SkyDNS

DNS как инструмент раннего выявления киберугроз в корпоративной инфраструктуре

SkyDNS

Павел Блинов

руководитель отдела приоритетных проектов

SkyDNS — сервис для комплексной защиты корпоративной сети на уровне DNS

Развиваем превентивные технологии и превращаем DNS в надёжный инструмент раннего обнаружения угроз, создавая новые стандарты сетевой безопасности.

ТОП-3

в мире по устойчивости DNS-резолверов — нам доверяют миллионы юзеров

1500+

компаний из промышленности, финансов, транспорта и ритейла уже под нашей защитой

15 лет

совершенствуем собственный центр аналитики угроз на базе AI и ML

3 млрд

DNS-запросов обрабатываем ежедневно

- Член ассоциации разработчиков ПО РУССОФТ
- Обладатель сертификата лаборатории AM Test Lab
- Включены в Единый реестр российского ПО

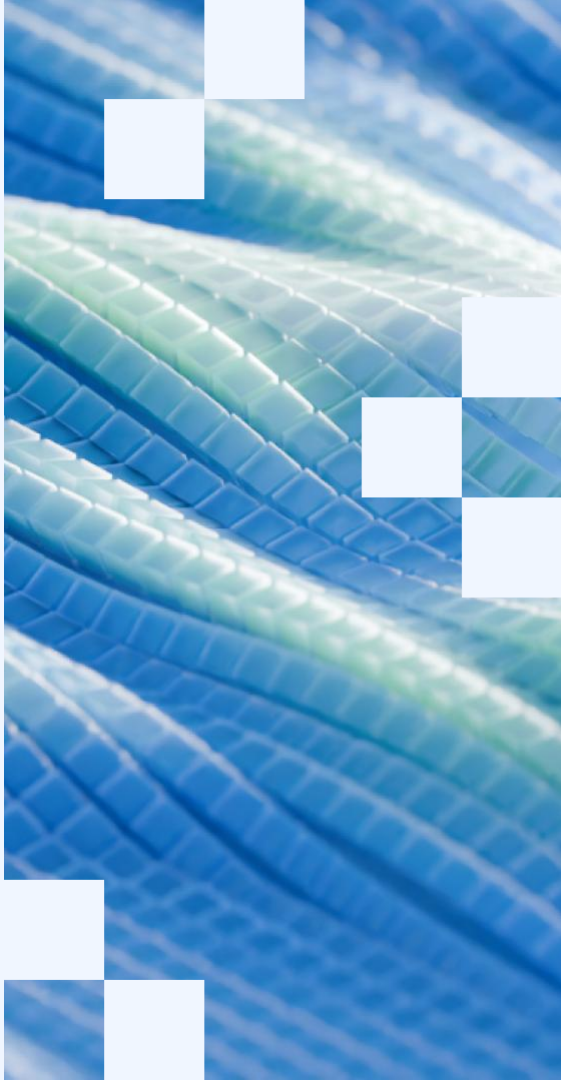
Современные вызовы требуют эшелонированной защиты

EDR & 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 могут выглядеть легитимно



DNS – стратегическая точка атак

90%

вредоносного ПО используют протокол DNS для атак и утечки (Techradar, 2024)

88%

компаний не мониторят DNS протокол и не анализируют (Efficientip, 2022)

34%

угроз можно предиктивно заблокировать на уровне DNS

Злоумышленники могут оставаться незамеченными годами

51 мин

Средняя продолжительность кибератаки на российские компании в 2024 году
«Информзащита», 2024

249 дней

В среднем злоумышленники находятся в инфраструктуре компании-жертвы до их обнаружения

IBM Data Breach Report, 2025

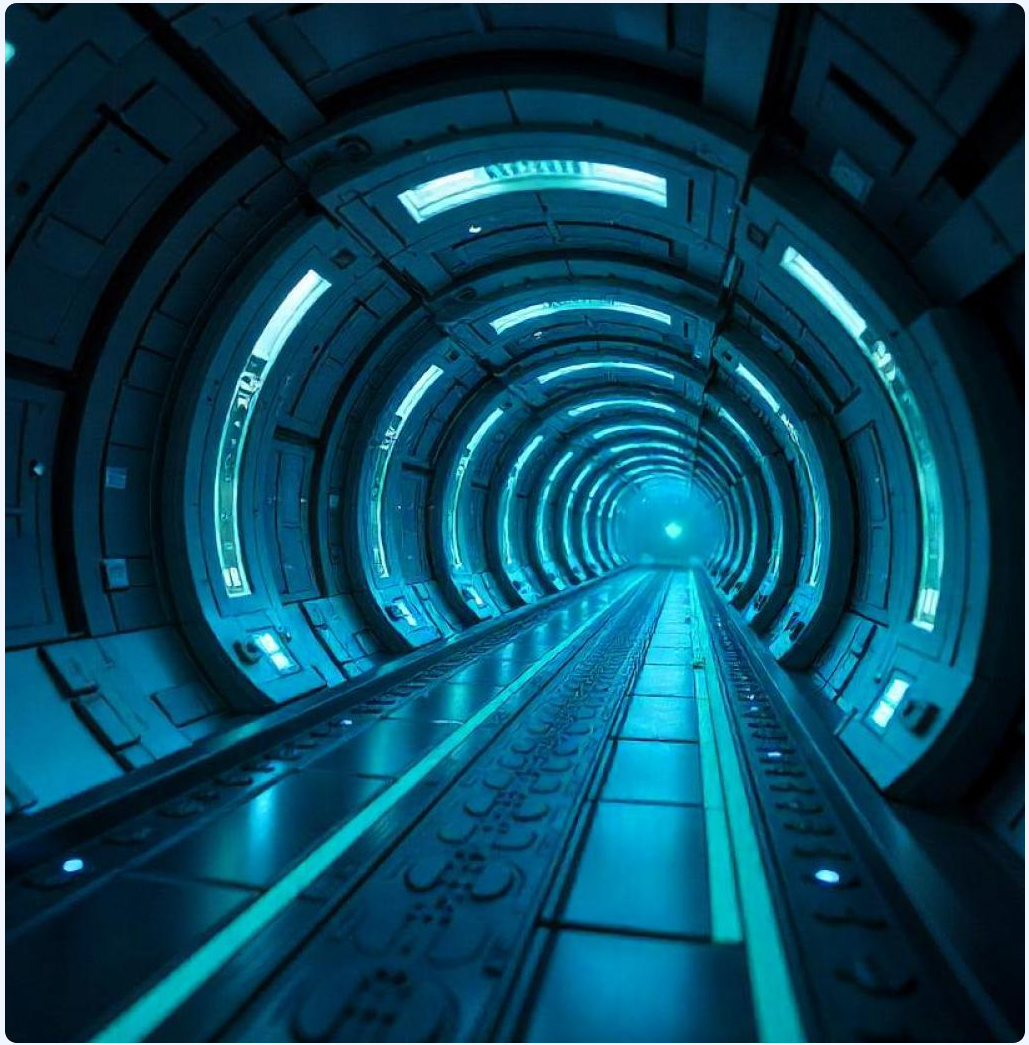
3 года

Длилось самое долгое пребывание злоумышленников в инфраструктуре

Отчет Positive Technologies, 2023

DNS-туннель

Метод передачи данных между двумя точками, например, между компьютером и сервером, через протокол DNS



Для чего используется DNS-туннель?

Для передачи управляющих команд

Для передачи файлов

Схема DNS-трафика

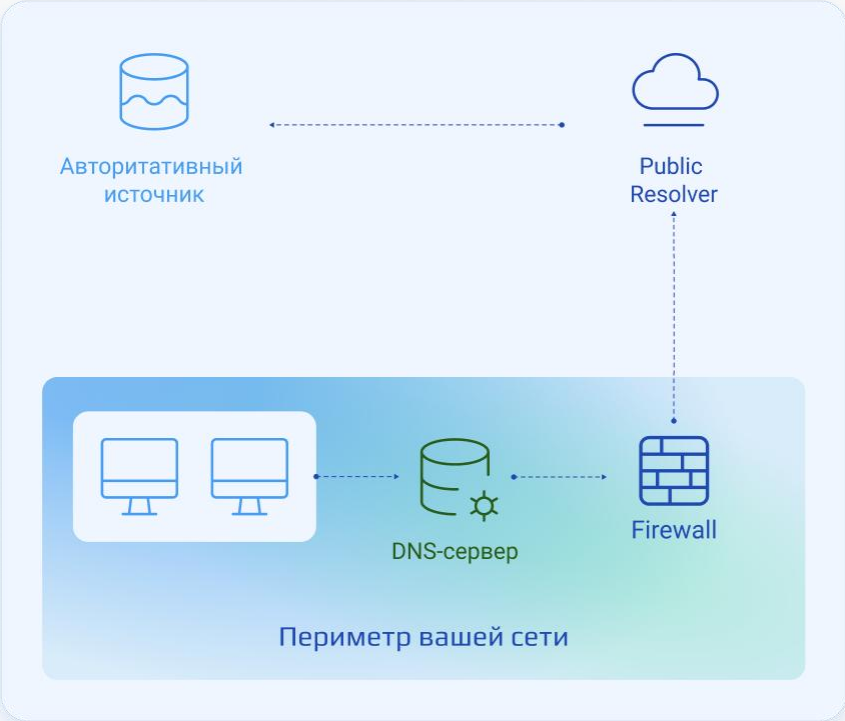


Схема DNS-трафика

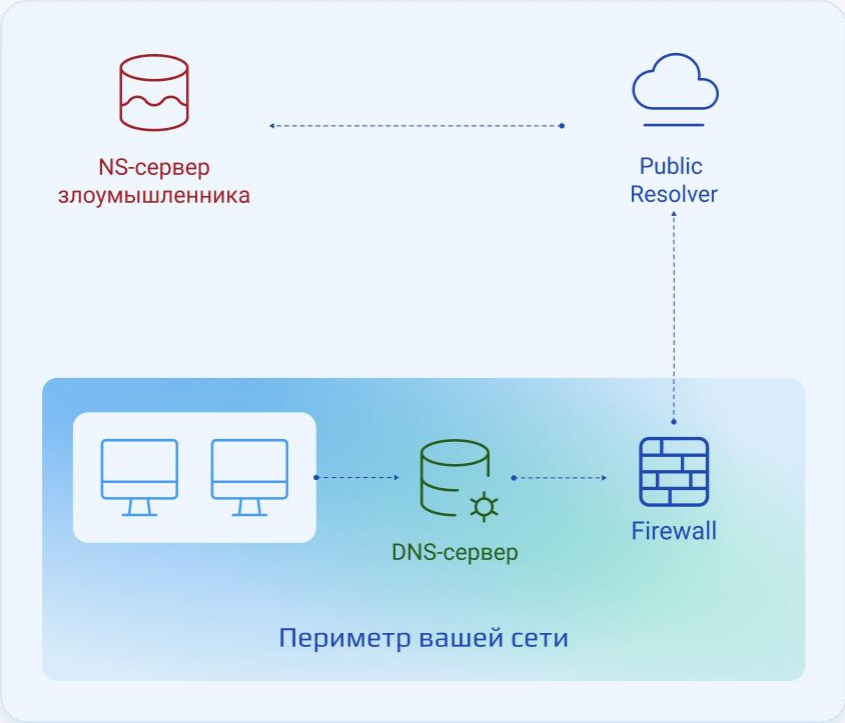
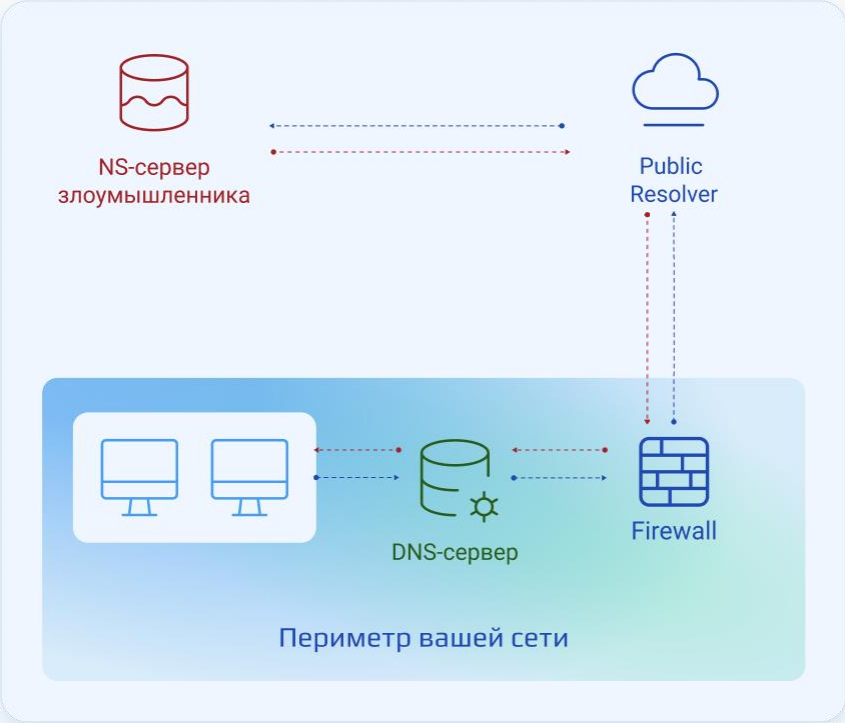
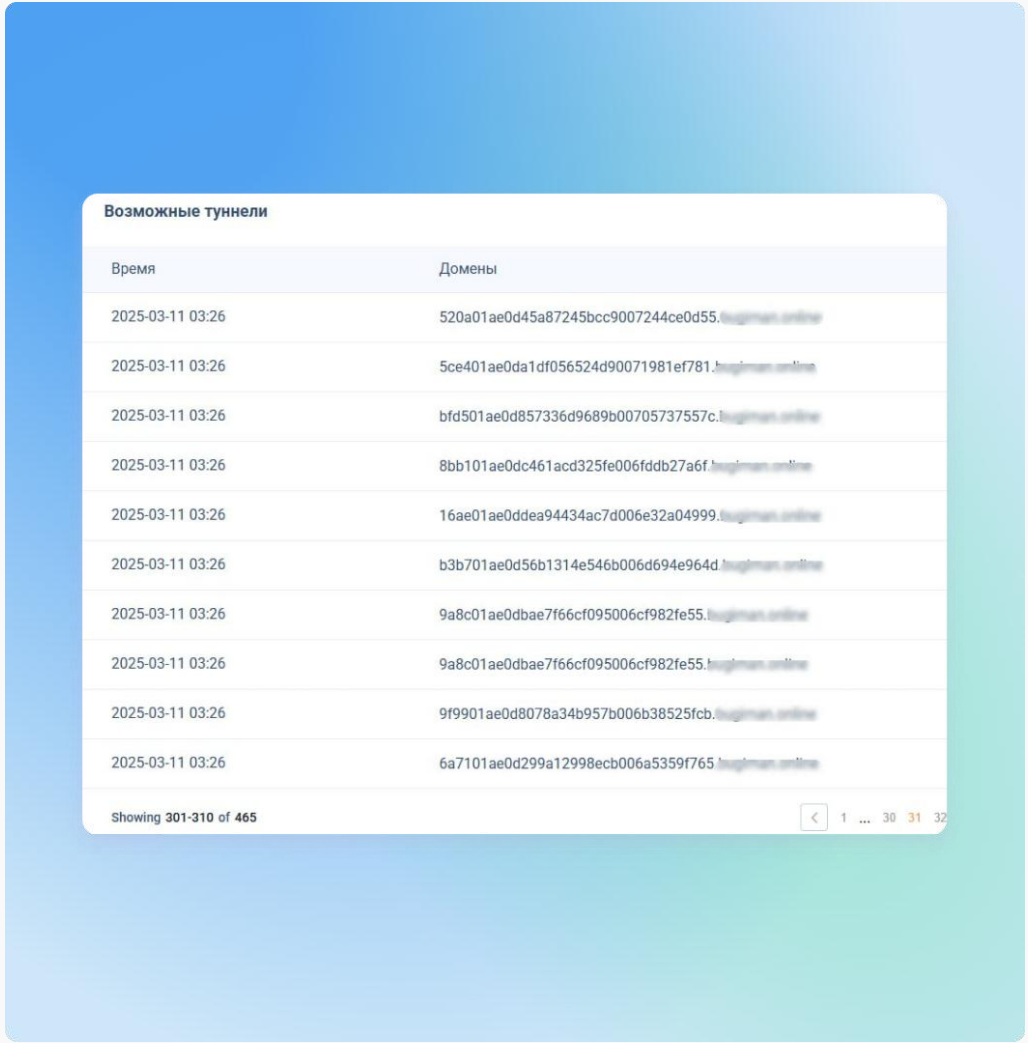


Схема DNS-трафика

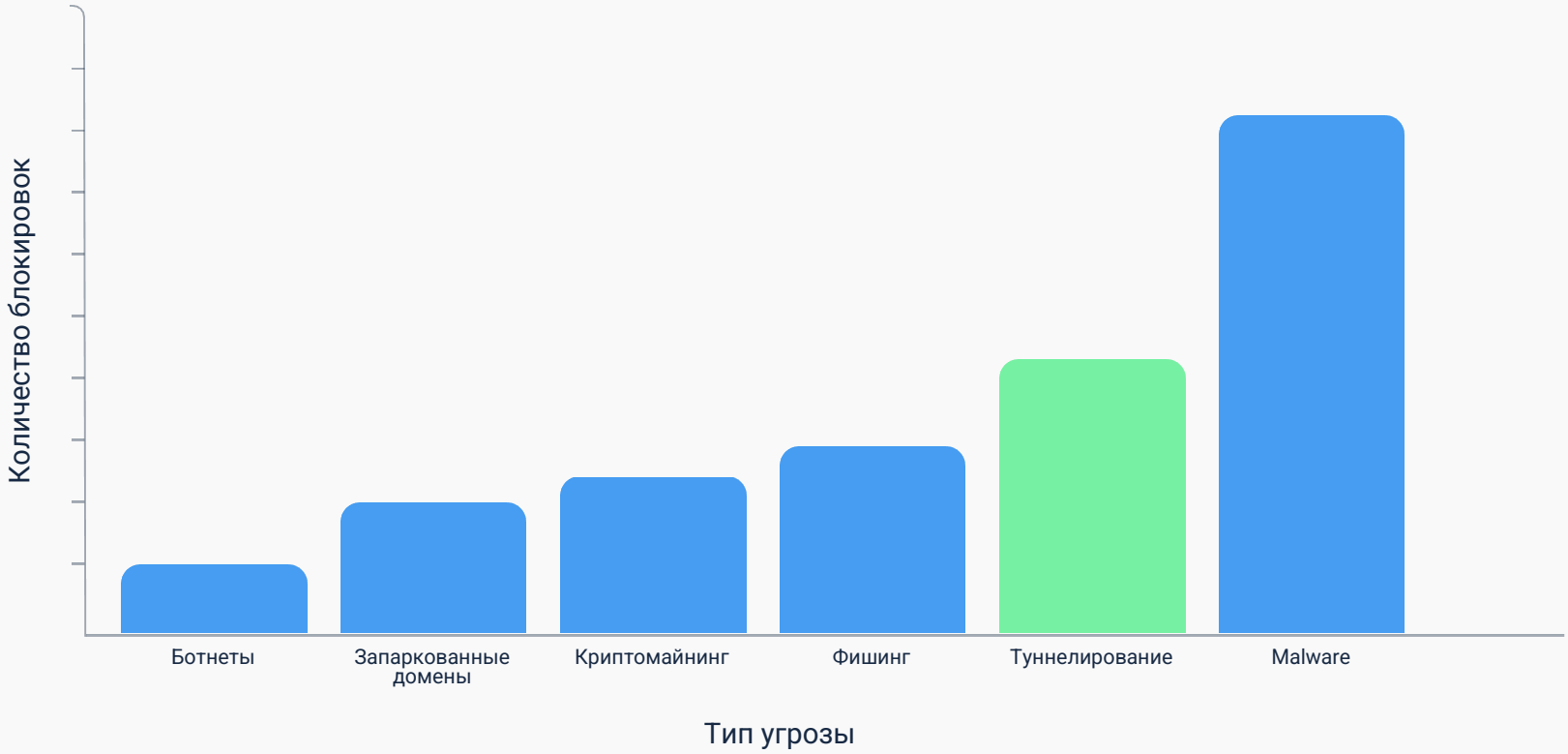


Как передается полезная нагрузка

Любая полезная нагрузка может быть передана прямо в самом домене в виде текста



ТОП блокировок по категориям за 2025



F6 рекомендует отслеживать DNS-трафик

В ежегодном отчете об угрозах в России и Беларуси F6 подчеркивает важность защиты DNS вектора, несмотря на то, что вендор не занимается разработкой решений класса защиты DNS

«Отслеживать трафик DNS: некоторые разновидности вредоносного программного обеспечения требуют связи с сервером или C2, вредоносное соединение может маскироваться под легитимный трафик, в том числе по протоколу HTTP»

Специфические DNS-угрозы

которые невозможно заблокировать на основании статических баз

DNS-туннели

DGA

Zero Day

Просто смена внешнего резолвера

Без изменений сети

работает вне вашей инфраструктуры, без нового ПО или оборудования, достаточно смены IP внешнего резолвера

Полная приватность

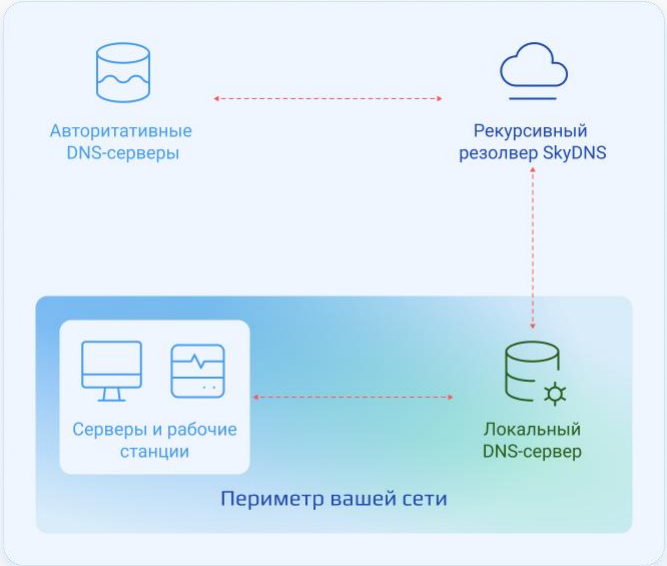
передается только публичная информация, которая и до этого покидала сеть

Максимальная безопасность

поставляется полностью очищенный DNS-трафик

Высокая скорость и отказоустойчивость

распределённая BGP Anycast сеть с серверами в разных регионах обеспечивает мгновенный отклик



Преимущества решения SkyDNS

Блокировка угроз в динамике: система мгновенно реагирует на подозрительные ресурсы

Непрерывная адаптация защиты к новым угрозам с помощью AI/ML-алгоритмов

Быстрая интеграция за 15 минут: просто смена резолвера, инфраструктура не меняется

Оставьте мне контакты,
и я свяжусь с вами