# Решения Fortinet как базис MSSP платформы для сетевой безопасности

Владимир Дрюков, Директор центра мониторинга и реагирования на кибератаки PTK-Солар JSOC

SECURITYDAY

# Серьезно? Рассказ о безопасности периметра?

# Case 1 – не обычная, но типовая компания

- **1 Исполнительный аппарат**
- **2 ЦОД**
- **18 филиалов**
- **70+ ДЗО**
- **Везде есть мелкие сервисы на периметре**
- **Из-за задержек каналов до ЦОД – разделенный доступ в интернет**

# Посчитаем защиту

- Кластер на площадке - $$$$
- ЗИП в филиале и ДЗО - $$
- Локальный специалист для обслуживания - $

---

x*(80+18)

=

$$$$$$$$$$$$$$$$

# С вовлечением поддержки интегратора

- Кластер на площадке - $$$$
- ЗИП в филиале и ДЗО - $$

---

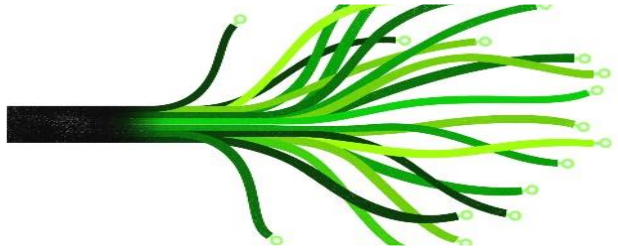
x*(80+18)

- Сервис интегратора - $$$$$

=

$$$$$$$$$$$$$$

# Смежные проблемы

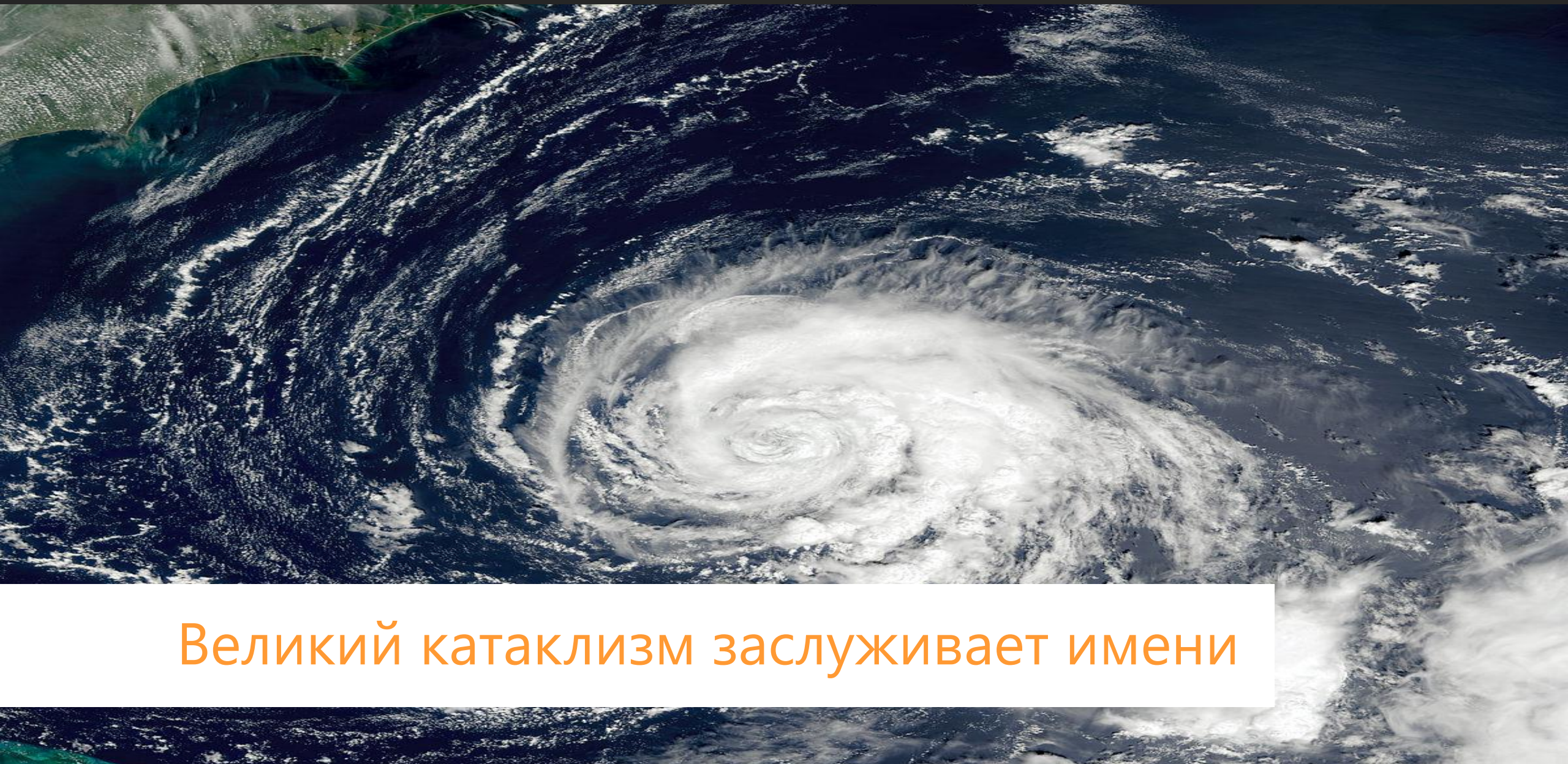


Децентрализованный доступ в Интернет – сложность управления и диагностики

Разорванность политик и контроля за их соблюдением

Необходимость ресурса для локальной диагностики проблемы

# Великий катаклизм заслуживает имени



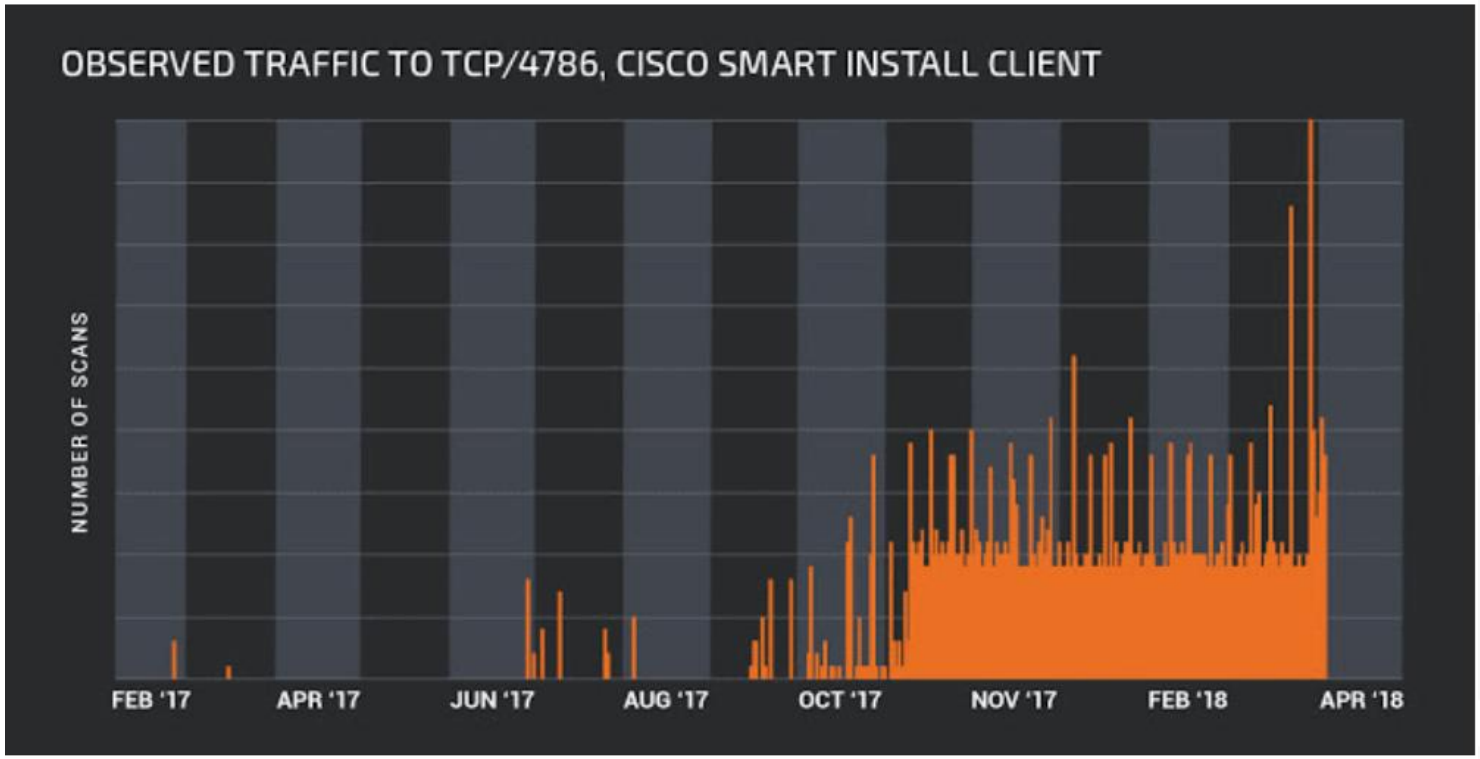
# Великий катаклизм заслуживает имени

# Великий катаклизм заслуживает имени

# Великий катаклизм заслуживает имени

# У нас свои катаклизмы

# У нас свои катаклизмы

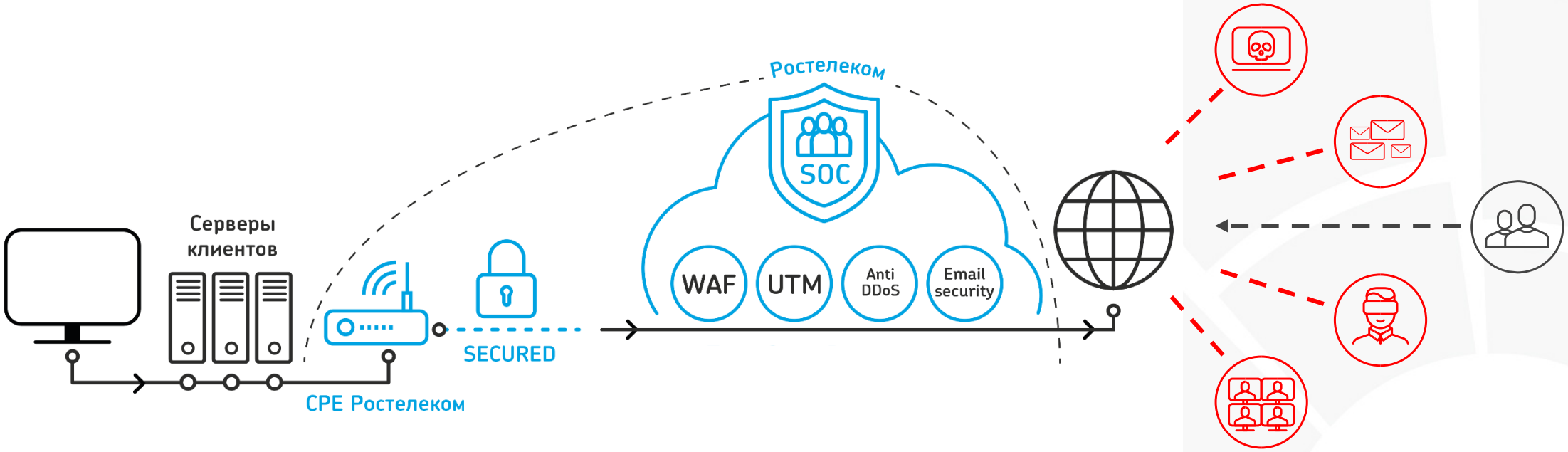



В настоящее время аналитики Cisco Talos обнаружили в интернете более 168 000 устройств

# И курьезы

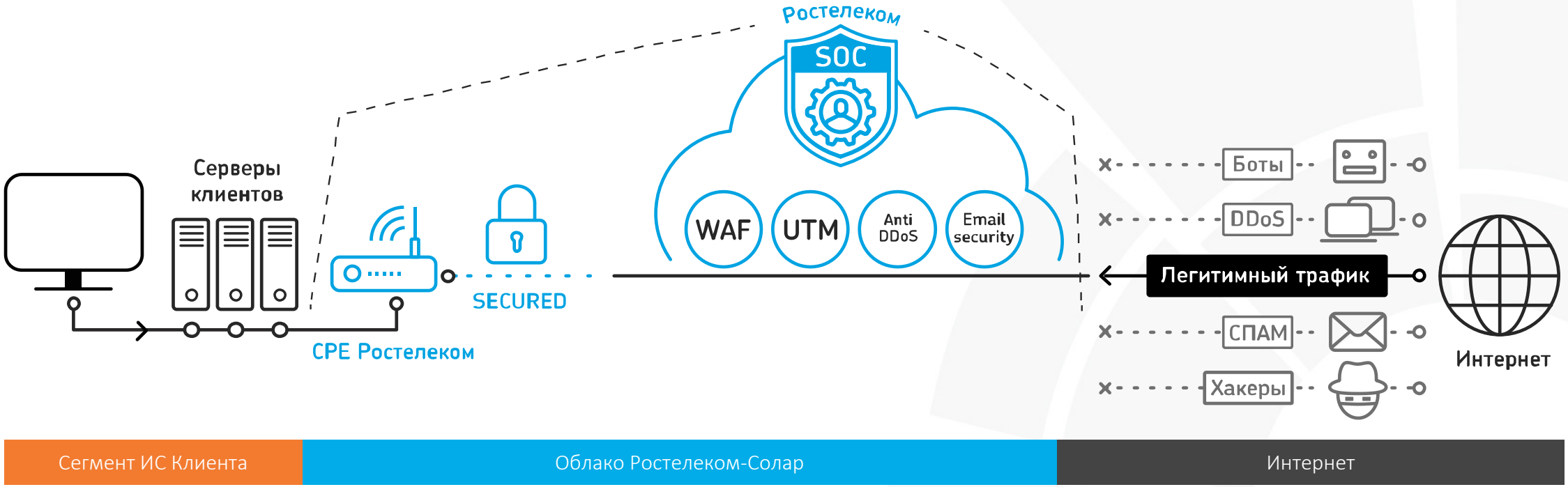
https://www.shodan.io/host/54.204.196.174

# Сервисный подход TelcoCloud




| Сегмент ИС Клиента | Облако Ростелеком-Солар | Интернет |
|---|---|---|

# Сервисный подход TelcoCloud



# TelcoCloud Delivery and Response Team

**Архитектура и кастомизация (3 человека)**

**CERT (опыление правилами mitigation) (6 человек)**

**Сервис-менеджеры Telco (5 человек)**

## Telco Operations

**Эксперты (3 человека)**

**2-я линия 11*5 (6 человек)**

**1-я линия 24*7 (8 человек)**

# Преимущества подхода

- **Экономика:**
  - Централизованные ноды вместе мелких инсталляций;
  - Дешевый ЗИП CPE вместо дорого UTM;
  - Единые ресурсы для обслуживания
- **Повышение управляемости:**
  - Централизация и унификация политик;
  - Единая отчетность;
  - Простое масштабирование как вверх, так и вниз
- **Добавленная безопасность:**
  - Проактивные правила от критических и массовых атак
  - SOC PTK-Солар на страже сетевой безопасности

# Спасибо за внимание!

rt.ru
rt-solar.ru
info@rt-solar.ru
+7 (499) 755-07-70


FORTINET®