データシート

Infoblox Threat Defense™ Business Cloud

予測型脅威インテリジェンスを搭載したプロテクティブ DNS は、影響を受ける前に、あらゆる場所ですべてを保護します

基盤的な DNS セキュリティで影響を受ける前に保護

インフラストラクチャ、データ、ユーザーの保護はこれまで以上に困難になっています。従来の事後対応型のセキュリティモデルでは、もはや対応しきれません。今日の脅威はより高速かつ巧妙で、従来の防御を回避するように設計されています。

- AIを活用した攻撃、例えば類似ドメイン、スミッシング、多要素認証（MFA）バイパス、標的型フィッシングは、従来のツールでは阻止できないほど急速に進化しています。
- 防御線はなくなりました。ユーザーはどこからでもクラウドアプリに直接接続でき、従来のツールでは設計上対処できないことによるギャップが生まれています。
- SD-WAN と支店は、集中化された検査ポイントを迂回して、インターネットに直接接続することがよくあります。
- IoT と非マネージドデバイスは、エンドポイントセキュリティだけでは保護できない盲点を生み出します。
- 従来のツールのほとんどは、既知のマルウェアの検出やコンテンツのフィルタリングに依存しており、今日の攻撃者にとっては遅すぎる事後対応型のアプローチです。

優位性を維持するために、組織は **DNS レイヤーでスケーラブルかつ先制的な保護を必要とします**。Infoblox は、エンドポイント、クラウドワークロード、または支店に到達する前に脅威を特定・ブロックする基盤的な DNS セキュリティを提供します。比類のない可視性、予測インテリジェンス、およびより広範なセキュリティスタックへのシームレスな統合により、Infoblox はアラートノイズの削減、運用の簡素化、および損害が引き起こされる前の攻撃の防止を支援します。

大規模なプロテクティブ DNS セキュリティ

最新のネットワークがデータセンター、SD-WAN、クラウドサービスおよび IoT インフラストラクチャを横断的に拡大する中、一貫したセキュリティカバレッジを維持することはより複雑になりますが、これまで以上に重要にもなっています。

Infoblox Threat Defense™ Business Cloud は、スケーラブルでクラウドネイティブな DNS セキュリティを提供し、運用上のオーバーヘッドを追加することなく、現在の環境と進化するデジタルイニシアティブを保護することで、セキュリティ体制を基盤から強化します。オンプレミス DNS の保護、分散ブランチへの可視性の拡張、リモートユーザーのサポートなど、Infoblox は必要な場所で DNS レイヤーの強化を実現します。

主な機能

- リアルタイムの脅威インテリジェンスを使用してランサムウェア、フィッシング、エクスプロイト、マルウェアをブロックし、最新の脅威を未然に防ぎます。
- 分析と機械学習を用いてデータ持ち出しを防ぎ、DNS トンネリング、ドメイン生成アルゴリズム（DGA）、DNSMessanger、ファストフラックス・アクティビティを阻止します。
- ネットワーク内外、マネージドまたは非マネージド（BYOD、IoT、OT）のすべてのデバイスを DNS レイヤーで保護します。
- Web フィルタリングとユーザーベースのアクセス制御を使用してコンテンツポリシーを適用します。
- ブランドを保護するために、Lookalike Domain Monitoring を使用して、悪意のあるドメインのなりすましを検出し、削除を可能にします。
- 強化された DNS テレメトリと脅威のコンテキストにより、調査を最大 3 倍高速化します。
- DNS アクティビティを IP アドレス管理（IPAM）資産メタデータと相関させることで可視性を高め、より迅速かつ正確なインシデント対応を実現します。
- 重大な脅威に優先順位を付け、迅速に対応するため、SOC Insights と AI 主導の調査サポートを活用します。
- SIEM、SOAR、次世代ファイアウォール（NGFW）、IPS、エンドポイント、およびその他のセキュリティツールと連携して脅威インテリジェンスとログを自動的に共有することで、エコシステム全体を統合します。

リアルタイムの脅威インテリジェンス、統合された可視性、SOARおよびSIEMツールとの統合により、セキュリティチームは脅威を迅速に検出し、優先順位を付けて対応できます。これにより、解決までの時間が短縮され、既存のセキュリティスタックのパフォーマンスが向上し、企業の脅威防御の総コストが削減されます。

クラウドから提供される Infoblox Threat Defense Business Cloud は、運用上の複雑さを増すことなく、変化する顧客のニーズに合わせて簡単に拡張できます。ユーザー、サイト、ワークロード全体で需要が増大するにつれて、セキュリティも自動的に拡張されます。

INFOBLOX SAAS の利点

Infoblox Threat Defense Business Cloud は、既存のオンプレミス・インフラストラクチャに次世代のセキュリティ機能を提供する SaaS（Software as a Service）ソリューションです。クラウドベースで柔軟に拡張可能なソリューションによって、以下が可能になります。

- 企業のセキュリティ体制を即座に改善
- あらゆる場所で、すべてのデバイスに簡単なセキュリティ保護を提供
- IT のオーバーヘッドを最小限に抑える

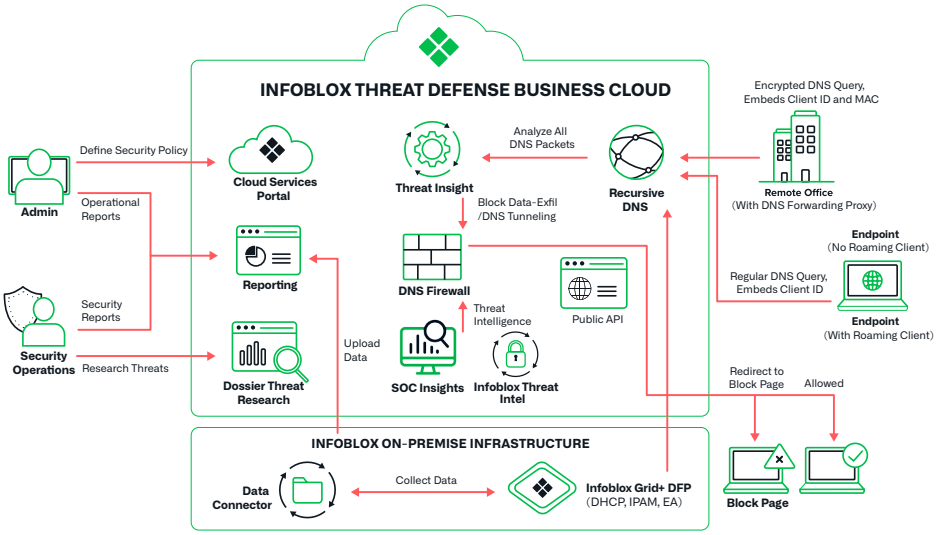

図 1. Infoblox Threat Defense Business Cloud のワークフローシナリオ

DNS FORWARDING PROXY

IoT、プリンター、レガシーシステムなど、エンドポイントエージェントをインストールできない環境の場合、Infoblox はデバイスレベルの可視性とポリシー適用を維持するための DNS Forwarding Proxy（DFP）を提供します。

この軽量な仮想アプライアンスは、元のクライアント IP を DNS クエリに埋め込み、その後 Infoblox クラウドに転送します。これにより、ローカルエージェントを必要とせずに、正確なソースのアトリビューション、脅威からの保護、一貫した適用が保証されます。

Infoblox NIOS 8.3 以降と統合されたこのプロキシにより、既存の顧客は追加のオンプレミス・インフラストラクチャやソフトウェアの展開をすることなく、クラウドベースの DNS セキュリティを有効化できます。

> *「昨今、インターネットユーザーが開いたリンクからランサムウェア、スパイウェア、アドウェアが侵入するケースが非常に多くなっています。Infoblox のクラウドセキュリティソリューションは、ユーザーを悪質なサイトに誘導するリダイレクトをブロックし、マシンの感染を防ぎ、ユーザーの安全を確保します。」*
>
> **シニアシステム管理者兼ネットワークエンジニア**
> **シアトルシティ大学**

Infoblox Endpoint Agent は、ローミングデバイスに安全な DNS レイヤー保護を提供し、ユーザーがネットワーク外で作業している場合でも可視性と制御を確保します。

この軽量なエージェントは、ノート PC やワークステーションにインストールして、デバイスが企業ネットワーク外にある場合でも可視性とポリシーの適用を確保できます。

- DNS クエリを Infoblox クラウドにリダイレクトし、検査と実行を行います。
- トラフィックを暗号化し、各クエリにデバイス ID とユーザーコンテキストのタグを付けます。
- インシデント調査と報告のためにユーザーレベルのアトリビューションを可能にします。
- デバイスが保護された企業ネットワーク内にあると、自動的にバイパスモードに切り替わります。

Endpoint Agent は、DNS Forwarding Proxy と組み合わせることで、可視性や保護にギャップを生じさせることなく、ユーザー、デバイス、環境を網羅的にカバーします。

ビルトイン

可用性

Infoblox Threat Defense Business Cloud は、グローバルなエニーキャスト配信、毎日のバックアップ、24 時間 365 日の監視により、99.999% の DNS 稼働時間（メンテナンスを除く）を実現します。

セキュリティ

すべての DNS クエリと保存されたデータは、転送中および保存時に暗号化されます。アクセス制御は、役割、IP、場所による制限をサポートします。

プライバシー

Infoblox は、定期的なパッチ適用、コード分析、侵入テストなど、セキュリティのベストプラクティスに従います。顧客データは論理的に分離され、固有の API キーによって認証され、第三者と共有されることはありません。

Infoblox Threat Defense がデータとインフラを保護する方法についての詳細は、
https://www.infoblox.com/jp/products/threat-defense/ をご覧ください。

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：20250723v1