whalebone

LIVRE BLANC

Le bouclier numérique de l'Europe

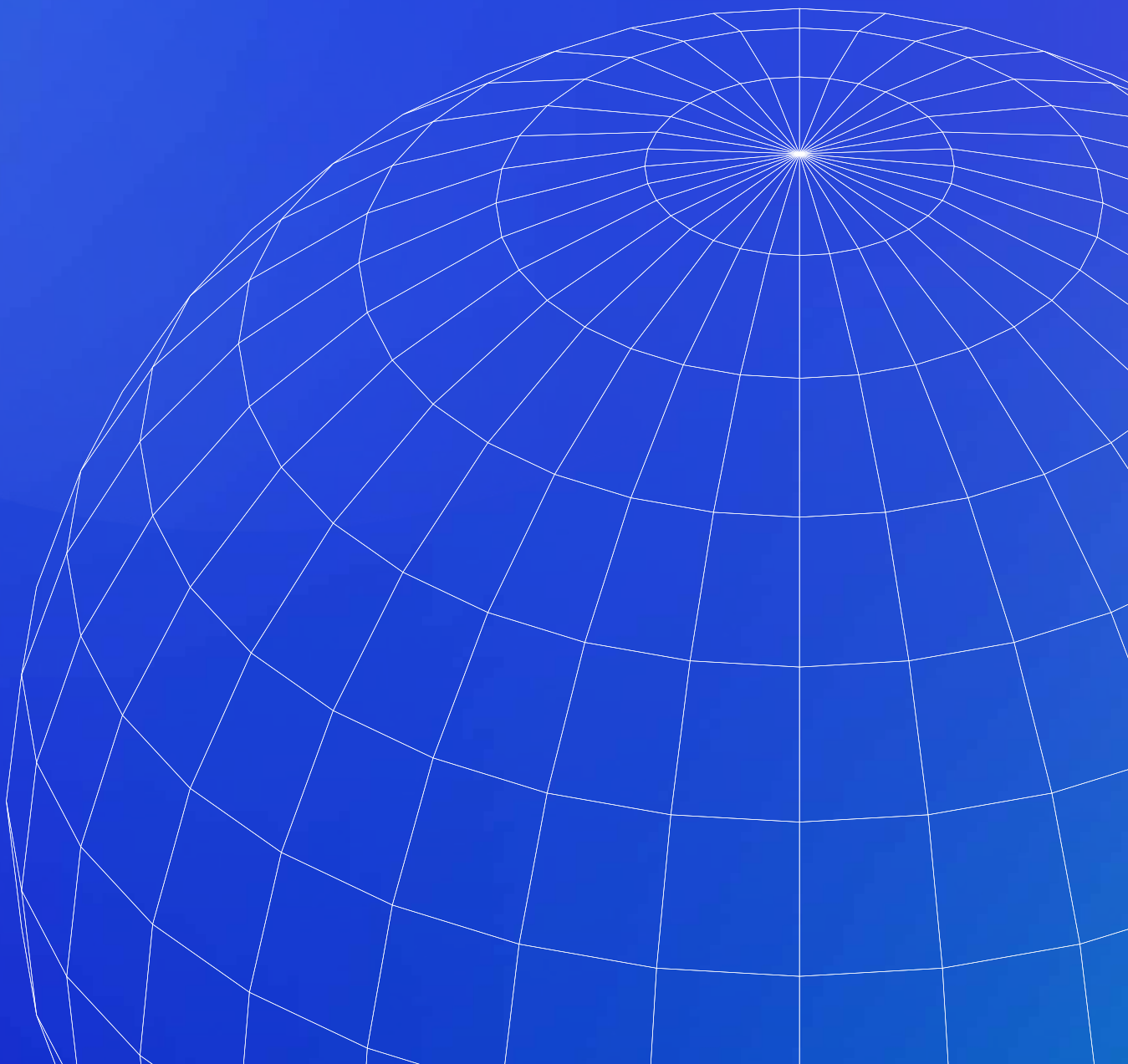
Pourquoi chaque pays se dotera d'un service national de DNS de protection (PDNS) — et comment DNS4GOV permet de le concrétiser



Un livre blanc de Whalebone sur le DNS de protection à l'échelle nationale

« Nous avions besoin d'une solution capable de détecter, par exemple, des campagnes d'hameçonnage imitant une banque locale ou un service d'authentification… Et ça fonctionne, tout simplement. »

GUILLAUME-JEAN HERBIET, RESPONSABLE TECHNIQUE DU SERVICE .LU, RESTENA



1. Le bouclier numérique de l'Europe : **De défenses fragmentées à une résilience collective**

Partout en Europe, les autorités nationales de cybersécurité sont confrontées à une contradiction structurelle croissante. Les cybermenaces se sont industrialisées, automatisées et affranchies des frontières, tandis que les capacités de défense restent fragmentées, propres à chaque organisation et largement réactives. Ministères, hôpitaux, municipalités, universités et opérateurs de services essentiels sont censés assurer leur défense de manière indépendante, alors qu'ils font face aux mêmes acteurs malveillants, aux mêmes détournements d'infrastructure et aux mêmes techniques d'attaque exploitant le DNS.

Les menaces fondées sur le DNS exploitent cette faiblesse sans relâche. Les campagnes d'hameçonnage, la diffusion de rançongiciels, les infrastructures de commande et contrôle (C2 ou C&C) et les activités soutenues par des États dépendent toutes de la résolution DNS pour fonctionner.

Pourtant, le DNS reste encore en dehors du périmètre de la plupart des architectures nationales de sécurité, des cadres de gouvernance et des dispositifs de visibilité centralisée.

Résultat : les attaquants bénéficient des effets d'échelle, tandis que les défenseurs restent cloisonnés.

L'expérience de Whalebone en Europe et à l'international fait apparaître un constat récurrent : les pays qui considèrent encore la sécurité DNS comme un simple complément restent aveugles aux premiers indicateurs d'une attaque. Ceux qui considèrent le DNS comme une infrastructure stratégique de défense gagnent en capacité d'action, en visibilité et en rapidité face aux menaces.

Les principaux acteurs mondiaux de la cybersécurité considèrent la sécurité DNS comme une couche fondamentale et indispensable de la cybersécurité, notamment pour les raisons suivantes :

- **UK National Cyber Security Centre:** les systèmes de DNS de protection empêchent les appareils de votre réseau d'accéder à des domaines malveillants.[1]
- **Gartner:** les organisations devraient mettre en œuvre une sécurité DNS afin de protéger les utilisateurs et les infrastructures critiques.[2]
- **GigaOm:** la quasi-totalité des cyberattaques commencent par une interaction avec le DNS.[3]
- **CISA:** le DNS est un composant fondamental des activités en ligne ; le PDNS doit donc être assuré comme un service à haute disponibilité.[4]
- **NSA:** n DNS sécurisé réduit l'impact de 92 % des attaques par logiciels malveillants.[5]

L'avenir n'est plus une hypothèse

Plusieurs pays parmi les plus avancés en matière de cyber-résilience ont déjà déployé un DNS de protection national à grande échelle. Le Royaume-Uni exploite un service PDNS à l'échelle nationale sous l'égide de son National Cyber Security Centre, protégeant par défaut les institutions du secteur public.

Des dispositifs similaires de protection DNS à l'échelle nationale existent au sein de la communauté Five Eyes, notamment aux États-Unis, en Australie et au Canada, selon des modèles coordonnés au niveau fédéral ou délégués.

Ces pays figurent régulièrement parmi les plus matures en matière de résilience nationale face aux cybermenaces, démontrant ainsi que le PDNS n'est pas un concept expérimental, mais l'un des fondements éprouvés d'une cyberdéfense moderne. L'expérience de Whalebone auprès des gouvernements en Europe et dans le reste du monde montre que les pays qui adoptent rapidement le PDNS bénéficient d'une détection plus rapide des menaces, d'une réduction de l'impact des attaques et d'une posture nationale de cybersécurité plus cohérente.

Dans le nouveau socle européen de cybersécurité, le DNS de protection (PDNS) n'est plus un projet pilote, une initiative d'innovation ou une amélioration facultative. Il est désormais aussi essentiel que la protection des terminaux, les pare-feu ou l'authentification multifacteur.

D’ici cinq ans :

Chaque État membre de l’UE exploitera un service national de DNS de protection (PDNS), directement ou par l’intermédiaire d’un opérateur national mandaté.

Les institutions publiques utiliseront ce service par défaut, sans avoir à gérer localement les procédures d’achat ni une charge technique supplémentaire.

Les CERT nationaux disposeront d’un point d’observation et de contrôle partagé à l’échelle nationale, mettant fin au manque actuel de visibilité sur le DNS.

Cette vision n’implique ni un DNS européen unique ni un résolveur supranational.

Elle repose au contraire sur une posture de défense commune : mise en œuvre au niveau national, souveraine par conception et renforcée collectivement grâce à la coopération européenne.

[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. La puissance du DNS de protection : **Une capacité qui passe à l'échelle là où d'autres dispositifs atteignent leurs limites**

Le DNS de protection occupe une position particulièrement stratégique dans l'architecture d'Internet.

Chaque appareil, utilisateur et application doit résoudre des noms de domaine pour fonctionner. Le DNS constitue ainsi la seule couche de contrôle couvrant naturellement l'ensemble du secteur public : des systèmes existants aux charges de travail dans le cloud, des réseaux de bureaux aux utilisateurs à distance.

Contrairement aux dispositifs qui interviennent plus en aval, le PDNS bloque les infrastructures malveillantes avant même qu'une connexion ne soit établie. Il permet ainsi de neutraliser silencieusement des catégories entières d'attaques, sans nécessiter l'installation d'agents sur les terminaux, de formation spécifique des utilisateurs ou de changement de comportement.

Lorsqu'un domaine malveillant est bloqué au niveau DNS, l'attaque échoue tout simplement.

Cette caractéristique rend également le PDNS particulièrement facile à justifier sur les plans opérationnel et politique : il n'inspecte pas les contenus, ne surveille pas les communications et n'interfère pas avec les usages légitimes.

Lorsque son périmètre est clairement limité aux domaines malveillants et que sa gouvernance est transparente, le PDNS doit avant tout être considéré comme un dispositif de protection des utilisateurs et des infrastructures publiques, et non comme un outil de surveillance.

Pourquoi le PDNS est efficace

- **Bloque les infrastructures malveillantes avant qu'elles ne puissent causer de dommages**
- **Protège automatiquement l'ensemble des utilisateurs et des appareils**
- **Ne nécessite aucun agent sur les terminaux ni changement de comportement des utilisateurs Fonctionne indépendamment des applications ou de l'architecture réseaue**

Délai de déploiement : une couverture nationale en moins d'un an

La plupart des initiatives nationales de cybersécurité nécessitent plusieurs années pour atteindre leur pleine maturité. Le déploiement de solutions de protection des terminaux, la modernisation des SOC, les programmes Zero Trust et les projets de segmentation réseau s'étendent généralement sur plusieurs cycles budgétaires et mandats politiques.

Le PDNS fonctionne selon une logique fondamentalement différente.

- **Intégration d'une institution : quelques heures**
- **Déploiement national : 3 à 6 mois après sélection de la solution**
- **Procédure d'appel d'offres : 1 à 3 mois**
- **Préparation du projet : 3 à 9 mois**

Le PDNS est la seule capacité de cybersécurité capable, de manière réaliste, de protéger l'ensemble d'un secteur public au cours d'un seul cycle budgétaire ou politique. Il est donc particulièrement adapté à l'environnement actuel des cybermenaces.

3. La collaboration en action : **Le modèle DNS4GOV**

De l'ambition politique à la réalité opérationnelle

Dans le cadre de l'initiative DNS4EU financée par l'Union européenne, Whalebone a été désigné chef de consortium afin de traduire la politique européenne de cybersécurité en un cadre opérationnel et souverain de protection DNS.

Le résultat est DNS4GOV : un modèle mature et opérationnel de DNS de protection à l'échelle nationale, déjà validé dans le cadre de déploiements gouvernementaux réels.

« Le filtre devrait être administré par l'État en coopération avec des fournisseurs privés disposant d'une expertise en matière de sécurité DNS [...] La solution pourrait, par exemple, s'inspirer de l'initiative DNS4GOV financée par l'Union européenne. »
— Rapport sur la cyberpolitique 2025, Confédération de l'industrie danoise

DNS4GOV a été spécifiquement conçu pour répondre aux besoins des administrations publiques à grande échelle : diversité des institutions, exigences strictes en matière de gouvernance, impératifs de haute disponibilité et fortes garanties de protection de la vie privée.

Pourquoi les approches développées en interne ont régulièrement montré leurs limites

Plusieurs gouvernements ont tenté de développer leur propre PDNS, mais se heurtent souvent aux mêmes limites :

- **renseignement sur les menaces insuffisant**
- **architecture peu adaptée à plusieurs entités**
- **contraintes de performance et de latence**
- **coûts opérationnels et besoins en personnel élevés**
- **gouvernance complexe des listes de blocage**
- **difficultés de déploiement à grande échelle**

Un PDNS national exige une exploitation continue, un renseignement constamment actualisé et une forte résilience. DNS4GOV répond à ces exigences grâce à une plateforme spécialement conçue pour un déploiement national.

Vue d'ensemble de l'architecture

Un déploiement national de DNS4GOV offre deux perspectives complémentaires :

Autorité centrale (NCSC/CERT)

L'autorité nationale dispose d'une visibilité agrégée et anonymisée sur les institutions participantes. Elle peut détecter les campagnes coordonnées, corréler les incidents, partager le renseignement sur les menaces et intégrer les outils SOC, SIEM et MISP existants.

Institutions publiques

Chaque institution conserve son autonomie et une visibilité sur son environnement : trafic DNS, rapports de protection, statistiques de blocage et intégration SIEM facultative. Des résolveurs sur site peuvent être déployés dans les environnements sensibles.

Cette architecture garantit :

- **visibilité centralisée et autonomie locale**
- **architecture souveraine et multi-entité**
- **déploiement à grande échelle**
- **gouvernance neutre fondée sur le renseignement sur les menaces**

4. Une protection immédiate
Un impact à long terme

Impact économique : éprouvé et mesurable

Le DNS de protection à l'échelle nationale a déjà démontré sa valeur à grande échelle.

Au Royaume-Uni, le National Cyber Security Centre indique que son service de DNS de protection a traité plus de 2 500 milliards de requêtes DNS, bloqué l'accès à plus de 1,5 million de domaines malveillants et protège activement plus de 1 400 organisations du secteur public, notamment l'administration centrale, les services de santé et les services d'urgence.

Sur la seule année 2022, le service a bloqué 11 milliards de requêtes DNS malveillantes, dont plusieurs millions liées à des activités de rançongiciels.

Ces chiffres publiés démontrent que le PDNS constitue une capacité nationale mature et à fort impact, assurant une protection continue de l'ensemble du secteur public en neutralisant les menaces avant qu'elles n'atteignent les utilisateurs ou les systèmes.

Ces économies résultent notamment :

- **des incidents liés aux rançongiciels évités**
- **de la réduction des compromissions par hameçonnage**
- **de la diminution du nombre de violations de données**
- **de la réduction de la charge liée à la réponse aux incidents (environ 25 %)**
- **des interruptions de services publics évitées**

En termes simples, le coût d'un seul incident majeur de rançongiciel dans le secteur public dépasse souvent le coût de plusieurs années d'exploitation d'un service PDNS.

Impact opérationnel

Au-delà des économies financières, le PDNS transforme en profondeur le fonctionnement des autorités nationales de cybersécurité.

Il réduit la pression exercée sur les équipes des SOC, améliore les capacités d'alerte précoce et permet de passer d'une défense réactive à une approche proactive.

À terme, il établit un socle de protection homogène pour l'ensemble des institutions publiques, quel que soit leur niveau de maturité individuel.

Confiance, neutralité et souveraineté

DNS4GOV est explicitement conçu pour assurer une protection contre les seules infrastructures malveillantes. Il n'impose aucun filtrage de contenus à caractère politique, n'inspecte pas les communications des utilisateurs et ne permet aucune surveillance.

Les listes de blocage reposent sur le renseignement sur les menaces, sont auditables et font l'objet d'une gouvernance transparente, garantissant ainsi la confiance du public et la solidité du dispositif sur le plan juridique.

5. Rejoindre le mouvement : **De la vision au déploiement**

Le DNS de protection n'est plus une question de « si », mais de « quand ».

Les pays qui ont agi rapidement bénéficient déjà d'une réduction immédiate des risques, d'une meilleure résilience nationale et d'un alignement sur la stratégie européenne de cybersécurité, tout en évitant les détours coûteux et inefficaces liés au développement d'une solution en interne.

DNS4GOV offre une voie éprouvée et alignée sur les orientations européennes pour passer d'une vision à un déploiement national.

N'attendez pas qu'une cyberattaque vienne démontrer votre vulnérabilité. Comblez dès aujourd'hui l'écart entre politique de cybersécurité et protection opérationnelle : contactez nos experts pour lancer votre pilote national DNS4GOV.

Tarification nationale indicative

La tarification indicative d'un service national de DNS de protection dépend principalement du nombre d'agents du secteur public et d'utilisateurs couverts, plutôt que de la taille géographique ou économique du pays.

Le coût annuel du service dépend du nombre et de la taille des institutions protégées, des volumes de trafic et des exigences en matière de rapports, auxquels s'ajoutent des frais de déploiement uniques correspondant à environ 20 % du coût annuel du service.

Naturellement, un secteur public employant plusieurs millions de personnes nécessite un périmètre et un modèle opérationnel différents de ceux d'un secteur public comptant quelques dizaines de milliers d'agents. À titre de comparaison, de précédents appels d'offres nationaux portant sur la sécurité DNS dans de grands pays hors d'Europe ont été attribués à des fournisseurs historiques pour des montants annuels nettement supérieurs, avant de migrer vers le modèle national plus évolutif et plus économique proposé par Whalebone.

Cet investissement ne représente qu'une fraction du coût économique et sociétal d'un seul cyberincident de grande ampleur.

Prochaine étape

Les gouvernements et autorités nationales de cybersécurité sont invités à :

- **participer à l'évaluation nationale de DNS4GOV**
- **évaluer le PDNS dans des conditions opérationnelles réelles**
- **définir leur cadre national de DNS de protection à long terme**

La technologie existe déjà. Les cybermenaces actuelles en démontrent déjà la nécessité. Il ne manque plus qu'une décision et une volonté d'agir. Choisir DNS4GOV va au-delà d'une simple amélioration de la sécurité : c'est un engagement en faveur de l'intégrité numérique de notre société. C'est décider de ne plus seulement réagir aux menaces d'hier, mais de contribuer dès aujourd'hui à définir la sécurité numérique de demain.

Contactez notre équipe pour lancer l'intégration de votre PDNS national :
DNS4GOV@whalebone.io

whalebone

À propos de Whalebone

Whalebone est une entreprise européenne de cybersécurité exclusivement spécialisée dans la sécurité DNS. En tant que chef de consortium et opérateur de DNS4EU, ainsi qu'architecte de DNS4GOV, Whalebone fournit aux gouvernements, aux CERT et aux opérateurs d'infrastructures critiques du monde entier des solutions souveraines de DNS de protection conçues pour passer à l'échelle.