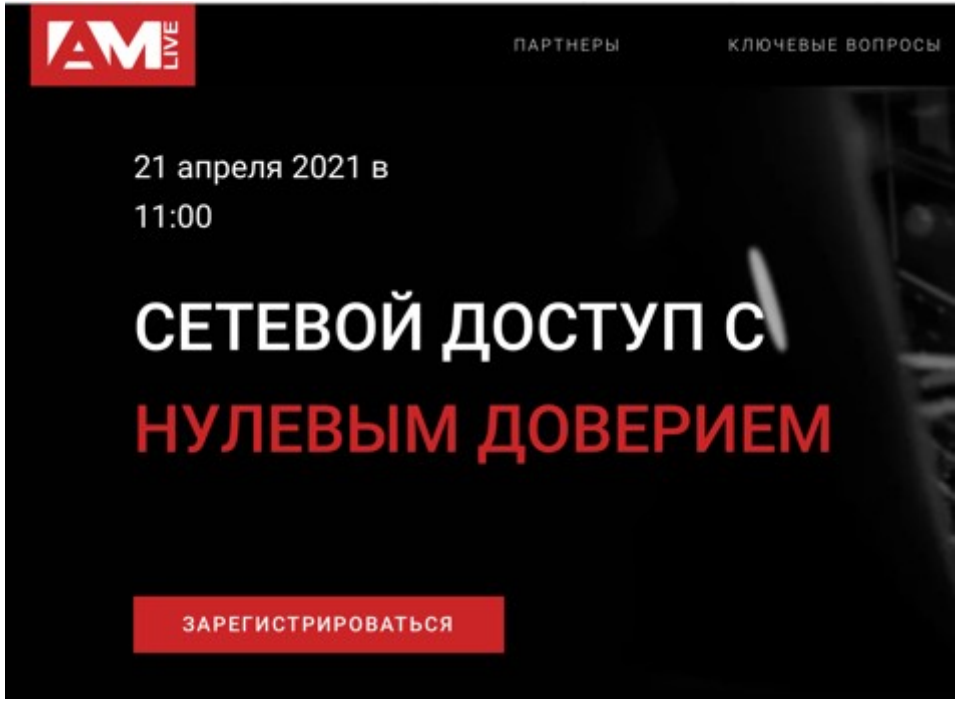
Все пользователи - удаленные

Абсолютная защита невозможна.

Но повысить ее до приемлемого уровня – реально.

КОД безопасности

Видео



https://live.anti-malware.ru/ztna

https://www.youtube.com/watch?v=7mUutYXKPJQ

КОД безопасности

Спасибо за внимание!
Вопросы?

Сергей Мущенко
s.mushchenko@securitycode.ru