Защита от DDoS-атак для госзаказчиков

МегаФон

Почему МегаФон?

Лидерство в цифровой экономике

Создаем цифровые проекты и продукты для задач Цифровой экономики:
ГЕОП, Частные Облака, Индустрия 4.0, **Цифровой бизнес**, **Умный город**, **Цифровое госуправление**

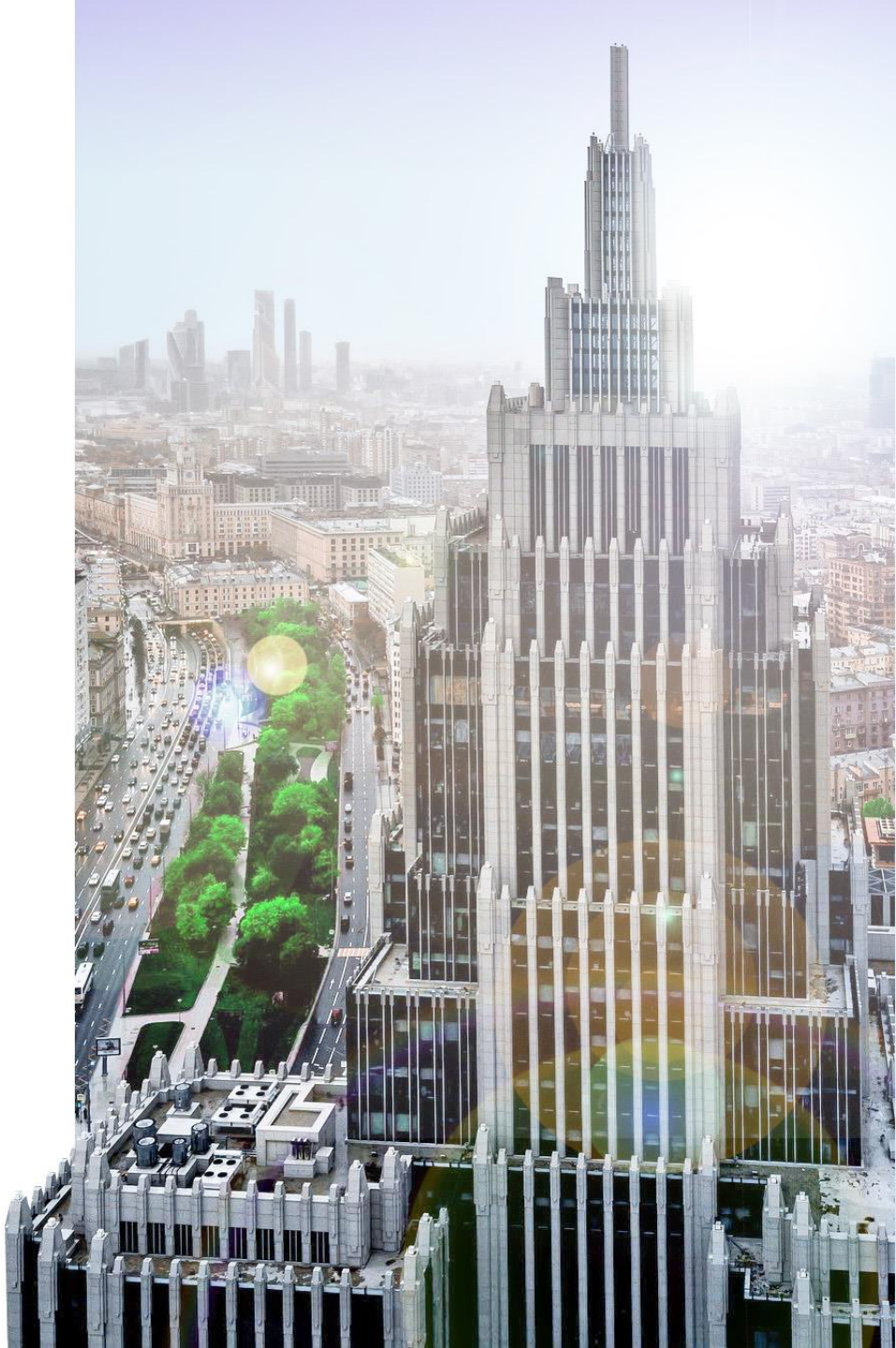
Развитие необходимых государству инноваций

Создаем комплексные проекты для государства и бизнеса, внедряем самые современные технологии, предлагаем полный спектр услуг для всех сфер деятельности: от облачных технологий и кибербезопасности до интернета вещей

Разносторонние компетенции в группе компаний

Обладаем многолетним опытом в создании решений для различных отраслей и направлений деятельности. Сертифицированные специалисты из единой группы компаний МегаФона способны решить любые задачи государственного заказчика

МегаФон



Защита от DDoS-атак

DDoS-атака — это экстремально большое количество запросов, отправляемых злоумышленником на ресурсы компании с целью перегрузить их и ограничить к ним доступ для пользователей.

Этот метод кибератаки используется во множестве сценариев: для дискредитации компании-владельца ресурса, ограничения ее деятельности, получения выкупа или для отвлечения внимания, пока происходит другое преступление (например, кража данных).

Наиболее частые цели DDoS-атак — это государственные и образовательные учреждения, средства массовой информации, а также финансовый и промышленный секторы.

Решение компании МегаФон построено на базе сертифицированных отечественных технологий и защищает информационные ресурсы от DDoS-атак любого формата и мощностью до 300 Гбит/с.

МегаФон

Законодательная и нормативно-правовая база

Федеральный закон от 27.07.2006 N 152-ФЗ «О персональных данных»:
DDoS-атака способствует краже данных, включая персональные.
Меры по защите персональных данных должны включать в себя защиту от подобных атак.

Федеральный закон от 26.07.2017 N 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (о безопасности КИИ РФ):
В соответствии с законом все КИИ должны функционировать бесперебойно. Защита от DDoS-атак позволяет исполнять этот закон в полной мере и повышает работоспособность КИИ.

Федеральный закон от 09.02.2009 N 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления»:
В соответствии с законом все государственные информационные ресурсы должны функционировать бесперебойно. Защита от DDoS-атак позволяет предоставлять непрерывный доступ населения к сайтам госведомств.

МегаФон

От каких атак защитит решение МегаФона

Flood Attacks
Атаки, переполняющие каналы связи за счет отправки большого числа запросов, не приводящих к установке соединения и создающих очередь «полуоткрытых соединений». Сервер перестает отвечать, а создание новых подключений невозможно

Amplification Attacks
Атаки с использованием эффекта усиления (амплификатора) для увеличения мощности. Сравнительно небольшие ресурсы злоумышленника становятся причиной значительно большего ущерба или полного отказа работы системы-жертвы

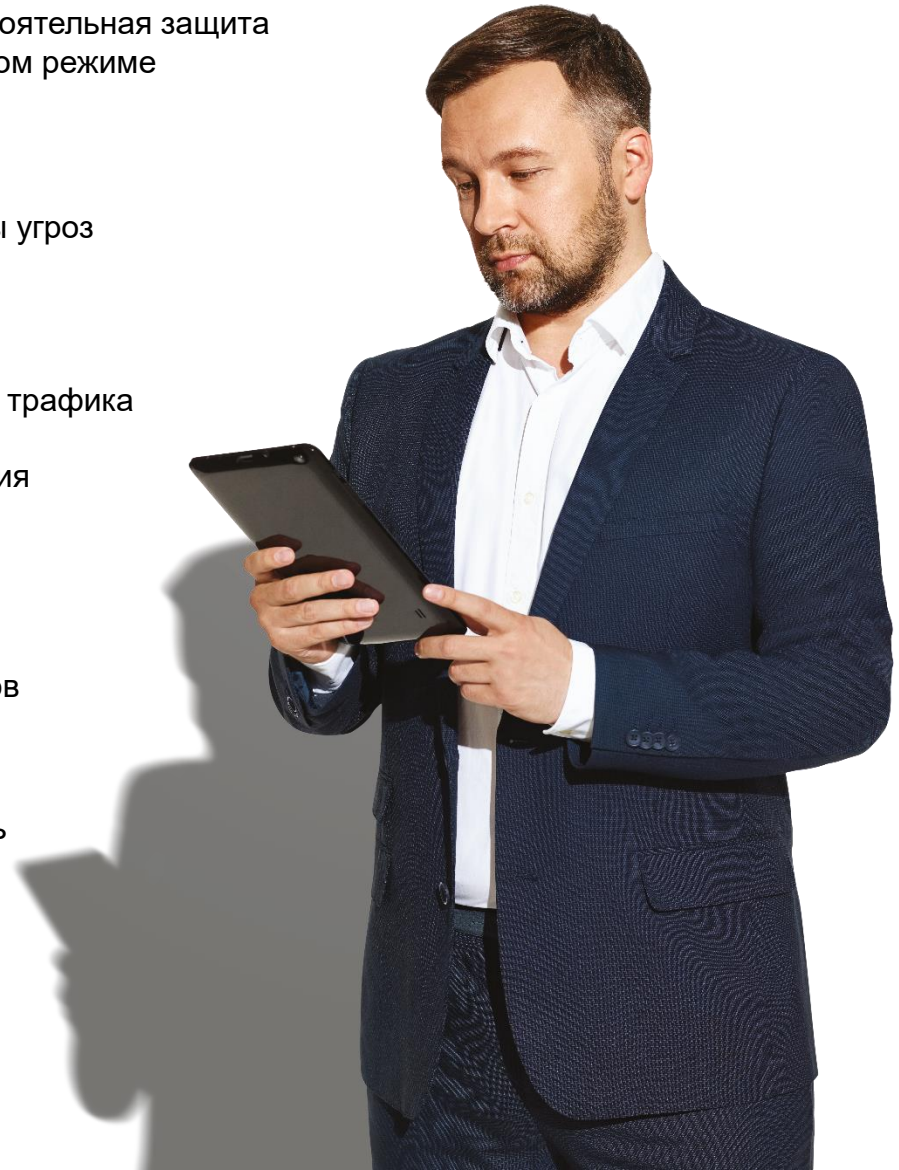
Volumetric Attacks
Атаки, перегружающие каналы или оборудование для препятствования работе сервиса. Уровни OSI 3-4

«Медленные» атаки
Отправка большого числа запросов, передающихся с очень медленной скоростью, из-за чего ресурсы сервера используются гораздо дольше, что мешает обработке запросов других пользователей

Application Layer Attacks
Атаки на приложения (веб-серверы, серверы баз данных, VoIP-телефонию и т.д.). Уровень OSI 7 – без раскрытия трафика SSL

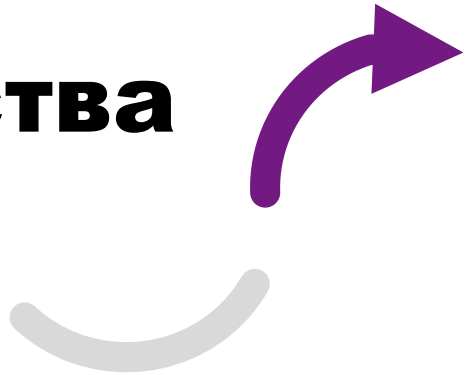
Технические возможности решения

- Отражение атак без покупки и установки нового оборудования или изменения сетевых настроек
- Отражение DDoS-атак мощностью до 300 Гбит/с на 3-4 уровнях модели OSI
- Автоматическое отслеживание и очистка трафика, включая NetFlow, в течение 5-15 секунд с технологией Fast Flood Detection
- Наличие собственной магистральной сети, что ускоряет процессы передачи данных по сети
- Блокировка паразитного трафика в сетях вышестоящих операторов с использованием BGP Flowspec и Blackhole
- Два варианта защиты: подавление в автоматическом режиме и самостоятельная защита через личный кабинет в ручном режиме
- Ежедневное обновление базы угроз
- Фильтрация зашифрованного трафика (HTTPS) в случае установки дополнительного оборудования
- Возможность «очистки» одного отдельного IP-адреса, а не в составе сети IP-адресов
- Гарантированная доступность услуги (SLA 99,9%)



МегаФон

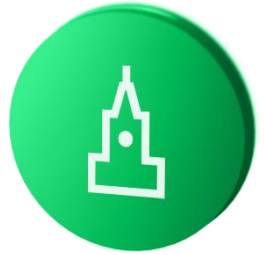
Преимущества решения



Подключение как в сети МегаФона, так и других операторов

Служба мониторинга и реагирования, работающая в режиме 24/7

Удобный русскоязычный личный кабинет



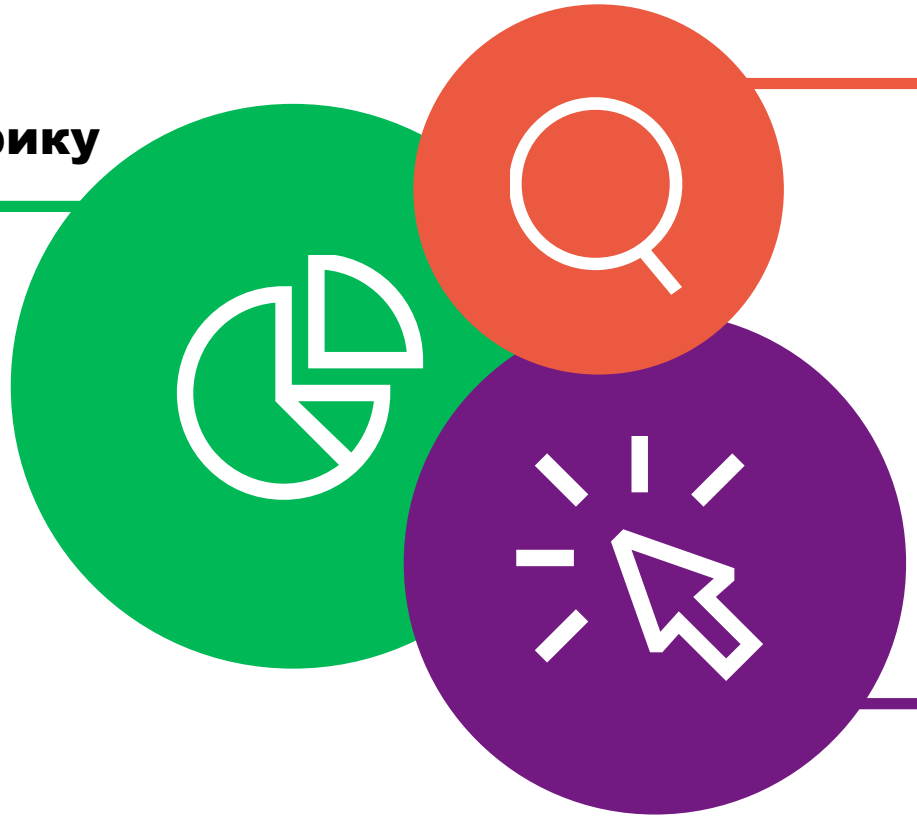
Отечественное ПО, сертифицированное ФСТЭК России (АПК Периметр)

МегаФон

Личный кабинет

Статистика по трафику

– Входящий трафик
– Исходящий трафик
– Отброшенный трафик
– Общий трафик



Зафиксированные атаки

– Текущие атаки
– Прошедшие атаки
– Фильтр по поиску аномалий
– Защищаемый IP-адрес
– Влияние атаки
– Время атаки
– Длительность атаки
– Сигнатуры атаки
– Задания по очистке

Принятые контрмеры

– Задания по очистке трафика
– Добавление заданий очистки
– Запуск заданий очистки
– Остановка заданий очистки
– Удаление заданий очистки
– Фильтрация заданий очистки

МегаФон