Fortinet Master Distributor

ソリューション名	FortiSandbox

SCSK
夢ある未来を、共に創る。

SCSKと実現する統合型セキュリティ対策

FortiSandbox

巧妙化する標的型攻撃、未知マルウェアへの脅威からの確実な防御

FortiSandbox 特徴

AIを活用した分析アプローチ

- 機械学習を活用してゼロデイ脅威の検出効率を飛躍的にアップ
- マルウェアの手法を継続的に学習し、マルウェアの挙動指標を自動的に更新
  - 静的分析：既知および新たなマルウェアを迅速に特定
  - 動的分析：振る舞い分析をベースに攻撃のライフサイクル全体を表面化

MITRE ATT&CK ベースのレポート、調査ツール

- 発見されたマルウェアはMITER ATT＆CKフレームワークにマッピングされ、詳細な分析レポートを提供
- セキュリティオペレーションチームはキャプチャしたパケット、トレーサーのログ、マルウェアのスクリーンショットなどをダウンロードし、対策へ利用可能

提供形態：

アプライアンス
FortiSandbox 500F
FortiSandbox 3000F 等

仮想マシン
FortiSandbox-VM

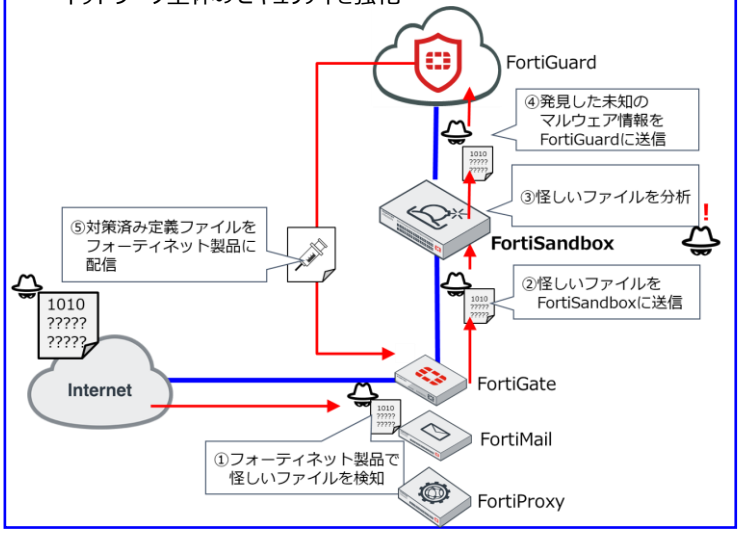
PaaS
FortiSandbox Cloud

SaaS
FortiGate Cloud Sandbox
FortiMail Cloud FortiSandbox 等

導入構成

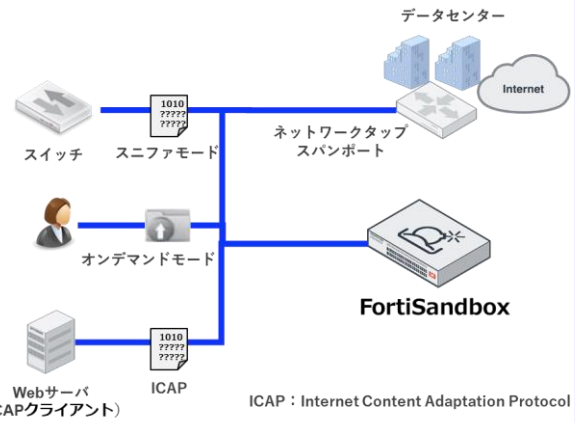
フォーティネット製品との統合

- 次世代ファイアウォールからメールセキュリティなどのフォーティネット製品が怪しいファイルを検知し、その怪しいファイルをFortiSandbox に送信
- FortiSandboxまでをフォーティネット製品で連携させ、ネットワーク全体のセキュリティを強化



スタンドアロン

- ICAPサーバーとして、あるいはネットワークスイッチのスパン（ミラーリング）ポートの入力が使用可能
- 管理者がGUIを使用してオンデマンドでファイルをアップロードすることも可能



記載されている団体名および製品名は、各社の商標または登録商標です。 Copyright © SCSK Corporation