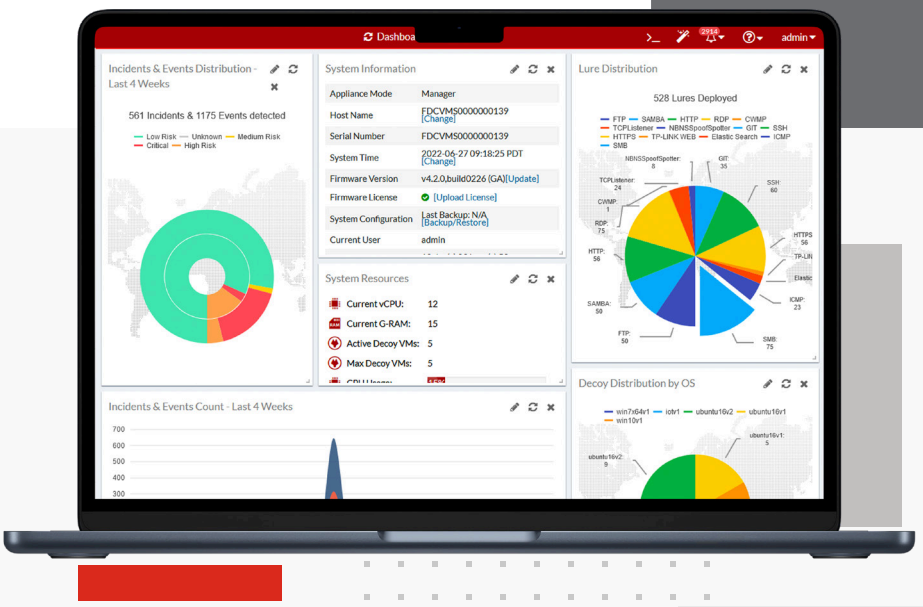
FortiDeceptor



主な利点

- 実用的なインテリジェンスを提供し、SOC の効果を強化
- 困難な領域（IoT および OT 環境）までサポートを拡大
- 具体化された警告を早期に提供（誤検知なし）
- リスクレベルの上昇に合わせて自動的に拡大
- 新たな脅威や未知の脅威、悪意のある内部関係者を検知

活動中のネットワーク内攻撃を検知して阻止する、ノンイントルーシブでエージェントレスのディセプションソリューション

FortiDeceptor は、フォーティネットのノンイントルーシブでエージェントレスのディセプションプラットフォームです。攻撃者を偽の資産に誘導し、最終的に存在を顕在化させることで、防御側の制御を取り戻します。

FortiDeceptor は、ハニーポットの概念に脅威分析と脅威減災の機能を組み合わせることで、現在のセキュリティ防御の大幅な強化を可能にします。これを実現するため、偽の鍵やファイルなどのデコイやトークンといったディセプション資産を置き、ディセプション資産のレイヤーを分散させ、IT / OT / IoT ネットワークの他の本物の資産と同じように見えて動作するトラップのシステムを作成することで、既知および未知の人為的攻撃や自動化された攻撃を騙し、検知し、隔離します。

FortiDeceptor を使用することで、攻撃者がミスを犯して初めてその存在を検知するのではなく、特権の昇格やマルウェアの実行の試行などの攻撃者のあらゆる行動が検知の機会となる、アクティブ防御アプローチを採用できます。

提供形態

アプライアンス

仮想マシン

脅威を早期に検知し、ネットワークへの影響を最小化

FortiDeceptor は、利用可能な IP アドレスを使用して、FortiDeceptor コンソールからデコイを展開し、実行することで動作します。デコイは、異なるネットワークセグメントの未使用の IP アドレスを利用するため、ネットワーク可用性に影響することはありませんが、攻撃者にはネットワークの重要な要素であるように見えます。これらの IP アドレスは、ネットワークの実際のホストやデバイスに対応するものではありません。

FortiDeceptor プラットフォームは、複数のディセプションコンポーネントで構成され、それらのコンポーネントを組み合わせることで、ネットワークの他の資産とまったく同一に見せかけたディセプション資産のスケーラブルなレイヤーを提供します。産業用制御システム、医療機器、ATM、貯蔵庫の計器、POS デバイス、IoT デバイス、ネットワークインフラなどの偽の資産であるこれらのデコイは、本物のオペレーティングシステムやサービスを実行し、偽ではあるものの少量のトラフィックを生成して攻撃者を誘導し、機密度の高い資産から引き離します。FortiDeceptor にはデコイの豊富なインベントリが提供されていますが、独自のデコイを用意し、自分のゴールデンイメージをアップロードすることもできます。

ディセプションレイヤーのイベントをさらに拡大するため、FortiDeceptor は、本物のエンドポイントやサーバーにパンくず（またはトークン）を配置し、偽の文書、ファイル、または偽の認証情報であるこれらのトークンを攻撃者が水平移動や暗号化の目的で利用するのを待機します。トークンは本物のファイルや認証情報と見分けがつかないように設計されているため、攻撃者やマルウェアは、これに誘導され、デコイへと水平移動します。FortiDeceptor は、偽の認証情報の使用を即座に検知し、アラートを生成し、内蔵するエンドポイント分離の機能や SOAR（セキュリティオーケストレーション、自動化、レスポンス）プレイブックを使用してエンドポイントを自動的に隔離します。

高速のインシデントレスポンス

FortiDeceptor は、高精度で誤検知ゼロのアラートを生成し、セキュリティチームが不正活動よりも優位に立つよう支援し、比類ない可視性を提供することで、攻撃、認証情報の窃取、水平移動、マルウェアの活動の検知と阻止を可能にします。また、パッチの適用や他のセキュリティ制御を利用できない場合は、それに代わるセキュリティ制御を提供します。パッチを利用できない OT 環境が一例ですが、パッチを利用できる環境であっても、メンテナンスには多くの時間と労力が必要です。

マルウェアまたは人間による攻撃が偽やデコイの資産に接触すると、アラートが生成され、SIEM（セキュリティ情報 / イベント管理）、SOAR、または使用中の脅威インテリジェンスプラットフォームに送信されます。次にデコイが活動のキャプチャと分析をリアルタイムで開始し、8 つの内蔵インテリジェンスエンジンを使用して脅威インテリジェンスを生成することで、詳細かつ正確な分析を可能にします。

FortiDeceptor の導入や管理にあたり、高度なスキルを持つセキュリティアナリストは必要ありません。デコイの展開から、隔離された攻撃と隔離されていない攻撃の証拠の分析、さらには、動的保護レイヤーの実装までのプロセス全体が一元化され、自動化されています。

進化する脅威からの保護

新たな脅威に対抗するため、FortiDeceptor は、新たに発見された脆弱性や不審な活動に基づいてオンデマンドでディセプションデコイを作成し、IT / OT / IoT 環境の自動化された動的保護を可能にします。

- **ゼロデイ保護の実装：**攻撃者は多くの場合、脆弱な資産を最初に標的にします。FortiDeceptor の高度なアウトブレイク機能により、公開されたばかりの脆弱性が存在するデコイが意図的に配置されるため、不正活動のキルチェーンの早い段階での誘導、自動検知、隔離が可能になります。FortiGuard Labs から脆弱性が報告されると、ソフトウェアアップデートを必要とせずに、脆弱性エミュレータがアウトブレイクデコイへのフィードとして自動的に送り出されます。
- **IOC（Indicators of Compromise：侵害指標）に対する迅速な脅威ハンティング：**FortiDeceptor と SOAR の統合により、SOAR プレイブックからディセプション資産の展開をオンデマンドで開始し、不正活動のハンティングと隔離に利用できます。不審な活動が検知された場合、SOAR プレイブックが、そのセグメントへのデコイやトーキンの展開を自動的に開始できるため、攻撃の検知とインテリジェンスの取得が容易になります。

FortiDeceptor を主要セキュリティツールやフォーティネット セキュリティ ファブリックと統合することで、脅威減災のオーケストレーションと攻撃インテリジェンスの強化も実現します。

OT / IoT 環境のディセプション

OT 環境は多様で、マルチベンダーのデバイスやシステムが多く存在し、その多くは、セキュリティを考慮して設計されていません。レガシーシステムにおいては、継続性、コスト、パッチの有無などの理由から、監視エージェントやセキュリティパッチの適用でセキュリティを強化する方法を必ずしも選択できるわけではありません。FortiDeceptor のデコイは、さまざまなタイプの IT / OT / ICS / IoT デバイスに加えて、SAP や ERP などのクリティカルなアプリケーションをシミュレーションし、パデューモデルのすべてのレベルへの展開が可能です。

FortiDeceptor は、アクティブとパッシブの資産の検出を自動的に実行して、資産のインベントリを作成し、IT / OT ネットワークに最適化されたデコイの配置を推奨します。オンラインまたはエアギャップのいずれのモードでも動作し、過酷な環境でも動作するように設計された Rugged 仕様のアプライアンスである FortiDeceptor Rugged 100G として利用することもできます。

FortiDeceptor の主なメリット

正確、早期の検知、高速レスポンス

- 潜伏時間を短縮し、誤検知を軽減
- 初期の偵察と水平移動を検知
- 攻撃の自動隔離機能の内蔵により、拡大する前に攻撃を阻止
- リスクレベルの上昇に合わせて自動的に拡大
- マルウェアが偽のファイルを暗号化した場合に、感染したエンドポイントの自動ブロックを開始することで、ランサムウェアの減災を支援
- FortiGuard Labs の最新アウトブレイクアラートに基づき、脆弱なデコイを自動的に展開
- フォーティネット セキュリティ ファブリックやサードパーティのセキュリティ制御と統合

実用的なインテリジェンスを提供し、SOC の効果を強化

- 高精度で実用的なアラートを攻撃者とのリアルタイムのやり取りに基づき生成
- 8 つの異なるフォレンジックエンジンを使用して不正活動を相関付けることで、アナリストによる調査、フォレンジック証拠の収集、監視、進行中の攻撃の自動停止を支援
- 進行中の攻撃のインテリジェンスと詳細なフォレンジックにより、可視性のギャップを解消
- 攻撃の再生と攻撃の視覚化を提供
- 自動化により、摩擦の少ない導入とメンテナンスが可能

困難な領域にまでサポートを拡大

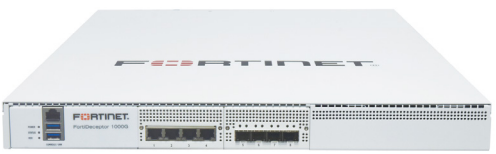
- 産業用システム / IoT / IoMT デバイスに対する脅威の顕在化とブロックを前提に設計され、最適化された、OT、IoT、IoMT デコイ
- エージェントレスかつノンイントルーシブ、ミッションクリティカルな業務への影響なし
- 1 日で完了する容易なインストールと利用、ネットワークトポロジの変更は不要
- 独自のテレメトリを提供できない資産に対する脅威を検知
- オンプレミス / クラウド / IT / OT / IoT / IoMT 環境などのあらゆる攻撃対象領域に対応
- オンラインとエアギャップの両方のモードで動作

技術仕様

	FortiDeceptor Rugged 100G	FortiDeceptor 1000G
システム性能		
RAM の種類とサイズ	DDR4-2400 48 GB ECC RDIMM（16 GB × 1 + 32 GB × 1）	DDR4-2400 48 GB ECC RDIMM（16 GB × 3）
オンボードのフラッシュメモリ	16 GB（M.2 2242）	2 GB USB
デコイ VM サポート	Windows 7、Windows 10、Windows 10（カスタマイズ可能な BYOL）、Windows Server 2016、2019 および 2022（カスタマイズ可能な BYOL）、Linux（Ubuntu、CentOS、Redhat）、macOS、SSL-VPN Server、Medical（PACS、Infusion pump）、POS、ERP、IoT（ルーター、スイッチ、プリンター、IP カメラ）、OT（PLC、HMI、MNG）、SAP、SCADA、Outbreak、VOIP（4G/5G）、TOMCAT、Webmin、Citrix、ESXi、Elastic-Search、SWIFT の組み合わせ	Windows 7、Windows 10、Windows 10（カスタマイズ可能な BYOL）、Windows Server 2016、2019 および 2022（カスタマイズ可能な BYOL）、Linux（Ubuntu、CentOS、Redhat）、macOS、SSL-VPN Server、Medical（PACS、Infusion pump）、POS、ERP、IoT（ルーター、スイッチ、プリンター、IP カメラ）、OT（PLC、HMI、MNG）、SAP、SCADA、Outbreak、VOIP（4G/5G）、TOMCAT、Webmin、Citrix、ESXi、Elastic-Search、SWIFT の組み合わせ
デコイサービス	SSL VPN、SSH、SAMBA、SMB、RDP、HTTP/S、SQL、GIT、DICOM、Telnet、FTP、TFTP、SNMP、MODBUS、S7COMM、BACNET、IPMI、TRICONEX、SRTP、MOXA、KAMSTRUP、GUARDIAN-AST、IEC104、EtherNet/IP、DNP3、JET-DIRECT、RTSP、UPnP、CDP、TCP ポートリスナー、SMTP、RADIUS、Mysql、MQTT、SIP、XMPP、3GPP、CANBus、B.BRAUN、VNC	SSL VPN、SSH、SAMBA、SMB、RDP、HTTP/S、SQL、GIT、DICOM、Telnet、FTP、TFTP、SNMP、MODBUS、S7COMM、BACNET、IPMI、TRICONEX、SRTP、MOXA、KAMSTRUP、GUARDIAN-AST、IEC104、EtherNet/IP、DNP3、JET-DIRECT、RTSP、UPnP、CDP、TCP ポートリスナー、SMTP、RADIUS、Mysql、MQTT、SIP、XMPP、3GPP、CANBus、B.BRAUN、VNC
ディセプション VM 数（出荷時）	ディセプションバンドル契約には、ディセプションデコイ、ディセプションルアーおよび FortiGuard サブスクリプションサービス（AREA、AV、IPS、Web フィルタリング）のライセンスが含まれます。1 VLAN 単価、最小 2 VLAN から注文可能。	ディセプションバンドル契約には、ディセプションデコイ、ディセプションルアーおよび FortiGuard サブスクリプションサービス（AREA、AV、IPS、Web フィルタリング）のライセンスが含まれます。1 VLAN 単価、最小 2 VLAN から注文可能。
ハードウェア仕様		
形状	デスクトップ：ファンレス設計	ラックマウント（1 RU）
インタフェース	6 × 1 GbE（RJ45）	4 × GbE（RJ45）、4 × GbE（SFP）
ストレージ容量	2.5 インチ SATA SSD 1TB（1 TB × 1）	2 TB（2 × 1 TB HDD）
利用可能なストレージ（RAID 構成時）	2 GB USB DOM、SATA-DOM または M.2（SATA）	1 TB
リムーバブル HDD	—	—
RAID 1	—	RAID 1
デフォルト RAID レベル	—	1
電源	100 ～ 240 V、1.8 A、50 ～ 60 Hz（外部 DC 電源）	650 W 冗長電源（1 + 0）、追加 / オプション電源（SKU：SP-FSA1000G-PS）
サイズ		
高さ × 幅 × 奥行	98 × 275 × 225 mm	44 × 438 × 600 mm
重量	5.73 kg	12.5 kg
動作環境		
AC 電源	—	100 ～ 240 V AC、50 ～ 60 Hz、650W、冗長電源（1 + 0）
DC 電源	入力：24 ～ 48 Vdc 3.45 ～ 1.77 A	
消費電力（最大）	+ 24 V（66.11 W）、+ 48 V（73.92 W）	253.2 W
消費電力（平均）	+ 24 V（54.1 W）、+ 48 V（60.5 W）	202.56 W
最大電流	+ 24 V（3.45 A）、+ 48 V（1.77 A）	
放熱	+ 24 V（259.69 BTU/h）、+ 48 V（286.34 BTU/h）	863.92 BTU/h
動作温度	0 ºC ～ 40 ºC	0 ºC ～ 40 ºC
保管温度	-40 ºC ～ 70 ºC	-25 ºC ～ 70 ºC
湿度	5 ～ 95%（結露しないこと）	10 ～ 90%（結露しないこと）
動作高度	最高 4,000 m	最高 2,250 m *
IP 規格・保護等級	IP40	—
準拠規格・認定		
認定	オンボードのフラッシュメモリ 8 GB 認定：FCC、ICES、CE、RCM、VCCI class A CB：低電圧指令（LVD）2014/35/EU IEC 62368-1 2nd Edition IEC 62368-1 3rd Edition UL/CSA：UL 62368-1 3rd Edition	FCC Part 15 Class A、RCM、VCCI、CE、UL/cUL、CB

* 最高温度での動作は、305 m あたり 1.5 ºC 低下します。

FortiDeceptor Rugged 100G



FortiDeceptor 1000G

技術仕様

FortiDeceptor VM	
システム性能	
デコイ VM サポート	Windows 7、Windows 10、Windows 10（カスタマイズ可能な BYOL）、Windows Server 2016、2019 および 2022（カスタマイズ可能な BYOL）、Linux（Ubuntu、CentOS、Redhat）、macOS、SSL-VPN Server、Medical（PACS、Infusion pump）、POS、ERP、IoT（ルーター、スイッチ、プリンター、IP カメラ）、OT（PLC、HMI、MNG）、SAP、SCADA、Outbreak、VOIP（4G/5G）、TOMCAT、Webmin、Citrix、ESXi、Elastic-Search、SWIFT の組み合わせ
デコイサービス	SSL VPN、SSH、SAMBA、SMB、RDP、HTTP/S、SQL、GIT、DICOM、Telnet、FTP、TFTP、SNMP、MODBUS、S7COMM、BACNET、IPMI、TRICONEX、SRTP、MOXA、KAMSTRUP、GUARDIAN-AST、IEC104、EtherNet/IP、DNP3、JET-DIRECT、RTSP、UPnP、CDP、TCP ポートリスナー、SMTP、RADIUS、Mysql、MQTT、SIP、XMPP、3GPP、CANBus、B.BRAUN、VNC
ディセプション VM 数（出荷時）	VM モデル 24 時間 365 日対応の FortiCare、ディセプションバンドル契約には、ディセプションデコイ、ディセプションルアーおよび FortiGuard サブスクリプションサービス（AREA、AV、IPS、Web フィルタリング）のライセンスが含まれます。1 ネットワーク VLAN 単価、最小 2 VLAN から注文可能。ディセプション VM を最大 20 台、ネットワーク VLAN を最大 128 台までサポート。
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、7.0 以降、KVM、Hyper-V、AWS、AZURE、GCP
仮想 CPU 数（最小 / 最大）	12 / 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）	16 GB / 無制限 **
仮想ストレージ容量（最小 / 最大）	200 GB / 16 TB ***

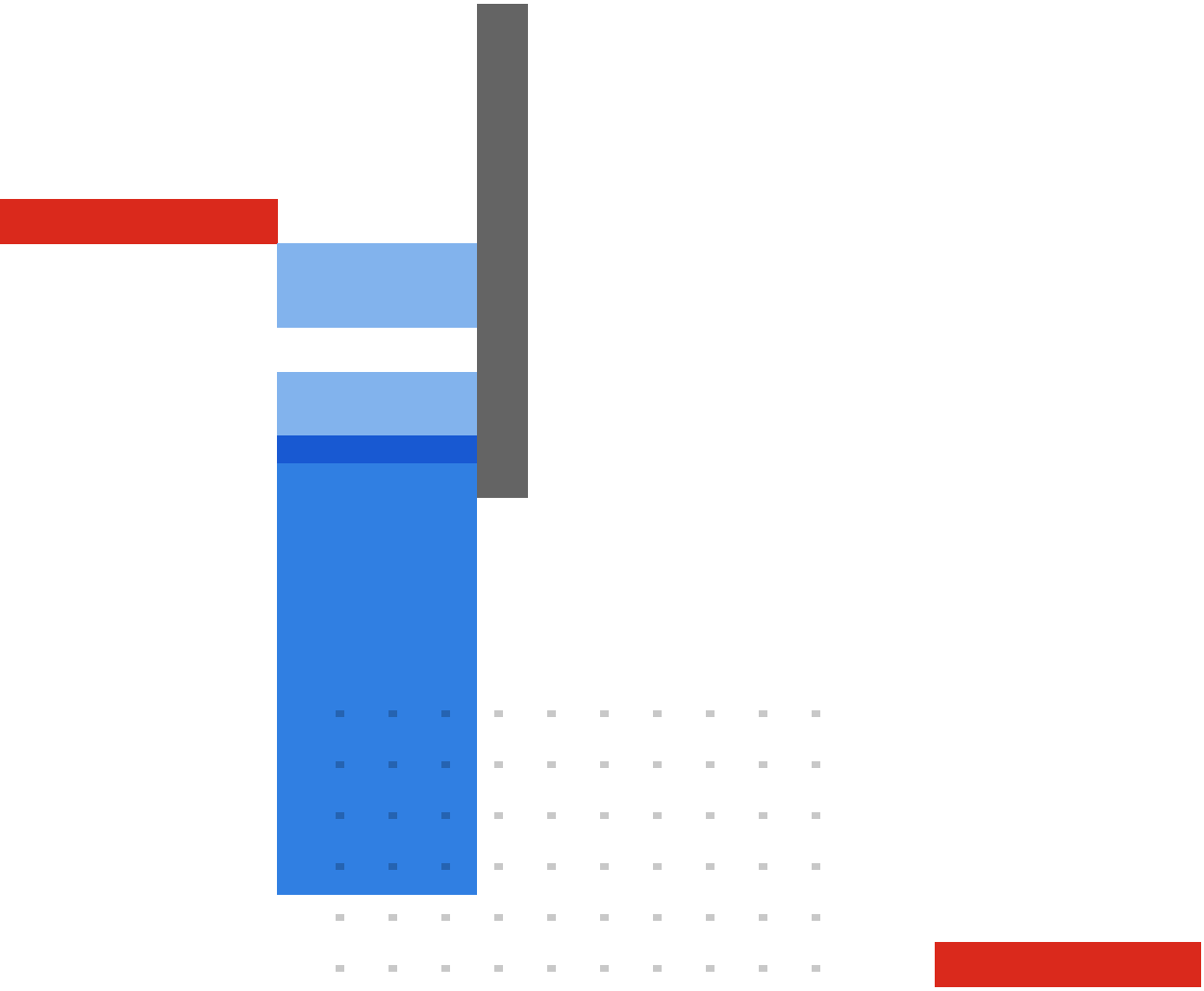
* 各ディセプション VM が 2Vcpu を必要とする場合、仮想 CPU 数は、ディセプション VM 数プラス 2 にすることを推奨します。

** 仮想メモリサイズは、4 GB プラス各ディセプション VM クローン用に 2 GB を追加することを推奨しています。

*** 本番環境における仮想ストレージサイズは、1 TB にすることを推奨します。

フォーティネット CSR ポリシー

フォーティネットは、サイバーセキュリティを通じてあらゆるお客様の進歩と持続可能性を推進し、人権を尊重する倫理的な方法でビジネスを遂行し、常に信頼できるデジタル世界を実現することをお約束します。お客様には、フォーティネットの製品およびサービスを使用して、違法な検閲、監視、拘留、または過剰な武力行使などの人権の侵害または乱用に関与したり、何らかの形で支援したりしないことをフォーティネットに表明し、保証していただくことになります。フォーティネット製品の利用にあたっては、フォーティネットの EULA（エンドユーザー使用許諾契約）を遵守し、EULA に違反すると疑われる場合は、フォーティネット不正告発規定に概要が記載されている手順で報告する必要があります。



フォーティネットジャパン合同会社

〒106-0032
東京都港区六本木 7-7-7　Tri-Seven Roppongi 9 階
www.fortinet.com/jp/contact

お問い合わせ

DS-FDC-R18-202402-R1