

Europe's Digital Shield

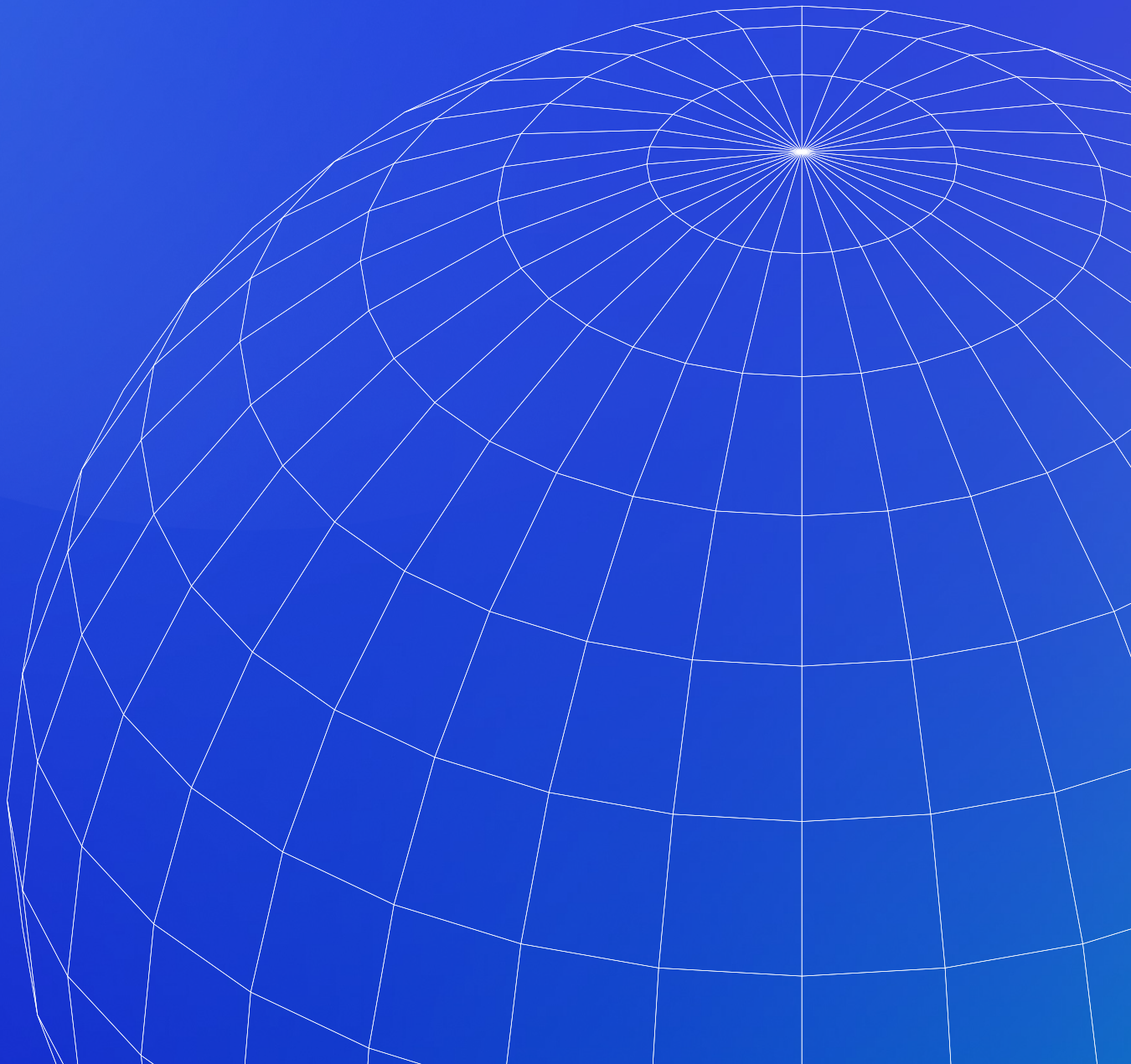
Why Every Nation Will Operate a National Protective
DNS (PDNS) — and How DNS4GOV Makes It Real

*A Whalebone Whitepaper
on National Protective DNS*



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

GUILLAUME-JEAN HERBIET, .LU SERVICE
TECHNICAL MANAGER, RESTENA



1. Europe's Digital Shield: From Fragmented Defense to Collective Resilience

Across Europe, national cybersecurity authorities face a growing structural contradiction. Cyber threats have become **industrialized, automated, and cross-border by default**, while defensive capabilities remain **fragmented, organization-specific, and largely reactive**. Ministries, hospitals, municipalities, universities, and utilities are expected to defend themselves independently, despite facing the same threat actors, the same infrastructure abuse, and the same DNS-based attack techniques.

DNS-based threats exploit this gap relentlessly. Phishing campaigns, ransomware delivery, command-and-control (C2 or C&C) infrastructure, and state-sponsored activity all depend on DNS resolution to function.

Yet DNS still sits **outside the scope of most national security architectures**, governance frameworks, and centralized visibility. As a result, attackers benefit from scale, while defenders remain siloed.

Whalebone's experience across Europe and internationally shows a consistent pattern: countries that treat DNS as only a 'nice-to-have' element of their cybersecurity remain blind to early indicators of attack; countries that treat DNS as strategic defense infrastructure gain leverage, visibility, and speed in countering threats.

Global cybersecurity leaders endorse DNS security as a must-have foundational cybersecurity layer, based on the following key points.

- **UK National Cyber Security Centre:** Protective DNS systems prevent malicious domains being visited by devices in your network.¹
- **Gartner:** Organizations should implement DNS security to protect users and critical infrastructure.²
- **GigaOm:** Almost all cyberattacks will start by interacting with DNS.³
- **CISA:** DNS is foundational to online activity — ensure PDNS is a high-availability service.⁴
- **NSA:** Secure DNS reduces the impact of 92% of malware attacks.⁵

The future state is no longer speculative

Several leading cyber-resilient countries have already implemented national Protective DNS at scale. The UK operates a nationwide PDNS capability under its National Cyber Security Centre, protecting public-sector institutions by default. Similar national-level DNS protection exists across the Five Eyes community — including the USA, Australia, and Canada — through

federally coordinated or delegated models. These countries consistently rank among **the most mature in national cybersecurity resilience**, demonstrating that PDNS is not an experimental concept but a proven foundation of modern cyber defense.

Whalebone's experience working with governments across Europe and

internationally shows that countries adopting PDNS early gain **faster threat visibility, reduced attack impact, and a more coherent national security posture**. In the emerging European cyber baseline, Protective DNS (PDNS) is no longer a pilot, an innovation project, or an optional enhancement. It is every bit as essential as endpoint protection, firewalls, or multi-factor authentication.



Within five years:

Every EU Member State will operate a national PDNS service, either directly or through a delegated national operator

Public institutions will use this service by default, without local procurement or technical burden

National CERTs will gain a shared national sensor and control point, replacing today's DNS blind spot

This vision does not imply a single European DNS or a supranational resolver. Instead, it reflects a shared defensive posture: nationally implemented, sovereign by design, and strengthened collectively through European cooperation.

¹<https://www.ncsc.gov.uk/guidance/protective-dns-for-private-sector>

²<https://www.gartner.com/en/documents/4002327>

³<https://gigaom.com/2024/03/18/dns-security-the-forgotten-hero-of-your-cybersecurity-strategy/>

⁴<https://www.cisa.gov/news-events/directives/ed-19-01-mitigate-dns-infrastructure-tampering>

⁵<https://www.defenseone.com/technology/2020/06/nsa-piloting-secure-domain-name-system-service-defense-contractors/166250/>

2. The Power of Protective DNS: Why It Scales When Other Controls Cannot

Protective DNS operates at a uniquely powerful point in the internet stack.

Every device, user, and application must resolve domain names to function, making DNS the **only control layer that naturally spans the entire public sector** — from legacy systems to cloud workloads, from office networks to remote users.

Unlike downstream controls, PDNS blocks malicious infrastructure **before** a connection is established. This prevents entire classes of attacks silently, without requiring endpoint agents, user awareness training, or behavioral change. When a malicious domain is blocked at the DNS layer, the attack simply fails.

This characteristic makes PDNS unusually easy to justify both operationally and politically, as it does not inspect content, monitor communications, or interfere with legitimate use.

When clearly scoped to malicious domains and transparently governed, PDNS is best understood as **consumer protection for public infrastructure** rather than any type of surveillance.

Why PDNS works

- **Blocks malicious infrastructure before damage occurs**
- **Covers all users and devices automatically**
- **Requires no endpoint agents or user behavior change**
- **Operates independently of application or network architecture**

Deployment time: nationwide in under a year

Most national cybersecurity initiatives take years to mature. Endpoint rollouts, SOC modernization, Zero Trust programs, and network segmentation projects typically span multiple budget cycles and political terms. PDNS is fundamentally different.

- **Institution onboarding:** hours
- **National rollout:** 3–6 months once a solution is selected
- **Tendering:** 1–3 months
- **Project preparation:** 3–9 months

PDNS is the only cybersecurity capability that can realistically protect an entire public sector within a single budget or political cycle, making it uniquely suited to today's threat environment.

3. Collaboration in Action: The DNS4GOV Model

From policy ambition to operational reality

Under the EU-funded **DNS4EU initiative**, Whalebone was appointed Consortium Leader to translate European cybersecurity policy into an operational, sovereign DNS protection framework. The result is **DNS4GOV** – a mature, production-grade model for national Protective DNS, already validated through real-world government deployments.

“The filter should be administered by the state in cooperation with private suppliers with expertise in DNS security [...] The solution could, for example, be developed with inspiration from the EU-funded initiative DNS4GOV.”

—Cyberpolitical Report 2025,
Confederation of Danish Industry

DNS4GOV was designed specifically to meet the needs of public administration at scale: diversity of institutions, strict governance requirements, high availability expectations, and strong privacy guarantees.

Why DIY approaches have consistently fallen short

Several governments have attempted to build PDNS internally. While well-intentioned, most efforts encounter the same structural barriers:

- **limited threat-intelligence coverage**
- **lack of multi-tenant architecture**
- **performance and latency**

constraints

- **high operational and staffing burden**
- **political pressure around blocklists**
- **inability to scale beyond pilot institutions**

Building and maintaining a national PDNS is not a one-off engineering task; **it is**

a permanent operational capability

requiring continuous threat intelligence exchange, tuning, and resilience. DNS4GOV avoids these pitfalls by providing a purpose-built platform rather than a bespoke project.

Architecture at a glance

A national DNS4GOV deployment provides two complementary perspectives:

Central authority (NCSC/CERT):

The national cybersecurity authority gains aggregated, anonymized visibility across all participating institutions. This enables early detection of coordinated campaigns, correlation of incidents across sectors, rapid propagation of threat intelligence, and

integration with existing SOC, SIEM, and MISP ecosystems — all under strict governance and neutrality controls.

Public institutions:

Each institution retains autonomy and visibility into its own environment, including daily protection reports, DNS traffic dashboards, phishing/malware blocking statistics, and optional integration with local SIEM systems. For sensitive or regulated environments, on-premises

resolvers can be deployed without sacrificing central visibility.

What the architecture delivers

- **Central visibility + local autonomy**
- **Multi-tenant, sovereign design**
- **High scalability without operational complexity**
- **Apolitical, threat-intel-driven governance**

4. Immediate Protection Long-Term Impact

Economic impact: proven and measurable

National Protective DNS has already proven its value at scale.

In the UK, the National Cyber Security Centre reports that its **Protective DNS service has processed over 2.5 trillion DNS queries, blocked access to more than 1.5 million malicious domains, and is actively protecting over 1,400 public-sector organisations** – including central government, healthcare, and emergency services.

In a single year (2022), the service blocked 11 billion malicious DNS requests, including millions linked to ransomware activity.

These publicly reported figures demonstrate that **PDNS is a mature, high-impact national capability that delivers continuous protection across the public sector** by neutralising threats before they reach users or systems.

These savings come from:

- prevented ransomware incidents
- reduced phishing compromises
- fewer data breaches
- reduced incident-response workload (around 25%)
- avoided disruption of public services

Put simply, the cost of one major public-sector ransomware incident often exceeds the cost of operating PDNS for several years.

Operational impact

Beyond financial savings, PDNS fundamentally changes how national cybersecurity authorities operate. It reduces pressure on SOC teams,

improves early warning capabilities, and enables proactive rather than reactive defense. Over time, it establishes a consistent baseline of protection across

all public institutions, regardless of their individual maturity.

Trust, neutrality, and sovereignty

DNS4GOV is explicitly designed to protect against malicious infrastructure only. It does not enforce political content

filtering, inspect user communications, or enable surveillance. Blocklists are threat-intelligence driven, auditable, and

governed transparently, ensuring public trust and legal defensibility.

5. Join the Movement: From Vision to Deployment

Protective DNS is no longer a question of if, but when. Countries that have acted early already benefit from immediate risk reduction, improved national resilience, and alignment with European cybersecurity strategy – while avoiding costly and ineffective DIY detours.

DNS4Gov offers a proven, EU-aligned path from vision to national deployment. Do not wait for a breach to prove your vulnerability. Bridge the gap between policy and protection today– contact our experts to launch your national DNS4GOV pilot.

Indicative national pricing

Indicative national pricing for Protective DNS is primarily driven by the number of public-sector employees and users covered, rather than the geographic or economic size of a country. Annual service costs depend on the scale of protected institutions, traffic volumes, and reporting requirements, with a one-time deployment fee of approximately

20 percent of the annual service level. Naturally, a public sector employing several million people will require a different scope and operating model than one serving tens of thousands. For context, previous national DNS security tenders in large non-European countries were awarded at significantly higher annual values under legacy

providers, before being transitioned to a more scalable and cost-efficient national model offered by Whalebone. This investment represents a fraction of the economic and societal cost of a single large-scale cyber incident.

Next step

Governments and national cybersecurity authorities are invited to:

- **Participate in the DNS4GOV national evaluation**
- **assess PDNS under real operational conditions**
- **shape their long-term national Protective DNS framework**

The technology already exists. The threat landscape already demands it. What remains is leadership taking action. Choosing DNS4GOV is more than a security upgrade; it is a commitment to the digital integrity of our society. It is the decision to stop reacting to the threats of yesterday and start defining the safety of tomorrow.

Contact our team to begin your national PDNS onboarding:
DNS4GOV@whalebone.io

About Whalebone

Whalebone is a European cybersecurity company focused exclusively on DNS security. As Consortium Leader and operator of DNS4EU – and architect of DNS4GOV – Whalebone delivers scalable, sovereign Protective DNS solutions to governments, CERTs, and critical-infrastructure operators worldwide.



whalebone.io | joindns4.eu