opentext™ | Cybersecurity

LIVRE BLANC

Webroot DNS Protection

Protégez votre personnel et votre réseau en tout lieu contre les menaces basées sur le web

Internet fait partie de la vie professionnelle quotidienne d'aujourd'hui. Les employés ont besoin d'utiliser le web pour d'innombrables raisons professionnelles, mais sans un contrôle sécurisé, privé et visible du trafic internet, les entreprises peuvent être exposées à un large éventail de menaces de sécurité.

En effet, le système de noms de domaine (DNS) est un vecteur d'attaque très convoité par les acteurs malveillants. Le DNS est un système Internet permettant d'attribuer des adresses IP (Internet Protocol) à des noms de domaine. En d'autres termes, le DNS interprète les noms d'hôtes conviviaux en adresses IP conviviales.

Servant de carnet d'adresses pour l'internet, le DNS offre par défaut aux acteurs malveillants une visibilité sur le contenu de chaque requête, et l'intégrité de la requête peut être compromise. Il n'est donc pas surprenant que les cybercriminels utilisent de plus en plus les requêtes DNS pour lancer leurs attaques :

- Plus d'un tiers de toutes les attaques passent par le DNS[1]
- Le phishing et les logiciels malveillants sont les deux grandes attaques par DNS que subissent les entreprises[2]
- 43 % des entreprises ne sécurisent pas leur serveur DNS[2]

80 %

des logiciels malveillants utilisent le DNS pour lancer l'attaque.

S'il n'est pas protégé, le DNS pose un problème de sécurité pour les entreprises, car 80 % des logiciels malveillants utilisent le DNS pour déclencher une attaque et voler des données.[3] Par ailleurs, les entreprises proposant couramment un modèle de travail à distance et hybride, le pare-feu du réseau n'est plus la solution unique et infaillible pour la sécurité web. Collectivement, ces dynamiques de marché poussent les entreprises à adopter la sécurité DNS.

La sécurité DNS fournit une couche de protection entre un employé et l'internet en bloquant l'accès à des sites inappropriés grâce à l'exploitation de renseignements sur les menaces. Bien entendu, la bonne solution doit également maximiser la confidentialité sans compromettre la sécurité et l'efficacité opérationnelle. En adoptant la sécurité DNS, les entreprises peuvent mieux contrôler leurs réseaux tout en maintenant la sécurité et la confidentialité nécessaires pour protéger leurs utilisateurs (qu'ils soient à distance ou au bureau) contre l'accès à des sites malveillants.

Ce document explore les problèmes de sécurité que pose le DNS et la façon dont Webroot DNS Protection aide les entreprises à se protéger contre les risques des menaces basées sur le web.

L'accès à Internet est essentiel pour la vie professionnelle « en ligne » d'aujourd'hui. Mais quels risques de sécurité cela crée-t-il pour les entreprises ?

Le personnel à distance a besoin d'une sécurité supplémentaire

Avec la main d'œuvre à distance et hybride d'aujourd'hui, les utilisateurs emportent leurs appareils à la maison, sur la route et dans le café du coin. L'utilisation d'Internet n'étant plus limitée par le pare-feu de l'entreprise pour empêcher les mauvais acteurs d'entrer, cela augmente la surface d'attaque de l'environnement numérique de l'entreprise.

Les responsables de la sécurité s'accordent à dire que cette surface d'attaque élargie est préoccupante, 66 % des CISO indiquant que le travail à distance rend leur entreprise plus vulnérable aux cyberattaques.[4]

Des attaques réussies entraînant des pertes financières

Le DNS a été conçu avant tout pour répondre correctement et efficacement aux requêtes Internet, et non pour remettre en question leur intention. Par conséquent, les cyberattaques utilisant le DNS sont devenues l'une des menaces les plus importantes pour la vie professionnelle moderne.

En fait, près de 79 % des entreprises ont subi des attaques DNS, et celles-ci coûtent beaucoup d'argent. Chaque attaque DNS réussie coûte en moyenne 924 000 USD aux entreprises. [5]

Attaques entraînant des interruptions de service

Les cybercriminels utilisent toute une série de techniques pour déclencher leur attaque DNS et livrer leur charge utile. Une fois à l'intérieur, ils peuvent installer des logiciels malveillants, voler des données sensibles, modifier le code et même installer de nouveaux points d'accès.

Nous avons tous entendu des histoires d'horreur : une seule attaque réussie peut perturber les opérations et occuper les équipes informatiques pendant des semaines pour restaurer les systèmes avec succès. En effet, 82 % des entreprises ont subi des temps d'arrêt de leurs applications, qu'elles soient internes ou dans le cloud, en raison d'attaques DNS.[5]

Une approche moderne de la protection de l'accès à Internet : Webroot DNS Protection

Webroot permet aux entreprises d'aborder facilement les risques de sécurité DNS avec une protection précise et efficace pour tous vos utilisateurs, qu'ils travaillent à distance ou au bureau.

Webroot DNS Protection sécurise votre réseau et les utilisateurs itinérants en filtrant le DNS et en éliminant les logiciels malveillants et autres attaques basées sur le réseau. DNS Protection est alimenté par notre solution de pointe BrightCloud Threat Intelligence qui utilise la sixième génération de ML et d'AI pour fournir à votre entreprise un filtrage opportun et précis des domaines, des URL et des adresses IP. De plus, notre solution prend entièrement en charge DoH (DNS over HTTPS), afin de garantir que toutes les requêtes DNS cryptées sont sécurisées et précises.

Protéger votre entreprise avec Webroot DNS Protection

Le DNS résout simplement les requêtes Internet et les traduit en adresses IP (Internet Protocol) uniques. Les mauvais acteurs exploitent ce service en texte clair de différentes manières. Avec Webroot DNS Protection, votre entreprise peut se protéger contre les risques de sécurité inhérents au DNS.

Webroot DNS Protection vous permet de contrôler le réseau de votre entreprise tout en maintenant la sécurité et la confidentialité nécessaires pour protéger vos utilisateurs (distants et itinérants) contre l'accès à des sites malveillants.

Protection à distance

Webroot fournit une couche de sécurité DNS efficace pour protéger votre personnel à distance. Grâce à l'agent DNS Protection, toutes les requêtes DNS (y compris celles des utilisateurs distants) peuvent être filtrées et enregistrées, quelle que soit la connexion Internet utilisée. Des politiques peuvent être définies au niveau du groupe ou de l'individu pour restreindre l'accès aux domaines malveillants et non autorisés et arrêter les violations avant qu'elles n'aient un impact sur le réseau.

Filtrage précis

DNS Protection est alimenté par notre BrightCloud Threat Intelligence (BCTI), qui utilise la sixième génération de ML et d'IA pour fournir un filtrage DNS opportun et précis. Il filtre avec précision les requêtes DNS, bloquant les sites de phishing et de logiciels malveillants en temps réel, tout en permettant aux entreprises d'éviter le fardeau administratif des faux positifs.

Prise en charge du DNS sur HTTPS (DoH)

Avec l'avènement de DoH, le trafic DNS crypté est devenu difficile à contrôler. Webroot résout ce problème pour les entreprises grâce à sa solution qui prend entièrement en charge DoH. L'agent distant de Webroot DNS Protection exploite également DoH pour toutes les communications avec le noyau, fournissant une résolution DNS sécurisée tout en garantissant que toutes les communications sont chiffrées et proviennent d'une source fiable. Cela permet aux entreprises de s'aligner sur les recommandations de la NSA.

Options de déploiement flexibles

Webroot DNS Protection offre deux options de déploiement : en tant que solution autonome ou en combinaison avec Webroot Endpoint Protection (EPP). L'agent DNS Protection peut être installé directement sur un système ou géré par Webroot EPP. L'option Webroot EPP offre une approche intégrée, permettant aux entreprises de gérer de manière centralisée la sécurité des terminaux et des DNS. Cette combinaison peut contribuer à réduire d'environ 33 % les menaces qui pèsent sur votre entreprise. L'option DNS autonome permet aux entreprises de déployer Webroot DNS Protection en tant que couche de sécurité tout en exploitant séparément les investissements existants dans une solution EPP ou EDR tierce.

Facilité de gestion

Il est facile de gérer DNS Protection à partir de la console de gestion Webroot, qui offre un point de vue unique pour la gestion de tous les produits Webroot. Grâce à la console, les clients peuvent rapidement déployer et gérer DNS Protection, ce qui permet aux équipes informatiques et de sécurité de réduire le temps d'administration et d'améliorer l'efficacité.

Réduire les coûts du service d'assistance

DNS Protection empêche les menaces de pénétrer dans votre entreprise au niveau de la couche DNS, ce qui réduit le nombre de compromissions, d'infections et les coûts de résolution associés auxquels votre équipe IT doit faire face. Cela permet de réduire le nombre d'appels à votre service d'assistance en raison d'infections.

Success story : Un MSP réduit de 40 % le nombre d'appels au service d'assistance grâce à Webroot DNS Protection

Fondée en 1986, Sedona Technologies est une grande société de services informatiques et d'ingénierie bien établie qui dispose d'une division de services gérés performante. L'entreprise possède des bureaux dans plus de 30 villes américaines et réalise un chiffre d'affaires annuel de plus de 110 millions de dollars.

Défis en matière de sécurité DNS

En cherchant à ajouter une protection au niveau du réseau aux offres de services de sécurité du MSP, ils ont rencontré des obstacles lors de la phase de déploiement d'une solution basée sur un proxy. Les clients de Sedona dont les utilisateurs effectuaient des requêtes DNS vers des sites malveillants étaient fréquemment infectés.

« À l'origine, nous n'avions pas opté pour une solution DNS, mais plutôt pour une solution basée sur un proxy. Mais il est devenu très difficile de travailler avec notre partenaire. Le nombre d'étapes nécessaires pour que le produit soit opérationnel pour un client a exigé beaucoup plus de ressources qu'il n'aurait dû ».

Cela a conduit Sedona à rechercher d'autres options pour protéger ses clients tout en économisant des ressources.

Comment Webroot DNS Protection a apporté des avantages

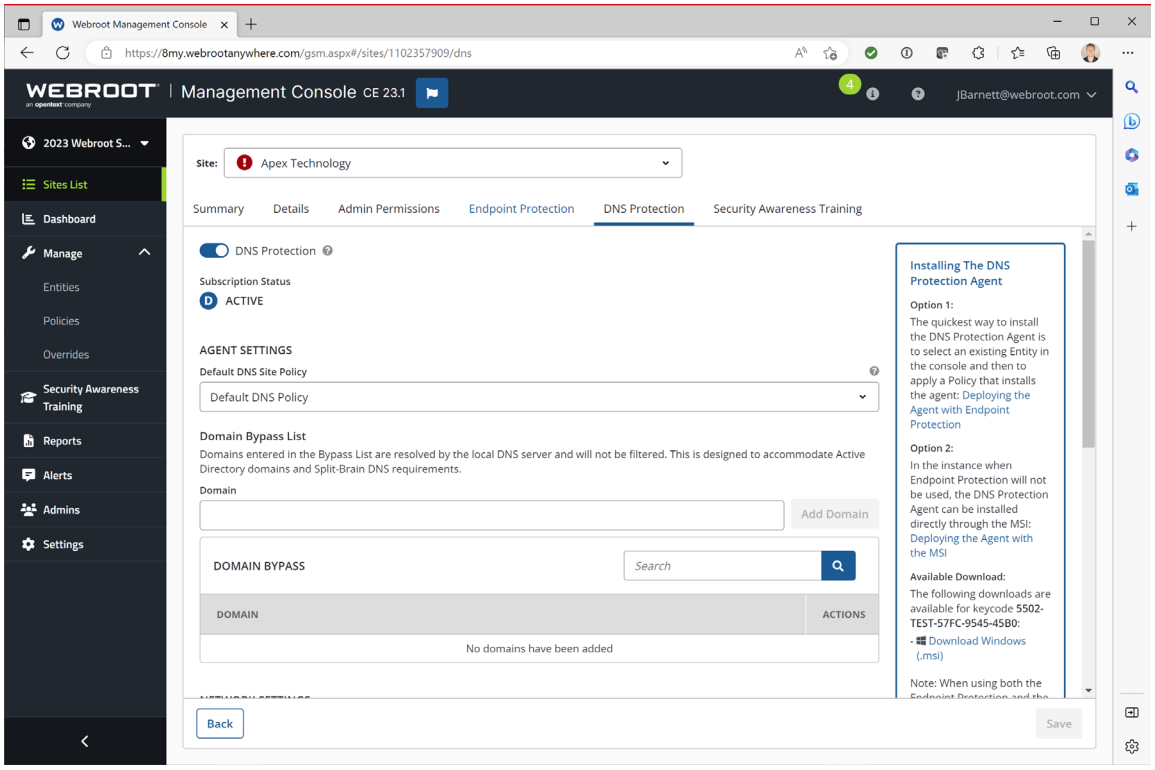
« Nous avions besoin d'une solution simplifiée et allégée. Nous avons évalué un grand nombre de produits de fournisseurs et, en fin de compte, la décision d'opter pour Webroot a été basée sur l'expérience de travailler directement avec le personnel. Vous avez été à l'écoute. Il n'y a pas eu de retard. Le niveau de service était tout simplement supérieur à tout le reste.

Que s'est-il passé après que Sedona soit passé à Webroot DNS Protection ?

- 270 menaces Internet bloquées quotidiennement sur l'ensemble de sa base de clients
- 51 tentatives de spear phishing bloquées mensuellement au cours d'un seul trimestre
- 40 % d'appels au service d'assistance en moins

« Pour nos clients équipés de DNS Protection, les appels au service d'assistance sont réduits de près de 40 %. »

- Jason Ballard
Responsable des solutions informatiques
Sedona Technologies



1. Global Cyber Alliance, 2021
2. EfficientIP 2022 Global DNS Threat Report, réalisé par IDC
3. Cyber Theory. The Threats from Unsecured DNS and Domains (Les menaces des DNS et domaines non sécurisés).
4. Verizon. Indice de sécurité mobile. 2022.
5. Webinar Care. Statistiques de sécurité DNS 2023. Janvier 2023.

opentext™ | Cybersecurity

OpenText Cybersecurity fournit des solutions de sécurité complètes pour les entreprises et les partenaires de toutes tailles. Assurant la prévention, la détection et la réponse, ainsi que la reprise, l'investigation et la conformité, notre plateforme unifiée de bout en bout permet aux clients de renforcer leur cyber résilience via un portefeuille de sécurité holistique. Grâce aux informations exploitables provenant de notre veille contextuelle et en temps réel sur les menaces, les clients d'OpenText Cybersecurity bénéficient de produits extrêmement efficaces, d'une expérience conforme et d'une sécurité simplifiée pour gérer les risques commerciaux. WP_021323