SkyDNS

ZTNA: Почему безопасность начинается с первого запроса, а не с доступа к сети

Пересмотр подходов защиты

Люди и опыт за продуктом SkyDNS

- Екатеринбург
- 15+ лет аналитики DNS-угроз
- Собственный центр аналитики угроз на базе AI\ML

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

На этом фоне приходит Zero Trust

«Никогда не доверяй — всегда проверяй»

Джон Киндерваг, автор концепции Zero Trust (2009)

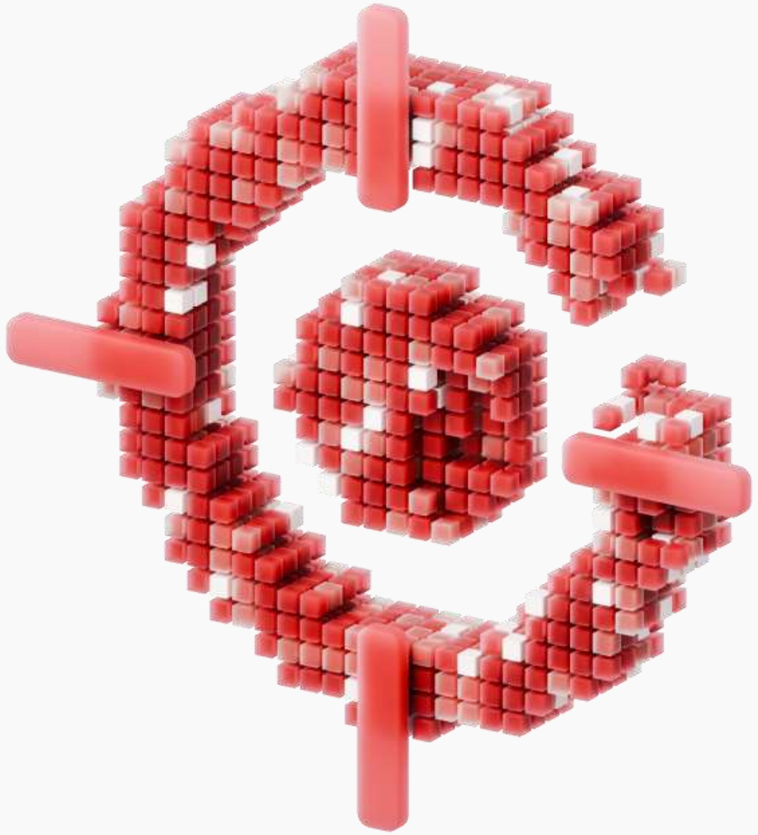
ZTNA без DNS

Ожидание:
ZTNA

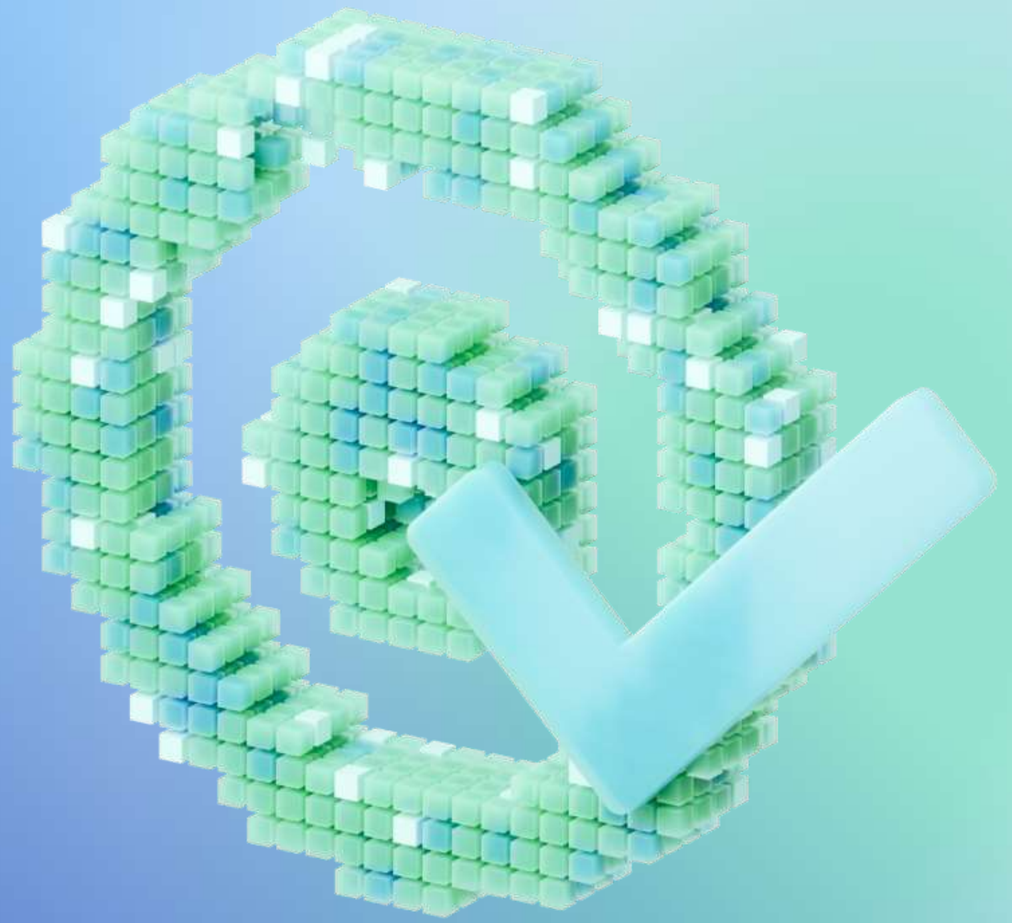
Проверяем каждый запрос с нуля

Реальность:
ZTNA без DNS

Проверяем все, кроме первого запроса



Zero Trust: Проверять каждый запрос. Значит и первый



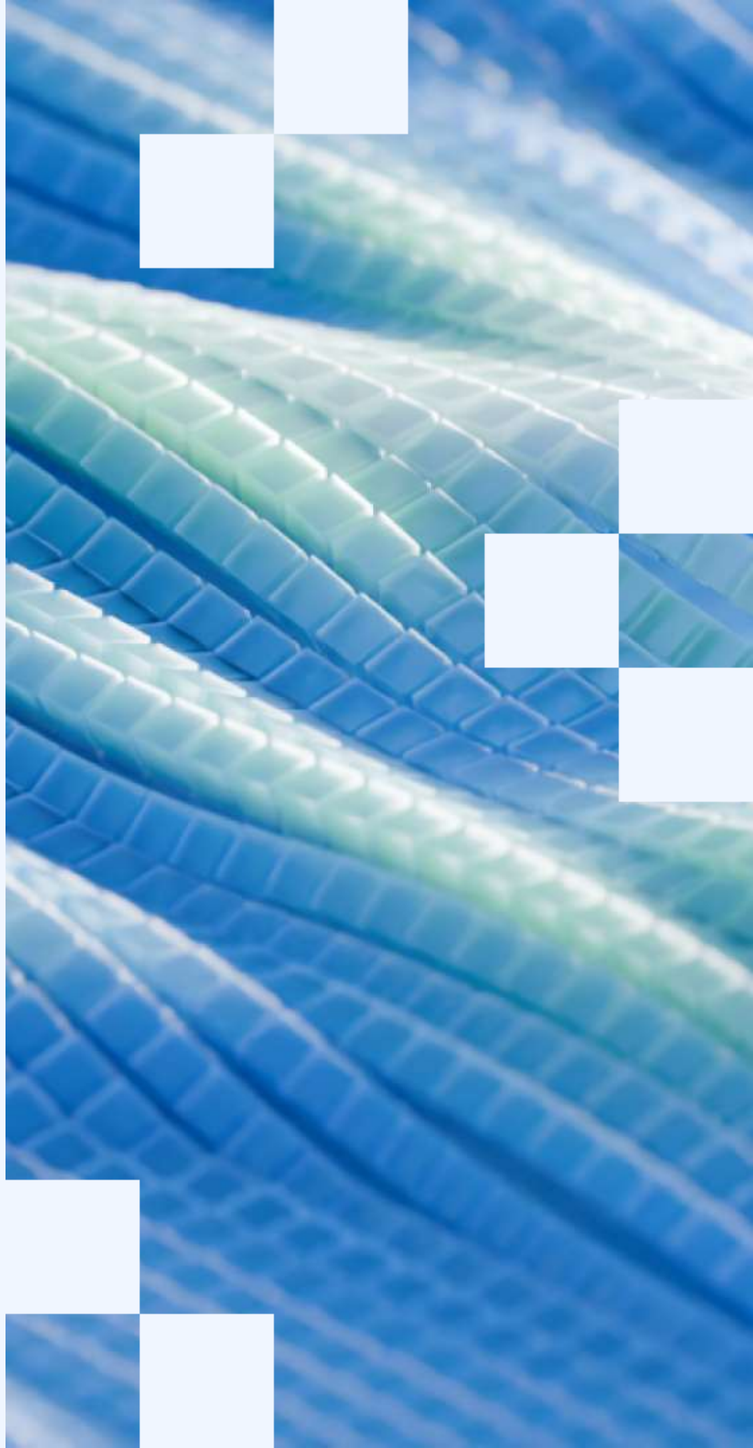
Реактивно, а не проактивно

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



Первый контакт с внешним миром — это DNS

Решение о доступе мы принимаем после того,
как запрос уже выполнен

Специфические DNS-угрозы

которые невозможно заблокировать на основании статических баз

DNS-туннели

DGA

Zero Day

Покрытие MITRE ATT&CK

DNS-контроль дает максимальную ценность в тактике Организации управления (C2C)

1 TA0001 Первоначальный доступ

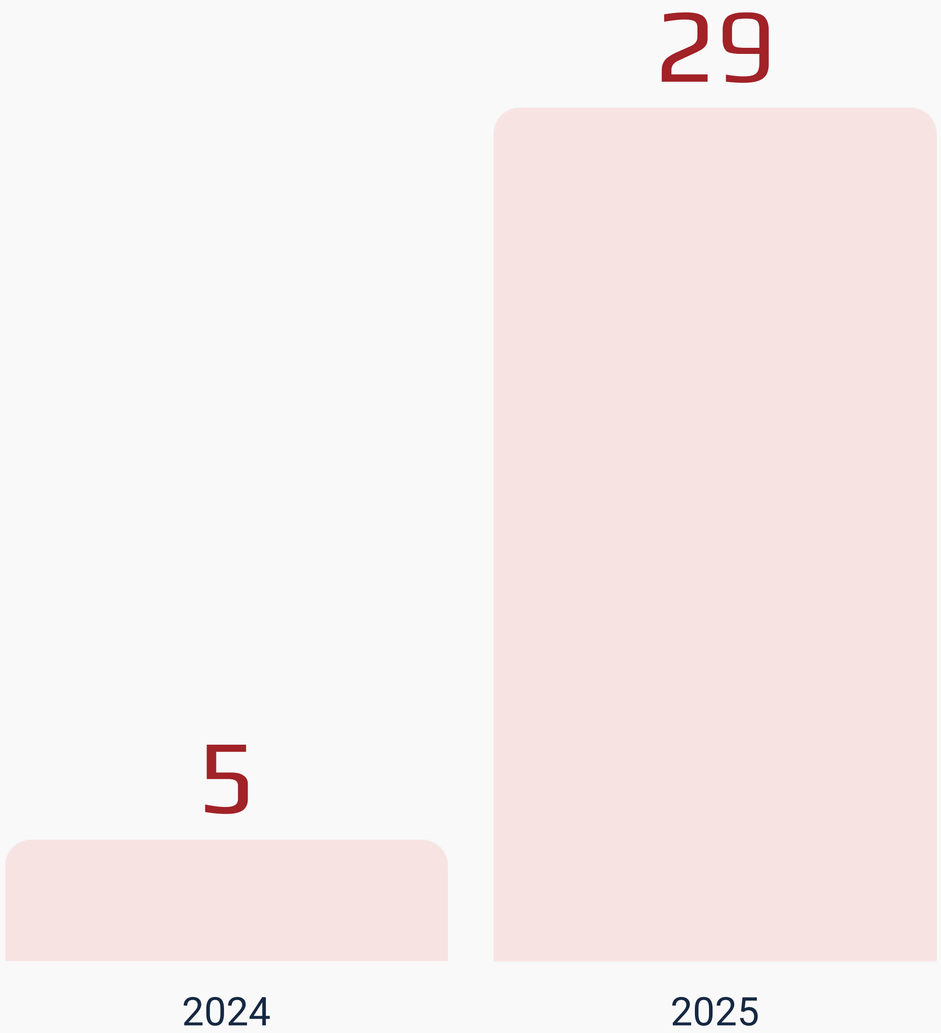
T1566.002: Целевой фишинг со ссылкой
T1189: Теневая (drive-by) компрометация

2 TA0011 Организация управления (C2C)

T1071.004: DNS
T1572: Туннелирование протокола
T1568: Динамическое разрешение

3 TA0010 Эксфильтрация данных

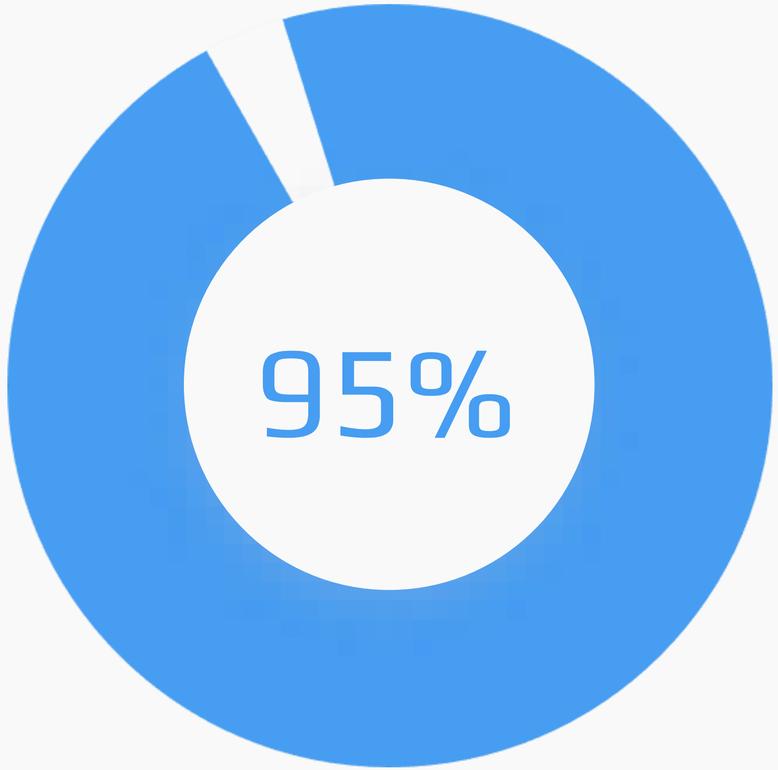
T1048: Эксфильтрация по альтернативному протоколу



1/3

Почти в **6 раз больше DNS-угроз** на пользователя

Источник: DNSFilter 2025 Annual Security Report



2/3

Вредоносных доменов нигде не «светятся» — их видит только одна компания

Источник: Infoblox 2025 DNS Threat Landscape Report

54,7%

3/3

Вредоносных доменов генерируются автоматически алгоритмами (DGA)

Источник: Infoblox 2025 DNS Threat Landscape Report

Статистика подтверждается на практике

Итоги пилотов 2025

у **5%** компаний

Действующее вирусное заражение

у **9%** компаний

Незаконный майнинг сотрудниками

у **11%** компаний

C2-трафик

у **30%** компаний

Ранее недетектируемые Zero-Day атаки

у **12%** компаний

Ранее неблокируемая DGA-активность

у **30%** компаний

DNS-туннели

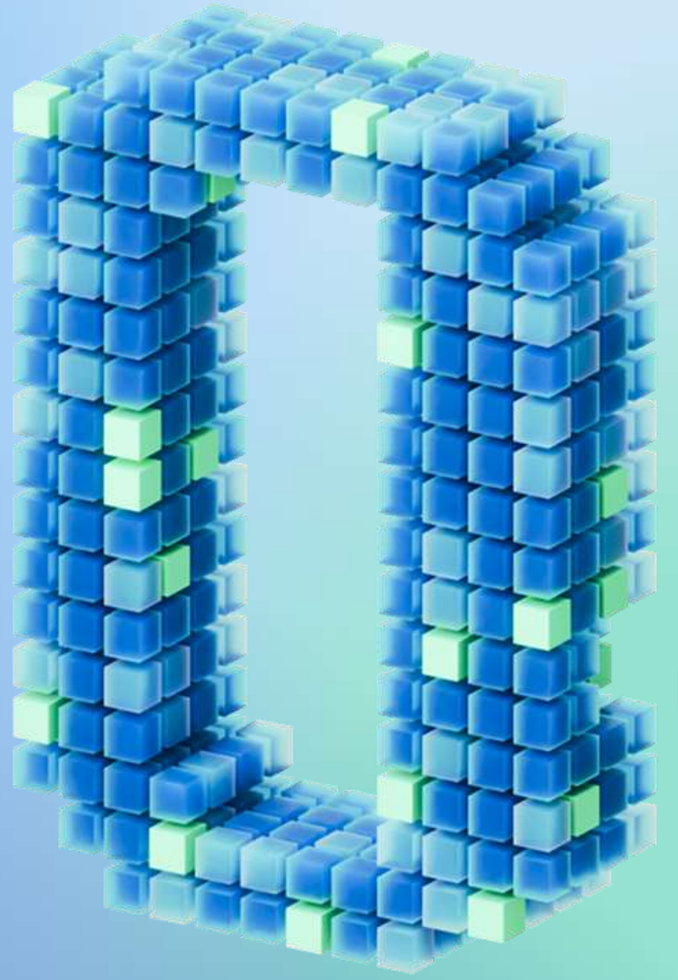
у **32%** компаний

Botnet-активность

Философия: MTTR = 0

DNS — один из самых ранних уровней, где атаки можно остановить.

Поэтому мы в SkyDNS сознательно сфокусированы именно на DNS-уровне.



ZTNA с первого запроса — это DNS-безопасность

1

ZTNA должно

начинаться с первого запроса, а не с доступа к сети

2

Обход СЗИ

возможен из-за сдвига точки контроля; первый запрос часто вне зоны видимости

3

DNS-безопасность

даёт контроль с самого начала и дополняет СЗИ

Оставьте мне контакты,
и я свяжусь с вами