

OpenText Core DNS Protection

Empêchez les attaques en contrôlant totalement le DNS

Fonctions

- Blocage des sources DNS alternatives ou non autorisées
- Protection contre l'accès aux domaines malveillants ou aux serveurs de commande et de contrôle (C&C)
- Chiffrement de toutes les requêtes DNS pour éviter les détournements DNS
- Consignation de toutes les requêtes DNS pour identifier les menaces, les vulnérabilités et les comportements suspects
- Prévention de l'exfiltration des données via le DNS

Avantages

- Réduction des logiciels malveillants de 27,1 % de plus par rapport à l'utilisation d'un antivirus seul (Rapport de 2023 sur les menaces d'OpenText Cybersecurity)
- Blocage de l'exfiltration des données et de la prolifération des logiciels malveillants via le DNS
- Protection des employés hybrides et à distance sur n'importe quel réseau
- Déploiement facile avec des résultats immédiats ; entièrement transparent pour les utilisateurs

Le DNS est la base !

Le DNS joue un rôle crucial pour accéder à toutes les ressources sur les réseaux et sur Internet. Il est donc essentiel de contrôler le DNS pour que le réseau soit stable et sécurisé. Malheureusement, il est difficile de contrôler le DNS de manière efficace depuis l'apparition du chiffrement DNS, la mise en place du travail hybride permettant de travailler « n'importe où » et désormais, les requêtes DNS au niveau des processus, qui peuvent être utilisées par des logiciels malveillants pour contourner les contrôles au niveau du système.

Voir plus loin que le navigateur

Le filtrage DNS est souvent associé à la navigation sur Internet et au filtrage des requêtes DNS correspondantes. Malheureusement, le simple filtrage des requêtes de navigateur est insuffisant, car les logiciels malveillants et les autres attaques peuvent détourner le DNS au niveau du processus, en contournant les contrôles de navigateur pour favoriser les attaques. En filtrant le DNS pour tous les processus, OpenText™ Core DNS Protection peut également parvenir à bloquer la communication avec les serveurs C&C, empêcher l'exfiltration des données et augmenter la visibilité grâce à des journaux complets permettant de lutter contre les infections.

DNS Leak Prevention et DoH

OpenText Core DNS Protection Leak Prevention demeure le leader du secteur en matière d'innovation, en créant de nouvelles méthodes pour contrôler et sécuriser le DNS grâce à trois brevets déjà déposés et d'autres à venir.

Notre fonction brevetée DNS Leak Prevention, par exemple, agit comme un pare-feu DNS au niveau du périphérique pour empêcher tout processus d'effectuer la résolution DNS en dehors de l'agent.

Leak Prevention ?

Chose which types of requests you want to prevent.

☒ Standard DNS Requests ?
 ☒ DoH Requests ?
 ☒ DoT Requests ?

Exclusions ?

×

Only IPv4 addresses are supported 1/50

Remove All

COMPLETE PREVENTION (53, 443 AND 853)

Prevents DNS leaks caused by applications, processes, and VPNs configured to use alternate DNS resolvers through standard DNS, DoH (DNS over HTTPS) and DoT (DNS over TLS).

Helps to ensure that DNS requests are managed, logged, and filtered by the DNS Protection Agent. This configuration blocks all three DNS protocols including standard DNS, DoT, and DoH.

OpenText Core DNS Protection a été la première solution DNS de protection à relever le défi du chiffrement DNS ou DNS over HTTPS (DoH), qui peut contourner les configurations système en permettant la résolution DNS chiffrée à partir de sources alternatives. Grâce au suivi et au contrôle de l'accès aux fournisseurs DoH, OpenText Core DNS Protection interrompt les connexions non autorisées en cas de tentatives de requêtes DNS.

Si le DoH a besoin de contrôle, il s'agit toutefois d'un mécanisme très puissant pour la résolution DNS. L'agent OpenText Core DNS Protection exploite pleinement le DoH pour permettre une résolution DNS fiable et chiffrée, garantissant ainsi que toutes les requêtes DNS restent privées au sein de votre entreprise et invisibles pour les fournisseurs de services Internet (ISP) ou tiers indiscrets.

Mise en oeuvre aisée et transparence pour les utilisateurs

OpenText Core DNS Protection est une solution SaaS native du cloud qui a fait ses preuves en matière de sécurité, de fiabilité, d'évolutivité et de performances. Qu'il s'agisse de protéger l'ensemble du réseau ou uniquement les périphériques mobiles, la console Web fournit des contrôles de stratégies DNS intuitifs ainsi que des rapports. L'agent DNS Protection peut être simplement envoyé aux périphériques en tant que MSI ou (en option) en tant qu'extension d'OpenText™ Core Endpoint Protection. Les administrateurs peuvent contrôler la manière dont toutes les requêtes DNS sont consignées, ce qui permet de choisir quelles informations sont capturées pour se conformer au RGPD.

Réseau ou périphériques mobiles

La solution OpenText Core DNS Protection peut être configurée afin de sécuriser l'ensemble du réseau, y compris le Wi-Fi d'entreprise, le LAN et même le Wi-Fi invité, réduisant ainsi les menaces pesant sur les périphériques BYOD ou tout autre terminal où vous ne pouvez pas ou ne souhaitez pas installer d'agent.

Pour les terminaux mobiles, l'agent OpenText Core DNS Protection assure le contrôle du DNS. L'agent achemine toutes les requêtes DNS via nos serveurs DNS renforcés, en veillant à l'application du filtrage, de la consignation et des contrôles de sécurité dont vous avez besoin pour permettre le travail hybride et à distance, quel que soit le réseau utilisé par le périphérique.

Réduction du nombre de faux positifs

Les mauvaises sources de renseignements sur les menaces sont souvent à l'origine des faux positifs. Ces derniers nuisent à l'expérience utilisateur en entraînant l'interruption des workflows, un véritable casse-tête pour les administrateurs. OpenText Core DNS Protection limite le nombre de faux positifs avec l'aide de notre plateforme propriétaire OpenText™ Threat Intelligence. La fonctionnalité éprouvée de machine learning de sixième génération d'OpenText fournit des renseignements de premier ordre sur les menaces, ainsi qu'une fiabilité, une précision, une profondeur et une rapidité inégalées.

Meilleure résilience contre les cyberattaques

OpenText Cybersecurity réunit les meilleures solutions de sa catégorie pour aider votre entreprise à rester cyberrésiliente. OpenText peut vous aider à prévenir les menaces et à vous en protéger, et vous permettre d'atténuer les risques en détectant et en réagissant rapidement, puis en récupérant les données en toute simplicité. Vous réduisez ainsi leur impact et assurez votre conformité au regard de l'évolution des réglementations.

Pour en savoir plus ou demander une version d'essai, [rendez-vous sur OpenText Core DNS Protection](#).

OpenText Cybersecurity fournit des solutions de sécurité complètes pour les entreprises et les partenaires de toutes tailles. De la prévention à la détection, en passant par la réponse, la récupération, l'enquête et la conformité, notre plateforme unifiée de bout en bout aide les clients à développer leur cyberrésilience via un portefeuille de sécurité global. Grâce à des informations exploitables issues de nos renseignements en temps réel et contextuels sur les menaces, les clients d'OpenText Cybersecurity bénéficient de produits hautement efficaces, d'une expérience conforme et d'une sécurité simplifiée pour les aider à gérer les risques métiers. DS_030623