

LIVRE BLANC

LES BONNES PRATIQUES DNS

Auteur :
Craig Sanderson,
Stratège principal en cybersécurité
chez Infoblox



TABLE DES MATIÈRES

1. INTRODUCTION	3
2. IMPACT DU DNS SUR LA CYBER-RÉSILIENCE, LA DÉFENSE EN PROFONDEUR ET LE MODÈLE ZERO TRUST	3
3. VECTEURS DE MENACE DNS	4
4. BONNES PRATIQUES DNS SÉCURISÉES	5
4.1 Utilisation d'un DNS protecteur	6
4.2 Sécurisation du protocole DNS	7
4.3 Sécurisation du service et de l'infrastructure DNS	8
5. SYNTHÈSE ET RECOMMANDATIONS	9

Ce livre blanc vise à fournir les meilleures pratiques de sécurité DNS (Domain Name System), qui ont deux objectifs : sécuriser le protocole et l'infrastructure DNS pour réduire les abus ou les erreurs de configuration, et utiliser le DNS pour fournir une couche supplémentaire de sécurité réseau dans le cadre d'une approche de gestion des risques de sécurité de type Zero Trust et/ou défense en profondeur.

1. INTRODUCTION

Pour accéder aux ressources Internet par nom de domaine (par exemple, [www.exemple\[.\]com](http://www.exemple[.]com)) plutôt que par adresse IP (93.184.216.34), les utilisateurs ont besoin d'un système capable de traduire ces noms de domaine en adresses IP et inversement. Cette traduction est la tâche principale du DNS. Dans les déploiements de réseau des entreprises modernes, l'infrastructure DNS est cruciale pour toutes les communications réseau internes ou avec Internet. En cas de défaillance, des réseaux entiers, ainsi que leurs applications et leurs utilisateurs, peuvent être mis hors service. Ainsi, le DNS est un élément crucial de la résilience numérique des entreprises et doit être régulièrement évalué ou réévalué.

Ces évaluations doivent inclure une analyse de la capacité des serveurs DNS à répondre aux besoins de l'entreprise, en particulier lors de l'adoption des protocoles DNS chiffrés. Les évaluations doivent également inclure un examen de l'état et de la configuration des serveurs afin de s'assurer que l'infrastructure DNS est optimisée dans le cadre d'une architecture hautement résiliente et redondante. Par ailleurs, les entreprises doivent intégrer des contrôles dans leur plateforme DNS afin d'exploiter le potentiel majeur du DNS en tant que couche clé d'une architecture de cybersécurité.

La plateforme DNS est déjà utilisée par tous les types de clients sur le réseau, y compris sur site, sur le cloud et dans toutes sortes d'appareils IoT. Ainsi, toute protection apportée par l'infrastructure DNS profite à tous les clients qui l'utilisent pour la résolution de noms, quel que soit le type d'appareil. C'est pour cette raison que les entreprises et les gouvernements devraient adopter, et ont d'ailleurs adopté, le DNS comme élément fondamental de leur stratégie de cybersécurité.

Cela s'est traduit par la mise à jour des recommandations en matière de bonnes pratiques publiées par l'Institut national des normes et des technologies (NIST) dans la [publication spéciale \(SP\) 800-81](#), ainsi que par leur intégration dans la [directive NIS2](#) de l'Union européenne.

2. IMPACT DU DNS SUR LA CYBER-RÉSILIENCE, LA DÉFENSE EN PROFONDEUR ET LE MODÈLE ZERO TRUST

Les récentes évolutions des bonnes pratiques en sécurité réseau ont renforcé l'importance du concept de défense en profondeur, qui repose sur l'idée qu'aucune mesure de protection n'est infaillible et que, par conséquent, une défense efficace s'appuie sur plusieurs couches successives. Ce style de cyberdéfense produit un système plus flexible, évolutif et résilient, qui résiste mieux à la compromission et s'aligne plus étroitement sur les principes du modèle Zero Trust.

Les principes du modèle Zero Trust partent du principe qu'aucun élément, nœud ou service ne doit être considéré comme digne de confiance par défaut. Cependant, le DNS reste souvent un élément négligé dans les stratégies du modèle Zero Trust, créant un écart important lorsqu'il est implicitement considéré comme fiable.

Pour aligner le DNS avec les principes du modèle Zero Trust, les entreprises doivent vérifier activement leurs sources d'information, en s'appuyant sur le DNS pour appliquer les politiques de sécurité, bloquer l'accès des utilisateurs finaux et des systèmes aux ressources malveillantes ou non autorisées, et assurer une visibilité sur les actifs pour la réponse aux incidents et l'investigation. Cela marque une évolution du rôle du DNS, qui passe d'un simple outil opérationnel à un levier à grande échelle pour renforcer la sécurité Internet et la résilience des réseaux.

Le modèle Zero Trust rompt avec une approche centrée sur la localisation pour adopter une stratégie axée sur l'identité, le contexte et les données, avec des contrôles de sécurité fins et dynamiques entre les utilisateurs, les systèmes, les applications, les données et les ressources. La résolution DNS permettant aux endpoints de consulter librement des noms de domaine publics,

les entreprises doivent sécuriser le DNS afin d'empêcher tout contournement des contrôles réseau du modèle Zero Trust. Cela pourrait impliquer la mise en œuvre de services DNS de protection et/ou de configurations de résolveurs DNS spécifiques pour certaines catégories d'endpoints. Le DNS protecteur est particulièrement utile pour protéger les appareils IoT et les technologies opérationnelles impliqués dans les secteurs de la fabrication et des infrastructures critiques, où le déploiement de solutions de sécurité aux endpoints s'avère souvent complexe.

3. VECTEURS DE MENACE DNS

L'infrastructure DNS est un vecteur de menace courant pour les campagnes d'attaque.¹ Les menaces qui pèsent sur le service DNS peuvent se traduire par de graves défaillances opérationnelles ou par une perte de données, d'intégrité et de confidentialité.

De plus, de nombreux acteurs malveillants, tels qu'[ALPHV Blackcat](#), utilisent des domaines frauduleux pour lancer des attaques par rançongiciel à grande échelle.² Vous trouverez ci-dessous une liste non exhaustive d'exemples de compromissions qui pourraient mettre en péril non seulement les services DNS, mais aussi tous les systèmes dont dépendent les entreprises :

- a. **Le déni de service distribué** : Un pirate pourrait envoyer un grand volume de requêtes pour mener une attaque par déni de service (DoS) contre un serveur/service DNS. L'attaquant pourrait utiliser de nombreux clients DNS tiers pour soutenir l'attaque (DoS distribué ou DDoS). La criticité du DNS explique pourquoi son ciblage est une tactique courante dans ces attaques.
- b. **La modification de configuration non autorisée** : Le fichier de configuration au niveau de la plateforme qui permet la communication DNS pourrait être corrompu ou faire l'objet de modifications non autorisées en raison de protections inadéquates, entraînant des perturbations allant de la rupture de la communication entre les hôtes DNS à la défaillance complète du service DNS lui-même.
- c. **L'exploitation des CNAME orphelins** : Lorsqu'un enregistrement DNS CNAME relie deux noms de domaine, il existe un risque que le domaine parent du nom canonique vers lequel pointe l'enregistrement ne soit plus enregistré par l'organisation cible. Par conséquent, des acteurs malveillants peuvent enregistrer le domaine parent, et les résolutions DNS aboutiront alors au domaine contrôlé par ces acteurs. Les enregistrements CNAME peuvent également être exploités si le nom canonique renvoie à une adresse IP qui n'est plus utilisée par le propriétaire du domaine et si l'attaquant parvient à prendre le contrôle de cette adresse IP, pouvant mener à des attaques.
- d. **L'exploitation de délégation boiteuse** : Les domaines sont délégués d'un niveau de la hiérarchie DNS à un autre, le plus souvent d'un domaine de premier niveau à l'entreprise qui enregistre le domaine. Lorsqu'une délégation est mise en place, il est nécessaire de spécifier les serveurs DNS autoritaires pour le domaine. Déléguer une zone à un serveur de noms qui ne fait pas autorité pour cette zone est ce que l'on appelle une délégation boiteuse. Ce type de délégation peut entraîner le détournement de domaine dans certaines circonstances.³ Lorsqu'un sous-domaine est délégué à un fournisseur d'hébergement DNS et que le contrat de fourniture des services DNS pour ce domaine expire, des acteurs de menace peuvent détourner la résolution de ce sous-domaine en contractant avec le fournisseur qui contrôle les serveurs ciblés par la délégation pour héberger ce sous-domaine sous leur contrôle. Cela permet ensuite à l'acteur malveillant de rediriger les demandes de résolution vers sa propre infrastructure, bénéficiant de la réputation positive du nom de domaine. Infoblox surveille les cybercriminels (tels que [Hazy Hawk](#)) qui se spécialisent dans l'exploitation de cette faille, ce qui conduit souvent à l'utilisation de ces domaines dans le cadre de campagnes de cybercriminalité allant du phishing à la fraude.
- e. **L'exploitation des domaines similaires** : Les cybercriminels exploitent largement les domaines similaires ou en typosquattage pour usurper l'identité d'entreprises ciblées.⁴ En s'appuyant sur la réputation positive d'organisations légitimes, ils augmentent considérablement le taux de réussite de leurs campagnes de phishing et de malware. Ces domaines similaires peuvent inclure des variantes subtiles de domaines légitimes ou utiliser la substitution de texte ou de caractères pour enregistrer un domaine qu'un utilisateur pourrait confondre avec celui de l'entreprise légitime. Les domaines similaires se sont révélés extrêmement efficaces dans les campagnes de phishing, car on ne peut pas attendre des utilisateurs ordinaires

qu'ils fassent la distinction entre les domaines légitimes et les domaines frauduleux. [Loopy Lizard](#) exploite largement les domaines similaires ou en typosquattage pour usurper l'identité d'entreprises ciblées.⁵

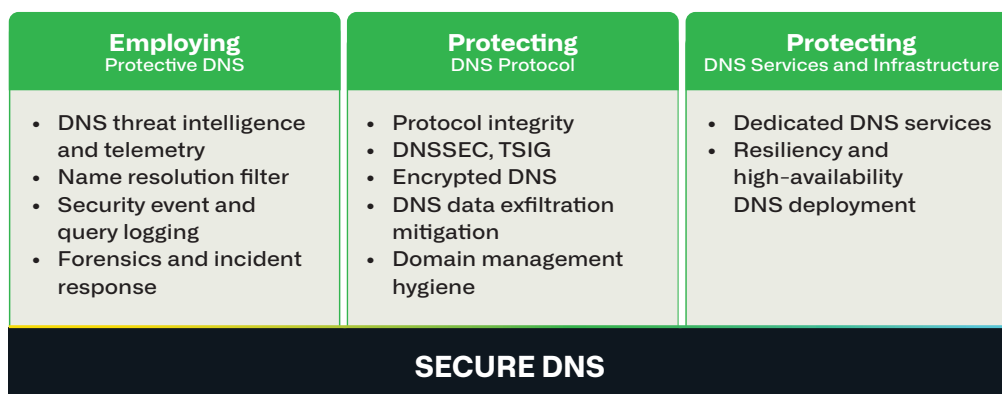
- f. **La commande et le contrôle (C2) des logiciels malveillants** : Les cybercriminels qui parviennent à compromettre un appareil cherchent à maintenir la communication avec celui-ci. Souvent désignée sous le nom de « commande et contrôle » (C2), la technologie DNS constitue une méthode privilégiée pour maintenir cette connexion, en raison de sa disponibilité quasi universelle et de l'absence de contrôle de sécurité DNS sur de nombreux réseaux. Ces canaux de communication permettent toute une série d'activités malveillantes, allant des chevaux de Troie d'accès à distance (RAT) aux ransomwares. Pour opérer à grande échelle et contourner les contrôles de cybersécurité statiques, les cybercriminels ont souvent recours à des algorithmes de génération de domaines (DGA) afin de disposer d'un ensemble dynamique de domaines permettant de maintenir le contrôle des appareils compromis. Les cybercriminels innovent dans ce domaine en exploitant des [DGA enregistrés](#), contribuant ainsi à des opérations de cybercriminalité à l'échelle industrielle orchestrées via le DNS.⁶
- g. **L'exfiltration de données DNS** : Le DNS est désormais un vecteur exploité par les cybercriminels. Comme la plupart des mesures de protection contre les fuites de données se concentrent sur le trafic des e-mails ou le trafic web, les cybercriminels se sont tournés vers le DNS pour exfiltrer des données hors des réseaux et des ressources compromises. En intégrant les données volées dans des requêtes DNS, ils peuvent les dissimuler à la vue de tous, en les mêlant aux milliards de requêtes DNS effectuées chaque jour et en les transmettant via un protocole auquel la majorité des réseaux laissent un accès ouvert et non surveillé par défaut.

4. BONNES PRATIQUES DNS SÉCURISÉES

L'intention initiale du DNS était de distribuer des informations telles que les mappages d'hôtes et d'adresses IP, les informations de routage des e-mails, etc. Il n'était donc pas traditionnellement considéré comme un outil pouvant servir à sécuriser les communications réseau. Cependant, le rôle joué par le DNS dans la quasi-totalité des communications réseau actuelles en fait un outil efficace non seulement pour surveiller, mais également pour gérer ces communications. C'est pourquoi la sécurité DNS a évolué. D'une simple fonction de protection de l'infrastructure et des protocoles DNS, il est devenu un contrôle de sécurité critique et un élément clé de la stratégie de sécurité de l'ensemble de l'entreprise. Il convient de noter que le DNSSEC (un protocole spécifique appelé DNS Security Extension) n'est qu'une partie du concept plus large de sécurité DNS et qu'il doit être mis en œuvre parallèlement à d'autres bonnes pratiques.

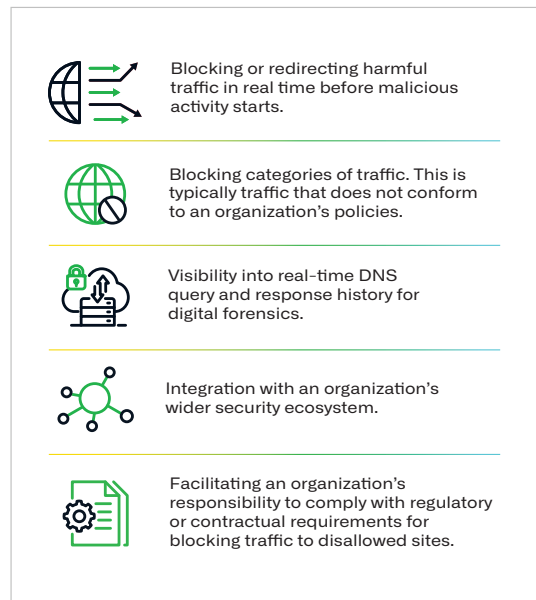
Dans les sections suivantes, nous aborderons les trois composantes essentielles des meilleures pratiques de sécurité DNS à prendre en considération, notamment :

- L'utilisation d'un DNS protecteur
- La sécurisation du protocole DNS
- La sécurisation du service et de l'infrastructure DNS



4.1 L'utilisation d'un DNS protecteur

Le DNS protecteur est un service ou produit DNS auquel ont été ajoutées des capacités de sécurité pour analyser les requêtes et réponses DNS et prendre des mesures pour atténuer les menaces. Le DNS protecteur empêche la distribution de malwares, de ransomwares, les tentatives de phishing et d'autres attaques centrées sur les liens web qui cherchent à diffuser des logiciels espions et des virus, et il bloque l'accès aux sites web malveillants. Le DNS protecteur peut être fourni sur site, déployé sur une infrastructure DNS interne, proposé sous forme de logiciel en tant que service (SaaS) ou de service cloud, ou encore, le plus souvent, sous la forme d'une solution hybride combinant les deux. Le recours à une solution hybride présente des avantages évidents. Ce modèle offre le plus haut niveau de résilience, garantissant qu'en cas de défaillance de la connectivité au service SaaS ou géré, il est possible de se rabattre sur un service sécurisé s'appuyant sur les capacités sur site. Il permet également une meilleure attribution des appareils grâce au déploiement sur site, tout en tirant parti de l'évolutivité et de la disponibilité de l'accès à distance d'un service cloud/SaaS.



Comme en témoigne le déploiement de plateformes de DNS protecteur par les gouvernements du monde entier, ainsi que l'initiative [DNS4EU](#) au sein de l'Union européenne, et le [service fourni par la CISA](#) pour le gouvernement américain, l'usage du DNS protecteur est désormais considéré comme une bonne pratique incontournable en matière de DNS.

L'utilisation d'un DNS protecteur devrait permettre d'obtenir les résultats suivants :

a. La Threat Intelligence et télémétrie

La surface d'attaque des entreprises évolue en permanence, il est donc primordial de pouvoir surveiller et perturber les communications malveillantes le plus tôt possible. Le DNS reste une constante dans ce paysage technologique en mutation, et il est particulièrement bien placé pour protéger les utilisateurs dans tous les environnements, des entreprises aux terminaux mobiles. De plus, le DNS constitue souvent la première interface avec les menaces, et permet de bloquer des attaques complexes en plusieurs étapes avant qu'elles ne progressent. En tant que point de contrôle de sécurité, le DNS n'est pas limité à un seul type de menace, contrairement à d'autres mécanismes de la pile de sécurité. Il peut protéger les utilisateurs et les entreprises contre les escroqueries, le vol d'identifiants, les ransomwares et l'exfiltration de données.

Cette approche requiert une threat intelligence, et la capacité à l'intégrer dans le résolveur DNS. Dans une infrastructure DNS, la threat intelligence est exploitée via des mécanismes tels que les zones de politique de réponse, ou RPZ, et peut être intégrée de manière fluide à la chaîne de résolution DNS via un certain nombre d'architectures.

b. Le filtrage de la résolution de noms

Le filtrage de la résolution de noms est un terme utilisé pour désigner l'infrastructure DNS qui applique une politique à la résolution DNS. Ces politiques sont généralement liées à la sécurité. Par exemple, une implémentation de DNS protecteur pourrait refuser de résoudre un ensemble de noms de domaine connus pour être utilisés dans des campagnes de phishing ou qui identifient une infrastructure de commande et de contrôle (C2) des malwares. Au lieu de résoudre ces noms de domaine en adresses IP ou en d'autres types de données, le DNS protecteur renvoie généralement une autre forme de réponse DNS, telle que NXDOMAIN (qui signifie « Domaine

inexistant »), indiquant que le nom de domaine recherché n'existe pas. Les implémentations de DNS protecteur enregistrent également les requêtes de noms de domaine qui déclenchent une politique, car ces requêtes peuvent indiquer une infection par des malwares ou d'autres activités malveillantes.

Le DNS protecteur est généralement mis en œuvre en utilisant des RPZ configurées sur un service DNS sur site, un service DNS récursif sécurisé basé sur le cloud, ou une combinaison des deux. Des services DNS récursifs sécurisés sont également disponibles sur Internet. Ces services proposent généralement un panneau de contrôle web qui permet aux administrateurs de personnaliser la politique de résolution appliquée aux requêtes des clients de l'entreprise. L'approche cloud offre une plus grande évolutivité, un meilleur stockage et une plus grande puissance de calcul, mais présente des inconvénients, tels qu'une perte de confidentialité, une latence plus élevée et des difficultés à attribuer rapidement et précisément les requêtes DNS à leur source. Les entreprises peuvent envisager d'utiliser une combinaison de services DNS sécurisés sur site et dans le cloud en tandem pour bénéficier des avantages de chacun. Le meilleur choix pour un déploiement DNS donné varie selon les besoins spécifiques du réseau et de ses utilisateurs.

c. Le DNS pour la forensique numérique et la réponse aux incidents

Les organismes publics et les entreprises réglementées devraient mettre en œuvre des mécanismes robustes de journalisation du trafic DNS afin de répondre aux exigences de conformité. La journalisation doit capturer à la fois le trafic DNS actuel et historique pour la forensique numérique et la réponse aux incidents. Ces journaux DNS devraient être intégrés aux autres journaux système pour faciliter la corrélation avec les autres journaux d'activité réseau, améliorant ainsi la visibilité et la traçabilité.

Dans les cas où la journalisation complète du trafic DNS est jugée trop gourmande en ressources, les entreprises peuvent envisager d'utiliser des solutions cloud, des méthodes d'enregistrement efficaces (par exemple, DNSTAP) ou une journalisation sélective. Cependant, il est impératif que les requêtes et réponses DNS associées à des domaines classés comme malveillants ou non autorisés par les services de DNS protecteur soient toujours enregistrées pour soutenir les objectifs de sécurité et de conformité. Pour être rapidement informées des requêtes susceptibles d'indiquer une infection ou une activité malveillante, les entreprises devraient intégrer les journaux du DNS protecteur de leurs serveurs de noms ou de leur service DNS récursif sécurisé à leur SIEM (gestion des informations et des événements de sécurité) ou à leur plateforme d'analyse des journaux.

4.2 La sécurisation du protocole DNS

Le protocole DNS est essentiel pour localiser les services nécessaires à la navigation web, à l'envoi d'e-mails et à d'autres applications critiques. Par conséquent, les plateformes de sécurité classiques, telles que les pare-feu de nouvelle génération, laissent souvent passer le trafic DNS sans entrave ni inspection. Les acteurs de la menace se tournent de plus en plus vers le DNS comme vecteur d'exfiltration. Selon l'Agence de cybersécurité et de sécurité des infrastructures (CISA) des États-Unis, « l'infrastructure DNS est un vecteur de menace courant pour les campagnes d'attaque ». Les acteurs de la menace intègrent souvent des données volées dans des paquets DNS, en s'appuyant sur l'infrastructure DNS pour relayer les données volées vers les serveurs DNS contrôlés par les acteurs de la menace. Les plateformes DNS sont idéalement placées pour évaluer les requêtes DNS récursives qu'elles reçoivent afin de détecter les tentatives d'exfiltration de données.

a. La protection de l'intégrité des services DNS

La protection de l'intégrité du protocole DNS est essentielle pour garantir la sécurité et la fiabilité des communications sur Internet. Le DNSSEC joue un rôle crucial en utilisant des signatures cryptographiques pour authentifier les réponses DNS, empêchant ainsi les attaques telles que l'empoisonnement du cache ou les interceptions de type « man-in-the-middle. » Par ailleurs, la signature de transaction (TSIG) renforce la sécurité du DNS en permettant l'authentification mutuelle et la vérification d'intégrité entre les serveurs DNS, à l'aide de clés secrètes partagées. Cela permet de sécuriser les transferts de zones et les mises à jour dynamiques contre les modifications non autorisées. La mise en œuvre de ces mécanismes, ainsi que de meilleures

pratiques telles que la limitation du débit, la surveillance des anomalies et l'application de contrôles d'accès stricts, contribue à maintenir la confiance et la résilience de l'infrastructure DNS face aux cybermenaces en constante évolution. De plus, les entreprises doivent s'assurer que les utilisateurs n'utilisent pas, délibérément ou par inadvertance, des services DNS publics sur Internet non autorisés.

b. L'utilisation du DNS chiffré et de l'authentification pour sécuriser le protocole

Traditionnellement, les communications entre les stub resolvers (résolveurs clients) et les serveurs DNS récursifs n'étaient pas chiffrées. Les messages DNS échangés entre les stub resolvers et les serveurs DNS sont encodés en binaire, mais cet encodage est bien connu et facile à décoder. Par conséquent, cette communication est exposée à des risques d'interception et de falsification, pouvant entraîner la fuite d'informations sensibles ou la redirection d'utilisateurs sans méfiance vers des sites malveillants.

Pour contrer ces menaces, l'Internet Engineering Task Force (IETF) a développé plusieurs extensions du DNS, regroupées sous le terme générique de DNS chiffré (Encrypted DNS). Tous ces protocoles chiffrent les communications entre les stub resolvers et les serveurs DNS récursifs et permettent éventuellement aux serveurs DNS récursifs de s'authentifier auprès des stub resolvers. Ces évolutions réduisent fortement les risques d'interception ou d'usurpation.

c. Les bonnes pratiques et hygiène DNS

Par ailleurs, l'exploitation de mauvaises configurations ou de l'expiration d'enregistrements ou de résolveurs DNS peut être simple à mettre en œuvre pour des acteurs malveillants, et compromettre gravement l'intégrité du DNS. Les cybercriminels ont prouvé que les attaques telles que le phishing ont beaucoup plus de chances de réussir si elles sont liées à des domaines appartenant à des organisations de confiance. Par conséquent, ils enregistrent souvent des domaines similaires qui ressemblent à l'entreprise ciblée, mais n'appartiennent pas à celle-ci. Plus préoccupant encore, une mauvaise hygiène des domaines faisant autorité peut permettre à des cybercriminels de prendre le contrôle de domaines appartenant à une organisation de confiance.

4.3 La sécurisation du service et de l'infrastructure DNS

Les appliances DNS, comme les autres appliances réseau, sont conçues pour être optimisées en termes de facilité de gestion, de sécurité et de performance. Les serveurs génériques ne peuvent pas offrir le même niveau d'optimisation que ces appareils, exposant ainsi les entreprises à des risques significatifs, étant donné l'importance du DNS en tant que service réseau.

Les entreprises utilisent fréquemment des serveurs Windows qui hébergent les services DNS et DHCP, souvent en conjonction avec Active Directory (AD), une autre brique essentielle de l'infrastructure d'identité. AD gère les accès des utilisateurs, les autorisations, et stocke des informations cruciales, ce qui en fait une cible privilégiée pour les cybercriminels.

Sans cette séparation des rôles, si un attaquant suit un chemin d'escalade classique et cible AD, cela compromet le service DNS et le réseau sur lequel il repose. Le DNS jouant un rôle de plus en plus important dans la stratégie de cybersécurité d'une organisation, un serveur DNS dédié sera essentiel pour atténuer ces risques.

De même, les cybercriminels cherchent régulièrement à exploiter des vulnérabilités dans les systèmes DNS, pouvant compromettre l'intégrité du service ou provoquer des attaques par déni de service (DoS).

Pour plus d'informations sur les DNS sécurisés, reportez-vous à la version la plus récente du document [NIST SP 800-81: Secure Domain Name System \(DNS\) Deployment Guide](#).

5. SYNTHÈSE ET RECOMMANDATIONS

Ce livre blanc met en lumière le rôle fondamental de l'infrastructure DNS dans la résilience numérique et la cybersécurité des entreprises. Il souligne la nécessité d'évaluer régulièrement les serveurs DNS pour s'assurer qu'ils disposent de capacités suffisantes et qu'ils sont configurés de manière optimale. Il explique également pourquoi le DNS constitue un socle essentiel de l'architecture de sécurité, au bénéfice de tous les clients qui utilisent l'infrastructure.

Pour faire face à l'évolution des menaces pesant sur la sécurité du DNS, voici des recommandations stratégiques à l'intention des responsables réseau et sécurité :

- Déployer un DNS protecteur partout où cela est techniquement possible, pour offrir des capacités de sécurité étendues à l'ensemble du réseau, incluant:
 - » Bloquer en temps réel tout trafic nuisible ou malveillant
 - » Filtrer les catégories de trafic non conformes aux politiques de l'entreprise
 - » Collecter et exploiter les données DNS (requêtes et réponses) en temps réel et en historique, pour faciliter les analyses forensiques et la réponse aux incidents
 - » Intégrer le DNS au reste de l'écosystème de sécurité, dans le cadre d'une stratégie de défense en profondeur ou du modèle Zero Trust
 - » Soutenir les obligations de conformité réglementaires ou contractuelles des entreprises, en bloquant le trafic vers les sites interdits (violation de droits d'auteur, restrictions légales, etc.)
- Chiffrer le trafic DNS, aussi bien en interne qu'en externe, chaque fois que cela est possible.
- Déployer des serveurs DNS dédiés pour réduire la surface d'attaque.
- Appliquer l'ensemble des recommandations techniques pour garantir la sécurité et la résilience des déploiements DNS et du protocole DNS lui-même.

Si vous souhaitez en savoir plus sur les menaces et les risques liés au DNS et sur les moyens de les atténuer, vous pouvez demander à Infoblox d'organiser un atelier gratuit sur la sécurité et de réaliser une évaluation de la sécurité DNS.

-
1. [CISA Launches its Protective DNS Resolver with General Availability for Federal Agencies](#). Eric Goldstein. Cybersecurity and Infrastructure Security Agency (CISA). 27 septembre 2022.
 2. [#StopRansomware: ALPHV Blackcat](#). Cybersecurity and Infrastructure Security Agency (CISA). 27 février 2024.
 3. [Cloudy with a Chance of Hijacking Forgotten DNS Records Enable Scam Actor](#). Jacques Portal. Renée Burton. Infoblox Threat Intel. Infoblox. 20 mai 2025.
 4. [Lookalike Domain Attacks Are on the Rise. Be on the Lookout for these Four Types](#). Renée Burton. Infoblox Threat Intel. Infoblox. 3 octobre 2023.
 5. [Loopy Lizard](#). Infoblox Threat Intel. Infoblox. Dernière consultation : 25 juillet 2025.
 6. [BDGAs: The Next Chapter in Domain Generation Algorithms](#) : James Barnett. Infoblox Threat Intel. Infoblox. 17 juillet 2024.



Infoblox réunit les réseaux, la sécurité et le cloud au sein d'une plateforme DDI sécurisée, offrant résilience et agilité aux entreprises. Notre plateforme s'intègre aux environnements hybrides et multicloud, automatise les services réseau essentiels et sécurise l'entreprise de manière proactive, tout en fournissant la visibilité et le contexte nécessaires pour agir rapidement, sans compromis.

Siège social
2390 Mission College Boulevard,
Ste. 501 Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com/fr