Вебинар

Как защититься от сетевых угроз быстро, эффективно и экономично

Ростелеком

О докладчике

Александр Баринов

Руководитель направления сервисов кибербезопасности компании Ростелеком-Solar

Занимаюсь созданием и развитием управляемых сервисов информационной безопасности (MSS)

Трансформирую российский рынок кибербезопасности

a.barinov@rt-solar.ru

Сетевые угрозы?

Сетевой периметр – главная цель киберпреступников

От защищенности сетевого периметра напрямую зависят непрерывность бизнес-процессов, оперативность принятия решений и репутация организации

Ростелеком

Масштаб сетевых угроз

47%

на столько выросло число инцидентов ИБ за один год

39%

всех атак нацелены на получение финансовой выгоды

49%

всех атак включали использование вредоносного ПО

54%

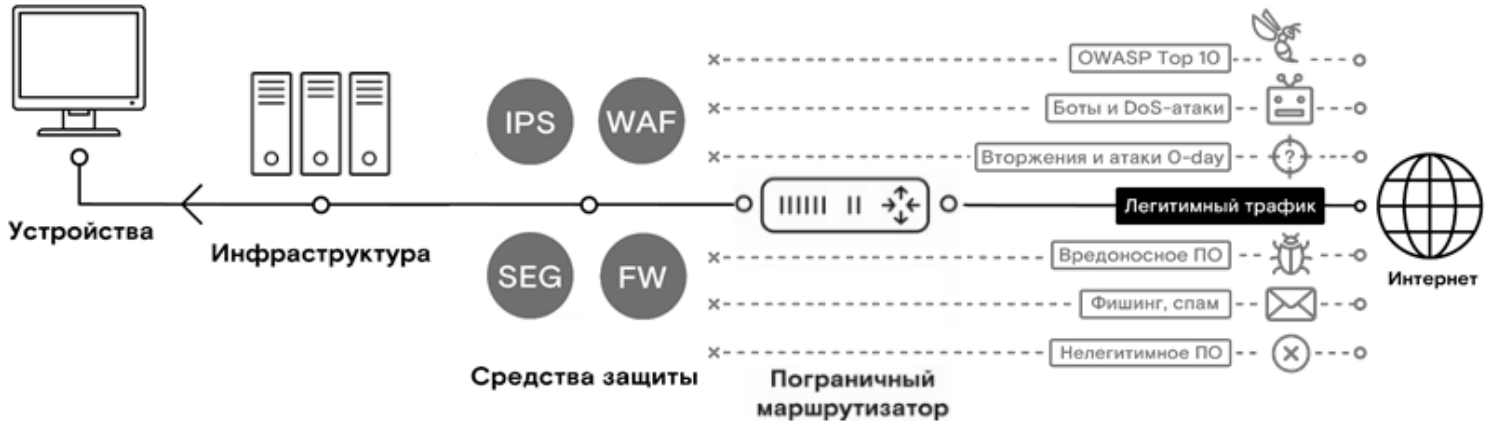
всех атак на организации были целевыми

Данные: Solar JSOC и Positive Technologies, 2018

Ростелеком

Как компании защищаются сегодня?

Все организационные и технические меры по защите информации применяются на площадке клиента



Ростелеком

Что предлагает интегратор?

Сложный проект, состоящий из следующих этапов:

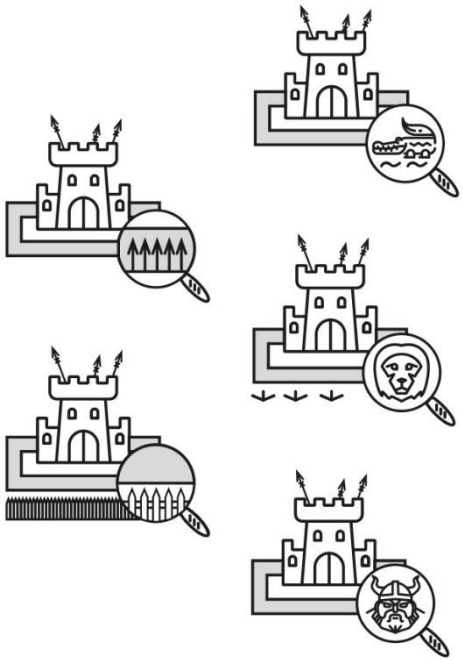
- Обследование информационной инфраструктуры
- Разработка модели нарушителя и угроз безопасности информации
- Разработка технического задания и технического проекта на создание системы защиты
- Внедрение системы защиты
- Передача системы в промышленную эксплуатацию
- Работы по ее обслуживанию

Box moving

Проект интегратора = перемещение коробочного решения к клиенту

Интегратор	Клиент
Мгновенная выручка за продажу «коробки»	Расходы на специалистов по ИБ для эксплуатации средств защиты

Традиционный подход



Традиционный подход можно сравнить со средневековьем, когда каждое предприятие и каждый филиал строят вокруг себя стены, выкапывают рвы, ощетиниваются пиками и т. д.

Инновационный подход к защите – сервисная модель

Периметровые средства защиты размещаются в инфраструктуре сервис-провайдера и эксплуатируются силами его специалистов

Ростелеком

Сервисная модель как идеология

Безопасность как сервис – это:

- Безопасность как функция,
  а не конструктор из технологий
- Безопасность в темпе – здесь и сейчас
- Безопасность без кадровых ограничений

Безопасность как сервис – мировой тренд

15%

доля рынка управляемых сервисов кибербезопасности (Managed Security Services, MSS) на мировом рынке ИБ

×3,6

инвестиции в технологии, предоставляемые в сервисной модели, больше, чем в традиционной

24/7

Обеспечение кибербезопасности в круглосуточном режиме без выходных и праздников

Ростелеком

Цифровизация

Еще одним активным драйвером перехода к сервисной модели обеспечения кибербезопасности является цифровизация экономики

Новый подход

Цивилизованное взаимодействие между предприятиями и филиалами, охранные функции отданы под централизованное управление

Ростелеком

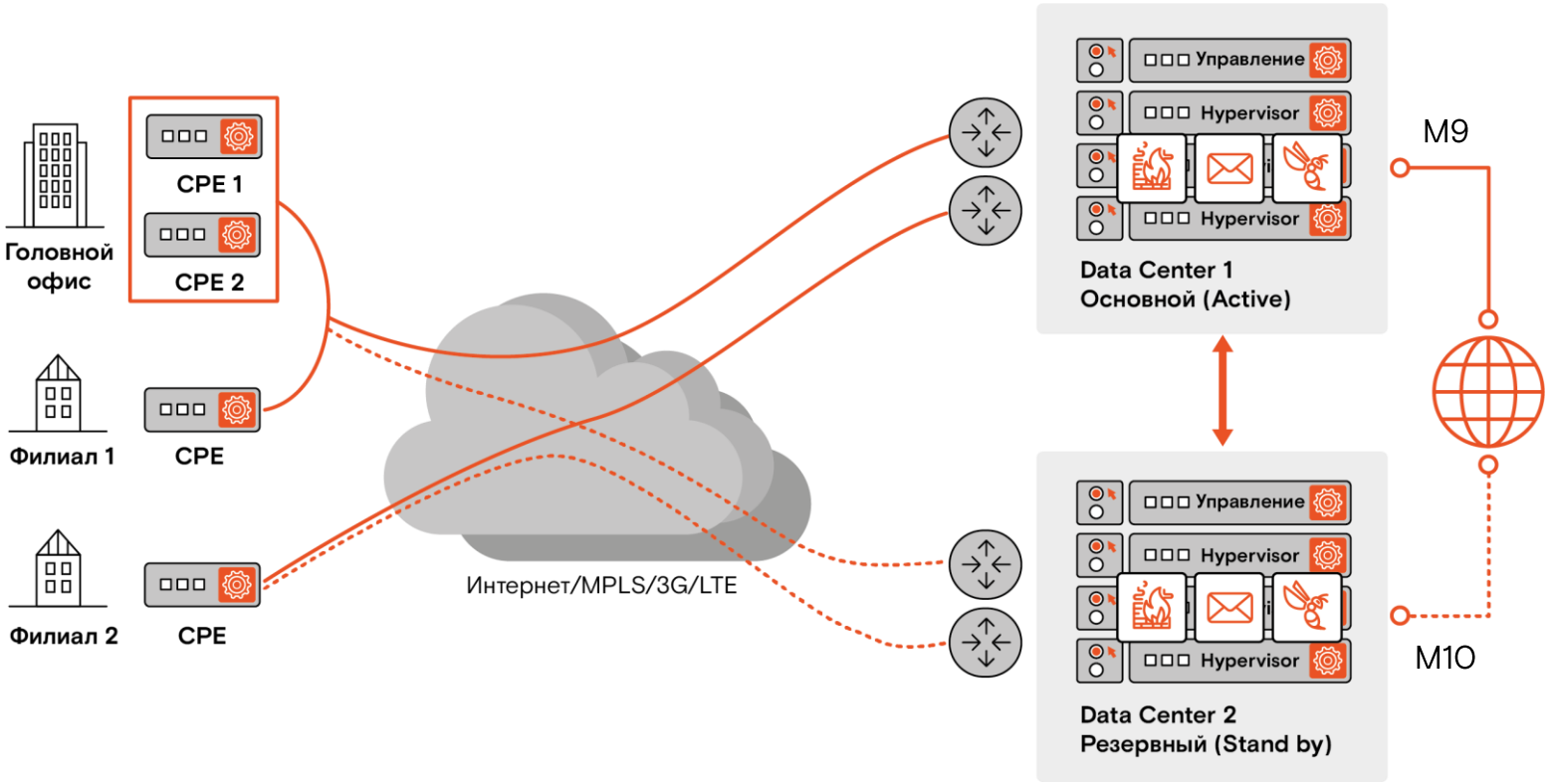
Единая платформа сервисов кибербезопасности

ЕПСК – платформа для размещения сервисов информационной безопасности, предназначенных для защиты информационных ресурсов заказчиков от актуальных угроз безопасности информации

ЕПСК использует передовые технологии (ZTP, SD-WAN) и является первым и единственным проектом такого рода в России

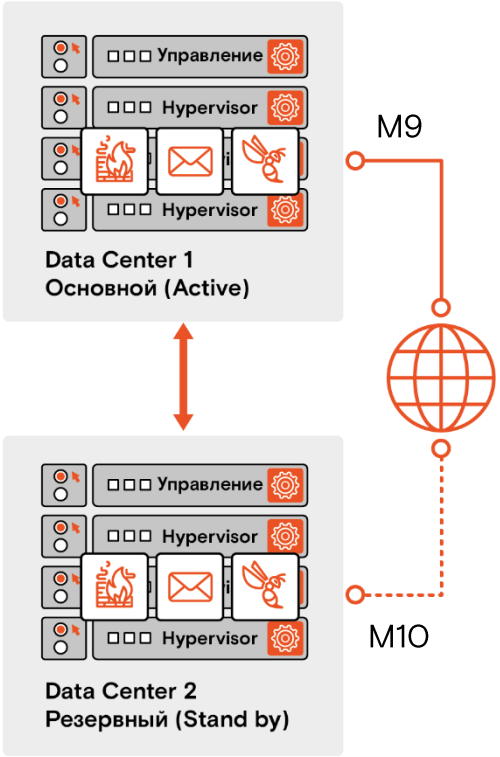
Ростелеком

Архитектура платформы



Ростелеком

Архитектура платформы



Ядро сервисной платформы сейчас базируется в двух георасределенных ЦОД, что обеспечивает резервирование инфраструктуры и сервисов

Во второй половине 2019 года появится третий ЦОД

Ростелеком

Архитектура платформы

Customer Premises Equipment (CPE) — телекоммуникационное оборудование, которое устанавливается на стороне клиента. Предназначено для передачи трафика между ЦОД Ростелекома и инфраструктурой клиента.

Задачи

- Подключения к локальной сети
- Перенаправления трафика в ЦОДы платформы
- Формирование шифрованного туннеля до платформы
- Обеспечение сетевой связности между офисами по схеме Full Mesh
- Организация отказоустойчивого подключения

Архитектура платформы

Zero Touch Provisioning – обеспечивает автоматическую настройку CPE без участия пользователя. Это позволяет развертывать сервисы кибербезопасности максимально быстро

SD-WAN – создает единую точку управления всей инфраструктурой. При перенастройке одного CPE обновления распространяются на все CPE в сети. Это позволяет быстро изменять параметры оказываемых сервисов

CPE

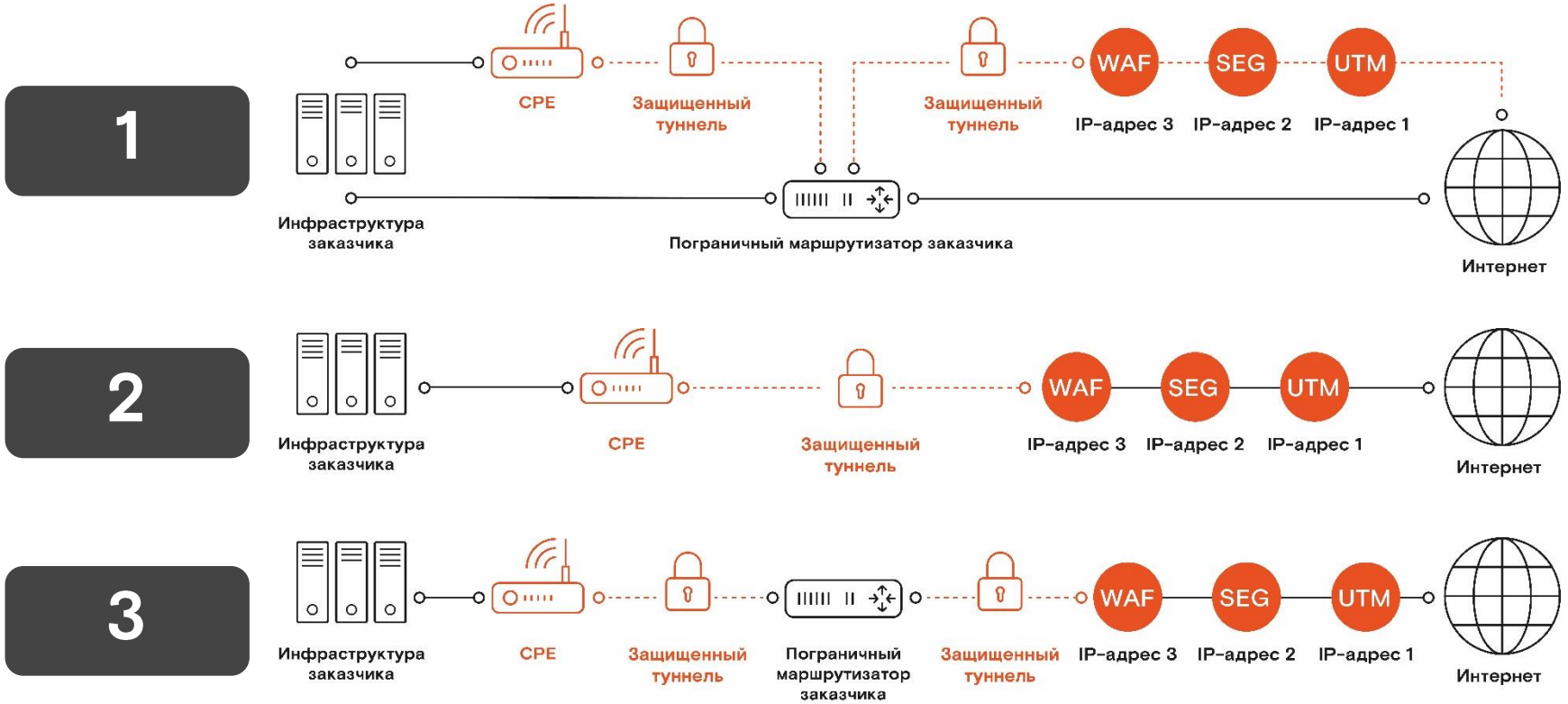
до 70 Мбит/с

до 200 Мбит/с

до 1 000 Мбит/с

Ростелеком

Варианты подключения



Ростелеком

Первые сервисы

Ростелеком

Сервисы сегодня

Ростелеком

Экосистема сервисов сегодня и завтра

- Сервис защиты от сетевых угроз (UTM)
- Сервис защиты электронной почты (SEG)
- Сервис защиты веб-приложений (WAF)
- Сервис защиты от DDoS-атак (Anti-DDoS)
- Новые сервисы – СКОРО

FORTINET ARBOR NETWORKS POSITIVE TECHNOLOGIES + Check Point SOFTWARE TECHNOLOGIES LTD

Ростелеком

Классический подход к защите сетевого периметра

Использование набора специализированных средств защиты

- Межсетевой экран (FW)
- Система предотвращения вторжений (IPS)
- Антивирусное ПО
- Веб-фильтры

=

- Дублирование функций
- Конфликт решений от различных вендоров
- Сложности при организации взаимодействия и управления этими системами

Комплексная безопасность сетевого периметра

Использование комплексной системы безопасности сетевого периметра

- Межсетевой экран (FW)
- Система предотвращения вторжений (IPS)
- Антивирусное ПО
- Веб-фильтры
- Контроль приложений
- Единая консоль управления функциями безопасности

=

UTM

Ростелеком

UTM требует

- Правильной настройки
- Постоянного обновления сигнатур
- Надзора ИБ-специалиста
- Расходов на амортизацию
- Периодического обновления лицензий
- Затрат на масштабирование
- Соблюдения условий эксплуатации

Много денег

Ростелеком

Решение проблем – UTM как сервис

- Размещается в облачной инфраструктуре Ростелеком
- Является частью Единой платформы сервисов кибербезопасности (ЕПСК)
- Управляется командой Solar JSOC – центра мониторинга и реагирования №1 в РФ
- Трафик между ЕПСК и заказчиком передается с помощью CPE по защищенному туннелю
- CPE управляются и конфигурируются автоматически, что позволяет подключать новые локации менее чем за 24 часа

Преимущества UTM как сервиса

- Объединение разрозненных функций защиты сети
- Централизация точек выхода в Интернет
- Мгновенное применение единых ИБ-политик
- Снижение затрат на ИБ-персонал и оборудование
- Применение актуальных настроек и сигнатур
- Единая система статистики по ИБ
- Подключение новых точек за 24 часа
- Мониторинг и реагирование в режиме 24×7

Ростелеком

Решаемые задачи

Комплексная борьба
с сетевыми
угрозами

Централизация
доступа в сеть
для филиалов

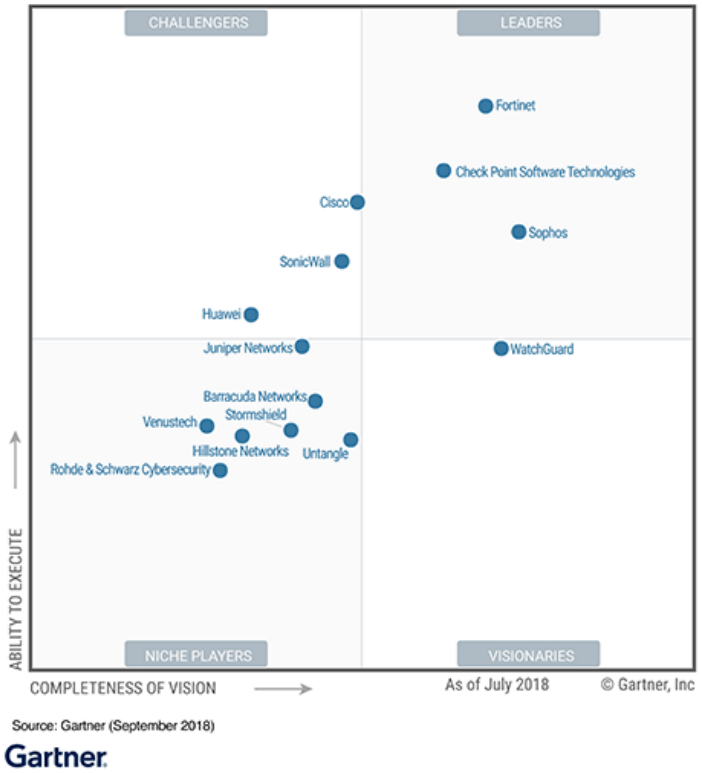
Применение
единых политик
безопасности

Защита от атак
в режиме
24×7×365

Схема работы сервиса

Ростелеком

Что «под капотом» сервиса UTM



Source: Gartner (September 2018)

Gartner

FORTINET

FortiGate™ Virtual Appliances

Ростелеком

Варианты сервиса UTM

FW

- Только межсетевой экран

FW+IPS

- Межсетевой экран
- Система предотвращения вторжений (IPS)

UTM

- Межсетевой экран (FW)
- Система предотвращения вторжений (IPS)
- Антивирусная фильтрация
- Веб/контент-фильтрация
- Контроль приложений
- Remote Access VPN
- Проверка SSL- и SSH-трафика

Преимущества сервиса

Экономия и эффективность

Снижение стоимости владения

Совокупная стоимость владения сервисами дешевле покупки, внедрения и последующей поддержки ИБ-решений

Устранение дефицита кадров

Отсутствие необходимости создания отдела из высококвалифицированных ИБ-специалистов

Экономия

Снижение затрат на оборудование и персонал, перевод капитальных издержек в операционные

Профессиональная команда

Настройка, обслуживание и разбор инцидентов безопасности лучшими специалистами отрасли

Технологичность и надежность

Доступность

Защита и мониторинг 24 часа в сутки без перерывов и выходных

Надежность

Эксплуатация распределенной отказоустойчивой инфраструктуры

Гибкость

Простая масштабируемость и быстрое изменение параметров услуги

Скорость

Быстрое подключение к сервисам и оперативное реагирование на инциденты

Соблюдение законодательства

Соответствие требованиям

Выполнение требований по информационной безопасности

Подходящие средства защиты

Эксплуатация сертифицированных решений лидирующих вендоров

Лицензии регуляторов

Компания является лицензиатом ФСТЭК России, ФСБ России и Минобороны России

Отслеживание изменений

Меры защиты всегда соответствуют всем новым законам и регламентам

Развитие сервисов управляемой безопасности

Ростелеком

О компании

ПАО «Ростелеком» – крупнейший в России провайдер цифровых услуг и решений, присутствующий во всех сегментах ИКТ-рынка

№1

провайдер
цифровых услуг

350+

точек доступа в России
и за рубежом

250

крупных российских компаний
под защитой

Ростелеком

Лицензии

Лицензии Ростелеком-Solar (компания ПАО «Ростелеком»)

- Минобороны России – на проведение работ, связанных с созданием средств защиты информации
- ФСБ России – на проведение работ, связанных с использованием сведений, составляющих государственную тайну
- ФСБ России – на разработку, производство и распространение шифровальных (криптографических) систем
- ФСТЭК России – на деятельность по технической защите конфиденциальности информации
- ФСТЭК России – на деятельность по разработке и производству средств защиты конфиденциальной информации
- Соглашение с ФСБ России в рамках ГосСОПКА о взаимодействии по предупреждению кибератак

География компании Ростелеком

Ростелеком

Основные тезисы

- Непрерывность бизнес-процессов зависит от защищенности сетевого периметра
- Традиционный подход к защите устарел и неэффективен
- Будущее за сервисной моделью безопасности
- Важна – экосистема сервисов и вектор ее развития
- UTM – комплексный подход к защите сетевого периметра, но при этом требует существенных вложений со стороны компании
- Решение данной проблемы – сервис, это удобнее и дешевле

Что дальше?

Задать вопросы Александру Баринову

+7 (499) 755-07-70

a.barinov@rt-solar.ru

Узнать подробнее или заказать сервис

utm@rt-solar.ru

Ростелеком

Предстоящие вебинары

Иван Мирошниченко

Руководитель направления развития сервисов кибербезопасности

09.07.2019

Новый взгляд «Ростелекома» на защиту веб-приложений

Ростелеком