FXシリーズ

ファイル共有やコンテンツ・ストアに潜むマルウェアを検知、駆除するコンテンツ脅威対策プラットフォーム

データシート

ハイライト

- 従来型のアンチウイルス・エンジンでは対応できない潜伏型のマルウェアを検知
- 隔離を行う防御モードと解析のみのモニター・モードに対応
- CIFSおよびNFS互換のファイル共有で再帰検査、定期検査、オンデマンド検査を実施
- WebDAVプロトコルを活用してSharePointをプロアクティブに保護
- PDFやMicrosoft Office文書、マルチメディア・ファイルなど多様なファイル形式の解析に対応
- AV-Suiteの統合によりインシデント・レスポンスの優先順位を効率よく判断し、マルウェアの命名規則に準拠
- FireEye CMおよびFireEye DTIクラウドを介して、別のFireEyeプラットフォームと脅威情報を共有

FX 5400およびFX 8400

概要

FireEye® FXシリーズは、さまざまな形式のファイルを利用した攻撃からコンテンツを保護するための脅威対策プラットフォームです。Webメールやオンラインのファイル転送サービス、クラウド、携帯型のストレージ機器は、ファイル共有やコンテンツ・リポジトリで広まるマルウェアの感染源になるおそれがあります。FireEye FXプラットフォームは、ネットワーク・ファイル共有やエンタープライズ・コンテンツ管理ストアを検査することにより、社員によって持ち込まれたマルウェアや、次世代型のファイアウォール、IPS、アンチウイルス、セキュリティ・ゲートウェイをすり抜けて侵入したマルウェアを検知して隔離します。

ファイル共有に潜むマルウェアが引き起こす問題

今日の高度なサイバー攻撃は、高機能なマルウェアとAPT攻撃（Advanced Persistent Threat：高度で持続的な標的型攻撃）と呼ばれる手法を用いてセキュリティ対策をすり抜け、ファイル共有やコンテンツ・リポジトリ内で感染を広げます。これによってマルウェアは、ネットワーク内に確固たる足がかりを築き、インターネットに接続していないシステムを含め、複数のシステムに感染を拡大します。このようなコンテンツベースのマルウェアに対して特に脆弱なのが企業のデータセンターです。従来型のセキュリティ対策は、このタイプのマルウェアを効果的に検知できず、ごく単純な方法で侵入を試みるマルウェアさえ見逃してしまうことがあります。サイバー攻撃者は、この弱点を突いてネットワーク・ファイル共有にマルウェアを侵入させ、多数のファイルに不正なコードを埋め込みます。その結果、一部のファイルだけを修復しても繰り返し被害が発生します。

高度なサイバー攻撃のライフサイクル阻止に欠かせないファイルの保護

APTによるネットワーク資産の侵害を防ぎ、機密情報の漏洩やそれに伴う深刻な被害の発生を防止するためには、ファイルに潜むマルウェアを検知する必要があります。FireEye FXシリーズは、特許技術のFireEye Multi-Vector Virtual Execution™（MVX）エンジンを使用してファイル共有やエンタープライズ・コンテンツ・リポジトリを検査し、PDF、Microsoft Office、vCard、ZIP/RAR/TNEFなどの広く使用されているファイル形式や、QuickTime、MP3、Real Player、JPG、PNGなどのマルチメディア・コンテンツに埋め込まれた未知の不正なコードを見つけ出します。アクセス可能なネットワーク・ファイル共有やコンテンツ・ストアに対して再帰検査、定期検査、オンデマンド検査を実施することにより、内部に潜むマルウェアを検知して隔離し、高度なサイバー攻撃を構成するライフサイクルの早い段階で攻撃を阻止します。

未知の脅威を見つけ出すFireEyeのMVXエンジン

FireEye FXシリーズは、未知の脅威の検知を目的とした専用技術であるFireEyeのMVXエンジンを使用して各ファイルを検査し、ゼロデイ・エクスプロイトなどの不正なコードが埋め込まれていないかどうかを確認します。FireEye MVXエンジンは、仮想環境の多様なWebブラウザ、プラグイン、アプリケーション、オペレーティング・システムでファイルを実行し、不正な活動の有無を確認します。

SharePointのコンテンツのプロアクティブな検査と隔離

FireEye FXシリーズは、SharePointリポジトリ内のコンテンツを継続的に検査し、マルウェアを確認した時点でアラートを発して永久的に隔離します。このプラットフォームはWebDAVプロトコルを活用してSharePointサービスと安全に統合し、SharePointリポジトリを活用する企業のビジネス・ワークフローを維持します。

YARAベースのルールでカスタマイズに対応

カスタムYARAルールをサポートするFireEyeFXシリーズは、独自のルールで大量のファイルを解析し、特定の組織を狙った脅威を見つけ出すことができます。

インシデント・レスポンスの優先順位を効率よく判断

FireEye AV-Suiteを使用すると、FireEye FXプラットフォームがブロックしたマルウェアをアンチウイルス・ベンダーの製品で検知できるかどうかを詳しく解析できます。これにより、インシデント・レスポンスの優先順位を効率よく判断し、既知のマルウェアの一般的な命名規則に準拠できます。

マルウェア情報の共有

FireEye CMプラットフォームを導入している場合、ダイナミックに生成されたリアルタイムの脅威情報をすべてのFireEye製品で共有し、ローカル・ネットワークの保護に利用できます。脅威情報は、FireEye Dynamic Threat Intelligence™ (DTI) クラウドを介して世界規模で共有され、同クラウドに参加するすべてのFireEyeプラットフォームに新しい脅威の情報が行き渡ります。

ルールのチューニングは不要、誤検知もほぼゼロ

FireEye FXシリーズの導入は、チューニングを行うことなくわずか1時間ほどで完了し、クライアント・アプリケーションを介さず容易に管理できます。また環境固有の要件に応じて、解析のみのモニター・モードと隔離を行う防御モードの2種類のモードを柔軟に選択可能です。このため、ファイル共有に潜むマルウェアの調査、またそのマルウェアの感染拡大を直ちに防ぐこともできます。

技術仕様

	FX 5400	FX 8400
パフォーマンス*	最大8万ファイル/日	最大16万ファイル/日
ネットワーク・インタフェース・ポート	10/100/1000BASE-Tポート x 2	10/100/1000BASE-Tポート x 2
IPMIポート (背面パネル)	搭載	搭載
前面パネルLCDおよびキーパッド	搭載	搭載
PS/2キーボードおよびマウス、DB15 VGAポート (背面パネル)	搭載	搭載
USBポート (背面パネル)	Type A USB 2ポート	Type A USB 2ポート
シリアル・ポート (背面パネル)	115,200 bps、パリティなし、8ビット、1ストップ・ビット	115,200 bps、パリティなし、8ビット、1ストップ・ビット
ストレージ容量	600 GB HDD 2台、RAID 1、2.5インチ、フィールド交換対応	600 GB HDD 2台、RAID 1、2.5インチ、フィールド交換対応
エンクロージャ	1RU、19インチ・ラックに適合	2RU、19インチ・ラックに適合
シャーシの寸法 (幅×奥行×高さ)	437×706×43.2 mm	437×711×86.6 mm
AC電源	冗長 (1+1) 750ワット、100～240 VAC、9-4.5 A、50-60 Hz、IEC60320-C14インレット、フィールド交換対応	冗長 (1+1) 750ワット、100～240 VAC、9-4.5 A、50-60 Hz、IEC60320-C14インレット、フィールド交換対応
DC電源	非搭載	非搭載
消費電力 (最大) (ワット)	463W	506W
熱放散 (最大) (BTU/時)	1,580 BTU/時	1,726 BTU/時
平均故障間隔 (時)	40,700時間	68,900時間
重量 (アプライアンスのみ/梱包時)	15 kg / 21 kg	19 kg / 26 kg
安全性に関する適合規格	IEC 60950、EN 60950、CSA 60950-00、CE Marking	IEC 60950、EN 60950、CSA 60950-00、CE Marking
EMC/EMIの適合規格	FCC (Part 15 Class-A) 、CE (Class-A) 、CNS、AS/NZS、VCCI (Class A)	FCC (Part 15 Class-A) 、CE (Class-A) 、CNS、AS/NZS、VCCI (Class A)
セキュリティ認定	CC NDPP v1.1	CC NDPP v1.1
規制への対応	RoHS、REACH、WEEE	RoHS、REACH、WEEE
温度 (動作時)	10° C～35° C	10° C～35° C
相対湿度 (動作時)	10%～85% (結露なきこと)	10%～85% (結露なきこと)
動作高度	1,500 m	1,500 m

注 : パフォーマンス値は、システム構成や処理するトラフィックの特性によって異なります。記載のパフォーマンスは、一般的な環境におけるファイル数に基づいています。

詳細はこちら

FireEyeは包括的なサービス・ポートフォリオを提供しています。詳細については、japan@FireEye.com、または(03) 4577-4401までお問い合わせください。

Accumuli Securityには、info@accumuli.com、または+44 (0) 1256 303 700からお問い合わせください。

FireEyeを選ぶ理由

専門知識、テクノロジー、インテリジェンス

FireEyeが提供する製品やサービスは、高度な専門知識とテクノロジー、そして業界随一の精度を誇るインテリジェンスに基づいています。FireEyeのセキュリティ専門家は、お客様と協力しながら組織固有の課題を把握し、現場経験豊富な一線級のエキスパートの手によって迅速に問題を解決します。また、脅威対策プラットフォームを活用することにより、APT攻撃や標的型攻撃、サイバー犯罪についての独自情報を収集し、各業種を狙う攻撃者の最新動向を把握しています。FireEyeは、今日のセキュリティ脅威からビジネスを保護するために必要な専門知識とインテリジェンスを提供します。

ファイア・アイ株式会社 | 〒101-0054 東京都千代田区神田錦町3-22 テラススクエア8階 | TEL: 03-4577-4401 | japan@fireeye.com | www.FireEye.jp
FireEye, Inc. | 1440 McCarthy Blvd. Milpitas, CA 95035 | +1 408 321 6300 | 877.FIREEYE (347.3393) | info@fireeye.com | www.FireEye.com