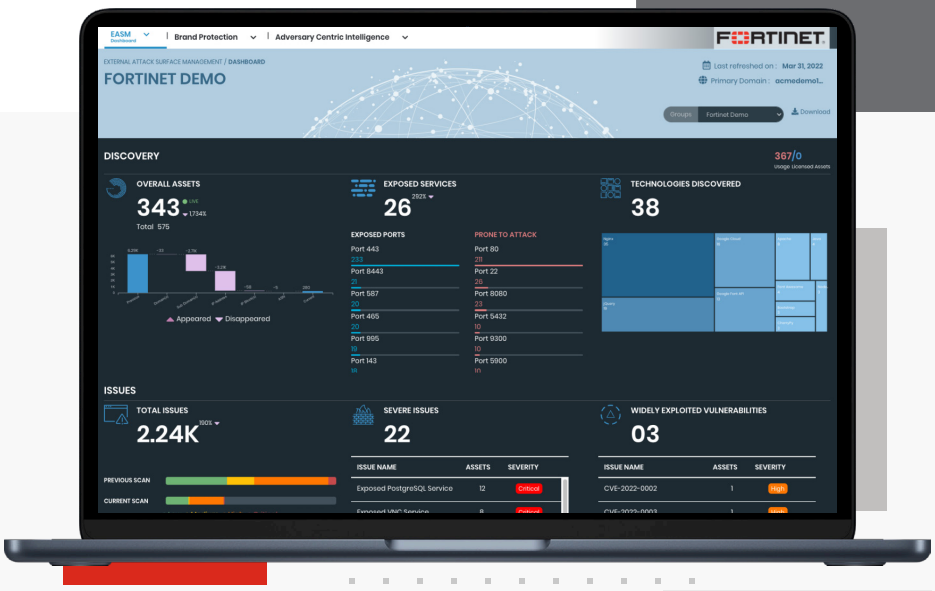
FortiRecon



ハイライト

攻撃対象領域をスキャンして、資産に対するリスクを迅速に特定

組織に対する多様な脅威を理解し、ブランドの評判を保護

インシデントへの迅速なレスポンス、攻撃者の正しい理解、資産の保護を支援

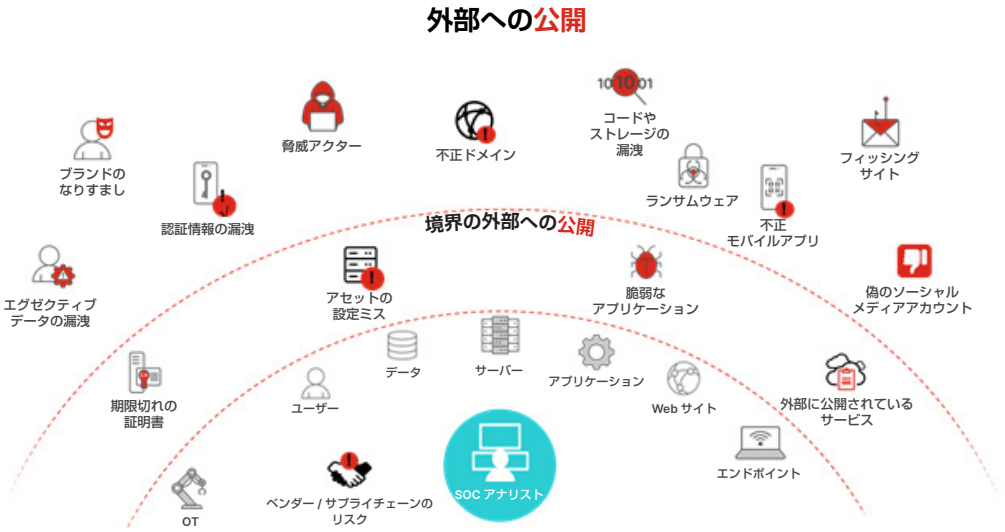
ダークウェブなどからの敵対的な活動の広範なビューと早期の警告を提供

デジタルリスク保護サービス

外部攻撃対象領域は、サイバー犯罪者が組織に侵入する目的で悪用する潜在的な多くの侵入場所を提供する可能性があります。サーバーの設定ミス、脆弱なソフトウェア、シャドー IT 資産、認証情報の漏洩は、直ちに脅威になる可能性がありますが、組織のセキュリティチームは多くの場合に、これらを監視するリソースも、組織の境界に対するこのようなリスクを追跡して特定するツールも持ち合わせていません。

デジタルリスク保護サービス

外部攻撃対象領域は、サイバー犯罪者が組織に侵入する目的で悪用する潜在的な多くの侵入場所を提供する可能性があります。サーバーの設定ミス、脆弱なソフトウェア、シャドー IT 資産、認証情報の漏洩は、直ちに脅威になる可能性がありますが、組織のセキュリティチームは多くの場合に、これらを監視するリソースも、組織の境界に対するこのようなリスクを追跡し、特定するツールも持ち合わせていません。



デジタルトランスフォーメーションにより、組織が急速に変化を遂げていることで、セキュリティチームは、ネットワークのリスクへの対策に追われています。脅威アクターは常にインターネットをスキャンして、組織のネットワークに侵入する足掛かりとなる防御のギャップを探しています。リソースの制約により、セキュリティ管理者がそれに追いつくのは時として容易なことではありません。

FortiRecon は、既存のセキュリティソリューションと同時に動作することで、攻撃側の視点でのインフラストラクチャの可視性と類似する組織を侵害する目的で利用される戦術や手法をセキュリティチームに提供する、SaaS ベースの DRP（Digital Risk Protection：デジタルリスク保護）サービスです。このサービスを組織に合わせてカスタマイズされた脅威インテリジェンスを組み合わせることで、継続的な対策の一環として、制御された方法で、確度の高いセキュリティ脅威を減災することができます。

主な利点

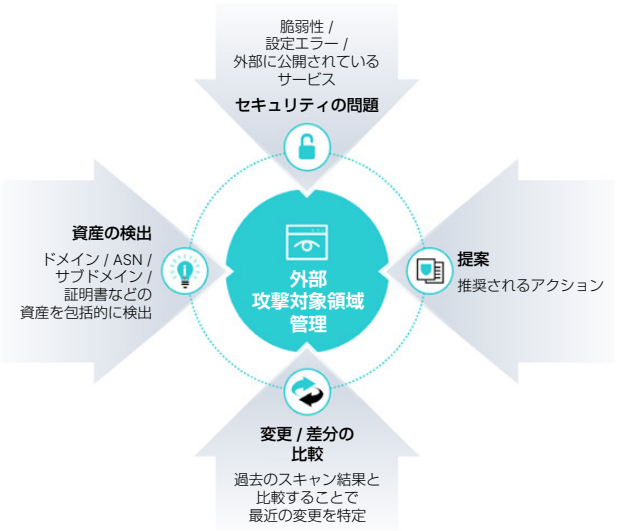
FortiRecon は、可視性とインテリジェンスを提供することで、リスクベースの制御された次のようなセキュリティアクションの実行を可能にします。

- 組織と関連会社のデジタル攻撃対象領域をマッピングすることで、外部の可視性のギャップとセキュリティリスクを特定する
- 修復の活動の優先順位をビジネスリスクに基づいて判断する
- ブランドに対する攻撃を特定し、レピュテーションに影響する前に減災する
- 効果的なセキュリティ制御を順守していることを確認する
- インシデントへの迅速なレスポンス、攻撃者の正しい理解、資産の保護を可能にする
- 組織に合わせてカスタマイズされた脅威インテリジェンスフィードにより、SOC アナリストの運用オーバーヘッドを軽減し、ダークウェブやその他のソースからの敵対的な活動を早期に警告する

EASM（外部攻撃対象領域管理）

外部に公開されている資産を特定して、外部リスクを減災

FortiRecon の EASM（外部攻撃対象領域管理）は、組織のデジタル攻撃対象領域とその関連会社を攻撃者側の視点で可視化します。攻撃者により外部に公開された既知および未知の企業の資産や関連する脆弱性、流出した認証情報、サードパーティのソフトウェアコードの脆弱性、パブリッククラウドサービスの設定ミスなどの、脅威アクターに悪用される可能性のある脆弱性を継続的に監視して特定することで、重大な問題に対する修復の優先順位付けの判断を支援します。



機能とハイライト

継続的な資産の検出と外部攻撃対象領域の監視：組織のドメイン、サブドメイン、IP アドレス、ASN、IP ブロックを自動的に識別し、シャドー IT システム、クラウドアプリケーション、脆弱なソフトウェアなどの外部に公開されている資産に起因する組織のリスクを特定して、動的かつカスタマイズ可能なインベントリを提供します。

リスクの検知と優先順位付け：脆弱性、設定ミス（オープンポートなど）、期限切れ / 間もなく期限切れになる SSL 証明書、外部に公開されているデータベースサービス、DNS 関連の問題、データ / 認証情報の漏洩などを特定し、その深刻度や脅威アクターの活動の調査に基づく活動中のエクスプロイトに基づき、リスクベースの修復の優先順位付けの判断についての提案を提供します。

認証情報の漏洩：ダークウェブやプライベートチャットルームを継続的に監視し、組織の認証情報の漏洩をアラートで通知します。

拠点や関連会社に基づく資産の監視：拠点ごと、部門ごと、または関連会社の組織に基づいて資産のインベントリを作成し、分類します。

変更の比較：資産の外部への公開と修復のトレンドの変化を継続的に分析し、追跡します。FortiRecon の履歴データは、時系列的な変更のパターン、ポリシー違反、改善の領域、その他の潜在的なリスク領域の特定に役立ちます。

BP（ブランド保護）

ブランドの侵害を防止し、評判を保護

FortiRecon BP（ブランド保護）は、独自のアルゴリズムを使用して、フィッシング、タイポスクワッティング、不正アプリ、ソーシャルメディアにおけるブランドやエグゼクティブのなりすましなどのWeb ベースの攻撃を検知します。これらはいずれも、顧客、従業員、パートナーを欺き、情報、パスワード、クレジットカード情報を手に入れる目的でサイバー犯罪者が使用する一般的な手法です。

偽のサイトやアプリケーションなどの活動を早期に検知して、テイクダウンのアクションを要求することで、企業のブランド価値、信頼、整合性、評判の保護を支援します。

機能とハイライト

タイポスクワッティング：不正 Web サイトの検知とテイクダウンを可能にします。

不正モバイルアプリ：さまざまなアプリストアの不正モバイルアプリの追跡とテイクダウンを可能にします。

ソーシャルメディア：企業のソーシャルメディアアカウント（Facebook、Twitter、Instagram、LinkedIn など）のなりすましを検知し、ブランドに対する議論を監視します。

フィッシングの検知：公式 Web ページに電子透かしを埋め込むことで、Web ページのクローニングや再ホスティングを追跡します。

コードレポジトリの外部への公開：パブリックコードレポジトリで外部に公開されている機密情報を発見します。

オープンバケットの外部への公開：クラウドストレージプラットフォーム経由で一般アクセスが可能なファイルを検知します。

エグゼクティブの保護：ソーシャルメディアプラットフォームでのアイデンティティのなりすましを監視し、防御します。

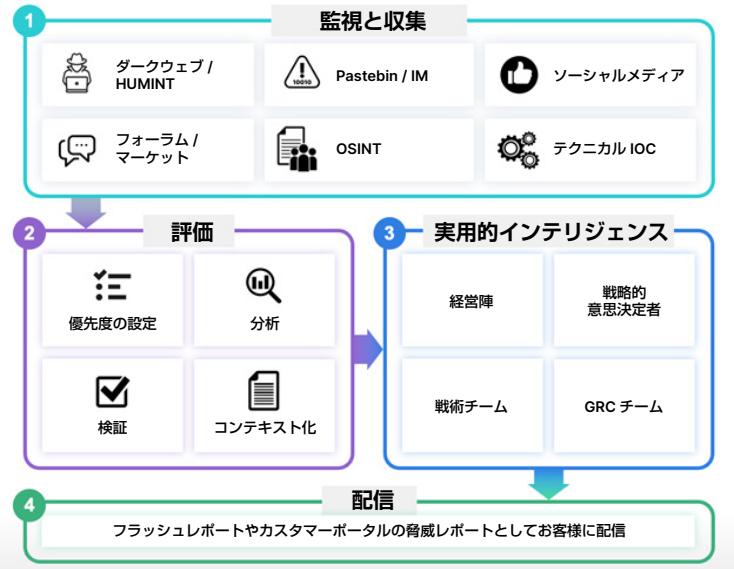
ロゴの検知：フィッシングサイトやタイポドメインでの不正なロゴの使用を特定します。

テイクダウンサービス：FortiGuard Labs のテイクダウンサービスを利用することで、ブランドへのなりすましに迅速に対応し、セキュリティチームによる調査時間を短縮します。

ACI（アドバーサリーセントリックインテリジェンス）

組織に合わせて高度にカスタマイズされた脅威インテリジェンス

FortiRecon ACI（アドバーサリーセントリックインテリジェンス）は、組織に対する差し迫った脅威に関する、精選され、コンテキストが付加された実用的インテリジェンスを提供することで、インシデントへの迅速なレスポンス、攻撃者の正しい理解、資産の保護を可能にします。ACI は、ダークウェブ、オープンソース、代表的な脅威から新たな脅威までに関する技術的な脅威指標を提供します。脅威アクターの実用的インテリジェンスを利用することで、リスクをプロアクティブに評価し、既存のセキュリティ対策の脆弱性を特定し、セキュリティ担当者の意識を向上させることができます。



機能とハイライト

脆弱性のインテリジェンスと優先順位付け：ダークウェブやオープンソースで活発に議論されている新しい脆弱性やエクスプロイトを監視して報告します。FortiRecon は、スキャン結果に加えて、広範な使用状況、CVE、CVSS に基づき、脆弱性スコアを再評価して優先順位を判断することで、効果的な修復を可能にします。

ランサムウェアのインテリジェンス：ランサムウェアの脅威アクターの活動を監視し、標的と TTP について報告します。

サプライチェーン / サードパーティのリスク評価：ランサムウェアのリスク、認証情報 / データの漏洩、ダークウェブのチャットでの言及、脆弱性の外部への公開、設定ミス、タイポスクワッティングなどのサードパーティのリスクを継続的な監視し、早期に可視化します。

認証情報の漏洩：組織に関連する認証情報の漏洩をアラートで通知します。

スティーラー感染：スティーラー感染や侵害されたユーザー認証情報を検知します。

カード詐欺の監視：クレジットカードの BIN コードを監視し、盗難されたカードを特定して報告し、侵害されたデータ、画像などを提供します（金融サービス機関にご利用いただけます）。

脅威リサーチ、インテリジェンスの収集、高度なクエリ：世界中の注目すべきサイバーイベントや過去の脅威活動などの最新のサイバーインテリジェンスに瞬時にアクセスし、早期の警告やレポートを入手できます。

提案：分析、評価、リスクの優先順位付け、修復を提案します。

追加機能

FortiRecon テイクダウンサービス

Web サイトのタイポスクワッティング、偽のソーシャルメディアアカウント、不正モバイルアプリなどのブランドなりすましは、サイバー犯罪者が使用する一般的な手法です。FortiGuard Labs の脅威エキスパートが、複数のソースからデータを自動的に収集して分析することで、ブランドのなりすましを特定します。不正な Web サイト、モバイルアプリ、ソーシャルメディアアカウントの迅速なテイクダウンの提供も可能です。

レポート

脅威インテリジェンスはさまざまな場所から提供され、その内容も多岐にわたるため、脅威アナリストがすべてを遅延なく処理するのは多くの場合に困難です。FortiRecon は、ノイズを除外し、組織にとって最も重要な対象に特化した、高度にカスタマイズされたレポートセットを提供します。

セキュリティ ファブリック統合

FortiRecon は、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ソリューションの両方への幅広い統合が可能です。

- FortiGate セキュリティ ファブリックの統合により、NAT 経由などによってデバイスから外部に公開される資産が自動的に検出され、スキャンやリスクレポートに追加されます
- FortiSOAR の統合により、FortiRecon が収集した情報から、自動化されたアクションを実行することができます（認証情報の侵害が発見された場合にユーザーのパスワードをリセットするなど）
- FortiSIEM は、FortiRecon レポートの結果を取り込んで関連付けることができます
- ForiDAST を統合することで、完全 Web アプリケーションスキャンを FortiRecon UI から開始できます

サードパーティとの統合

- 主要クラウドプロバイダーとの統合により、動的なクラウドベースの資産を自動的に検知し、FortiRecon のリスクレポートに追加することができます
- アラートの E メールによる通知に加えて、Microsoft Teams や Slack との統合も可能です
- REST ベースの API を、オーケストレーションやサードパーティソリューションへの統合に利用できます

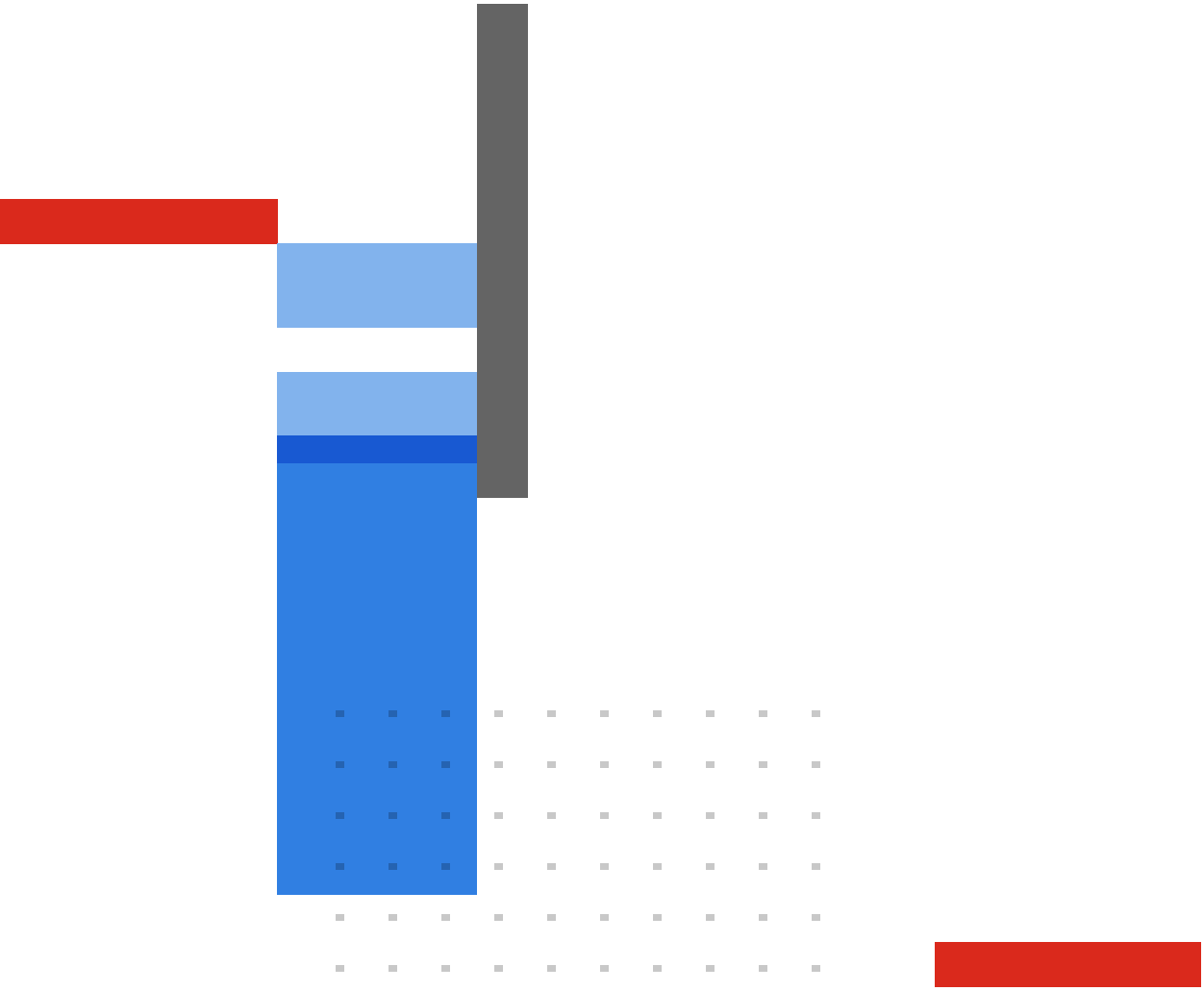
FortiRecon 製品の主な機能

ソリューションバンドル	機能	FortiRecon EASM	FortiRecon EASM / BP	FortiRecon EASM / BP / ACI
EASM（外部攻撃対象領域管理）	資産の検出	✓	✓	✓
	セキュリティの問題	✓	✓	✓
	資産のレポート	✓	✓	✓
	月次の資産の特定	✓	✓	✓
	週次の資産の特定			✓
	継続的な資産のスキャン			✓
	認証情報の漏洩	✓	✓	✓
	合併 / 買収のリスク評価	✓	✓	✓
	関連会社のリスク管理	✓	✓	✓
BP（ブランド保護）	ドメインの脅威：タイポスクワッティング		✓	✓
	ドメインの監視：フィッシング（電子透かし）		✓	✓
	ドメインの脅威：ブランドのなりすまし（ロゴの検知を含む）		✓	✓
	データ漏洩：ソースコードリポジトリ		✓	✓
	データ漏洩：クラウドストレージ		✓	✓
	不正モバイルアプリ		✓	✓
	エグゼクティブの監視		✓	✓
	ソーシャルメディアの監視：不正アカウント		✓	✓
	テイクダウン		✓	✓
ACI（アドバーサリーセントリックインテリジェンス）	インテリジェンスの収集：ダークウェブ			✓
	インテリジェンスの収集：オープンソース（OSINT）			✓
	インテリジェンスの収集：テクニカルインテリジェンス			✓
	インテリジェンスの収集：脅威アクター			✓
	ダークウェブマーケットプレイスの監視：スティーラー感染			✓
	ダークウェブマーケットプレイスの監視：クレジットカード詐欺			✓
	サプライチェーンのセキュリティ：脆弱性のインテリジェンス			✓
	サプライチェーンのセキュリティ：ランサムウェアのインテリジェンス			✓
	サプライチェーンのセキュリティ：ベンダーのリスク評価			✓
	IoC レピュテーション検索（IP / ドメイン / ハッシュ / CVE）			✓
配信	エグゼクティブレポート	✓	✓	✓
	24 時間 365 日のポータルへのアクセス	✓	✓	✓
	アナリストサポート		✓	✓
	リアルタイムアラート		✓	✓
	MSSP マルチテナントのサポート *			
統合	Open REST API	✓	✓	✓
	オーケストレーション（SOAR）	✓	✓	✓
	パブリッククラウド（AWS、GCP、Azure）	✓	✓	✓
	FortiGate	✓	✓	✓
	FortiDAST	✓	✓	✓

* FortiCare Premium ライセンスが必要です。

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-FRN-R06-202402-R1