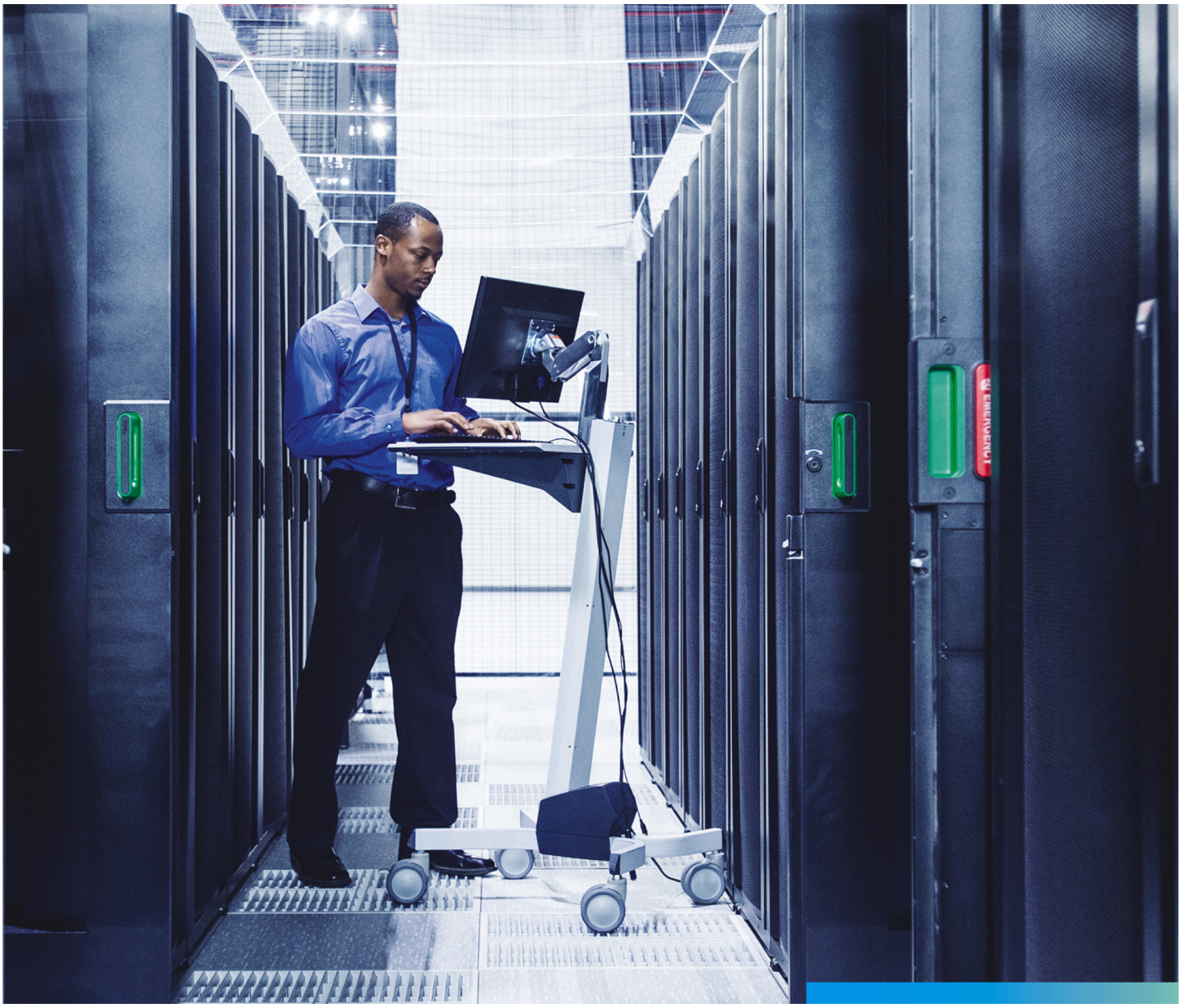

カタログ

セキュリティ

Fortify on Demand 動的アプリケーションセキュリティテスト

MICRO FOCUS

動的アプリケーション セキュリティテスト

Fortify on Demandはアプリケーションセキュリティをサービスとして提供し、ソフトウェアセキュリティ保証プログラムを簡単に実施するために、セキュリティテスト、脆弱性管理、セキュリティトレーニングなどが利用できます。Fortify on Demandは、DevOpsのスピードで開発者への継続的なフィードバックを行い、開発ツールチェーンと統合したスケーラブルな**セキュリティテスト**、**継続的なモニタリング機能**を備え、**セキュア開発**をサポートします。

ソフトウェア開発ライフサイクル全体を通じたアプリケーションの保護

組織は、アプリケーションポートフォリオの急速な規模の拡大と複雑化に直面しています。お客様がビジネスを継続する上で、リスクや脆弱性からアプリケーションを保護することは、必要不可欠になっています。ソフトウェアセキュリティ保証プログラムを成功させるには、ソフトウェア開発ライフサイクル (SDLC) のすべてのフェーズでアプリケーションを保護する必要があります。アプリケーションのセキュリティ保護は、コードの開発段階から始まります。その後、テストを通じてアプリケーションのセキュリティを検証し、アプリケーションの本番稼動後も継続して監視を行います。SDLC全体にアプリケーションセキュリティプログラムを組み込むことで、ポリシーの遂行、コンプライアンス、そしてセキュアなソフトウェアの実行を最もコスト効率に優れた形で実現できることが実証されています。しかし、ソフトウェア開発ライフサイクル (SDLC) にアプリケーションセキュリティを組み込んでいるエンタープライズセキュリティアーキテクトは、20%に満たない状況です。[1] 動的アプリケーションセキュリティテスト (DAST) は、品質保証 (QA) フェーズでソフトウェアの脆弱性を発見するのに不可欠です。また、Fortify on Demand DASTサービスを利用すると、本番稼動後のアプリケーションを継続して監視することもできます。

---

1 HPE「Application Security & DevOps」— 2016年10月

ソフトウェアセキュリティに不可欠なFortify on Demandの動的評価

Fortify on Demandの動的評価は、ソースコードの静的アプリケーションセキュリティテストを補完するもので、実際の本番環境や再現された本番環境でしか検出できない脆弱性を発見するのに役立ちます。動的テストでしか検出されない脆弱性には、構成に関連する脆弱性、高度なハッキング手法、およびアプリケーションのビジネスロジックを対象とした特定の攻撃経路などがあります。当社の動的評価では、実際のハッキング手法を再現することで、潜在的な脆弱性を発見して切り分けることができます。Fortify on Demandの動的評価は、オプションの継続的アプリケーション監視ソリューションを使用して、実際に動いている本番環境に組み込むこともできます。

Fortify on Demandの動的アプリケーションセキュリティテスト (DAST) 評価の特長は、以下のとおりです。

- 実際のハッキング手法とターゲットアプリケーションに対する攻撃を再現
- 複雑なWebアプリケーションやWebサービスの包括的なセキュリティ分析
- 攻撃対象領域をくまなくクローリングして、悪用される可能性のある脆弱性を発見
- サイト間VPNまたはFortify on Demandの正式なデータセンター IPアドレスのホワイトリスト登録を介して内部アプリケーションをテスト

当社のDASTテクノロジーは、Webアプリケーション、Webサービス、およびモバイルブラウザー向けに最適化されたアプリケーションをサポートしています。Fortify on DemandのDAST評価のユニークな点は、**WebInspectの自動テスト、手動分析、オプションのアクティブIAST、**および**継続的アプリケーション監視**という4つの基本的なコンポーネントが統合されていることです。

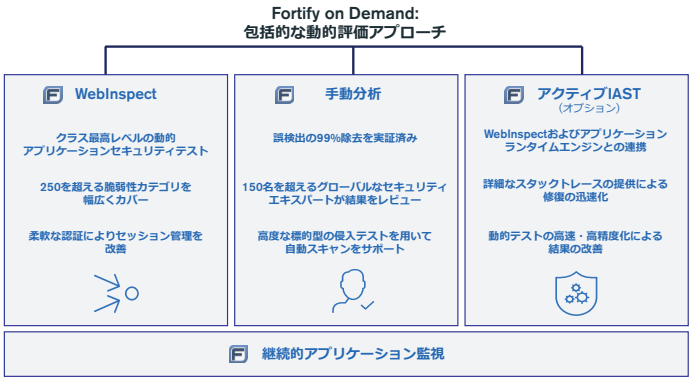

図1: Fortify on Demand: 包括的な動的評価アプローチ

WebInspectの最先端のDAST機能を活用

WebInspectは、Fortify on Demand DASTの基礎となるテクノロジーで、業界をリードする動的Webアプリケーションセキュリティ評価ソリューションです。WebInspectでは、今日の複雑なWebアプリケーションやWebサービスのセキュリティ上の脆弱性を詳細に分析できます。Fortify on Demandでは、QA、ステージング、および本番環境を通じて、すべてのWebアプリケーションとWebサービスの潜在的な脅威を検出できます。

WebInspectの主な機能は、以下のとおりです。

- 250を超える独自の脆弱性カテゴリをカバー
- スキャンの自動スケジュール設定およびスキャンブラックアウト期間中のスキャンの一時停止と再開のビルトインサポートにより、時間とリソースを節約
- 柔軟な認証によるセッション管理の改善 (特に複雑なアプリケーションの場合)
- 幅広いクライアント側言語のサポート (HTML5、Flash、JavaScriptなど)
- ほぼすべてのサーバー側言語をカバーする言語に依存しないスキャンテクノロジー
- シングルページアプリケーション (SPA) およびWebサービスでの評価が可能

当社の専任のアプリケーションセキュリティエキスパートが、スキャン結果を手動で分析

Fortify on Demandは、お客様の社内アプリケーションセキュリティチームの拡張として機能します。当社は企業が新規アプリケーションの開発に、少なからぬ時間とコストを投じていることを理解しています。また、企業には、広範囲にわたるレポートを精査して、スキャンカバレッジの検証や誤検出の除去を行うのに必要な時間やノウハウが十分に揃っていないかもしれません。Fortify on Demandでは、すぐに利用可能な結果を提供するため、一歩踏み込んだ対応として、150名を超えるグローバルなセキュリティエキスパートで構成される専任チームが、すべての動的スキャンの結果を手動でレビューします。これには、切り分けや誤検出の除去も含まれます。Fortify on Demandテストチームが行うタスクには、以下のような内容が含まれます。

- 認証用のマクロの開発 (必要な場合)
- スキャンカバレッジの検証
- 手動の監査と自動監査を集約して誤検出を99%以上除去 ― 修復に要する時間とリソースを節約

また、当社のチームは、Fortify on Demandのテスト手法を使用し、最大8時間にわたり対象のWebアプリケーションやWebサービスを手動で分析し、高度な標的型の侵入テストを用いてWebInspectのスキャン結果を補強することもできます。当社のエキスパートは、アプリケーションの認証方式、セッション管理、アクセス制御を詳細に調べ、ロジックの不備や開発者の誤った想定の有無を調査します。このように手動で分析を行うことで、以下のような自動検出できない脆弱性を見つけることができます。

- ユーザーアカウントの収集が可能
- 多段階認証の迂回
- パスワードリセットの不備
- 他のユーザーのデータまたは機密コンテンツへのアクセス
- 横方向または上下方向の権限のエスカレーション
- ショッピングカートの支払いなどの重要なトランザクションステップの省略
- 割引またはビジネス制限規定の悪用
- 開発者の誤った想定によるビジネスロジックの不備

動的評価を強化するためのアクティブIASTオプション

お客様がアプリケーションセキュリティソリューションとしてFortifyを選ぶ理由に、イノベーションとリーダーシップがあります。当社がFortify on Demandのお客様に対して、動的評価時に**アクティブIAST (対話型アプリケーションセキュリティテスト) エージェント**を統合できるオプションを提供しているのもその一例です。IASTエージェントはアプリケーションランタイムサーバーにインストールされ、Fortify on Demandの動的評価時にWebInspectと自動的に同期して機能します。IASTエージェントの主な利点は、以下のとおりです。

- カバレッジの改善 (攻撃対象領域となるすべての主要コンポーネントをテスト)
- 精度の向上 (誤検出の減少)
- 迅速な修復 (詳細なスタックトレースの提供により個々の問題を識別)

継続的アプリケーション監視による本番環境でのアプリケーションの保護

リリース前の包括的なセキュリティテストに加えて、Fortify on Demandの継続的アプリケーション監視を利用すると、本番稼動後のアプリケーションの常に変化するリスクに関する有益な情報を得ることができます。継続的アプリケーション監視は、本番環境に影響を与えない軽量の動的脆弱性スキャンとアプリケーションのリスクプロファイルを組み合わせることで、リスクに関連する状況の変化を通知します。自動化された非認証スキャンが、1週間単位で実行されます。このスキャンでは、OWASP Top 10の最も一般的な脆弱性と重大な脆弱性、およびいずれかのタイミングで本番環境に持ち込まれた (本番稼動前のテストで捕捉できていない) 構成の脆弱性に重点が置かれます。各スキャンに含まれるリスクプロファイル評価では、以下のような、攻撃対象となりやすい特徴や社内コンプライアンス要件の検査が行われます。

- 個人識別情報 (PII) の収集
- Eコマースの機能
- 認証方式および制限されたコンテンツ
- アプリケーションスタックのWebテクノロジー (アプリケーションサーバー、JavaScriptライブラリなど)

柔軟な動的評価サービスオプション

Fortify on Demandの動的評価は、アプリケーションセキュリティ目標に応じた2つのサービスレベルで提供されます。どちらのサービスレベルも、サブスクリプションまたはシングルスキャンとして購入できます。サブスクリプションパッケージでは、12か月の期間で回数制限なしにアプリケーションをスキャンできます。サブスクリプションでは、継続的な動的アプリケーションセキュリティテストプログラムの継続的なサポートが提供されます。

どちらのサービスオプションが適しているかは、アプリケーションのリスクレベルによって異なります。

1. **Fortify on Demandの動的評価サブスクリプション**は、すでにデプロイされている比較的リスクの低いアプリケーションや、ビジネスクリティカルとまでは言えないアプリケーションに最適です。動的評価は、より自動化された形で管理でき、サブスクリプション期間の間、繰り返し行われるリリースや新しい機能強化の際にセキュリティテストを行うことができます。
2. **Fortify on Demandの動的+評価サブスクリプション**は、ビジネスクリティカルなリスクの高いアプリケーションに最適です。特に、PIIを収集するアプリケーションや金融取引を処理するアプリケーションでは、潜在的なすべての脆弱性を見つけるのに、Fortify on Demandチームによる追加の手動分析が不可欠になっています。アプリケーションがセキュリティ被害を受けた場合の潜在的なリスクが高いほど、手動テストや分析の必要性も高くなります。

ライフサイクルやコンプライアンス要件が限定されたアプリケーションでは、シングルスキャンの方が望ましいこともあります。シングルスキャンには、フルスキャンを行って早期に報告された脆弱性に対する修正を検証するための修復スキャンも含まれます。修復スキャンは、最初の評価から30日以内に行う必要があります。影響の大きな手動テストを伴うWebサービスアプリケーションテストは、シングルスキャンとしてのみ利用できます (サブスクリプションでは利用できません)。

比較: Fortify on Demandの「動的」および「動的+」評価サービスサブスクリプションの比較

	Fortify on Demandの動的評価	Fortify on Demandの動的+評価
アプリケーションタイプ	Webサイト	WebサイトまたはWebサービス
WebInspect DAST	○	○
認証	○	○
セキュリティエキスパートによるレビュー (誤判定の除去を含む)	○	○
継続的アプリケーション監視 (サブスクリプションのみ)	○	○
アクティブIAST	オプション	オプション
手動脆弱性テスト	×	○

Fortify on Demandが提供する完全な動的スキャンソリューション

Fortify on Demandのサービス型アプリケーションセキュリティを利用すると、完全なソフトウェアセキュリティ保証を実現できます。脆弱性の悪用を防ぐには、SDLC全体を通じてアプリケーションのテストと監視を行うことが不可欠です。当社の動的評価では、従来のDASTにとどまらない幅広い機能が利用できます。今日の脅威に対処してビジネスを確実に保護するには、多角的なアプローチが必要です。以下のすべてに対応しているのは、Fortify on Demandだけです。

- WebInspectを活用した包括的な動的アプリケーションセキュリティテスト
- グローバルな150名を超えるセキュリティエキスパートで構成されるチームによる広範なスキャン結果の手動レビュー
- アクティブIASTやランタイムアプリケーションセルフプロテクション(RASP: Fortify Application Defender) などの先端テクノロジー
- 本番環境でのリスク評価プロファイルおよび継続的スキャンによるアプリケーションの継続的監視

では始めましょう!

Fortifyでは、ランタイムのアプリケーション監視に加え、業界で最も幅広い静的および動的アプリケーションセキュリティテストテクノロジーが利用できます。その高い品質は、業界をリードするセキュリティ調査によって裏打ちされています。

詳細情報

www.microfocus.com/fod

マイクロフォーカスエンタープライズ株式会社
jp-info-enterprise@microfocus.com

www.microfocus-enterprise.co.jp

www.microfocus.com