予測し
先手を打ち
勝ち抜く

AI を活用した高度な攻撃に 先制
型プロテクティブ DNS で対応

infoblox®

目次

事後対応型の「DETECT AND RESPOND」アプローチの問題点

従来の方法は、遅すぎて、リスクが高く、効果が薄れてきています。

従来のキルチェーンアプローチは廃れつつあります。このアプローチは、「最初の被害者感染」戦略を採用しており、別の組織を最初の標的（別名「最初の被害者：patient zero」）として、マルウェアの動作についてさらに詳しく学習し、その洞察を自社組織に適用するものです。

しかし、そのモデルはもはや成り立ちません。今日の脅威アクターは、業種、会社、さらには従業員に合わせたマルウェアを作成しており、貴社が最初の被害者となる可能性は指数関数的に高まっています。

脅威アクターの平均ブレイクアウト時間（攻撃者が最初のアクセスを取得してからネットワーク内を横方向に移動するのにかかる時間）は、わずか48分となっています。[1]これ は、組織が攻撃をネットワーク内でさらに拡散する前に、攻撃を検出、調査、修復するための時間が非常に短いことを意味します。

脅威アクターの平均的ブレイクアウト時間

最初の侵害
脅威アクターがネットワークへのアクセスを獲得

48分
ネットワークを横方向に移動するのにかかる平均時間

脅威アクターの影響

脅威アクターが不当な優位性を獲得

組織がサイバーセキュリティソリューションに年間 2,000 億ドル以上を費やしているにもかかわらず、[2]ランサムウェアのような侵害は依然として成功しており、現在のアプローチに重大なギャップがあることが浮き彫りになっています。

脅威アクターが新たなツールを用いて、より頻繁かつ高度でステルス性の高い攻撃を仕掛ける中、事後対応型のセキュリティソリューションではもはや十分ではありません。AI によって生成された使い捨てマルウェアは、今や非常に独自に細工されているため、あらゆる攻撃が「ゼロデイ」となり、それを検出するためのシグネチャや既知の動作は存在しません。

脅威アクターが AI を使用している方法

AI は膨大な量のデータを処理し、パターンから学習できるため、サイバー犯罪者はより高度で標的を絞った攻撃戦略を開発できます。

AI を活用したソーシャルエンジニアリング
顕著な手法の一つに、AI を活用したソーシャルエンジニアリングがあります。この手法では、攻撃者が非常に説得力のあるフィッシングメールやボイスフィッシング（ビッシング）通話を作成します。これらの通話は多くの場合、信頼できる個人からのように聞こえるため、被害者を騙して機密情報を漏らさせたり、安全なシステムへのアクセスを許可させたりすることが容易になります。

AI 主導のマルウェア開発
さらに、AI は悪意のあるコードの開発を加速し、従来のセキュリティ対策を回避できる高度なランサムウェアの作成に必要な時間を短縮します。この機能により参入障壁が低くなり、経験の浅いハッカーでも効果的なランサムウェア攻撃を導入できるようになります。

サイバー犯罪への参入障壁の低下
最終的に、AI はサイバー犯罪をより身近なものにしています。AI 搭載ツールがフィッシングキットの生成からマルウェア配信までを自動化することで、スキルの低い攻撃者でも信頼性のある有害なキャンペーンを開始できるようになりました。AIを活用した「アズ・ア・サービス」型のサイバー犯罪の増加は、業界全体で攻撃がより頻繁に、より多様に、そして予測がより困難になることを意味します。

サイバー攻撃環境の主なトレンド

ChatGPT や FraudGPT などのツールを使用すると、初心者の攻撃者でも、従来の防御を回避する高度なフィッシングメールや洗練された標的型マルウェアを作成できます。

ランサムウェア攻撃は、2024 年第 4 四半期と比較して 2025 年第 1 四半期に 132% 急増し、AIを使った詐欺的なソーシャルエンジニアリングによってネットワークへの初期アクセスを獲得しました。[3]

世界中で毎秒 11 人がマルウェア攻撃の被害者となっています。これは年間 3 億 4000 万人に相当し、今後も指数関数的に増加し続けると予想されます。[4]

脆弱性の悪用は、AI 主導の脅威により 34% 増加しました。[5]

調査対象となった最高情報セキュリティ責任者の 78% が、AI を活用した脅威が組織に重大な影響を与えていると報告しました。[6]

61% の組織が 2024 年にディープフェイク攻撃の増加を確認しました。[7]

トップレベルドメイン（TLD）の数は何倍にも増加し（30 年前は7件、現在は 1,500 件以上）、攻撃者が AI を使用して類似ドメインを簡単に作成できるようになりました。[8]

最新の攻撃におけるトラフィック分散システムの役割

トラフィック分散システム（TDS）は、脅威アクターによって悪質なアクティビティの強化に採用されています。Google AdSense が関連性の高い広告にユーザを誘導してウェブサイトの収益化を支援するのと同様に、サイバー犯罪者は悪質な TDS を使用して、多くの場合は乗っ取られたウェブサイトや欺瞞的な広告を通じてユーザを悪質なサイトに誘導します。このリダイレクトチェーンは攻撃者のインフラストラクチャを隠すように構築されているため、従来のセキュリティツールではほとんど見えません。ステルス性があり、スケーラブルであり、悲しいことに、脅威アクターにとって非常に有益です。

- 悪意あるアドテクはTDSを使って、主に情報窃取型マルウェアを配信し、企業のデータ侵害の中心的役割を担っています。
- TDS を使用して Lumma Stealer を配布する大規模な偽 CAPTCHA キャンペーンである Vane Viper は、10,000 以上のドメインからなる巨大なインフラストラクチャを有しています。2024 年第 4 四半期には、3,000 以上の広告主サイトを通じて 1 日あたり 100 万回の広告インプレッションを配信しました。

DNS の力で組織を先制的に保護

先制的セキュリティ対策は、サイバー脅威が被害を引き起こす前に予測、予知、阻止することに重点を置いた高度なアプローチです。

Gartner 社は、先制的サイバーセキュリティを次のように定義しています。「サイバー攻撃の目的を阻止・妨害し、または抑止するための積極的なアプローチ。サイバー攻撃における脅威アクターの生成AIの使用が増加していることを考えると、先制的なサイバーセキュリティテクノロジーは、AI対応マルウェア、ゼロデイ脆弱性、ランサムウェア、その他の関連脅威に対する組織の防御を強化する上で重要な役割を果たします。これらの脅威は、従来の『Detect and Respond（検出と対応）』ツールやアプローチだけでは効果的に軽減できないことがよくあります。」

組織は DNS を使用して、オンプレミスのインフラストラクチャ、クラウドワークロード、リモートユーザ、IoT/OT デバイスを含む環境全体を高度で最新の攻撃から保護できます。

プロテクティブ DNS アプローチは、ゼロデイ攻撃に依存しないため、先制的です。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を提供します。

予測型脅威インテリジェンス：

マルウェアの亜種や個々のドメインを追跡するのではなく、攻撃前の活動を追跡し、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特定します。

DNSテレメトリと機械学習を活用して、高リスクドメインを特定し、脅威がネットワークに到達する前にブロックします。

TDS を検出してブロックします。これらは、ユーザをフィッシングサイト、エクスプロイトキット、またはマルウェアペイロードに動的にリダイレクトするために使用されます。

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

米国国立標準技術研究所（NIST）は、サイバーセキュリティにおける DNS の重要性を認識し、権威ある文書である NIST SP 800-81 にプロテクティブ DNS をガイドラインを含めました。このガイドは、DNS がサイバー防御の基盤層としての役割を果たすことを強調し、プロテクティブ DNS を既存のセキュリティインフラストラクチャに統合することで、組織は従来のセキュリティシステムよりも早く脅威を検出してブロックする能力を強化できると述べています。

「DNS サーバーはエンドポイントの接続とデータフローに関する重要な洞察を提供し、多くの場合、他のシステムよりも早くセキュリティインシデントを防ぐことができます。」

-**NIST**

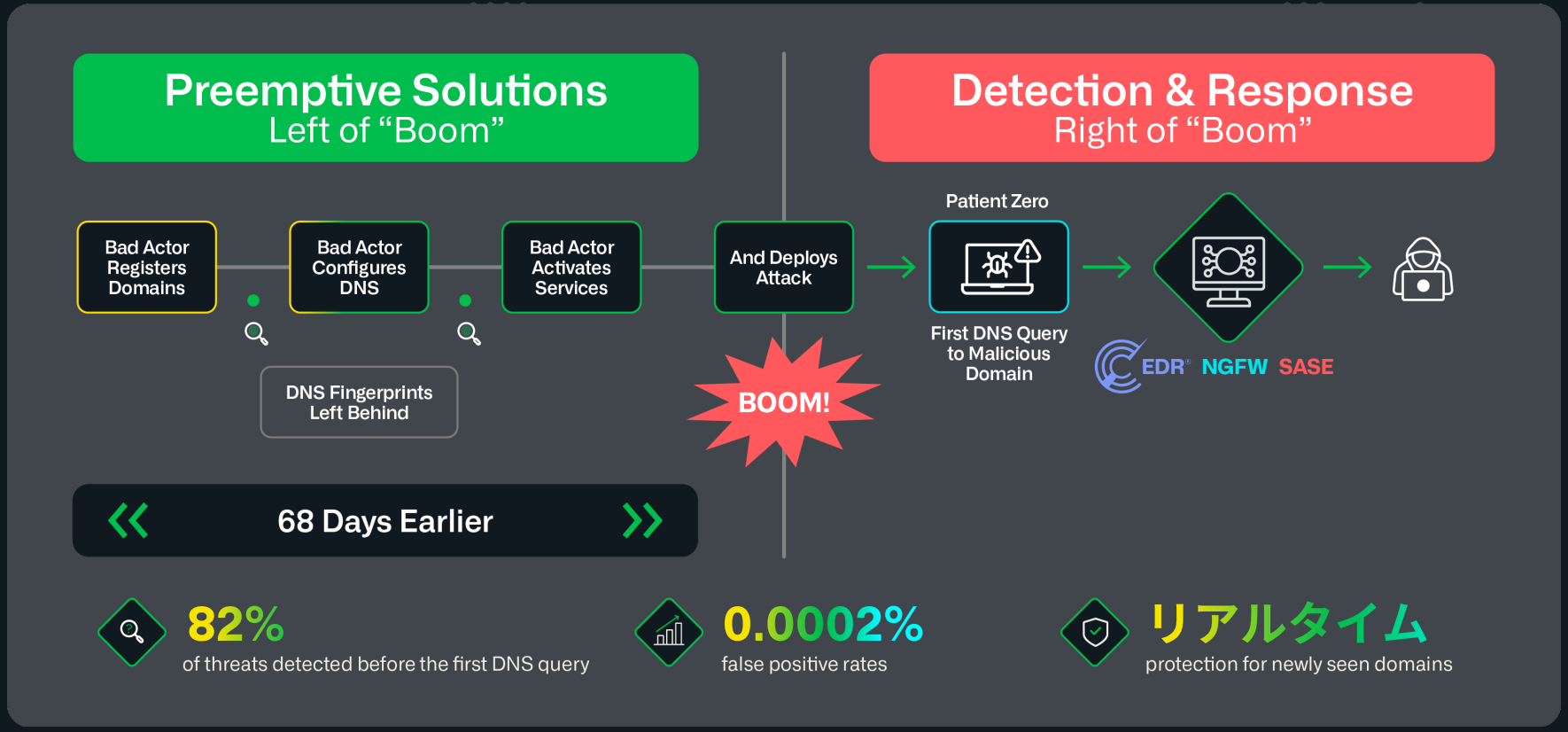
Infoblox の業界をリードするプロテクティブ DNS ソリューションである Infoblox Threat Defense™ は、事後対応型のセキュリティ対策に比べて多くの利点を提供します。

- 保護を**影響が出る前に**提供し、通信を意図した段階でも保護します。
- Infoblox は **DNS リゾルバ**（人間が判読できるドメイン名を機械が判読できる IP アドレスに変換するサーバーまたはソフトウェア）として、**ファイアウォールの背後にあるかどうか、SASE** エージェントがあるかどうかに関係なく、あらゆるデバイス（エンドユーザデバイス、IoT/OT を含む）からの**すべての DNS 接続を認識します。**
- **204,000 のリアルタイム**の脅威アクタークラスターまたは関連するサイバー攻撃活動のグループを監視します。
- 他の既知の悪意のある動作を探すセキュリティツールと比較して**5 倍多くの高リスク/中リスクドメインをブロックします**。
- 業界平均より **68.4 日早く**ブロックします。
- 最初の DNS クエリの前に**ドメインベースの脅威の 82% を検出します**。
- **誤検出**率は **0.0002%** です。
- **許可されていない AI の使用を** DNS アクティビティに基づいて識別してブロックします。
- **ダングリング DNS レコード**や類似ドメインによる露出を軽減するのに役立ちます。
- ファイアウォールやセキュリティ情報およびイベント管理（SIEM）システムなどの他のセキュリティツールの負**荷を 50% 軽減し**、システムに到達する前に**悪意のあるトラフィックをフィルターして排除**します。
- **ユーザとデバイスの属性**の簡単な特定と脅威の優先順位付けを資産インサイトで実現します。

INFOBLOX THREAT DEFENSE

204,000（現在も増加中）のほぼリアルタイムのクラスター／カルテルを発見し、監視

100 件以上の既知脅威アクターを特定・プロファイリング



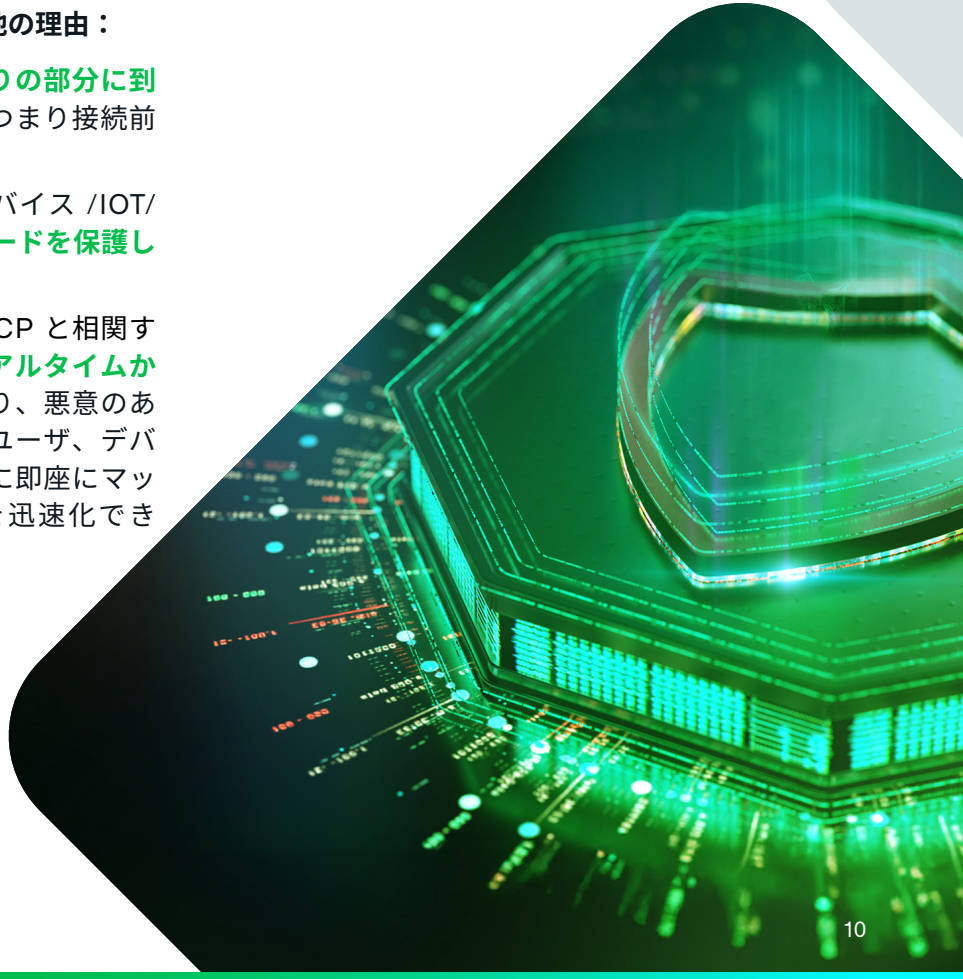
プロテクティブ DDI プラットフォームの力

プロテクティブ DNS は、DNS がすでに管理されている DDI プラットフォーム上で最も効果的に機能します。Infoblox は、統合されたプロテクティブ DDI プラットフォームを提供する唯一のベンダーであり、専門チームによる一元管理で、DNS 関連のあらゆる課題に迅速かつ確実に対応できます。

これにより、次世代ファイアウォール（NGFW）やセキュアアクセスサービスエッジ（SASE）ソリューションでプロテクティブ DNS を有効にする場合と比べて、運用とトラブルシューティングが大幅に簡素化されます。Infoblox を DNS リゾルバとして使用することで、組織は、企業の DNS クエリデータを脅威に対してモニターし、新しいドメインが Infoblox リゾルバに入った際にリスクを評価し、必要に応じてインラインでプロアクティブにブロックすることで、インシデントの発生を未然に防ぐ単一の統一プラットフォームの利点を享受できます。

プロテクティブ DNS を DDI プラットフォームで使用することが有利であるその他の理由：

- **セキュリティスタックの残りの部分に到達する前の最も早い段階、**つまり接続前段階でブロックします。
- 最も広い範囲でユーザ、デバイス /IOT/OT/ICS、**クラウドワークロードを保護します。**
- IP アドレス管理および DHCP と相関する DNS クエリに対する**リアルタイムかつネイティブの可視性**により、悪意のあるアクティビティを特定のユーザ、デバイス、またはワークロードに即座にマッピングして、調査と修復を迅速化できます。



ビジネス上の メリット

- データ漏洩によるリスクの低減。
- 平均して 1 か月あたり 500 時間の SOC アナリストの時間を節約し、年間 40 万ドルの生産性向上を実現。
- 投資回収期間が 6 か月未満で 243% のROI。
- 他のセキュリティツールによって生成されるアラートの数が 50% 削減され、運用コストが削減。

活用 事例

Infobloxのお客様は、さまざまなユースケースに Infoblox ソリューションを成功裏に導入しています。

ランサムウェアに対する積極的な保護

あるファストカジュアルレストランチェーンは、いくつかの注目を集めたランサムウェア事件の後、プロテクティブ DNS を実装することで、全体的なセキュリティ体制の改善へより積極的なアプローチを取ることにしました。また、脅威を監視するために DNS トラフィックを 100% 可視化したいと考えていました。

DNS を介したデータ流出の防止

ある大手健康保険会社は、レッドチームによる内部ペンテスト中に特定された DNS トンネリングに関するギャップを埋めましたが、既存の NGFW および SASE ソリューションではブロックできませんでした。

ゼロトラスト

ある運送会社は、DNS を活用したリモートアクセスと脅威検出を、エンドポイント検出と対応（EDR）やモバイルデバイス管理（MDM）などのエンドポイントソリューションと組み合わせて「誰でも、どこでも、一度に」保護するためのゼロトラストユーザとデバイス戦略を策定しました。

infoblox®

キルチェーンが始まる前に断ち切りましょう。
最初の被害者になることは避け、サイバーヒーローになりましょう。

詳細については Infoblox Threat Defense ページをご覧ください。
www.infoblox.com/jp/threat-defense

1. *CrowdStrike 2025 Global Threat Report: Beware the Enterprising Adversary*, Myers, Adam, CrowdStrike Blog, 2025年2月27日。
2. *Day 19: Analyzing DNS Logs — Detection Use Cases and How to Spot Malicious Activity*, Infosec Ninja, 2025年5月7日。
3. *Massive Surge In Ransomware Attacks—AI And 2FA Bypass In Crosshairs*, Winder, Davey, Forbes, 2025年3月25日。
4. *ITRC Annual Data Breach Report*, Identity Theft Resource Center, 2025年1月。
5. *Verizon 2025 DBIR Report*
6. *Top 40 AI Cybersecurity Statistics*, Fox, Jacob, Cobalt, 2024年10月10日。
7. *Speedy threat actors improving their lateral movement*, Hurley, Billy, IT Brew, 2025年3月4日。
8. ICANN—2012年、ICANN（Internet Corporation for Assigned Names and Numbers）はトップレベルドメイン拡張プログラムを開始し、組織がカスタムトップレベルドメインを申請できるようにしました。