

Secutec Secure DNS

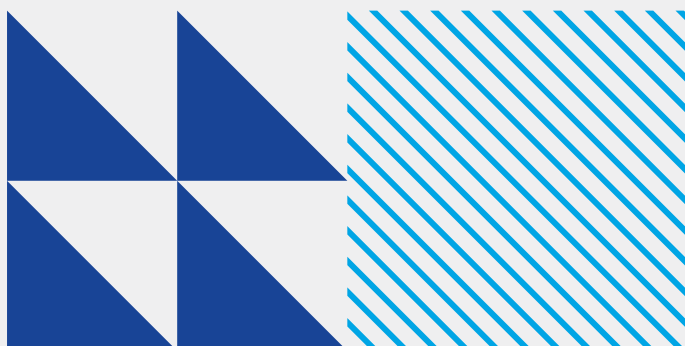
DÉTECTER ET BLOQUER LES NOUVELLES MENACES
PLUS RAPIDEMENT QUE VOTRE SOLUTION
DE SÉCURITÉ ACTUELLE



Le trafic Internet et les requêtes DNS constituent la principale porte d'entrée pour les logiciels malveillants, le hameçonnage, les rançongiciels et autres cyberattaques. Ne pas sécuriser vos connexions DNS pourrait donner lieu à n'importe quel cybercrime et générer des temps d'arrêt coûteux pour l'entreprise et des vols de données catastrophiques.

Secutec Secure DNS vous aide à surveiller et à protéger votre réseau d'entreprise, en détectant et en bloquant les requêtes DNS malveillantes que vos actuels antispam, firewall et proxys ne connaissent pas encore. C'est la solution de sécurité la plus efficace pour déjouer les logiciels malveillants, les attaques par hameçonnage ou toute autre cyberattaque.

Secutec Secure DNS est une solution de Secutec, un expert en cybersécurité au Benelux.



Qu'est-ce qu'un DNS ?

Lorsqu'un utilisateur de votre réseau tape dans son navigateur Web une **URL** (le nom d'un site Web), un **serveur de noms de domaine** (Domain Name Server, DNS) fait correspondre cette URL à une adresse IP. L'adresse IP appartient au serveur qui héberge le site Web demandé. Chaque URL sur Internet est associée à une adresse IP unique. Vous pouvez considérer un DNS comme l'**annuaire téléphonique d'Internet**, énumérant les URL et leurs adresses IP correspondantes. Une fois que le navigateur a reçu l'adresse IP correcte, il établit une connexion avec le serveur correspondant à l'adresse IP, pour transférer des informations.

91 % de tous les logiciels malveillants exploitent des connexions DNS non sécurisées

Les fournisseurs d'accès à Internet utilisent le plus souvent des connexions DNS sans les sécuriser. Cela signifie que votre entreprise utilise jour après jour les mêmes connexions non sécurisées. Il n'est pas étonnant que plus de 91 % des logiciels malveillants utilisent le DNS pour communiquer avec votre serveur, pour y dérober des données ou pour rediriger le trafic vers des sites malveillants. Aujourd'hui, les dangers sont très souvent cachés dans des applications, des documents et des sites Web innocents, invisibles aux firewalls et autres solutions de sécurité. L'ampleur de la cybercriminalité dans le monde ne cesse d'augmenter. Une attaque moyenne de logiciels malveillants coûte aux organisations environ 2750 USD*, soit une augmentation de 11 % d'une année à l'autre. Les attaques par hameçonnage et rançongiciel sont en augmentation.

3



Sans surveillance sécurisée du DNS, le réseau de votre entreprise est exposé à un large éventail de cybermenaces.



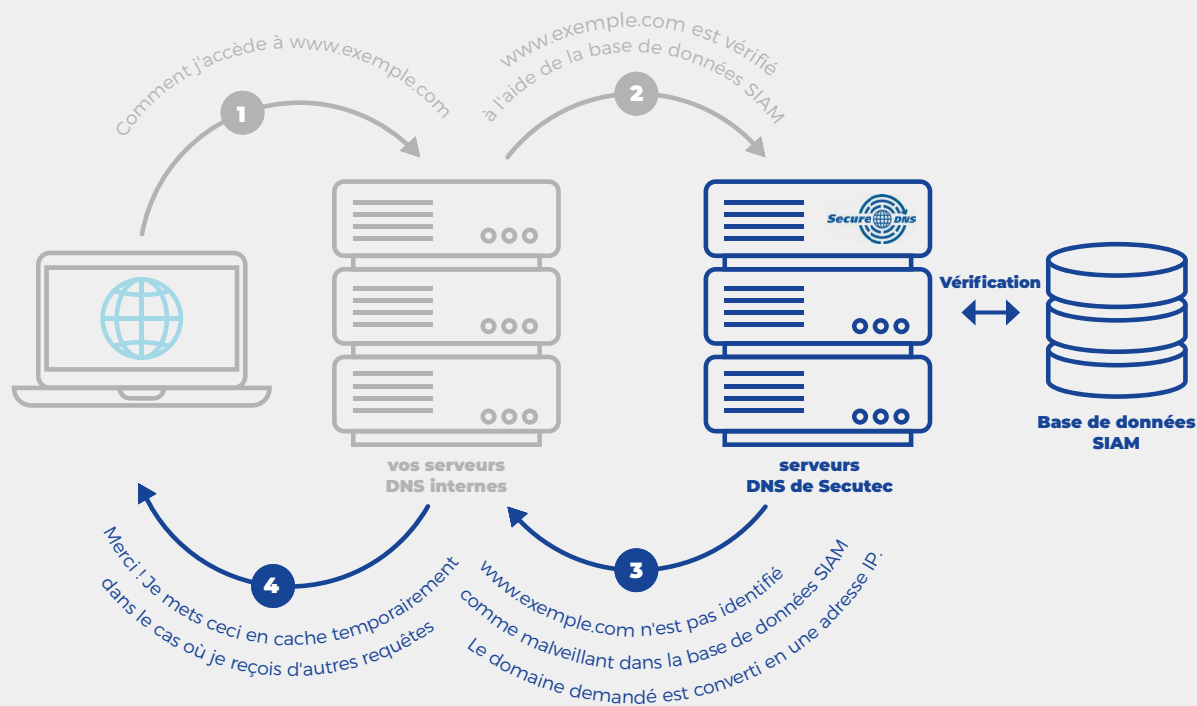
Geert Baudewijns – PDG Secutec

* Accenture Security Report 2019



En quoi Secutec Secure DNS surpasse-t-il tous les fournisseurs de cybersécurité ?

Secutec Secure DNS est une solution complémentaire à votre solution de sécurité actuelle. Nous sommes indépendants des fournisseurs et nous utilisons les connaissances locales et internationales en matière de cybersécurité.



En quoi consiste la base de données SIAM ?

La base de données SIAM, pour « Secutec Integrated Advanced Malware »,

La base de données SIAM est une base de données intelligente qui collecte des informations provenant de différentes sources à un stade très précoce. Secutec Secure DNS reçoit des informations de cette base de données SIAM pour savoir si un domaine est malveillant ou non.

Comment Secure DNS peut-il vous aider à avoir une longueur d'avance sur les cybermenaces ?

Secutec Secure DNS est un protocole rapide qui protège votre entreprise contre les noms d'hôtes malicieux. Il agit comme un logiciel de sécurité supplémentaire qui protège votre réseau contre les logiciels malveillants, les attaques par hameçonnage ou toute autre cyberattaque.

Secutec Secure DNS transmettra toutes les requêtes DNS de votre réseau à notre serveur Secutec Secure DNS. Ce serveur vérifiera la réputation du domaine de l'URL demandé. Si un utilisateur tente de naviguer vers un domaine qui a été bloqué, il ne pourra pas accéder à cette page Web, car la connexion ne sera pas établie. Si le domaine est sur la liste blanche ou

s'il n'est pas connu comme « malicieux », la connexion sera établie, permettant à l'utilisateur d'accéder au domaine demandé.

En bloquant les connexions malveillantes au niveau du DNS, nous ne bloquons pas uniquement le trafic Web qui devrait passer par vos proxys Web, mais également le trafic qui contourne le proxy.

Nous pouvons également rediriger le trafic Internet des travailleurs distants via le Secutec Secure DNS afin de nous assurer que tout le personnel de votre entreprise peut établir des connexions DNS sûres, quelle que soit leur localisation.

5



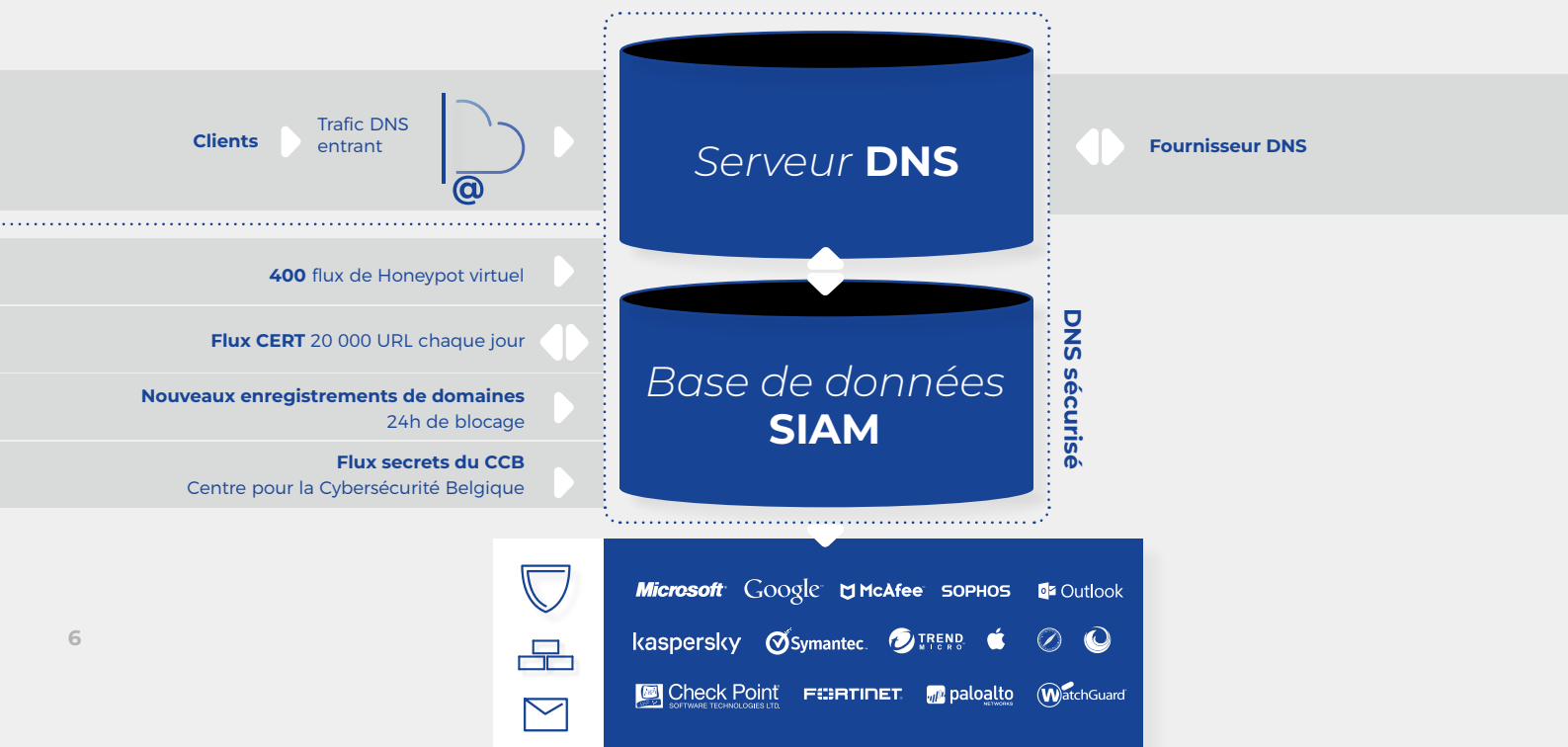
« Secure DNS fonctionne de manière simple et agréable ; je peux voir que notre antivirus fonctionne, mais Secure DNS offre une couche de protection supplémentaire ».



Pieter Verheyden - VAB



Un coup d'œil plus approfondi sur Secutec Secure DNS



6

- **Service Honeypot :** un « Honeypot » (ordinateur leurre) simule un système d'exploitation et permet à un attaquant de se connecter et d'exécuter des commandes ou de télécharger des logiciels malveillants. Notre réseau de Honeypots se compose de 12 centres de données et de 400 machines.
- **Flux CERT :** grâce à notre collaboration exclusive avec l'équipe fédérale belge de réponse aux urgences cybernétiques (Computer Emergency Response Team, CERT), nous avons accès à des informations portant sur 20 000 URL locales suspectes chaque jour.
- **Nouveaux enregistrements de domaines :** plus de 22 % de tous les domaines nouvellement enregistrés sont utilisés pour la cybercriminalité. C'est pourquoi nous bloquons les nouveaux domaines pendant 24 heures, ce qui nous donne le temps de les analyser correctement et de les recatégoriser si nécessaire.
- **Flux secrets du CCB :** nous échangeons des informations sur les cyberattaques locales avec le Centre pour la Cybersécurité de Belgique (CCB).
- **Navigateurs Web :** les données (les URL que nous identifions comme malicieuses) seront fournies à Microsoft, Google et Apple à partir des actions constatées sur Internet Explorer, Chrome, Firefox, Safari, etc.
- **Informations de plusieurs fournisseurs :** nous utilisons une base de données combinée de plus de 20 fournisseurs d'antivirus, de micrologiciels et d'antisipam.

Avantages de Secutec Secure DNS

Bloquer plus vite – détecter davantage – prévenir proactivement

- **Tableau de bord de rapportage** : afin de suivre vos performances, nous fournissons un tableau de bord détaillé de toutes les requêtes DNS et des menaces bloquées. Le tableau de bord de rapportage et d'alerte peut être entièrement personnalisé avec des rapports et des alertes personnalisés.
- **Service de sécurité très performant** : les domaines les plus malveillants sont bloqués à un stade plus précoce. Nous détectons également les menaces belges locales qui sont inconnues des autres fournisseurs de solutions de sécurité.
- **Sécurité complète du réseau** : Secure DNS protège chaque élément de votre réseau : PC, ordinateurs portables, serveurs, imprimantes, scanners, IOT, Blackbox, systèmes de minage de crypto-monnaies, etc.

La tranquillité d'esprit

- **Support technique dans les 24 heures** : vous avez besoin de notre aide ? Nos spécialistes en solutions sont là pour vous.
- **Mise en œuvre en moins de 60 minutes** : notre spécialiste en solutions configure vos paramètres DNS lors d'un appel distant. C'est si simple, et pourtant si efficient !

Une mise en œuvre aisée

- **Indépendante du système** : Secure DNS fonctionne avec n'importe quelle configuration informatique, de réseau ou de sécurité au sein de votre entreprise.
- **Intégration transparente dans l'infrastructure** : Secure DNS peut être facilement intégré à votre infrastructure informatique, qu'il s'agisse de DXL, PXGRID, SIEM ou autre.
- **Aucun matériel ni logiciel supplémentaire n'est nécessaire** : aucun temps d'arrêt, aucune interruption de service, ni aucun redémarrage de serveur ne sont nécessaires. Il suffit d'une modification de la configuration de vos paramètres DNS, sans charge supplémentaire sur votre système.

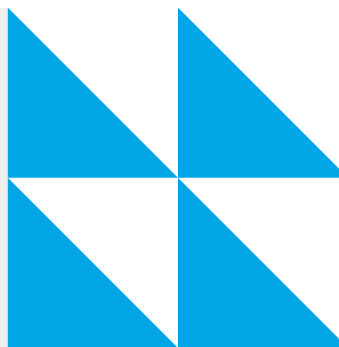
Une équipe en sécurité, partout d'où elle travaille

- **La garantie d'une navigation sûre sur le Web** : pour une sécurité informatique accrue.
- **Des connexions rapides assurées** : pas de latence ni de temps de traitement supplémentaire.
- **La cybersécurité à distance et mobile** : vous travaillez à domicile ou utilisez un autre réseau ? Nous pouvons rediriger le trafic internet des travailleurs distants par le biais du Secure DNS de Secutec.
- **Nous assurons la sécurité de tous vos appareils**, y compris ceux sur lesquels vous n'avez aucun contrôle, par exemple les écoles disposant d'un réseau d'invités pour étudiants.

7

Blocage de domaines non encore catégorisés

Il est crucial de réduire le délai entre l'enregistrement d'un nouveau domaine malicieux et sa mise sur liste noire, afin de minimiser les risques et les dommages potentiels pour les entreprises et les organisations. En particulier, les informations locales provenant de sources telles que le CCB et le CERT nous permettent de bloquer les domaines malveillants 12 à 24 heures avant les fournisseurs habituels d'antispam. En bloquant de manière proactive les nouveaux domaines pendant 24 heures, nous évitons les attaques par des nouveaux domaines, qui sont souvent utilisés pour les logiciels malveillants, le hameçonnage, les rançongiciels, etc. Et c'est exactement de cette manière que nous surpassons votre fournisseur actuel de logiciels anti-programme malveillant.



Soyez en sécurité, même en dehors de votre réseau ou en déplacement

Avec l'agent Secure DNS, toutes les connexions DNS des utilisateurs non-VPN se trouvant en dehors de votre réseau d'entreprise seront surveillées, vous apportant ainsi une plus grande tranquillité d'esprit. Toutes les requêtes DNS seront automatiquement transmises au serveur Secure DNS de Secutec, qui vérifiera la réputation du domaine de l'URL demandé. Si le domaine est sûr, la connexion sera établie. L'agent Secure DNS ne nécessite aucune installation matérielle. L'agent Secure DNS est la dernière nouveauté de notre solution Secure DNS. Il s'intègre dans notre philosophie d'innovation continue.

Pourquoi l'essayer vous-même ?

- **Solution multifournisseurs à prix abordable :** Secutec Secure DNS collecte des informations provenant de plus de 20 fournisseurs d'antivirus, de micrologiciel et d'antispam, de services Honeypot et d'agences locales de cybersécurité.
- **Surveillance automatique et alertes de détection :** Secutec Secure DNS surveille automatiquement toutes vos connexions DNS, 24 heures sur 24 et 7 jours sur 7. Lorsqu'il détecte un objet malicieux, vous en êtes immédiatement alerté.
- **Personnalisation :** chaque client est différent. C'est pourquoi nous proposons une approche à la carte. Vous avez besoin de modifications spécifiques, ou vous voulez bloquer certains domaines ? Faites-le nous savoir et nous le mettrons en œuvre.

Essayez Secutec Secure DNS gratuitement

Voulez-vous la solution la plus performante pour protéger le réseau de votre entreprise et vos précieuses données ?

Essayez Secutec Secure DNS pendant une période d'essai gratuite de 4 semaines.

Contactez-nous via sales@secutec.be ou
+32 3 877 82 93



Secutec Secure DNS

À vos marques, prêt, partez !

Implémenter Secure DNS en 4 étapes simples !

1. Créer un compte

Pour créer votre compte, nous avons besoin d'une liste des adresses IP publiques utilisées par votre entreprise.

2. Configuration

Configurer Secure DNS ne prend que 60 minutes. Après cela, vous êtes fin prêt !

3. Tests

Nous vous contacterons pour effectuer une requête de test et configurer vos redirecteurs DNS. Ceci garantira que les requêtes DNS sont reçues et résolues par notre service.

4. Prêt à fonctionner

Secutec Secure DNS est à présent installé. Connectez-vous au portail pour vérifier vos statistiques de trafic.

9

