FortiClient

セキュリティ ファブリック全体で、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。

Security Fabric Integration

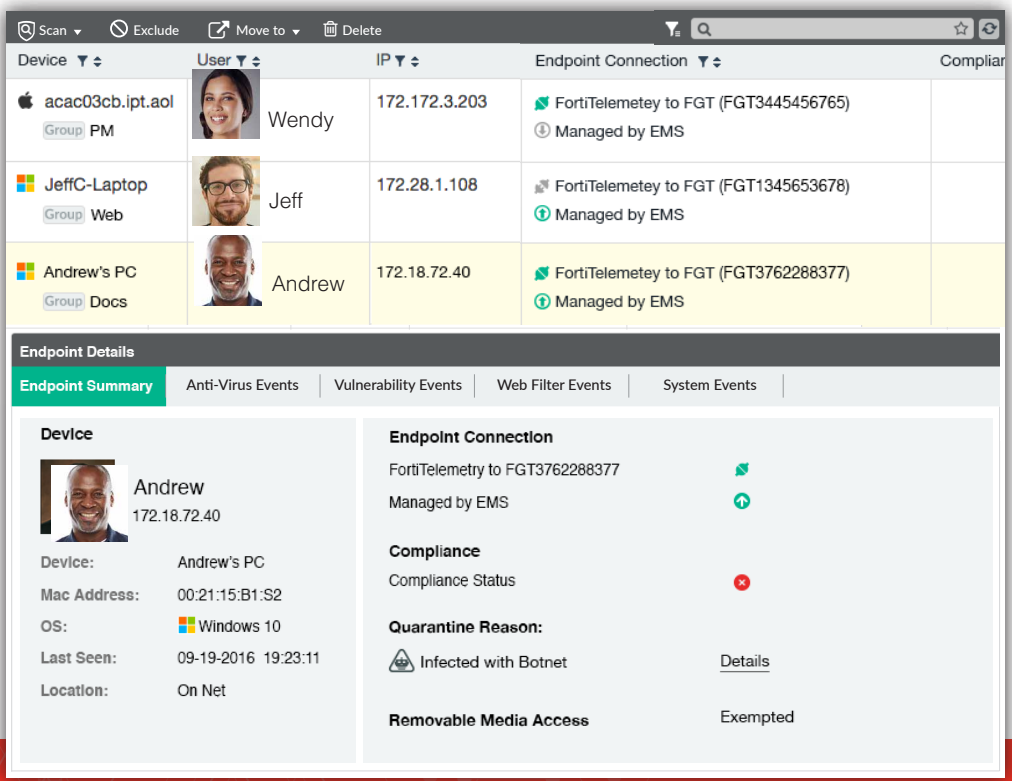
エンドポイントのテレメトリを共有することで、エンドポイントの認識、コンプライアンスおよび適用が可能になります。

高度な脅威からの保護

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、既知および未知の脅威に対する防御を自動化します。

セキュアなリモートアクセスとモビリティ

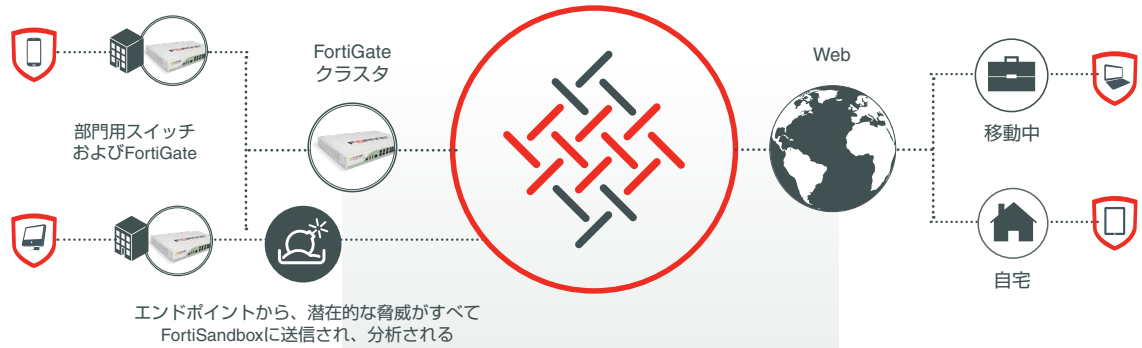
SSL および IPsec VPN 経由の使いやすくセキュアなリモートアクセスが可能です。



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
- Active Directory との統合
- 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 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



高度な脅威からの保護

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、エンドポイントの 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、他の FortiSandbox ユニットや 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。

Security Fabric Integration

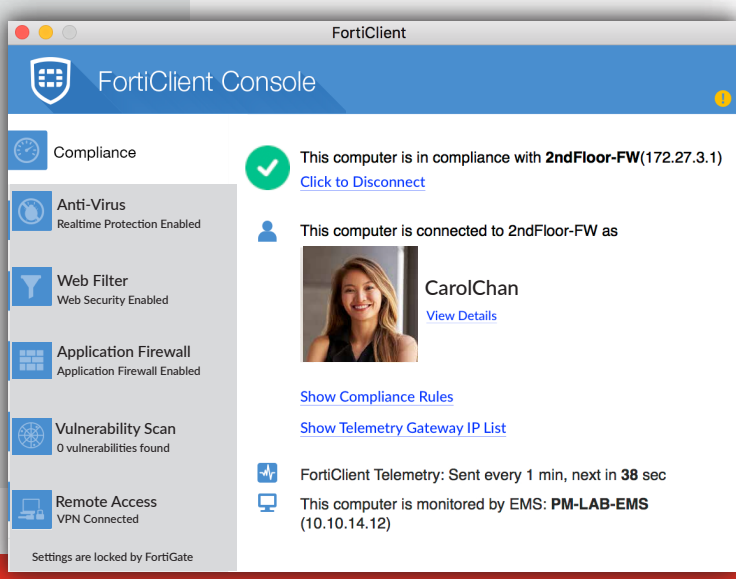
フォーティネット セキュリティ ファブリックの重要な構成要素として、FortiClient はエンドポイントをファブリックに統合し、高度な脅威の早期検知と防御を実現します。ゼロデイマルウェア、ボットネットの検知および脆弱性などのセキュリティイベントは、リアルタイムでレポートされます。ネットワークをリアルタイムで詳細に可視化することで、管理者は感染したエンドポイントを調査して隔離可能になります。フォーティネットのエンドポイントのコンプライアンスおよび脆弱性の検知機能によって、エンタープライズセキュリティポリシーの適用が簡素化されるため、エンドポイントが容易に標的となることはありません。

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の場所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高信頼性の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により、さらなる保護レイヤーが追加されます。従来のウイルス対策のようにシグネチャに頼ることなく、未発見や未修正の脆弱性が存在するアプリケーションを標的とするゼロデイ攻撃からの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
- エクスプロイトで使用されるさまざまなメモリ操作から保護
- Web ブラウザ、Java / Flash プラグイン、Microsoft Office アプリケーション、PDF Reader を保護
- エクスプロイトキットの使用を検知してブロック
- シグネチャ不要のソリューション

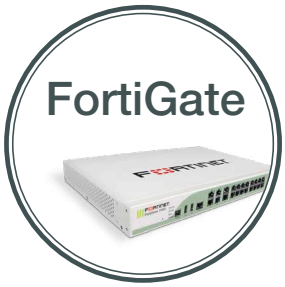


主な機能と特長

Windows、Mac、iOSおよびAndroidのエンドポイントの一元管理機能を提供

- リモートからの FortiClient 配備機能により、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。
- 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の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。
- メールアラートにより、管理者にあらゆるクリティカルなイベントの発生が通知されるため、優先的な対応が可能になります。

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。
- 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。

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 テレメトリライセンス
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	✓	
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		✓
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	✓（FortiAnalyzer へ送信）	✓（FortiAnalyzer へ送信）

追加機能：FortiClient 5.6 以降、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]	✓	✓				
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	✓	✓				

追加機能：Windows 向けの高度な脅威からの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

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 10、8.1、7、Windows Server 2008 R2 および Windows Server 2012、2012 R2、2016
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）

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 5.6 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 2016、2012、2012 R2、2008 R2

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

FORTINET
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