大手通信業者のネットワークセキュリティを強化し、クラウドファイアウォールサービスで顧客を保護

アメリカの通信事業者は、効果的かつ自動ネットワークセキュリティレイヤーを導入し、顧客をサイバー攻撃から守るためのクラウドセキュリティサービスを拡張しています。

顧客の課題：

- 企業ネットワークが既知の脅威ソースと通信しないよう保護する
- 優れたセキュリティを途切れることなく、顧客に提供する
- クラウドサービスを使用しつつ、厳格なパフォーマンス用件を満たす

選ばれたソリューション：

- 企業ネットワーク保護のために選ばれた ThreatSTOP IP ファイアウォールと DNS ファイアウォールサービス
- DNS ファイアウォールサービスは、顧客へ展開し、途切れることなく多くのメリットを提供
- 新規にハードウェアを用意する必要がなく、問題なく導入が完了

結果：

- 企業ネットワークのセキュリティレベルが目覚しく向上。クラウドサービスは迅速に導入され、管理の手間も不要
- セキュリティが確保されたサービスの提供により市場における差別化を実現し、マルウェア感染リスクの低減により顧客層の満足度を向上

顧客の課題：

米国の通信事業者が、精度の高い脅威インテリジェンスを使って TCP/IP と DNS 脅威を自動的に遮断するクラウドベースのセキュリティソリューションを探していました。理想的には、この脅威インテリジェンスデータを使って、既知と新規の脅威を遮断するファイアウォール規則を自動更新するソリューションである必要があり、そのユーザーがすでに使用してるファイアウォール(NGFW)や DNS、DDI、IPAM デバイスに対応していればなお望ましいと考えていました。また、競争入札で落札するためには、広い範囲にわたる顧客層にまでサポートが行き届くテクノロジーを選択する必要があります。何百万台というデバイスの DNS トラフィックを中断せず、かつ顧客からのサポートリクエスト件数を増やさずに保護するには、クラウドセキュリティサービスが必要不可欠と考えていました。

成功の鍵となる主な 3 要素：

- エンドユーザーに対する明確さ
- 非常に効果的な保護
- リスクの心配がない展開

企業概要

顧客タイプ：通信事業者（Forbes20）

業界：通信業界

場所：アメリカ合衆国

従業員数：175,000 人以上

そのユーザーは、自社ネットワーク、そして理想的には集中型クラウドソリューションを使用している顧客の両方でマルウェア感染率を減少させたいと考えていました。しかし、社内ユーザーと顧客に対して明確にするため、誤検知率が低いテクノロジーを選ぶ必要があります。セキュリティソリューションが原因で顧客との関係に問題が生じたり、サポートリクエスト件数が増加したりすることは、競争が激化している通信業界においては許されない事態です。またこの通信業者は、サービスへの接続を保証するためホワイトリストへのカスタム入力を行い、それを簡単に管理する機能や、社内セキュリティチームのアドバイスに応じてネットワーク接続の遮断を迅速に解除するメカニズムも必要としていました。

この通信事業者はインバウンドスキャンと攻撃の両方を遮断するだけでなく、ランサムウェア、フィッシング、そしてその他の標的型攻撃による DNS トラフィックについても懸念を持っていました。選択するソリューションは、広く脅威インテリジェンスを収集し、専門家チームによって管理され高い品質を保ち、非常に高い検知率を実現するものでなければなりませんでした。さらに、ユーザーは社内で生成した自社の脅威インテリジェンスと統合できるプラットフォームとしてのソリューション機能を求めていました。

サポートに関しては、技術的な機能や性能だけでなく、他のセキュリティ製品との連携について精通しており、ポリシー選定や継続的なセキュリティ関連の質問に対して専門的な意見を言うことができる、豊富な知識があり常に対応できを持ったスタッフによってサポートがあると考えていました。

ソリューション

POC（Proof of Concept）の後、この通信会社は DNS ファイアウォールと IP ファイアウォールサービスの両方を含む ThreatSTOP のプラットフォームを選定しました。ThreatSTOP のクラウドサービスは幅広いデバイスに対応しており、通信事業者の厳しい技術的要件を満たしていました。顧客トラフィックを保護するための展開をサポートするための次のパフォーマンス評価ポイントがクリアされていました：

- 選ばれるソリューションは、サポートする 1 秒あたりの DNS クエリ数が最低 445,000 必要である

- 最低 300,000 IOC において DNS RPZ フィードを使用した際、顕著なパフォーマンス低下がみられないパフォーマンスインパクトによるシステムリソースの増加が 3%以下である
- 段階的展開に対応するため、ソリューションはログのみ、または TAP モードをサポートする
- 計画に基づく RPZ ゾーン転送によりシステムパフォーマンスが著しく損なわれてはならない
- フィッシングカテゴリに対する誤検知は 1～2 ヶ月あたり 1 件未満である必要がある
- RPZ ゾーンのカスタマイズ：ホワイトリスティング、ブラックリストおよびリダイレクション（「グレーリスティング」）
- IPv4 と IPv6 両方のネットワークとデバイスに対応
- 複数のデータセンターとシームレスに統合するための IPv4 と IPv6 両方における Anycast サービス

展開は次の 2 つのフェーズで実施：第 1 フェーズでは、通信会社の実稼動環境において既存の次世代ファイアウォールと DDI/IPAM デバイス上で IP と DNS ファイアウォールクラウドサービスの効果を検証するために社内展開を行い、第 2 フェーズでは DNS ファイアウォール保護を顧客ベースにまで拡張しました。

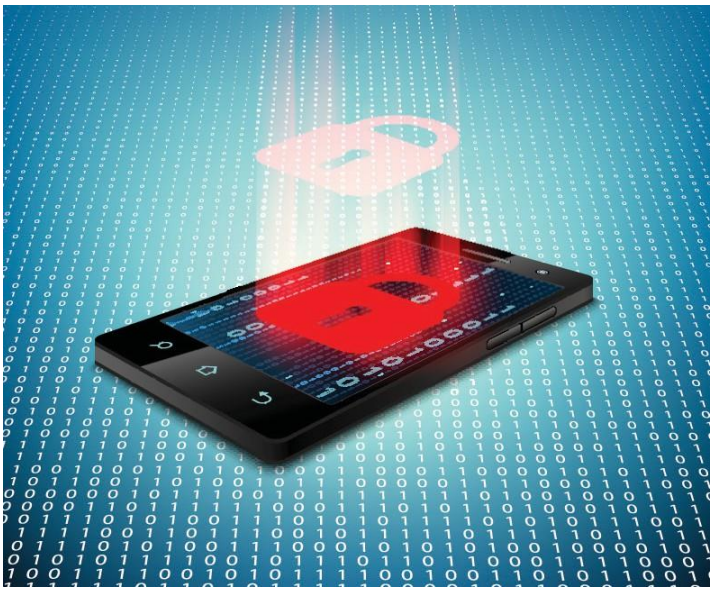
実装フェーズ

IP ファイアウォールと DNS ファイアウォールソリューションがユーザーの自社ネットワークに導入される際に、技術的問題は一切発生しませんでした。しかし、この大規模な導入により、セキュリティ増強を考慮する際にあらゆる組織が直面する最も基本的な問題が発生しました。ワークフローと日常的な業務運営に支障をきたす恐れのある誤検知を発生させずに総合的な保護レベルをどう向上させるかという問題です。

これに対処すべく、ユーザーは ThreatSTOP のセキュリティ調査チームと密に連携して、会社特有のニーズにあった各種ポリシーを作成しました。ThreatSTOP とユーザーのセキュリティチームは共同で、DDoS、脆弱性スキャナー、および標的型フィッシング攻撃で知られるインフラストラクチャなど、通信業界を標的とすることが多い特定タイプのマルウェアを遮断する社内用のポリシーを定義・実装しました。顧客向けに作られたポリシーは、過検知による過剰遮断の可能性を最小化にし、最悪の脅威を遮断する手法を採用しています。当初、ソリューションはログのみのモードで実装されるため、顧客のネットワークとセキュリティチームがソリューションの機能を観察し、通信を遮断しないレポート専用モードでソリューションのインパクトを把握することができます。ユーザーが測定結果に満足した場合、ソリューションは通信を遮断するモードに切り替えられ、接続が試行された時点で ThreatSTOP のソリューションによるリアルタイムの脅威遮断が開始されます。

ユーザーが選んだ ThreatSTOP が、候補とされていた他のテクノロジーよりも課題解決に優れていたことが明らかになるまで時間はかかりませんでした。ユーザーが調査した個々の RPZ フィードベンダーが有する脅威インテリジェンスデータは、迷惑メールやフィッシングなど特定の脅威タイプへの防御に特化されたものが多く、対象範囲が狭すぎました。ThreatSTOP なら、ユーザーは自社ネットワークと顧客の両方を、幅広い種類のマルウェアと攻撃タイプから守り、同じプラットフォーム内で自社の脅威インテリジェンスデータを活用することができました。 ThreatSTOP では、悪意があり、望ましくない接続試行の遮断を、ユーザーが自社ネットワーク内で強制的に実施することも可能でした。ThreatSTOP の IP ファイアウォールおよび DNS ファイアウォールサービスはローカルトラフィック規則を動的に更新し、解決方法を決定する際に DNS クエリトラフィックをネットワーク外に送信する必要がないため、TCP/IP でも DNS トラフィックでも追加のレイテンシが発生しません。

さらに、ThreatSTOP は特許に基づく DNS 利用方法によりセキュリティポリシー更新を送信しており、これは信頼性、スケーラビリティ、効率において優れていることが証明されています。調査対象であった他のソリューションは専用のコネクタを使用していましたが、通信事業者はこれが障害となる可能性が高いとみなし、接続性とセキュリティ保護のアップタイムを最大限に維持する責任があるネットワークチームにとっては懸念となっていました。



結果

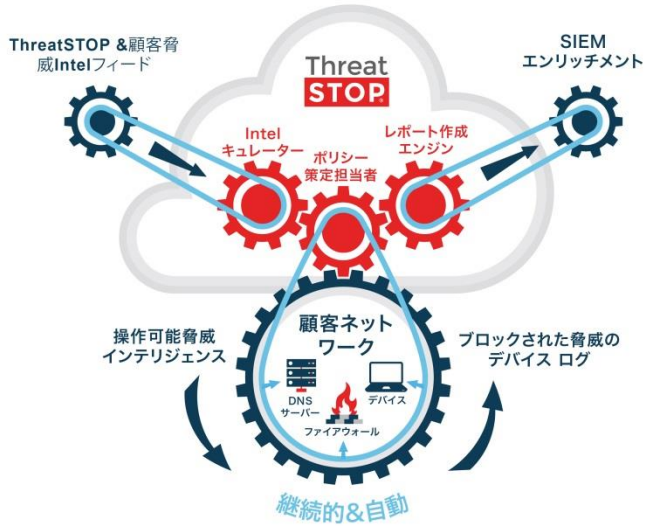
2014 年 8 月、ThreatSTOP の IP ファイアウォールと DNS ファイアウォールテクノロジーは世界各国で展開され、社内ネットワーク保護に加え、幅広い顧客層に対するセキュリティも格段に向上し続けており、これにより市場における差別化を図ることができました。競争が激化する通信事業で人材の消耗を低下できたのは ThreatSTOP の功績であると、このユーザーは、強く確信しています。感染した顧客のデバイスのサポート案件率は、展開前の類似案件率と比較して 28%も減少しました。ユーザーはサポート案件が増加すると予想していましたが、総合的にサポートの負荷が軽減されたことに非常に満足しています。ThreatSTOP はグローバル展開後、ThreatSTOP DNS ファイアウォールクラウドサービスを導入している 100 台以上の DNS サーバーについて、ユーザーからレベル 2 以上のサポートリクエストは一切受け取ったことがありません。

このユーザーでは、ThreatSTOP の IP ファイアウォールクラウドサービスを展開したことにより、自社ネットワークインフラストラクチャ内の感染率が減少し、社内で提出されるヘルプデスクへの質問の件数も減りました。さらに、IP ファイアウォールサービスが提供するインバウンドフィルタリングにより、パケットのヘッダコンテンツに基づく不要なインバウンド TCP/IP トラフィックが減少し、関連パケットトラフィックの受信や詳しい調査が必要なくなるために、帯域幅使用率が 20%近く減少しました。この帯域幅の減少により、多額のコストが削減され、ユーザーのネットワーク向けのセキュリティに対する姿勢が強化されたため、メリットは二倍になったと言えます。この通信業者のネットワークについて、ThreatSTOP は 24 時間当たり平均して 700 万件のインバウンド攻撃と悪意のあるアウトバウンド接続試行をかわしています。

ThreatSTOP の堅牢な IP ファイアウォールサービスは、2 年間を超える実稼動展開において 99.999%の総合的アップタイムを誇る安定性と信頼性の高いサービスを提供してきたことが証明されたため、現在このユーザーは、自社からインフラストラクチャをリースしている他の小規模な局地的 ISP 会社のトラフィックを保護するために第 3 フェーズの拡張を検討しています。

このユーザーのセキュリティチームは、ThreatSTOP の REST API を使って豊富なローカルイベントデータを利用し、IP アドレスとドメインに関するコンテキストデータを提供しています。ユーザーは ThreatSTOP の豊富な脅威インテリジェンスを既存の自社 SIEM システムと統合できるため、分析担当者は広範なネットワーク内で観察されるトラフィックに対して脅威分類、リスク評価、および時系列に沿ったそのレピュテーションの理解をより広く把握することができます。

現在、このユーザーは ThreatSTOP のクラウドベースソリューションこそが、急速に進化する競争の激しいスペースで成功するために欠かせない最低限の要件であると考えています。通信事業において競争する一方、企業は内部ネットワークセキュリティに引き続き照準を合わせており、このユーザーは移り変わりの激しい市場において明らかに優位を保っています。ThreatSTOP を導入することにより、ユーザーは戦略の隅々にまで防御を増強し、大切な顧客を守り、運用コストの大幅な削減を達成しています。



Michael Becce, MRB Public Relations, Inc. mbecce@mrb-pr.com |(732)758-1100 x104