Technology Blueprint

McAfee
An Intel Company

PCに求められる基本的なセキュリティ機能

今日のリスクに対応するエンドポイント保護の導入

SECURITY CONNECTED REFERENCE ARCHITECTURE

LEVEL 1 2 **3** 4 5

Security Connected

マカフィーのSecurity Connectedフレームワークは、複数の製品、サービス、パートナーの統合を可能にすることで、効率的かつ効果的に一元的なリスク軽減を実現します。20年以上の実績を持つセキュリティプラクティスを基盤に構築されたSecurity Connectedアプローチを通じて、規模やセグメントを問わず、すべての地域の組織がセキュリティ体制を改善し、セキュリティを最適化することでコスト効率を高め、戦略的にセキュリティとビジネスイニシアチブを整合させることが可能になります。Security Connectedリファレンスアーキテクチャーは、構想から実装までの具体的な手法を提供します。このアーキテクチャーを利用することにより、Security Connectedの概念をお客様独自のリスク、インフラストラクチャー、ビジネス目標に適合させることができます。マカフィーは、常にお客様を保護する新しい方法を見出すことに専心しています。

今日のリスクに対応するエンドポイント保護の導入

現状

多くの管理者は、エンドポイント保護にこれ以上の投資は必要ないと考えています。エンドポイントへの投資に懐疑的な管理者からは、「マシンが感染したら、構築しなおせばよい」、「単なるエンドポイントがどのような影響を及ぼすというのだ?」という声が聞かれます。

こうした管理者たちは、ウイルス対策製品によってすでに保護体制が十分であると考えています。では、なぜウイルス感染が発生しているのでしょうか? なぜ導入済みのウイルス対策製品は、Zeus や FakeAV といったマルウェアを阻止できなかったのでしょうか? 実際、最近のハッカーとマルウェアは、複数の感染経路と複雑な手法を駆使して PC に侵入しています。 かつては単一のウイルス対策ソリューションで十分でしたが、今日はすべての感染経路を保護する必要性が生じています。

課題

エンドポイントの保護を導入する組織は、様々な疑問を抱えています。「複数のレイヤーによる保護が必要なのか?」、「保護製品はエンドポイントのコンピューティングリソースをどれだけ消費するか?」、「どれだけの作業が必要になるのか?」。新たに検出される脅威の数は、毎日数万にのぼっています。シグネチャーは1日のうちに何回も更新する必要があり、もはや一般的なマルウェア対策にも十分とは言えなくなっています。適切な投資を怠れば、エンドポイントが感染するだけではなく、組織のインフラストラクチャー全体のセキュリティが低下する可能性があります。最初はその影響に気付かないかもしれません。しかし、問題を検知して阻止する前に、機密情報が盗まれたり、ネットワーク内の他のデバイスが感染したりしてしまう可能性があります。大きな問題は、最初に気付くエンドポイント感染ではなく、すぐには気付かない広い範囲への影響なのです。

- **最初のコンタクト**: 脅威は、USBによる物理的なアクセス、悪質なユーザー、電子メール、またはユーザーによる悪質なWebサイトの訪問によって、組織のシステムへのアクセスを取得します。
- **ローカルでの実行**: 攻撃者は、最初のコンタクトの後、重要情報や、システムへの認証アクセスの取得を目的とする何らかの攻撃やソーシャルエンジニアリングを行い、組織のネットワーク内にプレゼンスを確立します。
- **プレゼンスの確立**: 次に攻撃者は、システムを制御するために、マルウェアをダウンロードし、より高度な特権を取得し(ゲスト権限から管理者権限など)、バックドアを仕掛け、ステルス技法を利用し、行動を隠匿し、検出された際の無効化を非常に困難にすることで自身を保護します。
- **悪質なアクティビティ**: システムの制御権を獲得した攻撃者は、マシン内の機密ファイルの盗用から、ユーザーIDとアクセス特権(財務アプリケーション、顧客データベース、重要システムへのアクセスなど)の奪取、ネットワーク内の脆弱性の偵察、スパム中継点としてのボットネットへのシステムの統合まで、あらゆる実行が可能になります。

その例を説明します。

- **最初のコンタクト**: ユーザーがWebサイトを訪問すると、アカウントの期限切れが近いため、資格情報とその他の検証情報の入力が必要であることを通知する警告が表示されます。
- **ローカルでの実行**: ユーザーはすべてを正常の動作と思い込み、必要な情報を入力して「OK」ボタンを押します。その後、ユーザーは通常のWebページにリダイレクトされてネットサーフィンを続けますが、不正なアクティビティが行われたことに一切気付きません。
- **プレゼンスの確立**: しかし、ユーザーが「OK」ボタンを押したときに、悪質なWebサイトによってユーザーのブラウザーにマルウェアがダウンロードされました。このマルウェアは、ステルスモードでメモリー内、またはルートキットとして自己インストールを行い、管理者によって停止/削除されないようにタスクマネージャーとレジストリエディターを無効にします。その後、ユーザーが入力した情報を使用して、システムでより高度なアクセス権を取得します。

- **悪質なアクティビティ**: 次にマルウェアは「コマンド&コントロール」センターにアクセスし、ネットワーク内のエンドポイントや他のデバイスに対する搾取、詐欺、窃盗の指示を待ちます。マルウェアは、クレジットカード番号とログイン情報を探すことも、マルウェアを感染させるためにメーリングリストを探すこともあります。エンドポイントからアクセス可能なネットワーク共有に自身をコピーする場合もあります。それと同時に、脅威のレプリケーション機能により、このエンドポイントやネットワーク内の他のマシンにバックドアとトロイの木馬がインストールされます。ネットワーク共有は、大半が十分に保護されていないため、マルウェアの容易な配布手段になっています。犯罪者は、アクティビティを監視して、知的財産、個人の財務情報、企業秘密、個人のファイル、顧客の機密情報などの情報をこっそり盗み出すことができます。

攻撃では、複数の段階と複数の戦術が使用されるようになったため、現在エンドポイントは以前よりも脆弱になっています。

ソリューション選定の要素

アーキテクチャーには、次のような要素が影響します。

- どのアンチウイルスソリューションを現在使用しているか
- 最近ウイルス感染が起きたか
- エンドユーザーに管理者権限を与えているか
- 現在、ハードウェアのリサイクルをどのように管理しているか
- カテゴリーのみに基づくWebゲートウェイを使用しているか
- 外付けデバイスとリムーバブルメディアをどのように制御しているか
- 企業ネットワークに接続しているデバイスの健全性を検証しているか

解決策

このように複数の段階で構成される攻撃の登場により、デスクトップは、インストール済みの単純なウイルス対策プログラムだけでは保護しきれなくなっています。ウイルス対策は不可欠な要素に違いありませんが、エンドポイントを適切に保護するために必要な一連のソリューションのコンポーネントの1つに過ぎません。求められているのは、I/Oにとどまらない保護です。たとえば、従来のウイルス対策製品がディスクアクセスの監視のみを行う場合、ネットワークやメモリーの脅威を見逃してしまいます。最初のコンタクト、攻撃、悪質なアクティビティからの保護を実現するには、システムの各コンポーネントに対応する多層防御が必要です。さらに、脅威は進化しているため、各防御層を最新の状態に維持することが非常に重要です。

- **I/O**: ディスクの読み取り/書き込みはすべて保護が必要です。この役割を果たすのが、従来の典型的なウイルス対策です。ユーザーがファイルにアクセスするたびに、ウイルス対策が既知の脅威を検出するためのスキャンを行います。これが周知の基本的な保護手法です。
- **ネットワーク**: 有線または無線接続を介してマシンに出入りするデータは、不正な侵入か、許容される宛先とのコンタクトであるかの分析が必要です。こうした脅威に対する保護は、デスクトップファイアウォールが提供します。ファイアウォールを通過するすべてのパケットは、企業が定義したルールに照らして分析する必要があります。たとえば、安全なVPNまたはローカルの企業ネットワークを介した接続の場合にのみ特定のアプリケーションを許可し、マシンの他のインターフェイス(無線、3G USBキー)へのアクセスを制限するというルールを定義できます。この制御によって、ユーザーによる境界のセキュリティ/保護ポリシーの回避を制限できます。また、近隣の企業に無線ネットワークが導入され、自社には導入していない場合に、ポリシーを通じて、社員による近隣の無線ネットワークの使用をブロックできます。
- **メモリーとプロセス**: 今日の脅威の大半は、バッファオーバーフローによって引き起こされます。バッファオーバーフローはメモリーで発生します。脅威は、ユーザーに気付かれずにひっそり忍び込み、メモリーを破壊し、バイナリーコードを実行します。従来のウイルス対策ソリューションは、メモリーではなくI/Oに

焦点を当てているため、これらの脅威を検出できません。ウイルス対策ソリューションもファイアウォールも、SQLインジェクションを検出できません。ファイアウォール、ウイルス対策とも、特権のエスカレーションを阻止できません。これを阻止できるのがホストIPSです。ホストIPSソリューションは、メモリー内を検査し、パターンを分析し、バッファオーバーフローなどの脅威を検知します。

- **シグネチャー**: ウイルス対策、ホストIPS、その他の防御策は、何らかのタイプのシグネチャーを使用して動作するのが一般的です。シグネチャーは既知の脅威を阻止しますが、時間に依存します。つまりシグネチャーの効果は、最終更新時間によって決まります。今日重要なのは、シグネチャーに加えてリアルタイム保護機能を使用することです。進化の激しい攻撃や脅威に対しては、クラウドベースのインテリジェントサービスが保護に欠かせない要素になっています。ルートキットのような執拗で卑劣な攻撃が増加しているため、保護においては、OSの起動前に脅威を探し始めることも重要です。

エンドポイント保護に関して重要なもう1つの要素が、エンドユーザーです。大半のユーザーは「深刻なクリック病」を患っています。これは、 a)何が書いているか読まないため、 b)何があっても次のレベルに進みたいため、または c)単なる習慣となっているために、エンドユーザーが何でも目にするものをクリックしてしまう症状です。最初のコンタクトの大半は、クリック病が原因で確立されています。

- **コンテンツ制御**: 特定のサイトへのユーザーの訪問を防止するフィルタリングは提供されていますが、コンテンツの制御は必要ないのでしょうか？ カテゴリーとしては「適切」とされているサイトでも、このサイトに公然と、あるいはひそかに配置されているファイル、スクリプト、ダウンロードが悪質なものである場合があります。それはどのように把握すればよいのでしょうか？ そのためには、コンテンツ保護を通じてカテゴリーを補完する必要があります。コンテンツ保護とは、サイトがアダルトサイトやギャンブルサイトかどうかを区別するだけでなく、ダウンロードが危険か、ブラウザーヘルプオブジェクトがユーザーの同意なしにインストールされるか、アフィリエイトに問題がないか、などを把握するソリューションです。

ユーザーがノートPCを紛失したり、盗まれた場合にはどうなるでしょうか？ マシンを修理に出した場合はどうでしょうか？ マシンを組織外部に持ち出したとしても、セキュリティが低下しないようにデータを保護することが非常に重要になります。

- **エンドポイント暗号化**: 暗号化されたデバイスは、紛失や盗難に遭っても影響が少なくなります。データが暗号化されている場合にデバイスを紛失しても、デバイスは単なる金属の塊となり、データの安全性は維持されます。デバイスを修理に出したり、リプレースする場合でも同じです。マシンを廃棄する場合、多くの企業は破砕機を使って情報を破棄しますが、この手法は時間と費用がかかり、環境にも優しくありません。しかし、デバイスが暗号化されていれば、情報は安全です。したがって、データの漏えいを懸念することなく、慈善団体への寄付など、思い付くあらゆる手段で処分できます。

- **デバイス制御**: シンプルなUSBが悪夢のきっかけになることがあります。個人所有のUSBは、友人や家族のマシンとのデータやファイルの共有に使用されますが、すでに悪質なコードでセキュリティが低下しているマシーンを経由していることがあります。このUSBが企業のマシンに接続されると、自動実行機能によってこのデバイス内のすべての機能が実行されます。企業のセキュリティは、エンドポイントからUSBデバイスまでのアクセスを制限できるかどうかにかかっています。また、USBへのデータの転送も防止できなければなりません。ユーザーにiPodの接続を許可する場合でも、充電や音楽再生のための「読み取りのみ」に制限する必要があります。このようなきめ細かい制御が実現すれば、デバイスの柔軟な利用を許可しながら、機密データを保護することができます。

- **エンドポイントの健全性**: ネットワークへの接続前に管理対象デバイスの健全性を確認することは、外部からの攻撃を防止する非常に重要な要素です。ネットワークに接続するデバイスは健全ですか？ 企業環境で必要とされているものと同じ最新のパッチが適用されていますか？ マシンは最新の状態に更新されていますか？ ネットワークに接続する前に、必要なすべての保護製品（アクティブなウイルス対策ソフトやファイアウォールなど）が装備されていますか？ 効果的なソリューションは、これらの問いに対する回答を把握し、ポリシーへのコンプライアンス状況に基づいてシステムを許可、ブロック、または検疫します。検疫されたシステムは、必要なアップデートを行うために修復サイトにダイレクトする必要があります。

- **可視性**: これらの機能をすべて導入した際に、セキュリティの状態を示す総合的なビューを利用できますか？ 大量のデータやスプレッドシートを操作しなくても、数回のクリックだけで組織のリスク状況を表示できる必要があります。また、監査に対応するレポートを通じて、法規制・コンプライアンスの実証を支援する機能も必要です。経営陣は、見たいときにセキュリティの最新状態を確認できなければなりません。

マカフィーのソリューションで使用されているテクノロジー

このレベルのセキュリティを達成するために、マカフィーは徹底防御を実現するテクノロジーを組み合わせて使用することを推奨します。最初のコンタクトを防止できることが理想的ですが、それができない場合には、その次のセキュリティレイヤーの強化が必要です。このエンドポイントソリューションでは、マカフィーは、エンドポイント、アクセス制御、マルウェア、ネットワーク(有線と無線)、メモリー、I /O、プロセスなど、すべての感染経路を保護します。マカフィーのモジュールは、統合スイートとして実装することも、リスクと予算に応じて追加することもできます。

マカフィーが提案する製品は、McAfee® ePolicy Orchestrator®(McAfee ePO™)によって一元管理されます。McAfee Global Threat Intelligence™は、さまざまな製品に組み込まれたレピュテーションエンジンを通じて、リアルタイム保護を提供します。

まずは、組織に適切な製品から利用を開始してください。ウイルス対策を含むMcAfee VirusScan® Enterpriseを基盤としてインストールしたら、リスクの高いWebサイトや不適切なWebサイトへの偶発的なアクセスを防止するMcAfee SiteAdvisor® Enterpriseを追加します。ネットワークでの感染経路は、McAfee Host Intrusion Preventionとこの製品に含まれるデスクトップファイアウォールで保護します。データは、各デバイスの暗号化によって保護します(McAfee Endpoint Encryption for PCs)。

望ましくないデバイスや危険なデバイス(USB、3Gネットワークキー、モバイルデバイスなど)のネットワーク内での使用を防ぐために、中核システムの保護をMcAfee Device Controlの機能で補完します。ネットワーク接続前の管理対象デバイスの健全性は、McAfee Network Access Controlを使用して確認できます。

この組み合わせを使用することで、エンドポイントのI/O、ネットワーク、メモリー、プロセスの保護、Webの安全な利用、エンドポイントのデータの暗号化が可能になります。これらのレイヤーの導入により、最初のコンタクトや、それに続く手順を阻止し、攻撃が成功する可能性を低減できます。ユーザーは、オフィス、外出先、自宅からのネットワークに接続することができ、どこに居ても同様に保護されます。ポリシーは、エンドポイントが企業ネットワークに接続されていない状況でも施行されます。ネットワーク接続環境に応じた、柔軟なポリシーの設定が行えます。

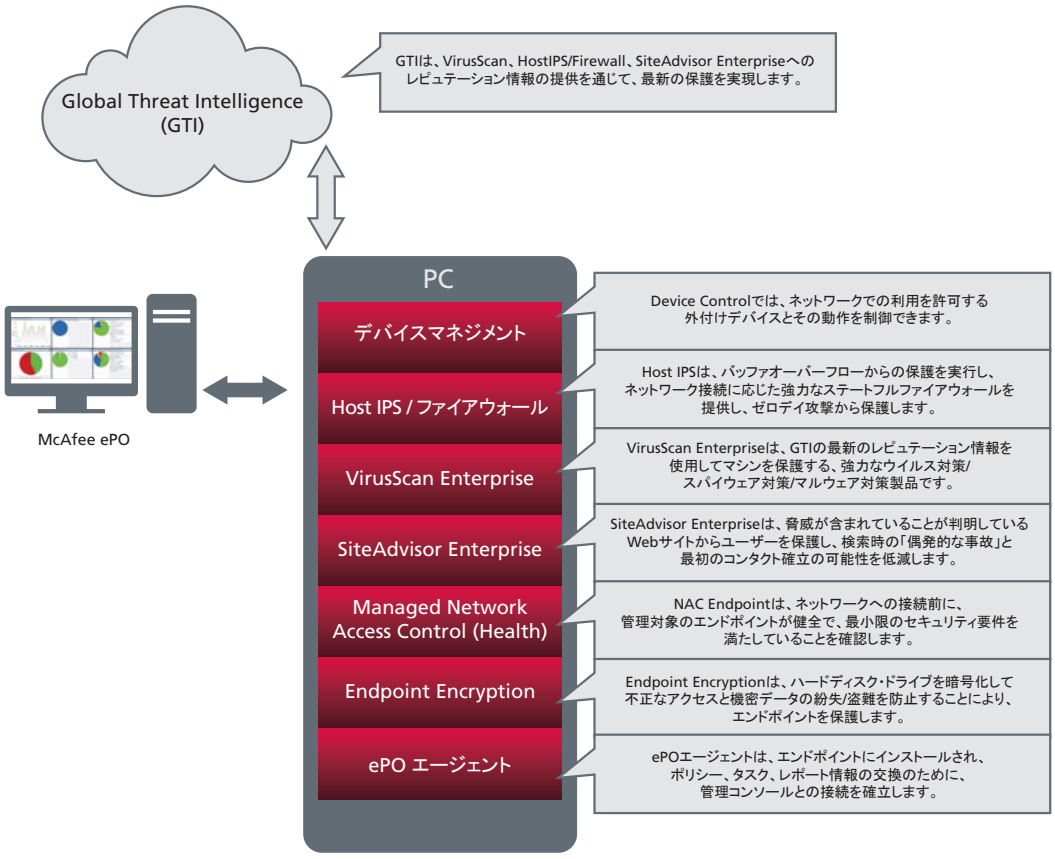
シグネチャーが利用可能になる前にリアルタイムで保護できるように、McAfee Global Threat Intelligence(GTI)がマカフィー製品と直接統合されています。McAfee GTIはクラウドサービスなので、インターネット接続されている任意の場所で機能します。McAfee VirusScan Enterpriseは、GTIのリアルタイムファイルレピュテーションを使用してシグネチャーを強化し、更新情報とのギャップを埋めます。McAfee Host IPSは、GTIを使用してアウトバウンドとインバウンドのIPレピュテーションを評価し、悪質なシステムやサイトとの通信を防止します。大半のボットは、組織のほとんどがアウトバウンドスキャニングを導入していないことにつけ込んで、外部への接続を使用してコマンド&コントロールセンターに接続するため、この制御はボットネットに対して非常に効果的です。McAfee SiteAdvisor Enterpriseは、GTIを活用してWebサイト内のURLのレピュテーションを評価、分類することで、ユーザーとの最初のコンタクトの確立をその場で防止します。

マシンがMcAfee ePOに接続すると、管理者はそのデバイスの完全な可視性を得ることができます。McAfee ePOの管理コンソールを通じて、CPU、ディスク領域、メモリー、OSのタイプとバージョン、タイムゾーン、リスクレベル、検知された脅威、対策などのハードウェアインベントリーの詳細を把握できます。入手できるのはPCの可視性だけではありません。McAfee ePOは、Mac、Linux、Solarisや、Apple iPad、iPod、iPhones、Android、RIM Blackberryを含むモバイルデバイスなど、マカフィーエージェントがインストールされているデバイスの可視性も提供します(マカフィーエージェントは、オプションのマカフィー製品を使用して、これらのプラットフォームで利用が可能で、可視性はデバイスによって異なります)。

McAfee VirusScan Enterprise

McAfee VirusScan Enterpriseは、一般の組織に導入されているありふれたウイルス対策製品ではありません。未知の攻撃に対抗する高度でプロアクティブなテクノロジーが搭載されています。VirusScan Enterpriseは、ウイルス、スパイウェア、ワーム、トロイの木馬、その他のセキュリティリスクから、システムとファイルの安全を守ります。マルウェアを検出して駆除するほか、隔離したアイテムを管理するポリシーを簡単に設定できます。

リアルタイムスキャンにより、リモート拠点を含むすべてのシステムが現在の脅威だけでなく新たな脅威からも保護されます。McAfee Global Threat Intelligenceのファイルレピュテーションサービスは、シグネチャーを待たずに、クラウド検索に基づいて悪質なファイルを検出してブロックします。この最新のリスク評価機能により、ゼロデイ攻撃をその場で阻止することができます。VirusScan Enterpriseは、Microsoftアプリケーションの脆弱性を狙うバッファオーバーフロー攻撃に対する防御も提供します。また、アクセス保護ルールを通じて、シグネチャーを使用せずに、レジストリエディターやタスクマネージャーの無効化などの望ましくない行動を阻止することや、マスメールワームによるメール送信を防止することも可能です。さらに高度な制御を行う場合は、カテゴリーを使用して、スパイウェア、アドウェア、リモート管理ツール、ダイヤラー、パスワードクラッカー、ジョーク、キーロガーなどの不必要なプログラムを停止できます。



McAfee SiteAdvisor Enterprise

Webサイトを単純に分類するだけでは、システムとユーザーは、セキュリティが低下したWebサイトや、承認サイト内の危険なWebページに晒されてしまいます。McAfee SiteAdvisor Enterpriseは、ユーザーがアクセスする前にWebサイトのリスクを評価できます。(企業が設定したポリシーと照らして)リスクが高すぎる場合には、ページをロードする前、またはページによってマルウェアがインストールされる前に、ページをブロックします。したがって、ユーザーが悪質なコードにアクセスすることはないため、IT部門がその後にクリーンアップする必要はありません。

「深刻なクリック病」を患っているユーザーは、危険な場所をサーフィンすることがなくなり、マルウェアに晒される機会が低減します。SiteAdvisorは、McAfee Global Threat Intelligenceを使用することにより、ユーザーが訪問しているWebサイトが安全かどうかを確認できます。「安全」とは、サイトにマルウェアが含まれていないこと、サイトが既知のスパム送信元ではないこと、ユーザーのブラウザーのセキュリティを低下させないこと、そしてサイトに過度なポップアップが含まれていないことを意味します。SiteAdvisorは、ユーザーにフィッシングサイトを警告するために、Outlook 2007/2010クライアント内の危険な可能性があるリンクを警告するメッセージを提供します。SiteAdvisorは、Internet Explorer、Firefox、Google Chromeをサポートしています。

McAfee Host Intrusion Prevention (ファイアウォールを含む)

大半のユーザーは、Microsoft Windows内にデスクトップファイアウォールが組み込まれていますが、不都合な介入を望まないユーザーはこの機能をオフにしているか、最小限の機能しか使用していません。果敢な攻撃者は、ほとんどのユーザーのファイアウォール機能を潜り抜けて侵入することができます。しかし、McAfee Host Intrusion Prevention(Host IPS)内のファイアウォールなら、ユーザーに不都合がないように、適切な機能を管理者が一元的に適用できます。マカフィーのデスクトップファイアウォールには、企業向けに構築されたルールが組み込まれています。たとえばこのルールでは、リモートユーザーが接続する際にVPN接続が必須であることや、社員が企業外部にいるときには一部のアプリケーションを使用禁止にする必要があることが前提になっています。

マカフィーのデスクトップファイアウォールは「接続の認識」と「接続の分離」機能を持ちます。ルールは、接続の場所に応じて施行されます。企業ネットワークに接続されているシステムに複数のネットワークインターフェイスがある場合、ファイアウォールはポリシーで許可されているもの以外のネットワークインターフェイスを利用しません。たとえば、マシンに有線と無線の2つのネットワークインターフェイスカード(NIC)があり、有線NICで企業ネットワークに接続するとします。接続分離機能により、このファイアウォールは有線NICのトラフィックのみ通過を許可し、無線NICへのすべてのトラフィックをブロックします。ファイアウォールは、企業の定義で許容されていない他のネットワークに無線で接続することを許可しません。ユーザーの自宅では、別のルールセットによって、インターネットへのアクセスを許可しながら、マシンの安全性が保持されます。

グローバルなレピュテーションを使用する動的なステートフルファイアウォールは、他に存在しません。McAfee Global Threat Intelligenceは、アウトバウンドとインバウンド両方のトラフィックを保護する通信レピュテーションを提供します。ボットネットが保護対象システムへの接続を試みると、GTIが受信トラフィックのレピュテーションが低いと判断し、ファイアウォールは発生する接続を許可しないため、マシンとネットワークを外部攻撃から保護できます。同様に、ネットワーク内部からボットがコマンド&コントロールセンターへのアクセスを試みると、GTIが送信トラフィックのレピュテーションが低いと判断し、制御ホストへのボットの接続をブロックします。

Host IPSは、この統合ソリューションに新しい側面を追加します。それがシグネチャーおよびビヘイビア分析機能です。Host IPSは、シグネチャーが存在する攻撃も、シグネチャーが存在しないゼロデイ攻撃も防止します。バッファオーバーフローに対する汎用保護では、シグネチャーを使用して多くの脆弱性から保護します。

Microsoft製品のパッチの適用に熱心な組織でも、Adobe、Mozilla、IBM、RealNetworksなど、すべてのエンドポイント製品とプラグインに最新のパッチを適用し続けることは困難です。Host IPSは、3つのレイヤー(シグネチャー分析、ビヘイビア分析、およびグローバルレピュテーション技術を使った動的でステートフルなファイアウォール)からなる保護により、侵入を阻止し、資産を保護し、ゼロデイ攻撃を含む既知の攻撃および新種の攻撃から組織を守ります。

McAfee Endpoint Encryption for PCs

McAfee Endpoint Encryption for PCs（EEPC）は、データ損失、データ盗難、そしてハードウェアをリサイクルまたは破棄する際のリスクに対する防御の第一線となります。

通常は、ユーザーが出社してマシンの電源を入れると、OSがロードされ、認証情報（ユーザーIDとパスワード）の入力を求められます。その後、ユーザーはOSに認識され、通常の作業に取り掛かります。

EEPCを使用する場合、OSは、ユーザーが認証されるまでロードされません。このモデルでは、パスワードをクラッキングする既知の攻撃がハッカーの役に立つことはありません。EEPCは、不正なユーザーによるデータへのアクセスを防止するために、起動前認証とオプションの二要素認証（スマートカードなど）を使用します。泥棒が盗んだドライブを他のマシンに接続する場合はどうでしょうか？ 何の問題もありません。データは暗号化されているため、第三者に読まれることはありません。ドライブは、盗難されたり紛失したりしても安全なだけでなく、修理に出しても、ハードウェアリサイクルなどの環境イニシアチブに参加しても安全性が保証されます。

McAfee Device Control

McAfee Device Controlでは、PCへの接続を許可/拒否するデバイスを制御できます。デバイスは読み取り専用に設定できます。特定のブランドのUSBキーのみを許可することや、シリアル番号を使用して特定のキーのみを許可することも可能です。また、モバイルデバイスをバッテリーの充電目的でのみ許可することもできます。McAfee Device Controlは、PC環境でのデバイスの接続方法や制御方法を柔軟に管理する手段を提供します。

McAfee Network Access Control

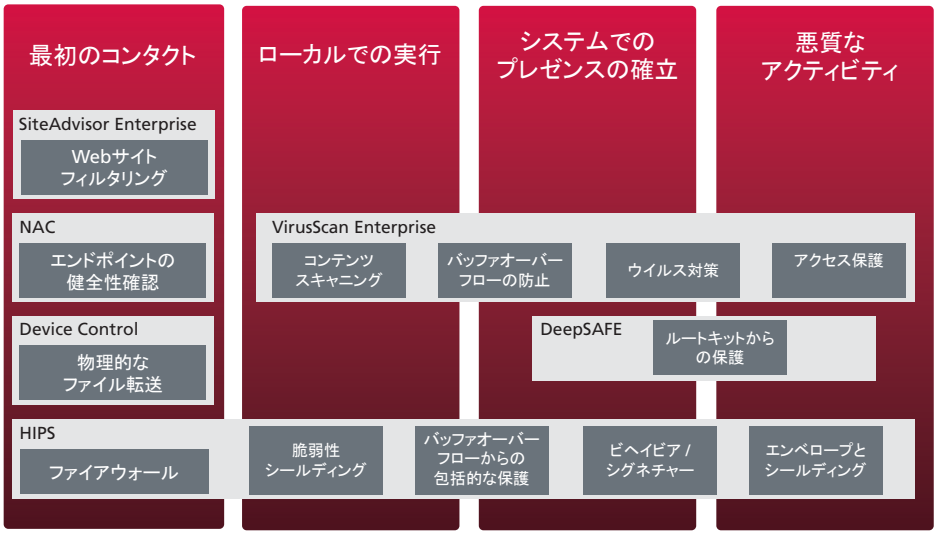
管理エンドポイント用のMcAfee Network Access Controlソフトウェアは、ビジネスやインフラストラクチャーに適応してアクセス制御の利点を提供します。McAfee Network Access Controlソフトウェアは、社員、請負業者、リモートユーザーなどの管理対象ユーザーをサポートしており、接続前に管理システムのコンプライアンスを確認するために、エンドポイントの状況を評価します。McAfee ePolicy OrchestratorとNetwork Access Controlソフトウェアを連動させると、不正なデバイスや未知のデバイスを検出して、セキュリティの問題を修正することができます。

McAfee ePolicy Orchestrator（McAfee ePO）

これらのエンドポイント保護モジュールはすべて、容易な実装と管理のために、一元的に管理および導入することができます。McAfee ePolicy Orchestratorでは、1つのコンソール、1つのエージェント、1つのロケーションから、環境の統合、確認、管理、体系化、レポート作成を行うことができます。McAfee ePOは、Microsoft Windows、Linux、Macを搭載するさまざまなPCの管理に対応し、こうしたシステムのステータスを単一のコンソールに表示します。これにより、管理が容易になり、可視性が高まるとともに、比類のない保護が実現します。

オプション

McAfee Site Advisor Enterprise Web Filtering for Endpointモジュールは、ネットサーフィンを許容サイトのみに制限するためのオプションの分類モジュールです。また、McAfee Web Gatewayを認識します。つまり、ユーザーがオフィスで接続している場合、McAfee SiteAdvisorはMcAfee Web Gatewayにフィルタリングを実施するように通知し、ユーザーがオフィスから外出するときは、SiteAdvisor自身がフィルタリングを制御します。



攻撃の4つの段階と、各段階に対応するマカフィー製品

導入効果

出社したときに現在のリスクを完全に把握できる状況を想像してみてください。まず、マカフィーのエンドポイント保護製品を通じて、リスクに晒されているか、その場合どこにリスクがあるのかをリアルタイムで確認することができます。また、この1週間あるいはここ1ヶ月で防止した脅威数や、保護に役立ったソリューションのコンポーネント、そして、SiteAdvisorを使用して悪質なサイトのブラウジングを防止したことによって、FakeAVのインストールを阻止できたことも把握できます。新しい脆弱性が発表された直近の「Patch Tuesday」(ベンダー各社のパッチ公開日)に、Host IPSによってその大半がプロアクティブに保護され、その残りがウイルス対策機能やMcAfee Global Threat Intelligenceを通じて保護されたことも把握することができます。

休暇を取っていた社員がウイルス感染を引き起こす問題も解消されます。McAfee Network Access Controlにより、この社員がマシンをネットワークに接続する前に、すべての適切なパッチと更新が適用され、マシンの健全性が保証されるためです。新しいメンテナンス担当者によって昨夜盗まれたマシンはどうなるでしょうか？ 企業データはEndpoint Encryption for PCsによって暗号化されており、盗まれたのはハードウェアのみなので安心です。この暗号化機能のおかげで、データのセキュリティを心配せずに、ハードディスク・ドライブを装着したまま古いPCをチャリティに寄付することも可能になります。

また、社内ポリシーで、機密データをユーザー所有デバイスにコピーできないように設定されているため、社員が自己所有のiPodに企業データを保管して持ち帰る心配もありません。Host IPSのファイアウォールは、セキュリティが低下したホストからボットネットのコマンド&コントロールセンターへの接続を阻止するので、新しいボットネットに加担する懸念もなくなります。翌朝に新種の脅威が登場しても、心配する必要はありません。急いでシグネチャーを導入しなくても、Global Threat Intelligenceが、ウイルス対策機能、ファイアウォール機能、またはSiteAdvisorを通じて対処してくれるはずです。

このように階層化されたマカフィーのエンドポイント保護製品があれば、1つのソリューションのもとで複数の機能を一元管理し、運用コストを削減することができます。また、I/O、ネットワーク、メモリー、Webコンテンツなどの異なるすべてのレイヤーに保護機能を導入することで、脅威に対するセキュリティが強化されます。さらに、紛失や盗難に遭ったり、ハードウェアをリプレースする場合にも、各マシン内のデータを保護することができます。そしてPCに侵入する前に脅威を阻止することにより、エンドポイントを再構築する必要性がなくなります。

Q&A

この文書で説明されたすべてのモジュールをインストールする必要がありますか。

すべてのモジュールのインストールは不要と思われるかもしれませんが、インストールするモジュールが多いほど保護レベルが高まり、すべてのモジュールを連動させることで最大限の保護が実現します。保護されていないそれぞれの感染媒体は、組織のリスクを高めます。お客様が最善の決定を下すことができるように、マカフィーではこれらのモジュールの多くをスイート製品として統合しました。このスイートは、各製品を個別に導入するモデルよりもはるかにコスト効率に優れています。

McAfee GTI は、 自社ネットワークの帯域幅に影響を与えますか。

GTIは、ルックアップの実行に単純なDNS要求を使用するので、帯域幅をほとんど消費しません。ファイルレピュテーション分析では、GTIを使用してすべてのファイルにアクセスするわけではありません。GTIは、ファイルが疑わしい場合や、シグネチャーファイルにエントリーがない場合にのみ使用されます。

McAfee Host IPS ファイアウォール上の GTI と McAfee SiteAdvisor Enterprise の違いは何ですか。両方とも同じものをチェックしているのですか。

そうではありません。Host IPSのファイアウォールは、インバウンドとアウトバウンドのIPレピュテーションのためにGTIが統合された完全なファイアウォールソリューションです。SiteAdvisor Enterpriseは、URLレベルでGTIと統合されたWebコンテンツフィルターです。Host IPSのファイアウォールは、接続先のIPアドレスのレピュテーションが高いか低いかをチェックします。メインのIPアドレスのレピュテーションが高くても、Webサイト内の他の領域は低い可能性もあります。Site Advisor Enterpriseは、ブラウズする際に、IPアドレス内の各URLを検証します。

追加情報

www.mcafee.com/japan/products/virusscan_enterprise.asp
www.mcafee.com/japan/products/siteadvisor.asp
www.mcafee.com/japan/products/host_intrusion_prevention.asp
www.mcafee.com/japan/products/endpoint_encryption.asp
www.mcafee.com/japan/products/device_control.asp
www.mcafee.com/japan/products/network_access_control.asp
www.mcafee.com/japan/products/epolicy_orchestrator.asp

＊本書は 2012 年 10 月時点での情報です。仕様等の変更が生じる場合や、一部、日本未発売の製品も含まれています。詳細はお問い合わせください。

著者について

Sylvain Dumasは、カナダのマカフィーのシニアセールスエンジニアです。彼は、コンピューター業界で25年以上の豊富な経験を培ってきました。1990年代は、Wang and Banyan Systemsで、当時最大級だったネットワークの構築に携わりました。1999年にマカフィーに入社後は、製品ライン管理を専門に活躍しており、お客様が単一の包括的なエコシステムに脆弱性管理、ネットワーク侵入防止、リスク管理を統合し、活用できるように熱心に支援しています。Sylvainは、セキュリティプロフェッショナル認定資格（CISSP）を取得しています。

McAfee An Intel Company
マカフィー株式会社
www.mcafee.com/jp

東京本社　〒150-0043 東京都渋谷区道玄坂1-12-1 渋谷マークシティウエスト20F　TEL：03-5428-1100(代) FAX：03-5428-1480
西日本支店　〒530-0003 大阪府大阪市北区堂島2-2-2 近鉄堂島ビル18F　TEL：06-6344-1511(代) FAX：06-6344-1517
名古屋営業所　〒460-0002 愛知県名古屋市中区丸の内3-20-17 中外東京海上ビルディング3F　TEL：052-954-9551(代) FAX：052-954-9552
福岡営業所　〒810-0801 福岡県福岡市博多区中洲5-3-8 アクア博多5F　TEL：092-287-9674(代) FAX：092-287-9675

MCABP-EPFP-1210-MC