# OpenText Core DNS Protection

DNSを完全に制御することで攻撃を防止

## 特長

- DNSの代替ソースまたは不正なソースをブロック
- 悪意のあるドメインまたはコマンドアンドコントロール(C&C)サーバーへのアクセスを防止
- すべてのDNS要求を暗号化してDNSハイジャックを防止
- すべてのDNS要求をログに記録して、脅威、脆弱性、疑わしい動作を特定
- DNSを介したデータ流出を停止

## 利点

- アンチウイルス単独と比較してマルウェアをさらに27.1%削減(OpenText Cybersecurity Threat Report 2023)
- DNSを介したデータ流出やマルウェアの拡散を防止
- あらゆるネットワーク上のリモートワーカーとハイブリッドワーカーを保護
- 導入が簡単で、迅速に結果を得られる一方、ユーザーへの透明性が高い

## 常にDNSが重要!

DNSは、ネットワークやインターネット上でアクセスされるすべてのものに不可欠であり、安定した安全なネットワークにはDNSの制御が不可欠です。残念ながら、DNS暗号化の出現、ハイブリッドワークの「どこからでも仕事ができる」という現実、そして現在ではマルウェアがシステムレベルの制御をバイパスするために使用できるプロセスレベルのDNS要求など、DNSの効果的な制御はますます困難になっています。

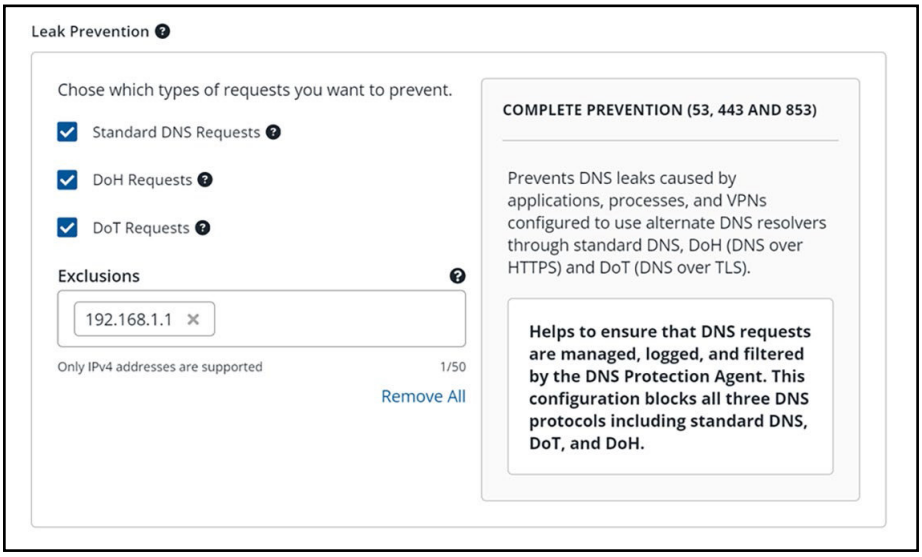
## ブラウザーを超えて

DNSフィルタリングは、多くの場合、インターネット上のWebサイトを閲覧し、それに対応するDNS要求をフィルタリングすることに関連しています。残念ながら、ブラウザーの要求をフィルタリングするだけでは不十分です。マルウェアやその他の攻撃は、プロセスレベルでDNSを利用する可能性があり、ブラウザーの制御をバイパスして攻撃を進行させるからです。OpenText™ Core DNS Protectionはすべてのプロセスの DNSをフィルタリングすることで、C&Cサーバーとの通信をブロックし、データ流出を防ぎ、包括的なログで可視性を高めることで、感染に対抗します。

## DNS Leak PreventionとDoH

OpenText Core DNS Protection Leak Preventionは、DNSを制御および保護するための新しい方法を開発し、技術革新で業界をリードし続けています。当社は3件の特許を取得しており、さらに多くの特許が申請中です。

たとえば、特許取得済みのDNS Leak Prevention機能は、デバイスレベルのDNSファイアウォールとして機能し、エージェントの外部でDNS解決につながるプロセスをすべて停止します。



OpenText Core DNS Protectionは、暗号化DNSまたはDNS over HTTPS (DoH)の課題に対処する最初の保護DNSソリューションです。代替ソースからの暗号化DNS解決を可能にすることでシステム構成をバイパスできます。DoHプロバイダーへのアクセスを追跡および制御することにより、OpenText Core DNS ProtectionはDNS要求が試みられたときに不正な接続を停止します。

DoHは制御を必要としますが、DNS解決のための非常に強力なメカニズムでもあります。OpenText Core DNS Protectionエージェントは、信頼性の高い暗号化されたDNS解決のためにDoHを活用します。そのため、すべてのDNS要求が組織内に留まり、ISPや他の覗き見から保護されます。

## 実装が容易でユーザーへの透明性が高い

OpenText Core DNS Protectionは、クラウドで開発されたSaaSソリューションであり、安全性、信頼性、および拡張性が高く、高性能であることが実証されています。ネットワーク全体を保護するかローミングデバイスを保護するかにかかわらず、Webベースのコンソールにより直感的なDNSポリシー制御とレポート作成が可能です。DNS Protectionエージェントは、MSIとして、またはオプションでOpenText™ Core Endpoint Protectionの拡張として、デバイスに簡単にプッシュできます。管理者は、すべてのDNS要求をログに記録する方法を制御でき、GDPRに準拠するためにキャプチャされる情報を構成できます。

## ネットワークまたはローミングデバイス

OpenText Core DNS Protectionは、企業のWi-Fi、LAN、さらにはゲストのWi-Fi接続を含むネットワーク全体を保護するように構成でき、エージェントが使用不可能または望ましくないBYODやその他のデバイス上の脅威を軽減します。

ローミングデバイスの場合、OpenText Core DNS Protectionエージェントが DNSを確実に制御します。エージェントは、すべてのDNS要求を当社の強化されたDNSサーバーを介してルーティングし、デバイスが使用しているネットワークに関係なく、ハイブリッドワークとリモートワークを強化するために必要なフィルタリング、ログ記録、およびセキュリティ制御を強制します。

## 誤検出の防止

誤検出は、多くの場合、脅威インテリジェンスの不足によって引き起こされます。ワークフローが中断することでユーザーに影響を与え、管理者にとって頭痛の種となります。OpenText Core DNS Protectionは、当社専有のOpenText™ Threat Intelligenceプラットフォームを活用することで、誤検出を最小限に抑えます。OpenTextの成熟した第6世代機械学習は、信頼性、正確性、深層性、適時性を備えた比類のない脅威インテリジェンスを提供します。

## サイバー攻撃に対する組織の災害耐性を強化

OpenText Cybersecurityは業界最高レベルのソリューションを統合し、企業のサイバーレジリエンスを支援します。OpenTextは、第一に脅威の発生を防止および保護し、迅速に検出して対応することで影響を最小限に抑え、データをシームレスにリカバリして影響を軽減するとともに、変化する規制への適応と準拠を支援します。

詳細または評価版のリクエストについては、OpenText Core DNS Protectionをご覧ください。

OpenText Cybersecurityは、あらゆる規模の企業とパートナー様を対象に、包括的なセキュリティソリューションを提供しています。予防から検知、リカバリ対応、調査、コンプライアンスに至るエンドツーエンドの統合プラットフォームにより、包括的なセキュリティポートフォリオを通じてサイバーレジリエンスの構築をサポートします。コンテキストに基づくリアルタイムの脅威インテリジェンスから得られた実用的なインサイトを活用できるため、OpenText Cybersecurityのお客様は、優れた製品、コンプライアンスが確保されたエクスペリエンス、簡素化されたセキュリティというメリットによって、ビジネスリスクを管理できます。DS_030623