



Whalebone

# DNS4GOV

ONBOARDING GUIDE

Designed for Cyber Resilience,  
**Built for Public Trust.**

# Index

Executive Summary .....4

FAQ: Am I the right person to be reading this guide? .....5

Whalebone Qualifications .....6

DNS4EU Consortium Partners .....6

What is DNS4GOV .....7

FAQ: What is the difference between DNS4EU and DNS4GOV? .....7

Benefits .....8

    Unified Protection for National Infrastructure.....8

    Instant Results, Zero Heavy Lifting.....8

    Simplified Rollout, Maximum Coverage .....8

    Trusted Infrastructure, Built for Global Impact.....8

    Example of Latency: DNS4EU Public Resolvers Map.....9

    Threat Intelligence MISP Platform.....10

    FAQ: Are there existing best practices for deployment? .....11

Dashboard Preview .....12

    Overview of your DNS traffic .....13

    Security policies .....14

    Device groups.....15

    Overview of threats detected in your DNS traffic .....16

    Example of Key Learnings from PoC.....16

Built to Scale – Supporting Institutions of Any Size.....17

    FAQ: How does Whalebone DNS4GOV compare with other services? .....17

Implementation Standard (Example Allocation of Responsibilities)..... 18

Common Governmental Deployment Scenarios..... 19

    Scenario 1: Overview .....20

    Scenario 2: NCSC managed .....20

    Scenario 3: Hybrid deployment ..... 21

    Scenario 4: National Plan.....21

    Scenario 5: Architecture model .....22

Maturity Levels for Governmental PDNS.....23

    Level 0 – Zero Deployment with No Configuration.....23

    Level 1 – Country–Level PDNS for All Organizations.....24

    Level 2 – Individual UI with Configuration and Reporting .....24

    Level 3 – On–premises DNS Resolvers and Roaming Agents.....25

Onboarding Timeline for DNS4GOV .....26

    Phase 1: Preliminary Steps & Design (1–3 months).....26

    Phase 2: Initial Rollout (3–6 months).....26

    Phase 3: Full–Scale Implementation (3–6 months).....26

Financial & Operational Considerations.....27


Next Steps .....27

Resources: Whalebone DNS4GOV Team.....27



# Executive Summary

Whalebone DNS4GOV is purpose-built to meet the evolving cybersecurity needs of government and public institutions – providing trusted protection, aiding regulatory compliance, and reinforcing infrastructure resilience from the ground up.



**This Whalebone DNS4GOV Onboarding Guide is designed to help government and public institutions rapidly deploy a secure, compliant, and privacy-preserving DNS solution.**

Built according to EU cybersecurity mandates in alignment with the European Union's DNS4EU program (for which Whalebone has served as Consortium Leader), Whalebone DNS4GOV provides critical protection against phishing, malware, and command-and-control threats – at the DNS layer.

This guide offers a step-by-step walkthrough for technical teams and decision-makers alike, helping overcome common adoption challenges such as bureaucratic inertia, political concerns, and complex procurement timelines. Whether your goal is to comply with regulations (such as the NIS2 Directive in Europe), strengthen national digital resilience, or leave a legacy of forward-thinking cybersecurity leadership, Whalebone DNS4GOV – and this guide – aim to help you in those regards. If you are involved in protecting public digital infrastructure, then yes this guide is for you.

# Am I the right person to be reading this guide?

If you are involved in protecting public digital infrastructure, then yes this guide is for you.

As DNS security is still an emerging layer in cybersecurity, implementing it can require a shift in mindset, particularly within government and public institutions. Whether you are a cybersecurity analyst, IT administrator, technical lead, or

decision-maker responsible for digital protection or regulatory compliance – and evaluating, implementing, or scaling security solutions for your institution – then this guide is designed to support your role.

“We needed a solution that can catch, for example, phishing campaigns mimicking a local bank or authentication service.”

**Guillaume-Jean Herbiet,**  
Ju Service Technical Manager at **Restena**



# Whalebone Qualifications

Approaching 10 years in business, Whalebone strives to be a cybersecurity market leader focused on protective DNS solutions.



The company has received multiple accolades highlighting its leadership in DNS security and commitment to protecting critical IT infrastructure, including being ranked by Deloitte among the **50 fastest-growing companies in Central Europe** and receiving a 2024 CyberSecurity Breakthrough Award for “Web Filtering & Control Solution of the Year.”

As **Consortium Leader for the DNS4EU program**, Whalebone was the only vendor selected by the European Commission for providing Protective DNS for the security, privacy, and sovereignty for organizations within the European Union. **Additionally, it is the market leader among telecommunications services providers.**

## DNS4EU Consortium Partners



Project Leader      cz Whalebone, s.r.o.	
<b>Consortium members</b> <ul style="list-style-type: none"><li>• cz CZ.NIC</li><li>• cz Czech Technical University Prague</li><li>• BE Time.lex</li><li>• DE deSEC</li><li>• HU Sztaki</li><li>• IT ABI Lab Centro di Ricerca e Innovazione per la Banca</li><li>• PL Naukowa i Akademicka Sieć Komputerowa</li><li>• RO Directoratul National de Securitate Cibernetică</li></ul>	<b>Associated partners</b> <ul style="list-style-type: none"><li>• BG Ministry of Electronic Governance</li><li>• cz CESNET</li><li>• FI F-Secure</li><li>• PT Centro Nacional de Cibersegurança</li></ul>

# What is DNS4GOV

DNS4GOV is a government-oriented solution such as those spearheaded by the UK, USA, Canada, and Australia, and is designed for implementing **large-scale protection for Government/Public institutions, their employees, and the citizens for which they provide services.**

It delivers state-of-the-art **Protective DNS (PDNS)** capabilities tailored for government and public sector organizations, such as municipalities, healthcare systems, educational institutions, and other government services.

Using advanced DNS filtering and monitoring, it proactively **prevents data breaches, blocks malicious IPs, defends against ransomware, and alerts you to DNS tunneling attacks.**

The service incorporates Whalebone's unique regional threat intelligence capabilities (with a TI exchange network developed for the European Union's DNS4EU program) and supports a Zero Trust DNS (ZTDNS) framework to ensure that **critical infrastructure is protected** from unauthorized connections and DNS spoofing.

Whalebone DNS4GOV requires no additional hardware and **provides centralized DNS policy management**, enabling scalability and secure operations across distributed networks.

Additionally, it assists government and public institutions in achieving compliance with regulatory standards — including NIS2 and other such requirements — by enhancing DNS security, **ensuring policy enforcement, and safeguarding critical infrastructure** against evolving cyber threats.

## FAQ / What is the difference between DNS4EU and DNS4GOV?

DNS4EU is an initiative of the European Union, kicked off when the European Commission appointed Whalebone as the program's Consortium Leader.

DNS4GOV is the PDNS solution that Whalebone developed as part of the DNS4EU program requirements — to align with the requirements of governmental institutions. It is a way for governments to secure, manage, and control data.

# Benefits

Thanks to DNS4EU and its trusted CERT ecosystem, any newly identified threats and attack campaigns are immediately propagated across all DNS4EU resolvers.

This ensures that national CERTs and public institutions benefit from real-time threat intelligence — blocking emerging threats within minutes and preventing their spread across networks.

## Unified Protection for National Infrastructure

DNS4GOV offers a multi-tenant architecture, allowing each government entity or institution to maintain visibility and control over its own protected environment, while being part of a nationally coordinated security consortium. This enables consistent protection across ministries, municipalities, healthcare networks, and more — all under one cohesive shield.

## Instant Results, Zero Heavy Lifting

The out-of-the-box nature of DNS4GOV means no need for costly development, custom integration, or in-house threat hunting. Institutions benefit immediately from Whalebone's unparalleled threat intelligence, derived from millions of endpoints, global partners, and the DNS4EU backbone.

## Simplified Rollout, Maximum Coverage

With a centralized deployment model and no per-institution licensing barrier, DNS4GOV is designed to encourage rapid adoption across hundreds or thousands of public bodies — without requiring additional budget or internal staffing. CERTs, digital ministries, or coordinating agencies can easily onboard entire sectors in weeks, not years.

## Trusted Infrastructure, Built for Global Impact

The DNS4EU backbone, shown in the map below, represents a growing network of redundant, privacy-first, and high-availability DNS resolvers deployed across the European Union. Operated by Whalebone under the mandate of the European Commission, these resolvers ensure that DNS traffic is handled securely, compliantly, and without reliance on non-EU jurisdictions.

While this infrastructure was originally developed as part of the DNS4EU program, the framework also powers DNS4GOV, the commercial solution tailored for governments and public sector institutions worldwide.

Wherever your institution operates, you benefit from a platform that is:

- **Backed by EU-grade privacy and data protection standards**
- **Designed to ensure low-latency performance and maximum uptime**
- **Distributed, redundant, and scalable**

This infrastructure is continuously expanding and can be extended or localized to meet specific national requirements as needed.



“We know how DNS can be used for malicious activities and how efficient DNS is to combat them.”

Guillaume-Jean Herbiet,  
.lu Service Technical Manager at Restena



Example of Latency:  
DNS4EU Public Resolvers Map



## Threat Intelligence MISP Platform

As a part of the DNS4EU project, Whalebone operates a Malware Information Sharing Platform (MISP) that connects CERTs to facilitate faster sharing of threat intelligence, creating a unique database of region-specific threats.

It is one of the most comprehensive data sets in existence, as our sources are governments, telecommunications partners, ISPs, educational research institutions, and other cybersecurity partners.

### Industry standard:

- Public and community data sourcing
- Proprietary threat intelligence, threat feed licenses
- Other partnerships, e.g. abuse operators
- In-house research by experienced security experts

### Whalebone’s Threat Intelligence

#### DNS4EU project:

- DNS4EU Consortium
- EU CERTS

#### Telco market leadership:

- Threats to telco & ISP customers provide probes in 40+ countries
- Telco fraud prevention teams
- Telco crowdsourcing

#### Added-value research:

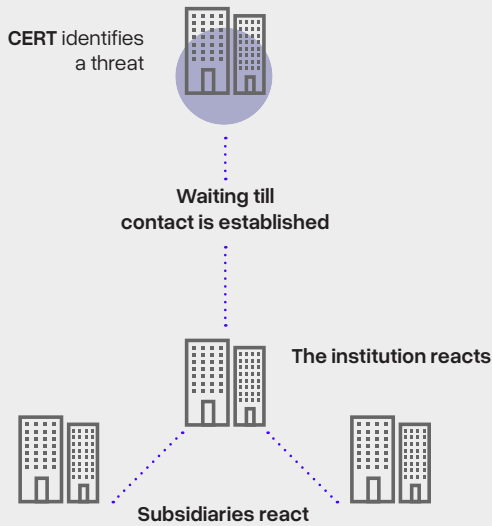
- AI agent for malicious domain prediction and early detection
- R&D with academia (CVUT, NASK)
- Whalebone Virtual Analyst
- Whalebone Tunnel Block
- Dark Web Scouting Team
- Whalebone DGA Sonar

#### Local & Regional Threat Intelligence:

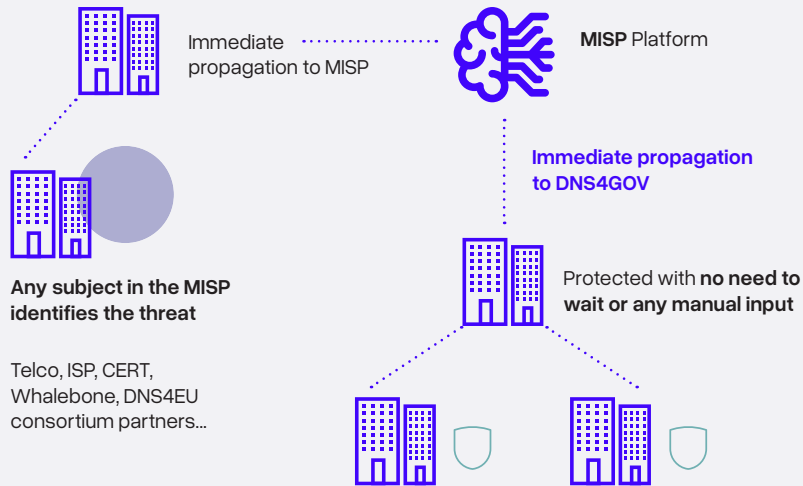
- Research of brands and sectors
- Adversary infrastructure monitoring
- Domain context analysis

- Open-source Threat Intelligence and sharing platform
- Distributed servers that can create, consume or forward TI data about malicious domains, IPs and more
- Any CERT, CSIRT, or commercial subject can run their own instance
- Able to enter many types of threats with context, tags, commentary, and more

How it works now



How it works with



# FAQ / Are there existing best practices for deployment?

Yes, DNS4GOV follows example initiatives in the UK, USA, Australia, and Canada. As of Q2 2025, the following DNS4GOV initiatives are underway:

Onboarding

- 20+ NCSCs in later stages of onboarding cycle
- 8 PoCs with European NCSCs

Threat Intelligence (TI) Sharing

- 17 CERTs in Malware Information Sharing (MISP) TI exchange network
- 40+ Consortium contacts with CERTs across Europe, for both public and private sectors

Ongoing Cooperation

- 50+ Conferences
- 16+ Workshops & webinars
- 800+ Participants reached
- 500+ Stakeholder Community Members

# Dashboard Preview

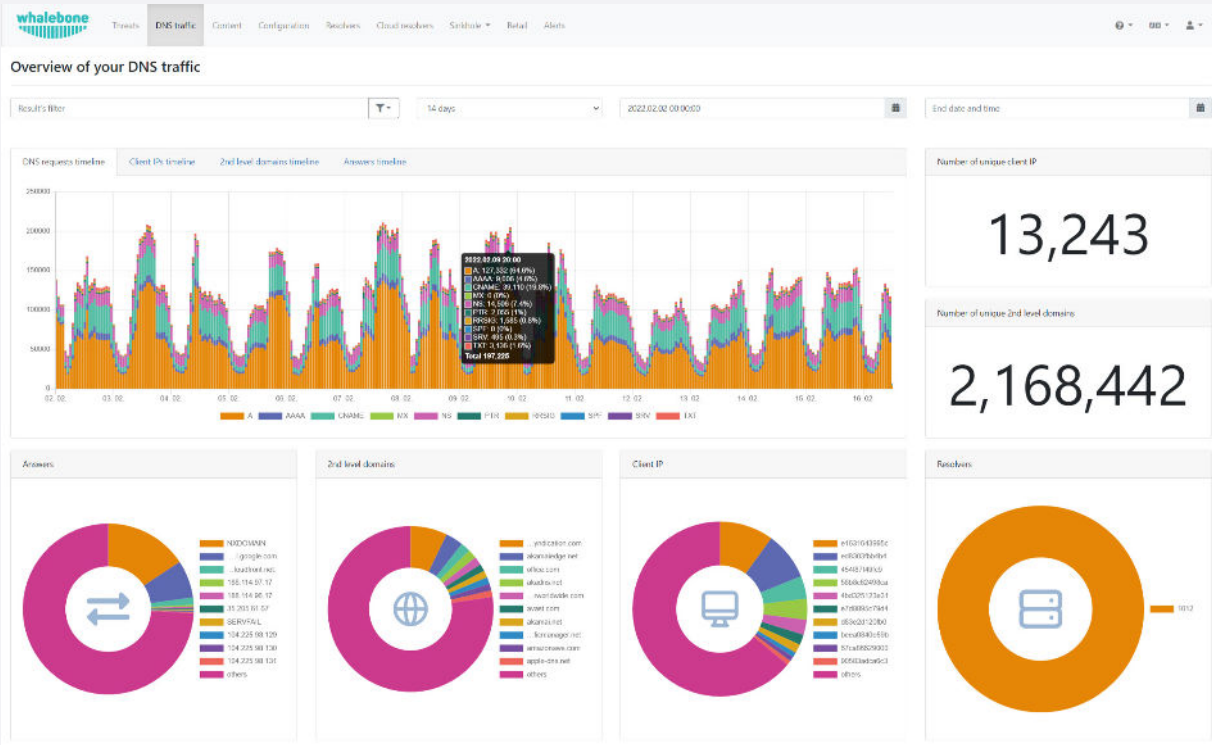
To help you understand what DNS4GOV looks like in practice, we've included several real screenshots from Whalebone's user interface. These dashboards offer visibility into traffic patterns, security enforcement, and device management – making it easy for public sector IT teams to monitor threats, enforce policy, and adapt configurations across complex environments.

**Please note:** the visuals shown reflect the interface at the time of publication and may evolve as the platform continues to improve.

## Overview of your DNS traffic

This dashboard provides visuals of DNS request types over time, highlights trends and patterns in usage across your network, and offers insights such as the number of unique client IPs, second-level domains, and resolution breakdowns by record type. Pie charts help quickly identify top domains, client sources, and resolver activity.

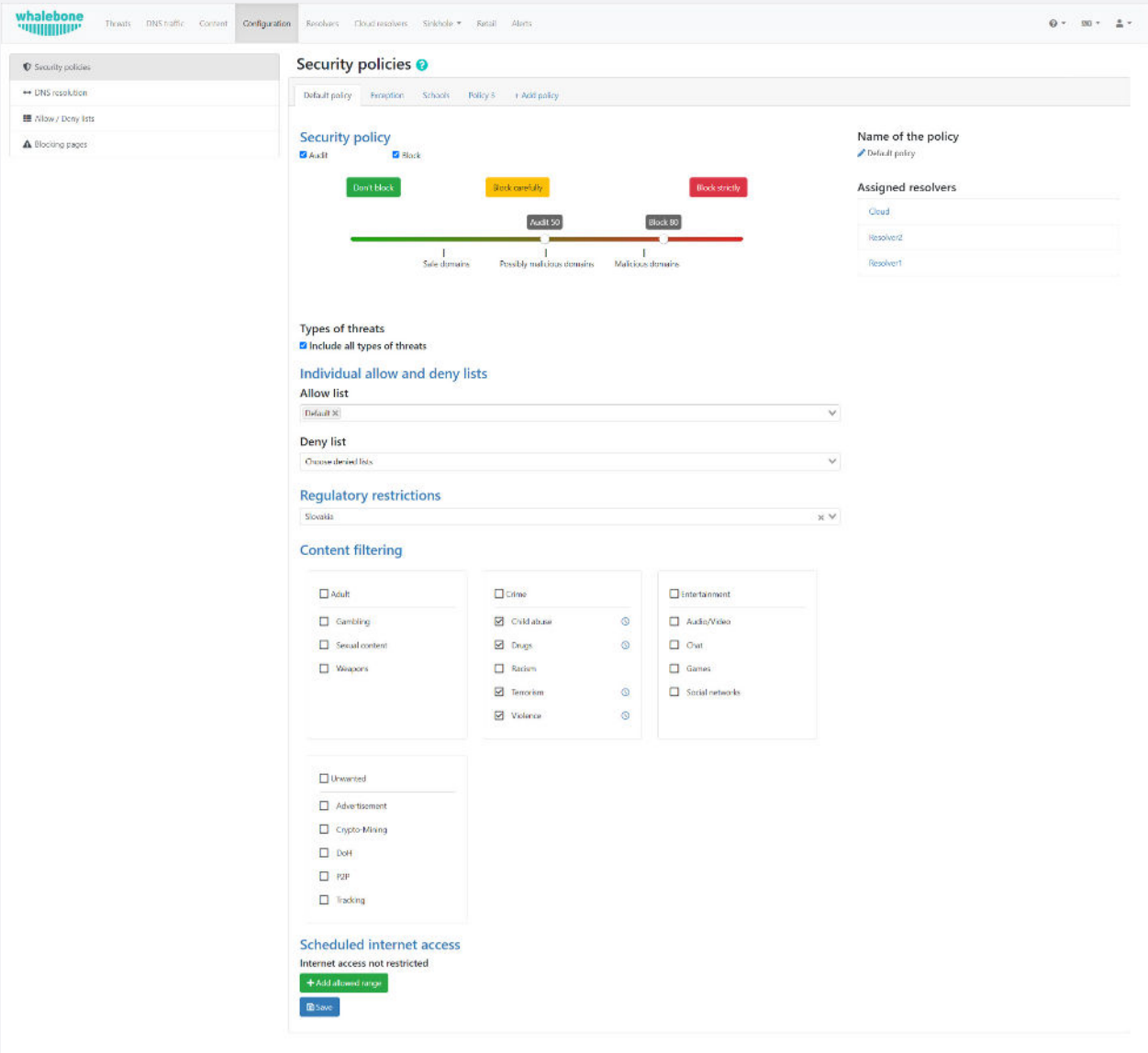
Visualizing DNS activity at a glance helps IT teams detect anomalies, validate normal behavior, and make data-driven decisions about policy and resource allocation.



Security policies

This interface allows administrators to fine-tune DNS protection levels based on threat severity, regulatory needs, and content control. Filters include threat types, allow/deny lists, and regulatory-specific restrictions (e.g., national compliance requirements). Content categories like gambling, adult content, or misinformation can be easily toggled.

Granular control over DNS resolution helps organizations tailor policies to fit national regulations, institutional goals, and specific user groups, while keeping management simple.





Device groups

This panel provides an overview of managed devices, grouped by policies like “Adblocker” or “Default.” Administrators can monitor device status, OS type, and incident history, with the ability to install agents or apply policies across entire groups.

Scalable device management ensures that even large institutions can rapidly apply and adapt DNS protections across thousands of endpoints – including those that are remote or mobile – all while keeping individual configurations aligned with broader security policies.

whalebone

Threats

DNS traffic

Content

Configuration

Resolvers

Cloud resolvers

Sinkhole

Alerts

Device groups

+ Add device group

Adblocker

Number of devices: 4

Security policy: Adblocker

Blocking page: Default

> Install to group

Default

Number of devices: 2

Security policy: Vychazi politika

Blocking page: Default

> Install to group

Devices

<input type="checkbox"/>	Active	Hostname	Group	Agent version	OS	OS version	Network type	Last activity	Incidents (last 30 days)
<input type="checkbox"/>	Yes	samsung SM-G960F	Default	4.7.2	Android	10	External	11 minutes ago	1
<input type="checkbox"/>	Yes	C57b7.8	Adblocker	2.1.2	iOS	15.2.1	External	3 minutes ago	0
<input type="checkbox"/>	Yes		Adblocker	2.1.2	iOS	15.2.1	External	2 minutes ago	31
<input type="checkbox"/>	No	WBRS	Default	2.10.2.0	Windows	6.2.9200	External	2 days ago	2
<input type="checkbox"/>	Yes	Petr's iPhone	Adblocker	2.1.2	iOS	15.3.1	External	2 minutes ago	2
<input type="checkbox"/>	No	samsung SM-A125U	Adblocker	4.7.2	Android	11	External	1 week ago	0

Total 6

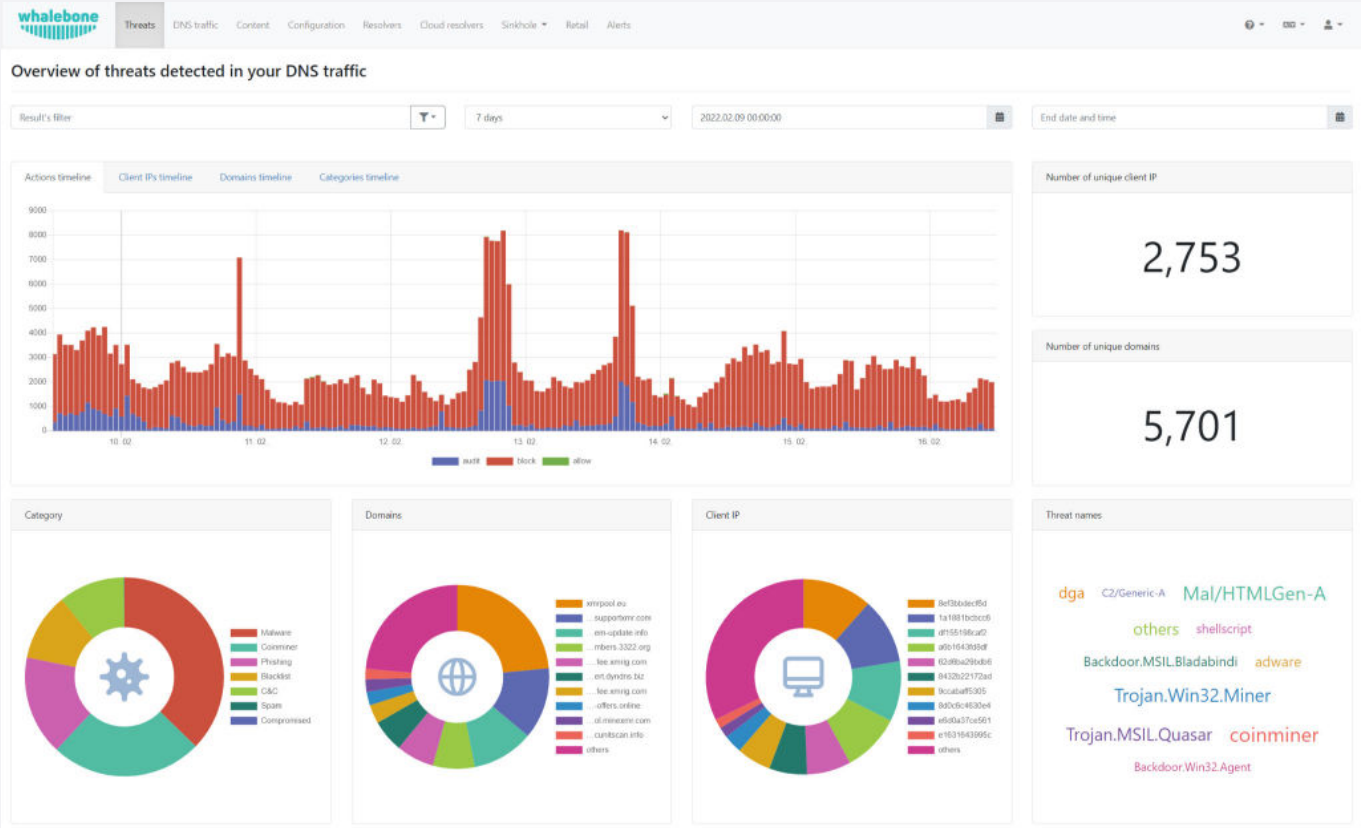
25

1

Overview of threats detected in your DNS traffic

This dashboard presents a detailed summary of threats identified through DNS-layer inspection, typically categorized by threat type (e.g., malware, phishing, botnets, C2 communication), severity, volume, and affected clients or domains. You'll often see trends over time and a breakdown of active incidents, blocked requests, and policy enforcement.

Being able to visualize threat activity in real time enables IT and CERT teams to respond swiftly to emerging attacks, prioritize incident response, and proactively harden their infrastructure. DNS-layer threat intelligence is especially powerful because it blocks malicious domains before a full connection can be established—often neutralizing threats before damage occurs.



Example of Key Learnings from PoC

A well-structured Proof of Concept (PoC) often provides the clearest path toward successful deployment. The example below captures real-world lessons learned during initial DNS4GOV implementations – offering valuable insights into both technical and organizational factors.

These learnings are not exhaustive, nor are they prescriptive. Rather, they are shared to help new adopters anticipate common challenges, recognize quick wins, and align their planning with proven practices. Each government environment is different, but understanding how others have approached onboarding can streamline your own journey and avoid costly missteps.

Key Learnings of PoCs

Malware – Random Domains (Hospital Scenario)

- Number of affected devices
- 4
- Time period
- 10 JUN – 30 JUL
- Number of malicious requests
- 19
- Details
- .xyz, .top, .life, .buzz TLDs – dictionary-generated domains
  - Low count does not indicate a DGA
  - Purpose rotates with whatever the current campaign is – malware/phishing/scam



“We are quite happy that the filtering is highly accurate, and we had relatively few issues with legitimate domains being blocked.”

Guillaume–Jean Herbiet,  
.lu Service Technical Manager at Restena



# Built to Scale

## Supporting Institutions of Any Size

DNS4GOV is designed to scale effortlessly, from protecting a single institution to enabling nationwide adoption. The platform supports onboarding **hundreds or even thousands of public organizations in a short period** of time, with minimal technical overhead or disruption.

Centralized coordination through **ministries, national CERTs, or digital government agencies** can accelerate adoption by offering a unified onboarding process and a shared security baseline.

**Active evangelization by national CERTs** — combined with DNS4GOV's proven integration flexibility — has enabled rapid, coordinated rollouts capabilities across public health systems, municipalities, education networks, and more.

Whether your goal is to secure one ministry or an entire national infrastructure, DNS4GOV's architecture and team are ready to support seamless, phased deployments at any scale.



### Easy scalability

Hundreds or thousands of organizations can be onboarded in a short time. Evangelization from national CERT helps with fast onboarding.

## FAQ / How does Whalebone DNS4GOV compare with other services?

Whalebone DNS4GOV is the only DNS resolver developed under the official DNS4EU initiative, purpose-built for the public sector. Unlike general commercial services, it offers:

- **Regional sovereignty (e.g. in the EU, no data leaves the EU)**
- **Compliance by design (e.g. NIS2 & GDPR in the EU)**
- **No data monetization (privacy is built in)**
- **Tailored deployment options for government IT environments**
- **Dedicated support from teams experienced in public-sector needs**

Not just another DNS filter, DNS4GOV is a strategic layer of defense designed specifically for governments.

# Implementation Standard

## Example Allocation of Responsibilities

The image below illustrates a sample division of roles and responsibilities that can be followed during the onboarding of DNS4GOV.

This is not a rigid framework but rather a reference model designed to help clarify how tasks might be distributed across various stakeholders – such as national CERTs, public IT administrators, Whalebone technical teams, and other supporting entities.

Each government or public sector environment will have its own operational structure, maturity level, and regulatory context, so the actual allocation may vary.

The goal of this model is to support efficient collaboration, reduce ambiguity, and speed up deployment by identifying who typically handles what, whether it be technical integration, policy decisions, communications, or user onboarding.

Supplier of protective DNS Whalebone National operator	Owner of the project Government entity who is a cyber security authority on a national level	The service provider National cyber security authority Ministry, CERT, MSP, operator, or implementer.	CERT National cyber security authority
Supplies the Provider with the actual solution	Allocates budget	Runs the proof of concept, makes sure everything fits	Supports the project from professional and expertise perspective
Tech support to Provider	Implements the project to legislation	Tech support to protected institutions	Provides national threat intelligence feed
Supplier technical documentation, onboarding materials, internal dissemination materials, etc.	Raises political support for the project	Manages who can access the protective DNS, who has authority to provide access to subsidiaries	Benefits from the regional threat intelligence shared by other CERTs in the ecosystem
Dissemination of materials and marketing support to achieve high adoption	Disseminates the project on national level, makes sure to get stakeholders' buy-in, political support		



# Common Governmental Deployment Scenarios

Below are a few common deployment models that we have encountered across government institutions of varying sizes and structures.

These examples are meant to illustrate how DNS4GOV can be integrated into existing public sector environments with minimal disruption.

Every institution has its own operational, regulatory, and technical requirements — and Whalebone is fully prepared to support customized deployments that meet your specific needs.

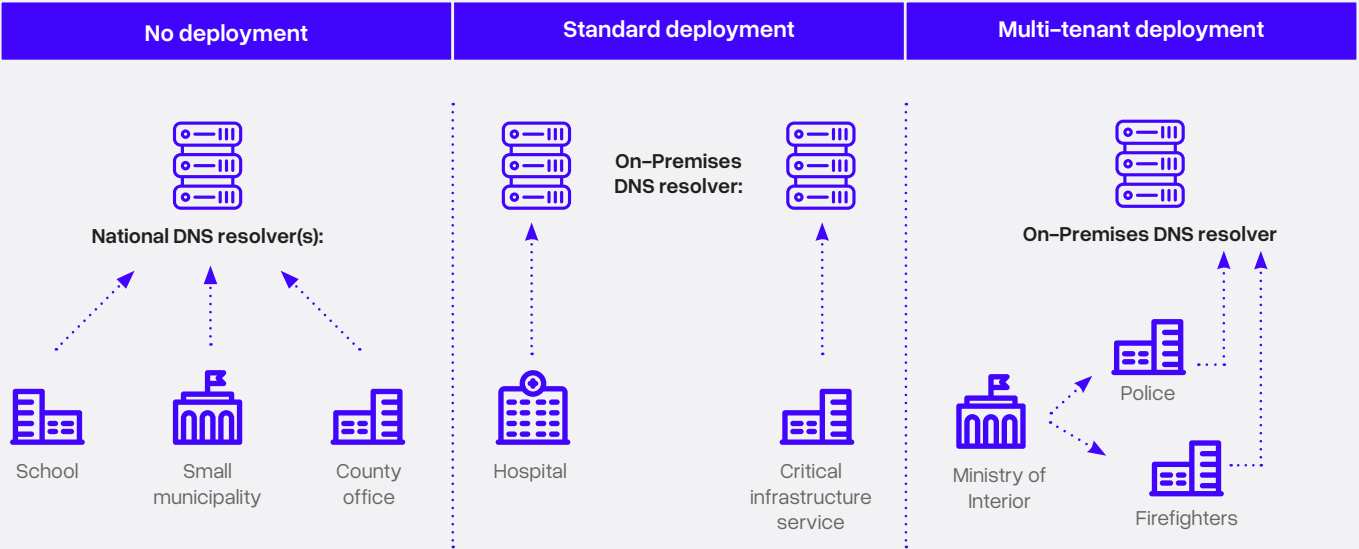
Whether you're securing a single agency or a national-level network, our team will work closely with you to design the most effective, scalable solution.

“This is basically the easiest thing – they just tell us to enable the protection for their institution and immediately start benefiting from it.”

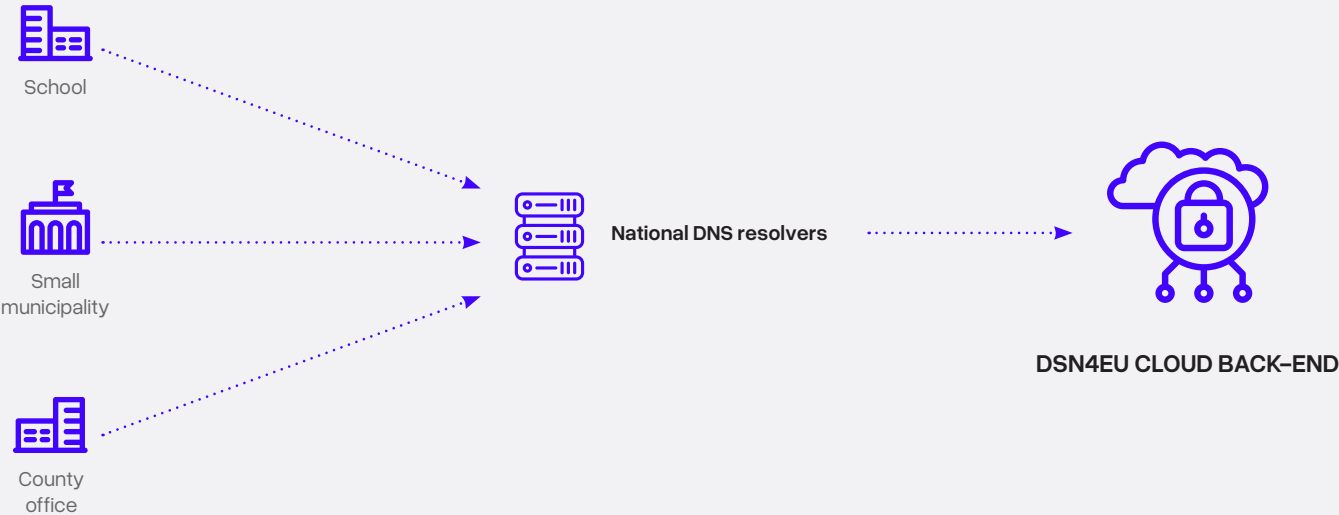
**Guillaume-Jean Herbiet,**  
.lu Service Technical Manager at **Restena**



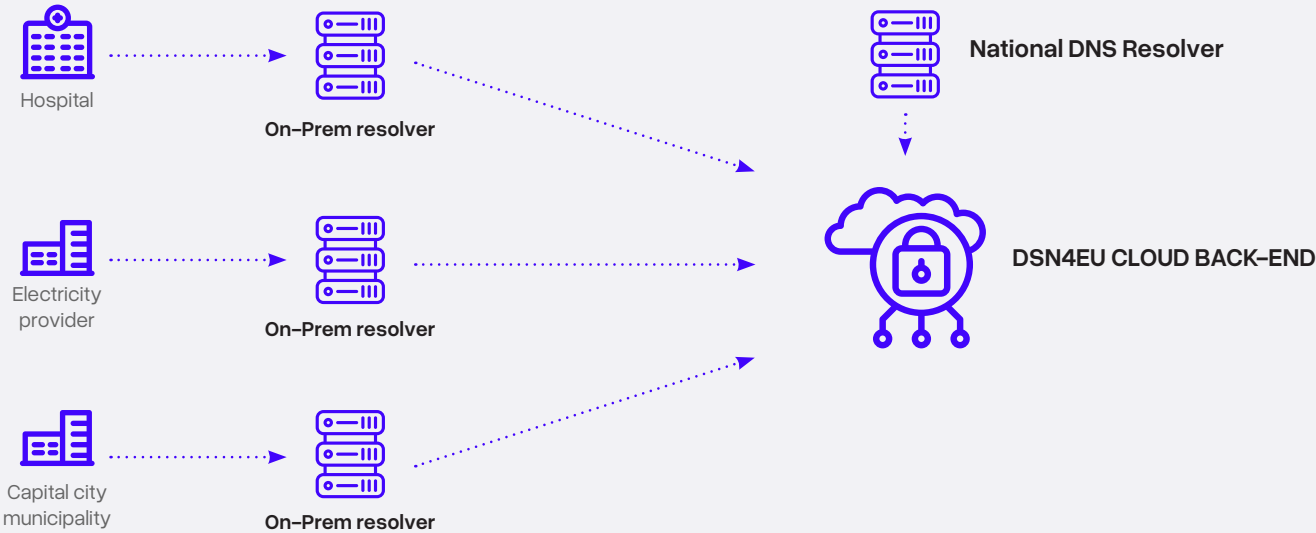
Scenario 1: Overview



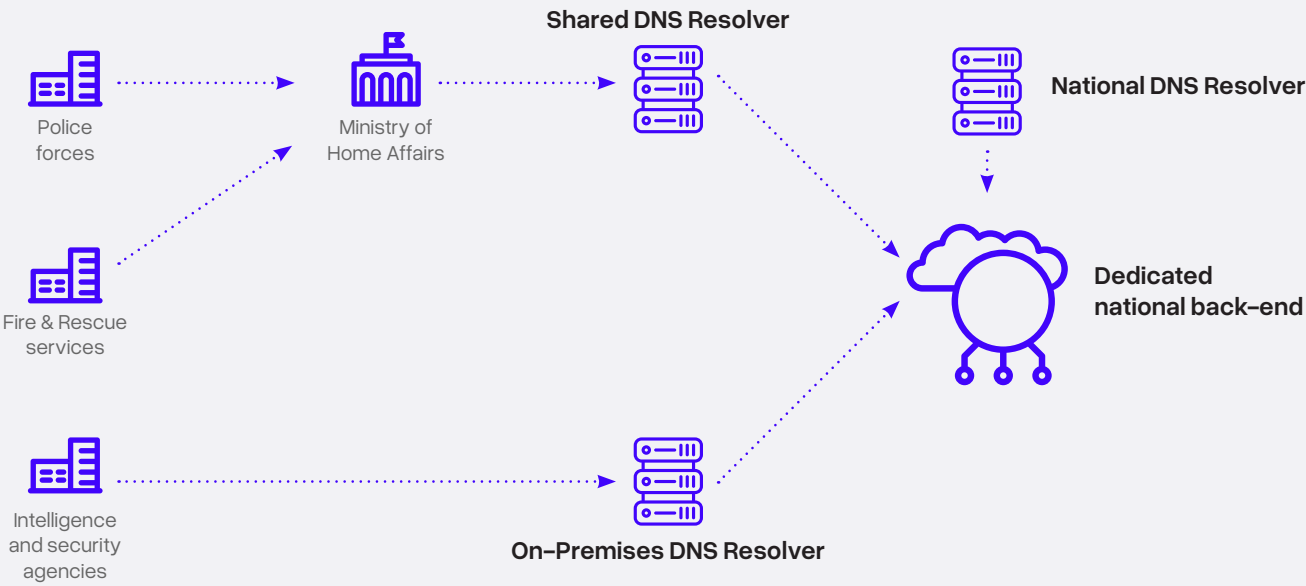
Scenario 2: NCSC managed



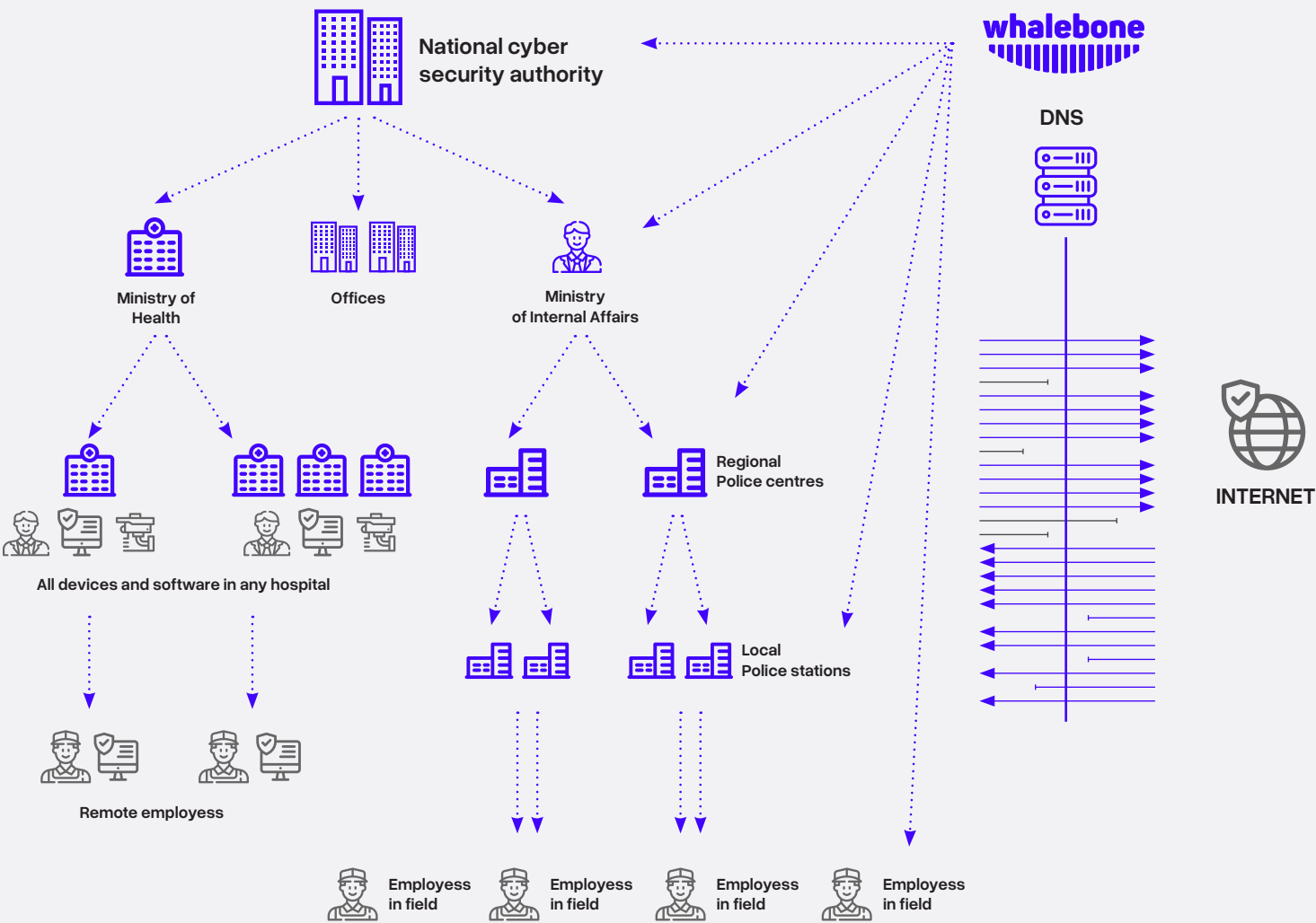
Scenario 3: Hybrid deployment



Scenario 4: National Plan



Scenario 5: Architecture model



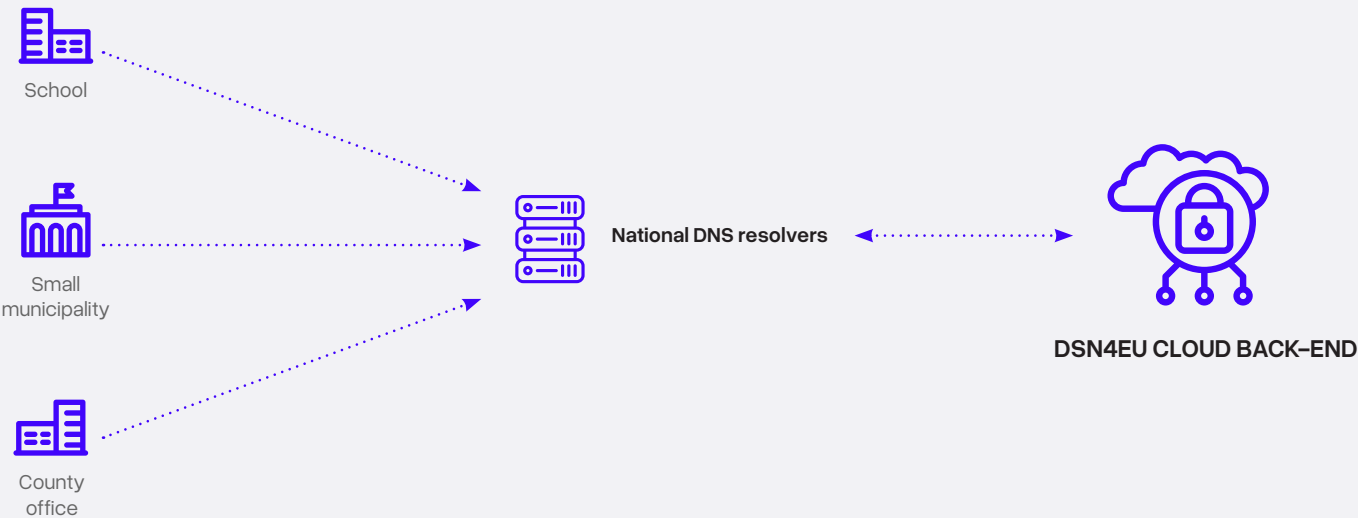
# Maturity Levels for Governmental PDNS

While the previous section outlines deployment patterns that we have commonly observed across various governments, the scenarios that follow represent the idealized maturity path for implementing PDNS at scale.

These stages reflect our vision of how public sector institutions can progressively evolve their DNS security posture – from initial adoption to full operational maturity – maximizing impact, efficiency, and cross-sector resilience along the way.

## Level 0 – Zero Deployment with No Configuration

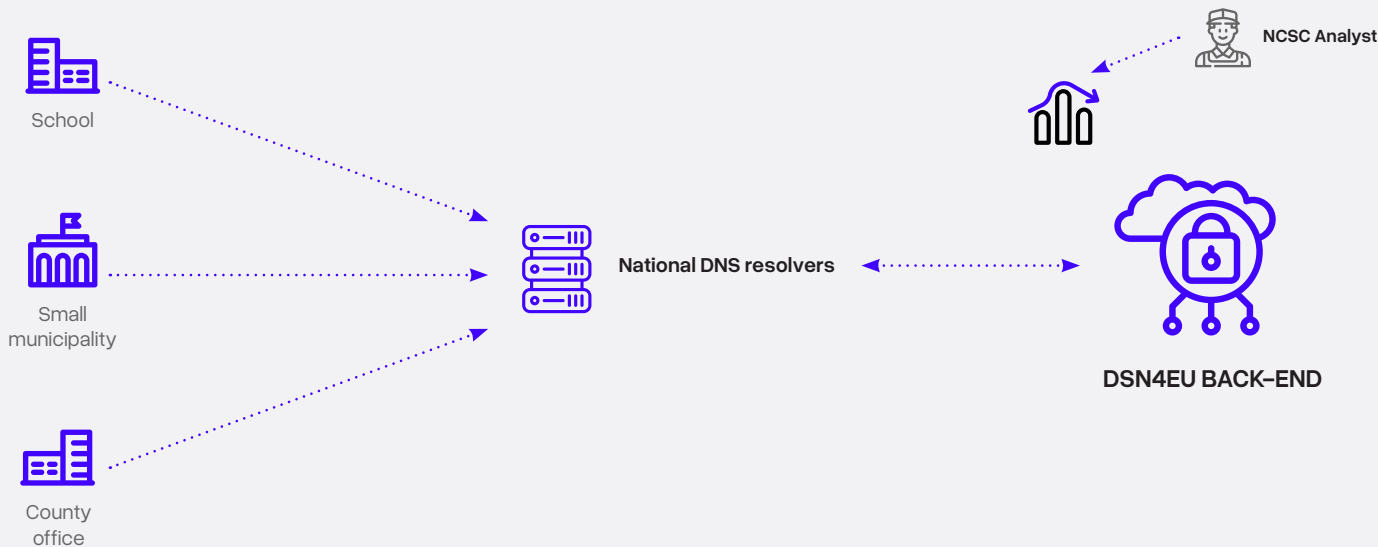
The agency searches for a simple solution with no compromises on Threat Intelligence. Whalebone operates dedicated resolvers powered by Whalebone and integrated NSCS TI feed.





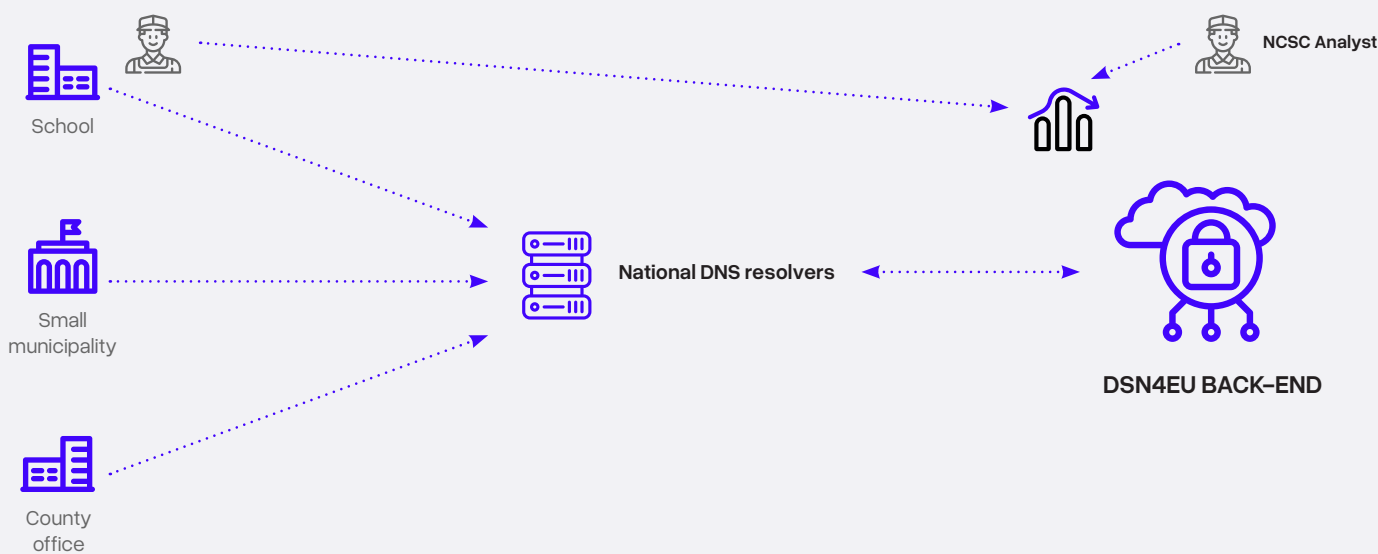
Level 1 – Country-Level PDNS for All Organizations

The agency searches for easy deployment and scalability. They launch the national DNS Resolver and start with evangelization efforts. The organization redirects the DNS traffic and starts to be protected.



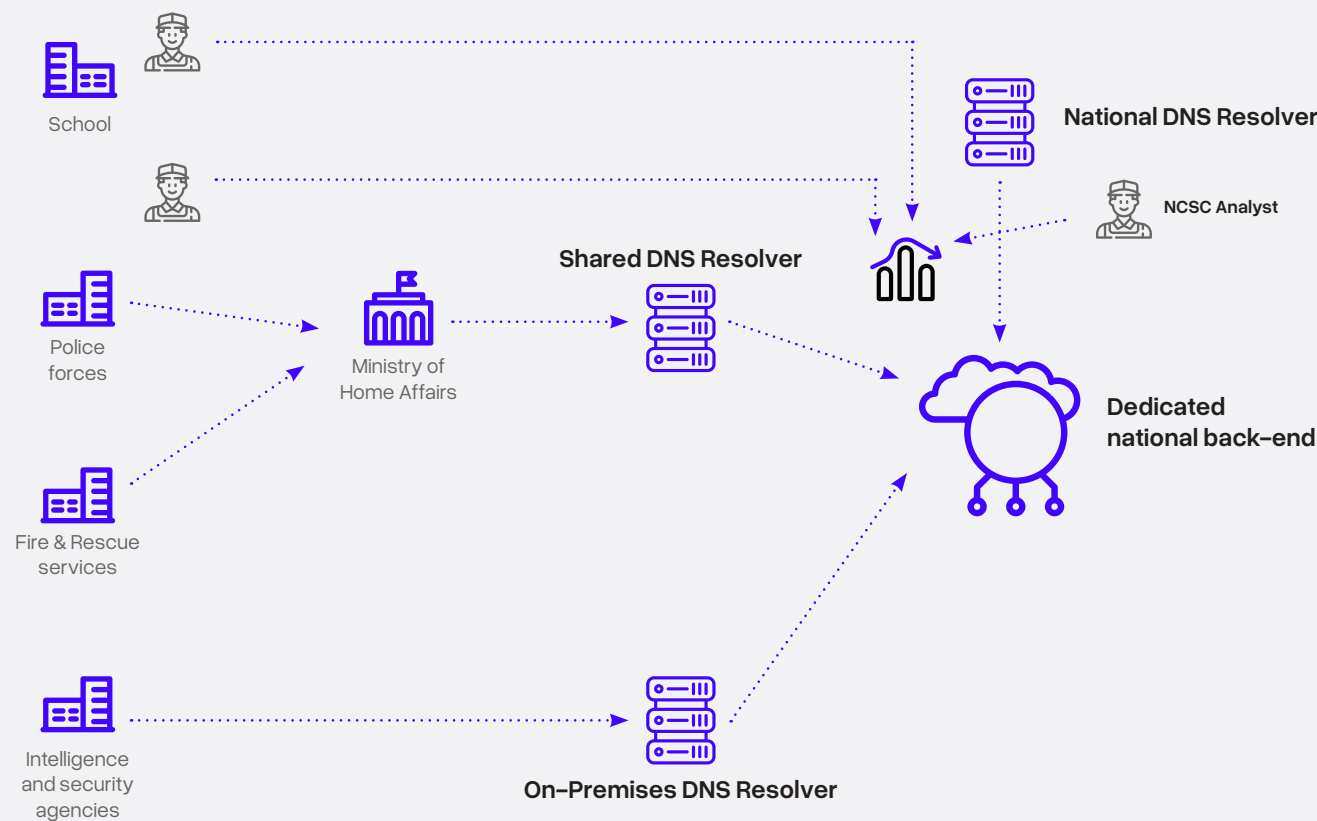
Level 2 – Individual UI with Configuration and Reporting

Organizations start to be more demanding in terms of traffic visibility, analysis, management, integration, and security/content policy definitions.



Level 3 – On-premises DNS Resolvers and Roaming Agents

The agency searches for easy deployment and scalability. They launch the national DNS Resolver and start with evangelization efforts. The organization redirects the DNS traffic and starts to be protected.



# Onboarding Timeline for DNS4GOV

The DNS4GOV onboarding process follows a structured, collaborative, and scalable approach. The timeline below outlines a typical three-phase path, starting with a focused pilot and progressing toward full-scale implementation.

While exact durations may vary depending on infrastructure and internal processes, this framework helps ensure early impact, streamlined adoption, and long-term cybersecurity readiness across the public sector.

Phase 1: Preliminary Steps & Design (1–3 months)	Phase 2: Initial Rollout (3–6 months)	Phase 3: Full-Scale Implementation (3–6 months)
<p>Run a pilot project with select government agencies to evaluate system effectiveness — suggested capacity 40% of Gov agencies</p> <p>Evaluate and prove effectiveness, mitigated risks, and potential ROI</p> <p>Prepare report describing the opportunity of protecting associated organizations based on the data from the pilot rollout(s)</p> <p>Design architecture for the full rollout and suggest recommended security policy based on learnings from the evaluation</p>	<p>Deploy DNS filtering infrastructure and implement initial cybersecurity policies</p> <p>Integrate threat intelligence feeds to enable real-time DNS protection</p> <p>Train key personnel on operational best practices and cybersecurity protocols</p> <p>Run performance benchmarks and end-to-end acceptance testing</p>	<p>Expand PDNS protection to all government entities and critical public institutions</p> <p>Enhance Security Operations Center (SOC) monitoring to detect and mitigate threats proactively</p> <p>Establish secure data-sharing mechanisms between your organization and intelligence services</p> <p>Establish long-term policy frameworks</p>

## Financial & Operational Considerations

Whalebone technology implementation and subscription

- **Subscription (annual)**
- **Implementation Fee (one-time charge)**

Additional governmental costs typically include

- **Infrastructure (servers, hosting, network equipment)**
- **Security and Threat Intelligence Analysis**
- **Operations & Maintenance**
- **Service management, Legal & Compliance**

## Next Steps

- **Align with selected government tenants to define desired onboarding phases and expected budget levels**
- **Determine the scope and ambition for Year 1 (Pilot or full-scale rollout?)**
- **Confirm pilot budget and identify participating agencies**
- **Launch the pilot with selected institutions**
- **Secure necessary funding and approval from key government stakeholders**
- **Develop a roadmap for full-scale deployment, including timelines and onboarding goals for all institutions**
- **Define service-level agreements (SLAs), operational expectations, and responsibilities**
- **Draft or propose a service specification to support a PO or RFP**
- **Begin shaping the multi-year (Year 2+) implementation and sustainability plan**

## Resources: Whalebone DNS4GOV Team

Government Liaison

George Buhai – [george.buhai@whalebone.io](mailto:george.buhai@whalebone.io)

Threat Intelligence Lead

Viliam Peli – [viliam.peli@whalebone.io](mailto:viliam.peli@whalebone.io)

Technical Consultants

Adam Merka – [adam.merka@whalebone.io](mailto:adam.merka@whalebone.io)

Vladimir Spurny – [vladimir.spurny@whalebone.io](mailto:vladimir.spurny@whalebone.io)

