DNSSense

The Pioneer of DNS Security

Explore the new frontiers of cybersecurity through next-gen AI-powered DNS detection & response solutions

Solution Brief

dnssense.com

Table of Contents:

» Introduction

DNSSense is the industry-leading provider of the first DNS-focused Detection and Response (DDR 2.0) solution set. Leveraging artificial intelligence and machine learning algorithms, DNSSense unlocks the full potential of the DNS protocol for neutralising the most sophisticated threats at the DNS layer that escape the radar of conventional security controls.

Trusted by over 10,000 companies across 74 countries, DNSSense is leading the global DNS security market by empowering organisations to derive maximum value from their security investments while bridging gaps in their network.

74 countries

10K+companies

1M+ unique users

DNSSense

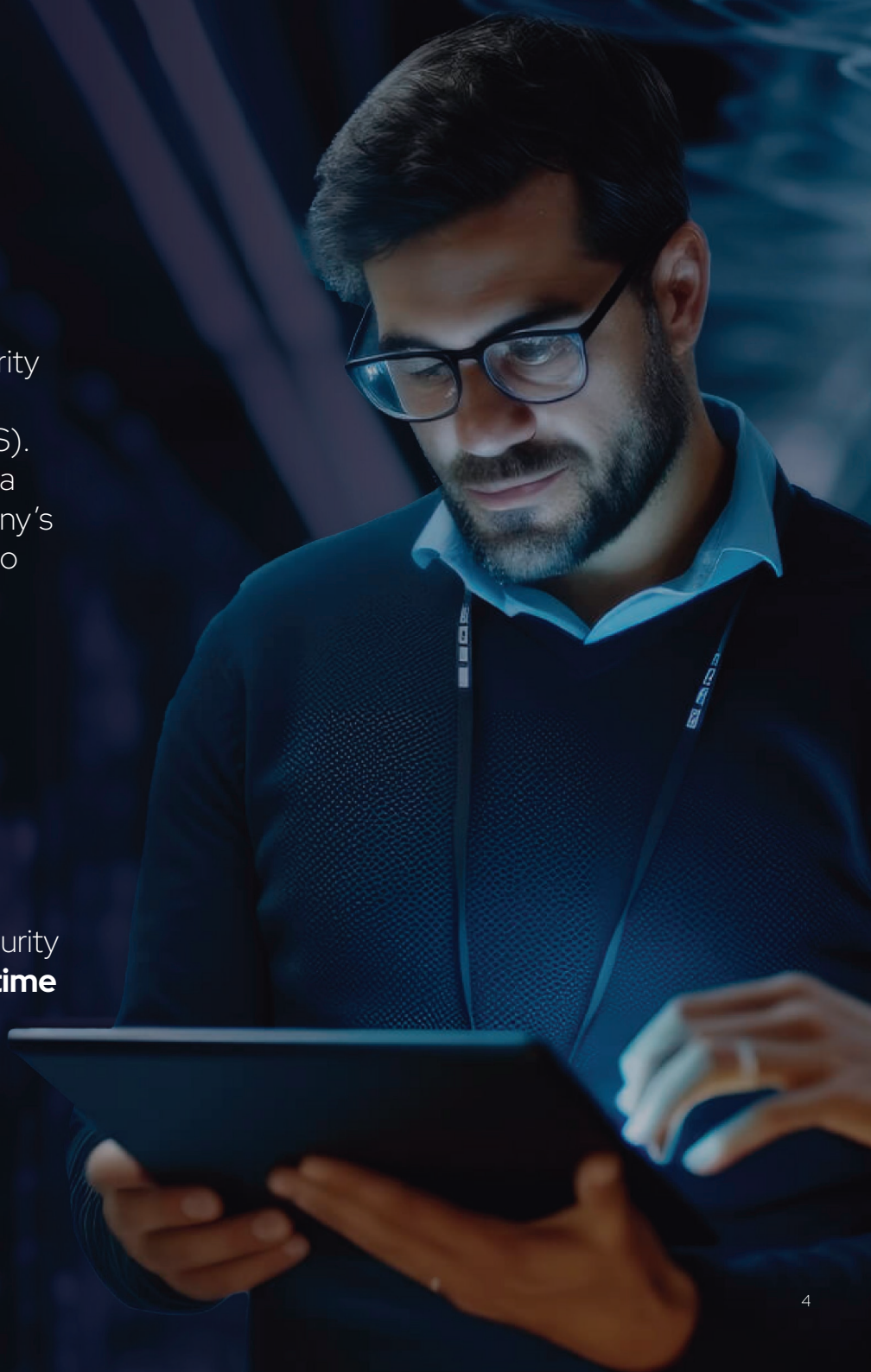
The Pioneer of DNS Security

» What is DDR?

Short for **DNS Detection and Response**, DDR is a cybersecurity approach that focuses on **proactive** monitoring, analysis, and response to threats that exploit the Domain Name System (DNS). DNS is a fundamental building block of the Internet, containing a wealth of data. As a result, it serves as a gateway into a company's environment, turning it into a **prime target** for threat actors who exploit this protocol for nefarious purposes[1].

» DNSSense DDR 2.0

DNSSense departs from traditional DDR approaches that rely on signature-based detection systems, outdated databases, and time-intensive manual processes. With its plug-and-play solutions, DNSSense streamlines security operations through **automated incident response** and intelligent data enrichment. It equips security officers with **traffic anomaly** investigation capabilities and **real-time domain insights**, shielding the security and integrity of their network infrastructure while enabling them to enhance the cyber defence maturity of their organisations.



1- For a more comprehensive analysis of the various methods by which DNS can be exploited as an attack vector, please consult our guidebook on integrating the MITRE ATT&CK framework into DNS security controls available at https://www.dnssense.com/reports/mitre-att-ck-framework

» DDR 2.0 Highlighted Features

DNSDome

It provides advanced-level protection against known and unknown threats.

- Cloud-Based Protection
- AI-Based DNS Tunneling Protection
- Malware-Ransomware-Phishing Protection
- Roaming Client
- XDR Integration via DNSEye
- SOAR Integration

DNSEye

It enables making sense of DNS logs and matures SOC & MDR teams' strategies.

- Advanced Traffic Anomaly Detection
- Automated Incident Response
- Streamlined Traffic Investigation
- Auto Data Contextualisation
- EDR/XDR Advanced Integration
- Alarm Fatigue Reduction
- Advanced Learning Mechanism for Action Automation
- Blind Spot Identification

CYBER XRAY

It provides unparalleled domain insights by using AI and ML.

- AI-Based Domain Classification (%100 Automated – In 2 seconds – No human effort)
- Cyber Threat Intelligence
- Tracking and Analysing the Entire Internet

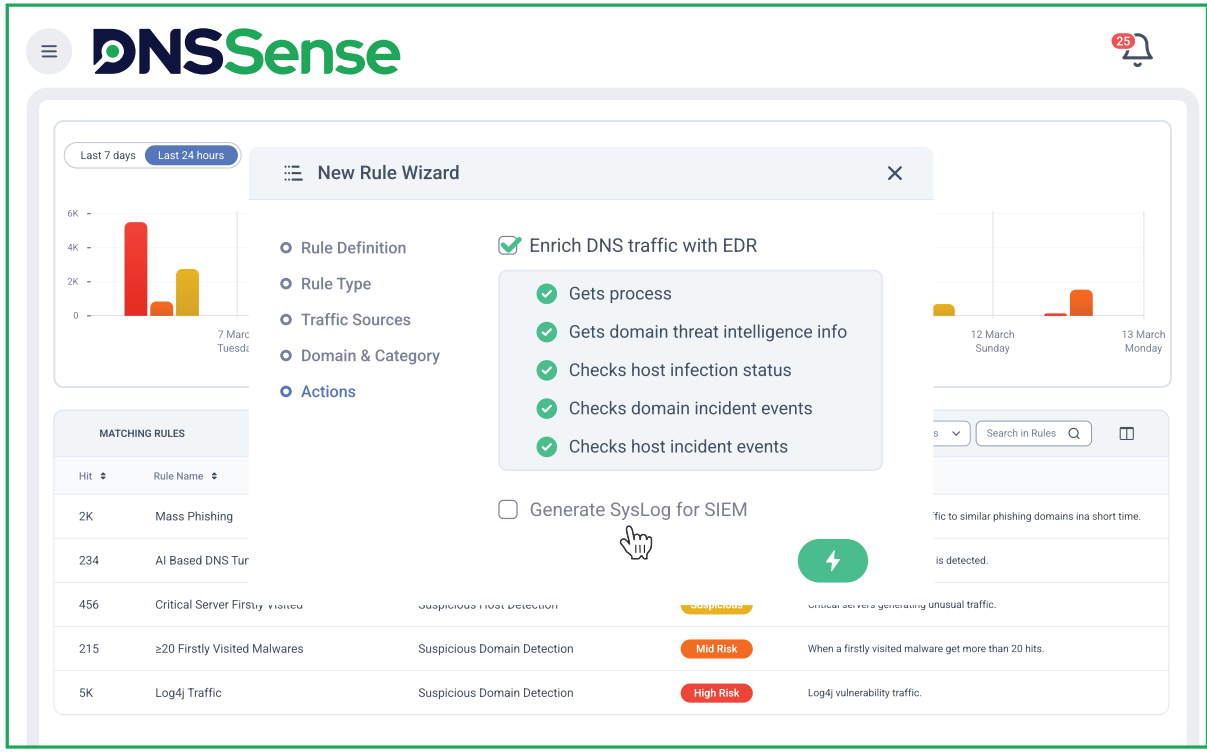
DNSEye

Advanced Traffic Anomaly **Detection** and Analysis

The Pioneer of DNS Security

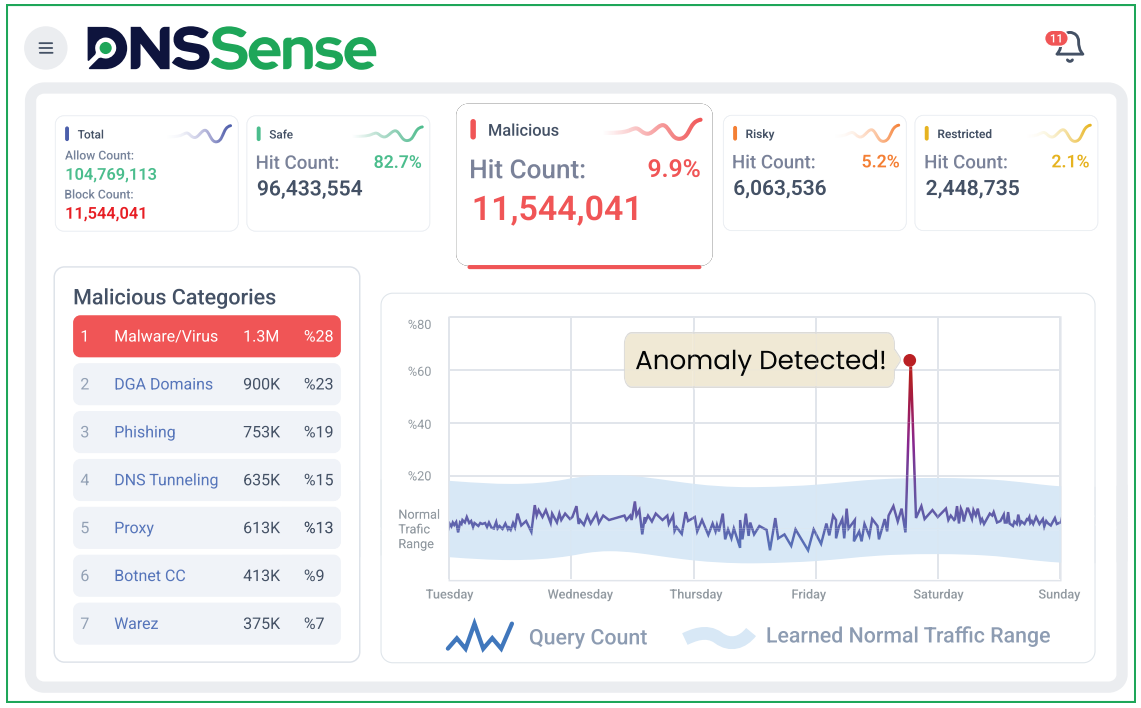
DNSEye is a crucial component of Extended Detection and Response (XDR) frameworks, acting as the first line of defence. Through **automated workflows**, advanced analytics, **data correlation** from multiple endpoints, and real-time domain threat intelligence, DNSEye offers unparalleled cross-layer visibility into previously incomprehensible DNS traffic. Using multiple state-of-the-art AI engines, DNSEye identifies **abnormal DNS patterns** indicative of malicious activity, enabling organisations to act on threats earlier in the kill chain.

DNSEye propels **SOC and MDR teams'** efficiency to new heights by contextualising DNS traffic with telemetry from Cyber X-Ray and DHCP, SIEM, and IAM platforms for automated discovery, attribution, and enhanced threat-hunting capabilities.



DNSDome

AI-Powered Defence & **Response** Across the Network



DNSDome is a protective cloud-based DNS service that provides **real-time protection** and response to the most sophisticated DNS-backed cyberattacks.

DNSDome harnesses insights from Cyber X-Ray's AI-based domain intelligence and DNSEye's unique reports to prevent **hard-to-detect tunneling attacks**.

Simple to implement yet highly effective, DNSDome safeguards all devices against a wide range of threats, including **ransomware**, **spam**, **phishing**, **malware**, and **zero-day attacks**.

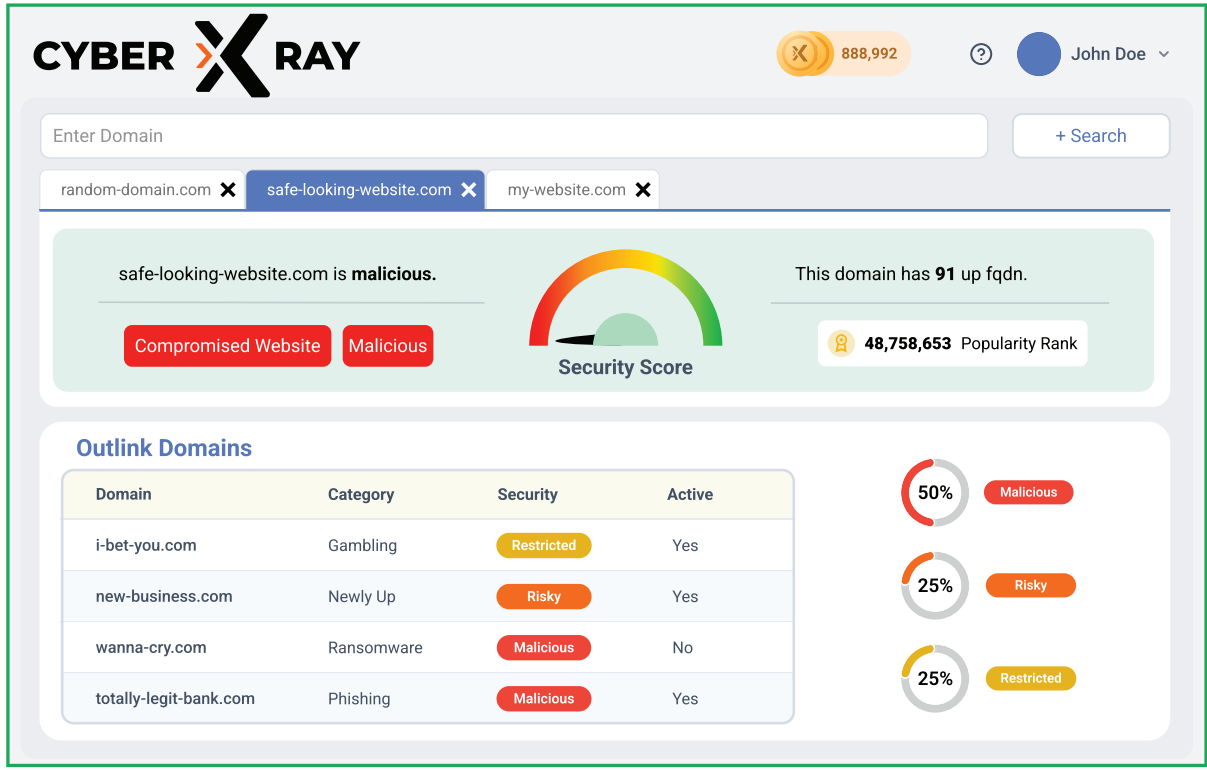
CYBER X RAY

World's Best Domain **Threat Intelligence** and **Classification** Service

The Pioneer of DNS Security

Built on proprietary technology, Cyber X-Ray is the world's best **AI-powered cyber threat intelligence** and forms the core of DNSSense's groundbreaking DDR 2.0 approach. It conducts **daily scans** of all Internet domains, storing and analysing hundreds of data points for each domain and subdomain. This combination of AI- and data-driven methods enables an unparalleled level of insight into every DNS query.

Rather than merely determining safe and malicious domains, Cyber X-Ray has the ability to instantly deliver **specific domain intelligence** on demand to DDR 2.0 solutions, enabling them to detect the most sophisticated cyber threats.



» DDR 2.0 in Numbers

90x

Less Strain

Lightning-fast deployments 90 times quicker than standard SIEMs.

80%

Less Dwell Time

Supercharge your cybersecurity efficiency with 80% faster incident detection.

99%

Savings on SIEM Costs

Slash DNS log-processing costs by an incredible 99%.

99%

Enhanced Data Correlation

Achieve a 99% surge in your SIEM correlation rule performance.

100%

DNS Layer Data Loss Prevention

Data loss worries are no more with our flawless prevention success rate.

60%

Less Log Forwarding

Cut down your XDR-SIEM log forwarding volume by 60% and simplify analysis.

» Signature-based Detection Systems Are Insufficient for Proactive Threat Response

Signature-based detection is a widely used approach for identifying malicious activity by comparing network traffic to **known signatures** or patterns. However, this method has limitations in detecting indicators of compromise (IOCs) for emerging threats that have never been seen before. This challenge is particularly pronounced when infected hosts attempt to connect to **inactive** or **abandoned** command-and-control servers to receive further instructions and payloads.

To address this problem effectively, it is crucial to complement signature-based detections with products that offer insights into **traffic behavior**, enabling a more contextual understanding of potential threats.

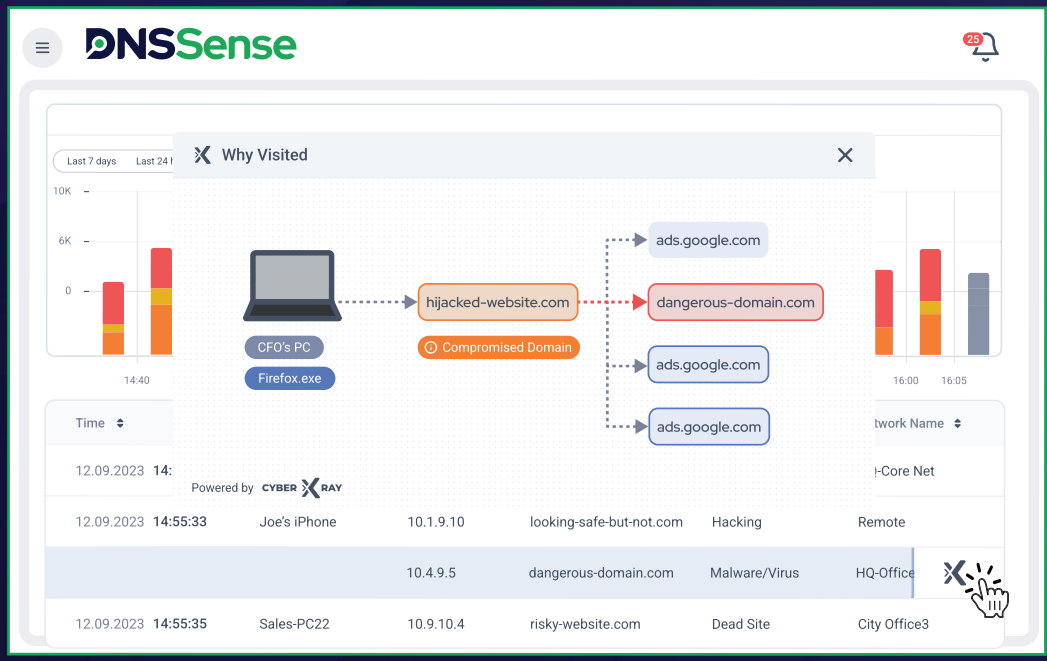
» DNSSense's Solution:

Traffic Investigation

A DNSEye Feature

DNSSense departs from traditional pattern recognition technologies by leveraging **artificial intelligence** and machine learning algorithms to detect the slightest **deviations** from normal DNS traffic distributions. This AI-driven approach, in conjunction with the most up-to-date security telemetry of internet assets from Cyber X-Ray, ensures unparalleled precision in detecting both well-established and previously **unknown threats** such as novel zero-day exploits.

Built into the "Traffic Investigation" module, the "**Why Visited**" feature possesses the remarkable ability to see beyond the surface, revealing the **actual paths** to compromised websites and unauthorised traffic redirections. it can also differentiate between voluntary and involuntary DNS requests made by users, while delivering crucial process information such as the **responsible users** or **applications** generating malicious traffic, as well as the initiation time, spread, and recurrence.



Basic DNS Tunneling Attacks Are Easy to Prevent, But What About Sophisticated Ones?

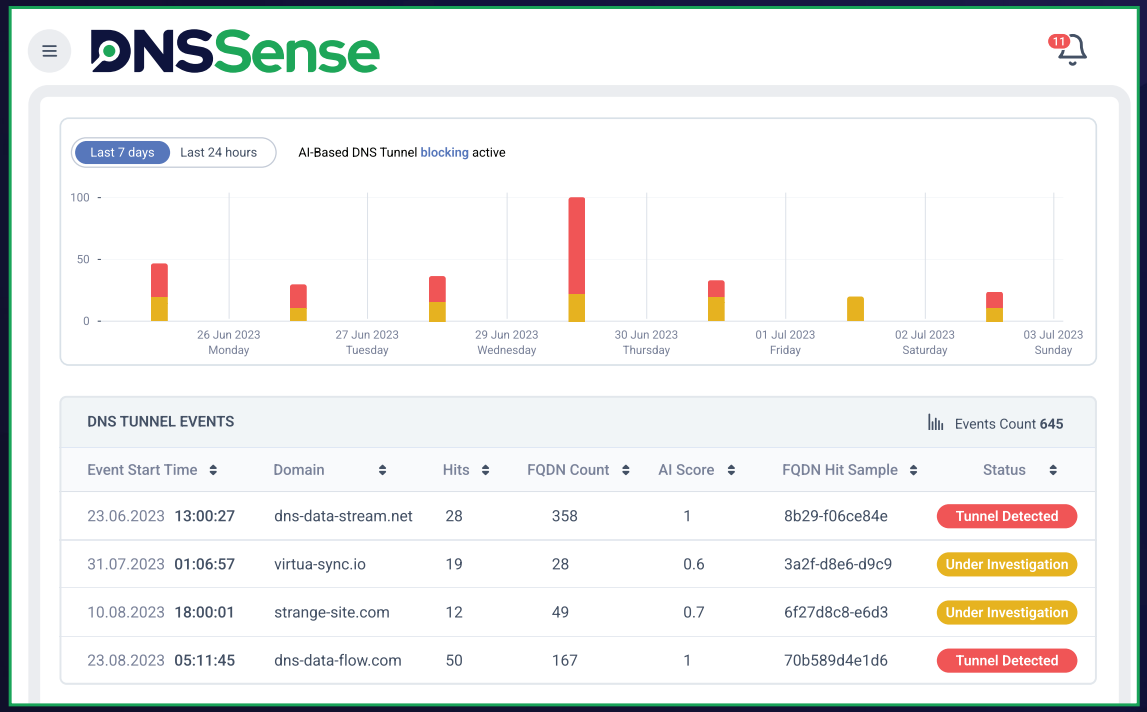
DNS traffic is not only extensive but also requires speed to function properly. Tracking thousands of queries per second presents a monumental challenge for cybersecurity, providing adversaries with opportunities to embed **concealed malicious data** within legitimate DNS traffic. This compromises network security and paves the way for data exfiltration and tunneling attempts through DNS queries.

Despite the market being flooded with vendors claiming to prevent **DNS data exfiltration**, evading these systems is surprisingly easy as they rely on pattern recognition technologies. Attackers can use basic DNS exfiltration tools with unique patterns and generate "**noise**" by making queries to legitimate websites to **blend in** with regular network traffic, making detection very difficult.

» DNSSense's Solution:

AI-based DNS Tunnel Defence

A DNSDome Feature



DNSSense's revolutionary DDR 2.0 technology combines AI-based and data-driven detection techniques to detect DNS traffic anomalies across multiple dimensions by correlating data from the responsible process to the **historical analysis** of target domains. This robust system enables the identification and prevention of even the most elusive DNS tunneling attacks including **ultra-slow DNS tunneling** that could persist for up to two years to transfer a mere 2MB of data.

» Manual Incident Response:
An Impractical and Drawback-Ridden Approach

As infrastructures and networks continue to expand, organisations are confronted with the daunting task of effectively managing and making sense of growing volumes of data. Manual security alert management presents significant limitations, including reliance on **human judgment**, heightened **risk of errors**, absence of standardised and **consistent response protocols**, delayed detection, prolonged downtime, and potential disruptions to operations in the event of successful attacks. These challenges underscore the need for **automated alternatives** that can ensure timely mitigation of security incidents without overwhelming the available resources.

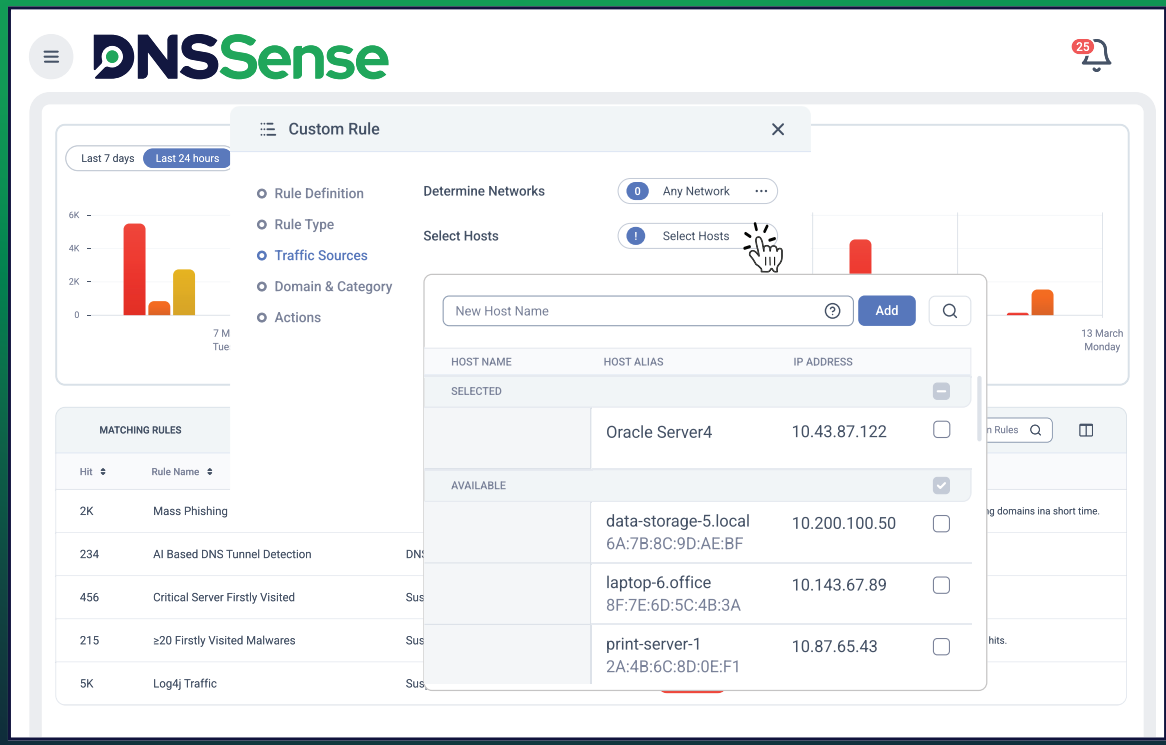
» DNSSense's Solution:

Security Incidents

A DNSEye Feature

DNSSense's "**Security Incidents**" module alleviates the weight of manual incident response, providing organisations with **real-time automated response capabilities.** By seamlessly integrating advanced analytics and aggregated intelligence feeds from Cyber X-Ray and other endpoints, it streamlines SOC/MDR services and automates workflows, enabling the most comprehensive analysis of DNS traffic.

"Security Incidents" goes beyond being a mere warning system and enables organisations to stay ahead of obscure DNS tunneling attempts and newly emerging cyber-attacks. With the ability to **define easily customisable incident scenarios** tailored to the unique needs of each organisation, the module ensures heightened security for critical devices.



» A Secure Corporate Ecosystem Requires a Zero-Trust Approach

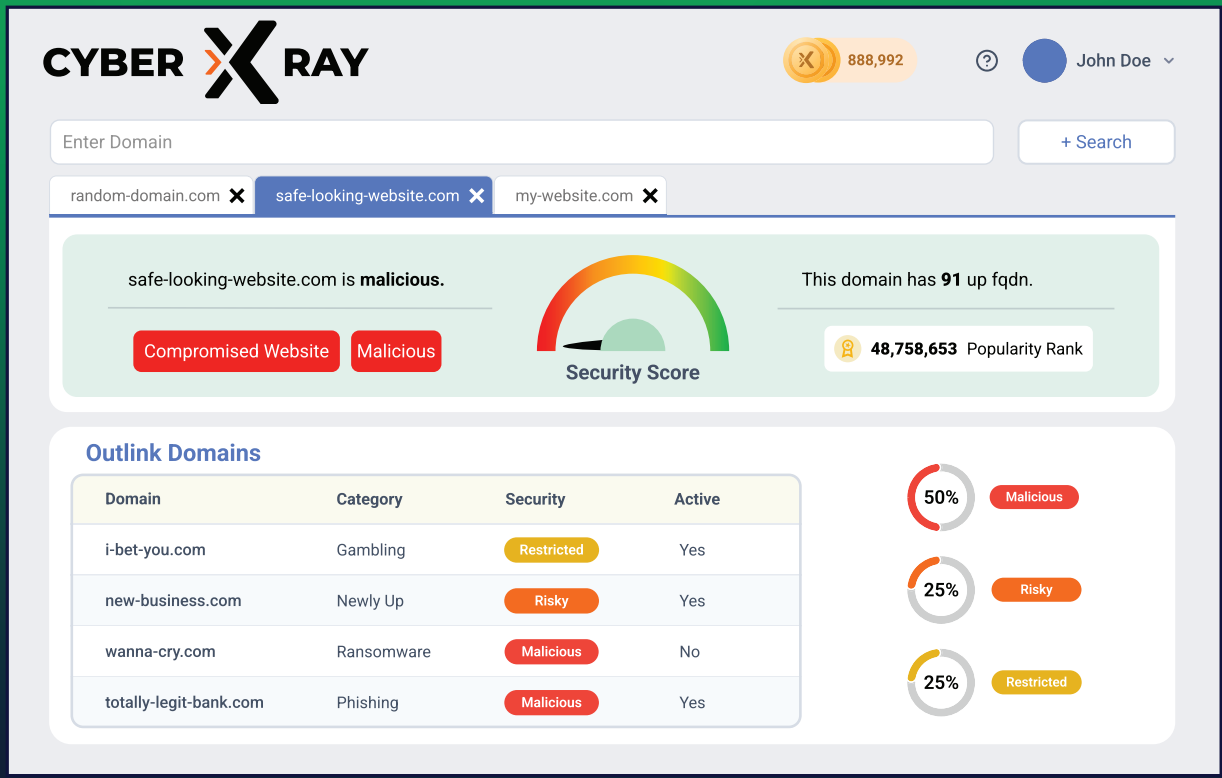
Every day, a large number of safe websites become victims of **unauthorised control** by malicious actors. These instances range from seemingly harmless **SEO hijacks** to **targeted attacks** on unsuspecting individuals, posing substantial risks to corporate assets. While these websites are commonly categorised as "Compromised Websites" within the Malicious category, it is crucial to recognise that **involuntary DNS requests** can also originate from trusted and reputable websites.

» DNSSense's Solution:

Zero-Trust Domain Classification

A Cyber X-Ray Feature

With Cyber X-Ray's Zero-Trust approach to domain classification, connection attempts to **Risky domains**, including **dead sites**, **parked domains**, as well as **Firstly Seen** and **Newly Registered** domains will trigger an immediate reclassification protocol. This process enables Cyber X-Ray to promptly identify even those websites that may appear benign on the surface but have actually been compromised or recently engaged in malicious activities.



» Raw DNS Logs Are Vast, Disperse and Difficult to Interpret

DNS traffic analysis is essential for identifying elusive threats, yet the collection and processing of logs present significant challenges. This is partly because DNS logs are generated across an organisation's infrastructure, making the task of gathering them from **diverse** and **dispersed sources** particularly challenging.

Another contributing factor is the sheer **volume** of logs, coupled with their varying **types** and **formats**, which further complicates parsing and processing them.

» DNSSense's Solution:

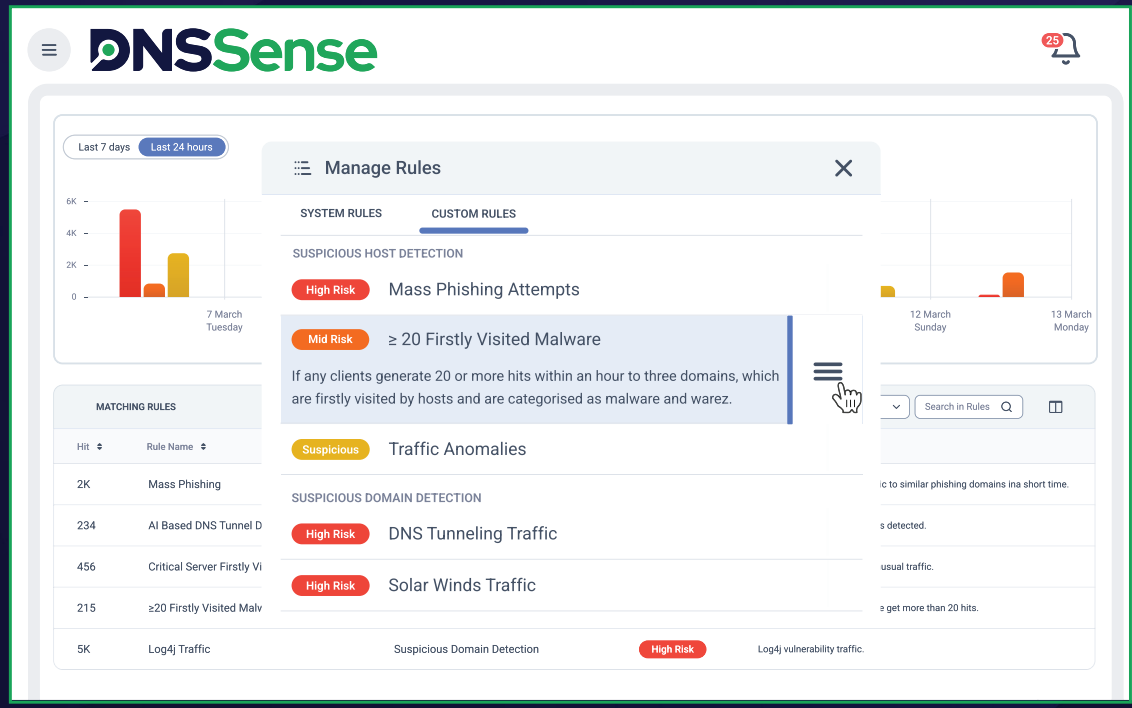
Intelligent Automated Log Collection & Seamless Integrations

A DNSEye Feature

The Pioneer of DNS Security

DNSSense's DDR 2.0 solutions have the ability to **contextualise** DNS traffic with telemetry from Cyber X-Ray and XDR, DHCP, SIEM, and IAM platforms. This **bidirectional enrichment** of DNS logs significantly enhances data correlation and cross-layer visibility, allowing SOC/MDR teams to receive **enriched alerts** for proactive threat detection and response.

By unifying DNS and endpoint data, security officers can streamline workflows and only focus on **relevant actionable insights**, significantly reducing **alarm overload** and **log-processing costs.**



» Defend from Firstly Seen Domains

Malicious domains are typically active for a **short period** before being abandoned, providing only a brief window of time for systems to be compromised.

Knowing that, organisations face the risk of clients establishing connections to domains that may later be identified as malicious.

Next-generation firewalls typically come with a default "any-any" rule, allowing traffic to **flow freely** and leaving organisations vulnerable to novel threats such as zero-day exploits. This is because a typical zero-day attack lasts **312 days** on average before being detected as shown by Bilge & Dumitras' studies.

Given that such attacks can occur at the DNS layer as well, it becomes even more difficult for businesses to discover breaches.

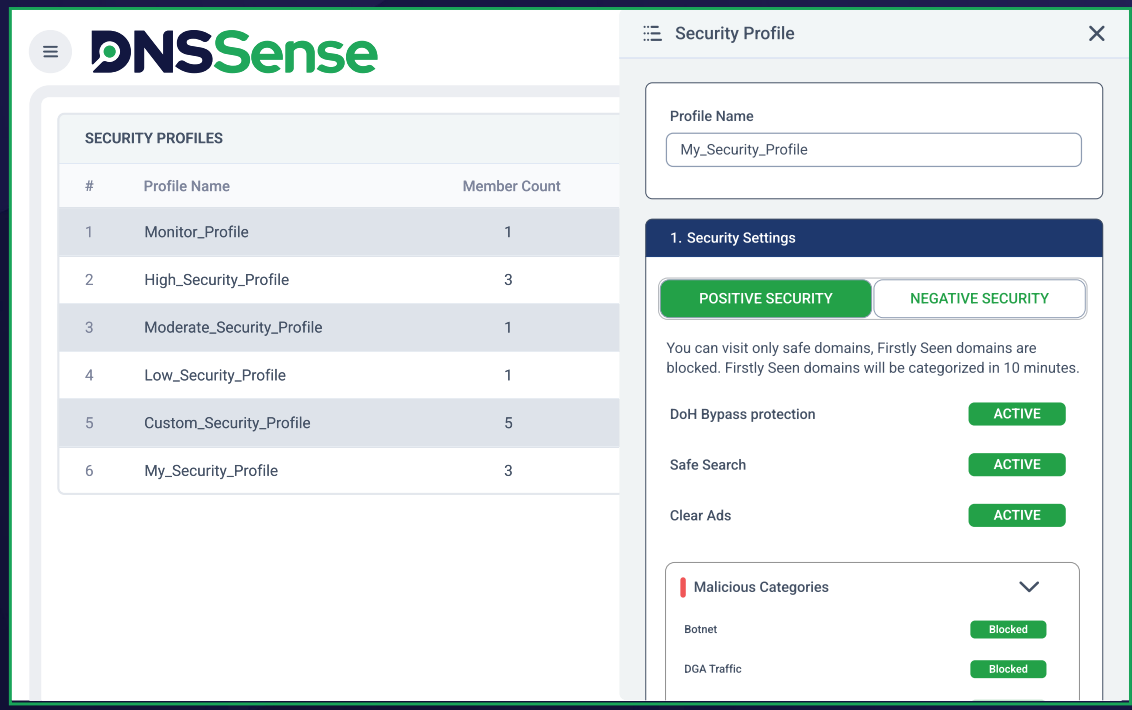
» DNSSense's Solution:

Positive Security Model

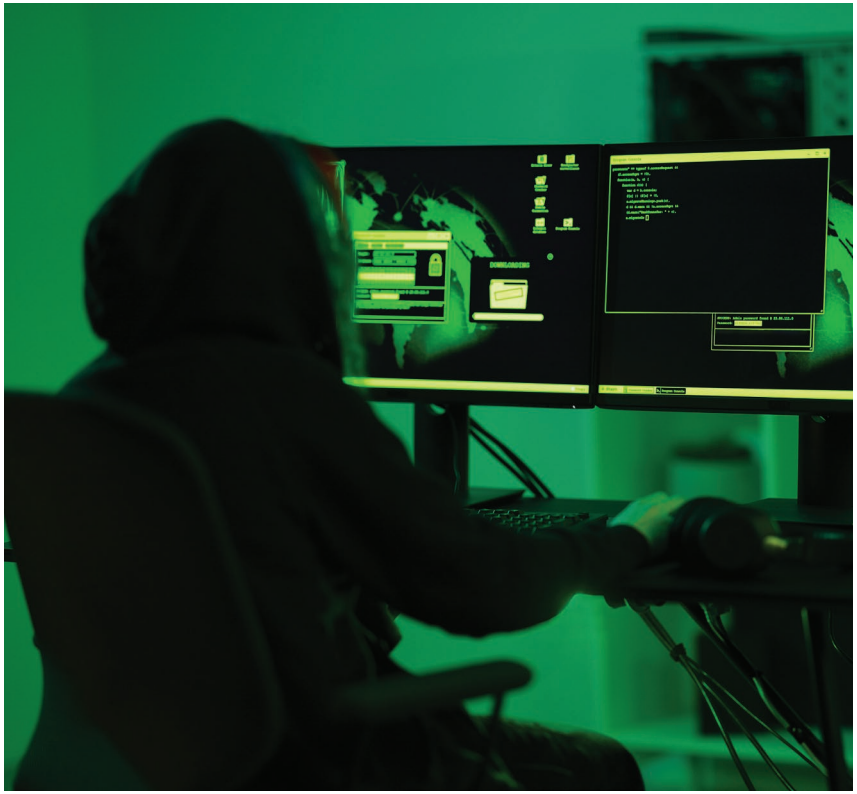
A DNSDome Feature

DNSSense helps establish a more secure posture through the implementation of a Positive Security model. This approach entails granting only the **specific access permissions** defined by users, thereby reducing the **attack surface**.

In cases where a domain is not categorised or falls into a potentially suspicious category, DNSSense takes immediate action by **blocking connection** until they are marked as safe within a matter of minutes, ensuring that any unclassified domains are promptly categorised. This **rapid categorisation** process is a highly effective precautionary measure that guarantees a secure online experience for users without sacrificing connectivity or triggering false positive alerts.



The Pioneer of DNS Security



» Unifying Security Efforts Through the Power of DNS

To address the growing incidents of **cyber-threats**, companies frequently increase their investments in training and technology, employing multiple lines of defence to reduce the risk of compromise.

However, cyber-attacks continue to succeed despite all these efforts. The reality is orchestrating an assorted cybersecurity arsenal across multiple layers can create hidden **security gaps**.

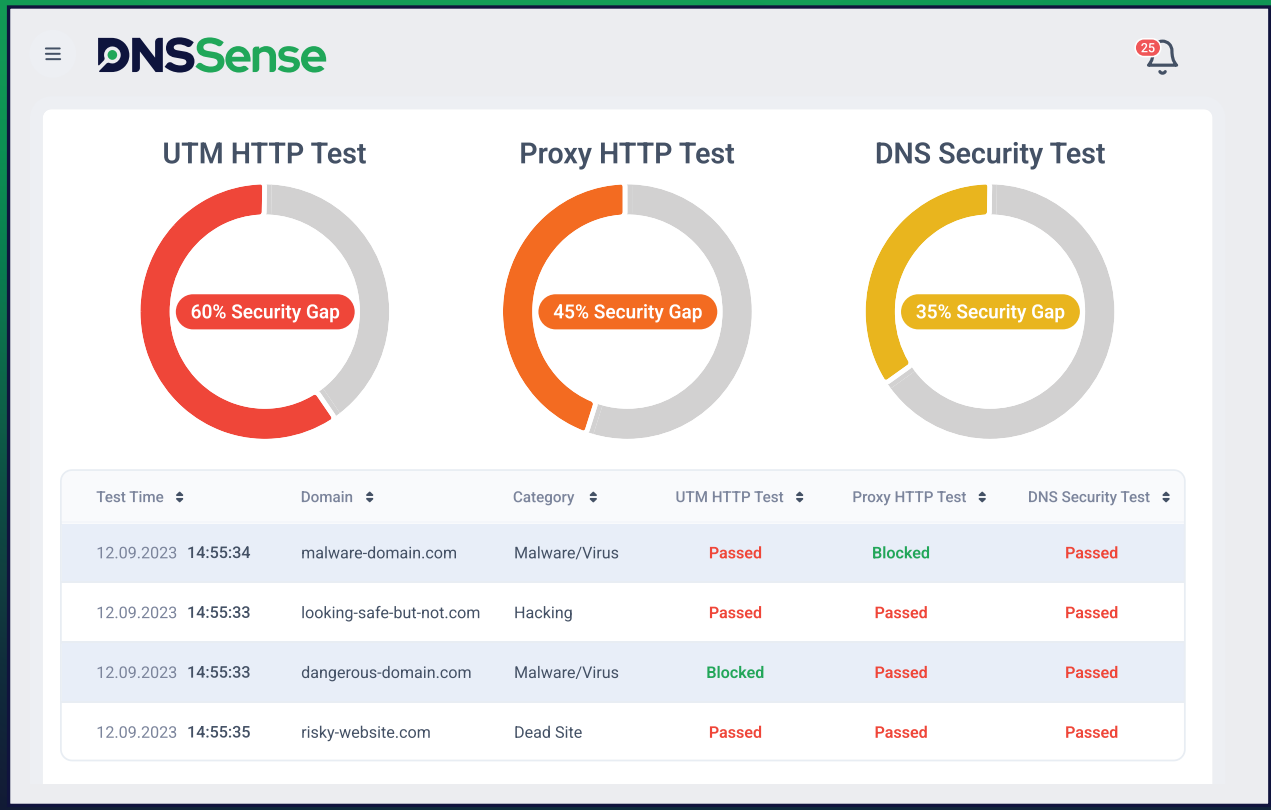
» DNSSense's Solution:

Security Gap Report

A DNSEye Feature

The "Security Gap" module of DNSSense has the unique ability to **simulate connections** to potentially malicious domains to measure the efficiency of existing security controls.

By highlighting the areas that may be liable to threats, **unauthorised access points**, or other security breaches, "Security Gap" enables security teams to **prioritise** security enhancements, **complement** their defence stack, and derive maximum value from their security investments.



» Enhanced Protection for Remote Workers

With more and more employees demanding **flexibility**, employers are caught between balancing the requests for remote working and achieving adequately secured **infrastructure**. Remote working increases the **attack surface** and risk profile of an organisation.

Legacy solutions, such as VPN technology, are both tricky to deploy and **overly permissive**, granting an unnecessary level of privilege and access to the internal network.

Devices outside the corporate network are also less likely to be strictly monitored for the manner of their use and security posture, especially if they are personal devices.

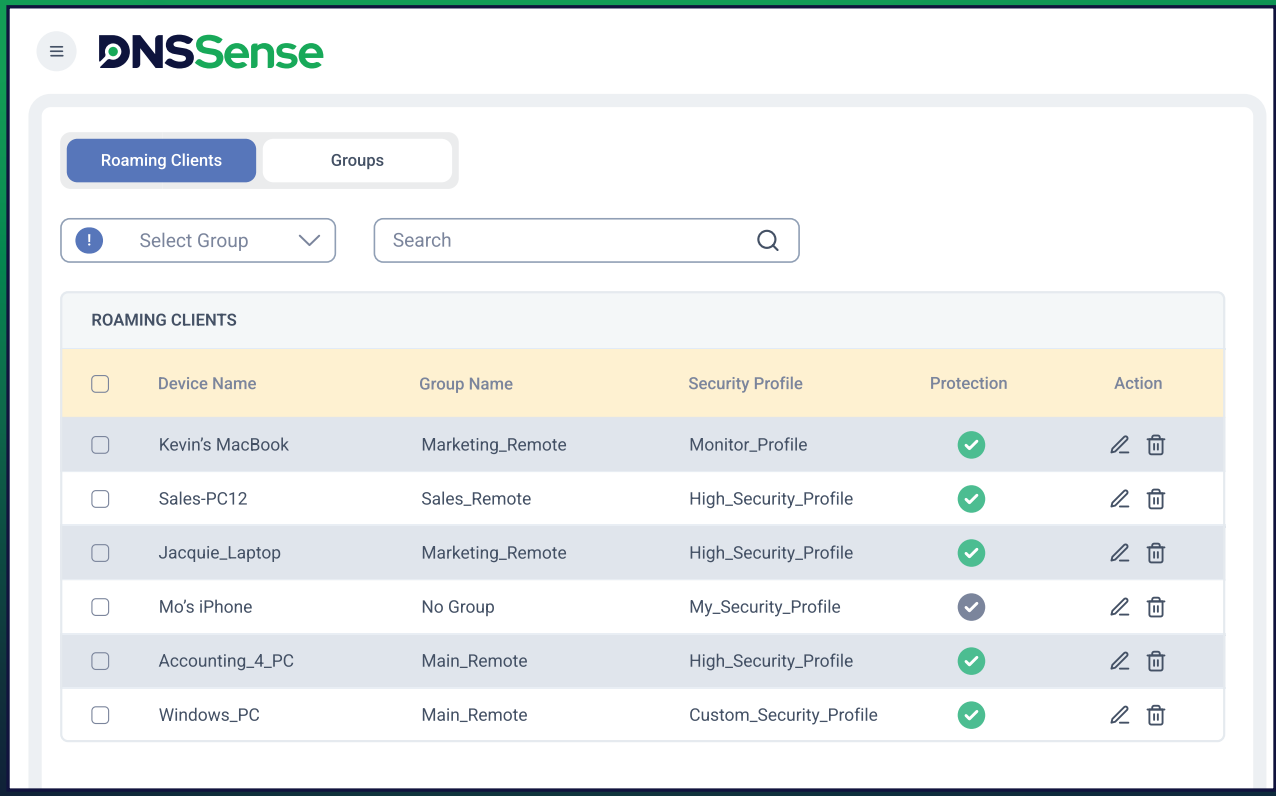
» DNSSense's Solution:

Roaming Clients

A DNSDome Feature

With the "Roaming Clients" module, protection for corporate employees and resources can be easily extended to **remote workers**, ensuring the same level of effective security **regardless** of their **location** or **platform**.

Simple and easy deployment and cross platform support allows security teams to quickly roll out the module, and a tamper proof agent prevents end users from switching off protection.



» DNSSense's Offices:

Türkiye

İstanbul Teknopark Bulvarı No:1
2A Blok Kat:2

+90 216 515 45 99

info@dnssense.com

United Kingdom

London, 338a Regents Park Road,
Office 3 And 4, N3 2LN

+44 (0)203 376 03 30

info@dnssense.com

Kazakhistan

17/1 Al-Farabi Ave., Nurly-Tau
Business Center, 5B, 20th floor

+7 707 341 84 45

info@dnssense.com

South Africa

Rialto Mews, Marigold Cres,
Sandton, 2063, Johannesburg

+27 76 717 4475

info@dnssense.com

Australia

Jubilee Place L 1/470 St Paul
Terrace, Fortitude Valley,
Brisbane QLD

+61 498 190 909

info@dnssense.com

Azerbaijan

49 Fizuli str., «SKS Plaza», Baku,
Azerbaijan, AZ1014

+994502310789

info@dnssense.com

DNSSense is the industry-leading provider of the first DNS-focused Detection & Response (DDR 2.0) solution set. Leveraging artificial intelligence and machine learning algorithms, it makes sense of previously unintelligible DNS traffic and neutralises the most sophisticated threats such as ultra-slow DNS tunneling attempts and unknown backdoors that escape the radar of conventional security controls. Trusted by over 10,000 companies across 74 countries, DNSSense is leading the global DNS security market by bridging security gaps and empowering organisations to derive maximum value from their security investments.

dnssense.com