データシート

FireEye SmartVisionエディション

企業ネットワーク内の疑わしい横展開移動を検知

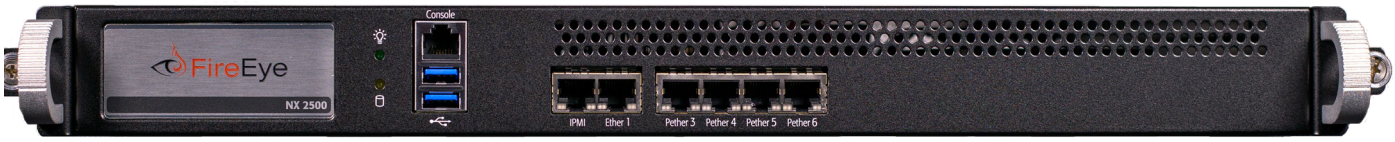

図1:NX 2500 SmartVisionハードウェア

メリット

- 従来は検知できなかったネットワーク内を移動する疑わしいトラフィックを検知
- 侵害後の活動を検知する時間を短縮
- ネットワーク全体を柔軟に拡張
- ネットワーク・セグメンテーションを可視化
- ネットワーク・フォレンジックとインシデント対応を改善
- 攻撃者のネットワーク滞在時間を削減

FireEyeSmartVisionエディションは、企業ネットワーク内を動き回る疑わしいトラフィックを検知するネットワーク・トラフィック解析（NTA）ソリューションです。内部への悪意のある攻撃を防御するために境界に配置される競合他社のネットワーク・セキュリティ・ソリューションとは異なり、FireEye SmartVisionエディションは、コア、ネットワーク・セグメント間、および主要なサーバー資産の直前など、ネットワーク全体に導入でき、不正な内部トラフィックを検知します。

FireEyeSmartVisionエディションを導入することで、セキュリティ・アナリストと管理者は、ファイアウォールやセキュリティ・ゲートウェイなどで見逃されていた、ネットワークを動き回る疑わしいトラフィックについて、新しい知見を得て可視化できるようになります。導入が容易で、FireEyeの業界最先端のCloud MVX™テクノロジーと連動する軽量のセンサーを使用することで、データセンターから遠隔地の支社に至るネットワーク全体にSmartVision エディションの可視化を拡大できます。

SmartVisionエディションのコア機能は、高度な相関分析および解析エンジンと、外部へのデータ送信の 試みを検知する機械学習モジュールを含む優れた脅威検知ソフトウェアであり、些細なセキュリティ侵害の証拠や痕跡を見つけ出す120以上の侵入検知ルールによって強化されています。

SMARTVISIONエディションのコンポーネント

SmartVisionエディションを使用するには次の3つのコンポーネントが必要です。

- 最小構成で1つ以上のSmartVisionセンサー（ハードウェアまたは仮想）
- FireEye MVXエンジンへの接続（オンプレミス、Smart Grid、またはCloud MVX*経由）
- FireEye OSリリース8.1.2以降（SmartVisionがアクティブ化されていること）

表1：SmartVisionエディションの機能

機能	説明
ネットワーク内を動き回る疑わしいトラフィックを検知	高度な相関分析および解析エンジンと、機械学習モジュールおよび120以上の独自のルールとを組み合わせて、ネットワークを動き回るステルス型の横展開（east-west）トラフィックを検知します
SMB/SMB2プロトコルを経由するオブジェクトを取り除く	FireEye MVXテクノロジーを使用して、WannaCryなどのマルウェアやランサムウェアだけでなく、疑わしいファイルや、SMBプロトコルを経由して内部を動き回るオブジェクトを取り除きます
アラートを可視化して、イベントのトリアージを迅速に実施	10分（誤差、前後5分）のL4およびL7のアラート・コンテキストを提供して、攻撃者の活動を迅速に調査して、フォレンジック分析を行います
幅広いメタデータ・プロトコルをサポート	以下のプロトコルを含む包括的な分析に必要なメタデータを生成します。FTP、HTTP、IMAC、IRC、POP3、RDP、RTSP、SMB、SMB 2、SMTP、SSH、TLS
既存のFireEyeネットワーク・セキュリティ導入環境を補完	第4世代および第5世代のネットワーク・セキュリティ・アプライアンスを導入されているFireEyeのお客様は、SmartVisionエディションを既存のインフラに容易に統合して、投資対効果をさらに高めることができます
FireEye Helixと統合	チーム間の連携に必要な、追加の脅威情報コンテキストと統合アラート・トリアージを提供します

FireEye SmartVisionエディションを導入すると、ネットワーク内を動き回る攻撃サイクル全体にわたって固有の攻撃活動が特定され、侵害後の滞在時間と情報漏えいリスクが減少します。

横展開移動を伴う攻撃ライフサイクルの8つのフェーズ

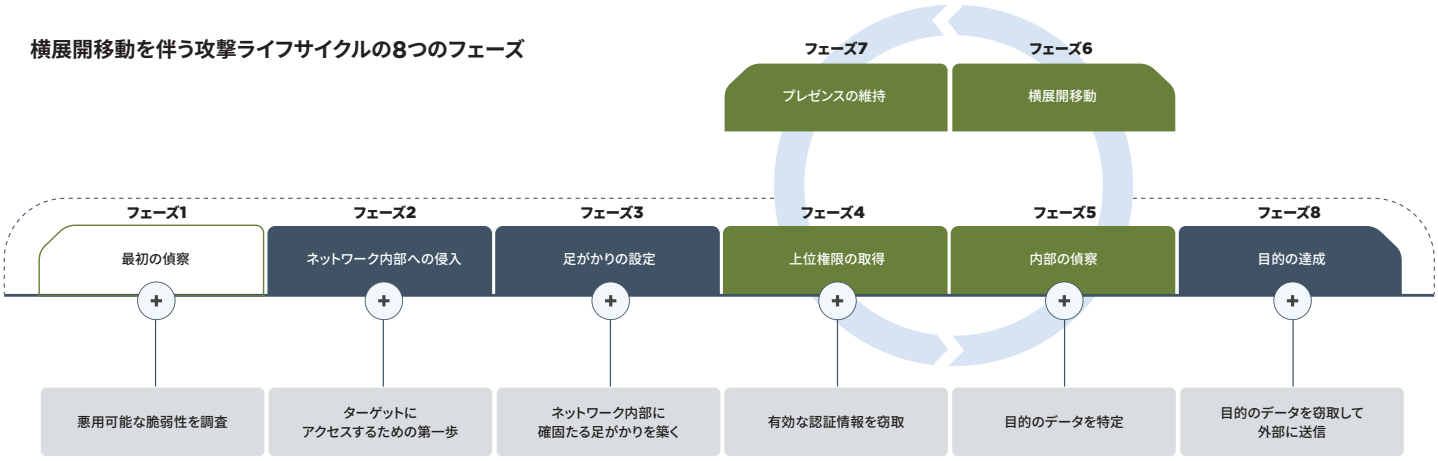

表2：SmartVisionエディションの仕様（ハードウェア・モデル別）		
モデル	SV-2500-HW	SV-5500-HW
センサー・モードでのパフォーマンス**	最大250 Mbps	最大5 Gbps
統合モードまたはハイブリッド・モードでのパフォーマンス**	最大100 Mbps	最大2.5 Gbps
ネットワーク・モニター・ポート	10/100/1000 BASE-T 4ポート	10GigE SFP+ 8ポート、1GigEバイパス 4ポート
管理ポート	10/100/1000 BASE-T 2ポート（前面パネル）	10/100/1000 BASE-T 2ポート
ストレージ容量	1 TB 3.5インチSATA HDD 1台、内蔵、固定	4TB HDD 2台、3.5インチ、SAS3、7.2krpm、フィールド交換対応、RAID1
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× 500× 3.2 mm	438× 620× 88.4 mm
AC電源	250W 1台、90～264 VAC、3.5-1.5 A、50-60 Hz、IEC60320-C14インレット、内蔵、固定	冗長電源（1+1）800W、100～240 VAC、10.5-4.0 A、50-60 Hz、IEC60320-C14インレット、フィールド交換対応
消費電力（最大）	85W	658W
重量（アプライアンスのみ/梱包時）	7.3 kg 12.8 kg	19.2 kg 29.0 kg
温度（動作時）	0°C～40°C 32°F～104°F	0°C～35°C 32°F～95°F
温度（非動作時）	-20°C～80°C -4°F～176°F	-40°C～70°C -40°F～158°F
メタデータ・プロトコルをサポート	FTP、HTTP、IMAC、IRC、POP3、RDP、RTSP、SMB、SMB 2、SMTP、SSH、TLS	FTP、HTTP、IMAC、IRC、POP3、RDP、RTSP、SMB、SMB 2、SMTP、SSH、TLS

表3：SmartVisionエディションの仕様（仮想モデル別）		
モデル	2550v	6500v
パフォーマンス**	最大250 Mbps	最大1 Gbps
ネットワーク・モニター・ポート	1～8	1～8
管理ポート	1または2	1または2
CPUのコア数	6	16
メモリ	16 GB	64 GB
ディスク容量	384 GB	512 GB
サポートするハイパーバイザ	VMware ESXi 6.0以降	VMware ESXi 6.0以降
メタデータ・プロトコルをサポート	FTP、HTTP、IMAC、IRC、POP3、RDP、RTSP、SMB、SMB 2、SMTP、SSH、TLS	FTP、HTTP、IMAC、IRC、POP3、RDP、RTSP、SMB、SMB 2、SMTP、SSH、TLS

* Cloud MVXは、既知および未知の脅威を簡単にリアルタイムで検知して取り除くように設計されています。Cloud MVXは、一般的なクラウドベースのサンドボックスとは異なり、ファイル形式とオブジェクトを分析するだけではなく、ネットワーク・トラフィックを再生して、複数のネットワーク・フローにわたる攻撃を特定します。

** パフォーマンスの数値は、個々のネットワーク条件によって異なります。

FireEyeの詳細については、**www.FireEye.jp**をご覧ください。

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 | 03－4577－4401 |
Japan@fireeye.com

© 2018 FireEye, Inc. All rights reserved. FireEyeはFireEye, Inc.の登録商標です。本資料のその他のブランド名、製品またはサービス名はそれぞれその所有者の商標またはサービスマークとして登録されている場合があります。**DS.SVE.JA-JP-042018**

会社概要
FireEyeは、インテリジェンス主導型のセキュリティ企業です。顧客企業は、FireEyeの革新的セキュリティ技術、国家レベルの脅威インテリジェンス、世界的に著名なMandiant®コンサルティングの知見が統合された単一プラットフォームを、自社のセキュリティ対策の一部としてシームレスに組み込むことができます。このアプローチにより、FireEyeは準備、防御、インシデント対応といった、組織がサイバー攻撃対策をするうえでの課題となっていた複雑性や負担を解消します。FireEyeは「Forbes Global 2000」企業の45%以上を含む、世界67か国以上の6,600を超える組織で利用されています。