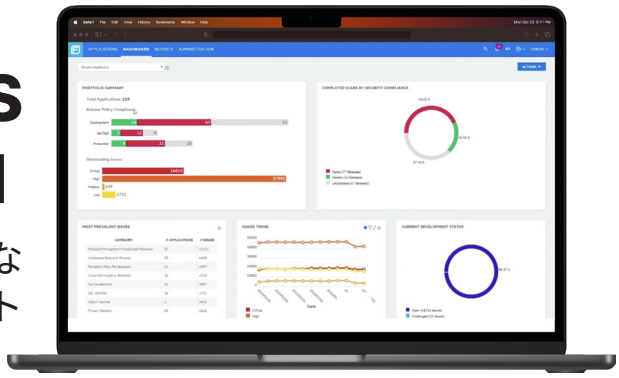
MSP が OpenText Core DNS Protection を販売すべき理由

ユーザーフレンドリーかつスケーラブルな OpenText Core DNS Protection でクライアントセキュリティを向上



サイバー脅威は MSP と SMB にとって非常に危険です。MSP は、DNS（ドメインネームシステム）Protection を使用することで、インターネットベースの攻撃がエンドポイントまたはネットワークに到達する前に、それらから SMB 顧客を保護する保護層を強化できます。インストール、管理、拡張が簡単なソリューションでインターネットを管理し、MSP ビジネスを成長させましょう。

ネットワーク感染の 88% は DNS フィルタリングによって削減できます。

OpenText Core DNS Protection

当社のソリューションを販売することで利益を得られる理由：

1 **最先端の DNS 保護を活用する**
ドメインフィルタリングが良好かどうかは、採用している脅威インテリジェンスによって決まります。OpenText 独自の OpenText™ Threat Intelligence Platform が、機械学習と AI 機能を活用して最高レベルの保護を提供します。

2 **SMB向けのユーザーフレンドリーなセキュリティ**
OpenText™ Core DNS Protectionは、小企業所有者とMSPの両方にとって使いやすいことを念頭に置いて設計されています。OpenTextは、コスト効率が高く、追加ハードウェアなしのクラウドベースソリューションであるため、数分で設定して使用することができます。

3 **顧客に安心感をもたらす**
責任を共有することで、SMB顧客に安心感をもたらします。特に、OpenText Core DNS Protectionによってビジネスが直面するセキュリティインシデントの数が減少していることが確認できることで安心に繋がります。さらに、このことによって脅威に関連するコストが減少し、時間とお金を節約し、生産性が向上します。

4 **コンプライアンスと人事の懸念を解決できる**
コンプライアンス要件（PCI、HIPAA、GDPRなど）を抱える顧客は、OpenText Core DNS Protectionによってデバイスおよびネットワーク全体でのインターネット使用の管理を簡素化できるため、すべての従業員のために任意のデバイス上でのコンプライアンスおよびゼロトラストアクセスを保証するのに役立ちます。

5 **管理を簡素化して時間を節約**
当社のカスタマイズ可能なコンソールは、数千人のユーザーに遅延なしで拡張できる時間節約ツールなど、サイバーセキュリティ管理を簡素化するシングルペインオブグラス(SPOG)を提供します。クライアントを別々に、一括で、または個別に簡単に管理できます。

6 **他のソリューションとの統合**
OpenText Core DNS Protectionは非常に柔軟性が高く、顧客の現在のインフラストラクチャ、ネットワークトポロジ、ツール、および管理システムスタックとシームレスに統合されます。また、さまざまなファイアウォール、デバイス、広く使用されているVPNもサポートします。

7 **最終帳尻損益を向上させる**
ドメインフィルタリングによってサイバーセキュリティ層を強化することの価値は、証明されています。OpenText Core Endpoint ProtectionおよびOpenText™ Core Security Awareness Trainingがバンドルされていれば、顧客に提供される価値は圧倒的です。

8 **サポートとツールで販売が向上**
受賞歴のあるOpenText Threat Intelligence以外に、販売およびマーケティングツール、トレーニング、リソースを提供しており、OpenTextソリューションを効果的に販売し、ビジネスを拡大するために必要なものはすべて揃っています。

OpenText Core DNS Protection を実際にご覧ください。
試用版を開始する。

DNS Protection について SMB からよく尋ねられる質問

OpenText Core DNS Protection とは何ですか？

DNS はインターネットのアドレス帳です。システムがインターネット上のリソースにアクセスするために必要とするアドレスにドメインを変換します。OpenText Core DNS Protection はこのアドレス帳にインテリジェンスと制御を適用します。これは、提供されるリソースが安全で適切であることを保証するのに役立ちます。

なぜビジネスに DNS フィルタリングが必要なのですか？

DNS フィルタリングは、セキュリティと生産性に大きな効果をもたらすことができます。品質インテリジェンスを備えた DNS フィルタリングを実行するシステムでは、さらされる脅威が 33% 減少します。つまり、ビジネスのリスクが軽減され、ユーザーの中断が減少します。さらに、DNS フィルタリングは利用可能なコンテンツを制御できるため、気が散るのを防止するのに役立ち、生産性をさらに向上させることができます。

OpenText Core DNS Protection は誰を対象としていますか？

OpenText Core DNS Protection は MSP を対象としており、DNS Protection はこの精神に従っています。導入と管理を簡素化するように設計されているだけでなく、クライアント保護に圧倒的な効果をもたらすために必要な機能を取り込んでいます。クライアント全体 (ネットワークとエージェントの両方) にエージェントを展開するのに必要な時間は数分で、レポートと請求は簡単でありながらニーズに合わせて調整されます。

DNS フィルタリングはどのように機能しますか？

平均的なシステムは 1 日に 2000 回の DNS リクエストを実行します。DNS フィルタリングは、DNS 解決を選択的に提供することで、これらのリクエストにインテリジェンスを適用します。悪意のあるまたは不適切なリソースが提供されなければ、システムおよびユーザーが脅威にさらされることはありません。

OpenText Core DNS Protection が独自の価値を持つのはなぜですか？

OpenText Core DNS Protection は BrightCloud® 脅威インテリジェンスを活用して DNS リクエストをフィルタリングします。これにより、業界をリードするインテリジェンスを使用して、フィッシングおよびマルウェアサイトを迅速に特定してブロックできます。さらに、OpenText Core DNS Protection は、DoH (DNS over HTTPS) を活用し、最先端の特性および機能性を提供することで、市場を革新し、リードしています。