データシート

Infoblox DNS Infrastructure Protection

DNS ベースの攻撃によるビジネスの中断を最小限に抑える

課題：サービスの中断

DNS はデジタルオペレーションの隠れたバックボーンです。すべてのウェブサイト、アプリ、ユーザーは接続を維持するため、これに依存しています。DNS サービスが停止すると、何百万ドルもの収益が失われ、顧客の信頼が失われる可能性があります。これは特に、ウェブサイト、メール、その他の公開アプリケーションをオンラインに保つ外部 DNS サービスに当てはまります。同時に、外部の DNS サーバーは公共のインターネットにさらされなければならないため、断続的に次のようなサイバー攻撃の標的になっています。

- **DDoS 攻撃**は、複数のソースからの大量のトラフィックでサーバーを圧倒し、ウェブサイトのクラッシュを引き起こします
- **DNS ハイジャック**は、攻撃者が DNS レコードを改ざんしてトラフィックを悪意のあるサイトにリダイレクトする行為です
- **キャッシュ・ポイズニング**は、攻撃者が悪質なコンテンツを提供したり、ユーザーを悪質なサイトにリダイレクトしたりするために、悪質なデータや無効なデータをネットワークのキャッシュに注入することです
- **NXDOMAIN の悪用**は、存在しないドメインのクエリで DNS サーバーを氾濫させ、サービスの中断を引き起こします

さらに、外部の権威 DNS レコードは世界中のインターネットサーバーに配布されます。そのため、攻撃者がデータを改ざんできた場合、悪質なデータの修正に数時間から数日かかり、その間にウェブサイトやその他のオンラインアプリにまったくアクセスできなくなる可能性があります。

Infoblox DNS Infrastructure Protection（旧称 Advanced DNS Protection）は、DNS サーバーを標的とした DDoS 攻撃やその他の攻撃を阻止します。この NIOS ソフトウェアアドオンにより、DNS インフラストラクチャが激しい攻撃を受けている場合でも、ミッションクリティカルなインターネット接続アプリケーションを稼働状態に保つことができます。

解決策：DNS ベースの攻撃による障害からビジネスを守る

DNS Infrastructure Protection は、重要な DNS サービスを標的とするさまざまな脅威を継続的に検出してブロックし、攻撃者による DNS 整合性の操作を防ぎます。DDoS や NXDOMAIN などのボリューム型攻撃と、DNS ハイジャック、キャッシュポイズニング、外部および内部 DNS サーバーを標的とするその他の脅威などの非ボリューム型攻撃の両方をブロックします。

正当なトラフィックをブロックする可能性のある画一的なアプローチとは異なり、DNS Infrastructure Protection は継続的に更新されるインテリジェンスを使用して本物の脅威を識別します。一方、DNS インフラストラクチャが攻撃を受けている間でも、実際のトラフィックの流れが維持されるため、ビジネスは稼働し続けます。

主な機能

ビジネスの中断を軽減：Infoblox DNS Infrastructure Protection は、正当なクエリに応答しながら、あらゆる種類の DNS 攻撃（ボリューム型攻撃や、DNS エクスプロイトや DNS ハイジャックなどの非ボリューム型攻撃を含む）を継続的に監視、検知、阻止します。また、DNS ハイジャック攻撃によって危険にさらされる可能性がある DNS の整合性も維持されます。Infoblox は、ミッションクリティカルなウェブサイトやアプリをオンラインで利用可能な状態に保つ上で役立ちます。

進化する脅威への適応：Infoblox DNS Infrastructure Protection は Infoblox Threat Adapt™ テクノロジーを使用し、新しい脅威や進化する脅威が出現すると、それに対する防御を自動的にアップデートします。Threat Adapt は、Infoblox の脅威スペシャリストが顧客のネットワークで確認したものなど、進化する攻撃手法に対して独自の分析とリサーチを適用し、保護をアップデートします。また、DNS の設定変更を反映して、自動的に保護を適応させます。

暗号化された DNS の有効化（DoH と DoT）

DNS クライアント（スタブ）リゾルバとローカル DNS サーバー（リカーシブリゾルバ）の間の通信は暗号化されていません。暗号化されていない通信は、データのスヌーピング、傍受、持ち出しの対象となり、これは DNS の「ラストマイル」セキュリティ問題として知られています。これを受けて、業界は DNS クライアントと外部インターネット DNS サーバー間のプライバシーと暗号化を提供するために、DNS over TLS（DoT）および DNS over HTTPS（DoH）を導入しました。ネットワーク上で DNS リゾルバを通じて暗号化を実装することで、セキュリティポリシーの要件に応じたセキュリティとコンテンツフィルタリングを提供しつつ、ユーザーのネットワーク体験を制御できます。DNS Infrastructure Protection は DNS 暗号化を最適化するため、ネットワーク上の暗号化された DoT および DoH 接続を終了できます。

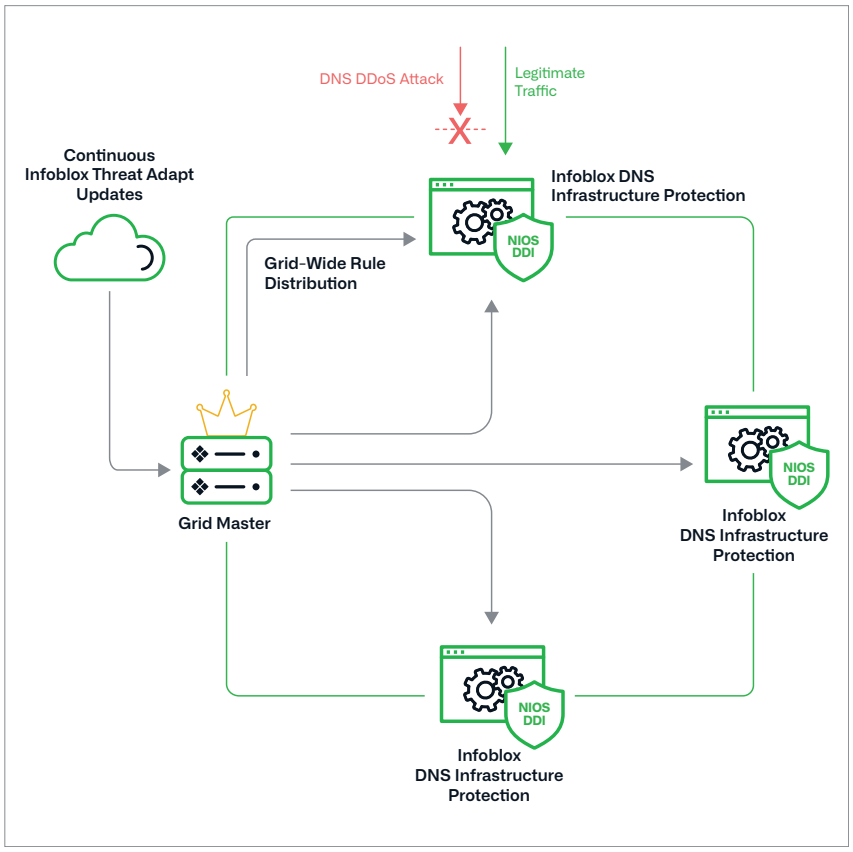

表 1. Infoblox DNS Infrastructure Protectionは、DNSベースの攻撃に対する独自の防御を提供します

単一画面での可視性を実現：DNS Infrastructure Protection は、リアルタイムおよび過去の DNS 攻撃パターンに対する広範囲かつ一元化された可視性を提供します。NetOps および SecOps チームは、脅威の発生源を追跡し、環境全体の攻撃ポイントを表示して、迅速な軽減を促進し、防御を継続的に改善できます。

物理、仮想、クラウドプラットフォームで利用可能：Infoblox を使用すると、仮想および物理の Trinzic アプライアンスにソフトウェア・サブスクリプションのアドオンとして導入するオプションがあり、共通モデルでサービスを実行し、オンプレミス、プライベート、パブリッククラウド環境をサポートできます。

お客様の声

「DDoS 攻撃によるサービスインシデントは半減し、ページ読み込み時間の長さに対する顧客からの苦情は大幅に減少しました。」

カスタマーサポート担当副社長、
大手サービスプロバイダー

「私は 4 年間、DNS、DHCP、IP アドレス管理のために Infoblox を使用しています。間違いない製品です。この製品が非常に高い成果をあげるため、リソースを移動させました。当社のグローバルネットワークは、わずか 1.5 人のフルタイム従業員で管理されており、65 台のデバイスを扱っています。」

グローバルインフラ担当マネージャー
Adobe（アドビ）

表 1:
DNS INFRASTRUCTURE PROTECTION が防御する攻撃の種類の概要

攻撃名	タイプ	仕組み
DNS リフレクション / DDoS 攻撃	ボリュメトリック	サードパーティの DNS サーバー（オープンリゾルバー）を使用して DoS または DDoS 攻撃を伝播
DNS アンプ攻撃	ボリュメトリック	特別に作成されたクエリを使用して増幅された応答を作成し、被害者にトラフィックを大量に送信
TCP/UDP/ICMP フラッド攻撃	ボリュメトリック	大量のトラフィックでネットワークまたはサービスをダウンさせることによる、レイヤー 3 でのサービス妨害
NXDOMAIN	ボリュメトリック	DNS サーバーに存在しないドメインへのリクエストが大量に送信され、キャッシュが飽和状態になり、応答時間の遅延が発生
ランダムなサブドメイン (水責め攻撃)、ドメインロックアップ攻撃、ファントムドメイン攻撃	低ステルス性	攻撃の一環として設定された架空または不正なドメインへのリクエストで DNS サーバーを氾濫させ、リソースの枯渇、キャッシュの飽和、送信クエリ制限の枯渇、パフォーマンスの低下を引き起こします
DNS ベースの脆弱性攻撃	脆弱性攻撃	DNS ソフトウェアの脆弱性を悪用した攻撃
DNS キャッシュポイズニング	脆弱性攻撃	不正なアドレスで DNS キャッシュデータを破損
プロトコル異常	脆弱性攻撃	不正なパケットやクエリを送信してサーバーの停止が発生
偵察	脆弱性攻撃	ハッカーが大規模な DDoS またはその他のタイプの攻撃を開始する前にネットワーク環境に関する情報を取得しようとする試み
DNS ハイジャック	脆弱性攻撃	ドメイン登録情報を上書きして不正な DNS サーバーに指定する攻撃
データ窃取 (既知のトンネルを使用)	脆弱性攻撃	攻撃は、DNS ポート 53 を通じて別のプロトコルをトンネリングすることを含みます。これは、ファイアウォールが非 DNS トラフィックを許可するように設定されている場合に可能であり、データの持ち出しを目的としています。

アプライアンスオプション

DNS Infrastructure Protection：物理および仮想プラットフォームで利用可能

Infoblox DNS Infrastructure Protection は、広範囲にわたる DNS DDoS 攻撃から防御し、中段のないサービスを確保します。これはさまざまな Trinzic ハードウェアおよびソフトウェア・アプライアンスに対するソフトウェア・サブスクリプション・アドオンであり、DNS の整合性を保護し、オンプレミス、プライベート、パブリッククラウド環境全体でビジネスオペレーションを中断させる可能性のある外部および内部の DNS DDoS 攻撃を防止します。

Infoblox は、ネットワーク、セキュリティ、クラウドを統合し、保護性に優れた DDI プラットフォームで企業のレジリエンスとアジリティを実現します。当社はハイブリッドおよびマルチクラウド環境を統合し、重要なネットワークサービスを自動化し、ビジネスを事前に保護することで、妥協することなく迅速に行動するために必要な可視性とコンテキストを提供します。

Infoblox株式会社
〒107-0062
東京都港区南青山2-26-37
VORT外苑前I 3F

03-5772-7211
www.infoblox.com/jp

バージョン: 20251007v3