

SOLUTION BRIEF

# FortiRecon ブランド保護で デジタル資産に対するブランドリスクと ビジネスリスクを可視化

## 概要

今日、ほとんどの CISO、CSO、そしてセキュリティオペレーションチームは、管理すべきサイバーセキュリティの課題を十分すぎるほど抱えています。しかし、通常のセキュリティの課題やカバー対象の範囲を外れた、ブランドに対するサイバー関連のリスクについてはどうでしょうか。このようなデジタルリスクの評価は、エンタープライズセキュリティアーキテクチャと企業の安全なデジタル環境における重要な拡張的対応範囲だと言えます。CLO（最高法務責任者）、CMO（最高マーケティング責任者）、リスクおよびコンプライアンスの責任者、そして他の経営陣たちは、このように従来のセキュリティ態勢の枠組みに収まらない課題の「拡張」領域で、迅速な措置を講じる必要に迫られる可能性があります。

フォーティネットの DRP（Digital Risk Protection：デジタルリスク保護）ソリューションの一部である FortiRecon BP（Brand Protection：ブランド保護）は、ブランド固有の脅威の全体像を提供します。これにより、ブランドと評判のリスク、認証情報の侵害、タイポスクワッシング、改ざん、不正アプリケーション、有害なソーシャルメディアへの投稿、ブランドのなりすまし、フィッシングなどのデジタルリスクについて、早期警告を受け取ることができます。

## ブランドも狙う攻撃者

ブランドを侵害するには以下のように多くの方法があります。

- サイバー犯罪者が正規の会社を装ってモバイルアプリを配信し、その企業の見込み客や顧客をリスクにさらす
- 認証情報が盗まれ、ニュースで報道されることにより、その企業が機密データの保護について信頼できないといった印象が拡散する
- 会社の Web サイトが改ざんまたは機能不全の状態にされ、オンラインでの購入や他の取引ができなくなる
- 攻撃者が企業の Web サイトを装って、訪問者に対して詐欺や攻撃を行う

## FortiRecon BP で可視性を向上し、リスクを軽減

FortiRecon BP は、ブランドがリスクにさらされやすい箇所を評価します。こうしたリスクは、企業の業界内での信頼性、お客様や世間からの評判、そして市場での評価を損なう可能性があります。

FortiRecon BP は、特に以下の領域でブランドに対するリスクが生じていないかを監視します。

- ソーシャルメディア：会社のソーシャルメディアアカウントのなりすまし
- Web：Web サイトに対するタイポスクワッシングや改ざんなどの不正な活動
- フィッシング：フィッシング目的のクローンや不正に立ち上げられたホスト（サーバ）による会社の Web ページを追跡
- モバイル：会社のモバイルアプリに似せて作成された不正なモバイルアプリ

「DRP（Digital Risk Protection：デジタルリスク保護）は会社のデジタルプレゼンスの一環であり、従来のサイバーセキュリティ権限の範囲を大きく外れたものです。従来のシステムは、ネットワーク、ユーザー、およびデータを保護するために構築されました。DRP はそれとは対照的に、デジタル資産を保護します。」<sup>1</sup>

FortiRecon BP は、アラートサービスとテイクダウンサービスによって、新たに発見された問題を直ちに通知し、減災対策をテイクダウンサービスという形で提供します。問題の初期発生時に警戒を促すために、フラッシュアラートと、その続報となる詳しいフラッシュレポートによって、見つかったブランドリスクについて具体的な詳細を知らせます。テイクダウンサービスはリスクを軽減するために、問題を起こしているアカウント、Web サイト、モバイルアプリに対処することができます。

## 組織の各部門の働きに関する知見

会社のブランドに対するリスクを理解することは、会社全体の多くの部門にとって利益になります。影響を受ける部門がリスクに備えられるようにするために、マーケティング、法務、カスタマーサポート、および他の部門への影響を理解することが重要です。各部門に必要な知見には以下のようなものがあります。

- **CLO**：会社に長期的な悪影響を及ぼす可能性がある法務上の潜在的リスクについて知る
- **CMO**：ブランドの潜在的なリスクや毀損について知り、マーケティングを活用して被害対策を実施する
- **CIO**：会社のデジタル資産や情報に対するこれらの追加リスクについて知る
- **リスク/コンプライアンス**：世界の国や地域ごとに異なる潜在的なコンプライアンスの課題に対処する
- **合併と買収 (M&A)**：新たに買収したブランドの潜在的リスクについて知る



## FortiRecon によるデジタルリスクからの保護

FortiRecon BP は、FortiRecon EASM (External Attack Surface Management : 外部攻撃対象領域管理) とともに、あるいは EASM および FortiRecon ACI の両方とともにライセンス契約できます。FortiRecon BP、EASM、ACI が付属する FortiRecon の総合ソリューションには、以下の機能が含まれます。

- デジタル資産の検出、アンダーグラウンドや公開フォーラムでの情報漏洩の検知、迅速な対処を可能にする早期警告などを含む幅広い機能
- アカウント、Web サイト、不正モバイルアプリケーションのテイクダウンサービス
- サイバーリスクをより広範に可視化できる柔軟なライセンス
- エグゼクティブレベルからテクニカルレベルまでのセキュリティスタッフが、直観的なグラフィカルユーザーインターフェース (GUI) を通じて 24 時間 365 日情報にアクセスできる
- 脅威とインシデントに関する専門知識の提供 (FortiRecon アナリストによる追加の解析からインシデントレスポンス / 評価サービスまで)

## フォーティネットによる包括的なセキュリティとサービスの提供

フォーティネット セキュリティ ファブリックは、FortiGuard 脅威インテリジェンスによる最新の保護を活用することで、攻撃ライフサイクルのあらゆる段階でエンドツーエンドのセキュリティを実現します。FortiGuard Labs 脅威リサーチチームは、オンデマンドの分析、評価、対策サービス、訓練も提供しており、豊富な知識と経験を活用して、世界中の数十億の脅威イベントを収集して分析し、関連性を特定します。これらの豊富な専門知識、経験あるダークウェブの研究者、多言語のインテリジェンス収集、HUMINT（ヒューマンインテリジェンス）のスペシャリストが協力してサービスを提供することにより、限定フォーラムや招待制フォーラムを含む最新の脅威活動に関する脅威インテリジェンスやデータへの比類ないアクセスが可能になります。生成される FortiRecon レポートのほぼ4分の1は、このサービスで収集されたヒューマンインテリジェンスのみに基づくものであり、リスクの最も現実的なビューを提供します。

### 終わりに

FortiRecon BP は、フォーティネット セキュリティ ファブリックの拡張機能として、攻撃ライフサイクルの初期段階での保護を可能にし、ネットワークにすでに採用されているセキュリティ対策の上位に、ブランド固有のリスクの可視化と修復を追加します。FortiRecon の詳細については、当社の [Web サイト](#)をご覧ください。

### ブランド保護の主な利点

- ブランドに対する潜在的リスクの回避
- ブランドに対する法務上のリスク、コンプライアンス上のリスク、および関連リスクに迅速に対処
- お客様のリスクと信頼喪失を最小限に抑制
- 幅広い市場で会社の評判を保護
- 競争力を維持

<sup>1</sup> [What is Digital Risk Protection and do you need it?]、British Assessment Bureau、2021年11月29日（英語）：  
<https://www.british-assessment.co.uk/insights/what-is-digital-risk-protection-and-do-you-need-it/>



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](http://www.fortinet.com/jp/contact)

お問い合わせ