OVERVIEW

FortiGuard セキュリティサービス

攻撃チェーンを分断し、組織を保護するには、拡大し続ける攻撃対象領域で新たに発見される攻撃を検知し、セキュリティ態勢を迅速に調整する必要があります。

現在のセキュリティ態勢でそれが可能でしょうか？

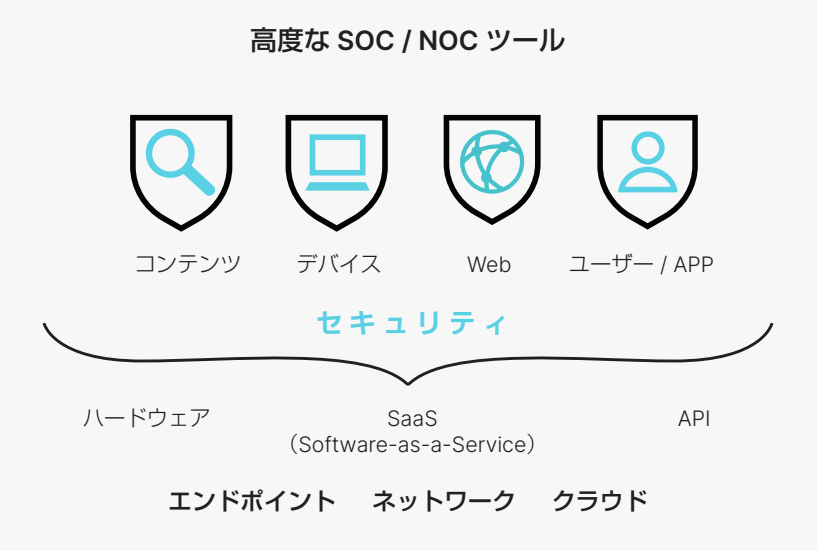
FortiGuard セキュリティサービスは、市場をリードする AI を活用したセキュリティ機能で継続的にリスクを評価し、フォーティネット セキュリティ ファブリックとエコシステムを自動的に調整することで、アプリケーションコンテンツ、Web、デバイス、ユーザーを保護します。連携型で一貫性のあるリアルタイムの防御をネットワークのエンドポイントやクラウドに提供し、最新の攻撃に対する保護を可能にします。

FortiGuard を選択する理由

包括的：目に見えない敵から保護することはできません。リアルタイムのレスポンスが必要であるとともに、包括的に保護することで、はじめてセキュリティギャップを解消することができます。

あらゆる場所で保護：ハードウェア、ソフトウェア、SaaS（サービスとしてのソフトウェア）のハイブリッドモデルをサポートする最大規模の製品ポートフォリオで、あらゆる攻撃対象領域と攻撃サイクルを保護する、連携型で一貫性のあるセキュリティ検知とレスポンスを可能にします。

あらゆる保護の統合：ネイティブかつ API ベースの統合で実現する、テクノロジーと脅威インテリジェンスの最大規模のエコシステムを提供します。



高品質の分析：AI / 分析システムは、適切なアドバイスやトレーニングなしには実現しません。統合データセットに基づき、信頼性の高いセキュリティ分析結果を提供します。

高品質のトレーニング：フォーティネットの AI は、業界最大規模で最も経験豊富なセキュリティリサーチ部門の 1 つである FortiGuard Labs によって継続的にトレーニングされています。

高品質のデータ：フォーティネットの AI は、エンドポイント、ネットワーク、クラウドからのインテリジェンスを始めとする、業界最大規模で最も多様なデータセットの 1 つを活用し、継続的にトレーニングされています。

圧倒的なスケーラビリティ：フォーティネットのプラットフォームは、1 日平均 1,000 億件以上のイベントを取り込んで分析し、毎日 10 億件以上のセキュリティアップデートをフォーティネット セキュリティ ファブリックとエコシステムに配信しています。

コミュニティの強化：世界中に展開されているファブリックやパートナーからの数百万のイベントを参照してお客様を保護し、コミュニティの既知の脅威における「第二」の最初の感染を防止します。

新たに発見された脅威に対する保護までの時間：セキュリティ態勢を時間通りに更新できなければ、攻撃シーケンスを分断できません。フォーティネットは、連携型の自動化された保護をほぼリアルタイムで提供します。

攻撃シーケンスの分断：関連するすべてのセキュリティテクノロジーによる新しい保護のホリスティックビューをほぼリアルタイムで生成することで、攻撃シーケンスに合わせた連携型の適用を可能にします。

広範囲の保護：新たに作成された保護を自動的に配布し、市場をリードする連携型の防御を活用して、フォーティネット セキュリティ ファブリックとエコシステムを調整します。

高度なツールの提供:フォーティネットは、高度な SOC / NOC ツール、トレーニング、そして諸機能に継続的に投資しており、お客様のチームを成功へと導きます。

業界をリードする認証 / テスト機関により実証されたセキュリティの有効性

シンプル性:アクティベーションまでの時間を短縮することが、デジタルイノベーションのペースを維持する鍵となります。フォーティネットは、選択、導入、利用が容易な高パフォーマンスなセキュリティを提供しています。

運用:組織の多様なユースケースに合わせてセキュリティ機能を組み合わせ、ハードウェア、仮想マシン、およびサービス（as-a-Service）のモデルで任意の製品に追加でき、これらすべてが、シナジー効果を生み出すようにゼロから設計されています。ファブリックマネジメントセンターを活用して、導入環境の統合ビューを提供します。

購入オプション：NGFW、クラウド、メール、エンドポイントなどに合わせて最適化されたバンドルを自由に組み合わせて選択できるだけでなく、EA プログラム（Enterprise Agreement）もご利用いただけます。

市場をリードする連携型のセキュリティ機能で攻撃ライフサイクルと攻撃対象領域を保護

Web セキュリティ

Web ベースの攻撃戦術を監視してデータやアプリケーションを保護し、お客様のコンプライアンスの遵守を支援します。

Web / ビデオ フィルタリング	FortiGuard の Web コンテンツ評価、URL の大規模データベース、および AI を活用した分析環境が、高精度の Web およびビデオフィルタリングサービスを可能にしています。きめ細かいフィルタリングを Web やビデオのカテゴリの許可、ログ、ブロックに適用することで、迅速かつ包括的な保護と法規制のコンプライアンスを可能にします。
DNS	DNS トンネリング、C2 サーバーの識別、ドメイン生成アルゴリズムなどの不正ドメイン攻撃戦術に対する首尾一貫した保護を提供します。
アンチボット / CS	不正コマンドの受け取りや情報の不正取得を目的とする、侵害されたリモートサーバーとの不正通信をブロックします。
地理的 IP 分析	地理的 IP は、IP トラフィックに位置情報を提供して地域ベースの脅威の管理を支援することで、このカテゴリの保護を強化します。
WAF	このサービスとフォーティネットの WAF 製品を併用して、数百のデータタイプや Web ロボットのパターン、脆弱性スキャンシグネチャ、不審 URL などを継続的に自動更新することで、SQL インジェクションやクロスサイトスクリプティングなどのさまざまな攻撃に対する防御が可能になります。

コンテンツセキュリティ

ファイルベースの攻撃戦術を監視、防止し、お客様のコンプライアンスの遵守を支援します。

クラウドサンドボックス

最高レベルの振る舞いベースの AI を活用した静的 / 動的マルウェア分析で、幅広いデジタル攻撃対象領域にわたり、ランサムウェアやクリプトマルウェアをはじめとする急速に進化を遂げている標的型の脅威に対処します。ゼロデイ、高度なマルウェアの検知とレスポンスの自動化によって、実用的なインテリジェンスと防止機能をリアルタイムで提供します。MITRE ATT&CK をベースとするレポート / 調査ツールを利用できます。

アンチウイルス

FortiGuard アンチウイルスは、セキュリティアップデートを自動配信して、最新のポリモーフィック型攻撃コンポーネント、ウイルス、スパイウェア、その他コンテンツレベルの脅威から保護します。業界をリードする高度な脅威検知エンジンを活用するこのサービスは、新たな脅威や進化する脅威によるネットワークやエンドポイント、クラウドへの侵害や重要情報へのアクセスを阻止します。

革新的な機能

モバイルマルウェア、クレデンシャル保護、FortiGuard CDR（コンテンツ無害化）、FortiGuard VOS（ウイルスアウトブレイク防止）、DLP、動的な成人向け画像分析など、このカテゴリにおける機能が追加されます。

アンチスパム

当社のメール製品と連動してペリメーターでスパムの量を劇的に削減し、E メール攻撃 / 感染の優れたコントロールを可能にし、標準的なリアルタイムブラックリストよりも優れた保護を提供します。

デバイスセキュリティ

デバイス / 脆弱性ベースの攻撃戦術を監視、防止し、お客様のコンプライアンスの遵守を支援します。

IPS

IPS は、FortiGuard リサーチの 850 以上のゼロデイディスカバリによってバックアップされており、膨大な数のシグネチャを含む極めて包括的な IPS ライブラリを用いて、ステルス型でネットワークレベルの最新の脅威 / ネットワーク侵入をブロックします。当社のコンテキスト認識ポリシーにネイティブに組み込まれ、攻撃検知メソッドを全面的に制御することで、複雑なセキュリティアプリケーションや回避テクニックに対応します。

OT / IoT

当社の OT サービスにより、きめ細かな可視性と制御のために一般的な ICS / SCADA プロトコルおよび機器を特定して規制し、自動化されたディスカバリ、リアルタイムクエリー、セグメンテーション、そして IoT デバイスのエンフォースメントでお客様の攻撃対象領域を削減します。

デバイス / OS 検知、IoT ハードウェア MAC アドレスベンダーマッピングアップデートなどの追加機能がこのカテゴリの中でさらなる保護を提供します。

一貫性のある連携型のセキュリティ検知とレスポンス

フォーティネット セキュリティ ファブリックには FortiGuard の実用的な脅威インテリジェンスがネイティブ統合されており、コンテンツ、Web、デバイス、ユーザーのセキュリティに関する豊富な機能が継続的に更新されます。

FortiGuard により、統合データベースの AI を活用した分析環境が最新の状態に維持されるため、すべての製品が同一の最新データを利用できます。異なる製品がそれぞれの機能や攻撃プレーンの場所に応じて、関連するすべてのセキュリティテクノロジーにアクセスできるため、一貫性のあるセキュリティが実現します。

ファブリックは一般的な標準とオープン API を採用しているため、既存の投資とフォーティネットの実用的な脅威インテリジェンスを連携させて活用できます。

		セキュリティドリブンネットワーキング		ゼロトラストアクセス	クラウドセキュリティ					ファブリックマネジメントセンター			オープンエコシステム
		FortiGate	FortiProxy	FortiClient	FortiWeb	FortiCASB	FortiADC	FortiMail	FortiDDoS	FortiSandbox	FortiAnallyzer	FortiSIEM	デベロッパーネットワークとオープンエコシステム
コンテンツセキュリティ	アンチウイルス	●	●	●	●	●	●	●		●			
	サンドボックスクラウド	●		●	●			●					
	クレデンシャルディフェンス				●								
	DLP ネイティブ（標準機能）	●	●										
	ウイルスアウトブレイク防止	●						●					
	アンチスパム		●					●					
Web セキュリティ	IP レピュテーション	●			●		●		●	●			
	Web およびビデオフィルタリング	●	●	●			●			●			
	ボットネット DB	●		●	●	●	●						
	地理的 IP	●		●	●								
	DNS	●	●										
	Web アプリケーション				●		●						
デバイスセキュリティ	脆弱性スキャン		●	●	●								
	IPS	●	●	●			●			●			
	IoT の Mac とベンダーのマッピング	●											
	IoT リアルタイムクエリ	●											
	OT の検知と保護	●											
	デバイス / OS 検知	●											
	IOC										●	●	●

脅威リサーチャーから提供されるサービス

SOC / NOC 向けの先進ツール

セキュリティオペレーショナルチーム / ネットワークオペレーショナルチーム
お客様のセキュリティ態勢を絶えず評価し、前進させて、お客様のチームを成功に導きます。

ファブリックレーティング

お客様のセキュリティ態勢を設計、実施し、継続的に前進させるためのガイドを提供します。ファブリックレーティングサービスは監査チェックを提供し、重大な脆弱性や構成の弱点を突き止め、実施するべきベストプラクティスを推奨します。

IOC（Indicators of Compromise: 侵害指標）

ネットワークに対する攻撃、脆弱性、持続型の脅威を継続的に監視する、侵害の自動防御システムです。お客様のデータを守ると同時に、不正アクセス、マルウェア、ブリーチに対する防御機能を提供し、深刻な脅威に対する保護を実現します。

脆弱性スキャン

脆弱性スキャンは、ネットワーク資産のセキュリティの弱点を、オンデマンドまたはスケジュールに基づきスキャンします。重要な資産のセキュリティ態勢に関する包括的レポートを提供し、リモート拠点にある FortiGate の自動スキャンを可能にします。

サービスとしてのSOC（SOC-as-a-Service）

エキスパートからなる当社チームにティア 1 分析を全面的にお任せいただくことで、チームの負担を減らすことができ、その他の重要な業務に集中していただけます。注意すべき重大な事象が発生した際にはお客様に通知し、行動計画を提案します。

購入オプション

以下のオプションから自由に選択し、組み合わせてご利用いただけます。

- アラカルト
- 製品やユースケースに最適なバンドル
- EA プログラム（Enterprise Agreement）

本データシートには、FortiGate 製品ラインの購入オプションとバンドルを記載しています。FortiGuard セキュリティサービスのその他の製品やユースケースでの利用については、各製品のデータシートを参照してください。

製品ラインナップ

	TP	UTP	Enterprise	360	FortiCare のみ
セキュリティアップデート / サービス					
アプリケーション制御	✓	✓	✓	✓	✓
IPS	✓	✓	✓	✓	
アンチウイルス	✓	✓	✓	✓	
ボットネット DB	✓	✓	✓	✓	
モバイルマルウェア	✓	✓	✓	✓	
FortiGate Cloud Sandbox	✓	✓	✓	✓	
アウトブレイク防止	✓	✓	✓	✓	
Web フィルタリング		✓	✓	✓	
セキュア DNS フィルタリング		✓	✓	✓	
ビデオフィルタリング *		✓	✓	✓	
アンチスパム		✓	✓	✓	
IoT クエリサービス			✓	✓	
ファブリックレーティング			✓	✓	
インダストリアルシグネチャサービスレーティング			✓	✓	
SaaS 管理					
FortiManager Cloud				✓	✓
FortiAnalyzer Cloud（すべてのログ）*				✓	✓
FortiCloud SOCaaS *				✓	✓
FortiAnalyzer Cloud の拡張				Cloud add-on	✓
SD-WAN オーケストレーション				✓	✓
SD-WAN 帯域幅テスト				✓	✓
SD-WAN OCVPN				✓	✓
サポート					
ハードウェアのサポート	✓	✓	✓	✓	✓
拡張サポート（24 時間 365 日）	✓	✓	✓	✓	✓
FortiConverter			✓	✓	
優先チケット処理 SLA				✓	
基本アップデートとサービス					
GeoIP のアップデート	✓	✓	✓	✓	✓
デバイス / OS 検知	✓	✓	✓	✓	✓
IoT Mac データベース *	✓	✓	✓	✓	✓
信頼できる証明書データベース	✓	✓	✓	✓	✓
インターネットサービス（SaaS）データベース	✓	✓	✓	✓	✓
DDNS	✓	✓	✓	✓	✓
IPv6 DDNS *	✓	✓	✓	✓	✓
重要なアドオン					
FortiDeploy	アドオン（複数の FortiGate をゼロタッチプロビジョニングするには、対象となる FortiGate の発注書につき 1 つ必要）				
ログと SOCaaS ストレージの拡張	FortiCloud アカウントアドオン				

* FortiOS 7.0 の新機能

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.com/jp/contact

お問い合わせ

OV-FortiGuard-Security-Service-202111-R1