データシート

Infobloxによる通信事業者のセキュリティ体制の向上

セキュリティの有効性と回復力を改善し、SecOps 効率を向上

課題

今日の通信サービスプロバイダー（CSP）ネットワークは、プライベート、パブリック、ハイブリッドネットワークにまたがるテレコクラウドへと進化しており、RAN、ケーブルおよびコアネットワーク、プライベートクラウドとパブリッククラウド、マルチアクセスエッジ・ロケーションにわたって運用ドメインが拡大しています。演算処理とストレージがエッジに移行し、数千の新しいサイトで新しいタイプのサービス処理と配信を可能にするにつれて、サードパーティ・アプリケーションや外部攻撃者からのセキュリティ脅威が発生する可能性が劇的に増加します。事業者は膨大な量の個人データを保管しており、通信サービスの安定性に責任を負っています。データセンター外にデバイスが広く展開されることで、アクセスポイントの数が増加し、攻撃者が悪用できる大規模な脅威の攻撃対象領域が生まれます。サイバー攻撃によるデータ侵害やサービス障害は、深刻な財務的損害や評判の損失、または顧客への影響を引き起こす可能性があり、競争の激しい市場ではどの企業にとっても耐え難い大きな打撃となります。

ファーエッジに導入されるリソースが増えるにつれ、オペレーターの IT チームとセキュリティチームは、物理、仮想、クラウド環境で、はるかに多くのポッド、VM（時には数百台、場合によっては数千のコンテナ）を管理する必要があります。パッチが適用されていないデバイスは、侵害の危険にさらされる可能性があります。検出および対応機能を備えたエンドポイント保護は必須ですが、すでに負担がかかっているセキュリティチームは、進化し成長するネットワークにおいて、どのような場合でも攻撃の兆候を認識する必要があります。CSP には、可視性を拡大して最新の脅威を特定し、調査を短縮し、効率的なインシデント対応を加速する、成熟したサイバーセキュリティ・ソリューションが必要です。

解決策

Infoblox のサービスプロバイダー向けソリューションは、加入者とデジタル世界をつなぐために不可欠な IP 接続を提供します。DNS、DHCP、IP アドレス管理（DDI）を統合し、ネットワークの可視性、スケーラビリティ、管理を自動化します。当社のソリューションは、セキュリティ、オーケストレーション、自動化、およびレスポンス（SOAR）システムを含む、セキュリティスタックの主要コンポーネントをすべて有効にすることで、インシデント対応時間を 3 分の 1 まで短縮し、セキュリティイベントが損害を引き起こす前に迅速に対応できるようにします。また、DDoS やその他の DNS ベースのリスクや攻撃によって引き起こされるビジネスの混乱を最小限に抑えるようにプロバイダーを支援します。

主な機能

セキュリティ保護を強化
他のソリューションでは検出できないエクスプロイト、フィッシング、ランサムウェア、およびその他最新のマルウェアを検出してブロックします。

可視性を高める
IP アドレス管理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・コンテキストを獲得し、イベントの理解と相関を最適化します。

インシデント対応を加速
数十のソースからイベント、ネットワーク、脅威インテリジェンスを自動的に関連付けることで、調査を最大 3 分の 2 迅速化し、修復までの時間を短縮します。

セキュリティ ROI の向上
より強力な防御とセキュリティ運用の効率化を通じて、最小限の労力で最大の価値を認識し、SIEM および SOAR プラットフォームやその他のセキュリティツールをさらに活用します。

セキュリティのオーバーヘッドを削減
DNS 上の豊富なイベント、脅威インテリジェンス、AI/ML ベースの分析を活用して、最新のマルウェアや DNS 脅威に対するスケーラブルな保護を提供します。

Infoblox は、拡大した境界防御の負担を軽減することで、脅威防御の総コストを削減します。当社のソリューションは、セキュリティイベント情報のリアルタイムな双方向共有と、手作業や人為的なミスに伴うコストを削減する自動化により、セキュリティチームが既存のサードパーティ製セキュリティソリューションからより多くの価値を得られるようにします。セキュリティアナリストは、イベントに関連する脅威インテリジェンスを一元的に把握し、脅威調査の時間を最大で 3 分の 2 短縮することができます。

ネットワークの中断を最小限に抑制
DNS の整合性を維持し、ネットワークをオフラインにする可能性のある外部および内部の DNS DDoS 攻撃を防ぎます。

主なメリット

他の防御では見逃す脅威を阻止

脅威インテリジェンスが向上すると、すべてのセキュリティツールの有効性が高まります。BloxOne® Threat Defense は、Infoblox、その他の商用ツール、サードパーティの政府ソースから脅威情報を収集、整理、集約します。Infoblox Cyber Intelligence Unit（CIU） による収集で、誤検出を最小限に抑えながら正確性を高め、お客様のニーズに合わせて収集をカスタマイズします。その後、正規化された「スーパーフィード」をセキュリティスタック全体で共有できるため、あらゆる防御対策の効果が高まります。

マルウェアやデータ流出をブロック

BloxOne Threat Defense は、DNS レベルで動作して、他のソリューションでは見逃されるような脅威を検知し、脅威ライフサイクルの早い段階で攻撃を阻止します。複数の情報源から収集した脅威インテリジェンスと高度な AI/ML を活用して、悪意のあるサイトへのアクセス、コマンド＆コントロール（C&C）通信、DNS ベースのデータ盗難、その他の悪意のある活動をブロックします。

ビジネスの中断を最小限に抑制

DNS は、あらゆる組織の基盤として、ミッションクリティカルなネットワーク接続を提供しています。DNS がダウンすると、ビジネスが中断するため、DDoS 攻撃が成功した場合、組織は毎月数十万ドルの収益を失う可能性があります。Infoblox Advanced DNS Protection（ADP）は、あらゆる種類の DNS／DDoS 攻撃から効果的に防御し、組織のサービスの稼働時間を維持します。

迅速な調査と修復

アナリストは、対応を迅速に行うために、イベントに関する信頼できる脅威情報やその他のコンテキストデータにアクセスする必要があります。BloxOne Threat Defense の一部である DossierTM を使用すると、アナリストはイベントに関連する脅威インテリジェンスを単一の画面で確認できます。イベント固有の情報に迅速にアクセスすることにより、脅威の調査時間を最大 3 分の 2 短縮できます。

SIEM、SOAR などを強化

サイバーセキュリティチームは、幾重にも張り巡らされた多層防御ツールを装備しているため、何十ものセキュリティツールを手動で管理し、毎日何百、何千ものアラートに対応する必要性に圧倒されることがあります。Infoblox の Ecosystem Exchange が提供する、高度に連携した各種インテグレーションにより、セキュリティチームはサイロを排除して、SIEM および SOAR ソリューションを最適化し、サイバーセキュリティエコシステム全体の ROI を向上させることができます。

自動化で SecOps の負担を軽減

BloxOne Threat Defense には、脅威情報、イベント情報、その他のデータをよりインテリジェントに活用できるようにサポートする多くの機能が含まれています。自動化により管理関連の諸経費が削減され、SecOps の調査や対応作業が効率化されます。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します。

ネットワークの変更と構成管理を簡素化および効率化

多くのネットワーク問題の根本原因は、変更に起因します。デバイスを手動で変更する際のミス、不適切な構成の設定が後に問題を引き起こし、重要なセキュリティポリシーとネットワーク保護を弱体化させることがあります。Infoblox NetMRI は、デバイスのプロビジョニングやセキュリティ操作などの日常的なワークフローを自動化し、コンプライアンスの強化とインシデント対応の迅速化を実現するネットワーク変更および構成管理ソリューションです。

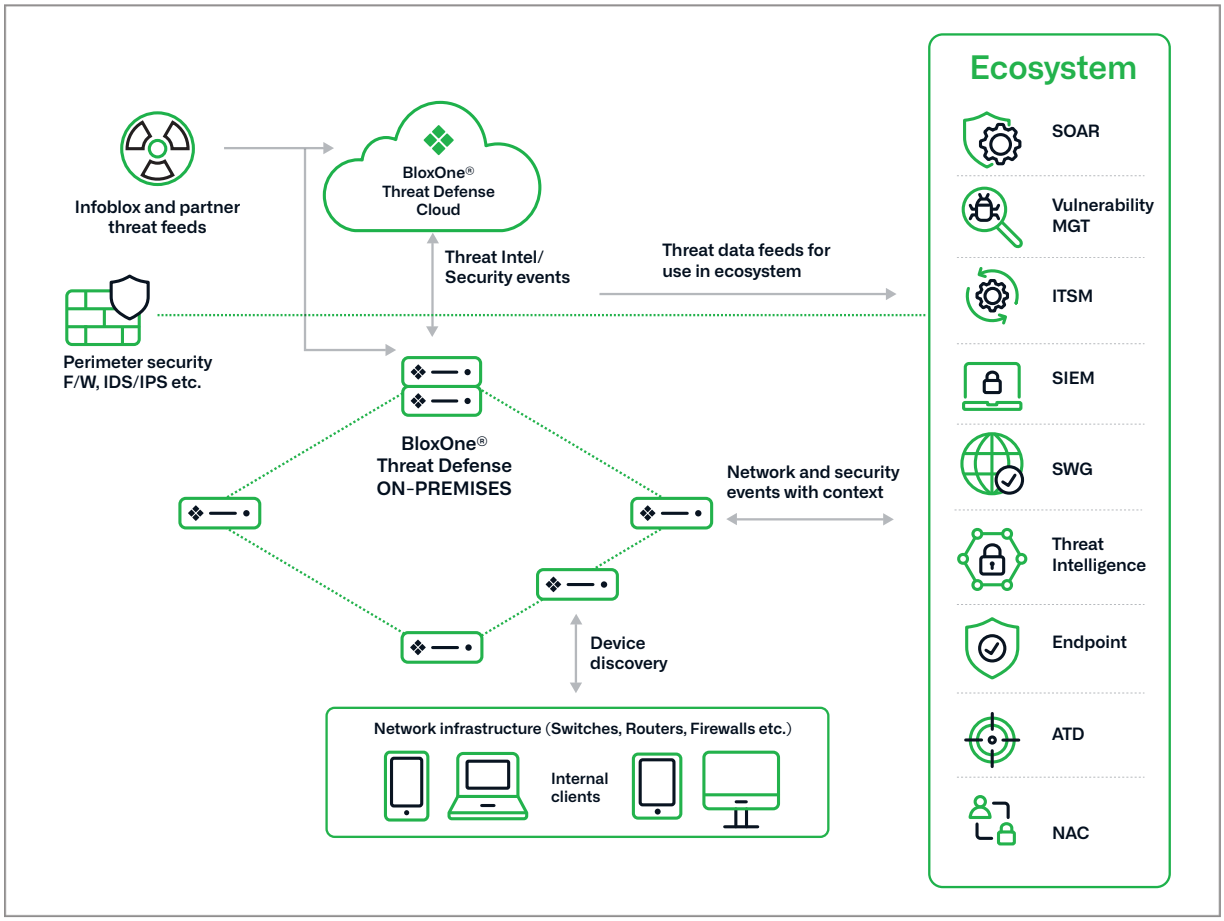

図 1：Infoblox は通信サービスプロバイダーのネットワークを強化し、最適化します

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：20240521v1