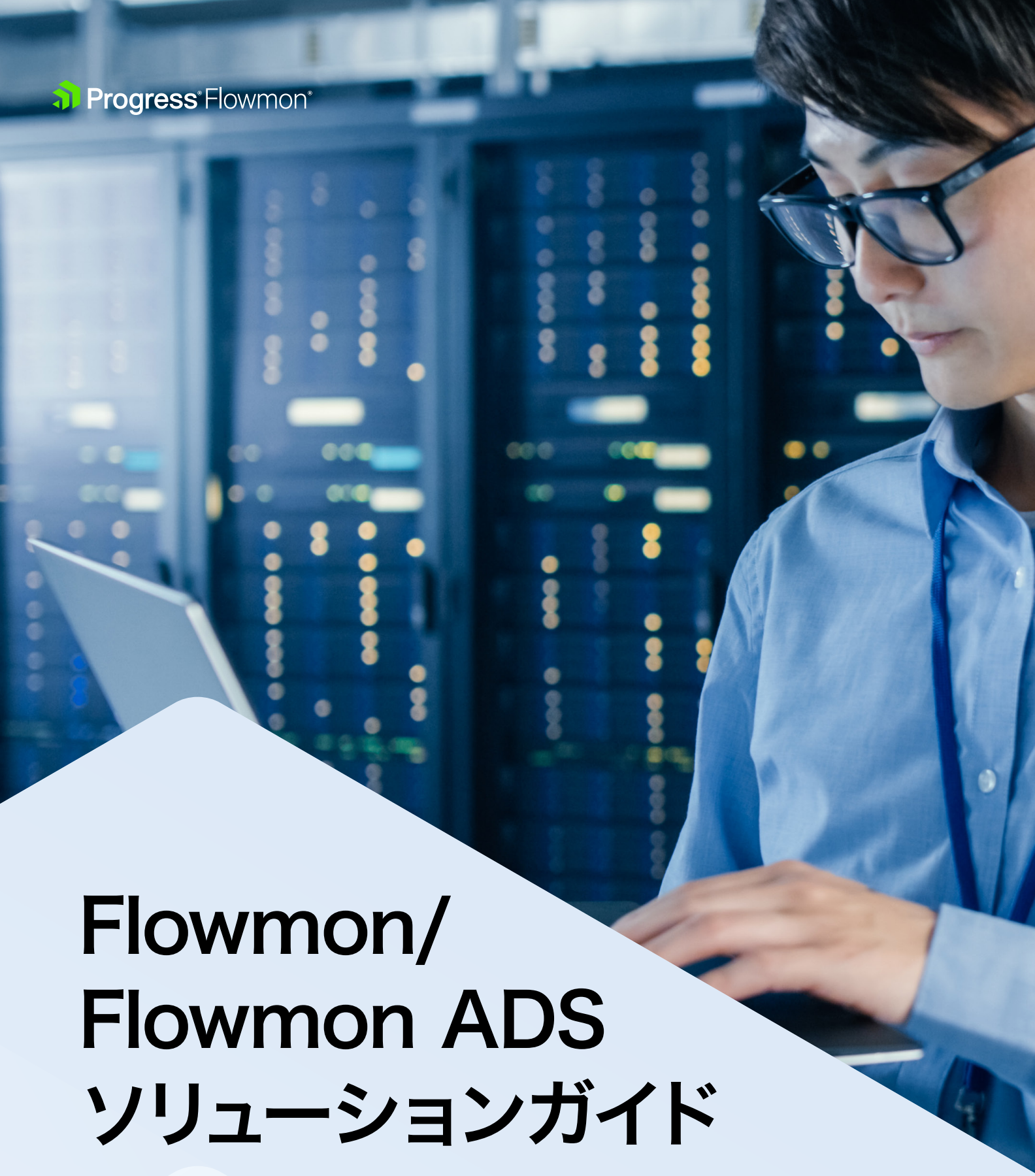


Progress® Flowmon®

Flowmon/ Flowmon ADS ソリューションガイド

ホワイトペーパー

Flowmon –
共通の目標への、1つのソリューション

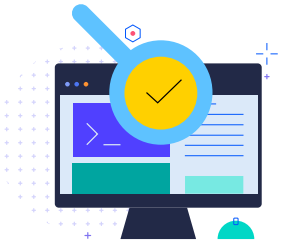
Progress® Flowmon® は、ネットワーク運用部門 (NetOps 担当部門) と、セキュリティ担当部門(SetOps 担当部門) が共有する目標、安定した頑健なデジタル環境、の達成に貢献します。ネットワークはより複雑になり、ハイブリッド環境がより一般的になってきている環境で、脅威はますます巧緻になって検出しにくくなっていますが、そのような状況にあって、新しい脅威に屈することなく、俊敏かつ安全に業務を処理していくための鍵となるのが Flowmon です。

NetOps のための監視と診断

- エンドユーザーエクスペリエンスの監視
- トラブルシューティングとフォレンジック
- 予測とプランニング
- クラウド/SaaS パフォーマンス

NetOps と SecOps との間の垣根を外す

- インフラストラクチャの設計と展開
- インシデントの監視と調査
- インシデント対応
- ポリシーの検証と実施



SecOps のためのネットワークトラフィック分析

- ネットワーク振る舞い分析
- 未知の脅威の検出
- 暗号化トラフィック分析
- 内部脅威の検出

収集

Flowmon は、既存のネットワークデバイスやセンサーなど、様々なソースからネットワークアプリケーションのテレメトリデータを収集します。

統合

多くの既存ツールやプラットフォームとシームレスに統合可能です。異種環境を完全にサポートし、ルーター、スイッチ、ファイアウォール、クラウドからテレメトリデータを抽出して収集します。

収集されるテレメトリデータ:

- Flowmon Probe で詳細なネットワークとアプリケーションのデータ (L2-L7)
- サードパーティーの NetFlow/IPFIX ソース、またはその他の L3-L4 データ

分析

収集されたデータは、機械学習、ヒューリスティック、高度なアルゴリズムを使用して処理されます。

インシデントへの迅速な対応

Flowmon はネットワークトラフィックを監視し、侵害の可能性があればプロアクティブに警告します。インシデントはリアルタイムで検出され、豊富なコンテキストと共に表示されるので、迅速に対応して適切な修復を行うことが可能です。

検出の強化:

IBM、Juniper、Hillstone、Fortinet、Cisco、VMware、Azure、AWS、Google、Keysight、Gigamon

リアルタイム
ゼロディで高度な持続的脅威に対応します。

理解

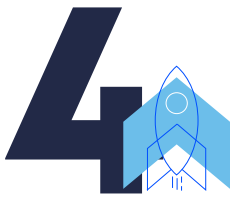
関連情報が抽出され、ダッシュボード上にわかりやすく表示されます。

NetOps と SecOps の融合

Flowmon は、NetOps と SecOps との融合を促進し、重複する機能に関しては、ツールの購入、サポート、トレーニングにかかるコストが最小限に抑えられます。

アラートのログ記録:

IBM、ArcSight、Splunk、McAfee、Fortinet、および Syslog を使用する CEF 形式のその他のプラットフォーム。



実行

ユーザーは簡単に全体の状況を捉えることができます。最も重要で関連性の高い情報は、明確でノイズがありません。

速やかな価値実現

合理化された展開、ユーザーへの支援、事前定義されたダッシュボードとレポート。操作は直感的にわかりやすく、価値を生み出すまでに長い時間はかかりません。

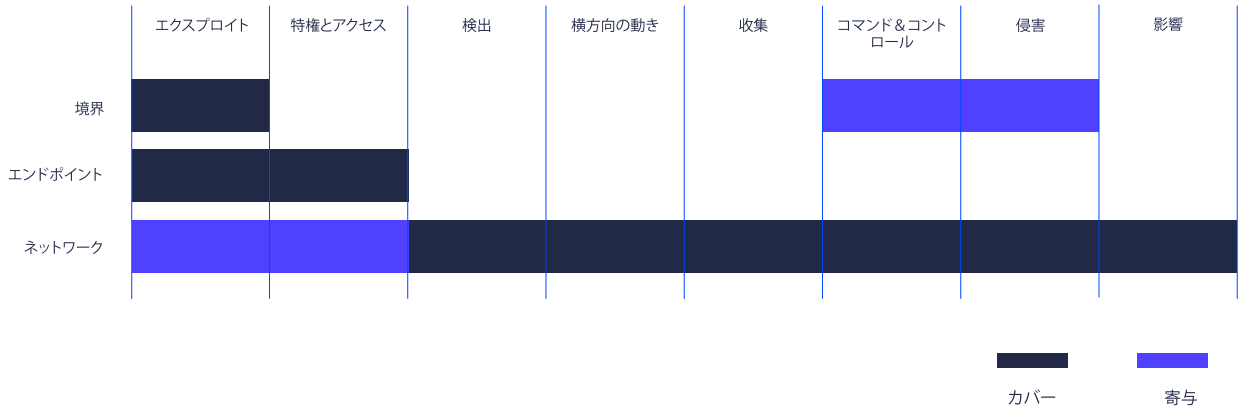
16倍
解決までの時間が最大で16倍速くなったとの報告があります。

自動応答:

Cisco、Fortinet、Hillstone、Allied Telesis

Flowmon の人工知能

ネットワークには内部脅威やデータ侵害のリスクが常に存在します。エンドポイントと境界保護の間の空白領域に発生する脅威は、ファイアウォールやウイルス対策では検出できません。そのため、セキュリティを階層化し、すべての死角をカバーすることが重要になります。Flowmon は、従来の対策を補完するものとして、脅威を検出した上で、自動対応やフォレンジック分析も可能とするアプローチを組み合わせています。



セキュリティと汎用性

これらすべてのメカニズムが同期して機能するので、このソリューションは強力です。ネットワークトラフィックを複数の観点からチェックし、様々な状況で使用できる用途が広いソリューションとして使えます。

検出のテクニック

- 機械学習
- 調整可能なベースライン設定
- ヒューリスティックス
- 振る舞いパターン分析
- レピュテーションデータベース
- シグネチャベースの検出

Flowmon の追加ソリューション – Flowmon ADS

Progress® Flowmon® ADS は、Flowmon のプラグインオプションとして使用できます。

攻撃の各段階で、Flowmon ADS が効果的に機能

検出 - ネットワーク上のデバイスやサーバーがランサムウェア攻撃された場合、最初に行われるのは、検出スキャンを実行して、拡散のためにネットワーク上の他のシステムを探すことです。これらは通常、同じネットワーク上で利用可能なデバイスを探す ARP スキャンを使用し、続いて垂直 TCP SYN スキャンを使用して、侵害できる可能性のあるサービスを探します。これらのスキャンの動きは、ADS が監視するネットワークフローデータの中に現れ、異常な振る舞いとしてフラグが立ちます。

認証情報攻撃 - ランサムウェア攻撃で他のシステムが検出されると、ブルートフォースログイン試行によってそのシステムにアクセスしようとします。たいていは、莫大な数の典型的なアカウントとパスワードの組み合わせを試して、首尾よくアクセスが許可される組み合わせを見つけるパスワードスプレー攻撃が使用されます。このブルートフォースログイン試行の発生があれば、ADS は、そのアクティビティを異常として強調表示します。

脆弱性の悪用 - よくある他の攻撃ベクトルは、パッチが適用されていないシステムの既知の脆弱性を悪用することです。IT システムには、攻撃者に悪用される脆弱性はつきもので、新しく脆弱性が発見されるとパッチが適用され、公表されます。ADS は、脆弱性が悪用され、攻撃者がネットワーク上で活動した後に頻繁に発生する異常なネットワークアクティビティを検出できます。

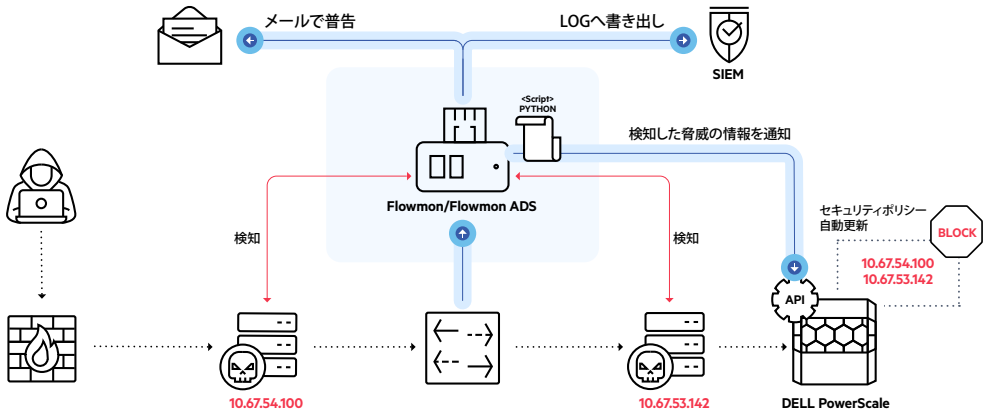
データ抽出 - 現在のほとんどのランサムウェア攻撃は、身代金を要求するための準備としてデータ抽出を行います。攻撃者は自分が制御するサーバーにネットワークからデータをコピーしていることを隠そうとします。そのためには、データをより小さなチャンクに分割し、DNS クエリを使用して抽出したり、ping することでネットワークからデータを抽出したりする手法が取られます。Flowmon ADS はこれらのイベントを検出することができます。さらに、フォレンジック分析のためにネットワークトラフィック全体をキャプチャすることも可能です。ランサムウェア攻撃が行われたとき、データが流出したかどうか、またどのようなデータが流出したかを知るのは困難な場合が多いので、これは非常に役立ちます。ネットワークから出たパケットを分析すると、そのトラフィックにデータが隠されているかどうかがわかります。

暗号化 - ランサムウェア攻撃の最終段階はデータの暗号化です。暗号化が始まる前にネットワーク上の攻撃者を検出できなかった場合は、暗号化のアクティビティを検出して、被害を軽減するための措置を講じることが重要です。
Flowmon を利用されているあるお客様は、最近、共有ネットワーク上の暗号化を発見し、感染したホストを迅速に特定して隔離することができました。被害は1つのデータストアと数個のファイルだけにとどまりました。

Flowmon ADS と Dell PowerScale インテグレーション

Flowmon は、ネットワークのトラフィックを可視化し、監視・分析することができます。Flowmon のオプション製品である Flowmon ADS は、振る舞い、マルウェア、ポートスキャン、ブルートフォースアタックなどのネットワーク上の異常や不審な挙動を検知し、アラート警告を出したり、自動応答などの対処をすることができます。

ネットワークのみならず、ネットワーク上には重要なデータ、バックアップデータを蓄積しているストレージなどが存在します。それらへの脅威を検知後、いち早く通信をブロックする必要があります。Flowmon ADS と Dell PowerScale ストレージのインテグレーションによって、脅威を速やかに通知して、ストレージ内に侵入される前にアクセスを遮断する処理を自動的にとることができます。



Flowmon ADS と Dell PowerScale との連携の流れ

① Flowmon/Flowmon ADS でネットワークトラフィックを監視

② Flowmon ADS がネットワーク上で振る舞い、マルウェア、ランサムウェアなどの脅威を検知

③ 警告をメール等で通知

④ 検知した IP アドレス、ポートなどの情報を Script から PowerScale API 経由で通知

⑤ PowerScale Firewall 上のセキュリティポリシーに対しルールを追加

⑥ PowerScale Firewall による該当の IP アドレスをブロック

使用条件

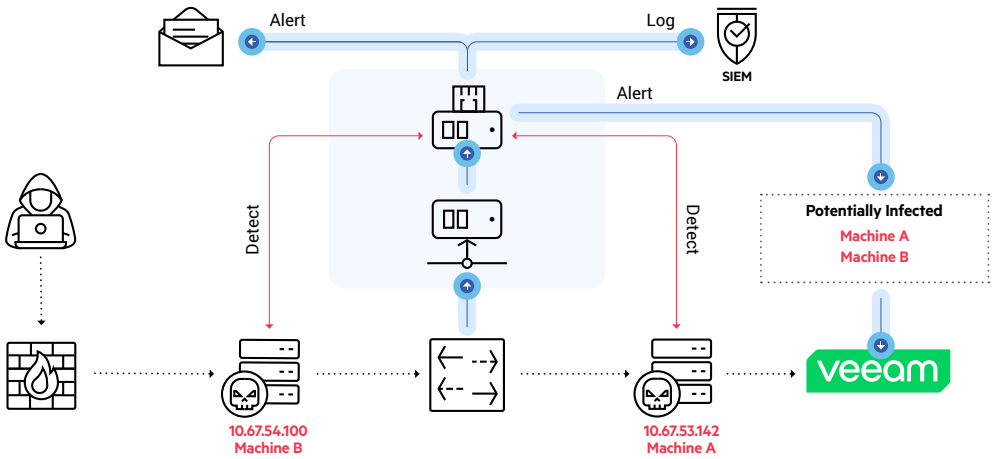
1. Dell OneFS 9.5.0.0 以上

2. Flowmon, Flowmon ADS のライセンスをお持ちのお客様は、このインテグレーションを追加費用無しに使用することができます。

Flowmon ADS と Veeam® とのインテグレーション

Flowmon は、ネットワークのトラフィックを可視化し、監視・分析することができます。Flowmon のオプション製品である Flowmon ADS は、振る舞い、マルウェア、ポートスキャン、ブルートフォースアタックなどのネットワーク上の異常や不審な挙動を検知し、アラート警告を出したり、自動応答などの対処をすることができます。

ネットワークのみならず、ネットワーク上には重要なデータ、バックアップデータを蓄積しているストレージなどが存在します。侵入者は、稼働中のデータだけではなく、バックアップデータも標的にします。Flowmon ADS は、それらの脅威をいち早く検出して、不審な振る舞い、マルウェアなどの詳細情報を Veeam サーバーに通知します。



Flowmon ADS と Veeam Management Server との連携の流れ

① Flowmon/Flowmon ADS でネットワークトラフィックを監視

② Flowmon ADS がネットワーク上で振る舞い、マルウェア、ランサムウェアなどの脅威を検知

③ 警告をメール等で通知

④ PowerScale Firewall 上のセキュリティポリシーに対しルールを追加

⑤ Veeam Management Server で不審な侵入情報を確認し、対処

備考： Flowmon, Flowmon ADS のライセンスをお持ちのお客様は、このインテグレーションを追加費用無しに使用することができます。

詳細については、お問い合わせください。
www.flowmon.com/jp/company/contact

プログレスについて

プログレス (Nasdaq: PRGS) は、ミッションクリティカルなアプリケーションとエクスペリエンスを開発および展開するのに役立つソフトウェアや、データプラットフォーム、クラウド、IT インフラストラクチャを効果的に管理できるようにするソフトウェアを提供しています。プログレスはテクノロジー分野での業務効率の向上に貢献できる経験豊富で信頼できるプロバイダーです。数十万の企業の、400万人を超える開発者と技術者の方々に、プログレス製品を何らかの形でご利用いただいています。詳細については、www.progress.com をご覧ください。

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®