SOLUTION BRIEF

フォーティネットで実現するワンステップ先の Microsoft Azure 向けセキュリティ

エグゼクティブサマリー

現代のセキュリティでは、すべてのデータセンター、支社、クラウド全体で、一貫したツールとポリシーを確保することが必要です。あらゆるコンピューティングで、ポリシー強制、可視化、オーケストレーションを完全に統一することを目指すべきです。しかし、平均的なセキュリティスタックには複数の異なるツールが含まれているため、運用のサイロ化やセキュリティギャップといった問題が起こり、完全な統一を達成することができません。

企業は、セキュリティ、ネットワーク、コンピューティングを統合・統一することの重要性を認識する必要があります。展開される場所に関係なく、アプリケーションとデータを保護する統合型のセキュリティ製品スイートが、そのニーズに応えます。

世界を動かす企業は Microsoft Azure を取り入れ、フォーティネットのエンタープライズ向けセキュリティソリューションでそのクラウド環境やデータセンターを保護しています。マイクロソフトとフォーティネットの連携は広範にわたるため、Microsoft Azure を利用しているあらゆる規模の企業が、この共同開発ソリューションを利用して、確実にクラウドへ移行し、そこで成長することができます。

クラウドへの移行に伴うセキュリティ上の課題を理解する

クラウドへの移行には、新たな収益源の創出から市場投入サイクルの短縮まで、さまざまなメリットがあります。しかし、クラウドへ移行する際は、特定のセキュリティ面に関する検討も行わなければなりません。フォーティネットの 2023 年クラウドセキュリティレポート[1] によると、95% の企業がクラウドのセキュリティを「とても」または「かなり」懸念しています。この結果には、以下の要因が影響しています。

- 組織の成長とともに拡大する攻撃対象領域
- ハイブリッドクラウドやマルチクラウドの展開に伴う煩雑性の悪化
- 断片的なセキュリティソリューションに起因する可視性の欠如
- リモートワークの普及に伴う、ネットワーク、デバイス、アプリケーションの継続的な増加
- 急速に進化する脅威情勢に対応できる有能なセキュリティ専門家の不足

フォーティネットの先駆的な Microsoft Azure 保護

現代の拡大し続けるネットワーク全域の煩雑性を軽減し、全体的なセキュリティ効果を高めるためには、FortiGuard Labs の継続的な研究に裏打ちされたフォーティネットセキュリティファブリックが不可欠です。Microsoft Azure を利用している企業は、連携して包括的な可視性と多層構造のセキュリティを提供する、フォーティネットとマイクロソフトの共同開発ソリューションを利用できます。

フォーティネットが選ばれる理由

100 以上に上るフォーティネットとマイクロソフト間の統合

マイクロソフト・パートナー・オブ・ザ・イヤーを受賞

ガートナーのマジッククアドラント 2022、ネットワークファイアウォール、SD-WAN、SIEM、エンタープライズ向け有線・無線 LAN インフラストラクチャ部門で「リーダー」評価を獲得

マイクロソフトは、2017 年からフォーティネットの Fabric-Ready パートナーに参加

1 フォーティネットの 2023 年クラウドセキュリティレポート

フォーティネットを利用した Microsoft Azure セキュリティのユースケース

ユースケース 1
安全に Microsoft Azure へ移行し、クラウド環境を構築する

Microsoft Azure にアプリケーションを移行するフォーティネットのお客様であれ、すでに Microsoft Azure を利用しており、自社環境に優れたセキュリティを求めている企業であれ、フォーティネットとマイクロソフトの連携ソリューションを利用すれば、クラウド環境を効果的に保護できます。フォーティネットは、ネットワーク、クラウドプラットフォーム、アプリケーションを保護するソリューションを通じて、Microsoft Azure に展開されるアプリケーションとワークロードを保護します。Microsoft Azure のインフラストラクチャと一体化されたフォーティネットの優れたセキュリティソリューションは、Microsoft コマーシャルマーケットプレイスからご購入いただけます。さらに、フォーティネットのすべてのセキュリティソリューションは、すべてのクラウドとデータセンターをカバーするセキュリティファブリックに含まれています。

FortiGuard Labs に裏打ちされたフォーティネットセキュリティファブリックは、1 日あたり 140 億件以上のセキュリティイベントを収集し、分析しています。人工知能と機械学習を活用し、継続的かつリアルタイムに脅威インテリジェンスを強化します。そして、このデータに基づいて最新の脅威を見つけ、対策を講じます。

- フォーティネットのソリューションは、Azure Sentinel、Azure Active Directory、Azure Security Center、Microsoft Defender for Cloud、Azure Cloud Functions、Azure Application Gatewayなど、多数のMicrosoft Azureサービスに統合されています。
- FortiGate Next-Generation Firewall (NGFW) for Azureは、ネイティブ環境、ハイブリッド環境、マルチクラウド環境を保護します。FortiGate は、ユニークアプリケーションを認識・理解し、自社独自のトラフィックに適切なセキュリティ判断を下し、ボットネットの検出とトラフィックのセグメンテーションに対応します。
- フォーティネットのWebアプリケーションファイアウォール（WAF）であるFortiWebは、ビジネスクリティカルなWebアプリケーションとそのAPIを攻撃から守ります。機械学習ベースの高度な機能によってセキュリティを強化し、管理者の負担を和らげます。
- Azure Virtual Machineと統合されているため、セキュリティを簡単にスケーリングできます。

ユースケース 2
Microsoft Azure に展開される Web アプリケーションとその API を防御する

ベライゾンの「2022 年データ侵害調査報告書」によると、セキュリティインシデントで最も深刻なアクションベクター（攻撃元区分）は Web アプリケーションであり、その数は侵害の 42% に相当します [2]。FortiWeb Cloud を利用すれば、単一のソリューションですべての Web アプリケーションと API を保護できるため、展開と管理が簡素化されます。また、企業にエンタープライズ機能が備わり、同時に時間と予算も節約できます。FortiWeb Cloud によって、高度なビジュアル分析と機械学習機能が提供されるため、OWASP Top 10 の脅威やゼロデイ攻撃といった脅威を防ぐことが可能になります。従来の WAF の領域を超え、以下のような高度な機能が実現されます。

- B2B通信やモバイルアプリケーションに対応するためのAPIの発見と保護
- 自動検知・緩和機能により、悪質なボットには対応しながら、善良なボットを歓迎するボット管理
- アナリストのアラート疲れを軽減し、迅速に最も重要な脅威に集中することをサポートする脅威分析
- FortiGuard Labsからの最新のシグネチャ情報と分析結果が反映された最新の脅威インテリジェンス

2 2022 年データ侵害調査報告書 ¦ Verizon

ユースケース 3
Azure Virtual WAN を統合し、グローバル SD-WAN を構築する

Azure Virtual WAN（vWAN）とは、Microsoft Azure ネットワークをバックボーンとした高速グローバルトランジットネットワークアーキテクチャの構築をサポートするネットワーキングサービスです。マイクロソフトの WAN ハブに Fortinet FortiGate Secure SD-WAN for Microsoft Azure vWAN を直接展開すれば、外部との通信（North-South トラフィック）と内部通信（East-West トラフィック）を両方とも保護し、セキュア SD-WAN 環境のグローバルバックボーンとして Microsoft Azure を利用することが可能になります。

このソリューションは、Azure vWAN に展開されるマネージドアプリケーションとして一連の FortiGate を展開し、階層 4 ～ 7 のインスペクションによってセキュア SD-WAN をサポートします。Fortinet のセキュア SD-WAN は、Azure vNET、インターネット、支社やデータセンター間に、エンタープライズクラスのセキュリティとブランチネットワークを実現します。SD-WAN と NGFW を簡単にすべてのトラフィックフローに統合し、FortiGuard Labs に裏打ちされたレイヤー 4 ～ 7 のインスペクションと制御を強制することができます。コスト効率に優れ、高速接続を提供する FortiGate for Azure vWAN は、自動化、ディープアナリティクス、自己修復によって、オペレーションを効率化します。

- vWANにFortiGateを展開することで、クラウド内の接続だけでなく、各拠点間の接続、リモートユーザーとの接続、プライベート接続も保護されます。
- FortiManagerに管理を集中させることで、環境を一元的に可視化し、設定ミスによる脆弱性を軽減します。
- カスタマイズ可能な規制テンプレート、監査記録、ロールベースのアクセス制御によってコンプライアンス管理とレポート作成を簡素化するFortiAnalyzerを通じて、常にコンプライアンスを維持し、監査関連のさまざまな手作業を解消します。

ユースケース 4
Azure Virtual Desktops で運用される Microsoft Windows の保護を強化

完全なデスクトップおよびアプリケーション仮想化ソリューションである Windows Virtual Desktop（WVD）は、クラウド内で稼働します。リモートワークを推進するために、WVD を利用する企業が増えています。しかし、データセンター、支社、そして拠点を経由するクライアントから Azure サービスへの接続には、高度なルーティングとセキュリティが必要です。FortiGate は、エンドポイントからクラウドまでを仮想プライベートネットワーク（VPN）でつなげ、これらのすべての場所にネットワークインスペクションを提供することで、ゼロトラストやデータ漏洩防止などの高度なセキュリティポリシーを強制することができます。

- FortiGateは、VPNを通じた、データセンター、支社、そして拠点を経由するクライアントからMicrosoft Azureリソースへのアクセスにネットワークインスペクションを提供することで、Microsoft Azureのコア機能を補完します。オンプレミスやクラウドを介して、エンドポイントと相互に接続します。
- FortiGateのディープパケットインスペクション機能と、暗号化されたトラフィックを検査するSSLインスペクション機能によって、ネットワークセキュリティを保証します。
- FortiGateはセキュアSD-WANに対応しているため、支社や仮想デスクトップ同士が安全に接続できるようになります。
- FortiGateは、ゼロトラストポリシーを強制し、マイクロソフト環境にアクセスしようとするリモートユーザーやデバイスに厳しいバリデーションを促すことができる理想的なソリューションです。

ユースケース 5
SAP S/4HANA への移行を保護する

既存の SAP システムをアップグレードしたり、S/4HANA に移行する企業の多くが、SAP ワークロード向けに最適化された Microsoft Azure を利用しています。フォーティネットは全体的なアプローチを採り、Microsoft Azure を含む SAP ランドスケープ全域を保護します。

- フォーティネットのSAPコネクターは、さまざまなSAPコンポーネントと通信し、新しく起動されたインスタンスを自動的に保護したり、SAP Enterprise Threat Detectorとデータを共有したり、予期せず新しいポートが利用された場合でも、それを自動的に検出してSAPトラフィックを保護することができます。
- フォーティネットのSAP向けソリューションは、オンプレミスまたはクラウド内にかかわらず、SAPランドスケープを保護し、あらゆるコンピューティングで一貫性のあるセキュリティポリシーとツールを確保します。
- フォーティネットは、マイクロソフトのSAPアドバイザリーボードに参加するなど、マイクロソフトやSAPと緊密に連携しています。そのような理由から、フォーティネットは、Microsoft Azureに展開されるSAP向けに最高のセキュリティを提供するセキュリティソリューションを実現することができています。

フォーティネットはマイクロソフトと協力し、SAP 向けに次のようなソリューションを開発しました。

- エンタープライズSAPランドスケープ向けネットワークセキュリティ
- SAPソリューション向けアプリケーションセキュリティ
- ゼロトラストのアクセスによるSAP ID管理の強化
- SAPセキュリティオペレーションセンターの設立
- RISE with SAPのセキュリティ

セキュリティ製品ではなく、セキュリティパートナーを探す

クラウドセキュリティについて判断する際は、戦術的に製品を選ぶのではなく、最高のグローバルセキュリティパートナーを探すことを重視してください。業界をリードするセキュリティプロバイダーであり、統合脅威管理ソリューションの世界的リーダーであるフォーティネットは、Microsoft Azureに展開されるお客様のワークロードとアプリケーションを安全に保ちます。包括的な脅威インテリジェンスと、20年以上にわたりサイバーセキュリティ分野で起こしてきたイノベーションや経験に裏打ちされた幅広い種類のフォーティネットのソリューションが、Microsoft Azureに展開されるあらゆるアプリケーションを保護します。

最先端の Microsoft Azure 向けセキュリティの詳細については、以下のウェブページをご覧ください。

www.fortinet.com/azure

フォーティネットジャパン合同会社

〒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-ky-Step-Up-Security-Microsoft-Azure-2308-R1