DNSSense

Новый подход к обнаружению вредоносных программ и обеспечению мониторинга для сетей, приложений и пользователей

Переосмысление защиты DNS

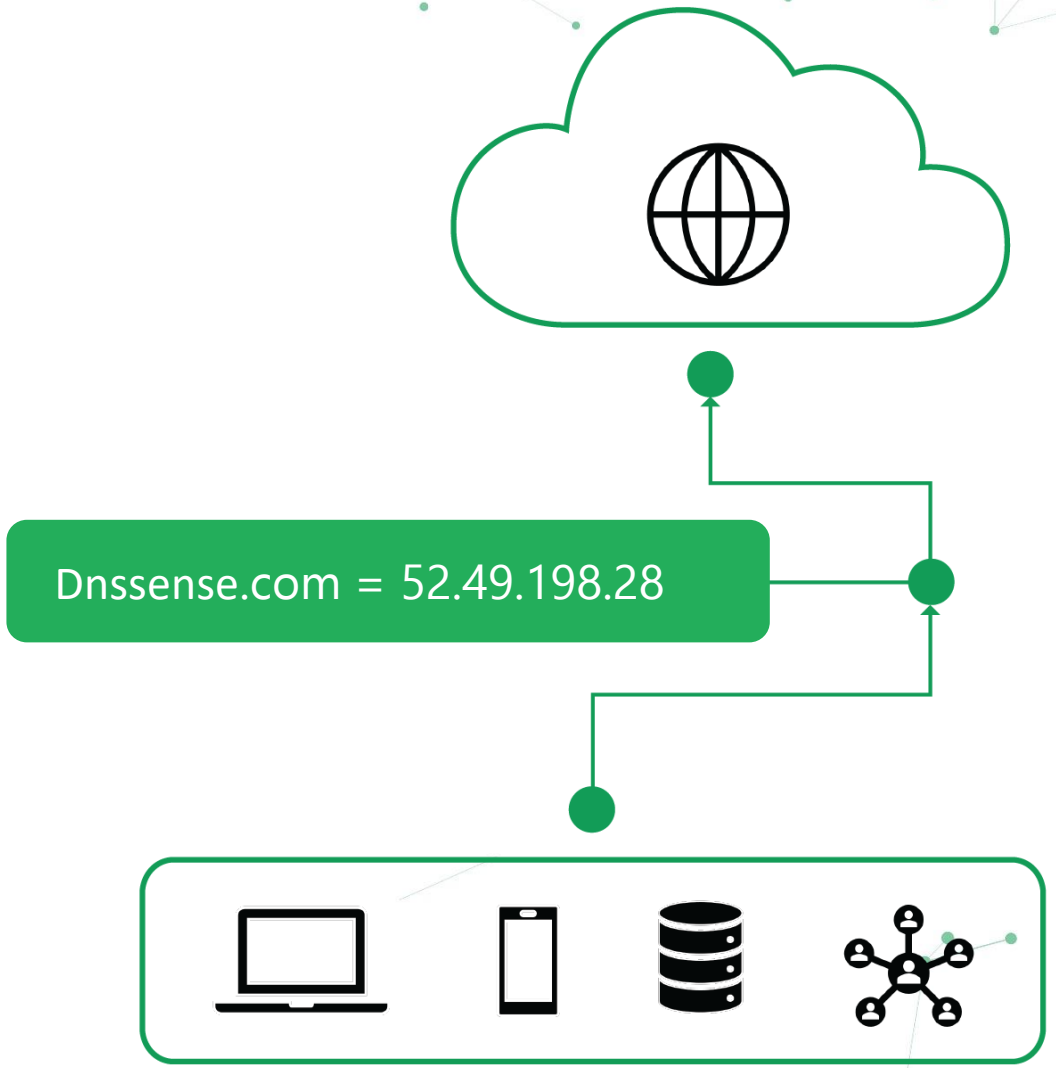
Олег Котов, CISSP

oleg.kotov@dnssense.com
+7 916 836 63 68

dnssense.com

» Что такое DNS?

- DNS расшифровывается как «Система доменных имён»
- Это первый шаг в подключении к Интернету
- «Телефонная книга» Интернета
- Используется всеми устройствами



» Какие службы полагаются на DNS?

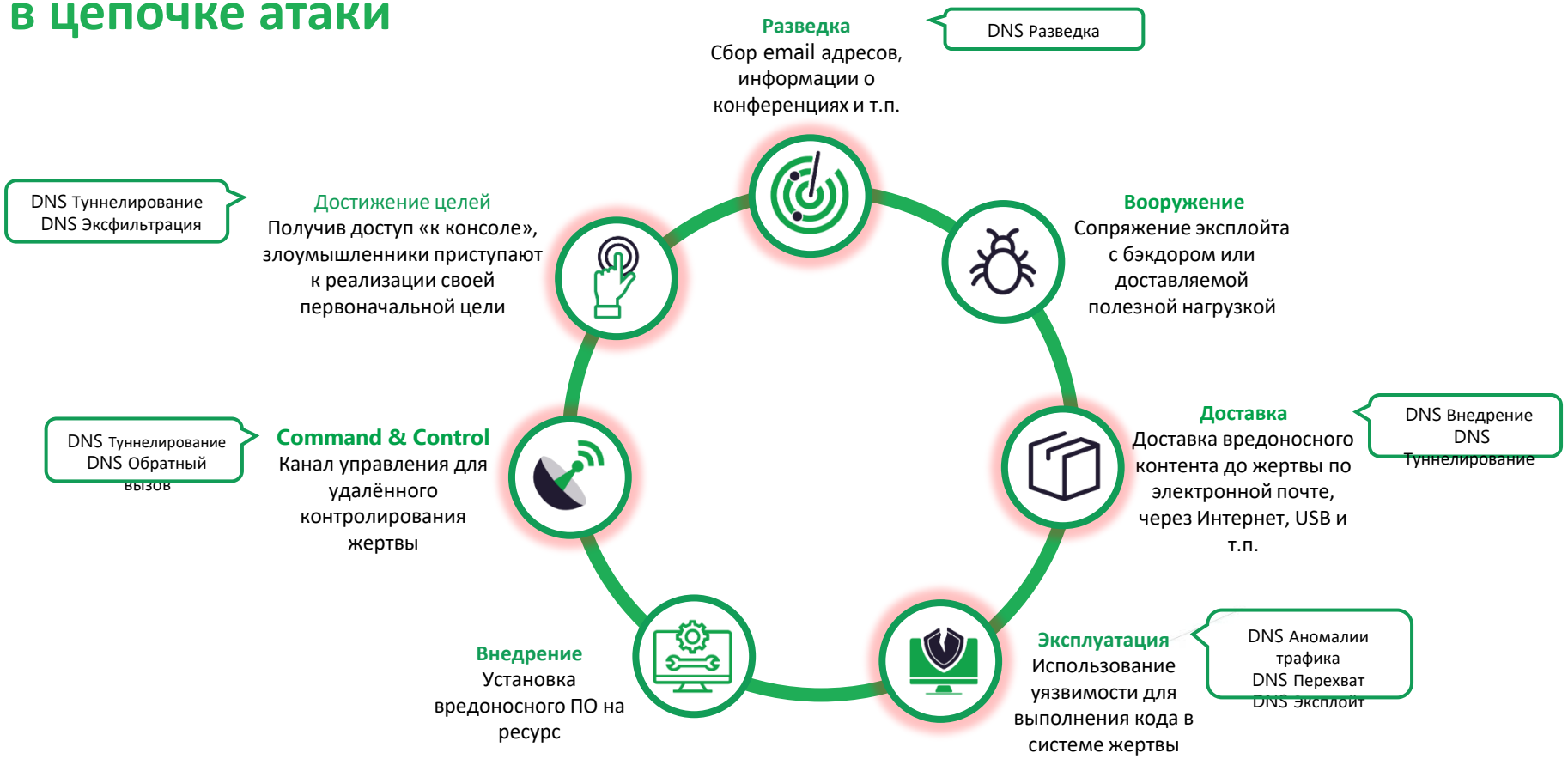
- Веб-страницы
- Почтовые серверы
- Многоуровневые веб-приложения
- Базы данных
- Инструменты обмена мгновенными сообщениями
- Доступ к внешней веб-почте
- Услуги онлайн-конференций
- VPN
- IoT приложения
- P2P ресурсы
- Брошюры и файлы документации со ссылками

... и многое другое ...

DNS в основании любой цифровой коммуникации
Бизнес зависит от работоспособности сетевой инфраструктуры, а она зависит от DNS

» DNS-запросы

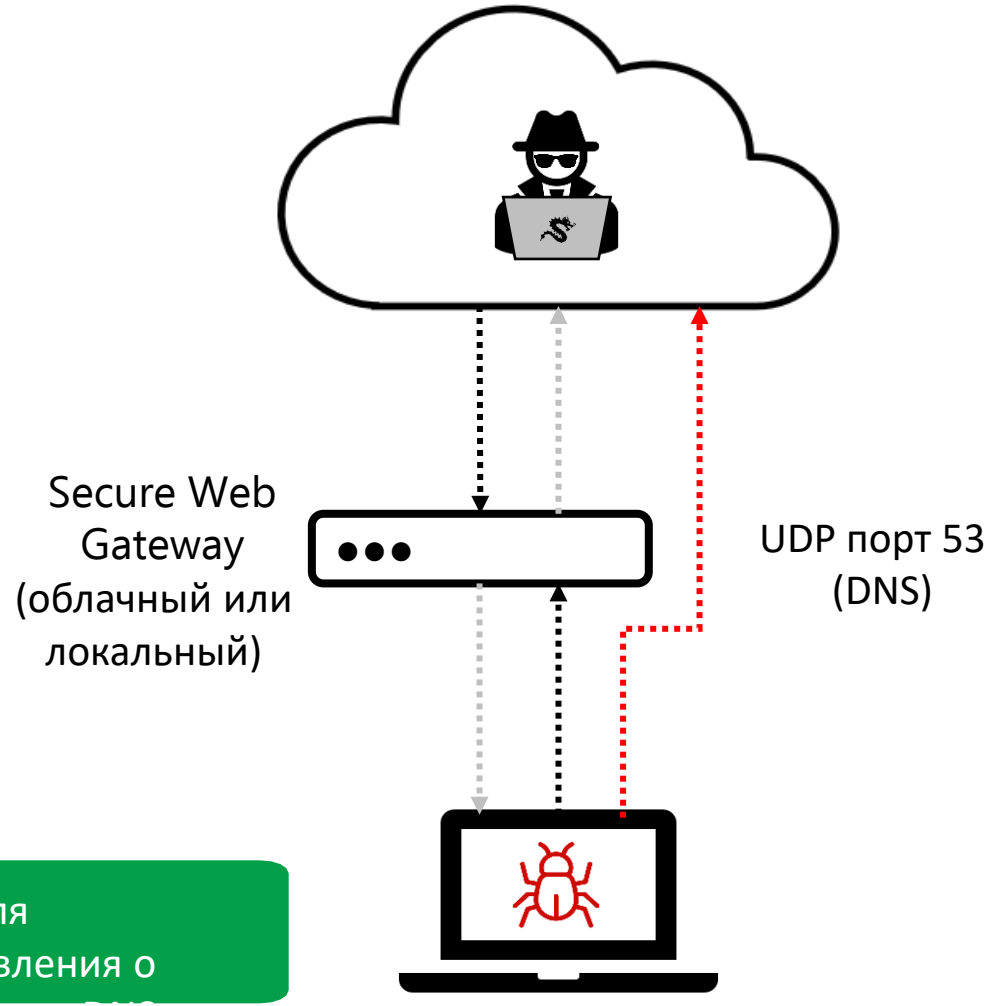
» DNS в цепочке атаки



DNS как главная угроза

95% вредоносных программ, используют DNS для :

- Связь с Command and Control серверами (C&C)
- Эксфильтрация и подмена данных
- Перенаправление трафика на вредоносные сайты



Существующие средства контроля безопасности не имеют представления о

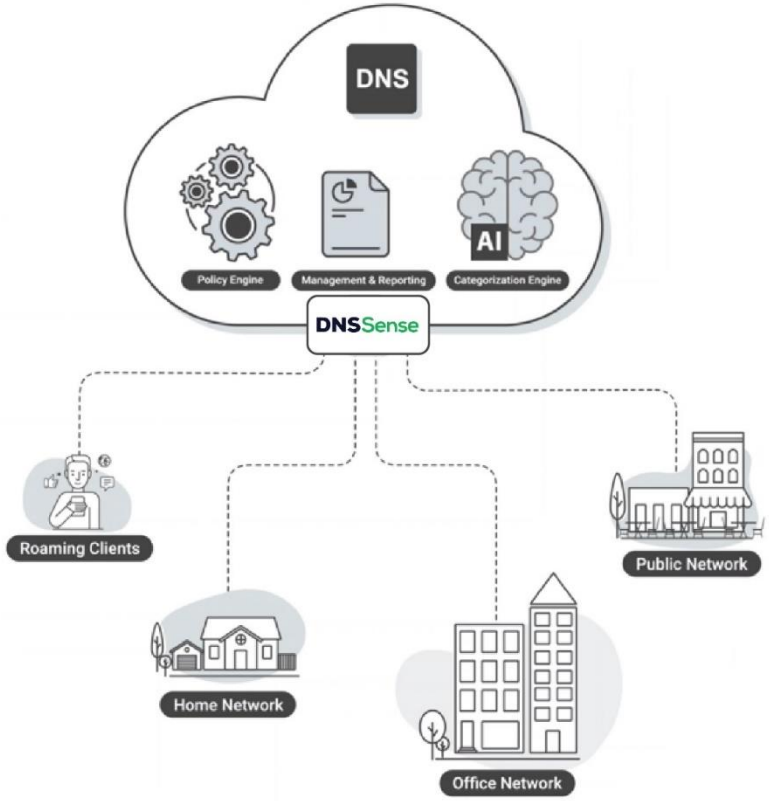
Уникальный механизм категоризации доменов на базе искусственного интеллекта

- **Полностью основанная на искусственном интеллекте категоризация доменов**
- **Лучшая в мире динамическая база данных угроз**
- **Классификация впервые увиденных доменов менее чем за 10 минут**
- **Более 800 параметров анализа для каждого домена**

www.cyber-xray.com

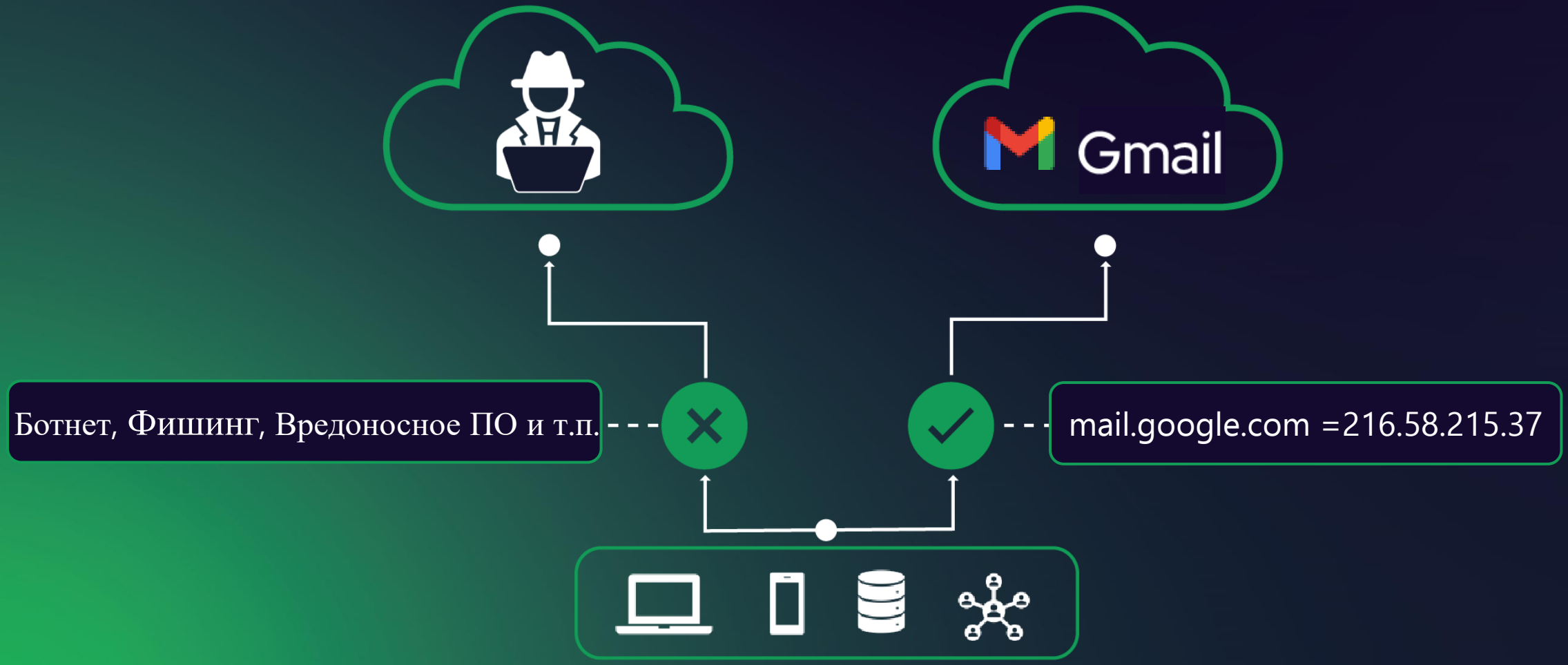
DNSDome

- **Облачный защитный DNS**
- **Активная защита от вредоносного ПО**
- **Защита всех устройств**
- **Защита клиентов в роуминге**
- **Быстрое развёртывание**

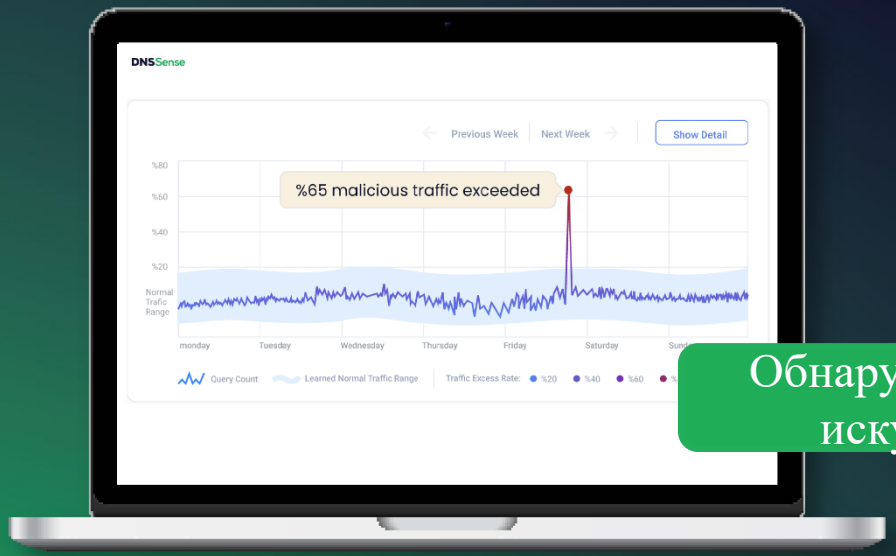


Самый продвинутый защитный DNS на рынке

» DNSDome – Облачное решение



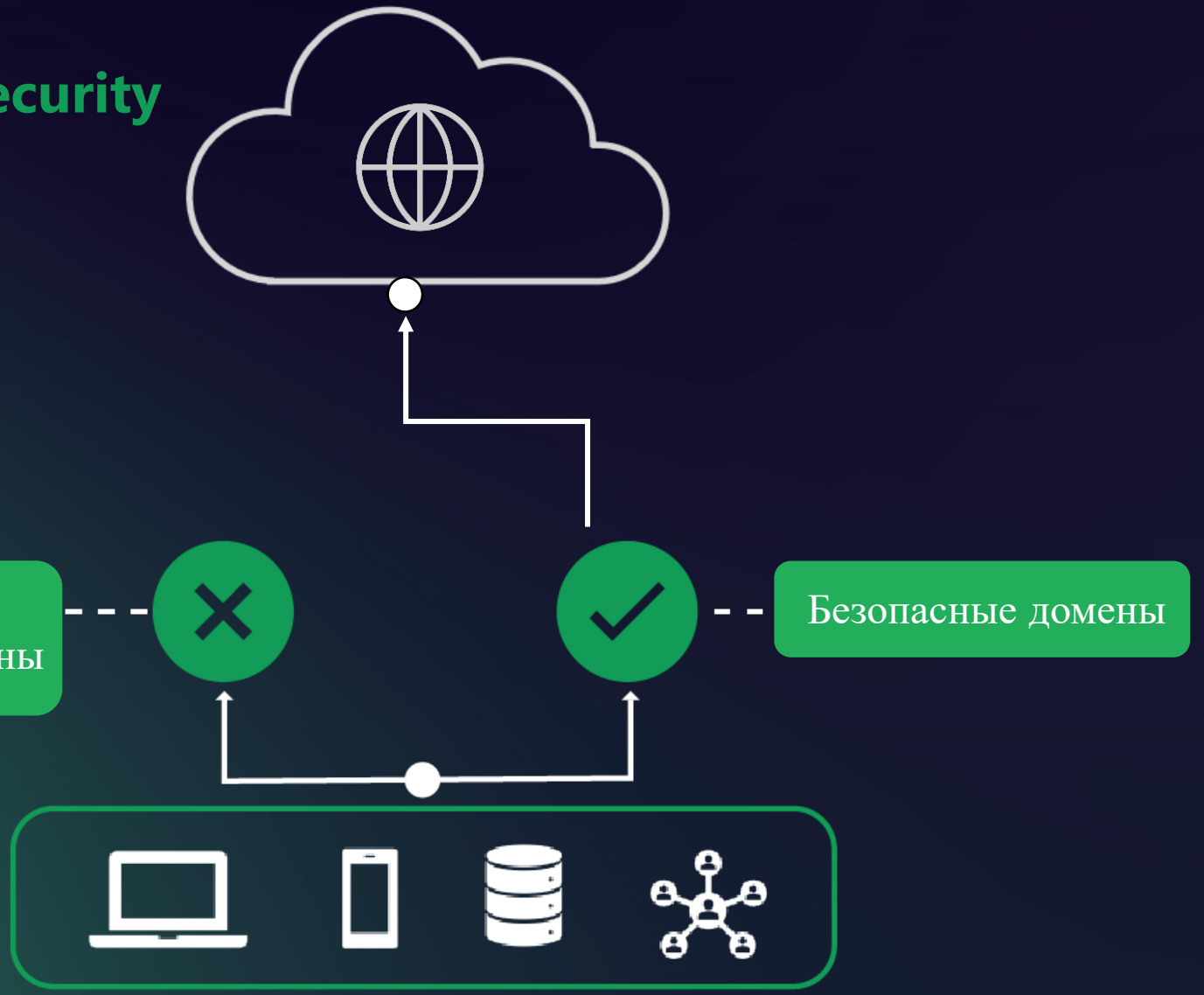
» DNSDome – Алгоритмы



Обнаружение аномалий на основе искусственного интеллекта

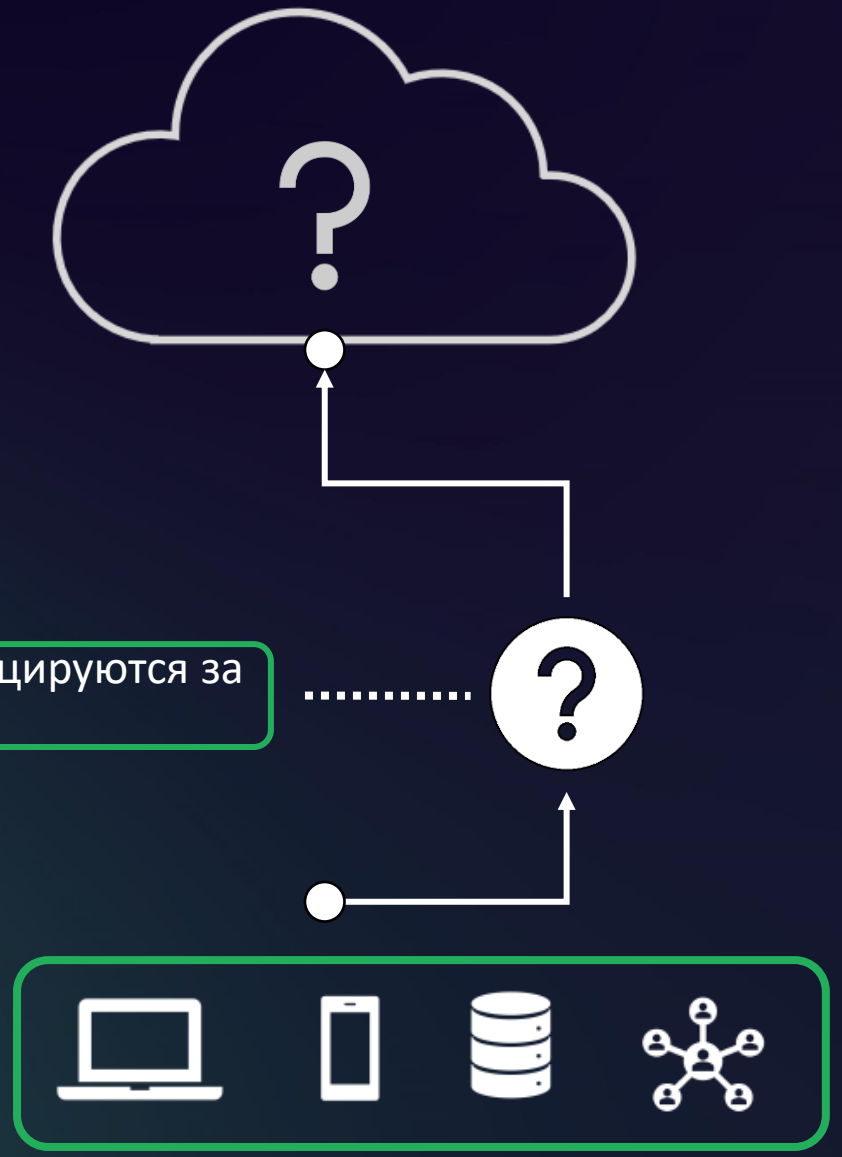
» DNSDome – Модель Positive Security

Ботнеты
Фишинг
Шифровальщики



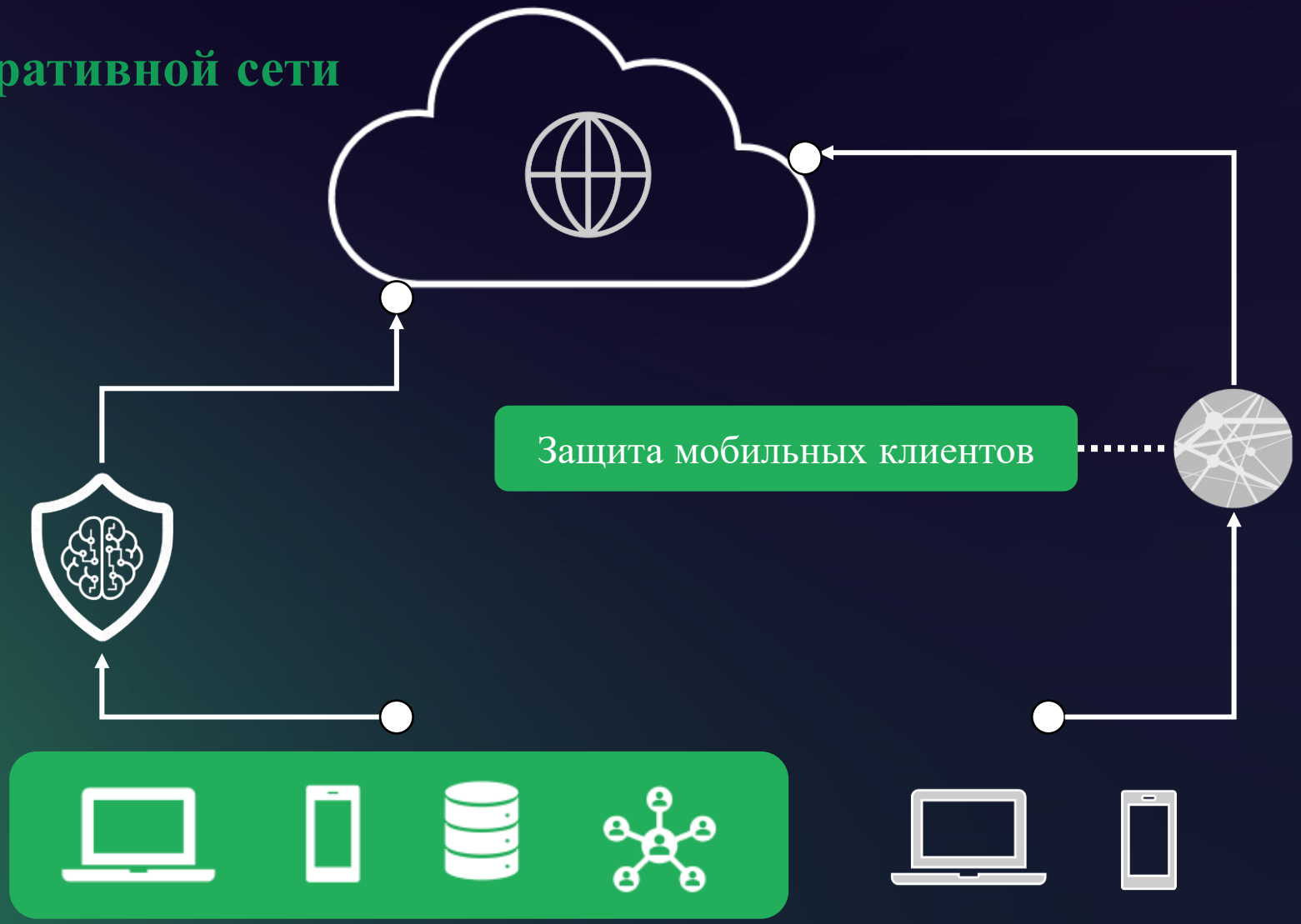
Making Sense of DNS

» DNSDome – Категоризация



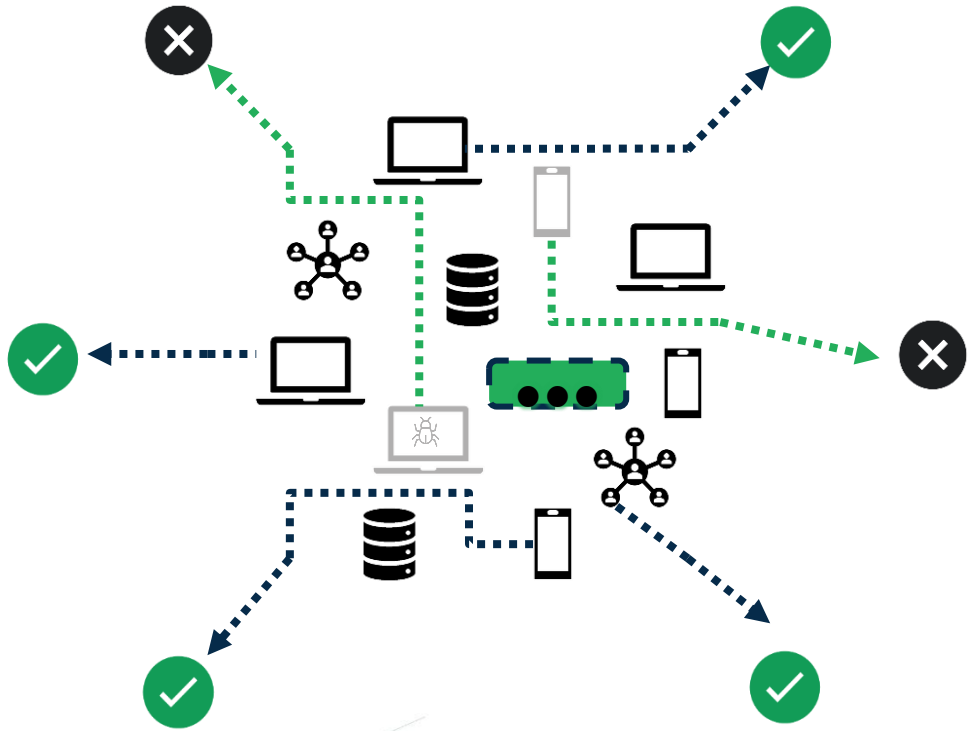
Впервые увиденные домены классифицируются за 10 минут!

» DNSDome – Вне корпоративной сети



DNSEye

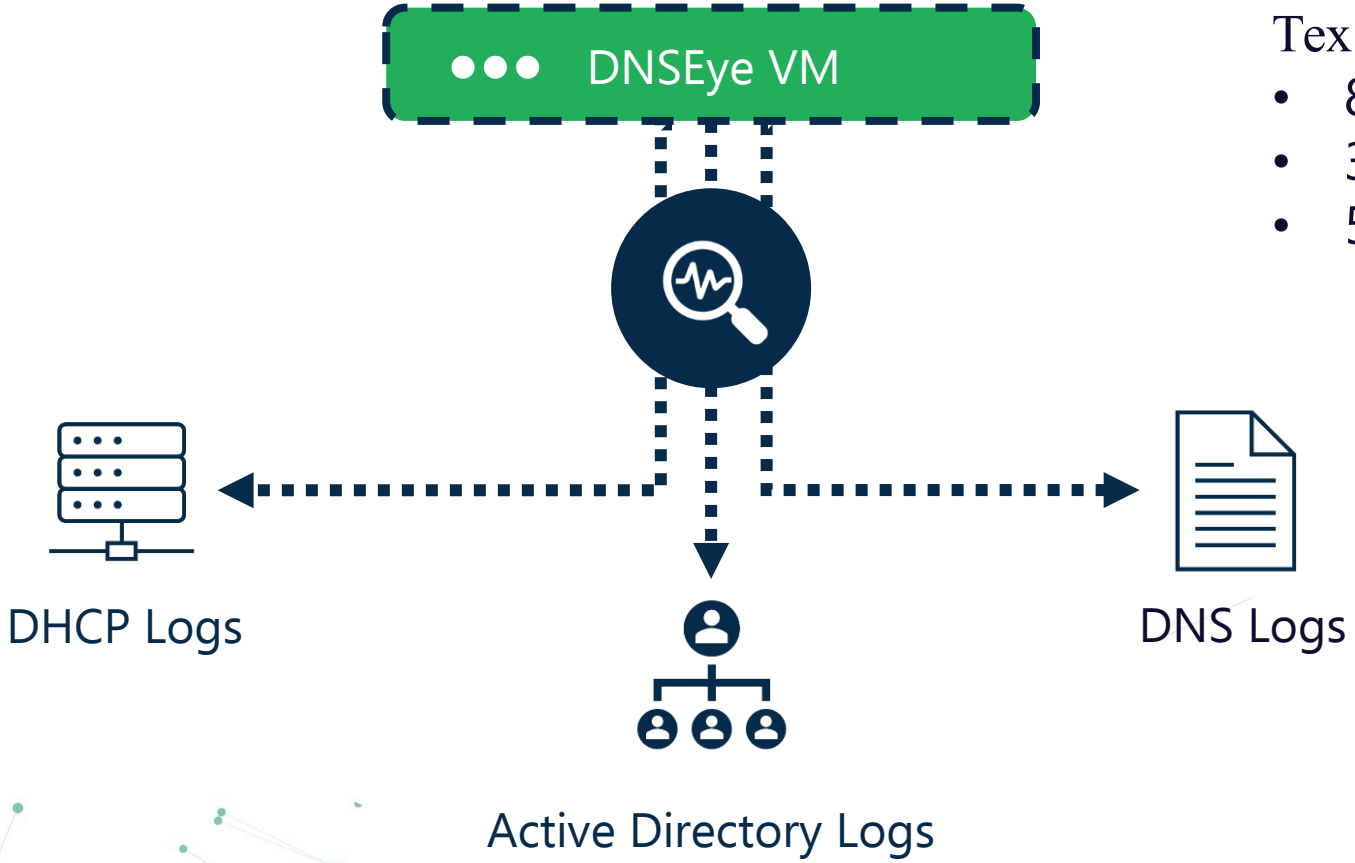
- **On-prem VM**
- **Обнаружение заражённых устройств**
- **Обнаружение аномалий**
- **Отчёт о первом посещении**
- **Отчёт о пробелах в безопасности**
- **SIEM интеграция**



Уникальный продукт, лидер рынка безопасности DNS в G2

» DNSEye – On-prem решение

DNSEye - Как это работает?



Тех.требования:

- 8 Core
- 32GB RAM
- 500GB HDD

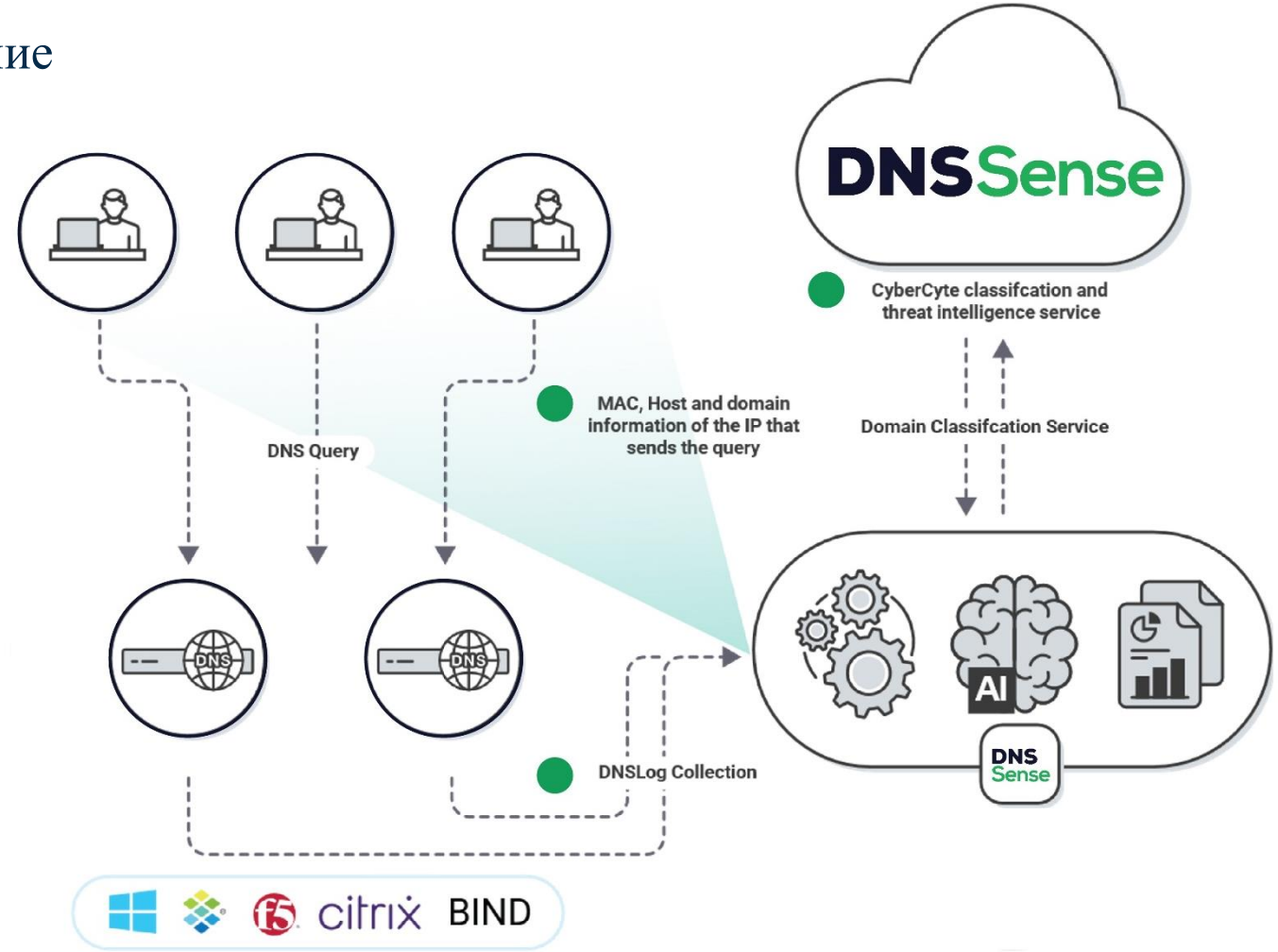
» DNSEye – On-prem решение

Microsof DNS Server Debug Log

11.03.2021 10:42:10 14E4 PACKET 000001FC8495F560 UDP Rcv 10.0.0.51 38a8 Q [0001 D NOERROR] A (3)bp2(7)blogger(3)com(0)
11.03.2021 10:42:10 14E4 PACKET 000001FC82B78080 UDP Rcv 10.0.0.51 8375 Q [0001 D NOERROR] A (7)walmart(3)com(2)br(0)
11.03.2021 10:42:10 14E4 PACKET 000001FC84DFB130 UDP Rcv 10.0.0.51 0bfa Q [0001 D NOERROR] A (7)rolloid(5)today(0)
11.03.2021 10:42:10 14E4 PACKET 000001FC8495F560 UDP Rcv 10.0.0.51 2af7 Q [0001 D NOERROR] A (13)digitaltrends(3)com(0)
11.03.2021 10:42:10 14E4 PACKET 000001FC82B78080 UDP Rcv 10.0.0.51 6c6c Q [0001 D NOERROR] A (8)navitime(2)co(2)jp(0)
11.03.2021 10:42:10 14E4 PACKET 000001FC84DFB130 UDP Rcv 10.0.0.51 5c69 Q [0001 D NOERROR] A (6)nvidia(3)com(0)
11.03.2021 10:42:10 14E4 PACKET 000001FC8495F560 UDP Rcv 10.0.0.51 b334 Q [0001 D NOERROR] A (13)eschoolplus31(3)k12(2)ar(2)us(0)
11.03.2021 10:42:10 14E4 PACKET 000001FC85441140 UDP Rcv 10.0.0.51 578c Q [0001 D NOERROR] A (4)tijd(2)be(0)
11.03.2021 10:42:10 14E4 PACKET 000001FC83AA25A0 UDP Rcv 10.0.0.51 9d96 Q [0001 D NOERROR] A (8)demorgen(2)be(0)
11.03.2021 10:42:10 14E4 PACKET 000001FC8495F560 UDP Rcv 10.0.0.51 4836 Q [0001 D NOERROR] A (9)ukunblock(5)today(0)
11.03.2021 10:42:10 14E4 PACKET 000001FC85441140 UDP Rcv 10.0.0.51 8634 Q [0001 D NOERROR] A (9)evangelio(4)blog(0)
11.03.2021 10:42:10 14E4 PACKET 000001FC825CF890 UDP Rcv 10.0.0.51 e1dd Q [0001 D NOERROR] A (5)stuff(2)co(2)nz(0)
11.03.2021 10:42:10 14E4 PACKET 000001FC82BBA070 UDP Rcv 10.0.0.51 222d Q [0001 D NOERROR] A (10)soul-anime(2)us(0)
11.03.2021 10:42:10 14E4 PACKET 000001FC85441140 UDP Rcv 10.0.0.51 6570 Q [0001 D NOERROR] A (6)letras(3)mus(2)br(0)
11.03.2021 10:42:10 14E4 PACKET 000001FC825CF890 UDP Rcv 10.0.0.51 261f Q [0001 D NOERROR] A (10)pentestlab(4)blog(0)
11.03.2021 10:42:10 14E4 PACKET 000001FC82BBA070 UDP Rcv 10.0.0.51 62c3 Q [0001 D NOERROR] A (8)yeloplay(2)be(0)
11.03.2021 10:42:10 14E4 PACKET 000001FC85441140 UDP Rcv 10.0.0.51 2ca0 Q [0001 D NOERROR] A (4)smbc(2)co(2)jp(0)

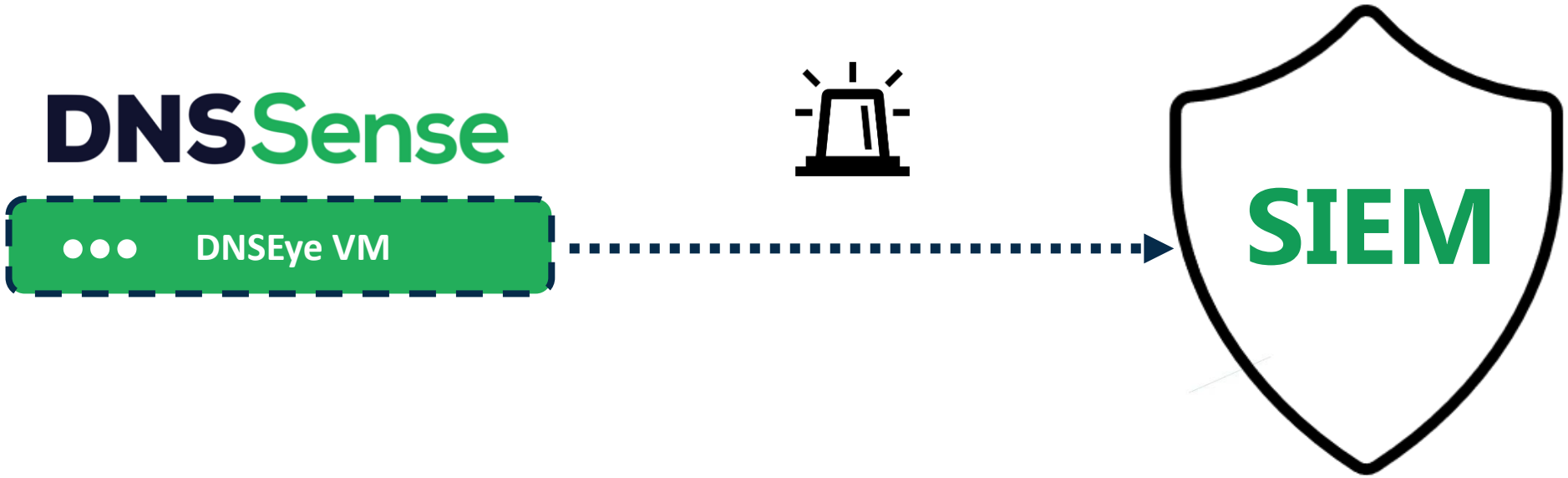
» DNSEye – On-prem решение

DNSEye – Масштабирование



» DNSEye – On-prem решение

DNSEye – Интеграция с SIEM на основе правил



» DNSEye – Security Gap

Выявление пробелов в защите

Domain	Categorory	User	Hostname	UTM HTTP Request	Proxy HTTP Request	DNS Request	Attack Result
qjcycc.com	DGA Domain	Jack Talk	CTO-Macbook	Passed	Passed	Passed	Attack Successful
Faccebook.com	Phishing	Darek Baker	Sales-PC1	Passed	Blocked	Passed	Attack Blocked By Proxy
zzgg123.com	Malware/Virus	Daniel W.	Daniel-Mac	Passed	Passed	Passed	Attack Successful
51news.xyz	Potentially Dangerous	Natalie B.	Natalie's Iphone	Passed	Passed	Passed	Attack Successful
realsrv.com	Malware/Virus	Tatiana K.	TanyaPC	Passed	Blocked	Passed	Attack Blocked By Proxy
instaggrm.com	Phishing	Johan	230X130	Passed	Passed	Passed	Attack Successful

» DNSEye – Security Gap

Security Gap - Как это работает?

1. Устройство виртуальной машины создаёт список вредоносных доменов, обнаруженных в журналах DNS

» DNSEye – Security Gap

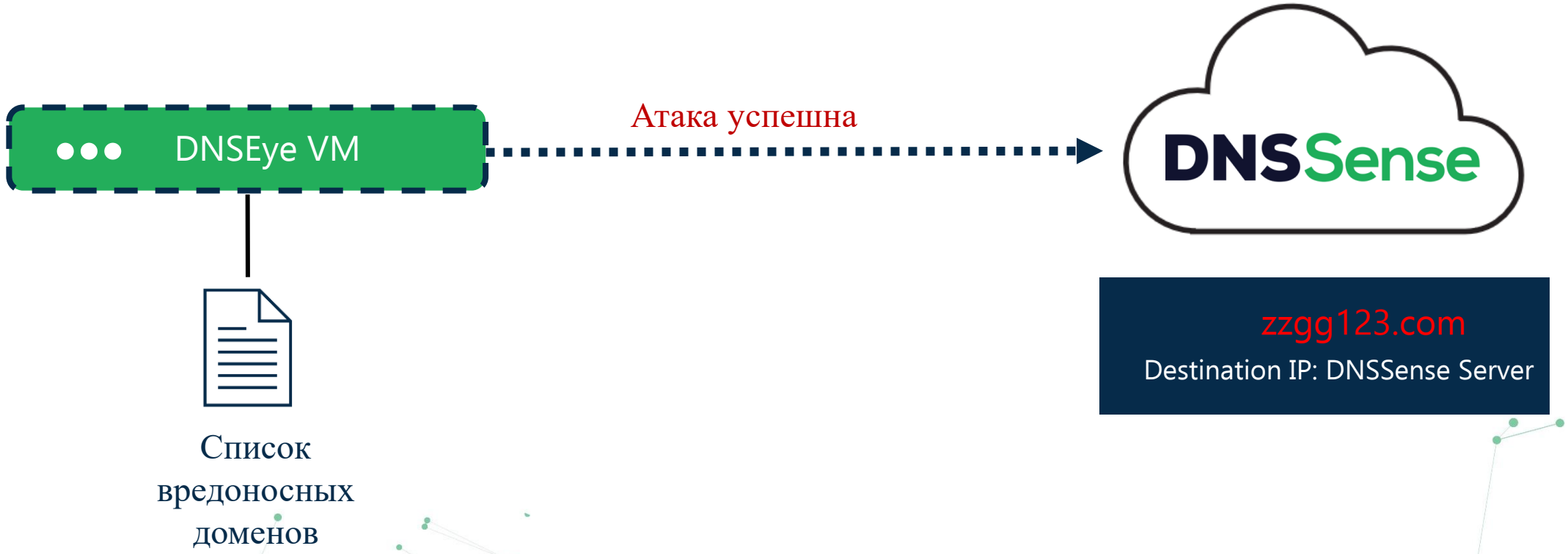
Security Gap - Как это работает?

2. Виртуальная машина пытается подключиться к вредоносным доменам, обнаруженным в журналах DNS

» DNSEye – Security Gap

Security Gap - Как это работает?

3. Если DNSSense получает пакет, это означает, что в безопасности есть брешь



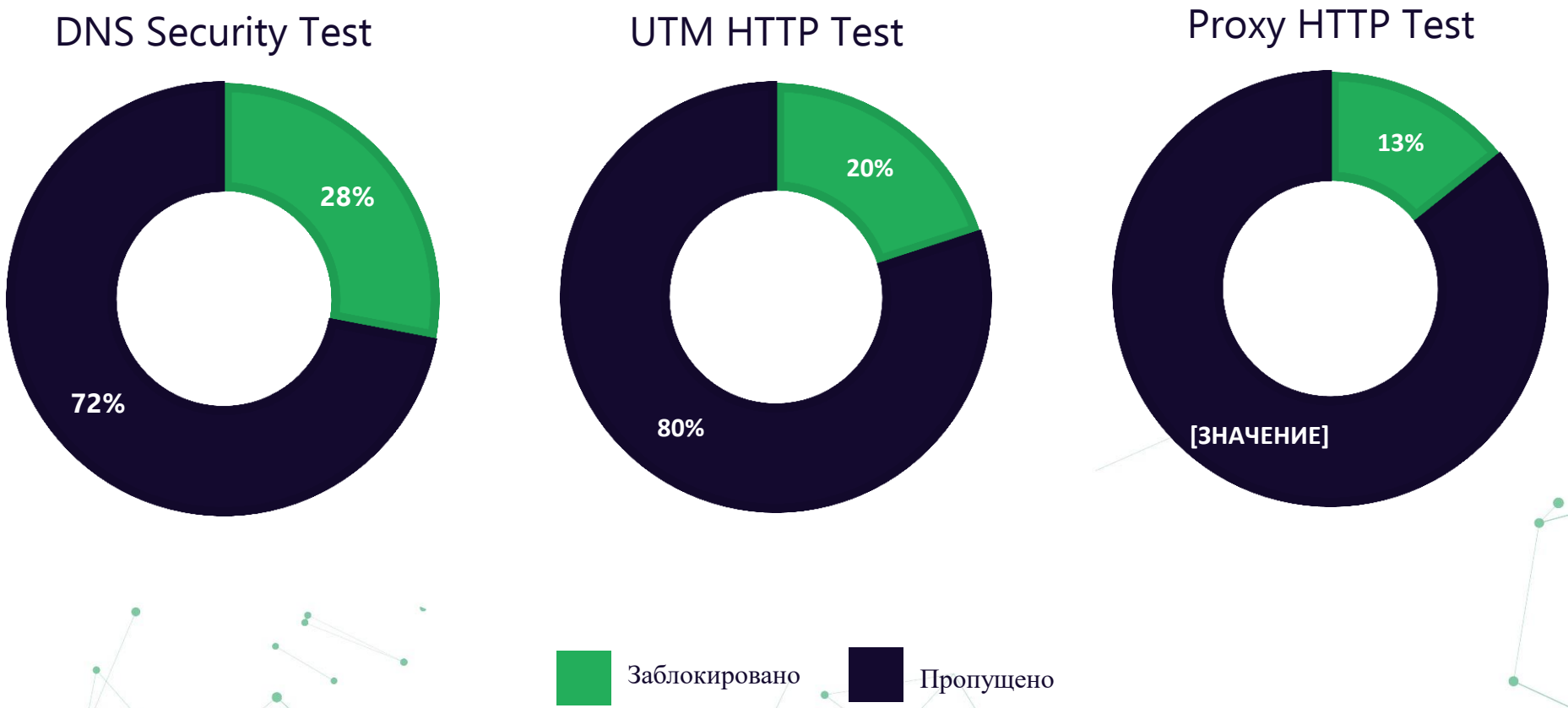
» DNSEye – Security Gap

Security Gap - Как это работает?

3. Если DNSSense не получает пакет, это означает, что атака была заблокирована

» DNSEye – Security Gap

Security Gap отчёт



Ценность решения

ВИДИМОСТЬ

- ✓ Сквозная видимость и анализ DNS-трафика без реорганизации инфраструктуры
- ✓ Обнаружение атак, заражений и попыток кражи данных в сети, которые ранее оставались незамеченными
- ✓ Выявление заражённых устройств и сотрудников потенциальных - мошенников, которые пытаются украсть данные
- ✓ Повысить уровень безопасности, закрыв обнаруженные пробелы

ЗАЩИТА

- ✓ Защита от вредоносных программ, фишинга, программ-вымогателей и атак нулевого дня
- ✓ Аналитика угроз на основе искусственного интеллекта
- ✓ Активная блокировка попыток кражи данных и масштабирование защиты на все части сети

ОТВЕТ

- ✓ Нарушение цепочек APT атак, выявляйте заражённых устройств и связанных с ними пользователей
- ✓ Интеграция SIEM на основе правил
- ✓ Интеграция с EDR

ВЛИЯНИЕ НА БИЗНЕС

- ✓ Скорость / экономия времени
- ✓ Экономия затрат
- ✓ Повышение производительности труда сотрудников
- ✓ Операционная эффективность

Making Sense of DNS

О DNSSense

DNSSense начинался как проект классификации доменов.

После разработки динамической инфраструктуры классификации доменов в 2016 году компания стала предоставлять облачную безопасную службу DNS для клиентов корпоративного уровня.

Вскоре DNSSense фокусируется на анализе DNS и продуктах Advanced DNS Visibility для нужд корпоративных сетей.

Сегодня, благодаря трём интегрированным продуктам, DNSSense позволяет своим заказчикам безопасно подключаться к Интернет, предоставляя при этом все данные анализа DNS, необходимые командам SOC.

Delivery Hero · IKEA · Allianz · TURKISH TECHNIC · BURGAN BANK · Emirates NBD · FARMASİ

Опыт

11 лет опыта в области расширенного моделирования искусственного интеллекта, классификации DNS и сотрудничества с глобальными терминами SOC

Интеллект

99% глобальных доменов

5млрд поддоменов обходится регулярно

Категоризация впервые увиденных доменов с SLA **10мин**

800 параметров анализа для каждого домена

Клиенты

10,000 Более 250 корпоративных

- eCommerce
- Медиа
- И другие...

2012

38 Банков используют DNSsense

Сотрудничество с крупными предприятиями и организациями с высоким уровнем риска для управления продуктом

Доверие

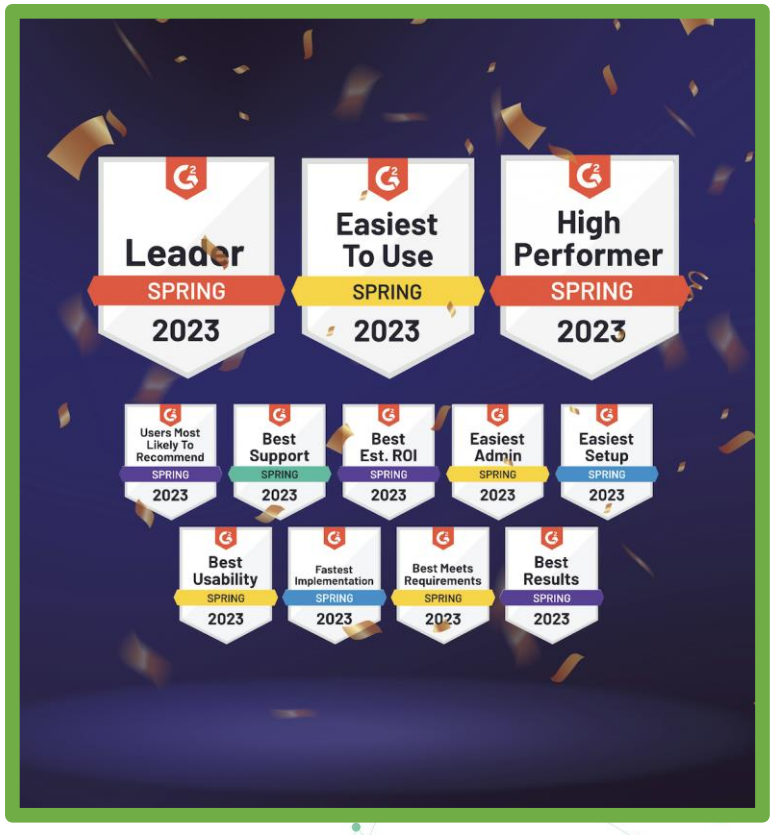
99% Удерживание клиентов

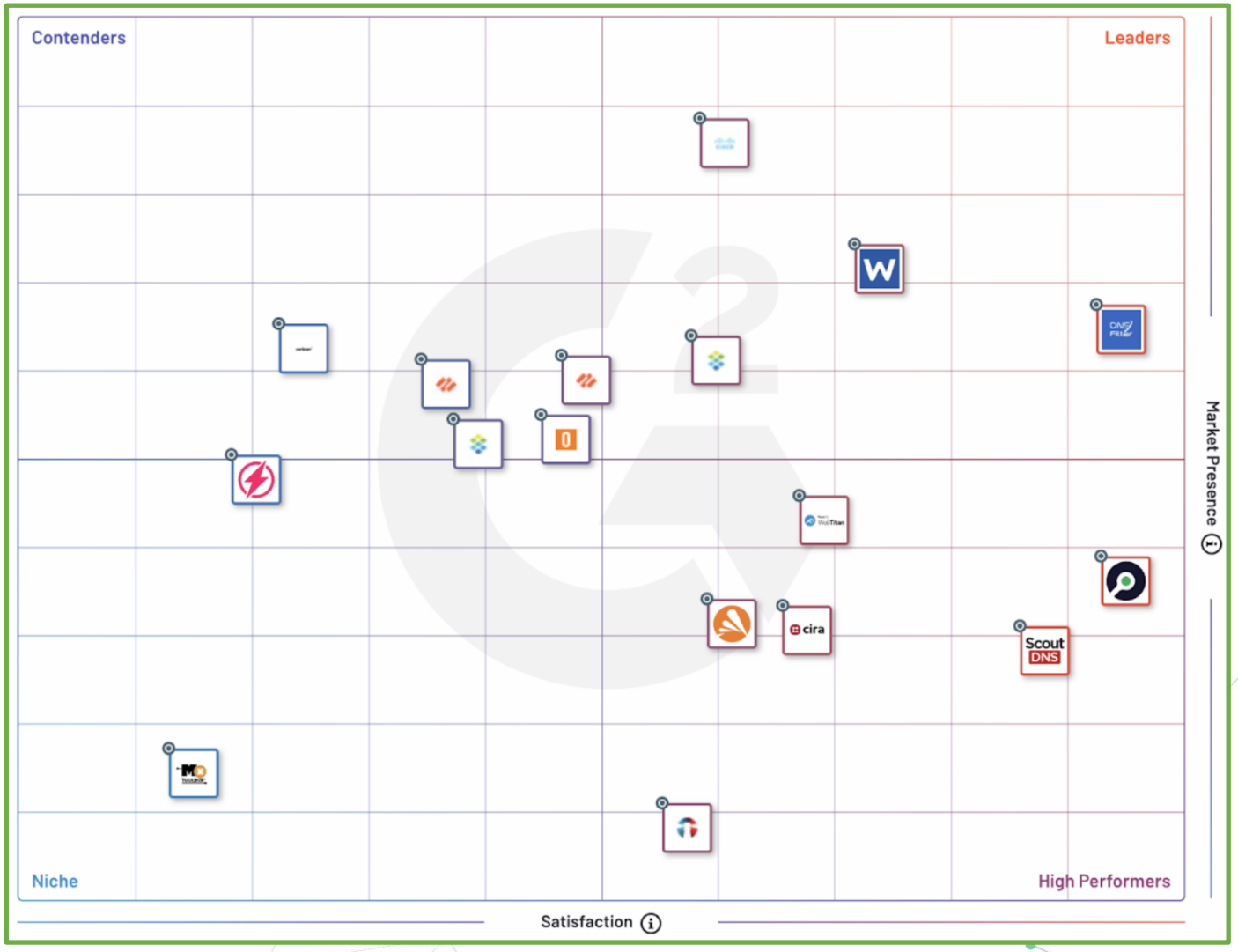
90% конверсия пилотов

Making Sense of DNS

G2 Все продукты

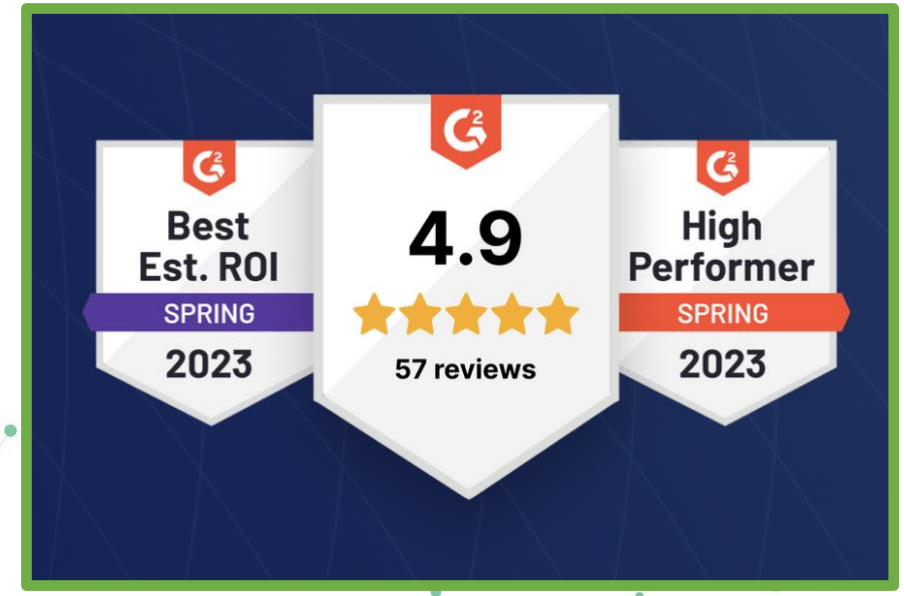
DNS Security

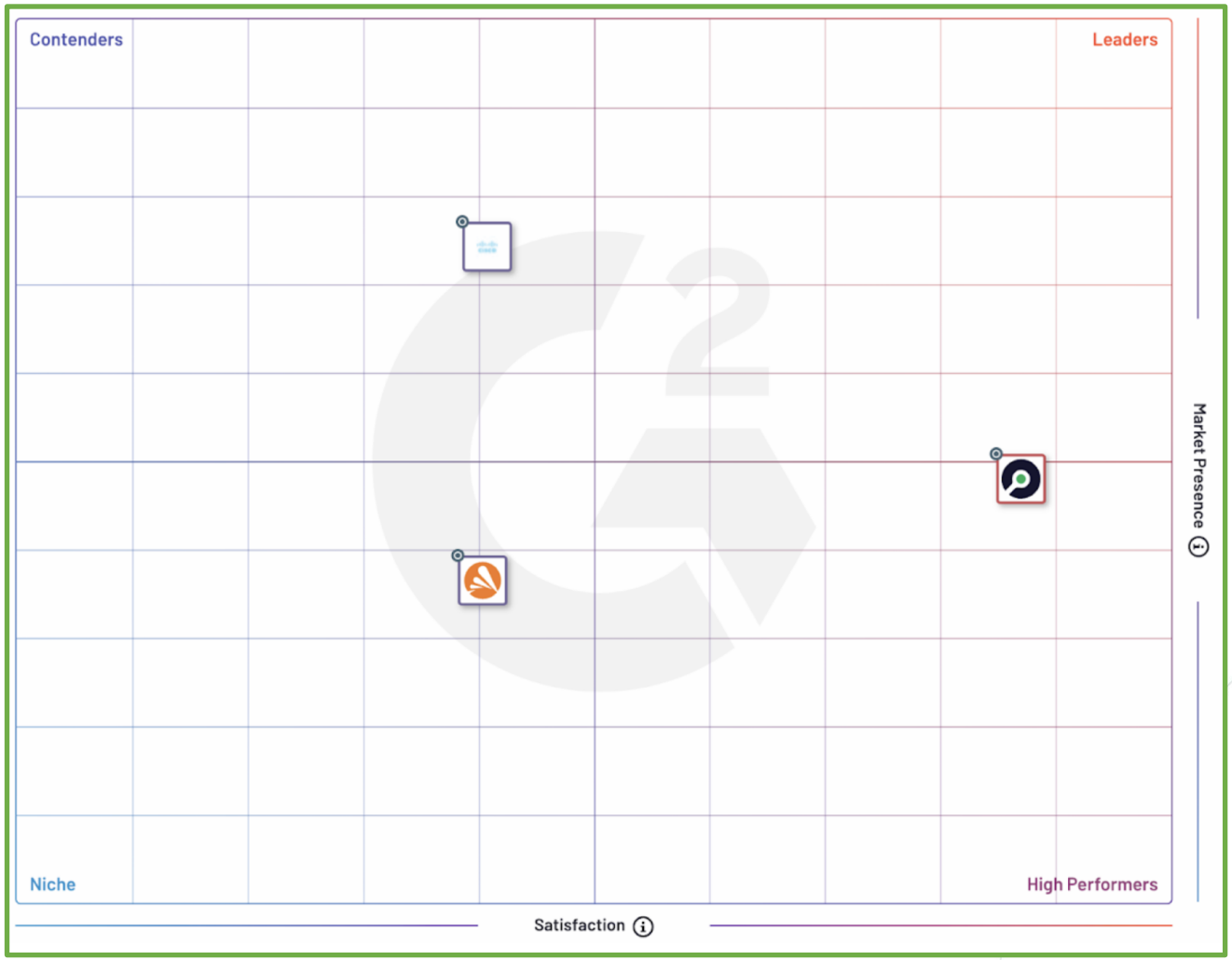




G2 Корпоративный сегмент

Почему мы лучшие в корпоративном сегменте?





Спасибо

Олег Котов, CISSP

oleg.kotov@dnssense.com
+7 916 836 63 68

DNSSense

dnssense.com