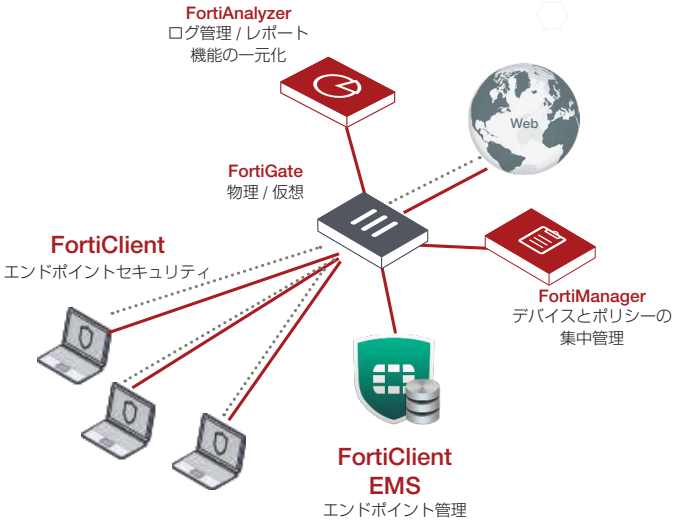
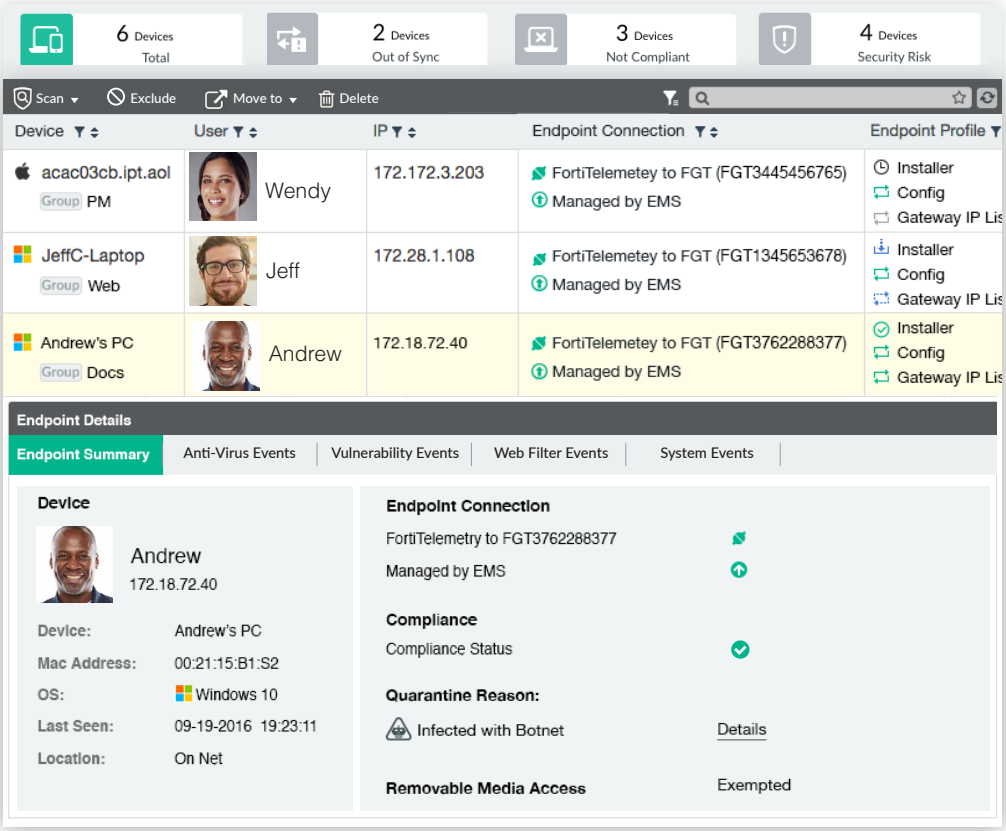
FortiClient

セキュリティ ファブリック上にある、ソフトウェアおよびハードウェアのインベントリを整然と可視化し、制御することができます。すべての攻撃対象領域において、脆弱性のある、あるいは感染したホストを特定し、システムおよびユーザーの詳細なプロファイルをすべて追跡可能です。



FortiClient のセキュリティ ファブリック統合により、すべての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、サンドボックス – 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。FortiClient に組み込まれたホストベースのセキュリティスタックと FortiSandbox との統合によって**高度な脅威保護**が実現し、既知および未知の脅威に対する防御を自動化します。SSL および IPsec VPN 経由の使いやすく**セキュアなリモートアクセスとモビリティ**が実現します。FortiClient は、すべてのエンドポイントを接続して一体型のセキュリティ ファブリックを構築します。



一元管理を実現する EMS

- 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 との統合
- 隔離の一元管理
- グループ割り当ての自動化
- 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

FortiClient のメリット

コンプライアンス、保護、セキュアアクセスなどのエンドポイント機能が、単一のモジュール型軽量クライアントに**統合**されます。

エンドポイントをセキュリティ ファブリック アーキテクチャにネイティブ統合することで、**エンドツーエンド**の脅威の可視化と制御が可能になります。

FortiSandbox と統合された FortiGuard 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。

パッチ管理および脆弱性保護を**統合**し、すべてのエンドポイントを堅牢化します。

Enterprise Management Server（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。

高度な脅威保護

次世代のエンドポイント保護ソリューションである FortiClient によって、エンドポイントは FortiSandbox への接続が可能になります。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は、FortiSandbox による**ビヘイビア（ふるまい）ベースの分析**を使用してリアルタイムで自動的に分析されます。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、クラウドベースの **FortiGuard** 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、それらの FortiSandbox や FortiClient エンドポイントと自動的にインテリジェンスを共有することで、既知または未知のマルウェアからの**攻撃を防止**します。

セキュリティ ファブリック統合

フォーティネット セキュリティ ファブリックの重要な構成要素として、FortiClient はエンドポイントをファブリックに統合し、高度な脅威を早期に検知し防御すると同時に、エンドポイントの可視化、コンプライアンスの制御、脆弱性の管理を実現します。FortiClient 6.0 では、FortiOS および FortiAnalyzer が **FortiClient エンドポイントテレメトリ**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。

セキュアなリモートアクセスとモビリティ

FortiClient は、SSL および IPSec VPN を使用して、事実上すべてのインターネット接続されたリモートからの企業ネットワークやアプリケーションへの**安全かつ信頼性の高いアクセス**を可能にします。また、VPN の**自動接続と Always Up（常時接続）**の機能を内蔵しているため、リモート接続のユーザーエクスペリエンス向上も実現します。さらに、二要素認証もサポートされており、さらなるセキュリティレイヤーが追加され、安全性が強化されます。VPN 自動接続、Always Up（常時接続）、Dynamic VPN Gateway Selection（動的 VPN ゲートウェイ選択）、およびスプリットトンネリングなどの優れた機能により、自宅や公共の場所から接続するあらゆる種類のデバイスで、スムーズなユーザーエクスペリエンスが実現します。

エクスプロイト対策

このビヘイビアベースの検知テクノロジーは、ゼロデイあるいは未修正の脆弱性が存在するアプリケーションを標的とした**ゼロデイ攻撃に対する保護**を可能にします。

未発見や未修正のアプリケーション脆弱性を標的とする**ゼロデイ攻撃から保護**

ヒープスプレー、バッファオーバーフローなどのエクスプロイトで使用される**さまざまなメモリ操作を検知**

PowerShell を使用する、あるいはその他のスクリプト化された攻撃などの**ファイルレスマルウェア攻撃をブロック**

Web ブラウザ、Java / Flash プラグイン、Microsoft Office アプリケーション、PDF リーダーを保護

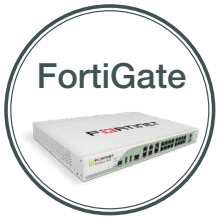
エクスプロイトキットの**識別およびブロック**、ドライブバイダウンロードの阻止

シグネチャ不要のソリューション

主な機能と特長

Windows、Mac、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

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



FortiClient のリモート・インストール

管理者はリモートからエンドポイントソフトウェアの配備および更新の制御が可能になります。

クライアントの一元プロビジョニング機能では、FortiClient の構成をワンクリックで数千台規模のクライアント向けに一括配備することができます。

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、攻撃対象を削減することができます。

Windows AD との統合機能によって、企業組織の AD 構造と EMS の同期が可能となり、同じ OU（組織単位）がエンドポイントの管理に使用できるようになります。

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。

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。

コンプライアンスの適用機能を利用して、企業組織のセキュリティポリシーを適用できます。承認済でポリシーに準拠しているリスクのないエンドポイントのみが、アクセスを許可されます。

エンドポイントの隔離

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

手作業による設定不要で、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。

FortiClient EMS および FortiGate エンドポイントライセンス

	FortiClient EMS ライセンス	FortiGate エンドポイントテレメトリ / コンプライアンスライセンス
プロビジョニング		
クライアントの一元プロビジョニング	✓	
クライアントソフトウェアアップデート	✓	
Windows AD の統合	✓	
FortiTelemetry ゲートウェイ IP リスト	✓	
ソフトウェアインベントリ	✓	
グループ割り当ての自動化	✓	
コンプライアンスの適用とセキュリティ ファブリック統合		
フォーティネット セキュリティ ファブリック統合		✓
セキュリティの状態チェック		✓
脆弱性 / コンプライアンスチェック		✓
最小システムコンプライアンス		✓
未承認デバイスの検知		✓
エンドポイントの自動隔離	✓	✓
リモート制御		
オンデマンドのアンチウイルススキャン	✓	
オンデマンドの脆弱性スキャン	✓	
ホストの隔離	✓	✓
テレメトリおよび監視		
クライアント情報（クライアントのバージョン、OS IP / MAC アドレス、割り当て済プロファイル、ユーザーのアバター）	✓	✓
クライアントのステータス	✓	✓
レポート	✓（FortiAnalzyer へ送信）	✓（FortiAnalzyer へ送信）

追加機能：FNDN で FortiClient カスタムインストールツールを無料で使用可能。リブランディングツールの使用には、FNDN サブスクリプションが必要。

互換性

	WINDOWS	MAC OS X	ANDROID	iOS	ChromeBook	Linux
セキュリティ ファブリック コンポーネント						
エンドポイントテレメトリ [1]	✓	✓	✓	✓	✓	✓
コンプライアンスの実施 [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 [1]	✓	✓				✓
エンドポイントの自動隔離	✓	✓				
ホストセキュリティおよび VPN コンポーネント						
ウイルス対策	✓	✓				✓
エクスプロイト対策	✓					
サンドボックス検知	✓					✓*
Web フィルタリング [2]	✓	✓	✓	✓	✓	
アプリケーションファイアウォール [1]	✓	✓				
IPSec VPN	✓	✓	✓	✓		
SSL VPN [3]	✓	✓	✓	✓		✓
その他						
リモートからのログ管理およびレポート [4]	✓	✓		✓	✓	
Windows AD SSO エージェント	✓	✓				
USB 接続デバイスの制御	✓	✓				✓

追加機能：Windows 向けの高度な脅威保護コンポーネント：FortiSandbox によるファイル分析およびホスト隔離の適用 [1]

[1] EMS による FortiClient の管理が必要 [2] Chrome OS との互換性も確保 [3] Windows Mobile との互換性も確保
上記リストは、各プラットフォーム向けの最新バージョン OS に基づきます。
[4] FortiAnalyzer が必要
* ファイル入力なし

技術仕様

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）
FortiClient 6.0.0 は、Windows XP / Windows Vista をサポートしません
Windows Server 2008 以降
Mac OS X v10.12、v10.11、v10.10、v10.9、v10.8
iOS 5.1 以降（iPhone、iPad、iPod Touch）
Android OS 4.4.4 以降（スマートフォンおよびタブレット）
Linux OS、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 VPN IPSec トンネル向けの IKE Mode 構成

注：すべての技術仕様は FortiClient 6.0 に基づいています。

FortiClient EMS

サポートされるオペレーティングシステム
Microsoft Windows Server 2008 以降

エンドポイント要件
FortiClient バージョン 5.6 以降、Microsoft Windows および Mac OS X 向け FortiClient、iOS および Android 向け 5.4

システム要件
2.0 GHz 64 ビットプロセッサ、デュアルコア（または仮想 CPU x 2）、4 GB RAM、20 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

CERTIFIED

FortiGuard Security Services
www.fortiguard.com

FortiCare Worldwide support
support.fortinet.com

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

Copyright© 2018 Fortinet, Inc. All rights reserved. この文書のいかなる部分も、いかなる方法によっても複製、または電子媒体に複写することを禁じます。この文書に記載されている仕様は、予告なしに変更されることがあります。この文書に含まれている情報の正確性および信頼性には万全を期しておりますが、Fortinet, Inc. は、いかなる利用についても一切の責任を負わないものとします。Fortinet®、FortiGate®、FortiCare®、および FortiGuard® は Fortinet, Inc. の登録商標です。その他記載されているフォーティネット製品はフォーティネットの商標です。その他の製品または社名は各社の商標です。