SkyDNS

Угрозы в слепой зоне

почему DNS защита
нужна даже при наличии NGFW

SkyDNS — это

Большой опыт на рынке

Мы уже 14 лет
на российском рынке
информационной
безопасности

Подтвержденная надежность

Наш сервис входит в мировой ТОП-3 по устойчивости DNS-резолверов — нам доверяют миллионы пользователей

Скорость ракеты

Мы самый быстрый публичный DNS-резолвер в России

Передовые технологии

Под капотом
собственные
технологии фильтрации
контента и ML-модели

Высокая производительность

Ежедневно обрабатываем миллиарды DNS-запросов — 15 млн пользователей под защитой

Отечественная разработка

Весь наш софт
зарегистрирован
в реестре российского
ПО

SkyDNS

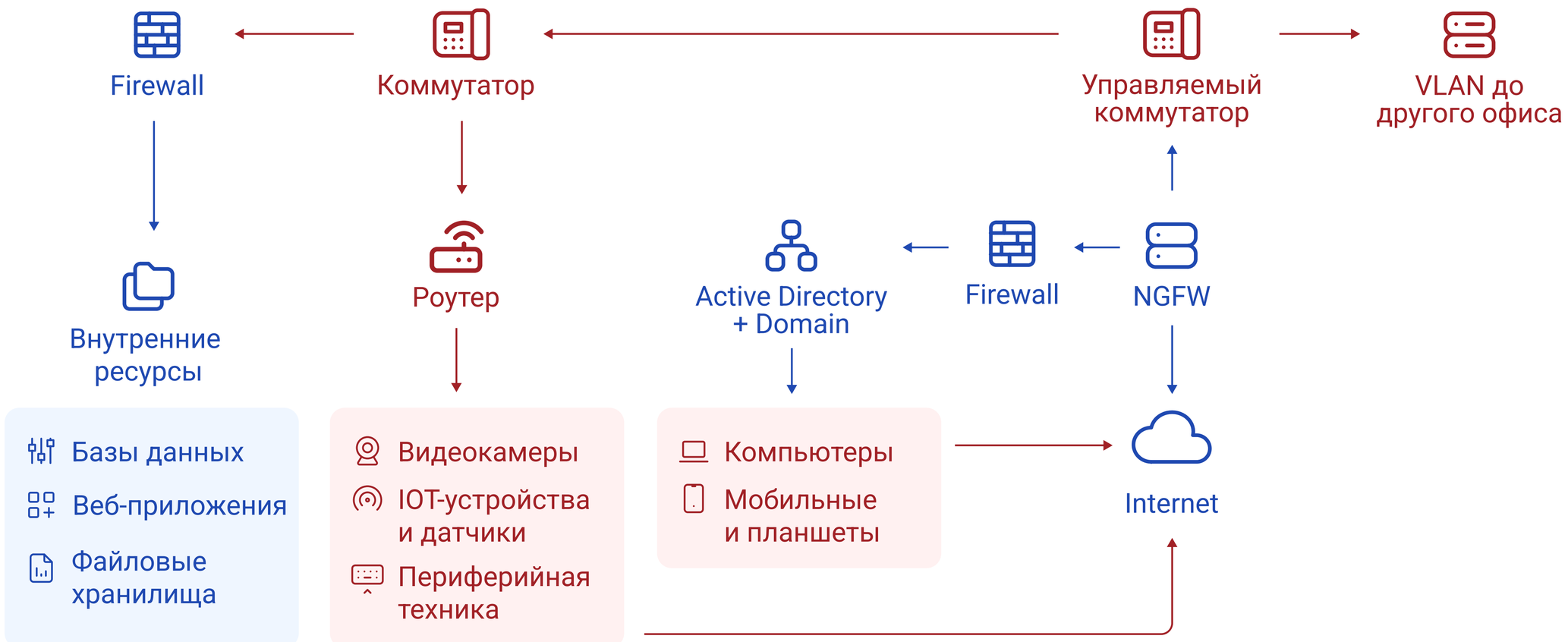
- 20 лет в IT, 3 года — в ИБ
- 500+ крупных клиентов из промышленности, финансов и ритейла доверили мне защиту от сложных кибератак
- люблю новые кейсы и новые вызовы

Павел Евтихов

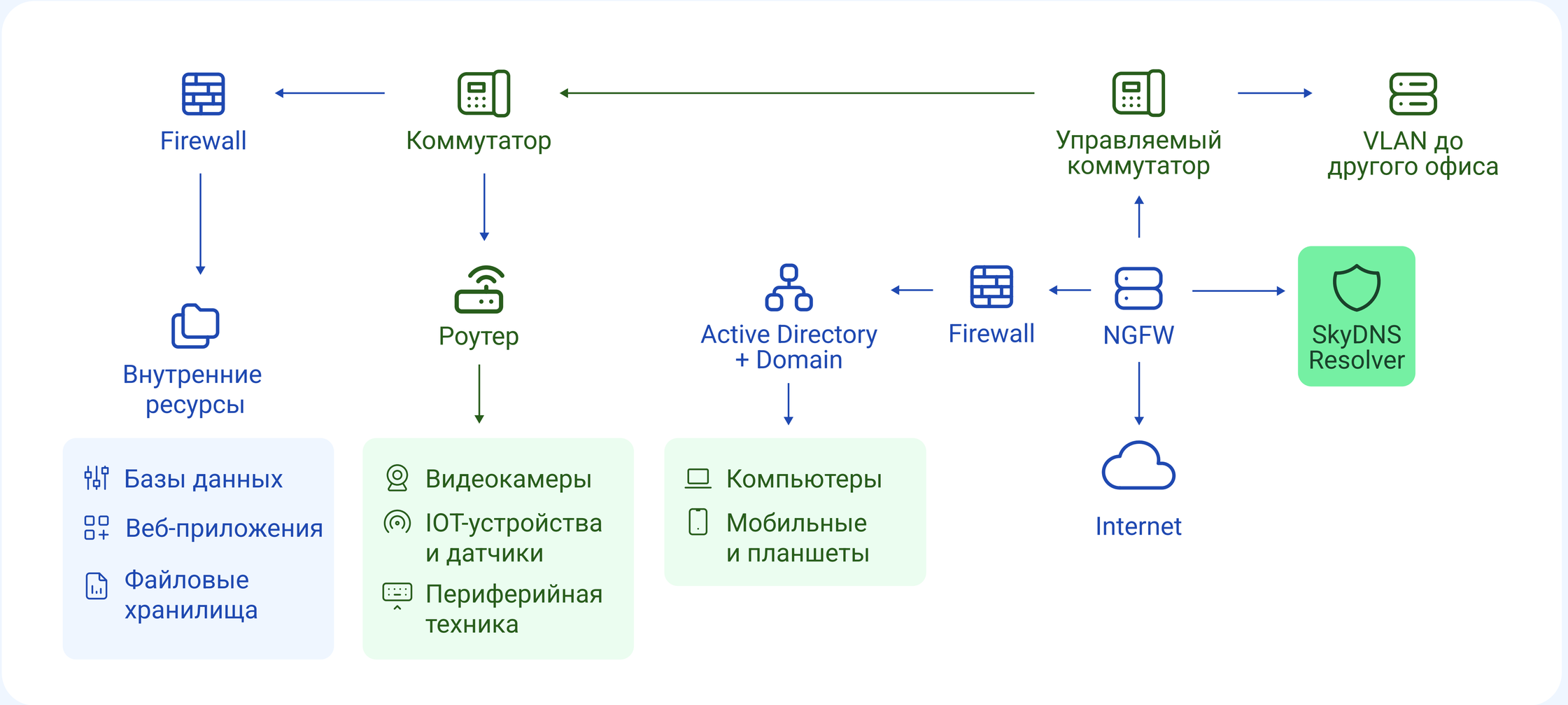
руководитель отдела внедрения

Как обычно выглядит периметр компании

Серые зоны периметра



Идеальный периметр с резолвером SkyDNS



Предотвратите утечку данных

Угроза эксфильтрации

DNS-туннели и C&C-коммуникации используются для скрытой передачи данных за пределы организации.
Такие каналы часто остаются незамеченными в течение длительного времени из-за отсутствия в инфраструктуре механизмов обнаружения в реальном времени.

EDR, DC, AV

Зависят от агента на хосте — выявляют слишком поздно, есть риск не установить
или не обновить клиента

NGFW

Фиксирует только аномалии в объеме трафика, не различает DGA-паттерны, а C&C-запросы выглядят легитимно

SkyDNS

- Глубокий анализ DNS-паттернов и индикаторов компрометации
- Блокировка на этапе резолвинга — еще до входа в периметр
- Нулевой шанс на скрытую эксфильтрацию данных

Обеспечьте полную видимость всех DNS-клиентов без агентов

Слепые зоны

Неавторизованные DNS-запросы от виртуальных машин, гипервизоров, IoT-оборудования и периферийных устройств (принтеры, камеры, терминалы и т.п.) часто остаются вне зоны действия стандартных средств защиты. Это формирует слепые зоны, создавая риски скрытых подключений, утечек и несанкционированного доступа к внутренним ресурсам.

EDR, DC, AV

Работают только на устройствах с установленными агентами; виртуальные среды и IoT-сегменты вне зоны видимости, инциденты не фиксируются

NGFW

Анализирует HTTP(S)-трафик, но не учитывает DNS-запросы от сетевых и периферийных устройств. Такая активность проходит мимо системы, исключая ее из зоны контроля и реагирования

SkyDNS

- Обнаружение всех DNS-активных устройств без установки агентов
- Автоматическое создание реестра клиентов и контроль активности в реальном времени
- Выявление «теневых» сегментов и обеспечение видимости на уровне сетевого взаимодействия

Выявляйте скрытые конфигурации и уязвимости сети

Угроза несанкционированного доступа

Сетевые устройства с предустановленным административным доступом и поддержкой удаленного выполнения команд представляют высокую степень риска. Уязвимости в операционных системах оборудования (Cisco, Juniper, MikroTik, Avaya и др.) могут быть использованы для получения полного контроля без обнаружения базовой защитой.

EDR, DC, AV

Не отслеживают выполнение скриптов и автоматических конфигураций на сетевых устройствах. Поэтому, не обеспечивают защиту в сегментах, где невозможно развертывание агентов.

NGFW

Не распознает вредоносные сценарии, выполняемые внутри сетевого оборудования, так как они маскируются под корректный DNS-трафик.

SkyDNS

- Обнаружение аномалий в DNS-конфигурациях
- Идентификация индикаторов компрометации (IOC)
- Мгновенное уведомление о попытке изменения конфигурации оборудования

Выявляйте атаки на раннем этапе

Угроза на ранних этапах вторжения

Типичный сценарий начинается с Zero-day phishing или открытия вредоносной ссылки. После первичного проникновения злоумышленник осуществляет сканирование внутренней инфраструктуры и подбор учетных данных (брутфорс), готовя почву для дальнейшего развития атаки.

Этап 1

Проникновение в периметр

Попадание в периметр через Zero-day phishing и открытие вредоносных ссылок.

Этап 2

Разведка и сканирование

Сканирование и брутфорс внутренних зон периметра.

Выявляйте атаки на раннем этапе

Угроза на ранних этапах вторжения

Типичный сценарий начинается с Zero-day phishing или открытия вредоносной ссылки. После первичного проникновения злоумышленник осуществляет сканирование внутренней инфраструктуры и подбор учетных данных (брутфорс), готовя почву для дальнейшего развития атаки.

EDR, DC, AV

Регистрируют активность только на скомпрометированных хостах — уже после начала выполнения вредоносного кода. Вмешательство происходит слишком поздно.

NGFW

Обнаруживает аномалии лишь при массовых атаках на уровне прикладного трафика (Layer 7) или при резком росте объема передачи данных.

SkyDNS

- Обнаружение признаков сканирования и брутфорса на этапе разведки
- Превентивное оповещение до проникновения в систему
- Снижение риска ущерба за счет раннего реагирования

Кейс 2

Усилили защиту торговой сети «Монетка»

Проблемы

Компания использовала отечественнын-е NGFW и антивирус, но в периметре оставались «слепые зоны». Данные об угрозах были разрознены между решениями, не было единого обзора безопасности по всей инфраструктуре, а устройства без агентов антивируса оставались незащищёнными.

Результаты

Заблокировали большое количество нецелевого трафика:

Торренты, майнинг криптовалют, нелегальный и “взрослый” контент

Значительно укрепили общую защиту сетевого контура:

Защитили от фишинга в реальном времени, уменьшили шанс утечки данных за счет распознавания скрытых каналов передачи данных,усложнили возможность связи с C&C-центрами злоумышленников

Защитили устройства, на которые невозможно установить антивирус:

Роутеры, маршрутизаторы, СКУД, IoT-устройства, камеры видеонаблюдения

Улучшили видимость сети за счет глубокого анализа трафика:

Определение объема и характера заблокированных угроз по 8 категориям ИБ. Почасовой и поминутный анализ активности всех устройств. Анализ трафика по доменам, устройствам и категориям контента

Кейс 2

Обеспечили нулевую турбулентность в периметре

Проблемы

Компания использовала отечественные NGFW и антивирус, но в периметре оставались зоны без контроля. Данные об угрозах хранились в разных системах, из-за чего не было целостной картины безопасности, а устройства без антивирусных агентов оставались уязвимыми.

Клиент

Российская авиакомпания, выполняющая 57 тыс. полетов в год по России и за рубежом

Результаты

Заблокировали большое количество вредоносного трафика:

Обращения к C2-центрам и ботнетам, подозрительные DGA-домены, скрытые майнеры

Значительно укрепили общую защиту сетевого контура:

Защитили от фишинга в реальном времени, уменьшили шанс утечки данных за счет распознавания скрытых каналов передачи данных,усложнили возможность связи с C&C-центрами злоумышленников

Защитили устройства, на которые невозможно установить антивирус:

Роутеры, маршрутизаторы, СКУД, IoT-устройства, камеры видеонаблюдения

Улучшили видимость сети за счет глубокого анализа трафика:

Определение объема и характера заблокированных угроз по 8 категориям ИБ. Почасовой и поминутный анализ активности всех устройств. Анализ трафика по доменам, устройствам и категориям контента

Кейс 3

Предотвратили атаки в контуре банка, которые пропустил межсетевой экран

Клиент

Региональный банк с парком из 600–700 компьютеров

Проблема

Клиент пользовался межсетевым экраном от Cisco и бесплатным публичным DNS-резолвером. Осознав, что нуждается **в дополнительном уровне защиты на уровне DNS,** начал искать подходящее решение.

Решение

Клиент искал сервис с простой и быстрой установкой, без необходимости изменения инфраструктуры. В итоге обратился к нам и с помощью нашей команды настроил облачный сервис за 15 минут.

Результат

Всего **за две недели тестового периода** среди 18 млн DNS-запросов наша система фильтрации **заблокировала 89 тыс. запросов** неприемлемого контента по выбранным банком категориям, а также **предотвратила 39 тыс. атак**, таких как вредоносное ПО, DGA и запаркованные домены. Самое интересное, что **данные запросы никак не блокировались уже имеющимися сервисами по ИБ**.

Статистика блокировок

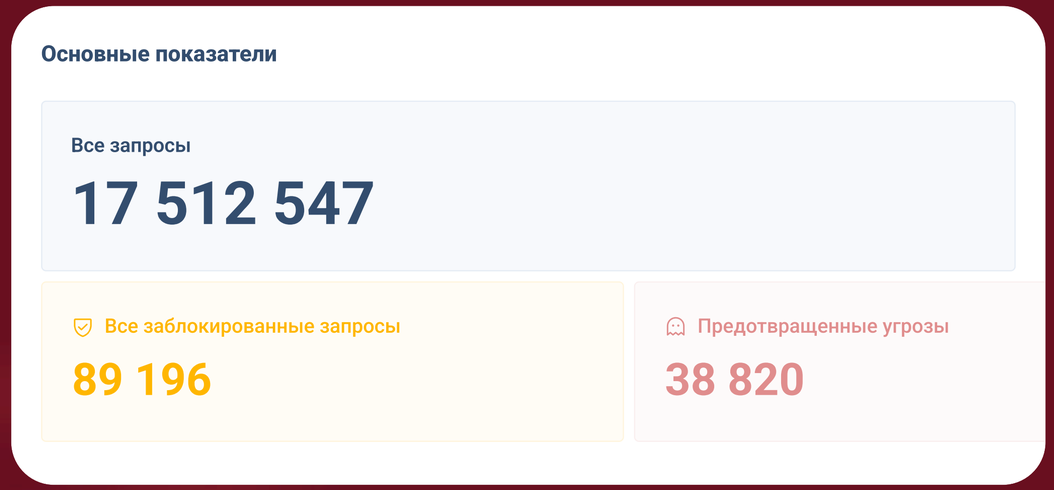


Фото 1: Статистика заблокированных DNS-запросов и атак за 2 недели демо

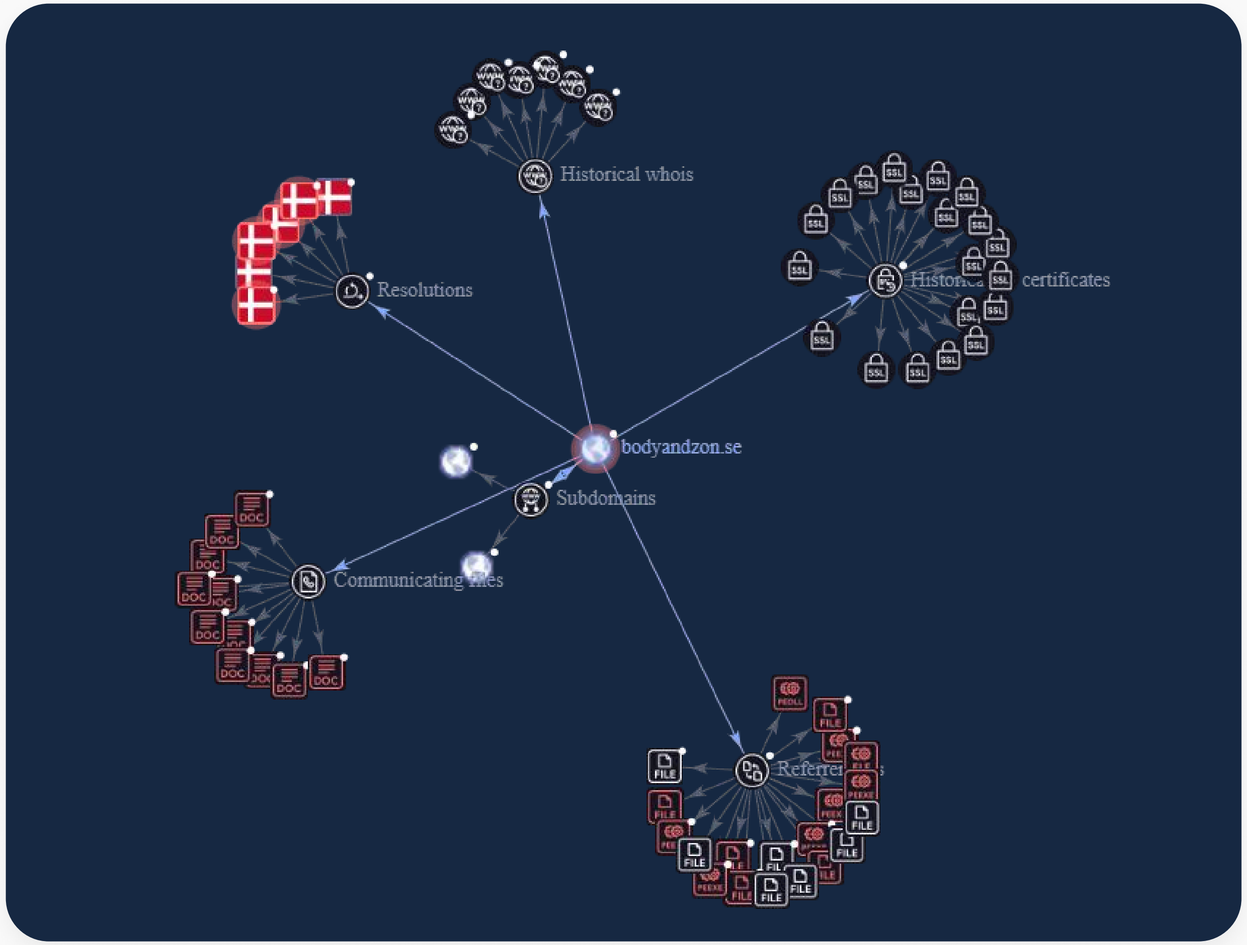
Категория	Количество блокировок
Вредоносное ПО	6759
DGA	6755
Запаркованные домены	23433
Реестр запрещенных сайтов	69485
Порнография и секс	4510
Казино, лотереи, тотализаторы	4184
Компьютеры и Интернет	2088
Бизнес, экономика, маркетинг	2071
Досуг и развлечения	1962
ИТОГО	**201633**

Таблица: Кол-во заблокированных DNS-запросов по категориям за 2 недели демо

Примеры угроз

bodyandzon.se

Bodyandzon.se связан с распространением вирусов, программ-вымогателей и троянов. Несмотря на то, что этот домен уже не существует, компьютеры клиента продолжают отправлять к нему запросы.

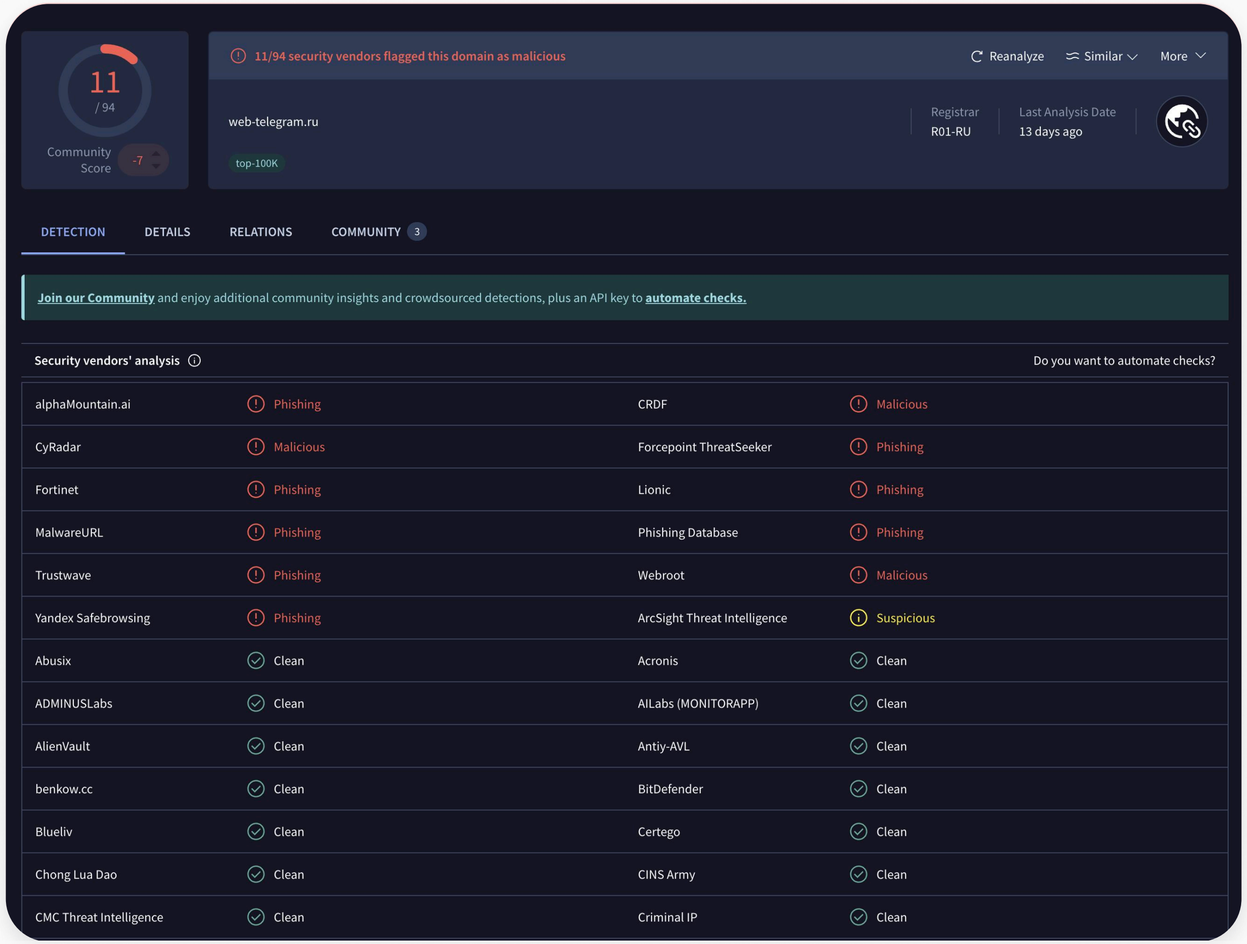


граф связанности домена bodyandzon.se с virustotal

Примеры угроз

web-telegram.ru

Неофициальный веб-клиент Telegram, который выглядит точь-в-точь, как официальный мессенджер. Сотрудники банка активно пользовались им в рабочих целях, не подозревая, что данный сайт может представлять угрозу.



Анализ домена web-telegram.ru на VirusTotal. 11 других вендоров тоже блокируют этот домен.

Подключение

Легко проверить в действии

Поддержка presale отдела на каждом этапе

Шаг 1

Подключение

Интеграция на сети занимает не более 15 минут

Шаг 2

Тестирование

Инфраструктура не меняется, появляется инструмент для мониторинга

Шаг 3

Выводы

Статистика по блокировкам и анализ данных

Специальный промокод

softlineweb2025

на расширенный тестовый период (14 дней)
регистрация по ссылке