フォーティネット セキュリティ ファブリックによる Microsoft Azure の高度なセキュリティの実現

要約

Microsoft Azure は、ハイブリッドクラウドの移行と共存のパスを容易にすることで、クラウドのコンプライアンスと保護を強化するよう設計されています。Microsoft Azure は、Azure やオンサイトの情報を保護する、さまざまなセキュリティソリューションやテクノロジーをサポートしています。さらに、Microsoft のエンタープライズサービスを積極的に採用し、現在は Office 365 の導入を通じてクラウドへの移行が進んでいる組織に独自のメリットを提供します。しかしながら、Azure と Office365 には、クラウド内のデータを保護するエンタープライズクラスの完全なセキュリティ機能はありません。このため、企業はパブリッククラウドとオンプレミスのインフラストラクチャのアプリケーションや情報を細部にわたって可視化し、きめ細かく制御する機能を追加しなければなりません。Azure 向けフォーティネット セキュリティ ファブリックは、マルチクラウドインフラストラクチャに一貫性あるセキュリティポリシーを適用することで、高度なクラウドベースの攻撃の可視化、制御、保護を可能にします。

Azure パブリッククラウドの さまざまなユースケースを保護

Azure 向けフォーティネット セキュリティ ファブリックによって、一貫性あるクラス最高レベルのエンタープライズセキュリティが Microsoft Azure ベースのクラウド環境に拡張されます。セキュリティ ファブリックは、クラウドベースアプリケーションに対する多層型セキュリティをはじめとする強力なセキュリティによって、オンプレミスのデータセンター全体とクラウドの両方の環境のビジネスワークロードを保護します。セキュリティ ファブリックは、次のような多くのエンタープライズクラウドの一般的なユースケースをサポートしています。

1. **ハイブリッドクラウド**：企業には、クラウドのワークロードに合わせて拡張できる、シームレスなセキュリティオーケストレーションが必要です。フォーティネット セキュリティ ファブリックに含まれる次世代ファイアウォール（NGFW）は、ネイティブの Azure セキュリティ機能を補完し、クラウドインフラストラクチャのあらゆる種類の安全で暗号化された接続をサポートします。NGFW は、パブリッククラウド環境または自社のデータセンターのオンプレミスのどちらからでも管理できます。
2. **高度な脅威保護**：最新のビジネスアプリケーションが、パブリッククラウドインフラストラクチャに配備される割合が確実に増加しています。それと同時に、ブリーチのパターン別件数がもっとも多いのは、Web やメールのアプリケーションであることが明らかになっています。Azure 向けフォーティネット セキュリティ ファブリックには、FortiWeb、FortiMail、FortiSandbox などのセキュリティ ファブリック ソリューションを活用し、そのようなビジネスクリティカルアプリケーションを既知およびゼロデイの攻撃から保護するよう設計されたソリューションが含まれています。これにより、サーバーへの終わりのないパッチ適用が不要になります。また、PCI DSS（Payment Card Industry Data Security Standard） や HIPAA（Payment Card Industry Data Security Standard）などの法規制やセキュリティ基準へのコンプライアンスもサポートしています。さらに、FortiSandbox は、悪意あるファイルのアップロードによって開始する高度な持続的脅威に伴うリスクから、コラボレーション型 Web サイトを保護できます。
3. **セキュアアクセス VPN**：フォーティネット セキュリティ ファブリックは、Azure のリモートアクセス VPN の VPN トラフィックをクラス最高レベルのパフォーマンスで保護します。Azure のマルチリージョンのグローバルインフラストラクチャを活用することで、組織は世界中に展開されている自社のサービスを瞬時に拡張し、リモートアクセス VPN ターミネーションをエンドユーザーに近い場所で提供できます。リモートアクセス VPN は、クラウドベースのアプリケーションだけでなく、プライベートリンクや VPN などの異なる形態でクラウドに接続する、オンプレミスのアプリケーションへのアクセスにも利用できます。
4. **クラウドサービスハブ（vNET）**：クラウドプロバイダの接続では、一般的な中規模の企業のパフォーマンスに対応することはできません。Azure ベースの仮想ネットワーク（vNET）によって、企業は世界中の複数のネットワークでセキュリティサービスを共有できるようになります。ネットワークの可視性、VPN 接続、次世代ファイアウォール（NGFW）、高度な Web アプリケーションファイアウォール、サンドボックス、メールセキュリティをはじめとする、フォーティネットの広範なソリューションの活用により、セキュリティ ファブリックは、はるかに多くのサービスの利用を可能にすると同時に、クラウドの柔軟性とオンデマンドの拡張性を活かした最適な価格性能比を実現します。
5. **Office 365 の保護**：Office 365 や Azure を使用するクラウド環境ではファイルが添付される割合が高く、ほとんどの脅威が組織への侵入手段として電子メールを悪用する事実も考慮すると、Office 365 ベースの電子メールやビジネスアプリケーションの保護の必要性がかつてないほど高まっています。FortiMail、FortiSandbox、FortiCASB の組み合わせによって、Office 365 の保護に不可欠な機能が提供されます。セキュリティ ファブリックでは、メールメッセージを詳細に可視化できるため、ゼロデイ脅威からの保護と Office 365 の API 層の監視が可能になります。

セキュリティ ファブリックによる Azure のセキュリティの補完

セキュリティ ファブリックは、多層型の強力な保護と運用の効率化によって、Azure 内のアプリケーションを既知および未知の脅威から保護し、グローバルなセキュリティインフラストラクチャのクラウドからの管理を可能にします。Azure 向けセキュリティ ファブリックには、次のような特長と機能があります。

一元的な制御と管理：セキュリティ ファブリックでは、クラウドとオンプレミスの両方のセキュリティ機能を Azure から集中管理できるため、人的エラーが回避できると同時に、IT 担当者の限られたリソースを別の重要な業務に活用できます。

クラウドネイティブの可視化と制御：企業は、セキュリティ ファブリックによって Azure アプリケーション環境の詳細な可視化が可能になります。それぞれの配備環境向けに構成計画を立てる必要がなくなり、インテントベースのポリシーを適用できるようになります。動的アドレスグループやクラウドベースのリソースの論理的な名前を使用することで、クラウドインフラストラクチャにおけるセキュリティ ファブリック リソースのスケールアウトに合わせて、セキュリティポリシーを拡張して適用することができます。

シャドー IT の制御：組織において IT 運用の合理化とセキュリティ制御の統合が進むに伴って、多くのビジネス部門がクラウドベースサービスを自ら調達するようになりました。セキュリティ ファブリックは、Azure インフラストラクチャの利用状況の可視性を向上し、使用パターンに対する制御を強化することで組織をリスクから保護できるようになるという大きなメリットを IT 部門にもたらします。

ゼロデイ攻撃からの保護：フォーティネット セキュリティ ファブリック ソリューションでは、クラウドインフラストラクチャに優れた拡張性を備えるゼロデイ攻撃保護機能が完全に統合されます。これによって、高度な持続的脅威に対する組織のリスクが軽減され、どのような規模のアプリケーションであっても安心してクラウドに導入できるようになります。

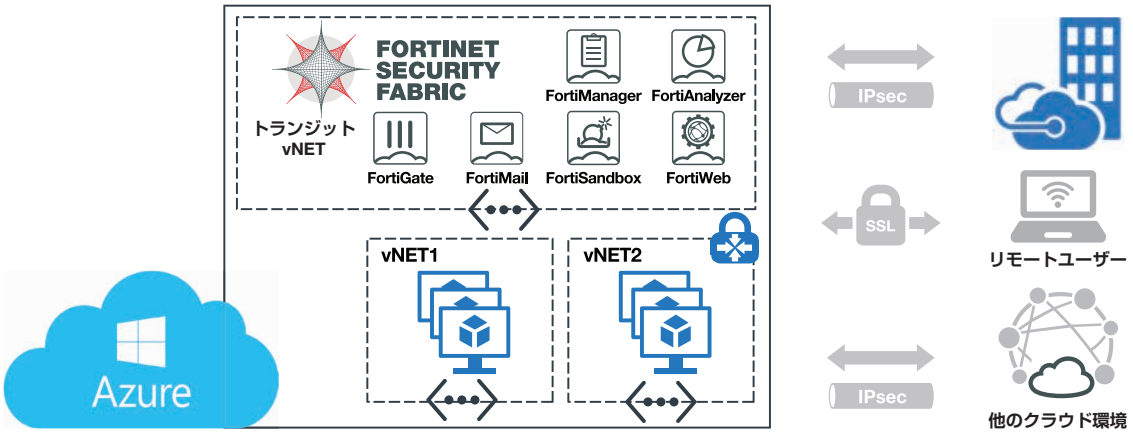

図 1：Microsoft Azure 向けフォーティネット セキュリティ ファブリック

コンプライアンスへの対応：セキュリティ ファブリック ソリューションは、クラス最高レベルの保護機能を提供し、PCI DSS（Payment Card Industry Data Security Standard）などの現行の業界標準だけでなく、EU の一般データ保護規則（GDPR：General Data Protection Regulation）などの最新のデータ保護法へのコンプライアンスも支援します。

あらゆる脅威に対抗する統合型対策

Azure 向けフォーティネット セキュリティ ファブリックを構成するさまざまなソリューションは、エンドユーザーが安心して利用できる Azure クラウド環境を実現するよう各々が設計されています。これらのソリューションは、いずれもフォーティネットの仮想マシン（VM）フォームファクタを採用しているため、フォーティネットのチャネルパートナーから購入した VM のライセンスをプラットフォーム間で移動できます。例えば、**BYOL（Bring-Your-Own-License）**モデルを使用している場合、VMware で使用している FortiGate VM の VM ライセンスは Azure プラットフォームの FortiGate でも機能します。さらに、**PAYG（Pay-As-You-Go）オンデマンド利用モデル**を Azure マーケットプレイスから直接使用して、FortiGate、FortiMail、FortiWeb を利用することもできます。

フォーティネット セキュリティ ファブリックには、以下のソリューションが含まれます。

- **FortiGate VM NGFW** は、業界最高レベルの脅威防御機能を提供し、最も高度な既知および未知のサイバー攻撃からの保護を可能にします。FortiGate VM は、お客様の要件に合わせた拡張や縮小が可能であると同時に、サポートするさまざまなユースケースに合わせて複数の異なるサイズで提供されます。
- **FortiMail** メールセキュリティゲートウェイは、FortiGuard Labs の最新のテクノロジーとサービスを活用して高度な脅威からのトップクラスの保護を常に提供するとともに、統合された強力なデータ保護機能によってデータの喪失を防止します。
- **FortiSandbox** は、高度な検知、自動化された減災、実用的インテリジェンス、柔軟な導入形態の強力な組み合わせによって、標的型攻撃とそれに伴うデータ損失を防止します。
- **FortiWeb** WAF（Web アプリケーションファイアウォール）は、既知 / 未知両方の脆弱性に対するエクスプロイトの攻撃から、ホスティングされている Web アプリケーションを保護します。 多層型の相関的な検知メソッドを活用することで、FortiWeb は既知の脆弱性およびゼロデイ攻撃の脅威からアプリケーションを保護します。
- **FortiManager** は、大規模あるいは分散型の企業の管理とポリシー制御を一元化することで、ネットワーク全体のトラフィックベースの脅威に対する実用的インテリジェンスを提供します。 高度な脅威を封じ込めることができるだけでなく、優れた拡張によって、最大 10,000 台のフォーティネットデバイスを管理できます。
- **FortiAnalyzer** は、フォーティネット製品からのデータの収集、分析、相関付けによって可視性を向上させ、強力なセキュリティアラート情報を提供します。 FortiGuard IOC（Indicators of Compromise：侵害指標）サービスと組み合わせることで、侵害されたホストの優先度順リストが提供されるため、すぐに対策を実行できます。
- **FortiCASB** は、可視性、コンプライアンス、データセキュリティ、および脅威保護をサポートする、クラウドネイティブのクラウドアクセスセキュリティブローカー（CASB）サブスクリプションサービスです。 包括的なレポートツールによって、ユーザー、行動、およびクラウド上の保存データに関する実用的なインテリジェンスを提供します。
- **ファブリックコネクタ**は、フォーティネット セキュリティ ファブリックのオープン統合を可能にすることで、お客様のエコシステム内の複数の既存のコンポーネントによるファイアウォールやネットワークセキュリティの動的なネットワークフローへの挿入を自動化します。

リスクを軽減する多層型保護

フォーティネットは、プライベート、パブリック、ハイブリッドのクラウドプラットフォームにおけるセキュリティの可視性と管理の阻害要因を解消します。その結果、セキュリティ部門のリーダーはすべての攻撃対象領域に対応するセキュリティネットワークを構築できるようになります。

Azure 向けフォーティネット セキュリティ ファブリックは、組織のオンプレミスからクラウドまでの環境で、共有レポジトリモデルによる一貫性あるセキュリティ保護を実現します。包括的な多層型セキュリティと脅威対策による Azure ユーザーの保護が可能になると同時に、運用、ポリシー管理、可視性の合理化が実現し、セキュリティのライフサイクル管理が改善されます。

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.co.jp/contact

お問い合わせ