2023

Решения для комплексной защиты от киберугроз: возможности для партнеров CloudMTS

Центр мониторинга и реагирования (SOC) МТС RED

Типы продуктов

Услуги

Оценка практической ИБ
Red Team
& Purple Team

Экспертный аудит и консалтинг
Управление рисками и построение функций кибербезопасности

Расследование инцидентов
Digital Forensics

Анализ защищенности
Pentest

Сервисы и продукты

Шифрование каналов связи (ГОСТ)

Непрерывное тестирование на проникновение
Continuous PenTest

Безопасная разработка приложений
Встраивание контролей безопасности в процесс разработки

Защита веб-приложений
Web-Application Firewall

МТС SOC
Мониторинг безопасности инфраструктуры

Защита от DDoS
Противодействие атакам, направленным на отказ в обслуживании интернет-ресурсов

Security Awareness
Повышение киберграмотности сотрудников

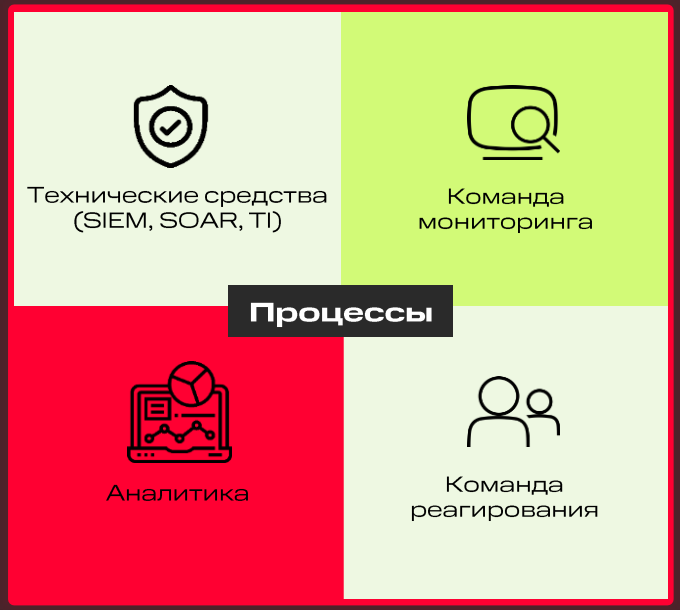
Обогащение и киберразведка
Поиск актуальных для компании угроз

M T C RED

Возможные атакующие	Средства защиты информации				
	АВПО и фаерволы	SOC	Pentest	Anti-DDoS	Кибер-грамотность
Автоматические системы сканирования и «школьники»	✓				
Вымогатели и мошенники	✓	✓			✓
Кибернаемники и кибервойска	✓	✓	✓	✓	✓

MTC RED

Из чего состоит SOC?



Личный кабинет

Удобный

Дружелюбный интерфейс
и разные срезы данных
для полной прозрачности

Информативный

Наглядные дашборды
и расширенная статистика
по всем событиям для принятия
эффективных решений

MDR != SOC

	MDR	SOC
Тип	Сервис	Сервис\Собственный
Краткое описание	Автоматическое детектирование инцидентов информационной безопасности и реагирование на конечных устройствах.	Сбор событий информационной безопасности с источников инфраструктуры
Основной инструмент оказания сервиса	EDR	SIEM
Источники событий для анализа	Фиксация и анализ событий агентом EDR установленного на Конечных устройств\Сервер Заказчика. События СЗИ вендора фиксирующих телеметрию с источника.	События сетевого оборудования (Маршрутизаторы, комутаторы) События журналов ОС (Журнал событий безопасности, Sysmon, Syslog и т.д) События СЗИ (IPS. DLP, NTA, IDM, EDR и тд) События журналов приложений (Бизнес системы, БД, Почта и тд) События оборудования АСУ ТП (ПЛК, SCADA)
Возможность корреляции событий из разных источников	Нет	Есть
Проверка инцидентов False positive	Проверка инцидентов FP на основе событий полученных с агентов EDR	Проверка инцидентов FP с учетом событий со всех источников подключенных к SIEM
Возможность взаимодействия с НКЦКИ	Нет	Есть
Предоставляемая структура в рамках сервиса	Фокус на автоматическое детектирование и реагирование на инциденты ИБ с минимальным привлечением специалистов ИБ.	Группа мониторинга и реагирования (1 и 2 линия мониторинга инцидентов) Группа предоставления сервиса (Закрепленные за заказчиком Сервис Менеджер и Аналитик) Группа развития сервиса
Совместимость с инфраструктурой	Наличие списка поддерживаемых типов и версионности источников	Возможность подключения любых источников не зависимо от версии и типа источника.
Использование TI в разработки контента	Есть	Есть
Возможность разработки контента по запросу Заказчика	Нет	Есть

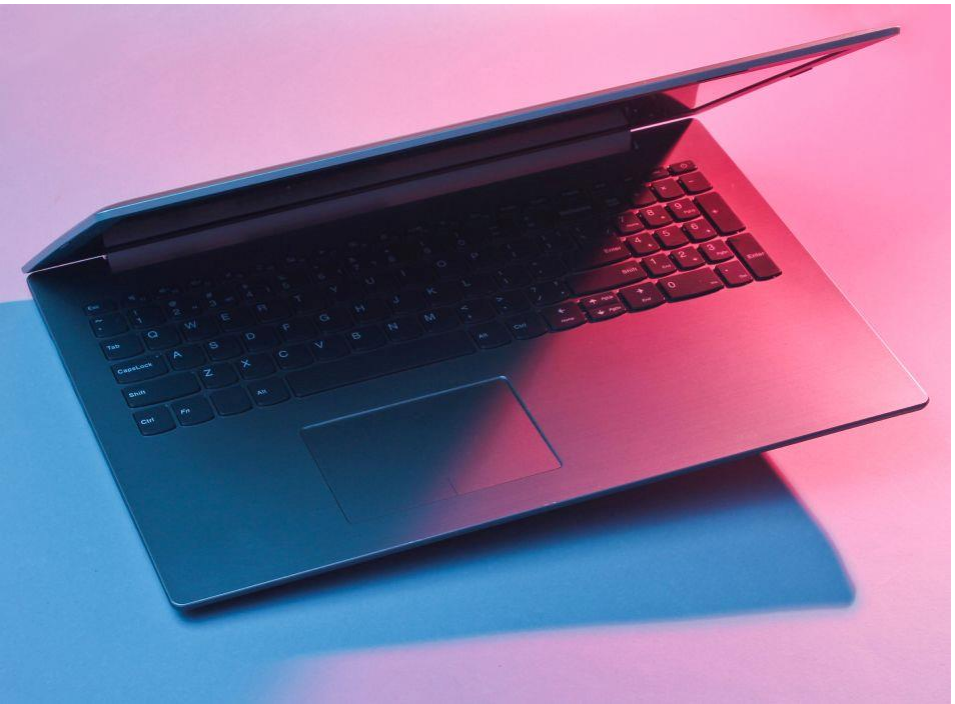
M T C RED

MTC RED
Ваши вопросы

Сервис защиты от DDoS-атак

Опасность DDoS-атак

Организованная DDoS-атака приводит к простою бизнеса, потере репутации и убыткам,
а для государственных информационных систем – к угрозе безопасности населения



В 9 РАЗ

выросло количество DDoS-атак в 2022 году

700 ₽

требуется, чтобы запустить DDoS-атаки

> 50 ДНЕЙ

продолжалась самая долгая DDoS-атака в 2022 году

Данные на основе открытых источников и внутренних исследований МТС RED

Защита от DDoS-атак

Блокирует DDoS-атаки на инфраструктуру и веб-ресурсы, чтобы обеспечить стабильный доступ к ним легитимных пользователей

1

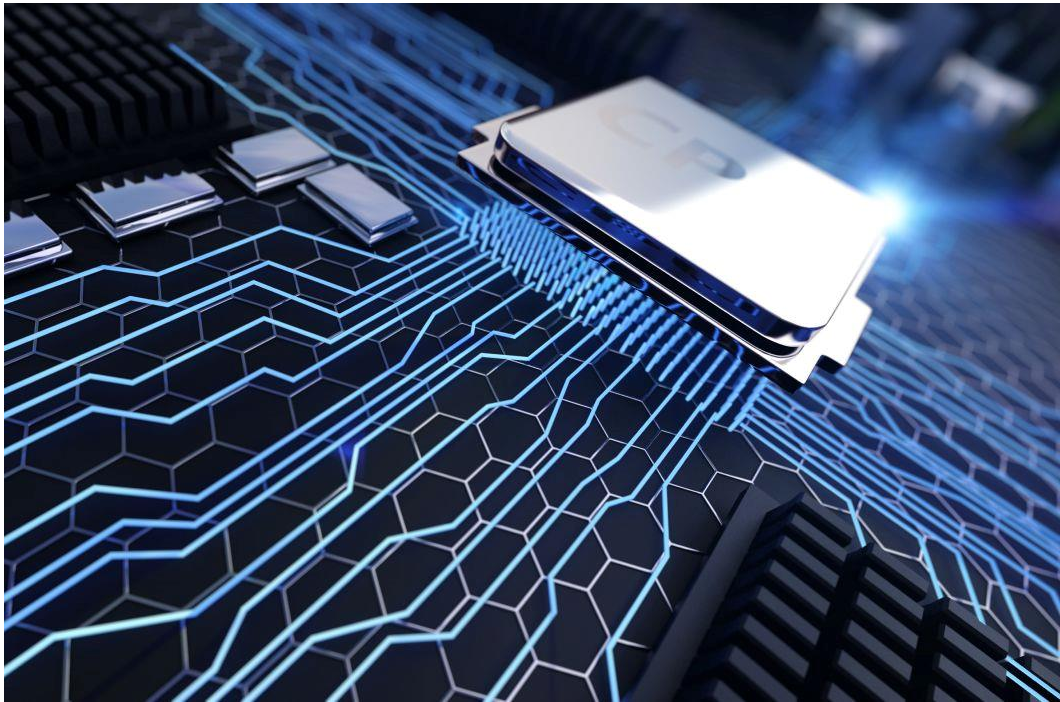
В случае DDoS-атаки трафик в автоматическом режиме или по согласованию с заказчиком переводится на очистку

2

Круглосуточный мониторинг и защита от атак на уровне каналов (L3-L4) и приложений (L7) без раскрытия ключей HTTPS-трафика

3

Экспертная поддержка и схема защиты под конкретные бизнес-требования



Непрерывный контроль работы веб-ресурсов

01

Настройка правил мониторинга и фильтрации трафика

02

Выделенная команда экспертов с практическим опытом защиты от кибератак

03

Гибкий функционал под задачи бизнеса и реакция на актуальные угрозы

04

Регулярные отчёты в Личном кабинете

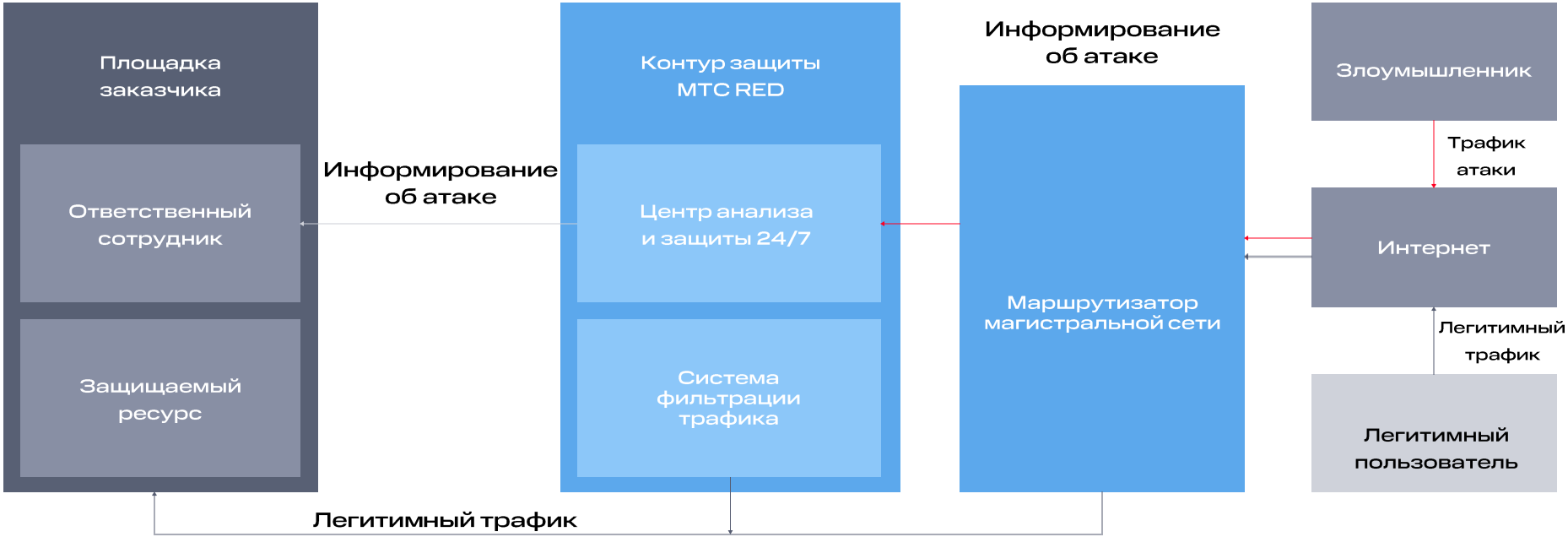
05

Обслуживание и техническая поддержка в круглосуточном режиме

06

Гарантированный уровень сервиса SLA – от 99% доступности

Схема работы сервиса



Выгодное решение под ключ для защиты инфраструктуры и веб-ресурсов

01 Быстрое подключение за 1 день после заполнения опросного листа

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

03 Облачная модель предоставления сервиса

04 Работы по подключению и обеспечению безопасности веб-ресурсов на стороне МТС

05 Сервис базируется на решении, входящем в Реестр российского ПО

Как узнать больше об Anti-DDoS?

На сайте облачного бизнеса МТС

Web application firewall (WAF)

Почему необходимо защищать веб-приложения?

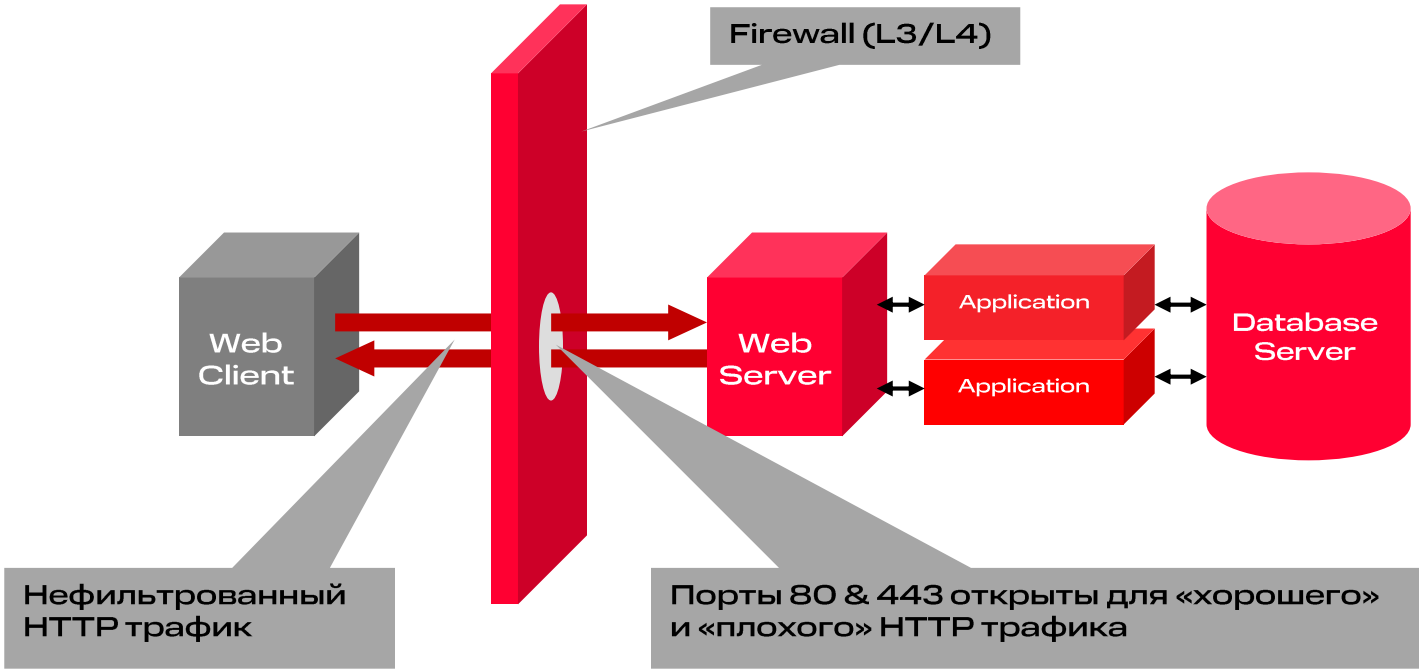
- Традиционные средства защиты (Firewall, IPS) не защищают веб-приложения и веб-сайт, при этом более 75% атак хакеров направлены на уязвимости веб-приложений/веб-сайтов, т.к. такие атаки не заметны для ИБ инфраструктуры и ИБ служб компании

- Уязвимости веб-приложений/сайтов несут в себе риски компрометации и фрода учетных записей и персональных данных пользователей, паролей, номеров кредитных карт и т.д.

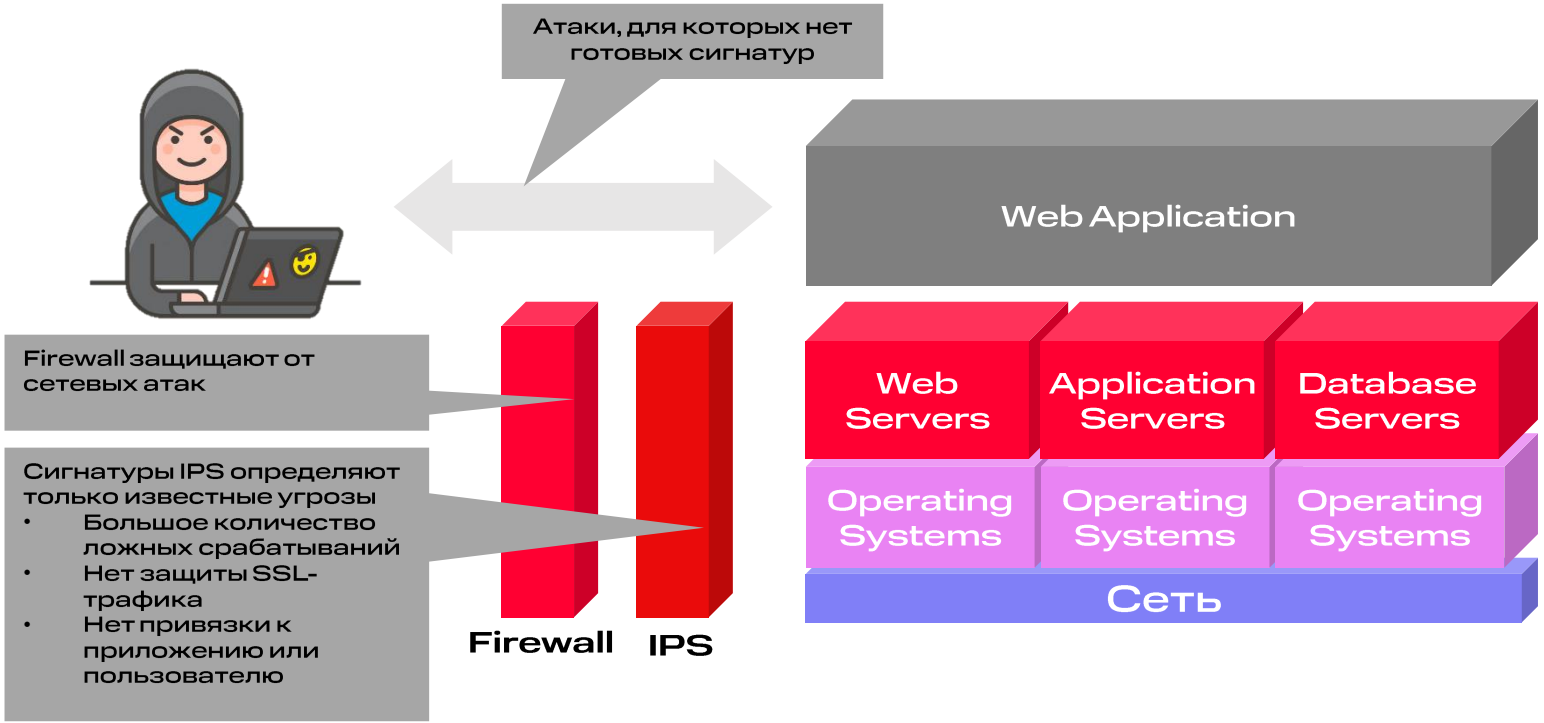
- Наглядное сравнение средств защиты веб-приложений приведено в таблице

Функция защиты веб-приложений	WAF	IPS	Firewall
Автоматическое обучение, поведенческий анализ	Да	Нет	Нет
Защита пользователей веб-приложений/веб-сайта	Да	Нет	Нет
Корреляция событий веб-приложений/пользователей	Да	Нет	Нет
Сканер уязвимостей веб-приложений	Да	Нет	Нет
Виртуальный патчинг (блокировка доступа пользователей до исправления уязвимости)	Да	Нет	Нет

Принцип работы традиционного Firewall



Фокус более 75% атак направлен на веб-приложения



Реальные угрозы для онлайн бизнеса и сайта

Применение Web Application Firewall позволяет исключить:

- **Кражу персональных данных** и другой конфиденциальной информации путём взлома ключевых веб-ресурсов
- **Атаки на пользователей сайта** путём заражения страниц сайта вирусами и размещения ссылок, содержащих инструменты взлома
- **Понижение позиций ресурса** в поисковых системах и нарушение рекламной политики путём манипуляций с кодом сайта
- **Нарушение работоспособности веб-приложений,** включая удаление или искажение файлов, баз данных и т.п.
- **Подмену содержания страниц:** размещение противозаконного или ложного контента, в том числе, поддельных новостей, неправильных цен на товары, ложной контактной информации, адресов электронной почты и т.д.

Кому нужна защита с помощью WAF

- Все вертикали бизнеса, использующие интернет в качестве среды взаимодействия с пользователями и заказчиками (сайт, веб-приложения, ERP, CRM, форумы, чаты и т.д.)
- Бизнес-процессы построены (оптимизированы) благодаря Интернет

Банки, страховые и финансовые организации

Госсектор, бюджетные организации (фед. и рег.)

ТЭК, предприятия

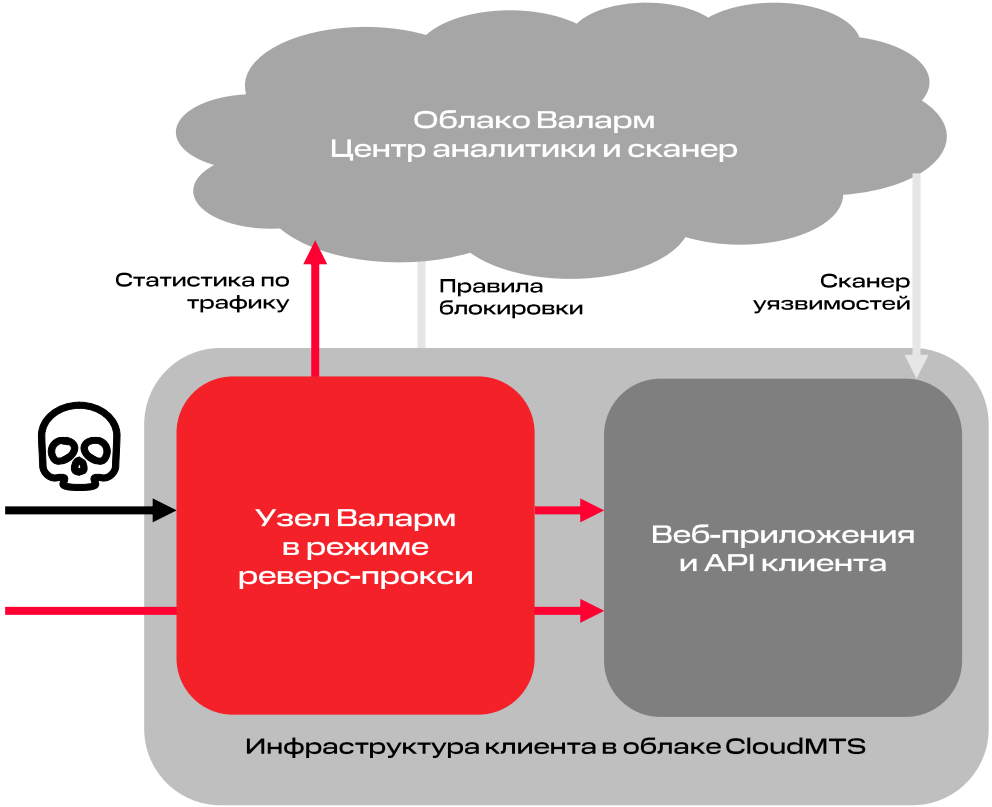
Транспорт

Все бизнесы интернет-индустрии, интернет магазины и различные сайты (игровые, развлекательные, новостные и т.д.)

Основные цели использования WAF

- защита от хакерских атак, направленных на веб-приложения, атак из перечня OWASP Top 10 и атак на бизнес-логику приложений и ботов
- автоматический поиск уязвимостей в веб-приложениях
- анализ всех входящих HTTP-запросов и мгновенная блокировка любого вредоносного запроса
- непрерывный сбор метрики со всего трафика и обработка собранной метрики в облаке, применяя машинное обучение
- формирование индивидуального профиля защищаемых ресурсов
- проверка сетевых ресурсов компании облачным сканером на наличие уязвимостей

Принцип работы



- Локально установленные узлы Валарм в инфраструктуре CloudMTS проксируют весь веб-трафик и блокируют атаки
- Поведенческий анализ логики приложения, содержимого запросов и пользовательской активности создает профили приложения, которые отправляются в облако Валарм
- Используя профиль приложения и собирая данные об атаках, облако Валарм создает адаптированные правила безопасности, сокращая ложные срабатывания
- Облако Валарм проверяет возможность реальной эксплуатации уязвимости, оценивает ее тяжесть, и группирует атаки в инциденты с одной и той же первопричиной

Преимущества WAF от CloudMTS и Валарм

- Непрерывное обучение при изменении веб-приложений
- Сканеры периметра и уязвимости
- Virtual Patching - ограничение доступа к уязвимым частям приложения до их устранения
- Работает без сигнатур и подтверждает угрозы в реальном времени
- Чувствительная для клиента информация не покидает периметр
- Инциденты регистрируются только для подтвержденных уязвимостей
- Искусственный интеллект для надежной защиты
    - Автоматическая настройка и самообучение системы на реальном трафике и атаках
    - Лучшее обнаружение атак Zero Day, поведенческих атак, OWASP Top 10, ботов и подбора паролей
    - Активный анализ угроз и перепроверка атак
- Современный стек
    - Поддержка API и протоколов HTTP
      HTTP/2.0,WEBSOCKETS, REST API, JSON, XML, SOAP
    - Независим от применяемых приложений
- Поддержка DevOps
    - Различные варианты развертывания
    - Поддержка и интеграции с различными внешними системами (RESTful API)

Преимущества WAF as a service перед установкой железа

- Перевод затрат в OPEX
- Доступность регулярных обновлений и защита от новых киберугроз
  - железо быстро устаревает и ломается, необходимы затраты на поддержку
  - у железа наступает период «End of support»
- Нет необходимости держать и обучать специалистов
- Гибкое управление затратами по мере роста бизнеса и объемов трафика

Как мы подключаем и поддерживаем

01

клиент заполняет опросный лист

02

установка WAF (на VM) в сегмент заказчика или технологический тенант

03

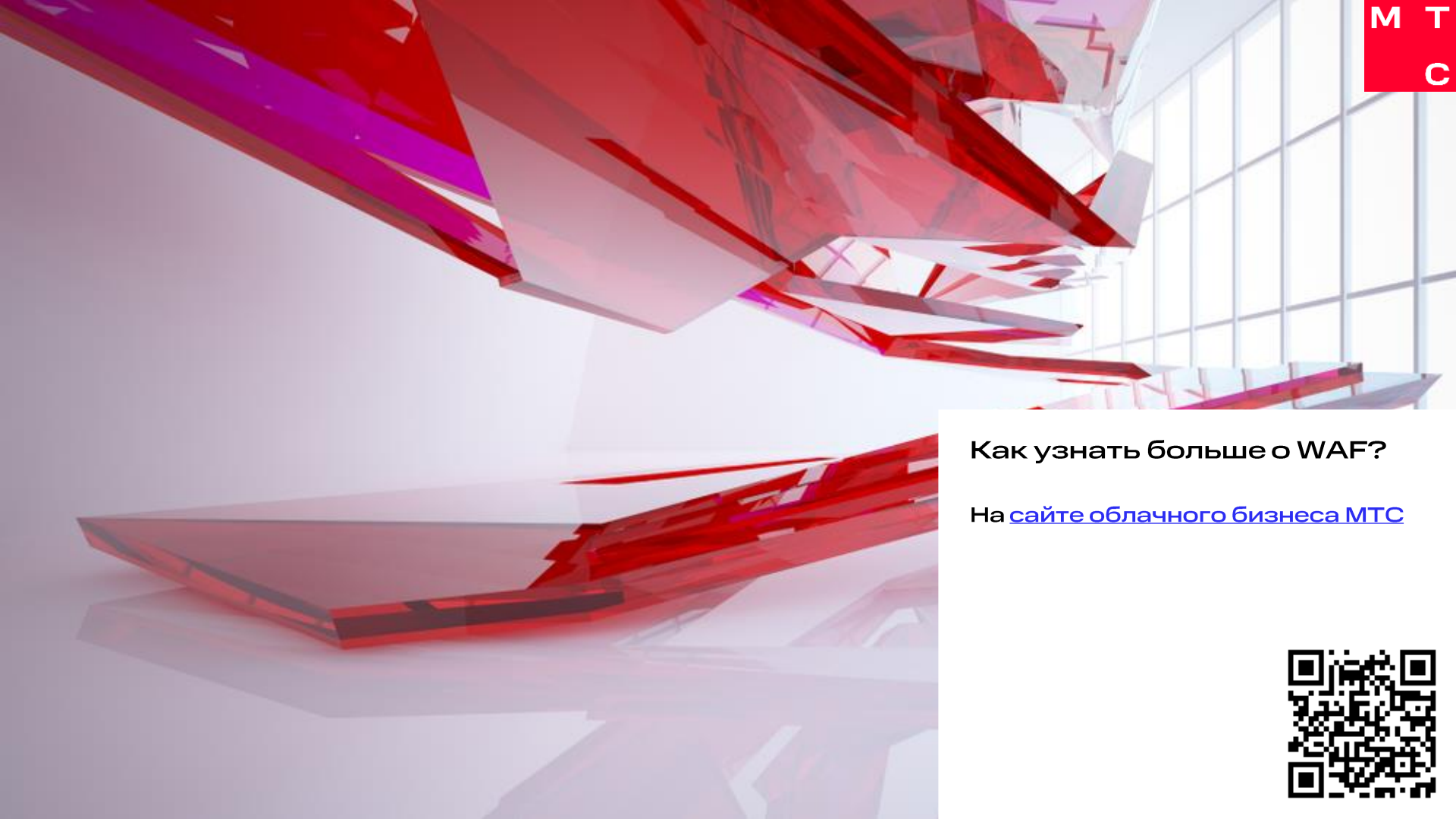
настройка и обучение WAF под систему заказчика

04

предоставление доступа к личному кабинету – waf.cloud.mts.ru

Возможен тестовый период до 1 мес

Техническую поддержку 1 и 2-го уровней обеспечивает CloudMTS



Как узнать больше о WAF?

На [сайте облачного бизнеса МТС]

Аттестованный сегмент ФЗ-152

Виртуальная инфраструктура. Аттестованный сегмент 152-ФЗ

Предоставление в пользование виртуальной ИТ-инфраструктуры, удовлетворяющей требованиям законодательства РФ по защите информации.

- решение подходит для ИСПДн любого типа и уровня защищенности;
- размещения ГИС в облачной инфраструктуре;
- значимая часть «головной боли» уходит при размещении ИС в виртуальной инфраструктуре, она аттестована по уровням УЗ-1 и К-1;
- возможность интеграции с другими сервисами информационной безопасности CloudMTS;
- при размещении инфраструктуры клиент получает выписку из модели угроз, разграничение зон ответственности, заключается договор и поручение на обработку ПДн согласно ФЗ-152

Общество с ограниченной ответственностью «Национальный аттестационный центр»
Лицензия ФСТЭК России
на деятельность по технической защите конфиденциальной информации от 23 января 2006 г. № 0437

УТВЕРЖДАЮ
Заместитель технического директора
ООО «НАЦ»
С.А. Сафонов
«30» ноября 2020 г.

АТТЕСТАТ СООТВЕТСТВИЯ
№ Н-44/20
Информационная система
«Защищенный сегмент облачной платформы #CloudMTC»
ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Выдан «30» ноября 2020 г.

уч. № 761

Сценарии использования и возможности. Аттестованный сегмент 152-ФЗ

Сценарии использования

Компании, бизнес-процессы которых подразумевают сбор паспортных и иных персональных данных

Интернет-магазины, которые собирают, хранят банковские реквизиты, запрашивают другие сведения о клиентах или имеют программу лояльности

Коммерческие организации, которым необходимо подключаться к государственным информационным системам (ГИС)

Компании, которые работают с системами управления услугами, биллинга или маркетинговых коммуникаций и другие организации, обрабатывающие персональные данные

Возможности сервиса

Обеспечиваем уровень защищенности персональных данных УЗ-1 в соответствии с требованиями законодательства

Предлагаем отказоустойчивую виртуальную инфраструктуру с уровнем доступности 99,95% для размещения ИСПДн и ГИС

Используем решения защиты информации, сертифицированные ФСТЭК и ФСБ

Заключение официального договора и поручения на обработку ПДн в соответствии с 152-ФЗ

Защищенный аттестованный сегмент облака для размещения мощностей заказчика и обработки ПДн и ГИС

Облачная инфраструктура полностью соответствует требованиям приказов **ФСТЭК № 17 и 21**

За счет наличия аттестованной виртуальной инфраструктуры **УЗ-1/К1** упрощается процедура аттестации ИС клиента

Преимущества реализации ИСПДн в облаке ФЗ-152

Реализация на собственной инфраструктуре

Высокие единовременные затраты и стоимость владения

Уникальность каждой системы защиты ПДн

Долгий срок реализации (проект, поставка, внедрение)

Необходимость мониторинга и изучения законодательства

Необходимость разработки документации на ИСПДн

Необходимость иметь в штате высококвалифицированных специалистов

Реализация на облачной инфраструктуре

Низкие единовременные затраты и стоимость владения

Отработанное типовое решение в облачной инфраструктуре

Оперативное развертывание (от 1 дня)

Мониторинг и обеспечение соответствия законодательству — зона ответственности исполнителя

Все необходимые шаблоны документов предоставляет исполнитель

Сертифицированные специалисты исполнителя

Наличие сертификата PCI DSS, оценки соответствия ГОСТ 57580

Контакты

Как узнать больше
об аттестованном сегменте
152-ФЗ?

На сайте облачного бизнеса МТС

Партнерская программа CloudMTS

Что дает партнерство с CloudMTS

CloudMTS предоставляет гибкие условия сотрудничества для роста вашего бизнеса. Мы разработали партнерскую программу, чтобы обеспечить легкость, эффективность и прибыльность

Индивидуальный подход

- Мы находимся в диалоге с партнерами, адаптируем партнерские программы и ищем пути достижения совместного успеха

Доступность и простота

- Четкий путь для достижения рентабельности
- Простая и быстрая интеграция с текущими бизнес-процессами
- Отсутствие расходов на внедрение и полная техническая поддержка

Технологичность и инновации

- Предоставляем в одном окне весь инфраструктурный стэк (Colo, Cloud, каналы)
- Расширяем портфель услуг, ориентируясь на запросы рынка, при этом сохраняем технологическую стабильность
- Геораспределенная инфраструктура, разветвленная филиальная сеть в регионах

Кто может стать партнером CloudMTS

Юридическое лицо или ИП – системные интеграторы и ИТ-компании, оказывающие услуги консалтинга и аутсорсинга

Агент

Рекомендует клиентам облачные сервисы МТС

от 10%*

вознаграждение

от ежемесячных платежей
ваших клиентов

*Доступные сервисы и размер базового вознаграждения определяются условиями договора

Как работает агентская схема

#1
Партнер заключает агентский договор с CloudMTS

#2
С согласия клиента агент передает CloudMTS ИНН, контакты и ТЗ

#3
Менеджер CloudMTS прорабатывает ТЗ, заключает договор с клиентом

#4
С первого дня тарификации клиента агент получает ежемесячное вознаграждение

#5
Размер вознаграждения агента зависит от подключенных сервисов и объема потребления

Пример расчета кейса для агента

Сервис	Стоимость, ₽ в мес	НДС, ₽ в мес	Стоимость с НДС, ₽ в мес
WAF	100 000	20 000	120 000
Виртуальная инфраструктура. Аттестованный сегмент 152-ФЗ	150 000	30 000	180 000
SOC	200 000	40 000	240 000
Общая стоимость:	**450 000**	**90 000**	**540 000**

Вознаграждение партнера:
45 000 ₽ ежемесячно = 540 000 ₽ за первый год

Не является публичной офертой, стоимость приведена в демонстрационных целях

Как агенту заработать больше?

Привлекать новых клиентов

При привлечении

2 и более

клиентов период ежемесячных выплат продлевается

Стать реселлером CloudMTS

Расширить свой портфель облачными сервисами и зарабатывать чистую маржу без капитальных затрат

Реселлер

Использует облачные сервисы МТС в своих решениях

30%*

скидка
на облачные сервисы

*Средний размер скидки. Доступные сервисы и коммерческие условия определяются индивидуально

Как работает реселлерская схема

#1

Партнер заключает реселлерский договор с CloudMTS

#2

Реселлер заключает договор с клиентом на потребление облачных сервисов

#3

Реселлер отвечает за первую линию техподдержки, 2-3 линия на стороне CloudMTS

#4

CloudMTS предоставляет реселлеру необходимые инструменты для старта продаж

#5

Реселлер увеличивает выручку с каждого клиентского кейса, используя прогрессивную шкалу скидок

Приглашаем на мероприятия CloudMTS

23 ноября, 11:00 (мск)

Вебинар «Больше, чем просто офис: возможности бизнес-приложений для партнеров CloudMTS»

30 ноября, 11:00 (мск)

Вебинар «Облачная инфраструктура: возможности для партнеров CloudMTS»

Как узнать больше
о партнерской программе?

Свяжитесь с менеджером

Игорь Кочелков
Менеджер по работе с партнерами CloudMTS