ソリューションノート

INFOBLOX による現代的なゼロトラストの実現

はじめに

今日のデジタル環境では、ゼロトラストセキュリティモデルの採用がますます不可欠になっています。ガートナーの調査によると、世界中の63%の組織が、高度なサイバー脅威の軽減や業界ベストプラクティスの遵守を目的として、ゼロトラスト戦略を完全または部分的に導入しています。しかし、一般的なゼロトラスト戦略にはギャップがあります。多くの組織は、ユーザーがインターネット上でアクセスするドメインを暗黙のうちに信頼しています。これにより、組織は脅威アクターが所有する不審な、悪意のある、または類似のドメインにさらされる可能性があり、情報漏えいにつながる恐れがあります。ネットワーク内のトラフィックの流れを理解しなければ、ゼロトラストは実現できません。Infoblox は、ハイブリッドおよびマルチクラウド環境のセキュリティ確保において DNS が果たす重要な役割を強調し、ゼロトラストに対する最新のアプローチを提供しています。

> *ほとんどの組織では、ゼロトラスト戦略は通常、組織の環境の半分以下しか対処できず、軽減できるのは企業全体のリスクの 4 分の 1 以下です。*
>
> **Gartner**

ゼロトラストを施行する理由

ゼロトラストは、侵害は避けられないことを前提とし、そのような侵害の影響を最小限に抑えることに重点を置いたセキュリティフレームワークです。ゼロトラスト採用の主な推進要因には以下が含まれます。

- 脅威アクターの高度化
  - » ランサムウェアと類似ドメインによるスピアフィッシング
  - » トラフィック分散システム (TDS)
- ハイパーコネクティビティとデジタルイニシアティブ
  - » ハイブリッド、マルチクラウド環境
  - » IoT/OTとリモートワーク

ハイパーコネクティビティと、マルチクラウドやハイブリッドネットワークの採用などのユビキタスなデジタル変革により、侵害はますます一般的になっています。最初の侵入後、脅威は横方向に非常に迅速に移動する可能性があります。ゼロトラストアプローチは、侵害の範囲、影響、コストを抑えることができるため、組織はあらゆるインシデントに迅速に対処し、業務の中断を最小限に抑えることができます。

ゼロトラストの原則には、侵害を想定する、全く信頼せず常に検証する、最小権限のアクセスを使用する、常時監視、脅威の横移動を制限するためのセグメンテーションなどがあります。

ゼロトラストにおける DNS の考慮事項

DNS はゼロトラスト戦略において重要な役割を果たします。従来のゼロトラストモデルでは、DNS を見過ごし、暗黙のうちに信頼することがよくあります。これは重大なギャップとなり、ユーザーやデバイスがランサムウェア、フィッシング、類似ドメイン、ゼロデイ DNS などの脅威にリンクされた悪意のあるドメインにアクセスできる状態を作り出し、ネットワークを侵害にさらします。Infoblox は、ゼロトラスト戦略では DNS を暗黙のうちに信頼すべきではなく、以下を確保すべきであると強調しています。

- **暗号化および認証された DNS 接続**
- **データ持ち出しとゼロデイ DNS 脅威の監視**
- **悪意のあるドメインへのアクセスを防ぐプロテクティブ DNS（PDNS）**

Infoblox のアプローチには、プライバシー保護のための暗号化された DNS、アクセス決定のための最新の資産データ、および高リスクのドメイン、コマンドアンドコントロール（C2）通信、データ持ち出しをブロックするための PDNS が含まれます。

エンタープライズ向けの暗号化された DNS

NIST SP 800-207 には、「すべての通信は、利用可能な最も安全な方法で行い、機密性と整合性を保護し、ソース認証を提供する必要があります」と記載されています。これには再帰的なDNS解決のためのプライバシーの有効化（スヌーピング対策）を含める必要があります。暗号化には一般的に認知されている指定ポート 853 を使用するDNS over TLS（DoT）と、ウェブトラフィックを分散するためにポート 443 を使用する DNS over HTTP（DoH）が含まれます。

エンタープライズ向けプロテクティブ DNS

Infoblox のエンタープライズ向けプロテクティブ DNS（PDNS）ソリューションは、次のような事前対応的なセキュリティを提供します。

- **高リスクドメインの解決を拒否することで、初期感染を防止**
- **進行中の C2 通信の停止**
- **データ持ち出しを阻止**

Infoblox PDNS は、脅威インテリジェンス、AI/ML エンジン、DNS ポリシーの適用を統合し、サイバー脅威に対する包括的な保護を提供します。コンポーネントには、以下が含まれます。

- **再帰的 DNS サーバー：**ドメインの IP アドレスを検索し、クライアントに返します
- **DNS 脅威インテリジェンス：**脅威アクターが所有する、リスクが高く悪意のあるドメインを特定
- **AI/ML 学習エンジン：**組織の DNS トラフィックをリアルタイムで検査し、行動分析を実行することで、高度な脅威を特定
- **DNS ポリシー Engine/RPZ：**設定されたポリシーに基づいて DNS 解決を許可または拒否

デバイスレベルの適用

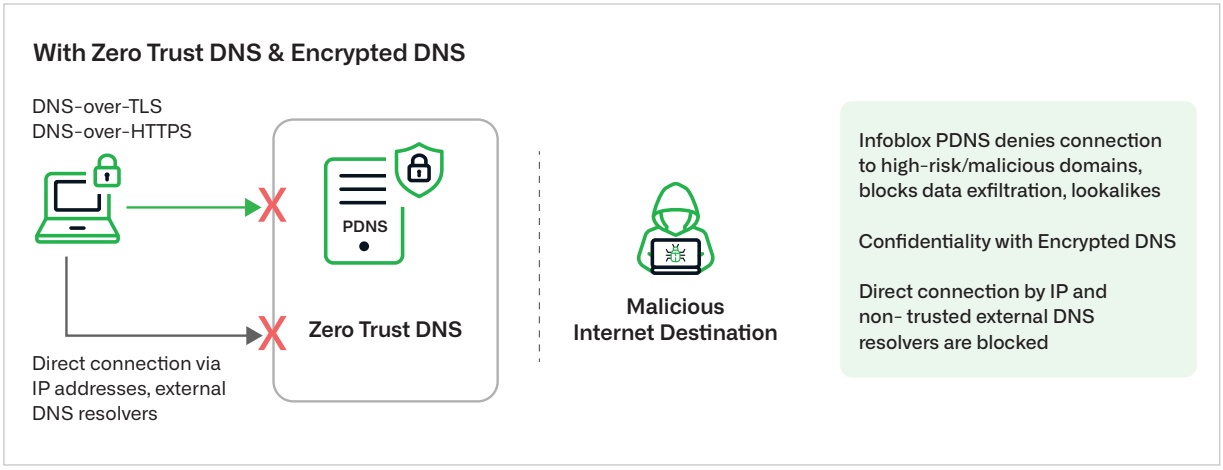
Infoblox の Zero Trust DNS モデルには、DNS バイパスを防ぎ、送信 IP トラフィックを制限するためのデバイスレベルの適用が含まれています。これにより、デバイスは承認された PDNS サーバーにのみ接続されるようになり、ネットワーク全体のセキュリティが強化されます。

資産検出と ZERO TRUST システムへのデータ入力によって、アクセスを判断

すべてのネットワーク資産に対する可視性は、ゼロトラストにとって非常に重要です。Infoblox の Universal Asset Insights は、ハイブリッド、マルチクラウド環境全体の資産の統合ビューを提供し、検出と分析を自動化します。これにより、最新の資産インベントリを維持し、不正なデバイスを検出し、デバイスのアクティビティと ID を関連付けることができます。DNS と IPAM メタデータはテレメトリーの重要なソースであり、詳細なクライアント情報とネットワークの動作を Zero Trust システムへの入力として提供します。アクセスに関するより良い決定やポリシーの割り当てに使用できますが、ユーザーやデバイスの位置情報、ネットワークスイッチポートなどに基づいてアクセスが許可される場合と許可されない場合があります。たとえば、Infoblox は、デバイスがプリンターであり、特定のドメインにのみアクセスできることを通知できます。もう 1 つの例として、Infoblox は IoT/OT デバイス（カメラなど）を識別し、過去 1 週間に特定の DNS 呼び出しのみが行われたことを判断できます。管理者は、これらのカメラに対してゼロトラストポリシーを作成することを決定できます。

自動化とオーケストレーション

Zero Trust は、セキュリティ対応機能をサポートする上で、自動化とオーケストレーションに大きく依存しています。Infoblox はさまざまなセキュリティツールやプラットフォームと統合し、ポリシーの適用、脅威の検出、インシデント対応を自動化し、コンテキスト情報を提供します。



結論

Infoblox の Zero Trust ソリューションは、最新のネットワークを保護するための堅牢なフレームワークを提供します。DNS ベースのセキュリティ、資産の可視性、および自動化を統合することで、Infoblox は組織が効果的なゼロトラスト戦略を実装し、サイバー脅威のリスクを軽減し、全体的なセキュリティ体制を強化できるようサポートします。

Infoblox はネットワークとセキュリティを統合して、比類の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
2-26-37VORT外苑前I 3F

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

バージョン：20241205v1