DATA SHEET

FortiDeceptor

FortiDeceptorは、従来型のセキュリティ制御を回避してネットワークに侵入した悪意のあるアクティビティを可視化し、キルチェーンを分断してマルウェアの活動を停止させることで、高度な攻撃を欺いて顕在化させ、排除します。ディセプションVM、あるいはデコイ（decoy：おとり）となる内部の保護レイヤーを自動的に作成し、ネットワークに侵入した攻撃者を誘導して活動を停止させます。

フォーティネット セキュリティ ファブリックは、フォーティネットのエンタープライズファイアウォールを活用する包括的なエンドツーエンドの保護機能によって、高度な持続的脅威に対抗します。FortiDeceptorを侵害防止システムとして追加することで、脅威を欺き誘い出すディセプションベースの検知機能、そして実用的で自動化された強力なセキュリティアラート情報が提供され、防御の範囲がさらに拡張されます。FortiDeceptorでは、ディセプションVMとデコイ（おとり）による保護レイヤーが配置され、その**ディセプションレイヤー**の背後にある重要なネットワーク資産を攻撃者から隠す役割を果たすため、攻撃者を撹乱してリダイレクトすると同時に、ネットワーク上の攻撃者の存在を顕在化させることができます。

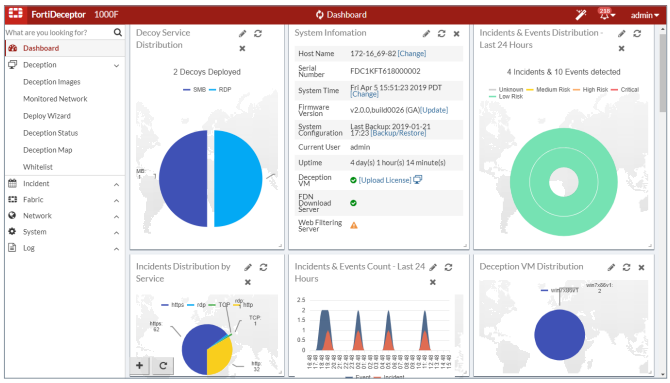

図1：FortiDeceptorダッシュボード

高度な脅威ディセプション

ディセプション：ディセプションVMインスタンスとデコイを一元的な場所から管理し、外部と内部の脅威を欺きます。本物の資産と区別不可能な、WindowsとLinuxのOS VMによるディセプション用の外観を配備して攻撃者を誘導し、攻撃者の存在を顕在化させます。

顕在化：迅速かつ正確な検知と実用的なアラートによって、ハッカーのアクティビティを顕在化します。ハッカーのラテラルムーブメントをトレースして相関付け、Web UI、電子メール、SNMPトラップ、ログでセキュリティ管理者に通知します。ハッカーの水平方向の移動やアクティビティの詳細なフォレンジック情報を分析し、インシデントと攻撃者のトラフィックのキャンペーン情報を相関させます。

排除：攻撃者を本番サーバーからディセプションホストへとリダイレクトすることで、脅威を排除します。フォーティネット セキュリティ ファブリックは攻撃者を隔離するとともに、C&Cサーバーへの接続を停止してキルチェーンを分断し、ネットワークへの侵入やマルウェアの感染を阻止します。

ハイライト

ディセプションVMの配備とデコイの用意：ハッカーを欺き、ディセプションVMに誘導します。

アクティビティの監視：ログイン / ログアウト、Windowsの共有アクセス、侵入行為、Webページのアクセスなどを監視します。

イベントの相関付けとインシデントの作成：ホストへのログイン、ペイロードをダウンロードするためのWebサイトへのアクセス、ディセプションVM毎のログアウトに関する情報を基に、イベントの相関付けとインシデントの作成を行います。

攻撃の排除：侵入やWebサイトのアクセスを特定して阻止し、攻撃中に仕掛けられたすべてのファイルのマルウェアをスキャンすることで、デコイからの／デコイへの攻撃を排除します。

カスタムレポートや包括的レポートの生成：GUIからの操作で、PDF形式のレポートをインシデントテーブルから生成できます。

アラートの構成と送信：電子メール、SNMP、またはsyslogサーバー経由でアラートを送信できます。

脅威の管理

FortiDeceptor が配備するディセプション VM とデコイを活用して攻撃者の行動を検査し、不正な目的であるかどうかを判断します。稼働中の本番サーバーから攻撃者を遠ざけてディセプションホストへとリダイレクトできるため、重要な企業資産が保護されます。攻撃が検知されると実用的インテリジェンス（IOC と TTP）が生成され、フォーティネット セキュリティ ファブリックとの統合によってそれらの情報がインラインの広範なセキュリティ制御で共有されるため、これらの未知の脅威をリアルタイムでプロアクティブにブロックできます。企業は、現在の攻撃を停止するとともに、自動レスポンスプロセスを作成して将来の攻撃を阻止 / 検知することができます。また、アラートと対策のためのインテリジェンスがセキュリティ運用チームに通知されるため、キルチェーンを分断して攻撃を直ちに停止することが可能です。

導入例

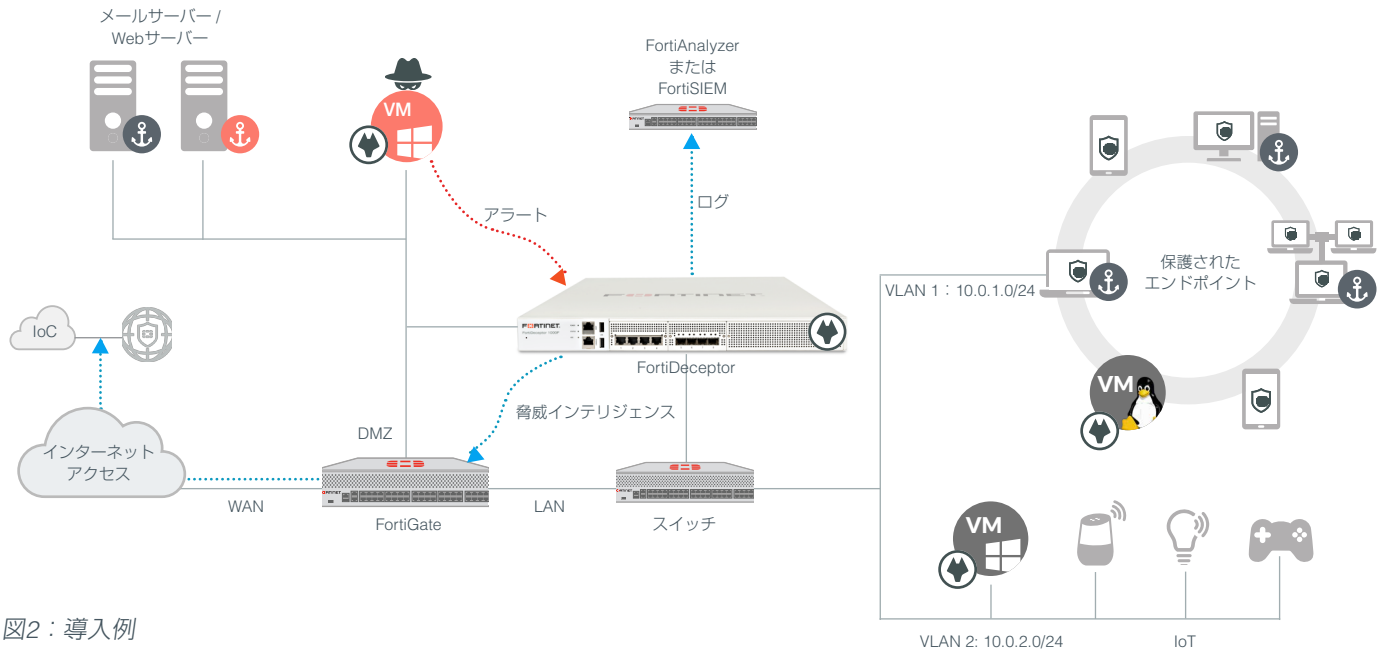

図2：導入例

技術仕様

FortiDeceptor VM	
システム性能	
ディセプションVM OS	Windows、Ubuntu
サポートするVMインスタンス数（最大）	16（Windows / Linux）
サポートするVLAN数（最大）	32
標準ディセプションVM数	0（最大 256 デコイまでアップグレード可能）
仮想マシン	
サポートするハイパーバイザー	VMware vSphere ESXi 5.1、5.5、6.0 以降、KVM
仮想CPU数（最小 / 最大）	4 / 無制限 * インテル バーチャライゼーション・テクノロジー（VT-x / EPT）または AMD Virtualization（AMD-V / RVI）
仮想ネットワークインタフェース	6
仮想メモリ容量（最小 / 最大）	4GB / 無制限 **
仮想ストレージ容量（最小 / 最大）	200GB / 16TB***

* 仮想 CPU 数は、VM インスタンス数プラス 1 にすることを推奨します。** 仮想メモリサイズは、4GB プラス各 VM インスタンス用に 2GB を追加することを推奨します。
*** 本番環境における仮想ストレージサイズは、1TB にすることを推奨します。

技術仕様

	Fortideceptor 1000F
システム性能	
RAM の種類とサイズ	DDR4-2400 48 GB ECC RDIMM（16 GB x 3）
オンボードのフラッシュメモリ	2 GB USB
ディセプション VM OS	Windows、Ubuntu
サポートする VM インスタンス数（最大）	16（Windows）/ 16（Linux）/ 16（Windows と Linux の混在）
サポートする VLAN 数（最大）	32
ディセプション VM 数（出荷時）	2 x Windows（1 x Windows 7、1 x Windows 10）、8 x Linux
ハードウェア仕様	
形状	ラックマウント（1 RU）
インタフェース	4 x GbE（RJ45）、4 x GbE（SFP）
ストレージ	2 TB（2 x 1 TB）
利用可能なストレージ（RAID 構成時）	1 TB
リムーバブル HDD	—
サポートする RAID レベル	RAID 0、1
デフォルト RAID レベル	1
冗長電源（ホットスワップ対応）	✔
サイズ	
高さ x 幅 x 奥行	4.4 x 43.8 x 58.0 mm
重量	10.9 kg
動作環境	
AC 電源	100 ～ 240 V AC、50 ～ 60 Hz
消費電力（最大 / 平均）	116.58 W / 66.93 W
放熱	397.77 BTU/h
動作温度	0° C ～ 40° C
保管温度	-40° C ～ 70° C
湿度	5 % ～ 90 %（結露しないこと））
動作高度	最高 2,250 m
準拠規格	
認定	FCC Part 15 Class A、C-Tick、VCCI、CE、UL / cUL、CB

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

DS-FDC-R3-201905-R1