SOLUTION BRIEF

FortiEDR が実現する POS システムにおけるリアルタイムの確実なエンドポイントセキュリティ

概要

脅威環境が進化を続ける中で、組織を攻撃から保護することはますます困難になっています。高度なエクスプロイトやツールが出回り、それを悪用する犯罪者が増え続けています。インターネットに接続された脆弱な POS（販売時点情報管理）システムやデバイスは、攻撃の格好の標的になっています。これらの POS システムを保護するには、インシデントの検知とレスポンスに人工知能（AI）や機械学習（ML）を採用し、エンドポイントにおけるリアルタイムのレスポンスと検知を可能にするセキュリティアプローチが必要です。FortiEDR を導入することで、セキュリティ担当者は POS 端末を感染前と感染後に保護できるようになり、データやシステムの整合性に影響が及ぶ前に高度なマルウェアやデータ侵害をブロックできます。

新しい高度な脅威に狙われる POS システム

脅威の数が増えると同時に高速化と高度化も進んでいることから、CISO は常に悪意のあるエクスプロイトの脅威にさらされています。特定のエンドポイントに存在する脆弱性をネットワークへの侵入口として悪用しようとするサイバー犯罪者により、エンドポイントは最大の標的になっています。特に POS システムや POS 端末は、旧式あるいは専用の組込み型オペレーティングシステムで動作する傾向があるため、多くの CISO にとって悩みの種となっています。また、必ずしもパッチが公開されないという事実が問題をさらに悪化させています。さらには、アンチウイルスやエンドポイントの検知 / レスポンスの最新ソリューションの大半は旧式のオペレーティングシステムをサポートしていないため、多くの POS システムは未だシグネチャベースで時代遅れのアンチウイルスソリューションによって保護されている状況です。

65 カ国 67 社の企業で確認された 2,200 を超えるデータ侵害のうち、約 14.5% に POS（販売時点情報管理）システムの端末やコントローラに対するリモート攻撃が関係していたほか、約 5% ではクレジットカードのスキミング装置が POS 端末へと物理的に埋め込まれていました。これには、ガソリン給油用の端末から ATM までのあらゆる POS 端末が含まれます [1]。

POS システム保護の要件

これらの POS 端末を保護するために、CISO は自らのチームが以下の対策を確実に実行できるようにしておく必要があります。

- **さまざまな攻撃からシステムを保護：**総当り方式のハッキング、バックドアマルウェア、盗まれた認証情報の使用、フィッシング、またはメモリスクレイピングなどの攻撃から、デバイスをオフラインにすることなく保護し、ビジネスを続行可能にする。
- **攻撃や高度なマルウェアを検知：**侵害されたシステムの検知が遅れると、攻撃者が水平移動して顧客のカード情報をスクレイピングし、外部に持ち出す時間を与えることになり、企業ブランドの評判が悪化する。
- **可視化とセキュリティ対策の制御：**保護されていない、脆弱性が存在する、あるいは望ましくないと思われるアプリケーションが実行中のシステムを発見する。
- **パフォーマンスに対する負荷を増加させない：**処理能力もリソースも限られ、なおかつ旧式のオペレーティングシステムにも対応する POS システムのパフォーマンスを維持する。

セキュリティ担当者は、上記に加えて高度なマルウェアの防止と検知、リアルタイムの脅威除去と封じ込め、侵害の自動停止、リスクの解消と確実な事業継続などを実現し、レガシーあるいは POS 専用の幅広いオペレーティングシステムをサポートする、軽量のエンドポイントセキュリティソリューションが必要です。同時に、予防は重要ではあるものの 100% 完璧な保護を保証するものではない点を留意することも大切です。しかしながら、セキュリティ侵害を避けることは難しいとはいえ、データの喪失を防ぐことは可能です。

高度でありながら軽量のエンドポイント保護

FortiEDR（Endpoint Detection and Response：エンドポイントの検知とレスポンス）は、特許取得済のコード追跡機能を使用して侵入前と侵入後の両方でマルウェアを検知してブロックする、AI と ML を活用した高度なエンドポイント保護ソリューションです。フォーティネット セキュリティ ファブリックに統合された FortiEDR は、POS システムを含むすべてのエンドポイントを透過的に可視化すると同時に、直感的なユーザーインタフェースを提供することで迅速かつ容易なエンドポイントのポリシー管理、そして感染時の減災を可能にします。このようなセキュリティを実現するため、このソリューションは次世代アンチウイルス（NGAV）、アプリケーションの通信制御、仮想パッチ、EDR の自動化によるリアルタイムのブロックや脅威の検知、インシデント対応の機能を、単一のエージェントにすべて統合しています。

FortiEDR は、POS システムの保護対策として利用可能なプロアクティブでリアルタイムのセキュリティを提供します。FortiEDR の中核機能には次のものがあります。

軽量のエンドポイントセキュリティソリューションが、レガシーまたは POS 専用のオペレーティングシステムを幅広くサポートし、リスクを伴うことなく高度なマルウェアの防止と検知、リアルタイムの脅威の除去と封じ込め、侵害の自動停止、確実な事業継続を可能にします。

機械学習に基づく NGAV でマルウェアを防止する：FortiEDR は、不正な侵入をカーネルレベルで可視化することで、従来型のアンチウイルス等の対策を回避する高度な脅威を完全に把握することができます。シグネチャを使用しないため、シグネチャデータベースのダウンロードや更新のオーバーヘッドを削減すると同時に、最新およびレガシー両方のオペレーティングシステムの軽量かつ効率的な保護を可能にします。

脅威をリアルタイムで検知し、解消する：FortiEDR は、侵入の特定を自動化して感染後（侵入後）に脅威を外科的に封じ込めるほか、リアルタイムで脅威を検知して除去することでデータの持ち出しやランサムウェアによる暗号化を阻止します。その結果、お客様はランサムウェアなどのマルウェアによる侵害やそれに伴う被害を回避できます。

アプリケーションと脆弱性を可視化してリスクを軽減する：FortiEDR は、攻撃対象領域に対する高度で自動化されたポリシー制御機能のほか、POS システムをはじめとするインターネット接続デバイスすべての脆弱性の評価とセキュリティの機能を備えています。これにより、セキュリティおよびオペレーションの両チームはアプリケーションやエンドポイントを検知して追跡し、CVE やアプリケーション評価のデータと相関付けることで、脆弱性が存在するアプリケーションが POS 端末で実行中かどうかを判断し、それらの情報に基づいてプロアクティブなリスクベースのポリシーを実行することもできます。FortiEDR を導入することで、セキュリティおよびオペレーションの両チームは脆弱性が存在するアプリケーションやシステムを容易に特定すると同時に、仮想パッチを活用して減災し、次のパッチメンテナンスまで脆弱なシステムをプロアクティブに保護します。

パフォーマンスへの影響を最小限に抑える：FortiEDR は攻撃をリアルタイムで封じ込めるため、組織にリスクを与えることなく、POS 端末の利用を継続することができます。また、FortiEDR は最小限の CPU パワーで動作し、過剰なネットワークトラフィックを生成することもありません。つまり FortiEDR は、わずか 1% 未満の CPU および 120 MB 未満の RAM 利用率を実現するほか、ネットワークトラフィックの生成がホストあたり毎分 1 kb 未満の単体型軽量エージェントを提供します。

フォレンジック分析を活用する：さらに FortiEDR は、セキュリティおよびオペレーションの両チームによる詳細なフォレンジック調査を可能にするほか、POS システムに対して急速に進化する脅威の完全な可視化や、セキュリティにおける問題への自動対応を実現する優れた柔軟性も提供します。その結果、セキュリティオペレーションセンター（SOC）チームは最適な時間の活用が可能になります。

FortiEDR のカスタマイズされたプレイブックを利用し、インシデント対応と減災のオーケストレーションおよび自動化を実現することで、セキュリティおよびオペレーションの両チームによる脅威への対応時間が短縮されます。リスクベースのアプローチを採用する FortiEDR は、資産の価値、エンドポイントのグループ、脅威の分類に基づいて、レスポンスをカスタマイズできます。さらに、選択したデバイスあるいは POS システムを含むエンドポイント環境全体で、封じ込めたマルウェアによって実行された変更を手動または自動で容易にロールバックできます。

迅速かつ容易な実装：FortiEDR エージェントは、サポート対象の各オペレーションシステム向け標準インストーラパッケージとして提供され、Microsoft SCCM（System Center Configuration Manager）などの標準のリモート無人導入ツールを使用して、容易にインストールできます。ローカルでの構成や再起動は必要ありません。

終わりに

FortiEDR は、セキュリティおよびオペレーションの両チームを支援し、POS システムに対する動きの速い攻撃の防止、検知、封じ込め、減災を実現します。FortiEDR を導入することで、POS 端末を網羅する高度なマルウェアの検知と減災に関連する複雑さ、そしてコストの戦略的な削減が可能になります。さらに、インシデント対応の時間的プレッシャーを最小限に抑えつつ、データ侵害やサイバー攻撃による混乱を引き起こすことの多い脆弱性のエクスプロイトを防止することで、膨大なアラートへの対応や脅威の長期間の潜伏、あるいは侵害に対する不安を解消します。

[1]「Data Breach Increase Shows Endpoints Are Under Attack」、Joe Stanganelli 氏、Security Now、2018 年 4 月 16 日（英語）：
https://www.securitynow.com/author.asp?section_id=706&doc_id=742214

FORTINET
フォーティネットジャパン株式会社

〒106-0032
東京都港区六本木 7-7-7
Tri-Seven Roppongi 9 階
www.fortinet.com/jp/contact

お問い合わせ

SB-FortiEDR-POS-202003-R1