Windows Defender ATP が高度な脅威の検出を支援

サイバー攻撃の高度化に対応するため、Microsoft IT は、新しいクラウド ベースのサービス Windows Defender Advanced Threat Protection (ATP) を実装しました。能力の高い敵対者が攻撃元となる少数の攻撃に焦点が置かれた Windows Defender ATP は、機械学習、ビッグ データ、およびセキュリティ分析を活用し、コストがかかるオンプレミス ソリューションを構築することなく、マイクロソフトが自社のネットワークを狙った高度な標的型攻撃を検出し、調査して、それらに対応するのを支援します。

サイバー攻撃が高度化し、その特性が進化していく中で、Microsoft IT は、オペレーティング システムのセキュリティ機能やウィルス対策製品で提供される保護機能の他に保護レイヤーを追加する必要があることを悟りました。私たちは、現在、侵害は必ず起こるものと想定しておかなければならない世界に生きているため、侵害を素早く検出し、侵害に素早く対応して、侵害の影響を軽減させることができる必要があります。マイクロソフトは、機械学習、ビッグ データ、およびセキュリティ分析の能力を活用し、マイクロソフトとエンタープライズのお客様がマイクロソフトのネットワークを狙った高度な標的型攻撃を検出し、調査して、それらに対応するのを支援するクラウド ベースのサービス Windows Defender Advanced Threat Protection (ATP) を開発しました。

マイクロソフトは、Windows 10 Anniversary Update のリリースに組み込まれた Windows Defender ATP を使用可能にすることで、ますます高度化する攻撃に対抗できるよう、エンドポイントの可視性を向上させ、脅威検出機能を強化できるようにしました。これによって、コストのかかるオンプレミス ソリューションを構築することなく、これらの攻撃に対応するマイクロソフトの能力が向上しています。マイクロソフトは、Windows Defender ATP やそのクラウド ベースのセキュリティ サービスを採用することで数多くのメリットを短期間のうちに実現しました。このメリットには以下のようなものがあります。

- **容易な展開と管理:** Windows Defender ATP では Windows 10 の組み込みエージェントが使用されるため、従業員のデバイスやエンドポイントのオンボーディングを容易に行うことができます。オンプレミス インフラストラクチャは不要です。
- **接続性の向上:** Windows Defender ATP は、常時接続デバイス向けの常時接続サービスです。
- **スケーラブル:** マイクロソフトは、50 万台を超えるデバイスのデータのオンボーディングを行ってきました。Windows Defender ATP サービスは、マイクロソフトのニーズの増大に応じて拡張します。
- **正確なアラートの提供:** Windows Defender ATP は、マイクロソフトのセキュリティ専門家が支えるインテリジェントで実用的なアラートを提供します。
- **より迅速にトリアージを行う機能の提供:** Windows Defender ATP は、迅速なホストのトリアージを可能にし、調査用の詳細なイベント タイムラインを提供します。
- **効率性の向上:** Windows Defender ATP は、集中的な対応とエンタープライズの脅威の抑制を可能にします。
-

ビジネスの課題

従来の脅威検出監視システムは、ほぼ全員が企業ネットワークに接続し、主に物理データセンターのサービスにアクセスしているシナリオをサポートするよう構築されていました。従業員のモバイル化が進み、大半のサービスがクラウドへ移行する中で、マイクロソフトは、自社のエンドポイントの監視や保護におけるさまざまな課題に対応するのを支援するクラウドの機能に目を向ける必要がありました。

大規模な監視

マイクロソフトは、25 万人を超えるアクティブ ユーザーを有しており、50 万台を超えるコンピューターを監視しています。マイクロソフトは、Windows のリリースごとに、追加機能を監視する必要があります。マイクロソフトが受信するデバイスあたりのデータ量が増加しており、マイクロソフトは、それらのデータを集約し、結果を改善し、それらのデータを分析して侵害を示す行動がないか調べる、より効果的な方法を必要としています。侵害を検出するのに必要となる情報の収集と管理を行うエンタープライズ クラスのオンプレミス ソリューションを維持管理するのは複雑で困難でした。

能力の高い敵対者

Windows Defender などのマルウェア対策 (AM) ソフトウェアは、特定されている大半の脆弱性や攻撃に対処する脅威耐性やマルウェア保護機能のレイヤーを提供していますが、敵対者の能力は日々高くなっており、敵対者は価値の高い知的財産やビジネスに大きな影響を及ぼす情報を狙うようになってきています。

能力の高い敵対者は、オペレーティング システムやアプリケーションの機能に存在する脆弱性を突いてデバイスを侵害する機会を狙っています。また、強い決意を持った攻撃者は、マルウェアを一切使用せず、代わりにソーシャル エンジニアリングの手法 (ユーザーを騙してアクセス権限や特権を得るスピア フィッシングなど) を用いて、マルウェア防御機能を回避する方法を見つけています。

Windows Defender ATP の役割

Windows Defender ATP は、能力の高い敵対者が攻撃元となる高度なサイバー攻撃に焦点が置かれています。侵害が検出されると、Windows Defender ATP によってこれまでにないレベルの洞察が提供されます。マイクロソフトは、侵害の可視性、侵害の範囲に関する詳細情報、および高度な攻撃の種類やその挙動を明らかにするのに役立つ関連情報を手にしています。この新たな洞察は、マイクロソフトが高度化する新しい脅威に対応するのに最適な方法を素早く判断するのに役立っています。

図 1: 侵害後の検出機能、調査機能、および対応機能を提供し、Windows Defender のマルウェア保護機能に基づいて構築されている Windows Defender ATP

さまざまな機能を「強化」し、デバイスの ID や情報の保護機能、および一定レベルの脅威耐性を提供するいくつかのテクノロジが Windows に組み込まれています。Windows Defender (または他の従来のウィルス対策ソフトウェア) は、外部からの脅威の大半を認識し、追加の脅威耐性を提供する役割を果たします。Windows Defender ATP

は、これらのテクノロジに置き換わるものではなく、これらのテクノロジと連携するよう設計されました。Windows Defender はさまざまな脅威を阻止できるよう支援し、Windows Defender ATP は環境を監視して、侵害を示す異常な行動を探します。これによって、マイクロソフトのネットワーク事業への高度な脅威や、既知の攻撃者の行動に対する可視性が向上しています。Windows Defender ATP により、マイクロソフトは、アラートを通じて生成される分析や機械学習を用いて、コンテキスト内で潜在的なセキュリティ侵害を特定することが可能になっています。

Windows Defender ATP サービスのアーキテクチャ

Windows Defender ATP サービスは、以下の 3 つの要素で構成されています。

- **クライアント エンドポイント動作センサー:** Windows 10 Anniversary Update に組み込まれており、サービス登録時にアクティブ化されるクライアントは、エンドポイント (クライアント コンピューター) の関連セキュリティ イベントや動作をログに記録します。
- **クラウド セキュリティ分析サービス:** エンド ポイントのデータとビッグ データを連携させることで、行動のシグナルを洞察、検出、および脅威への対応に結び付けることができます。マイクロソフトは、セキュリティ領域における多くの情報を蓄積してきました。Windows Defender ATP は、Windows エコシステム (マイクロソフトの悪意のあるソフトウェアの削除ツールなど)、エンタープライズ クラウド製品 (Office 365 など)、およびオンライン アセット (Bing や SmartScreen の URL 評価機能など) にわたってマイクロソフトが持つ独自の視点を活用し、異常な行動、敵対者の手法、および既知の攻撃とのそれらの類似点をより効果的に検出するのを支援できます。
- **マイクロソフトの脅威インテリジェンス:** マイクロソフトのセキュリティ専門家および調査担当者は、データを調査し、新しい行動パターン、潜在的な持続的標的型攻撃 (APT) アクティビティのアラート、またはマイクロソフトのグローバル センサー ネットワークから収集される脅威インテリジェントと相関するデータ侵害がないかを調べます。

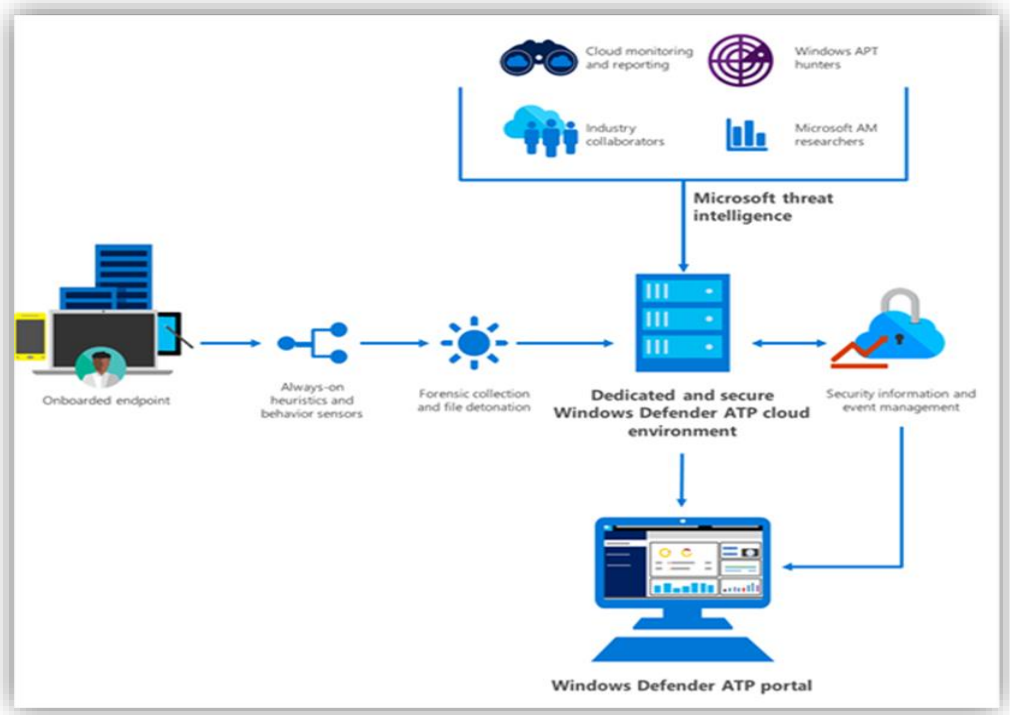

図 2: Windows Defender ATP サービスのコンポーネント

クライアント デバイスのオンボーディング

Windows Defender ATP は Windows 10 Anniversary Update に含まれているため、マイクロソフトのクライアント マシンにエージェントをインストールする必要はなく、サービスを有効にするだけで済みました。Windows デバイスのオンボーディングは、展開方法として、System Center Configuration Manager とグループ ポリシー オブジェクトを使用して行われました。これら 2 つの方法で、50 万台を超える固有の Windows デバイスでサービスが有効にされました。

クライアント デバイスは、サービスと通信するためにインターネットに接続している必要があります。Windows Defender ATP の原動力となる動作センサーは、CPU の使用量がごくわずかであり、バックグラウンドで実行されます。また、Windows Defender ATP のクラウド サービスと通信し、データのレポート作成を行うために使用される容量も、1 日あたり最大で 5 MB です。

マイクロソフトの脅威インテリジェンス

Windows Defender ATP によって、マイクロソフトは、マイクロソフトと世界中の独立したセキュリティ専門家の知識ベースを組み合わせて活用することが可能になっています。それらの情報は、アラートが出されている脅威の種類を特定し、潜在的な影響を評価するのに役立っています。マイクロソフトは、脅威インテリジェンス コミュニティ内の情報を活用し、マイクロソフト独自の経験でその情報を補強しています。

専用の安全な Windows Defender ATP のクラウド環境

Windows Defender ATP は、コード ファイル データ (ファイル名、サイズ、ハッシュなど)、プロセス データ (実行中のプロセスとハッシュ)、レジストリ データ、ネットワーク接続データ (ホストの IP とポート)、マシンの詳細情報 (GUID、名前、オペレーティング システムのバージョンなど) を含む情報を収集します。

Windows Defender ATP サービスによって収集されたお客様のデータは、マイクロソフトのデータセンターに保管されます。これらのデータは、マイクロソフトのプライバシー プラクティス、セキュリティ プラクティス、および Microsoft Trust Center のポリシーに従って管理されます。詳細については、「信頼されたクラウド」と「Move your datacenter to a cloud you can trust」を参照してください。

Windows Defender ATP ポータル

マイクロソフトは、Windows Defender ATP ポータルを使用して、潜在的な持続的標的型攻撃 (APT) アクティビティやデータ侵害のアラートを監視し、それらに対する対応を支援しています。Windows Defender ATP サービスは、Windows Defender ATP エージェントによって収集、分析、および集約されたデータを使用します。マイクロソフトは、Windows Defender ATP ポータルを使用して、Windows Defender と Windows Defender ATP から出されたアラートの確認、分類、およびトリアージを行っています。

ポータルの主要要素には以下のようなものがあります。

- **メイン ポータル:** さまざまなビュー ([Dashboard]、[Alerts Queue]、および [Machines View]) の確認に使用されます。
- **ナビゲーション ペイン:** [Dashboard]、[Alerts Queue]、[Machines View]、[Preferences Setup] 間の移動に使用されます。
- **検索バー:** さまざまなエンドポイントにわたるマシン、ファイル、外部 IP アドレス、またはドメインの検索に使用されます。ドロップダウンのコンボ ボックスでエンティティの種類を選択できます。
- **設定:** 構成設定 (アラートのしきい値を調整するのに使用されるアラートの抑制ルールなど) へのアクセスに使用されます。

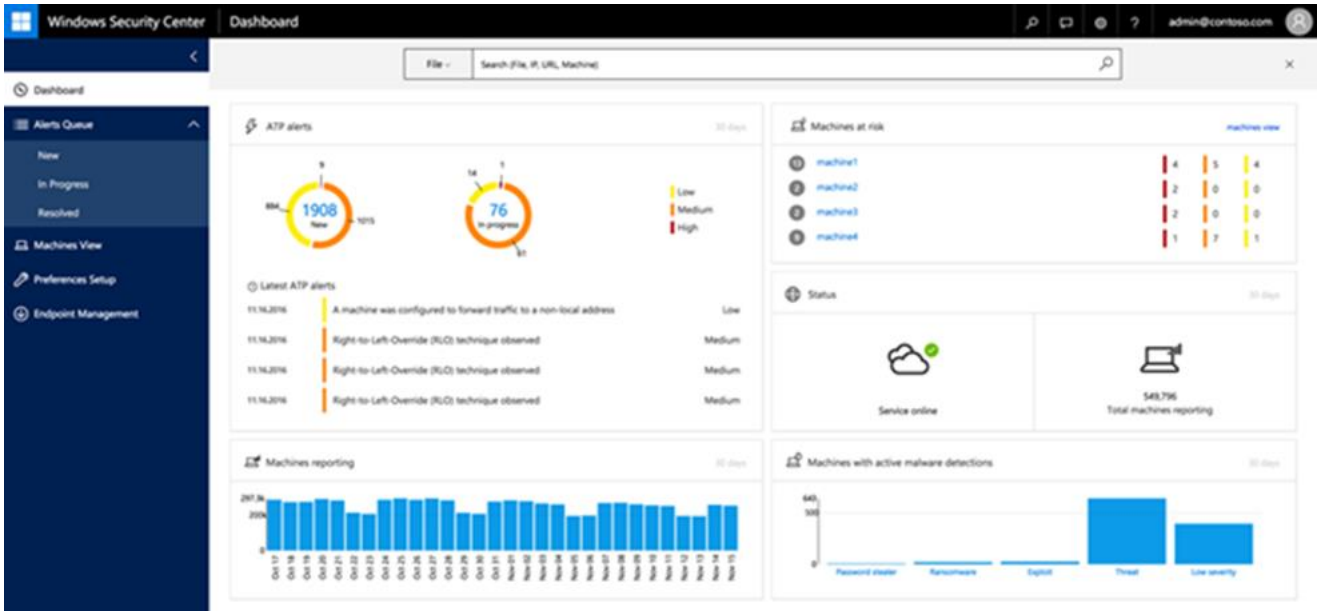

図 3: Windows Defender ATP ポータル

注: Windows Defender はマイクロソフトのエンドポイントのリアルタイムのマルウェア対策保護機能として使用されているため、マルウェア関連の検出情報が表示されています。

ポータルの使用方法は、3 つの重要要素 (正確性、速度、効率性) によって補強されています。このポータルによって以下が実現されています。

- [Alerts Queue] の正確なアラート
- 詳細なイベント タイムラインや包括的な検索機能による調査速度の向上
- 企業全体を素早く動き回り、侵害を調査して、他のシステムに影響がないか確認する機能の提供によるマイクロソフトの企業対応の効率性向上

ポータルを通じて、マイクロソフトは、ファイルや IP アドレスなどの監視対象インジケータに関する豊富な情報を把握しています。それらの情報は、マイクロソフトが侵害の範囲についての理解を深めるのに役立っています。例えば、悪意のあるファイルが電子メールで送信され、組織内のユーザーがそれを開き、侵害が発生した場合、調査を行い、それが単独のインシデントであるのか、電子メールでそのファイルを受信した受信者が他にも存在するのかを確認できます。複数の受信者がそのファイルを受信していた場合、早期検出機能、および同様のサイバー攻撃のデータとの相関に基づいてサイバー攻撃の特性について理解する機能によって、より簡単に状況を食い止めて、侵害の影響を軽減させることができます。

メリット

マイクロソフト クラウドの能力とマイクロソフトのセキュリティ専門家の共有知識を活用することで、Windows Defender ATP は、従来よりも素早く正確に悪意のあるアクティビティに関するアラートを Microsoft IT に出すことができます。また、Windows Defender ATP は Windows 10 Anniversary Update に含まれているため、Center Configuration Manager やグループ ポリシー オブジェクトを使用して、システムへの従業員のオンボーディングを簡単に素早く行うことができます。

Windows Defender ATP を使用することで、複雑なオンプレミス ソリューションを構築したり、それを管理するための専用リソースを用意したりすることなく、企業ネットワーク環境やデバイス エンドポイントへの脅威をより素早く検出できます。また、俊敏性が向上することで、時間とリソースが節約され、侵害がもたらす可能性のある被害の規模が抑えられます。攻撃にはさまざまな種類がありますが、その中には情報を狙った攻撃や、ネットワークおよびネットワーク上のリソースのパフォーマンス低下を目的とした攻撃もあります。より素早く攻撃に対応できる能力とより多くの情報が提供されることで、マイクロソフトが提供しているすべてのサービスのパフォーマンスと品質を確保できます。

Windows Defender ATP は、センサー ネットワークと機械学習を組み合わせて使用してパターンを検出します。また、分析は継続的に改善されていきます。