Progress Flowmon

サイバー攻撃への マルチベクトル防御ソリューション

データシート

ソリューションの必需品

Superna

- Ransomware Defender
- Smart Airgap API ライセンス

プログレス製品

- 異常検出システムがインストールされた Flowmon アプライアンス
- Smart Airgap API を統合するためのカスタムスクリプト

セキュリティに関する検討事項

1. セキュリティイベントの監視と対応に関して、セキュリティ運用のレベルは高く保てているか?
2. 保護する必要のある重要なアプリケーションサーバーはあるか?
3. 侵害の恐れがある業務上重要なファイルやデータはあるか?
4. 侵害が発生してしまった場合、修復までの時間はどれくらいまでが許容可能か?

サイバー攻撃が頻発する現在、非構造化ファイル、オブジェクトストレージ、その他あらゆるファイルやデータが攻撃者のターゲットになります。脅威はますます進化して高度化しており、企業や顧客の資産をサイバー攻撃から保護するために、高いレベルのセキュリティ戦略を備える必要があります。

ビジネスの課題

サイバー攻撃が激増している昨今、デジタル資産を保護するために複数の検出ベクトルを含む高度な戦略を立てることが課題となっています。検出ベクトルとは、悪意のあるアクティビティを識別して対応するためのアプリケーションスタックを指し、例としては、エンドポイント保護、電子メールゲートウェイ、ファイアウォール、ネットワーク検出と応答システム、ストレージデバイスなどがあります。

今日の脅威は、最初の侵害から攻撃開始までにかかる時間が短くなっています。そのような脅威、サイバー攻撃への試みに対しては、検出して対応し、修復するまでの時間を短縮する必要があり、複数の入力を迅速かつインテリジェントに集約し、解決を自動化できるソリューションが必要です。また、攻撃開始前に長期間アイドル状態にある脅威については、数週間または数か月にわたる様々な異常の全体像を作成し、それらを侵害として特定できるソリューションが必要です。いずれの場合も、本質的にマルチベクトルであるソリューションを実装することが求められます。

ネットワーク防御とストレージ防御の統合

推奨されるのは、ネットワーク検出とストレージレイヤの防御との統合です。ネットワーク防御とストレージ防御を統合することで、ランサムウェアの試みに対し、早期の警告、検出、修復が可能になり、脅威に対抗することができます。Superna の Ransomware Defender と Flowmon を組み合わせたソリューションは、重要なビジネスデータを保護するのに最適です。

ソリューションの利点

- ネットワーク監視での機械学習テクノロジーを用いた異常検知によって攻撃を早期の段階で検知
- 自動化で、マルチドメインの脅威アラームを読み取って処理するための人的介助で発生するタイムラグをなくし、数秒で応答が可能
- ネットワークとストレージドメイン全体の脅威に関する知識を組み合わせて、迅速な対応が可能
- Ransomware Defender の Enterprise Cyber Vault と統合して、侵害されたデータの複製をブロック
- ユーザー、ファイル/オブジェクト、ネットワークデバイスに対する脅威の根本原因を迅速に特定し、セキュリティ運用を支援
- ランサムウェア攻撃に遭ってしまった場合の修復コストを削減。バックアップのみのアプローチ (Cyber Vault を使用) で、何日も要さずに数分でデータを復旧できる保護ソリューション

マルチベクトル防御ソリューションの仕組み

このソリューションは、プログレスの Flowmon 異常検出システム (Anomaly Detection System、ADS) のインテリジェントなネットワーク検出と応答機能と Superna のストレージ層防御を組み合わせることで、重要なデータを安全に保護するものです。

Flowmon が提供するネットワークの可視性を活用して潜在的な攻撃を早期に検出、警告でき、それが Superna の Ransomware Defender のデータ保護ワークフローのトリガーになります。

多くの場合、攻撃者は最初に意図したターゲットをポートスキャンでマッピングするか、アプリケーションサーバーに対してブルートフォースでログインを試みます。このような初期段階の指標は、Flowmon で簡単に検出でき、統合されたマルチベクトル防御ソリューションとしてプロアクティブな保護手段を提供します。

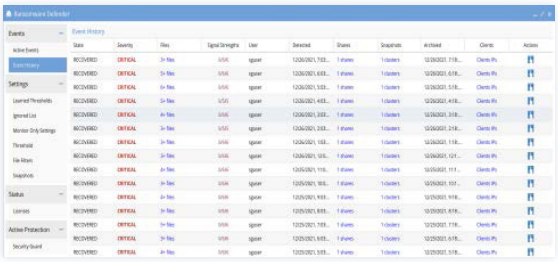
ランサムウェア攻撃の目的は、重要なデータにアクセスしてシステムやファイルを使えないようにし、復旧させるために身代金を要求してビジネスに損害を与えることです。したがって、エコシステムを保護するためのストレージ中心のアプローチが重要になります。Superna の Ransomware Defender は、I/O レベルでクライアントの動作を監視し、ゼロデイ検出エンジンを使用して悪意あるアクティビティをリアルタイムで検出します。疑わしいアクティビティが検出されると関連するファイルが追跡され、初期段階のアクティビティから攻撃チェーンの次段階へと進行するのを防ぐため、不審なエンティティはストレージ環境からロックアウトされます。また、回復ポイントとして、変更を加えられないスナップショットも作成されます。

ハッカーが
ネットワーク防御を調査

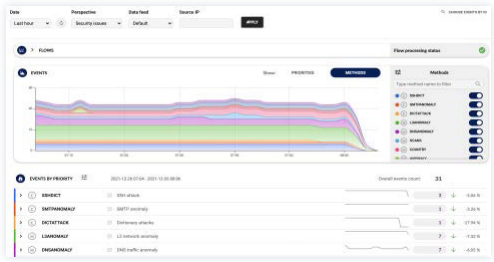
ネットワークセキュリティ防御で
疑わしいアクティビティを検出

Smart Airgap API リクエストで
ストレージ層に脅威の可能性を通知

Ransomware Defender は、
プロアクティブにデータの
スナップショットを作成し
セキュリティ層に追加データを
ログ記録



Superna の Ransomware Defender



Flowmon 異常検出システム (Flowmon ADS)

Superna について

Superna は、非構造化データの管理、保護、安全対策におけるグローバルリーダーです。Superna は5か国で事業を展開しており、様々な産業に携わっている、2,600 を超える顧客を抱えています。スケールアウト NAS に保存された顧客のファイルは数十億にも達し、拡張しやすくシンプルで使いやすい Superna 製品がファイルの保護と安全管理に寄与しています。

Flowmon に関する詳細は、ホームページをご覧ください:
www.flowmon.com/jp

プログレスについて

プログレス (Nasdaq：PRGS) は、テクノロジーが牽引する世界において専心的にビジネスを推進し、多くの企業がイノベーションのサイクルを加速し、躍進して業績を向上させていくプロセスを支援します。プログレスは信頼できるプロバイダーとして、インパクトが大きいアプリケーションを開発、展開、管理するための最高の製品を提供し、お客様は必要なアプリケーションとエクスペリエンスを開発し、適切な手法で展開し、すべてを安全かつ確実に管理することが可能になります。1,700のソフトウェア会社と350万の開発者を含め何十万もの企業が目標達成のために確信を持ってプログレス製品を利用しています。詳細については www.progress.com をご覧ください。また、LinkedIn、YouTube、Twitter、Facebook、Instagram へのフォローをお願いいたします。

プログレス・ソフトウェア・ジャパン株式会社
〒106-0047
東京都港区南麻布4-11-22 南麻布T&F ビル
www.flowmon.com/jp
sales_japan@progress.com

Progress