FortiSandbox

未知の脅威に対抗する多層型サンドボックス

今日、サイバー犯罪者たちが従来のマルウェア対策ソリューションを巧妙に回避し、ネットワークの奥深くに持続的で深刻なマルウェアの脅威をもたらすケースがますます増えています。このような巧妙な標的型攻撃では、圧縮、暗号化、ポリモーフィズムをはじめとするさまざまな方法でマルウェアが隠ぺいされており、シグネチャベースの脅威検出機能を巧みに回避します。最近では、バーチャルな「サンドボックス」環境さえも、仮想マシン検出や「時限爆弾」などの手口を使用して回避されるケースも発生しています。今日のこのような攻撃に対抗するためには、単なるマルウェア対策、バーチャル サンドボックス、あるいは独立した監視システムの導入を超える、トータルな統合アプローチが必要不可欠です。

FortiSandboxは、プロアクティブな脅威検出と対策機能を提供するとともに、脅威の本質を把握することで実効性の高い対策を可能にする、堅牢で導入の容易な統合ソリューションです。FortiSandboxの基盤となっているのは、独自の二重構造のサンドボックスです。このサンドボックスは、豊富な実績を誇るフォーティネットのマルウェア対策オプションであるFortiGuardサブスクリプション サービスによって提供される最新の脅威情報によって、完全なセキュリティを実現します。FortiSandboxを導入することで、脅威対策における長年の実績に裏付けられたフォーティネットの専門知識を企業の現場で包括的に活用可能となります。

未知の脅威の検出と対策

不審なコードは、仮想OSで実行される前に多層型のプリフィルタにかけられ、その挙動が詳細に分析されます。実効性の高いこのプリフィルタでは、フォーティネットのAVエンジン、クラウドベースの脅威データベースとの照会、そしてOSから独立したコード エミュレータによるシミュレーションによる緻密なスクリーニングが行われ、その後完全な仮想ランタイム環境で実行し、検証されます。不審なコードが検出されると、検証結果に基づいてマルウェア対策用のシグネチャが作成されると同時に、他の脅威データベースも更新されます。

実効性の高い脅威対策を実施可能

不審な挙動は高中低の各レベルのリスクにすべて分類され、直感的なダッシュボードに表示されます。また、コードを仮想的に実行することで発生するシステムの動作、セキュリティの弱点を突く攻撃、Webトラフィック、ダウンロード、通信などの挙動に関する情報は、すべて詳細なログとレポートで確認することができます。

容易な導入

FortiSandboxは、単体のアプライアンスで数多くのプロトコルの検証をサポートしているため、ネットワーク インフラストラクチャを簡素化し容易に運用することが可能です。さらに、FortiGateと統合することで既存のセキュリティ フレームワークに強力なセキュリティ機能を追加することができます。

未知の脅威に対する対策、
脅威の高度な可視化、
そして総合的な
レポート機能を提供する
究極の統合ソリューション

- **セキュアな仮想ランタイム環境で未知の脅威を事前に発見**
- **独自の多層型プリフィルタを活用し、すばやく効果的に脅威を検出**
- **脅威のライフサイクル全体を完全に可視化する詳細なレポート機能**
- **単体のアプライアンスで数多くのプロトコルを検証可能となり、容易な導入とコスト削減を実現**
- **FortiGateと統合することにより、インフラストラクチャを重複させることなくセキュリティを強化**
- **NSS Lab BDS（ブリーチ検出システム）テストで実証された高度なセキュリティ**

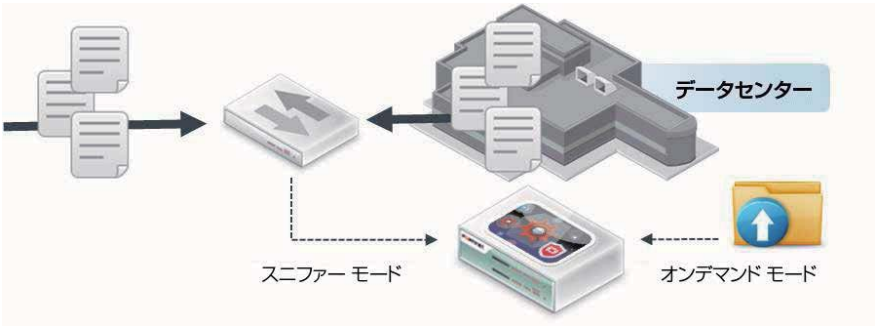
NSS LABS RECOMMEND

導入オプション

FortiSandboxは、市場で最も柔軟性の高い分析アプライアンスで、お客様固有の構成や要件に最適な導入オプションを選択することができます。
さらに、導入企業・組織は3つの検査モードを選択することが可能です。

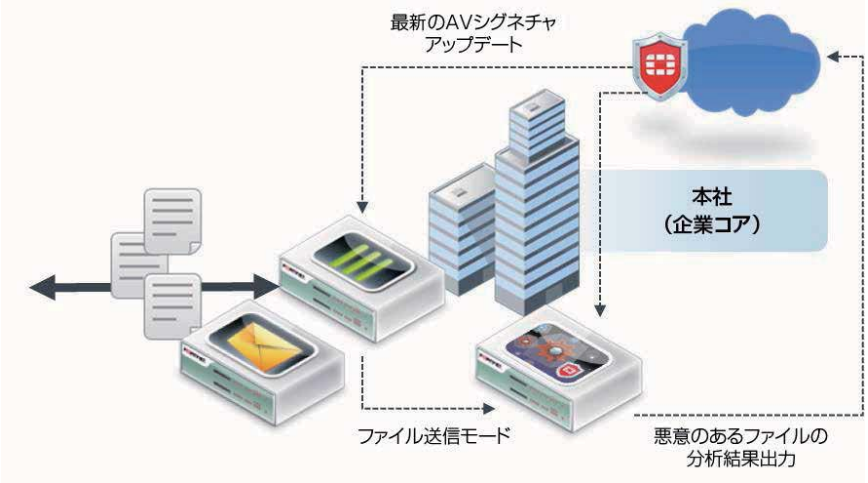
スタンドアロン

この導入オプションでは、ネットワークスイッチのスパン(ミラーリング)ポートからの入力と、管理者がGUIを使用してオンデマンドでアップロードするファイルからの入力が使用できます。また、この導入オプションは、さまざまなベンダーの製品を利用して既に脅威保護システムを導入済のお客様が、保護機能をさらに強化する際に最適な構成です。



*FortiGate/FortiMail との統合

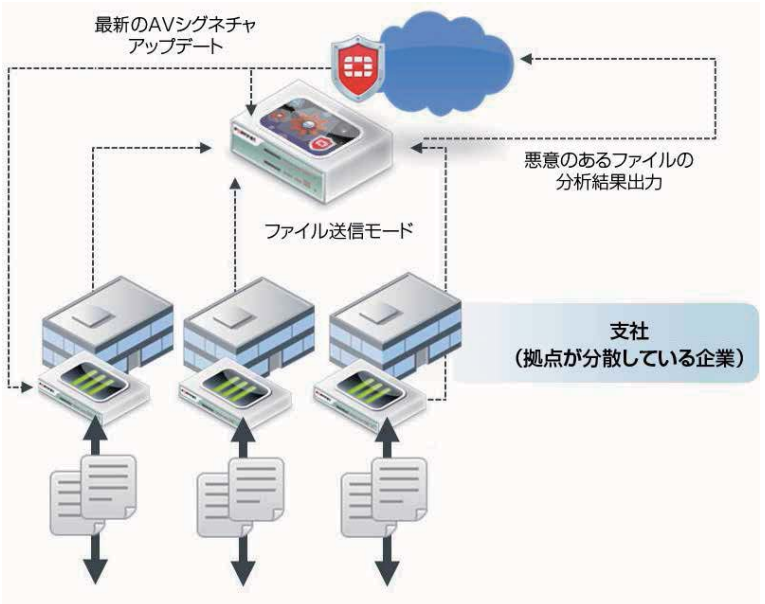
FortiGateをインターネットセキュリティゲートウェイとして活用し、不審なファイルをFortiSandboxに送信するように設定することができます。このシームレスな統合により、シンプルなネットワーク構成が可能となると同時に、HTTPSなどのSSL暗号化プロトコルをはじめとするさまざまなプロトコルや数多くのアプリケーションに対応可能となります。



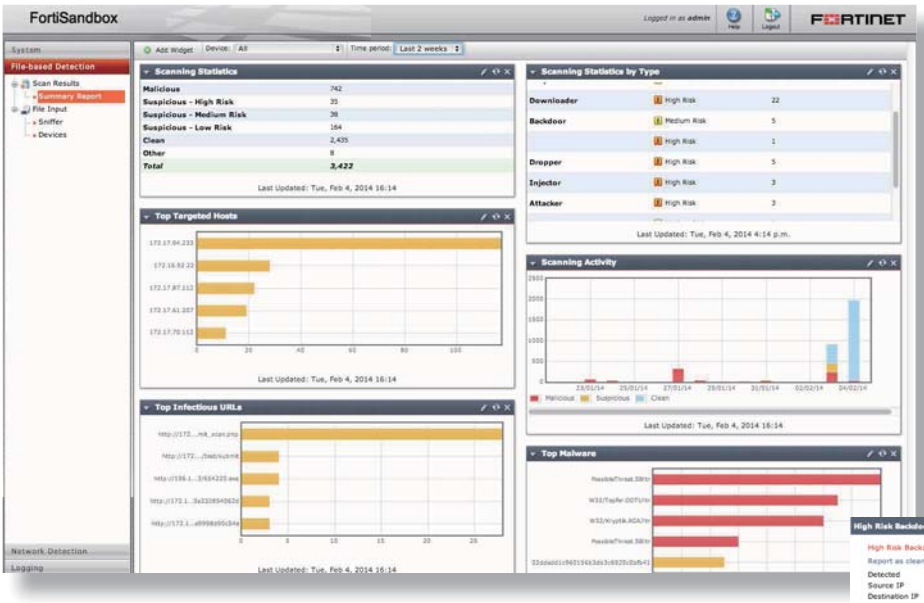
* FortiOS V5.0.4以降、FortiMail V5.1.0以降が必要

分散する FortiGate との統合

この導入オプションは、企業組織の各支社にFortiGateを導入済であり、分散した環境から不審なファイルを送信し、FortiSandboxで一元的に検証を行う場合に最適です。また、この導入オプションでは、TCOを極めて低く抑えるメリットがもたらされると同時に、リモート環境の脅威に対する強力なセキュリティが実現します。



機能

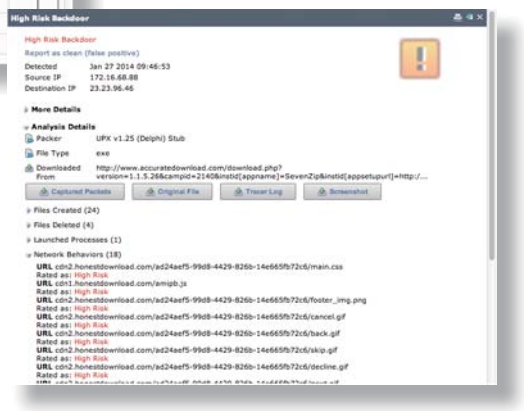


脅威の状態をリアルタイムに可視化するダッシュボード

仮想マシンによるサンドボックス

セキュリティ保護された仮想環境で不審なファイルやリスクの高いファイルを分析する最先端の機能により、システムの動作やコールバックの検出を活用して攻撃のライフサイクル全体を掌握し、すでに導入済の防御対策を補完して完全なセキュリティを実現します。

詳細なファイル分析レポート



ファイル分析ツール

キャプチャしたパケット、オリジナルファイル、トレーサーのログ、スクリーンショットを使用した詳細なレポート機能によって、ファイルの検査後に詳細な脅威情報が提供され、実効性の高い対策を実施できます。これにより、保護対策の迅速な修正や更新が可能になります。

多層的なファイル処理によって効率的なリソースの利用が可能となり、セキュリティ、処理能力およびパフォーマンスを向上

AVエンジン

- トップレベルのAVスキャン（95%以上の検知率、リアクティブ/プロアクティブな脅威検出に対応）を実行します。実効性の高いプリフィルタとして機能します。

クラウド データベースとの照会

- 最新のマルウェア情報をリアルタイムに確認
- 共有情報にアクセスし、瞬時にマルウェアを検出

コードエミュレーション

- 意図された動作をすばやくシミュレート可能
- OSから独立し、仮想マシン回避技術やコードの難読化を検出

完全な仮想サンドボックス

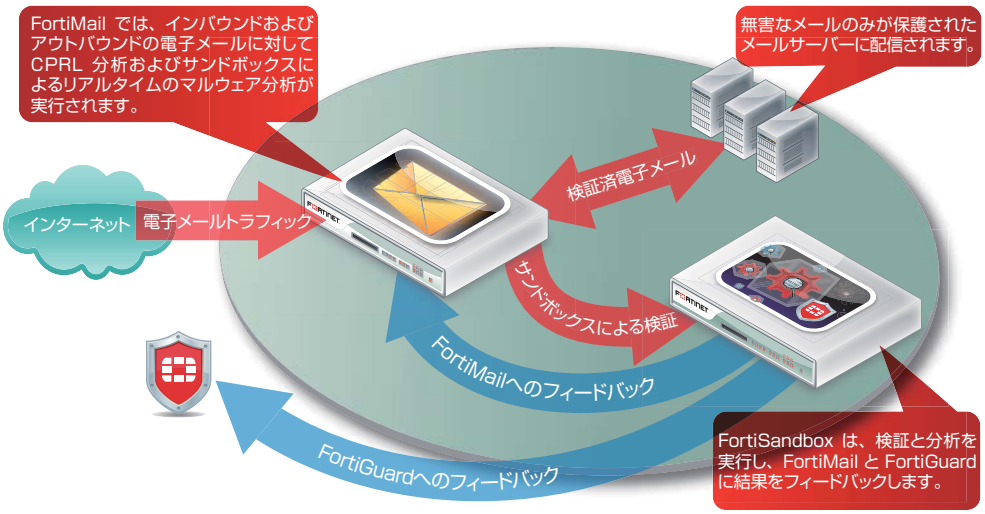
- セキュアなランタイム環境で挙動分析と評価を実行可能
- 脅威のライフサイクル全体の情報を掌握

コールバックの検出

- 脅威の最終目的、コールバック、データ流出を特定

FortiMail との連携による修復

今日では、カスタムマルウェアを仕込んで特定の受信者を標的に電子メールが送信され、ソーシャルエンジニアリングによってユーザーがその電子メールを開くように仕向ける高度な脅威が数多く発生していることから、企業はSEG（Secure Email Gateway）にサンドボックス機能を統合してセキュリティの強化を図る必要があります。具体的には、この統合されたランタイム環境で分析が行われる間SEGは電子メールの配信を保留し、最終的に分析結果に基づいてポリシーを適用します。



FortiMailは不審なメールを保留し、FortiSandboxへ送信します

主な機能と特長

管理

- WebUIおよびCLIによる設定が可能
- 複数の管理者アカウントを作成可能
- 設定ファイルのバックアップとリストア
- 不審なファイルが検出されると電子メールで通知
- 電子メールによるレポート送信
- 一元化された検索ページでは、管理者による検索条件のカスタマイズが可能
- 高頻度なシグネチャの自動更新
- 仮想マシンの状態監視

ネットワーク/導入

- 静的ルーティングのサポート
- ファイル入力方式: オフライン/スニファー モード、オンデマンドのファイル アップロード、統合されたデバイスからのファイル送信
- WebベースのAPIを利用してユーザーがサンプルをアップロードし、間接的にスキャンを実行可能
- 閉じたネットワーク環境でスキャンするサンプルに対して、擬似的にネットワークアクセスをシミュレーションするオプション
- デバイスの統合:
  - ファイル送信方式: FortiGate、FortiMail
  - データベースの更新: FortiManager（V5.0.6以降）
  - リモートログ管理: FortiAnalyzer、Syslog Server

高度な脅威保護

- 仮想OSサンドボックス:
  - 複数Windowsインスタンスの同時処理に対応
  - 侵入対策技術: スリープ状態のコール、プロセスおよびレジストリの照会
  - コールバックの検出: 活性化したマルウェアが実行する不審なURLへのアクセス、ボットネットによるC&Cサーバとの通信、および攻撃トラフィック
  - キャプチャしたパケット、オリジナルファイル、トレーサーのログおよびスクリーンショットのダウンロード
- 検査ファイルサイズは無制限。最大ファイルサイズの設定も可能
- サポートするファイルタイプ:
  - アーカイブ: .tar、.gz、.tar.gz、.tgz、.zip、.bz2、.tar.bz2、.bz、.tar.Z、.cab、.rar、.arj
  - 実行ファイル（.exe、.dllなど）、PDF、Windows OfficeドキュメントおよびJavascript
  - メディアファイル: .avi、.mpeg、.mp3、.mp4
- サポートするプロトコル/アプリケーション:
  - スニファーモード: HTTP、FTP、POP3、IMAP、SMTP、SMB
  - FortiGateとの統合モード: HTTP、SMTP、POP3、IMAP、MAPI、FTP、IMおよびこれらのSSL暗号化バージョン
  - FortiMailとの統合モード: SMTP、POP3、IMAP
- スニファーモードでのネットワーク脅威検知: ボットネットの挙動やネットワーク攻撃、不審なURLへのアクセスの特定
- オプションで不審なファイルをクラウドサービスに自動送信し、アナリストによる分析とシグネチャの作成が可能

監視およびレポート

- リアルタイムの監視用ウィジェット（ソースおよび期間を選択して表示可能）: スキャン結果の統計、スキャン実行情報（経時的）、標的となったホスト上位リスト、検出されたマルウェア上位リスト、感染されているURL上位リスト、コールバック ドメイン上位リスト
- イベントの詳細ビューアー: 挙動、マルウェア名、評価、種類、ソース、送信先、検出時刻およびダウンロード経路を動的にテーブル表示
- ログ – GUIでの表示、RAWログファイルのダウンロード
- 不審なファイルに関するレポート生成: ファイルの特性や挙動に関する詳細レポート – ファイルの変更、プロセスの挙動、レジストリの挙動、ネットワークの挙動、仮想マシンのスナップショット
- 追加的な分析: ファイルのダウンロード – サンプル ファイル、サンドボックス トレーサーのログおよびPCAPキャプチャ

技術仕様

	FortiSandbox-1000D	FortiSandbox-3000D
ハードウェア仕様		
形状	2 RU	2 RU
ネットワーク インタフェース	6x GbE RJ45 インタフェース、2x GbE SFP インタフェース	4x GbE RJ45 インタフェース、2x GbE SFP インタフェース、2x 10 GbE SFP+ インタフェース
内蔵ストレージ	4 TB(最大 8 TB)	8 TB(最大 16 TB)
冗長電源	○	○
システム性能		
VMのサンドボックス処理(ファイル数/時)	160	560
AVスキャン処理(ファイル数/時)	6,000	15,000
VM数	8	28
サイズ		
高さ x 幅 x 奥行	89 x 437 x 368 mm	84 x 482 x 755 mm
重量	12.52 kg	32.5 kg

	FortiSandbox-1000D	FortiSandbox-3000D
動作環境		
消費電力(平均 / 最大)	115 / 138 W	392 / 614.6 W
電流(最大)	100 V / 5 A、240 V / 3 A	110 V / 10 A、220 V / 5 A
放熱	471 BTU/h	2131.14 BTU/h
電源	100 - 240 VAC、60 / 50 Hz	100 - 240 VAC、60 / 50 Hz
湿度	5 ～ 95%(結露しないこと)	20 ～ 90%(結露しないこと)
動作温度	0 ～ 40℃	10 ～ 35℃
保管温度	-25 ～ 70℃	-40 ～ 65℃
準拠規格		
規格・認定	FCC Part 15 Class A、C-Tick、VCCI、CE、BSMI、KC、UL/cUL、CB、GOST	

	FSA-VM
システム要件	
ハイパーバイザーのサポート	VMware ESXiバージョン5.0またはそれ以降
仮想CPU数(最小 / 最大)	4 / 無制限 (仮想CPU数をWindows VM数 + 4と一致させることを推奨します)
仮想メモリ容量(最小 / 最大)	8 GB / 無制限
仮想ストレージ容量(最小 / 最大)	30 GB / 16 TB
仮想ネットワーク インタフェース(最小)	6
システム性能	
VMのサンドボックス処理(ファイル数/時)	システム構成に依存
AVスキャン処理(ファイル数/時)	システム構成に依存
VM数	2 ～ 52(適切なライセンスの購入によるアップグレードが必要)

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 7-18-18
住友不動産六本木通ビル 8 階
www.fortinet.co.jp/contact

お問い合わせ

DS-FSA-DAT-R4-201411-R1