opentext™ | Cybersecurity

データシート

DNS保護：Webroot® DNS Protection

セキュリティとプライバシーの両方を守る、保護のためのフィルタリング

ドメインネームシステム(DNS)はインターネットのアドレス帳です。フルマネージドのDNSセキュリティソリューションはあらゆる組織のサイバーレジリエンス戦略に不可欠な要素であり、インターネット接続のセキュリティとプライバシーを保護するための基盤となります。DNSリクエストからはリクエストの内容を読み取ることができるため、悪意のある攻撃者がDNSリクエストを標的とするケースが増えており、攻撃を受けたリクエストは整合性が損なわれる可能性があります。攻撃者はDNSリクエストからユーザーが使用しているアプリケーションを知ることができるだけでなく、どのWebサイトを訪問しているかも暗号化されていない情報として取得できます。

Webroot® DNS Protectionは、NSA (アメリカ国家安全保障局)の推奨事項に従ってDNS over HTTPS (DoH)をフルサポートするとともに、DNSリクエストのフィルタリングと整合性確保を継続的に実施する制御のためのオプションを通じてプライバシーとセキュリティの保護を提供します。また、DNSの可視性とログ収集のレベルをカスタマイズできます。Webroot® DNS Protectionは、セキュリティ強化されたWebrootのDNSリゾルバーのインフラストラクチャを利用してGoogle Cloud™内に安全にホストされるため、Googleが全世界のデータセンターを通して提供しているアクセシビリティ、信頼性、安定性、パフォーマンスを活用できます。

ネイティブDoHのプライバシーとセキュリティを提供するDNSサービス

世界的に認められたリアルタイム脅威インテリジェンスを搭載

SaaSソリューションとして設計され、低遅延、高い信頼性、安全なホスティングを保証するWebroot® DNS Protectionは、サイバー攻撃に対する組織のレジリエンス強化という目的に特化して構築されています。SaaSソリューションであるため、スタンドアロンのDNS Protectionエージェントとしても、Webroot Endpoint Protectionと組み合わせても展開できます。いずれの展開方法でも、クラウドベースのWebroot管理コンソールから、ネットワークデバイスでもローミングデバイスでも簡単かつシンプルな方法ですばやく実行できます。展開が完了すれば、DoHを介するすべてのDNSリクエストがネットワークユーザーおよびローミングユーザーのエージェントレベルでフィルタリングされるようになります。管理者がすべてのDNSリクエストのログ記録方法を制御できるため、GDPRに準拠した形でプライバシーを構成しながら、リクエスト全体を遺漏なくフィルタリングすることができます。

Webroot® DNS Protectionは、BrightCloud® Threat Intelligenceによる第6世代のマシンラーニングを活用してWebサイトのドメインを調査し、各Webサイトをそれぞれ正確なカテゴリに分類します。BrightCloud® Threat Intelligence Servicesは、ドメイン、URL、IP、ファイル、モバイルアプリなどの間でデータを相互に関連付けて、インターネット上の脅威の状況を包括的に可視化し、その状況を継続的に更新しながら表示します。

メリット

- DNSベースのネットワークフィルタリングサービスにより、ダウンロードされるマルウェアを最大75%削減
- インターネットの使用状況の全体を可視化し、インターネットに対して行われたすべてのリクエスト(DNS over http (DoH)の制御を含む)に関するインサイトを提供
- 悪意のある、または疑わしいインターネットロケーションに対する応答の数を減らすことで感染を抑制
- 強制可能なきめ細かいアクセスポリシー
- ローミング保護: Windowsエージェントを使用して、ローミングユーザーを対象とする一貫したオフネットワークフィルタリングを実行
- 柔軟な展開オプション: スタンドアロンのDNS Protectionエージェントとしても、Webroot Endpoint Protectionと組み合わせても展開可能

ネットワークデバイスでもローミングデバイスでもすばやく簡単に展開できるSaaSソリューション

特徴

Webroot® DNS Protectionでは、すべてのDoHインターネットリクエストを、安全性の高いGoogle Cloud™サービスでホストされているセキュリティ強化されたWebrootのDNSサーバーを介して送信することで、DoHによるプライバシーとセキュリティ上のメリットを最大限に活用しつつ、DNSリクエストを効果的に保護および管理するために必要なログ収集、可視性、フィルタリング、セキュリティ制御の機能を利用できるようになります。アプリケーションがDNSリクエストを直接暗号化し始めると、ファイアウォールはインターネット上でアクセスされる要素に対する可視性と制御を失います。Webroot® DNS ProtectionはDoHプロバイダーを追跡してフィルタリングし、最初にリクエストが行われたときにその接続を停止して、ユーザーが制御できるようにします。

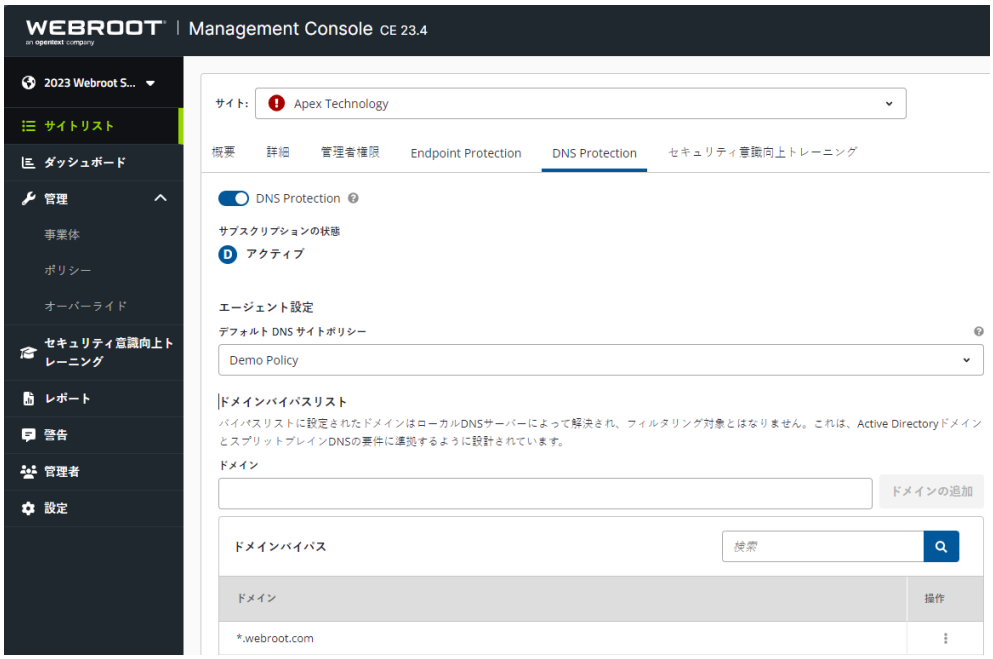
DoHを介したすべてのDNSリクエストは、ネットワークユーザーおよびローミングユーザーのエージェントレベルでフィルタリングされます。Webroot® DNS Protectionを利用することで、組織によるすべてのDNSリクエストの機密性が維持され、脅威アクターによる不正な閲覧から保護されます。Webroot® DNS Protectionでは、企業のWi-Fi、LAN、さらにはゲストWi-Fi接続を介してインターネットにアクセスする、すべての種類のデバイス(Windows、Linux、Apple®、Android®のデバイスなど)を保護できます。またパートナーや顧客も、静的IPアドレスを必要とせずにネットワーク全体を容易に保護できるようになります。Webroot® DNS Protectionは、一般的なVPNソリューションを介して接続する際のDNSの機能性を強化します。

サイバー攻撃に対する組織のレジリエンス強化に特化したソリューション

ポリシーベースのきめ細かなアクセス制御によって侵入の件数を削減

OpenText Cybersecurityはクラス最高のソリューションを結集することで、ビジネスにおけるサイバーレジリエンス確保を可能にします。CarboniteとWebrootは、ユーザーが脅威の発生を未然に防いでシステムを保護し、迅速な検出と対応によってサイバー攻撃の影響を最小限に抑え、シームレスなデータ復旧によって被害を軽減するとともに、絶えず変化する規制にも適応し準拠できるように支援します。

Webroot® DNS Protectionはネットワーク、グループ、デバイスブラウザ、ユーザー、およびローミングユーザーのレベルでのDoHをフルサポートしており、可視性とDNSフィルタリングによるアクセス制御のメリットを提供します。またインターネットの使用状況の全体が可視化され、インターネットに対して行われたすべてのリクエストに関するインサイトが提供されるため、管理者はより多くの情報に基づいてアクセスポリシーを決定できるようになります。悪意のある、または疑わしいインターネットロケーションに対する応答の数を減らすことで、感染の発生を抑制できます。このような仕組みによってDNSフィルタリングは侵入および感染の件数と関連する修復コストを大幅に削減します。強制可能なきめ細かいアクセスポリシーを利用することで、管理者は個人、グループ、またはIPアドレスに基づく高度でカスタマイズ可能なポリシー制御を通じて、スタッフの生産性や雇用主の注意義務、さらにはHRやコンプライアンスの要件にも対処できるようになります。以上のメリットを総合的に提供するWebroot® DNS Protectionは、セキュリティや運用効率を損なうことなくプライバシーを維持できるよう組織を支援します。



opentext™ | Cybersecurity

お問い合わせ：オープンテキスト株式会社 info.sdm.b2b@opentext.com