BYDNS

Обзор возможностей сервиса byDNS



Подключение в один клик

Не требуется покупка нового оборудования



Не требуется установка нового ПО



BYDNS

Возможности сервиса

Централизованная блокировка приложений: программы удаленного доступа, VPN, мессенджеры, магазины игр – админ может запретить в один клик использование конкретных приложений на конкретных устройствах

Защита от специфических DNS-угроз, таких как спуфинг, DGA и DNS-туннелирование, которые не блокирует ни один NGFW

Защита от неприемлемого контента: блокировка 60 категорий тематических ресурсов

Защита сети от вредоносного трафика (фишинг, вирусы-шифровальщики)

Мощная аналитика на основе подробной статистики поможет заглянуть вглубь трафика вашей компании и понять, что происходит на уровне сети Интернет

Применение профилей фильтрации на всю сеть, на группы пользователей или индивидуальные устройства – отлично подходит для многофилиальных организаций

BYDNS

Специфические DNS-угрозы

Спуфинг

Подмена информации в DNS-ответе с целью отправить пользователя на ресурсы злоумышленников вместо оригинальных ресурсов

DNS-туннелирование

Передача любой информации (команды, файлы) внутри DNS-протокола в обход всех правил фильтрации firewall

DGA

Использование алгоритмически создаваемых доменов с коротким времени жизни, хранение которых в специализированных базах лишено смысла, т.к. они "одноразовые" и постоянно создаются новые

BYDNS

Что дает вам наша статистика?

Анализ трафика по доменам, устройствам и категориям

Вы можете отслеживать, какие сайты посещают сотрудники в рабочее время и какие категории контента блокируются. Это помогает лучше понять рабочую активность и повысить эффективность работы.

Выявление аномалий в трафике

Статистика позволяет оперативно находить отклонения в сетевом трафике, которые могут сигнализировать о заражении устройств или других уязвимостях сети.

Почасовой анализ активности

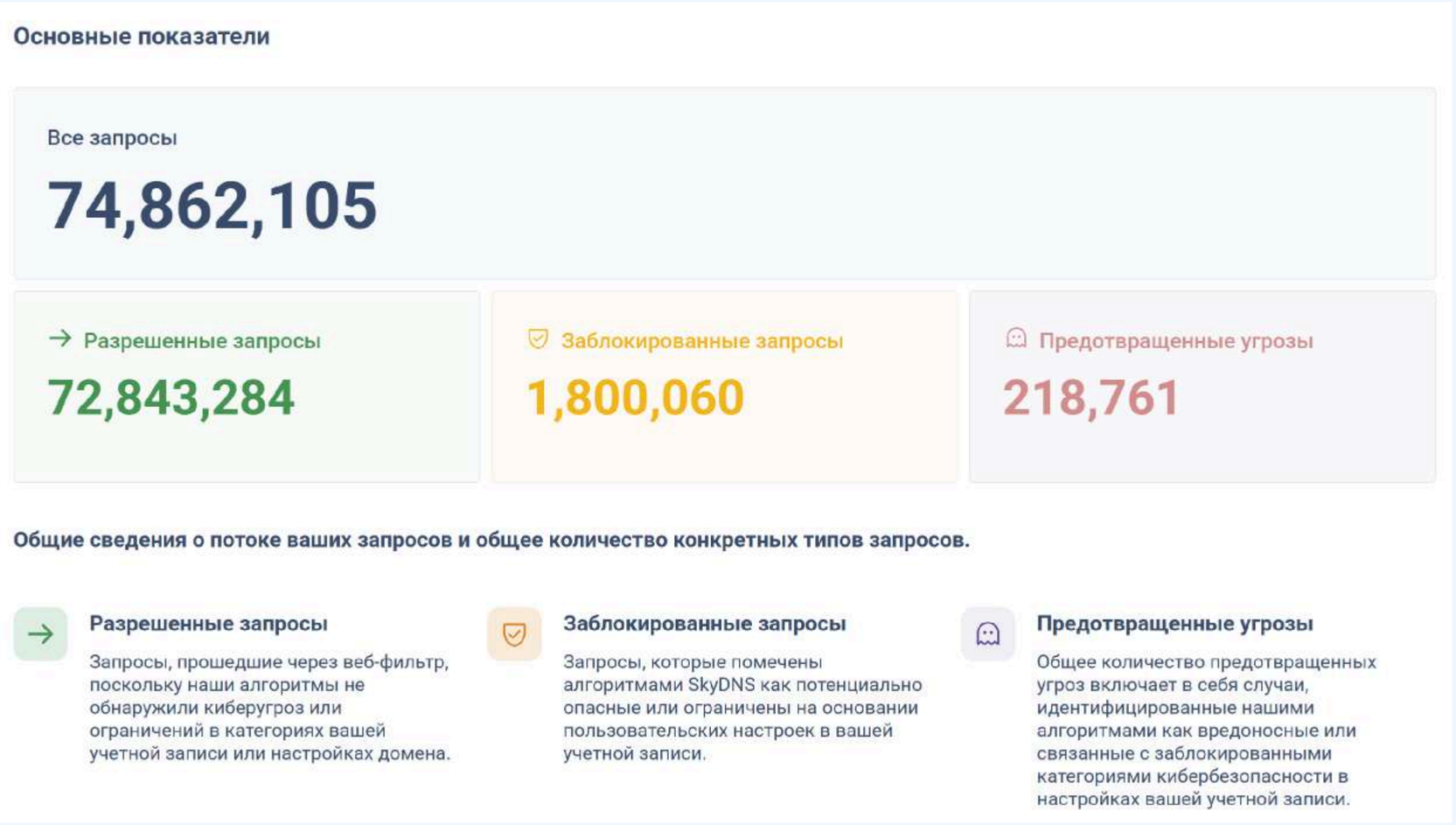
Наблюдайте за активностью устройств в режиме реального времени. Это помогает выявить возможные проблемы с сетью, признаки DNS-угроз или работу сотрудников вне рабочего времени.

Объем и характер заблокированных угроз

Посмотрите, с какими типами угроз сталкивается ваша сеть и как они эффективно блокируются. byDNS классифицирует угрозы по 7 ключевым категориям: Ботнеты & C2C, Phishing & Typosquatting, Cryprojacking, DGA, Ransomware, Malware, Запаркованные домены.

BYDNS

Общая статистика

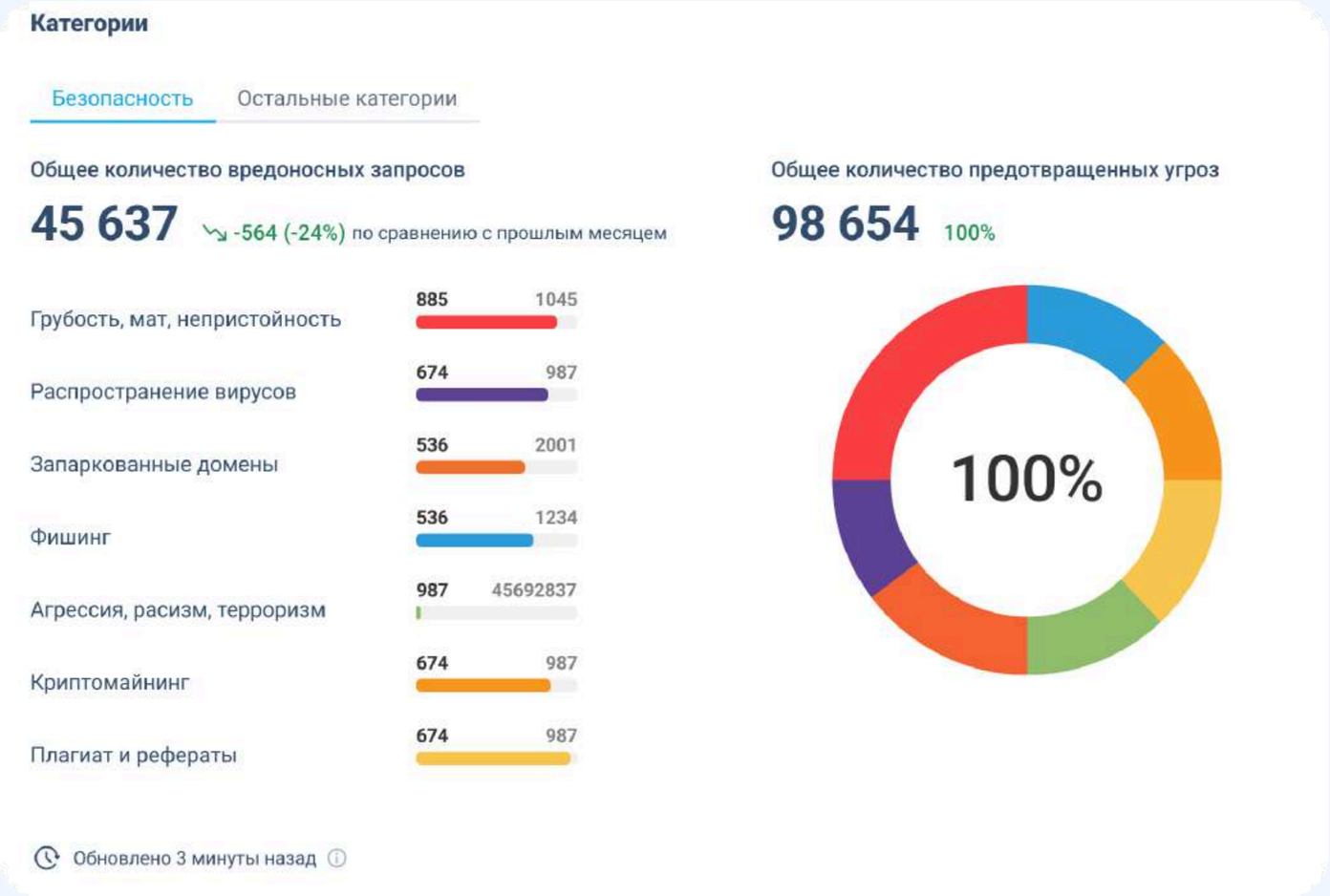


Наглядность и простота восприятия

Сразу отображается общая картина,
с возможностью перейти в конкретный раздел
и изучить нужный запрос детально

BYDNS

Общая статистика



Аналитика угроз и эффективности блокировки

Можно увидеть все категории вредоносных запросов и моментально проверить, сколько угроз было заблокировано

BYDNS

Почасовая статистика

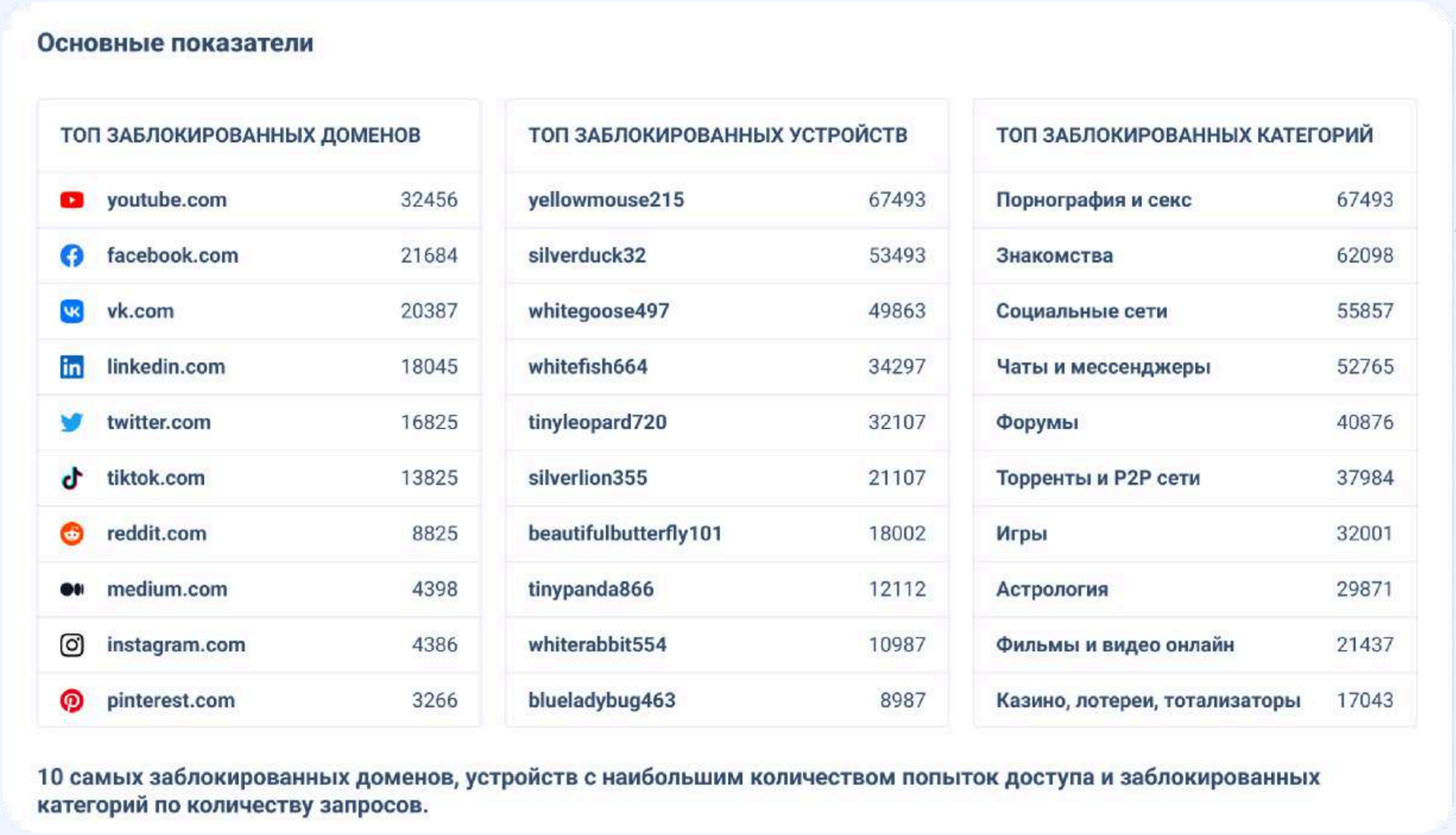


Видимость всплесков аномальной активности

График позволяет быстро заметить нежелательную активность без необходимости изучать отчёты. Активность можно отследить в любое время, даже ночью

BYDNS

Блокировка приложений



Основные показатели

ТОП ЗАБЛОКИРОВАННЫХ ДОМЕНОВ		ТОП ЗАБЛОКИРОВАННЫХ УСТРОЙСТВ		ТОП ЗАБЛОКИРОВАННЫХ КАТЕГОРИЙ	
youtube.com	32456	yellowmouse215	67493	Порнография и секс	67493
facebook.com	21684	silverduck32	53493	Знакомства	62098
vk.com	20387	whitegoose497	49863	Социальные сети	55857
linkedin.com	18045	whitefish664	34297	Чаты и мессенджеры	52765
twitter.com	16825	tinyleopard720	32107	Форумы	40876
tiktok.com	13825	silverlion355	21107	Торренты и P2P сети	37984
reddit.com	8825	beautifulbutterfly101	18002	Игры	32001
medium.com	4398	tinypanda866	12112	Астрология	29871
instagram.com	4386	whiterabbit554	10987	Фильмы и видео онлайн	21437
pinterest.com	3266	blueladybug463	8987	Казино, лотереи, тотализаторы	17043

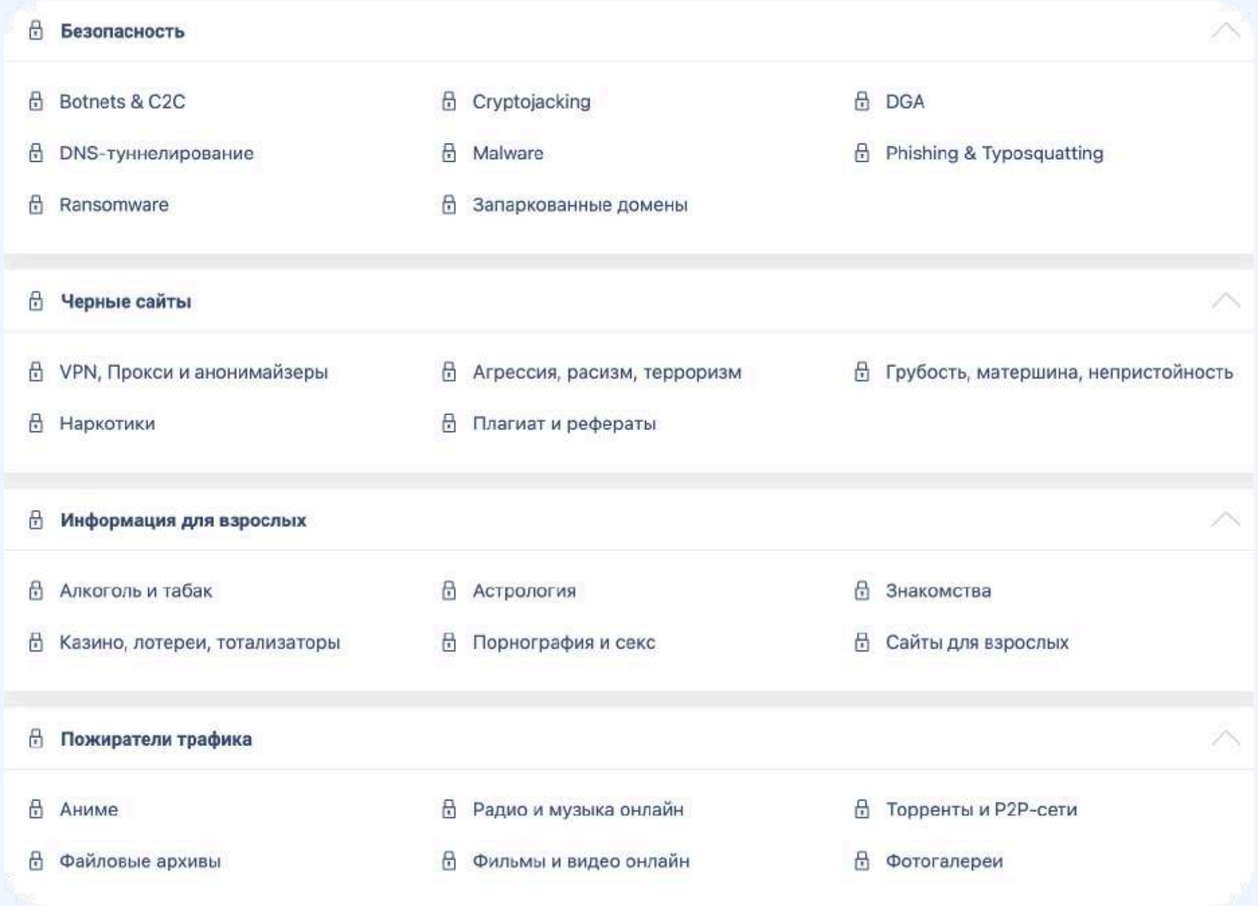
10 самых заблокированных доменов, устройств с наибольшим количеством попыток доступа и заблокированных категорий по количеству запросов.

Контроль использования приложений

В один клик можно заблокировать любое приложение на конкретном устройстве. Система отслеживает соблюдение корпоративных регламентов и сразу выявляет попытки обхода правил. Механизм одинаково эффективно работает как локально, так и с облачными экосистемами.

BYDNS

Категории фильтрации

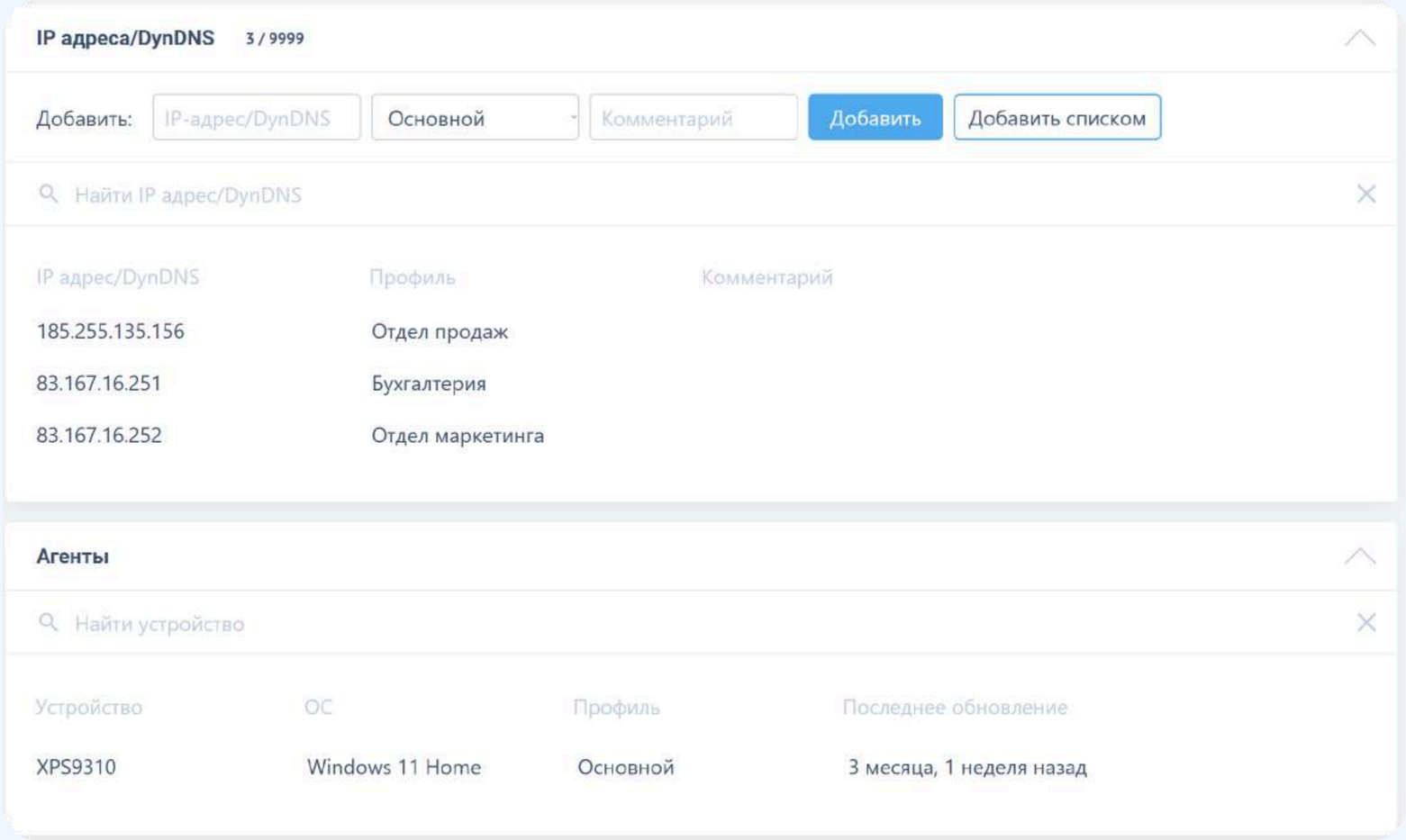


Защита распространяется даже на самые изощрённые угрозы на DNS-уровне

Широкий охват в 60 категорий тематических ресурсов позволяет с лёгкостью настроить фильтрацию трафика под ваши нужды и соблюдать все установленные правила — от внутренних корпоративных до регуляторных требований надзорных органов

BYDNS

Профили фильтрации



Универсальная интеграция

Гибкость внедрения на любом уровне — от сетевой инфраструктуры до конкретных устройств, отделов, пользователей.
Доступны различные сценарии подключения, как локально, так и облачно.

BYDNS

Статистика блокировок

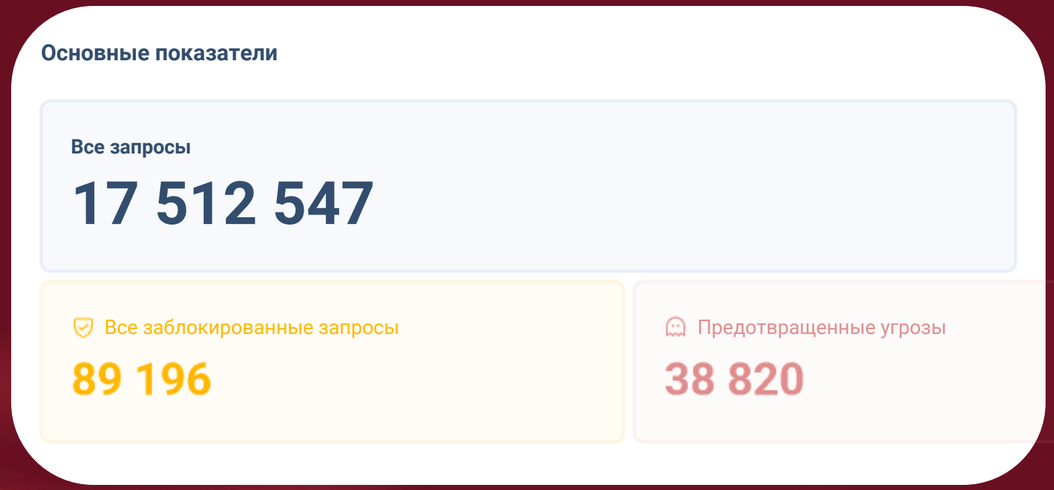


Фото 1: Статистика заблокированных DNS-запросов и атак за 2 недели демо

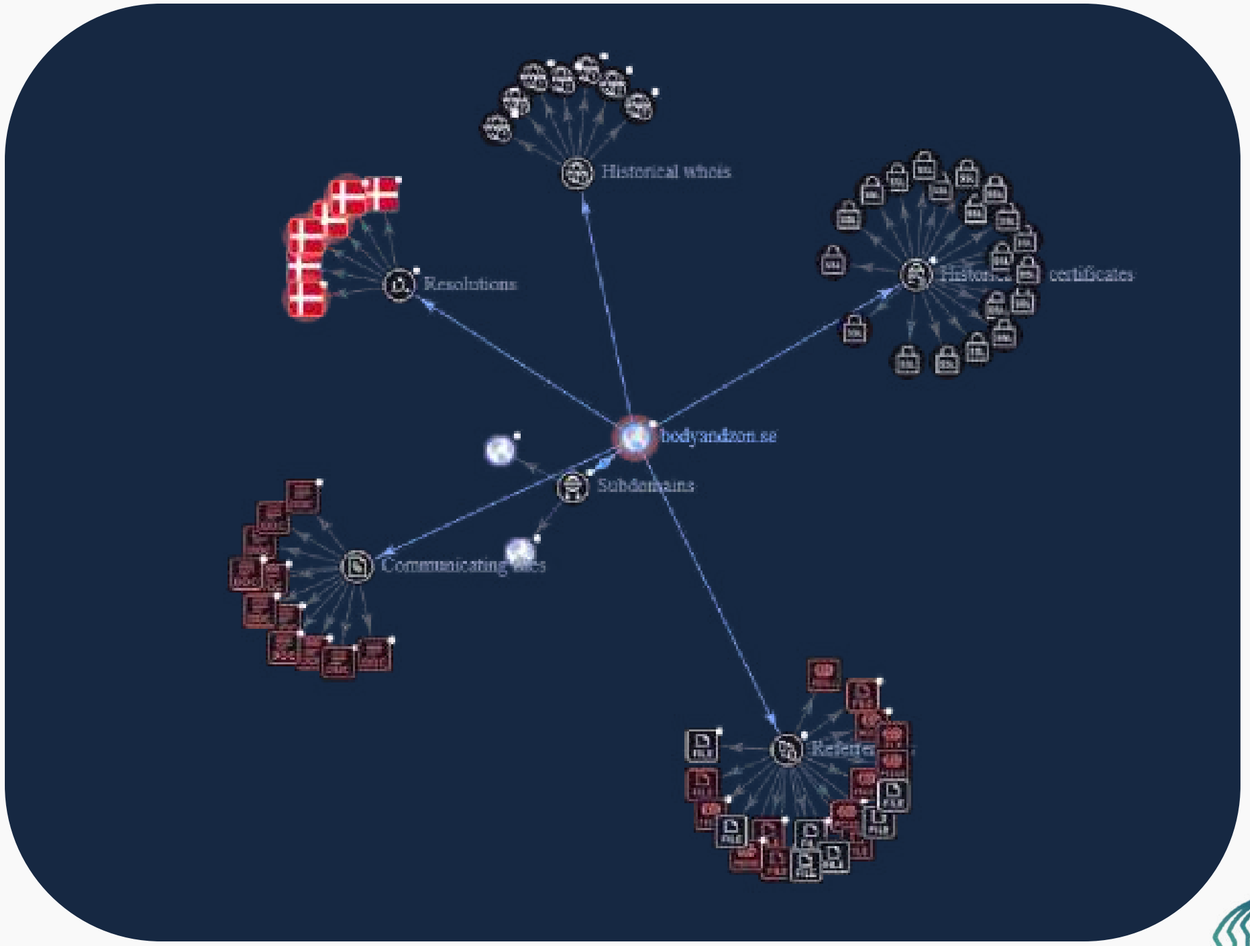
Категория	Количество блокировок
Вредоносное ПО	6759
DGA	6755
Запаркованные домены	23433
Реестр запрещенных сайтов	69485
Порнография и секс	4510
Казино, лотереи, тотализаторы	4184
Компьютеры и Интернет	2088
Бизнес, экономика, маркетинг	2071
Досуг и развлечения	1962
ИТОГО	**201633**

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

Примеры угроз

bodyandzon.se

Одним из самых часто посещаемых и заблокированных ресурсов оказался домен bodyandzon.se, связанный с распространением вирусов, программ-вымогателей и троянов. Несмотря на то, что этот домен уже не существует (он числится незарегистрированным и снова доступен к регистрации), компьютеры клиента продолжают отправлять к нему запросы. Возможно, такие действия могут быть связаны с одной из группировок, которые активно используют DNS для командования, контроля или для скрытия своих действий. Это может быть как работа с ботнетом, так и попытка скрыть свою активность через DNS запросы, что характерно для таких группировок, как Lazarus Group или REvil, которые использовали DNS в своих атаках.



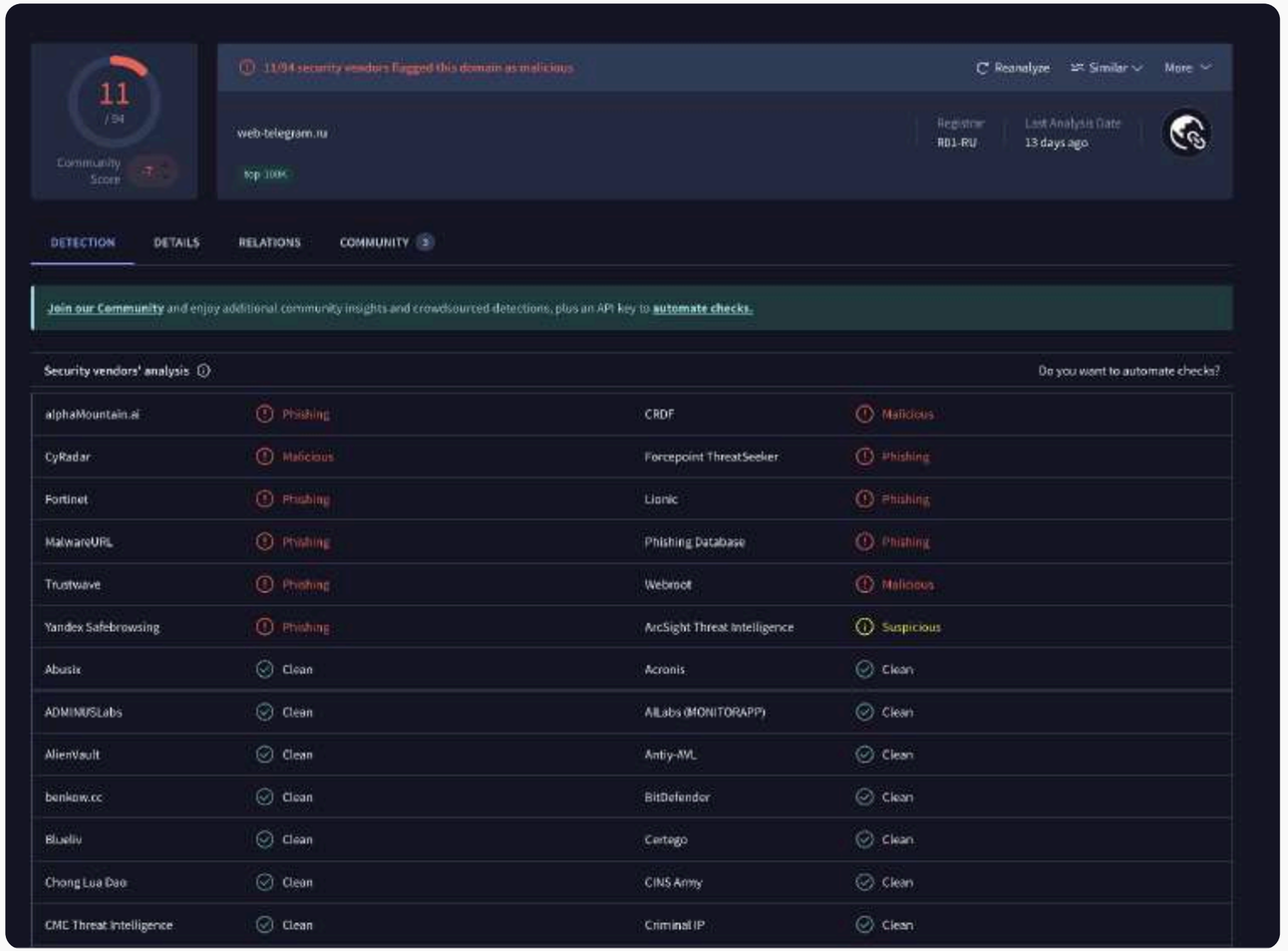
граф связанности домена bodyandzon.se с virustotal

BYDNS

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.

BYDNS

Итог

Представители ИБ отдела банка были настолько впечатлены масштабом заблокированных угроз, что сразу же после теста приобрели годовую лицензию.

«Мы даже не представляли, насколько может быть уязвима наша корпоративная сеть без надежной DNS-фильтрации. Советую увеличивать слои безопасности и отдавать предпочтение надежным DNS-резолверам. Как говорится, на NGWF надейся, а сам не плошай»

комментирует директор ИБ отдела банка

BYDNS

Как byDNS усилит вашу защиту

Если у вас нет межсетевого экрана

- byDNS берет на себя значительную часть функций защиты сетевого периметра.
- Защищает от фишинга, вирусов, шифровальщиков и других угроз, которые обычно блокируются межсетевыми экранами.
- Дополняет безопасность, снижая риски заражения и потери данных.

	Нет средств защиты
Блокировка по своим спискам	
Блокировка по подключаемым спискам	
Фильтрация тематического трафика	
Блокировка опасных доменов	
Защита от спуфинга	
Защита от DNS-туннелей	
Защита от угроз, связанных с DGA	
Защита от атак нулевого дня	

новый уровень защиты

ничего не добавит

дополнительный уровень защиты

BYDNS

Как byDNS усилит вашу защиту

Если у вас уже есть межсетевой экран

- Усиливает существующую защиту за счет актуальной базы вредоносных доменов.
- Охватывает 1618 TLD зон (70% всех зон).
- Дополнительный уровень фильтрации снижает вероятность пропуска угроз.

	Нет средств защиты	Есть NGFW или UTM
Блокировка по своим спискам	✓	✗
Блокировка по подключаемым спискам	✓	✗
Фильтрация тематического трафика	✓	✗
Блокировка опасных доменов	✓	+
Защита от спуфинга	✓	✓
Защита от DNS-туннелей	✓	✓
Защита от угроз, связанных с DGA	✓	✓
Защита от атак нулевого дня	✓	✓

✓ новый уровень защиты

✗ ничего не добавит

\+ дополнительный уровень защиты

BYDNS

Как byDNS усилит вашу защиту

Защита от специфических DNS-угроз

- Защищает от атак, с которыми не справляются NGFW, UTM и Proxy — спуфинг, DGA и DNS-туннелирование.
- Обеспечивает многоуровневую защиту.

	Нет средств защиты	Есть NGFW или UTM	Есть Proxy
Блокировка по своим спискам	✓	✗	✗
Блокировка по подключаемым спискам	✓	✗	✗
Фильтрация тематического трафика	✓	✗	✓
Блокировка опасных доменов	✓	+	+
Защита от спуфинга	✓	✓	✓
Защита от DNS-туннелей	✓	✓	✓
Защита от угроз, связанных с DGA	✓	✓	✓
Защита от атак нулевого дня	✓	✓	✓

✓ новый уровень защиты + дополнительный уровень защиты ✗ ничего не добавит

BYDNS

Подключение

Легко проверить в действии

Поддержка presale отдела на каждом этапе

Подключение

Интеграция на сети занимает не более 15 минут

Тестирование

Инфраструктура не меняется, появляется инструмент для мониторинга

Выводы

Статистика по блокировкам и анализ данных

BYDNS

BYDNS



byDNS.kz

+7 708 988 98 98

01@abi.kz