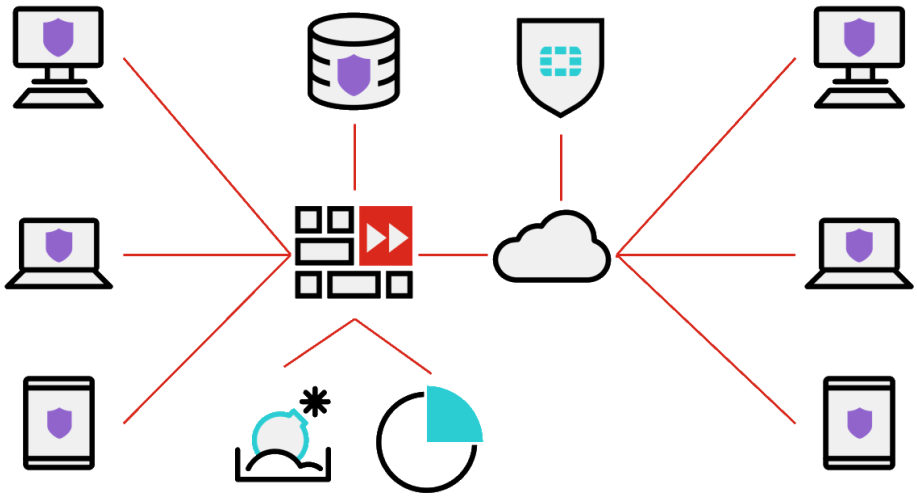
DATA SHEET

FortiClient 7.0

可視性と制御、エンドポイント保護、VPN とゼロトラストテクノロジーを使用したセキュアなリモートアクセスを提供するエンドポイントエージェント



FortiClient が持つフォーティネット セキュリティ ファブリック統合機能により、テレメトリを通じたエンドポイントの可視化を実現します。すべてのセキュリティ ファブリックコンポーネント - FortiGate、FortiAnalyzer、EMS、管理された AP およびスイッチ、FortiSandbox においてエンドポイントの統合ビューが提供され、追跡と認識、コンプライアンスの適用およびレポートが可能になります。従来の仮想プライベートネットワーク（VPN）トンネルや新しい自動化された ZTNA トンネルにより、セキュアなリモート接続が実現します。ローカルまたはリモートのエンドポイントにセキュリティと保護を提供します。

統合エンドポイント向けに統合された、コンプライアンス、保護、セキュアアクセスなどの機能を単一のモジュール型軽量クライアントで利用できます。

ゼロトラストの適用により、アプリケーションへのセッションごとのアクセスを実現する、暗号化された自動トンネルが使用されます。

FortiGuard を活用する FortiSandbox との統合により、エクスプロイトや高度なマルウェアに対する**高度な脅威保護**が実現します。

FortiClient EMS および FortiGate により、**管理およびポリシーの適用が簡素化**されます。

一元管理ツール

- シンプルで使いやすい UI
- FortiClient のリモートインストール
- リアルタイム表示のダッシュボード
- ソフトウェアのインベントリ管理
- Active Directory（AD）との統合
- 隔離の一元管理
- グループ割り当ての自動化
- 動的アクセス制御
- メールアラートの自動送信
- カスタムグループのサポート
- スキャンや隔離のリモート制御
- オンプレミスとクラウドベースのオプション

FortiGuard Security Services
www.fortiguard.com

FortiCare Worldwide Support
support.fortinet.com

メリット

セキュリティ ファブリックとの統合

FortiClient は、エンドポイントをフォーティネットのセキュリティ ファブリックに統合し、高度な脅威を早期に検知して防止します。この統合により、ネイティブでのエンドポイント可視化、コンプライアンス制御、脆弱性管理、自動化を実現します。FortiClient では、FortiOS および FortiAnalyzer が **FortiClient エンドポイントテレメトリのインテリジェンス**を活用して IOC（Indicators of Compromise：侵害指標）を識別します。**自動化機能**によって、管理者はリアルタイムの調査とポリシー設定を実行し、疑わしいエンドポイントや感染したエンドポイントを隔離することでインシデントを封じ込め、脅威の拡散を防止するといったインシデント対応の自動化が可能になります。フォーティネットのエンドポイントのコンプライアンスおよび脆弱性の管理機能によって、エンタープライズセキュリティポリシーの**適用が簡素化**されるため、エンドポイントが容易に攻撃の標的となることを防ぎます。

Web フィルタリングと SaaS 制御

FortiClient は、リモート Web フィルタリングを提供し、Web セキュリティとコンテンツフィルタリングを実現します。Web アプリケーションファイアウォールは、ボットネット対策と、Web ベースのアプリケーションや SaaS（Software-as-a-Service）を含むきめ細かいアプリケーショントラフィック制御を実現します。

ZTNA

FortiClient ZTNA は FortiOS と連携し、ローカルとリモートの両方のユーザーによるアプリケーションへの安全できめ細かいアクセスを可能にします。各セッションは、FortiClient から FortiOS のプロキシポイントへの暗号化された自動トンネルを使用して開始され、ユーザーとデバイスの検証が実行されます。検証されると、そのセッションについてアクセスが許可されます。多要素認証を使用して、さらなるセキュリティレイヤーを追加することもできます。ZTNA によって、より優れたリモートアクセスソリューションが実現するとともに、エンドポイントの場所に関係なく、アプリケーションへのアクセス制御について一貫したポリシーを得ることができます。

エンドポイントの感染予防策

FortiClient は、脆弱性スキャンとオプションのパッチ自動適用により、組織の攻撃対象領域を縮小します。このアプローチとゼロトラストアクセス原則を組み合わせることで、組織の感染予防策とセキュリティ態勢を強化できます。

マルウェアやエクスプロイトの防止

FortiClient は、高度なマルウェアや脆弱性の悪用を防ぐため、FortiClient Cloud Sandbox と統合し、FortiGuard のグローバルな脅威インテリジェンスサービスを活用します。

FortiClient は、FortiClient Cloud Sandbox との統合により、FortiClient エンドポイントにダウンロードされたすべてのファイルをリアルタイムで分析します。FortiClient および FortiSandbox をご利用いただいている世界中の何百万人ものユーザーが、FortiGuard のクラウドベースの脅威インテリジェンスプラットフォームを介して既知および未知のマルウェアに関する情報を共有しています。FortiGuard は、このインテリジェンスを FortiClient エンドポイントと自動的に共有して、新たな脅威から保護しています。

VPN

FortiClient は、VPN 接続の柔軟なオプションを提供します。SSL（Secure Sockets Layer）と IPsec（インターネットプロトコルセキュリティ）の両方の VPN に対応します。スプリットトンネリング機能により、SSL VPN を利用するリモートユーザーは、通常の SSL VPN トンネルのようにトラフィックが企業の VPN ヘッドエンドを通過することなく、インターネットにアクセスできます。この機能により、遅延が低減され、ユーザーエクスペリエンスが向上します。同時に、FortiClient は、インターネットベースのトランザクションが VPN 接続に「逆流」して企業ネットワークを危険にさらさないようにするための保護機能を備えています。

FortiClient は、シンプルなリモート接続に加えて、自動接続や常時接続の VPN、動的 VPN ゲートウェイ選択などの機能により、リモート接続のユーザーエクスペリエンスを向上させます。多要素認証を使用して、さらなるセキュリティレイヤーを追加することもできます。

ランサムウェア対策

ランサムウェア攻撃の最近の増加に対応するため、FortiClient にランサムウェア保護が新たに追加され、不正プログラムによる変更をロールバックしてエンドポイントを感染前の状態に戻す機能を提供します。

サービス

FortiClient マネージドサービス

多忙な IT チームを支援し、作業をオフロードするため、フォーティネットは、FortiClient エージェントの構成、展開、監視を合理化する FortiClient マネージドサービスを提供しています。このマネージドサービスには、以下のサービスが含まれます。

- **FortiClient Cloud の初期プロビジョニング**：マネージドサービスチームがお客様と協力し、FortiClient クラウド環境の以下の機能をセットアップして構成します。
  - エンドポイントグループのセットアップ
  - ZTNA
  - VPN
  - エンドポイントセキュリティ
  - 脆弱性管理
  - セキュリティプロファイルとポリシーの構成
  - エンドポイント態勢チェックルール
  - FortiClient カスタムインストーラーの作成とインストーラーの継続的なアップデート
- **エンドポイントのオンボーディング**：マネージドサービスチームが、お客様のユースケースに合わせた FortiClient インストーラーを作成し、招待メールをユーザーに送信してオンボーディングすることで、FortiClient Cloud で管理し、プロビジョニングできるようにします。
- **セキュリティ ファブリックのセットアップと統合**：マネージドサービスチームが、FortiClient Cloud をフォーティネット セキュリティ ファブリックと統合し、ZTNA、インシデントレスポンス、自動化などのユースケースをサポートできるようにします。
- **エンドポイント脆弱性監視**：マネージドサービスチームが、お客様のエンドポイントを監視して高リスクのエンドポイントを特定し、サイバー攻撃の標的になりやすい深刻度が「クリティカル」や「高」の脆弱性が存在するエンドポイントを警告します。マネージドサービスチームが、これらの脆弱なエンドポイントを検知してレポートし、修復するようにお客様に提案します。

ベストプラクティスサービス（BPS）

FortiClient ベストプラクティスサービスは、導入、アップグレード、運用に関するリモートガイダンスを提供する専門チームへのアクセスを可能にする、アカウントベースの年間サブスクリプションです。このサービスをご利用いただくことで、お客様の導入環境、ユーザー要件、リソースなどの情報の共有が可能になり、提供していただいた情報に基づき、推奨されるベストプラクティス、サンプルコード、ツールへのリンク、その他の資料や支援を BPS のエキスパートが提供することで、迅速な採用を可能にし、ベストプラクティスの導入に向けてお客様を支援します。このサービスを担当するチームがお客様のデバイスにログインしてお客様に代わって何かを変更することはありません。このサービスは、サンプル構成やプレイブックなどのコンサルティングとガイダンスを提供するサービスであり、オンサイトのプロフェッショナルサービスではありません。

主な機能と特長

一元管理ツールにより、Windows、MacOS、Linux、Chrome、iOS および Android のエンドポイントの一元管理機能を提供します。FortiClient EMS がオンプレミス管理を、FortiClient Cloud がクラウドベース管理を提供します。

ソフトウェアのインベントリ管理により、インストールされたソフトウェアアプリケーションおよびライセンス管理が可視化され、セキュリティ対策を強化できます。インベントリ情報を使用し、脆弱性を抱えている可能性のある不要なアプリケーションや古いアプリケーションを検知してアンインストールすることで、攻撃対象領域を削減できます。

Windows AD との統合機能によって、企業組織の AD 構造と一元管理ツールの同期が可能になり、同じ組織単位を AD サーバーから使用できるため、エンドポイント管理が簡素化されます。

リアルタイムでエンドポイントのステータスが表示されるため、エンドポイントの最新アクティビティやセキュリティイベントが常に把握可能です。

脆弱性ダッシュボードでは、企業組織における攻撃対象領域を管理できます。脆弱性のあるエンドポイントを容易に特定し、対策を講じる事が可能です。

FortiClient の一元的な展開とプロビジョニング機能を活用することで、管理者はリモートからエンドポイントソフトウェアを展開し、更新を制御できます。FortiClient の構成をワンクリックで簡単に数千台規模のクライアントに展開できます。

FortiSandbox との統合により、構成や不審なファイルの分析を支援します。サンドボックス設定が管理対象エンドポイント間で同期されるため、セットアップが簡素化されます。FortiClient から送信されたファイルの詳細な分析結果を一元管理ツールで利用できます。管理者は、完全なプロセスツリーをグラフィカルに可視化するなど、ファイルのすべての振る舞いを確認できます。

ネットワーク内のすべてのエンドポイントの認識と制御を実現

テレメトリにより、ユーザーのアバターを含むエンドポイントの状態が FortiGate のコンソールでリアルタイムに可視化されるため、管理者はネットワーク全体の包括的なビューを確認できます。また、テレメトリによりすべてのファブリックコンポーネントにおいてエンドポイントの統合ビューが確実に提供されます。

動的なアクセス制御によってコンプライアンスを適用するためには、エンドポイントのセキュリティ態勢に基づいて EMS が仮想グループを作成する必要があります。続いて、作成された仮想グループの情報を FortiGate が取得し、ファイアウォールポリシーの設定用に利用することで動的なアクセス制御が実現します。グループの動的な作成により、セキュリティポリシーに対するコンプライアンスの自動化と簡素化が可能になります。

エンドポイントの隔離機能では、感染したエンドポイントをネットワークから即座に切断し、他の重要な資産に感染が広がることを防止します。

インシデント対応の自動化によって、手動による設定不要で、疑わしいエンドポイントや感染したエンドポイントを検知し、隔離します。

アプリケーションベースのスプリットトンネルは、アプリケーションベースのスプリットトンネルをサポートし、高帯域幅のアプリなど、VPN トンネルから除外するアプリケーショントラフィックを指定できます。

キーワード検索による Web フィルタリング / YouTube フィルターは、指定した単語やパターンを含む Web ページをブロックするほか、指定した YouTube チャンネルのブロックまたは許可を設定することでユーザーのアクセスを制限します。

バンドル

FortiClient のエディション	ZTNA	EPP / APT	マネージドサービス [3]	Chromebook
ZTNA エージェント	Windows、macOS、Linux	Windows、macOS、Linux	Windows、macOS、Linux	Chromebook
多要素認証（MFA）によるゼロトラストエージェント	✓	✓	✓	
EMS または FortiClient Cloud による一元管理	✓	✓	✓	✓
ログ管理 / レポート機能の一元化	✓	✓	✓	✓
動的セキュリティ ファブリック コネクタ	✓	✓	✓	
脆弱性エージェントと修復	✓	✓	✓	
MFA による SSL VPN	✓	✓	✓	
MFA による IPSec VPN	✓	✓	✓	
FortiGuard Web フィルタリング	✓	✓	✓	✓
FortiSandbox との統合（オンプレミスまたは PaaS）	✓	✓	✓	✓
USB デバイス制御	✓	✓	✓	
次世代エンドポイントセキュリティ				
AI 機能を活用する NGAV		✓	✓	
FortiClient Cloud Sandbox[1]		✓	✓	
エンドポイントの自動隔離		✓	✓	
アプリケーションファイアウォール [1]		✓	✓	
アプリケーションインベントリ		✓	✓	
ランサムウェア対策 [2]		✓	✓	
マネージド FortiClient サービス				
エンドポイントのオンボーディング			✓	
初期プロビジョニング			✓	
セキュリティ ファブリックのセットアップ / 統合			✓	
脆弱性監視			✓	
エンドポイントセキュリティ監視			✓	
その他のサービス				
ベストプラクティスサービス（BPS）コンサルティング	アカウントのアドオン	アカウントのアドオン	—	アカウントのアドオン
FortiCare サポート	✓	✓	✓	✓
オンプレミス / エアギャップオプション	✓	✓		✓

1. FortiClient（Linux）はこの機能をサポートしていません。
2. FortiClient（Windows）のみがこの機能をサポートしています。
3. 日本での提供予定時期は未定。

プラットフォームごとの機能と要件

	Windows	MacOS	Android	iOS	Chromebook	Linux
ZTNA エージェント						
エンドポイントテレメトリ [1]	✓	✓	✓	✓	✓	✓
動的なアクセス制御を使用するコンプライアンスの適用 [1]	✓	✓	✓	✓		✓
脆弱性スキャンによるエンドポイント監査および修復	✓	✓				✓
リモートからのログ管理およびレポート [2]	✓	✓		✓	✓	✓
IPsec VPN	✓	✓	✓			
SSL VPN [3]	✓	✓	✓	✓		✓
ZTNA リモートアクセス	✓	✓				✓
Windows AD SSO エージェント	✓	✓				
USB デバイス制御	✓	✓				✓
エンドポイントセキュリティ						
アンチウイルス	✓	✓				✓
クラウドベースの脅威検知	✓	✓				
サンドボックスの統合（オンプレミス）	✓	✓				✓ [4]
サンドボックスの統合（クラウドベース）	✓	✓				
エンドポイントの自動隔離	✓	✓				
Web フィルタリング [5]	✓	✓	✓	✓	✓	
アンチエクスプロイト	✓					
アプリケーションファイアウォール	✓	✓				

追加機能：FortiSandbox Cloud サブスクリプションを追加して、プロアクティブに高度な脅威保護を実現可能。

1. FortiClient の一元管理には EMS または FortiClient Cloud が必要
2. FortiAnalyzer が必要
3. Windows Mobile との互換性も確保
4. ファイル入力なし
5. Chrome OS との互換性も確保

上記のリストは、各プラットフォームの最新 OS に基づいています。

FortiClient
サポートされるオペレーティングシステム *
Microsoft Windows 7（32 ビット / 64 ビット）
Microsoft Windows 8、8.1（32 ビット / 64 ビット）
Microsoft Windows 10（32 ビット / 64 ビット）
Microsoft Windows Server 2012 以降
macOS 11 以降、10.15、10.14
iOS 9.0 以降
Android 5.0 以降
Linux Ubuntu 16.04 以降、Red Hat 7.4 以降、CentOS 7.4 以降（KDE または GNOME デスクトップ環境）
認証オプション
RADIUS、LDAP、ローカルデータベース、xAuth、TACACS+、デジタル証明書（X509 形式）、FortiToken
接続オプション
Windows ログオン前の VPN 自動接続
FortiClient IPSec VPN トンネル向けの IKE Mode 構成

FortiClient EMS
サポートされるオペレーティングシステム
Microsoft Windows Server 2012 以降
エンドポイント要件
FortiClient 6.4 以降、Windows および macOS X 向け FortiClient、iOS および Android 向け 6.4
システム要件
2.0 GHz 64 ビットプロセッサ、仮想 CPU x 6、8 GB RAM、40 GB のディスク空きスペース、ギガビット（10 / 100 / 1000 BaseT）
Ethernet アダプタ、インターネットアクセス

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