SOLUTION BRIEF

Google Cloud 向け フォーティネットクラウドセキュリティ

概要

組織は IT 運用を最新化してアプリケーション開発を加速し、イノベーション達成までの時間を短縮することで、デジタルイノベーション時代における競争的優位を維持しようとしています。Google Cloud は、ビジネスイノベーションを実現する最新のツールをお客様に提供しています。ハイブリッドクラウドやマルチクラウドのインフラストラクチャでは、クラウドコンピューティングによってデジタル攻撃の対象領域が拡大しています。ハイブリッドクラウドインフラストラクチャでの攻撃対象領域の拡大に対処するために、フォーティネット セキュリティ ファブリックは広範囲にわたるセキュリティソリューションを提供しています。これにより、ネットワークセキュリティ、アプリケーションセキュリティ、クラウドプラットフォームセキュリティを 1 つのプラットフォームに統合することが可能になります。フォーティネットのアプローチは、セキュリティと Google Cloud をネイティブに統合することで、種類豊富なセキュリティソリューションを提供し、最終的には管理の簡素化とセキュリティ運用の自動化を実現します。Google Cloud のお客様は、Google Cloud でもオンプレミスでも任意のアプリケーションを自由に実行しながら、あらゆる場所で一貫したセキュリティを維持できるようになります。

Google Cloud 向けの高度なセキュリティ

Google Cloud 向けフォーティネットクラウドセキュリティは、クラス最高レベルの一貫したエンタープライズセキュリティを実現します。フォーティネット セキュリティ ファブリックは、オンプレミス、データセンター、ならびにクラウド環境でビジネスワークロードを保護し、クラウドベースのアプリケーションに適した多層型セキュリティを提供します。このソリューションは、仮想マシン（VM）、コンテナ、SaaS（Software-as-a-Service）といったさまざまな形式で、ネットワーク、アプリケーション、およびクラウドプラットフォーム向けのセキュリティ機能を提供しています。それぞれのインスタンスにおいて、フォーティネットのセキュリティ機能は Google Cloud とネイティブに統合されます。

Google は各種の基本的なセキュリティツールをお客様に提供し、セキュリティニーズに基づいた Google Cloud コンピューティングインフラストラクチャに対応しています。しかしながら、これらのツールは、基本的ニーズに応じて有効なセキュリティ機能を提供する一方、短期間での新機能開発と市場への製品投入を目指しているアプリケーション開発チームにとっては、運用面で多大なオーバーヘッドとなります。さらに、セキュリティ責任共有モデルに基づくと、Google Cloud はクラウドインフラストラクチャの保護、テナントの分離、およびサービスの継続的運営のみに責任を負っています。お客様がクラウド内で構築するアプリケーション、ならびに利用するサービスは、お客様の責任において保護する必要があります。クラウドリソースのセキュリティ保護は複雑なうえ、クラウドプロバイダーによって異なるため、クラウドセキュリティの不備は多くの場合、お客様の過失によって起こります。Google Cloud 向けフォーティネットクラウドセキュリティを使用すると、組織はオンプレミスからクラウドに至るすべての環境で、責任共有モデルが規定する一貫したセキュリティ態勢を維持することができます。フォーティネットクラウドセキュリティは、包括的で多層型のセキュリティ / 脅威保護を提供することで、組織のセキュリティ態勢を全体的に強化し、構成ミスを低減します。

拡大する脅威

76% の組織は、単一の調達先への依存や過大な支払いをなくすために、2 社以上のクラウドプロバイダーを利用しています。39% の組織は、ハイブリッドクラウドインフラストラクチャを使用して、既存のアプリケーションを最新化するうえでの自由度を高めようとしています [1]。Google の Anthos では、Google コンピューティングサービスをオンプレミスのデータセンターやエッジまで拡張できます。Anthos はオープンソースのテクノロジーを基盤にしているため、

Google Cloud 向けの エンタープライズセキュリティ

FortiCNP での継続的な脅威の可視化、FortiEDR と Google Cloud Security Command Center によるリアルタイムの保護

使い慣れたツールでワークロードを管理し、セキュリティ上の脅威を表示して、IT の効率性を高めます。

高度なセキュリティ / 脅威保護

最新の脅威インテリジェンスを入手し、リアルタイムで情報を共有することで、巧妙な攻撃によるリスクを軽減します。FortiGate セキュア SD-WAN と Network Connectivty Center（NCC）の統合により、支社から Google Cloud へのアクセスを保護します。

エッジからクラウドまでの 全域に対応するセキュリティ

一貫したセキュリティと汎用性の高いセキュリティ管理画面を使用して、場所を問わずアプリケーションを実行することで、柔軟にワークロードを展開できます。

アプリケーションを最新化する際、オンプレミス環境とクラウド環境の間で一貫性を保つことができます。Kubernetes のコンテナオーケストレーションのようなオープンスタンダードにおける Google のリーダーシップによって、オンプレミスとパブリッククラウドの最も優れたコンピューティング機能が結合され、ビジネスイノベーションや、クラウド支出を最適化する価格設定が可能になります。フォーティネットクラウドセキュリティは、オンプレミスやさまざまなクラウドに継続的セキュリティを提供し、Google Cloud ユーザーを保護します。

Google Cloud セキュリティを補完するセキュリティ ファブリック

フォーティネット セキュリティ ファブリックは、多層型の保護と運用の効率化によって、オンプレミス、データセンター、ならびにクラウド環境でビジネスワークロードの安全性を維持します。Google Cloud 向けフォーティネット セキュリティ ファブリックの主な機能は次のとおりです。

- **一元的な制御と管理**
  クラウドとオンプレミスのいずれにおいても、フォーティネット セキュリティ ファブリックのリソースは Google Cloud から集中管理できます。こうしたシンプルな管理によって、人的エラーを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集約させることができます。
- **クラウドネイティブな可視化と制御**
  FortiCNP のクラウドネイティブ保護（CNP）は、実用的なインテリジェンスを活用してセキュリティ情報にコンテキストを追加し、最も重要なリソースを優先することで、セキュリティを簡素化し、セキュリティチームが効果的にクラウドのリスクを管理できるようにします。
- **ゼロデイ攻撃からの保護**
  最新の脅威インテリジェンスを入手して、エッジからクラウドまでの全域でアプリケーションのセキュリティを維持し、拡張性に優れたゼロデイ攻撃保護機能を提供します。この機能は Google Cloud と完全に統合されています。FortiGuard Labs のグローバルセキュリティ研究チームには、215 名を超える専任エキスパートが在籍しています。AI（人工知能）/ ML（機械学習）システムは、毎日 1,000 億件以上のセキュリティイベントを収集、分析しています。
- **コンプライアンスへの対応**
  有益な即時セキュリティレポートから、標的型攻撃に関する実用的インテリジェンスを入手します。Payment Card Industry Data Security Standard（PCI DSS：クレジットカード業界データセキュリティ基準）、Health Insurance Portability and Accountability Act（HIPAA：医療保険の携行性と責任に関する法律）などの現行の業界標準だけでなく、EU の General Data Protection Regulation（GDPR：一般データ保護規則）などのデータ保護法へのコンプライアンスも支援します。

あらゆる脅威に対する防御

フォーティネットは、オンプレミスやクラウド環境でセキュリティの可視性と管理を阻害している要因を取り除きます。Google Cloud 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、組織のセキュリティ態勢を強化し、エンドユーザーの Google クラウド環境に対する信頼を高めるよう設計されています。

ソリューションには、以下の柔軟な調達オプションを適用することも可能です。

- **BYOL（Bring-Your-Own-License）**
  フォーティネットのチャネルパートナーから購入したさまざまな製品のライセンスは、プラットフォーム間で移行できます。
- **PAYG**
  フォーティネットソリューションの多くは、Google Cloud マーケットプレイスの PAYG（Pay-As-You-Go）オンデマンド利用モデルを使って導入できます。

Google Cloud 向けフォーティネット セキュリティ ファブリックには、以下の製品が含まれています。

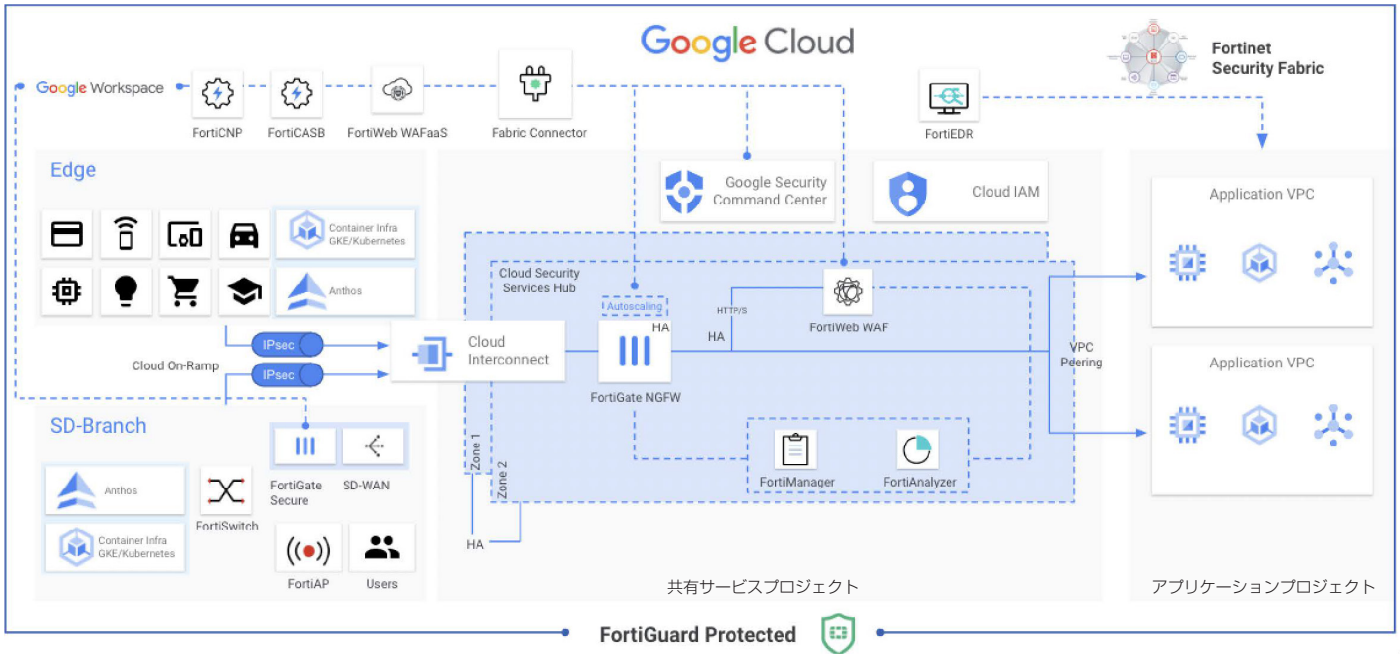
- **FortiGate NGFW（BYOL、PAYG）**
  業界最高レベルの脅威保護機能を提供し、既知および未知の高度なサイバー攻撃を防御します。FortiGate は、API を使用してインフラストラクチャを認識するため、HA（高可用性）環境を自動的に構成し、フェイルオーバーのシナリオを作成することができます。FortiGate VM によって、Google Cloud の Network Connectivity Center（NCC）との統合が可能になります。NCC はハイブリッドクラウドやマルチクラウドにおいて、Google Cloud が提供するネイティブクラウドのアンダーレイと、フォーティネットのセキュア SD-WAN および Cloud on Ramp（クラウド接続サービス）との調整を行います。
- **FortiWeb（BYOL）**
  FortiWeb は VM として展開され、OWASP Top 10 、ゼロデイ攻撃、アプリケーションレイヤーに対するその他の攻撃など、既知および未知の脆弱性を狙った攻撃から Web アプリケーションや API を保護します。

- **FortiWeb Cloud WAF-as-a-Service（SaaS PAYG）**
  SaaSサービスとして提供されるFortiWeb Cloudは、ボット減災やAPI検出などの機能を備え、OWASP Top 10やゼロデイ攻撃、アプリケーションレイヤーに対するその他の攻撃から、パブリッククラウドでホストされているWebアプリケーションを保護します。
- **FortiManager（BYOL）**
  フォーティネットは、拡張エンタープライズ全体の管理とポリシー制御を一元化し、ネットワーク全域のトラフィックに関連した脅威について、実用的インテリジェンスを提供します。FortiManagerは、高度な脅威を封じ込めるほか、優れた拡張性によって最大10,000台のフォーティネット製品の管理を可能にします。
- **FortiAnalyzer（BYOL）**
  このソリューションは、フォーティネット製品からデータを収集、分析、相関付けして可視性を向上させ、信頼性の高い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も提供されるため、ただちに対策を実施できます。
- **FortiCNP（BYOL、PAYG）**
  FortiCNPは、クラウドサービスプロバイダー（CSP）のセキュリティサービス、およびフォーティネットのセキュリティ ファブリックとネイティブに統合された、クラウドネイティブ保護（CNP）プラットフォームであり、包括的で豊富な機能を備えたクラウドセキュリティソリューションによってクラウドワークロードを保護します。
- **FortiADC（BYOL）**
  FortiADCは、卓越したロードバランシングとWebセキュリティを使用して、アプリケーションのパフォーマンスを最適化します。グローバルなサーバーロードバランシング、リンクロードバランシング、ユーザー認証などを実行し、企業アプリケーションに適した可用性、パフォーマンス、セキュリティを実現します。
- **ファブリックコネクタ**
  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な統合を可能にします。これにより、お客様のエコシステムに既存の多様なコンポーネントを使用して、Google Cloudにファイアウォールやネットワークセキュリティを自動的に導入できます。さらには、Google Cloudのセキュリティインテリジェンスサービスを統合することも可能です。

FortiEDR

FortiEDRは、MITRE ATT&CKで認定された振る舞いベースのエンドポイントの脅威検知とレスポンス（EDR）テクノロジーを使用して、Google Cloudのワークロードを保護します。FortiEDRは攻撃対象領域を縮小し、攻撃をリアルタイムで検知して無害化します。また、ポリシー違反を解消するための、広範囲かつカスタマイズ可能な自動化手順もサポートしています。

参考アーキテクチャ



フォーティネット セキュリティ ファブリックを Google Cloud まで拡張するユースケース

Google Cloud 向けフォーティネット セキュリティ ファブリックは、一貫性のあるエンタープライズセキュリティを提供します。フォーティネット セキュリティ ファブリックは、クラウド専用アプリケーションに適した多層型セキュリティなどの機能によって、オンプレミス、データセンター、およびクラウド環境のワークロードを保護します。このソリューションは、Google Cloud 関連の広範囲な企業ユースケースに対応しています。

1. **ネットワークセキュリティ**
   クラウドセキュリティサービスのハブを使用して、拡張可能な多層型セキュリティを実装します。Google Cloud インフラストラクチャの規模と柔軟性を活用し、効果的で摩擦の少ないネットワークセキュリティソリューションを構築できます。
   - 分散型エンタープライズ / SD-WAN
   - ハイブリッドクラウド
   - VPC 間のセグメンテーション
   - リモートアクセス
   - GKE クラスタ用の境界セキュリティ

2. **アプリケーションと Web トラフィックのセキュリティ**
   ゼロデイ攻撃、ボットネット攻撃、API 攻撃など、既知および未知の脅威からビジネスクリティカルなアプリケーションを保護します。また、サーバーの脆弱性によるリスクを緩和し、最新の法律、規制、標準の遵守を支援します。
   - Apigee 向け API セキュリティ
   - Web アプリケーションセキュリティ
   - 規制遵守
   - リスク管理
   - ボット対策

3. **クラウドワークロードの保護**
   - 構成の評価
   - クラウドアカウントのアクティビティ監視
   - クラウドトラフィックの監視
   - クラウドデータのセキュリティスキャン

エンタープライズ保護によるリスクの軽減

Google Cloud 向けフォーティネットクラウドセキュリティを使用すると、組織はオンプレミスからクラウドに至るすべての環境で、責任共有モデルが規定する継続的かつ一貫したセキュリティ保護を維持することができます。フォーティネットクラウドセキュリティは、包括的で高度なセキュリティと脅威保護の機能を Google Cloud ユーザーに提供します。一元化されたポリシー管理を通じた継続的な制御と可視化により、セキュリティの複雑さを緩和します。フォーティネットクラウドセキュリティを使用すれば、ネットワークの攻撃対象領域全体を組織のセキュリティアーキテクチャでカバーできると共に、機密データのコンプライアンスは維持され、その安全性は確保されます。

[1]「2022 年クラウドセキュリティレポート」、Fortinet、2022 年

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-Fortinet-Dynamic-Cloud-Security-for-Google-202310-R1