データシート

Infoblox Threat Defense™ Advanced

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。

DNS は、すべてのサイバー攻撃に対する最初の防衛線

DNS は、あらゆるサイバー攻撃の検出と防止における最前線です。フィッシングメール、スミッシングメール、または悪用された脆弱性のいずれから始まるかにかかわらず、ほぼすべての攻撃は悪意のあるドメインへの DNS クエリを生成します。その結果、DNS は、オンプレミス、クラウド、エッジのいずれにおいても、ユーザー、デバイス、IoT/OT、ワークロードを含む企業全体のセキュリティを確保するための、強力で一元的な可視化と制御のポイントとなります。

あらゆる通信の最初のステップとして、DNS レイヤーで脅威アクティビティを検出・ブロックすることで、悪意のあるトラフィックが下流のツールに到達してアラートをトリガーする前に阻止できます。DNS データをデバイスおよび資産のコンテキストと相関させることにより、NetOps チームと SecOps チームは環境全体で何が起こっているかをより深く把握できるようになり、運用効率とセキュリティ体勢の両方が向上します。

従来型の「検知して対応」は限界

脅威アクターは、より大規模な、巧妙かつステルス性の高いキャンペーンを仕掛けるために、ますますAIを利用するようになっています。独自に作成された使い捨てのマルウェアを生成するため、従来の「検出と対応」ツール、つまり「ペイシェント・ゼロ」の感染を待っているツールは効果がありません。すべての攻撃は、シグネチャや既知の動作が存在しない「ペイシェント・ゼロ」のシナリオになります。「検出と対応」ツールは、多くの場合キルチェーン内での対応が遅すぎるため、損害を防ぐことができないことがあります。したがって、異なる先制的アプローチが必要です。脅威が環境に侵入したり横方向に移動したりする前に阻止するアプローチです。これにより、攻撃を早期にブロックできるだけでなく、従来の「検出と対応」ツールの負荷も軽減されます。

DNS は上流の制御ポイントとして機能し、セキュリティチームが脅威をユーザー、ワークロード、またはエンドポイントに到達する前に早期に検出してブロックする機会を提供します。

DNS による先制的セキュリティ

Infoblox Threat Defense™ Advanced は、独自の**先制アプローチ**を脅威検出にもたらします。これは「ペイシェント・ゼロ」に依存しません。脅威アクターのインフラストラクチャが武器化される前にブロックする**予測型脅威インテリジェンス**と、顧客ネットワーク内の DNS クエリのアルゴリズム /ML ベースの分析を組み合わせて使用し、影響が出る前に保護します。セキュリティインシデントに関与する資産の迅速な特定、エコシステム統合、直感的なワークスペースを通じて、既存のセキュリティ投資対象からのより迅速な検出、より迅速な対応、そしてより大きな投資収益率（ROI）を実現します。

事実と数字

- **204,000** の脅威アクターのクラスターをリアルタイムで監視し、なお増加中
- 誤検知率を **0.0002%** に低減
- 最初のクエリの前に **82%** の脅威をブロック
- 攻撃の平均 **68.4** 日前に保護を提供
- 既知の悪意のある動作を探すツールと比較して **5** 倍の高リスク / 中リスクドメインをブロック
- SOC アナリストの時間を 1 か月あたり平均 **500 時間**節約*
- 生産性向上により年間 **40 万ドル**のコスト節減をサポート*
- 数万件のアラートを数件に削減*

SANS 2025 SOC Survey によると、SOC の全面的な活用を妨げる上位 10 の障壁のうち 7 つは、アラート、ツールの統合、およびスキル不足に関連していることが判明しました。

* 実際の顧客データに基づく。

影響を受ける前に脅威をブロック

Infoblox Threat Defense は、リアルタイムの DNS トラフィックにアルゴリズム / 機械学習分析を使用した予測型の DNS 脅威インテリジェンスを適用し、脅威のアクティビティがネットワークに影響を与える前にブロックします。多くの場合、他のツールでは検出できない脅威も検出します。Infoblox は、DNS レイヤーで脅威を阻止することで、下流のセキュリティツールのアラート量と作業負荷の削減にも役立ち、顧客からは次世代ファイアウォール（NGFW）とエンドポイントの検出と対応（EDR）システムでのアラートが最大 50% 削減されたと報告されています。

> *「セキュアな DNS は、特定のネットワークへのマルウェア導入成功を目的としたマルウェアの攻撃能力を 92% 削減できます」。*
>
> **Anne Neuberger、**
> **サイバーセキュリティ局**
> **局長国家安全保障局（NSA）**

主要な機能	説明	Infoblox Threat Defense	NGFW	SASE	EDR
エンタープライズ全体でのセキュアなリゾルバーと DNS クエリのログ記録	DNSクエリデータからドメインを特定し、悪性判定して対処します	●	◑	◑	◑
DNS の包括的な動作監視	悪意のある活動について、すべての DNS レコードタイプを監視します	●	●	◔	○
類似 / ドッペルゲンガードメインの検出と削除	類似 / ドッペルゲンガー攻撃面（アタックサーフェス）を低減します	●	○	◑	○
ゼロデイ DNS 保護	組織に脅威を及ぼす可能性のある新規または新興のドメインを特定します	●	◑	◑	○
動作ベースの DNS トンネリング検出	データの流出/侵入、C2 通信などに使用される DNS トンネルを検出します	●	◑	◑	○
疑わしい/高リスクのドメインに対するプロアクティブな保護	将来的に悪意のあるキャンペーンで使用される可能性がある疑わしいドメインを事前に識別・ブロックします	●	◑	◑	◑
ネイティブな自動コンテキスト付与	クライアントやシンクホールを使わずに、ユーザー/デバイス/送信元IP/所在地/MAC/VLANなどのネットワーク文脈を自動付与します	●	◑	◑	◑
脅威分散システム（TDS）のプロアクティブな検出と妨害	個々のドメインだけでなく、脅威アクターのTDSインフラ自体を特定し、ドメイン回転による回避を妨害します	●	◔	○	○

図 1. 他のツールでは網羅的な対応ができない、Threat Defense 独自の機能。

THREAT DEFENSE の主な機能

- **「影響が出る前に保護」する監視。** CISO やセキュリティチームが、先制的なセキュリティ戦略を実行し、影響が出る前に無力化された脅威に関する明確で定量化可能な指標を自信を持って取締役会に報告できるようにします。これにより、重要な時間的優位性を獲得し、セキュリティオペレーションセンター（SOC）の負担を軽減します。
- **資産発見とインベントリ統合。**セキュリティインシデントに関連する資産を迅速に特定し、インシデントの評価と対応を速めます。
- **セキュリティワークスペース。**シンプルで直感的なUIにより、セキュリティチームは環境内で何が起こっているかを理解し、セキュリティリスクを軽減する方法を提案できます。
- **検出モード。**既存のITやネットワークインフラを変更せずに、簡単に導入し、概念実証を実行できます。

予測型のインテリジェンスで先制的セキュリティを強化

Infoblox は独自の DNS 脅威インテリジェンスの先駆者であり、業界を牽引しています。同社は防御的なアプローチだけでなく、先制的なアプローチを取っています。その洞察を活用して、脅威アクターのインフラストラクチャを構築中の段階で追跡し、多くの場合、攻撃が始まってもいない段階でサイバー犯罪を発生源から阻止します。

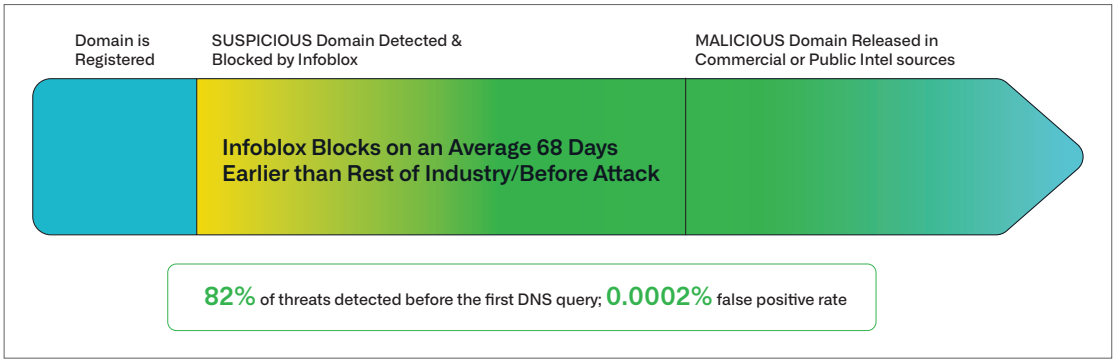

図 2. Infoblox Threat Intelligence は、セキュリティ業界の他製品よりも迅速に脅威から保護できます。

Infoblox が独自の DNS 脅威インテリジェンスを作成する仕組み

DNS のエキスパート：Infoblox は、DNS 内に潜む脅威アクターを発見するための秘訣を知っています。チームはリスクの高いまたは疑わしいドメインから始め、点と点をつなげて攻撃者のインフラストラクチャを特定し、他の場所で認識される前に、その展開や新たな脅威の表面化を追跡します。

脅威の専門知識：Infoblox は、悪意のあるアクターがどのように活動し、マルウェア、ランサムウェア、フィッシング、DNS ベースのエクスプロイトなどの脅威がどのように顕在化するかを理解しています。この専門知識は、類似ドメイン、DNS コマンドアンドコントロール（C2）アクティビティ、登録済ドメイン生成アルゴリズム（RDGAs）およびその他の疑わしい行動を検出する予測システムを強化します。

データサイエンス：Infoblox は、機械学習と高度なデータサイエンスを膨大な量の DNS クエリデータに適用します。これにより、データ持ち出し、ドメイン生成アルゴリズム（DGA）、および幅広い回避型脅威に対するほぼリアルタイムの保護が可能になります。

SOC INSIGHTS でよりスマートに作業

アラート疲れやアナリストの燃え尽き症候群から長期にわたる調査と対応の取り組みまで、Infoblox Threat Defense は追加の SOC Insights パッケージにより SOC の負担を大幅に軽減します。

- AI 主導の分析により、何十万ものアラートを一握りの洞察に絞り込み、アナリストが最も重要なことを把握できるようサポートします。
- ログ、脅威インテリジェンス、その他のデータ収集と相関構築を自動化し、アナリストが調査と対応を迅速に開始できるようにします。
- 資産の発見とインベントリの統合によりインシデント対応を迅速化し、アナリストが影響を受けたデバイスをより迅速に特定できるようにします。

図 3. Infoblox Threat Intelligence が共有した、類似ドメインのリスクの増大に関する驚くべき調査データ。

価値の高い DNS ログを大規模にエクスポート

Infoblox を使用すると、高精度の DNS クエリとイベントデータを SIEM、SOAR、またはデータレイクに簡単に送信して、一元的な可視性と脅威の相関関係把握の高速化を実現できます。

- 価値の高い DNS イベントのみをフィルタリングして転送し、SIEM の取り込みコストとアラートノイズを削減します。
- Infoblox Cloud Data Connector を使用して、強化された DNS ログをリアルタイムでストリーミングします。
- すべてのツールに必要なコンテキストを提供することで、エコシステム全体の検出と対応を改善します。
- 認定された双方向統合を通じて他のツールとシームレスにデータを共有し、エンドツーエンドの検出、トリアージ、対応を改善します。

DOSSIER で調査を迅速化

Dossier は、脅威を検証し、侵害の兆候（IOC）に基づいて行動し、調査を迅速化するための強力な統合調査ツールをアナリストに提供します。異なるプラットフォーム間で切り替える必要はありません。

- 社内、Infoblox、およびサードパーティの脅威インテリジェンスを 1 つの直感的なインターフェースに統合します。
- 組み込みのエンリッチメントとリンク分析を使用して、IOC を迅速に調査し、関連する脅威を発見します。
- 手動によるデータ収集とコンテキストの切り替えを排除することで、調査時間を最大 67% 削減します。

標的型詐欺からブランドを保護

Infoblox は、「類似ドメイン監視」と「ドメイン脅威軽減サービス」という2つの統合機能を提供し、なりすましベースのサイバー攻撃からブランド、顧客、従業員を保護します。これらを組み合わせることで、新たな脅威を可視化し、悪意のあるドメインがビジネスに影響を及ぼす前に、迅速かつ効果的な対策を講じることができます。

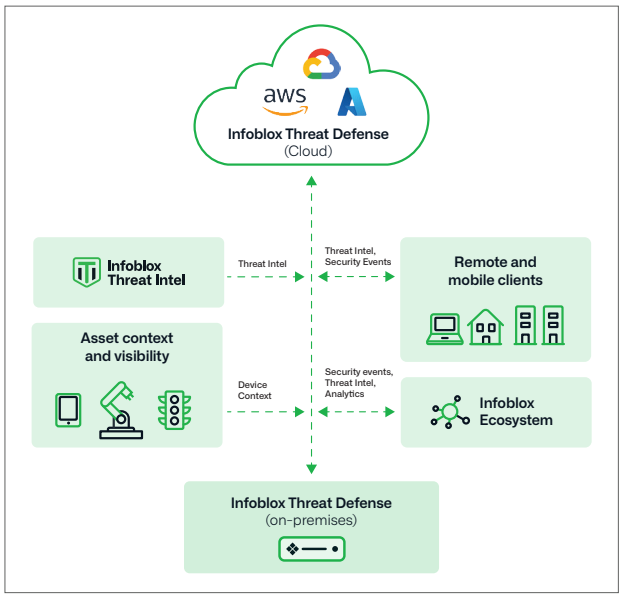

図 4. Infoblox のハイブリッドアーキテクチャは、今日の AI に対応した脅威の状況に対抗するため、どこでも保護を提供し、どこでも展開を可能にします。

類似ドメイン監視

ブランドや信頼できる第三者を悪用するなりすまし攻撃に先手を打ちましょう。

- 貴社、サプライチェーン、または顧客向けの資産になりすますために登録されたドメインを検出します。
- 従業員や顧客をターゲットにしたフィッシングや詐欺キャンペーンで使用されるドメインを特定します。
- 優先度の高いドメインのリスク状況の変化をモニターし、リアルタイムのアラートを受信できます。

ドメイン脅威軽減サービス

実環境で稼働中の悪性ドメインを迅速に検証し、テイクダウンします。

- 人間主導のインシデント検証と概要レポートを通じて、悪意のあるアクティビティを確認し、文書化します。
- 世界中の ISP、ホスティングプロバイダー、規制機関と調整して、迅速な（多くの場合24時間以内に）削除を行います。
- 軽減された脅威を、削除後 30 日間監視し、追加費用なしで再アクティブ化の試みを検出・削除します。
- フィッシング、マルウェアホスティング、C2　インフラストラクチャ、盗難データなど、さまざまな種類の脅威に対処します。

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

Infobloxはネットワークとセキュリティを統合して、これまでにないパフォーマンスと保護を提供します。Fortune 100企業や新興企業から高く信頼され、ネットワークが誰に、そして何に接続されているのかをリアルタイムで可視化し制御することで、組織は迅速に稼働でき、脅威を早期に検知・対処できます。

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：20250121v1