McAfee Web Gateway Cloud Service

ユキビタスな保護を提供するクラウドベースのWebセキュリティ

巧妙な脅威からWebを保護するには高度な技術が必要になりますが、それによってコストが増えたり、管理が煩雑になるとは限りません。クラウドからWebセキュリティを提供することにより、セキュリティ チームは、メンテナンス用のハードウェアやリソースを用意することなく、オンプレミスのアプライアンスと同じ高度な脅威対策を利用できます。ネットワーク境界の外側からのアクセスが増えても、外出先のデバイスやユーザーにとってクラウドが共通の接続点になります。トラフィックを特定の場所にリダイレクトするセキュリティを構築するよりも、エンドポイントを効果的に保護できます。エンドポイントとすべての場所をクラウドに接続することで、ユキビタスな保護を実現できます。この新しい境界は従来のネットワーク境界のように乗り越えられることはありません。

主な特徴

- コスト効率の最も優れた方法でWebセキュリティを配備。オンプレミスにハードウェアやソフトウェアを用意する必要はありません。
- 高度な保護機能を提供。トラフィックの処理時に振る舞いをエミュレーションし、ゼロデイ マルウェアをミリ秒単位で阻止します。
- モバイル環境のユーザーも保護。クラウドから保護対策を提供することで、従来のネットワーク境界の垣根を排除します。
- McAfee® ePolicy Orchestrator®（McAfee ePO™）Cloudによる効率的な管理。統合管理コンソールでIntel Securityのすべてのクラウド サービスを管理できます。
- 実証済みのアーキテクチャ：McAfee® Web Gateway Cloud Serviceは、世界の大企業で採用されているオンプレミス アプライアンスであるMcAfee Web Gatewayのマルチテナント バージョンとして作成されています。

コスト効率の良いユキビタスな保護

オンプレミスでのWebセキュリティ アプライアンスの管理は多額なコストがかかるだけでなく、すでに多忙なセキュリティ チームをさらに疲弊させることになります。Webセキュリティをクラウド サービスとして配備することで、総所有コストを抑えることができます。ハードウェア アプライアンスを購入する必要も、所有や保守の必要もありません。アプライアンスの保守やソフトウェアのアップグレード、パッチの適用などを担当していた人員をIT部門やITセキュリティ部門内でより戦略的な業務に割り当てることができます。

また、アプライアンスとクラウド サービスを併用するハイブリッドな環境も構築できます。多くの企業はこのモデルを採用し、ネットワーク上のアプライアンスを制御し、小規模なリモート オフィスや移動中のユーザーをクラウド サービスで保護しています。

ネットワーク上のWebゲートウェイ アプライアンスでフィルタリングするために、リモート オフィスからMPLS（Multiprotocol Label Switching）回線経由でWebトラフィックを中継していたITチームにとって、クラウド型のWebセキュリティは大きなメリットがあります。トラフィックの中継はコストがかかり、ネットワークが複雑になります。リモート オフィスからのトラフィックがクラウドに直接ルーティングされて保護できれば、MPLS回線を使用する必要がなく、ネットワーク アーキテクチャを簡素化できます。

これまでは、モバイル環境のユーザーやデバイスは保護できず、IT部門から見えない存在でした。このため、Webにアクセスできる従業員をネットワーク境界内に限定する必要がありました。Webセキュリティをクラウドに移行することで、このような境界をなくすことができます。モバイル環境のユーザーとデバイスからのWebトラフィックはクラウドに自動的にルーティングされるので、自宅や空港、コーヒーショップなど、社外環境でも安全な接続を維持できます。物理的な障壁がなくなり、エンドポイントがどこにあっても保護することができます。

intel Security

グローバルで高性能なアーキテクチャ

McAfee Web Gateway Cloud Serviceはエンタープライズ向けのソリューションです。多くの組織が、現在のオンプレミス ソリューションよりも優れたパフォーマンスを実現できます。たとえば、オンプレミスでセキュリティ能力を強化する場合、新しいアプライアンスを購入して配備しなければなりませんが、配備の完了までに数日から数週間かかる場合があります。弊社のクラウドの場合、サービスが柔軟な設計になっているため、能力の増強は15分程度で終わります。

オンプレミス アプライアンスに障害が発生し、修理が必要になると、インターネットへの接続が切断されるだけでなく、障害発生時にWebへのフェールオープンが有効になっている場合にはセキュリティ ポスチャが低下する可能性があります。データセンターで障害が発生した場合、弊社のクラウド サービスは最も近いデータセンターにすべてのWebトラフィックを自動的に転送し、継続性を維持します。

弊社のクラウド サービス アーキテクチャは、世界最大の相互接続点（IXP）でインターネット バックボーンに接続しています。これにより、中間のインターネット サービス プロバイダー（ISP）のルーティング ホップ数が減るので、接続の待ち時間が少なくなります。Microsoft Office 365やGoogleなど、人気の コンテンツ プロバイダーへのホップ数が少なくなるので、オープン ネットワークに直接接続するよりも、弊社のクラウド サービスを介したほうが速く接続できます。

McAfee Web Gateway Cloud Serviceではグローバルにサービスが提供されます。Webトラフィックを処理するデータセンターの場所と状態は、**https://trust.mcafee.com**で確認できます。Webコンテンツは、ユーザーが接続している場所ではなく、Googleの検索結果と同様に当該地域の言語で配信されます。

洗練された脅威の阻止

非常に巧妙なマルウェアや標的型攻撃は、従来の防御策を回避し、システムやネットワークに侵入してきます。このような脅威に対して、セキュリティ チームはエンドポイントの修復に追われ、常に後手に回ることになります。従来のURLフィルタリングやシグネチャ ベースのアプローチと異なり、McAfee Web Gateway Cloud Serviceは、ファイル、JavaScript、HTMLのインライン エミュレーションを行い、ゼロデイやファイレスのマルウェアからエンドポイントを保護します。これにより、ゼロデイ マルウェアの侵入を阻止し、URLフィルタリングとシグネチャを利用 するソリューションよりも

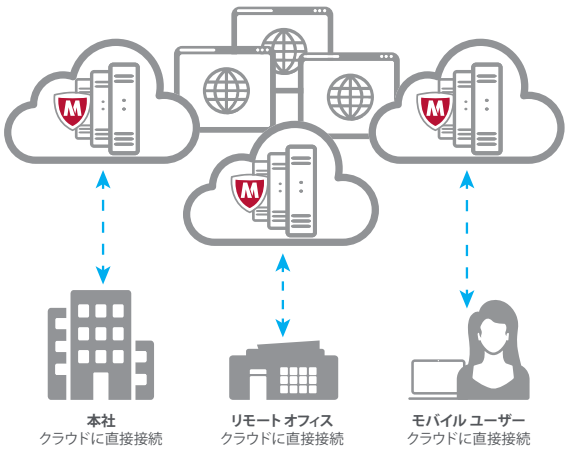

図 1. McAfee Web Gateway Cloud Serviceの配備

ブロック率が約20%向上します。マルウェア インシデントの発生数も減少するため、コストの削減だけでなく、リソースをより柔軟に活用することができます。

Webの脅威は、Webセキュリティの検出を回避するために、暗号化トラフィックで送信されます。クラウド ストレージやソーシャル メディアなど、ほとんどのクラウド アプリケーションがデフォルトで暗号化トラフィックに対応しています。McAfee Web Gateway Cloud Serviceは、暗号化されたHTTPSトラフィックを完全に復号して検査します。暗号化されたチャネル内でもマルウェアを阻止し、クラウド アプリケーションの可視性を実現します。

ほとんどのITチームは、増え続けるクラウド アプリケーションに苦慮しています。特に、シャドウITは大きな課題です。ユーザーが選択したサービスがリスクとなる可能性があります。HTTPSを含むすべてのWebトラフィックが可視化されれば、事前定義のレポートで、アクセスされたWebサイト、使用中のクラウド アプリケーション、対応するデータポイントを確認し、リスクを診断できます。IT部門が承認したものと実際に使用されているものを比較すれば、シャドウITを簡単に見つけることができます。クラウド アプリケーション、特にクラウド ストレージがマルウェアの散布方法として利用されるケースが増えています。マルウェアを散布するアプリケーションを識別することで、ポリシーを決定できます。アクセスされているクラウド サービスを考えると、1,600を超えるクラウド アプリケーションを統制し、アップロードやメッセージングの防止、アプリケーションのブロックなどを行い、リスクを回避する必要があります。

McAfee Web Gateway Cloud Serviceの稼働状況

弊社のデータセンターの場所、可用性、状況については、**https://trust.mcafee.com**をご覧ください。

効果的なセキュリティ管理

複数のコンソールとポリシーでのセキュリティ管理は煩雑な作業になります。オンプレミスとクラウド ベースのWebセキュリティを別々に管理すると、管理者の負担はさらに増加します。ハイブリッド環境の場合、オンプレミスとクラウドの両方を1つのコンソールで管理し、特定のポリシーと共通のレポート インターフェースを使用する必要があります。

オンプレミスのハードウェアやソフトウェアなしでMcAfee Web Gateway Cloud Serviceを単独で配備する場合には、McAfee ePO Cloudで管理します。この統合管理コンソールは、Intel Securityが提供するクラウド ベースのすべてのセキュリティ サービスとエンドポイント セキュリティに対応しているので、効率的なセキュリティ管理が可能です。

エンドポイント デバイスにWebセキュリティを配備するのは簡単ではありません。特に、ルーティングや認証が問題になります。オプションのエンドポイント クライアントであるMcAfee Client Proxyを使用すると、弊社のクラウド サービスに自動的にルーティングし、認証を行うことができます。これにより、一貫したポリシーでクラウドに接続できます。McAfee Client Proxyは、ハイブリッド環境でシームレスに機能します。ネットワーク内では、アプライアンスへのルーティングを、モバイル環境ではクラウド サービスへのルーティングを自動的に行います。ルーティングと認証に追加のオプションがあります。これらのオプションは組織の要件に合わせて選択できます。

詳細情報

詳細については、**http://www.mcafee.com/jp/products/web-protection.aspx**をご覧ください。

McAfee. Part of Intel Security.
マカフィー株式会社
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　〒450-0002 愛知県名古屋市中村区名駅 4-6-17 名古屋ビルディング 13F TEL 052-551-6233（代）FAX 052-551-6236
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）
www.intelsecurity.com