データシート

BloxOne® Threat Defense Advanced

セキュリティ体制を基盤から強化し、最適化

大規模な基盤セキュリティの必要性

従来のセキュリティモデルでは、今日のデジタルトランスフォーメーションの時代に対応できません。

- 境界が変化し、ユーザーはどこからでもクラウドベースのアプリケーションに直接アクセスできます。
- IoT の導入は、保護のために従来のエンドポイント技術を受け入れないデバイスの爆発的な増加につながっています。
- ほとんどのセキュリティシステムは複雑で、これらの動的な環境を保護するために必要なレベルにまで簡単に拡張することはできません。

組織が必要としているのは、追加のインフラストラクチャの導入や管理を必要とせずにネットワーク全体を保護する、スケーラブルでシンプルな自動化されたセキュリティソリューションです。

INFOBLOX は、既存の脅威防御への投資を最大化するスケーラブルなプラットフォームを提供

Infoblox BloxOne Threat Defense Advanced は、包括的な DNS Detection and Response（DNSDR）ソリューションで、他のソリューションが見逃している脅威活動を検出し、攻撃者のサプライチェーンを混乱させるハンティングを使用して、キャンペーン前の DNS 脅威インテリジェンスによって攻撃を事前に阻止します。インテリジェントなエコシステム統合と自動化により手作業が軽減されるとともに、Infoblox 独自の AI 主導の分析により、アナリストを最も重要なことに集中させ、平均修復時間を短縮し、既存のセキュリティツールの ROI を高め、全体的な SecOps 効率を向上させる洞察を提供します。

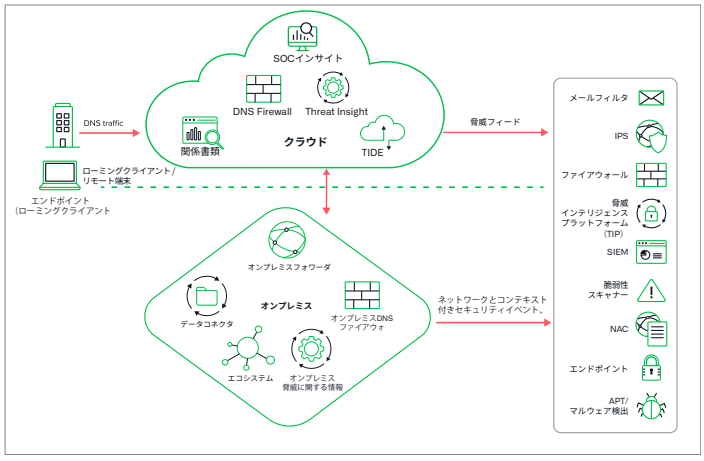


図 1: *Infoblox* ハイブリッドアーキテクチャにより、どこでも保護され、どこでも導入可能

主な機能

- 他のソリューションでは見逃されるセキュリティ上の弱点、フィッシング、ランサムウェア、その他の最新のマルウェアを検出してブロック
- プラットフォームや OS に関係なく、BYOD、IoT、ICS などの DNS 層でユーザーとデバイスを保護
- 高リスクのアプリケーションを検出し、シャドー IT、インサイダー、コンプライアンス、その他のリスクを管理
- DNS ベースのデータ窃取、DGA、DNSMessenger を含む
- 機械学習 / AI 分析を使用してデータ窃取手法を防止
- 不適切または不要な Web コンテンツへのユーザーアクセスを制限し、活動を追跡
- 最も価値の高いインターネット資産を類似ドメイン監視を使用して企業ブランドを保護
- 調査を 3 倍加速化し、脅威への対応と脅威ハンティング活動を効率化
- 可視性の向上 : IPAM 資産メタデータと統合することで、正確な可視性と豊富なネットワークコンテキストを取得し、イベントの理解と相関関係を最適化
- SOC Insights を使用して、最も重要な脅威に対する調査と対応を迅速に開始し、AI 主導の洞察で平均修復時間を短縮

セキュリティオペレーションセンターの効率を最大化

インシデント対応時間の短縮

- 悪意のある活動を自動的に阻止し、調査、隔離、修復のためにセキュリティエコシステムの残りの部分に脅威データを提供
- コンテキストによるネットワークと脅威インテリジェンスのデータ、Infoblox エコシステム統合(SOAR を実現するための最重要要因)を使用して SOAR ソリューションを最適化し、脅威への応答時間と運用コストを削減
- Infoblox SOC Insights を使用して、単純なマルウェアリスクのランク付けダッシュボードの枠を超え AI 主導の分析により、どのイベントが最も重要かを把握

セキュリティポリシーと脅威インテリジェンスのポータビリティを統合

- 内部と外部ソースから脅威インテリジェンスデータを収集・管理し、既存のセキュリティシステムに配布
- セキュリティスタック全体にわたる脅威インテリジェンスの有効性を向上させながら、脅威フィードのコストを削減

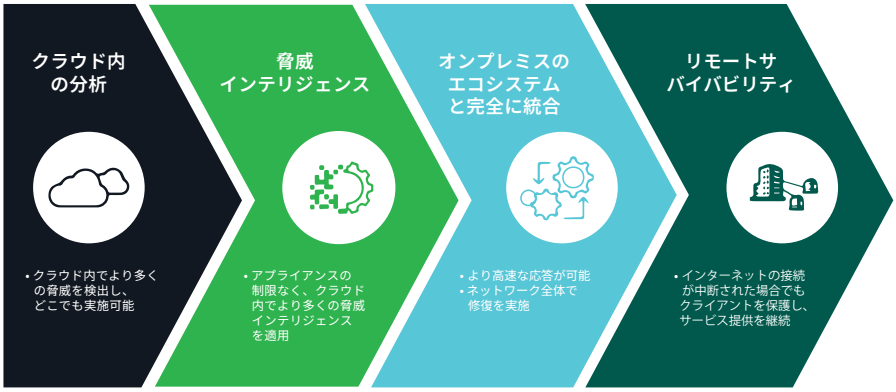
脅威の調査とハンティングの迅速化

- 最も重要な脅威に対する調査と対応から迅速に開始し、単純なマルウェアのリスクをランク付けしたダッシュボードを超えた AI 主導のインサイトにより MTTR を短縮
- 自動化された脅威の調査、関連する脅威についてのインサイト、専門のサイバーソースによる調査視点を加えて、セキュリティアナリストに提供することで、脅威に関して迅速かつ正確な判断を可能にし、脅威アナリストチームの **生産性を 3 倍向上**

図2: *BloxOne Threat Defense*はサイバーセキュリティエコシステム全体と統合されています

> 今のこの時代には、手に負えないほど多くのランサムウェア、スパイウェア、アドウェアが、インターネットユーザーによって開かれ、そのリンク経由で侵入してきています。*Infoblox* 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てくれます。
>
> **上級システム管理＆ネットワークエンジニア**
> **シアトル市立大学**

ハイブリッドアプローチにより、導入場所を選ぶことなく保護



クラウドでの分析

- クラウドの優れた処理能力を活用し、機械学習ベースの分析を使用するデータ窃取、ドメイン生成アルゴリズム（DGA）、ファストフラックス、ファイルレスマルウェア、辞書に基づく DGA など、より広範な脅威を検出
- クラウド内の脅威を検出し、場所を選ぶことなく適用して、本社、データセンター、リモート端末、モバイルデバイスを保護します。

脅威インテリジェンスのスケーリング

- Infoblox のリサーチとサードパーティプロバイダーからの包括的なインテリジェンスを適用して、オンプレミスまたはクラウドでポリシーを適用し、残りのセキュリティインフラストラクチャに自動的に配布
- 各サイト用のセキュリティ装置に多額の投資を行うことなく、クラウド内にもっと多くの脅威インテリジェンスを適用

セキュリティエコシステムとの強力な統合

- オンプレミスの Infoblox とサードパーティのセキュリティ技術と完全に統合できることで、ネットワーク全体での修復が可能になり、それらの技術への投資利益率が向上

リモートサバイバビリティ／弾力性

- インターネット接続に障害が発生した場合でも、オンプレミスの Infoblox がネットワークのセキュリティを確保

BloxOne Threat Defense を使用して、データとインフラストラクチャを保護する方法の詳細情報は、https://www.infoblox.com/products/bloxone-threat-defense をご覧ください。

INFOBLOX セキュリティへの投資利益率

負荷のかかるセキュリティデバイスを軽減

- すでに利用可能な DNS サーバーを防御の第一線として使用することで、ファイアウォール、IPS、Web プロキシなどの境界セキュリティデバイスの負荷を軽減
- **NGFW* に送信された**トラフィックを最大 60 倍削減

既存投資の ROI を改善

- 脅威と攻撃者の情報を双方向で共有することで周辺機器や補完製品からより多くの価値を引き出す
- DNS データを SIEM に送信する場合は、これらのプラットフォームへの疑わしい DNS データのみを送信することで、SIEM ソリューションのコストを削減

自動化

- 自動化により人間による操作 / エラーのコストを削減
- ベテラン人材不足を克服 - 実装（数か月ではなく数時間で構成）に要する要求と運用に必要なスキルとコストを 60% 削減
- 深く脅威インテリジェンスを実現する使いやすい単一コンソールにより、脅威アナリストの生産性が 3 倍向上

*実際の顧客データに基づく

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 2-26-37
VORT 外苑前 3F

03-5772-7211
www.infoblox.com

バージョン：20240122v1