カタログ

セキュリティ

Fortify on Demand モバイルアプリケーション セキュリティテスト

MICRO FOCUS

モバイルアプリケーション 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モバイル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。モバイルアプリケーションセキュリティテスト (MAST) は、開発、品質保証 (QA)、および本番稼動の各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。

開発および本番環境でのモバイルアプリケーションの保護

世界中には何十億という数のモバイルアプリケーションが存在し、その数はIoT (モノのインターネット) の出現によってさらに急増を続けています。安全でないモバイルアプリケーションの蔓延は、企業や個人にとって脅威となります。より多くのアプリケーションを短期間で開発するよう求める圧力は、一層強いものになりつつあります。Fortify on Demandのモバイルアプリケーションセキュリティテストは、幅広いモバイルアプリケーションセキュリティテスト手法に対応し、スピードと使いやすさを兼ね備えたソリューションです。Fortify on Demandは、クラウドベースのサービスとして、モバイル攻撃対象領域での脅威に幅広く対応できます。また、ソフトウェア開発ライフサイクル (SDLC) から本番環境までを通して、アプリケーションを常にセキュアに維持するのに役立つ専門知識も提供されます。当社は、お客様がイノベーションに専念できるように、アプリケーションセキュリティのあらゆる課題に対処する専門知識、ツール、およびトレーニングを提供しています。

あらゆるモバイル攻撃経路を対象としたアプリケーションセキュリティテスト

Fortify on Demandのモバイル評価は、多くの場合、統合フェーズとテストフェーズで行われます。これは、開発の早い段階でクライアントやサーバーのソースコードに対するFortify on Demandの静的評価を補完するものです。Webアプリケーションの動的テストと同様に、Fortify on Demandのモバイル評価では、コンパイル済みのアプリケーションバイナリを使用して実行時の攻撃を再現します。Fortify on Demandのモバイルセキュリティ評価に対するアプローチは、単純な挙動分析やレピュテーション分析にとどまらず、テクノロジースタック全体 (クライアント、ネットワーク、サーバー) をカバーしており、300を超える独自の脆弱性カテゴリを識別することができます。このアプローチは、1つのコンポーネント (クライアントなど) で発見された脆弱性を別のコンポーネント (サーバー) のテスト時にも使用できる包括的なアプローチで、ハッカーが用いる手口と同様の複合的な攻撃経路を明らかにすることができます。Fortify on Demandのお客様が行う作業は、モバイルアプリケーションバイナリ (iOSの場合はIPAファイル、Androidの場合はAPKファイル) をFortify on Demandポータルに提供することだけです。

クライアント、ネットワーク、およびサーバーコンポーネントをカバーする Fortify on Demandモバイルアプリケーションセキュリティテスト

図1: クライアント、ネットワーク、およびサーバーコンポーネントをカバーするFortify on Demandのモバイルアプリケーションセキュリティテスト

モバイルアプリケーションバイナリの自動評価を数分で実行

多くの場合、モバイル開発者はモバイルバイナリのセキュリティを堅牢にしていません。Fortify on Demandは、独自のフレームワークを用いてモバイルアプリケーションバイナリファイルをスキャンし、数分で問題点を検出します。モバイルバイナリをFortify on Demandにアップロードすると、自動的にスキャンが実行され、パッキングやプライバシーの問題の確認、エンドポイントURLのレピュテーション分析が行われます。Fortify on Demandのモバイルバイナリ分析は、以下のような、モバイルアプリケーションパッケージ内に組み込まれた脆弱性を発見するのに役立ちます。

- ハードコードされた機密情報
- 弱いコード署名証明書
- 弱いSSL証明書
- 既知の脆弱性を含むライブラリ
- セキュリティオプションの不適切な設定 (アプリケーションのトランスポートセキュリティの無効化)
- レピュテーションに疑問のあるWebエンドポイント

WebInspectでの業界をリードするWebサービスの評価

Fortify WebInspectは、業界をリードする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、今日の複雑なWebアプリケーション、モバイルアプリケーション、および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。WebInspectでは、ブラックボックスセキュリティテストテクノロジーでは検出されないことの多いリスクを含めて、どのAppSecプロバイダーよりも多くのWebアプリケーション環境で、多くの脆弱性を検出できます。

Fortify on Demandは、WebInspectのモバイルスキャンを利用して、モバイルアプリケーションのバックエンドコンポーネントでWebに関する脆弱性を検出します。

Fortify on DemandのモバイルデバイスのWebスキャンでは、最初に物理的なAndroidまたはiOSデバイス上でモバイルアプリケーションを実行し、WebInspectでバックエンドのWebトラフィックを記録して、Web分析に取り込むホストとRESTfulエンドポイントを識別します。その後、Fortify WebInspectを使用して、指定されたワークフローの脆弱性をスキャンします。

WebInspectの主な機能は、以下のとおりです。

- 300を超える独自の脆弱性カテゴリをカバー
- 高度なモバイルマクロ記録と柔軟な認証処理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)
- 必要な認証レベル (なし、VPN、ホワイトリスト、多要素) に基づいた内部および外部向けWebアプリケーションに対応
- ネイティブのモバイルアプリケーションデバイススキャン
- 幅広いクライアント側言語のサポート (HTML5、Flash、JavaScriptなど)
- ほぼ全てのサーバーサイドで使われる言語をカバー (HTTP/ネイティブ、XML、PHP、Visual Basic、C++、JavaScriptおよびJSP、Python、Ruby on Rails、JSON、.Net、AJAX)
- スキャンブラックアウト期間のビルトインサポートによる評価時の時間とリソースの節約
- XMLデータエクスポートファイルパッチを介した、Imperva、F5、Citrix、Barracuda、Radware、およびFortinetなどの主要なWebアプリケーションファイアウォール (WAF) との統合の簡素化

すべての攻撃経路を対象とした複雑な脆弱性に対する手動セキュリティテスト

Fortify on Demandのモバイル+評価の手動テストでは、モバイルセキュリティテストのエキスパートが、Fortify on Demandのテスト手法を用いて対象のモバイルアプリケーションとバックエンドWebトラフィックを最大8時間にわたり手動で分析します。このエキスパートによる手動分析は、実際のデバイス上で行われます。そのため、実際の実行時のコンテキストでアプリケーションを分析することができます。このセキュリティテストでは、アプリケーションを実際に実行し、Webトラフィックを取り込み、実行状況を観察します。この分析には、アプリケーションのバイナリの手動検査、高度なWebアプリケーションテスト、およびデバイス上/ランタイムの問題に関する挙動分析などが含まれます。Fortify on Demandのモバイルセキュリティエキスパートがモバイルアプリケーションを手動で操作することで、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。

- デバイス上に安全ではない形で保管された機微な情報 (パスワード、クレジットカード番号、APIトークンなど)
- 安全でないアプリケーションインタラクション (安全でないIntentやアプリケーションで登録されたURLスキームなど)

- ユーザーアカウントの収集が可能およびその他の認証の不備
- 横方向または上下方向の権限のエスカレーションを通じた他のユーザーのデータや機密コンテンツへのアクセス
- アプリケーションの意図しない開発、デバッグ、または管理領域へのアクセスが可能
- 開発者の誤った想定によるビジネスロジックの不備

Fortify On Demandの柔軟なライセンスモデル

Fortify on Demandのモバイル評価は、アプリケーションセキュリティ目標に応じた2つのライセンスモデルで提供されます。お客様は、リスクプロファイル、AppSecの成熟度、開発頻度、コンプライアンス要件などの要因に基づいて、アプリケーションごとにこれらのモデルを組み合わせて使用できます。大半のお客様は、期間内にアプリケーションの評価を回数制限なしに実行できるサブスクリプションを選択しています。

1. **Fortify on Demandのモバイル評価サブスクリプション**は、自動化、スピード、アジリティを実現するために最適化された、成熟度の高いAppSec環境やDevOps環境に最適です。「モバイル」のサービスレベルでは、ユーザーが当社のセキュリティエキスパートによる手動レビューか、数分で完了する完全自動スキャンかを選択できます。大半のお客様は、最初のオンボーディング評価ではエキスパートレビューを使用し、その後の継続的インテグレーションおよび継続的デプロイメント(CI/CD)ツールとの統合では自動のモバイル評価を使用します。
2. **Fortify on Demandのモバイル+評価サブスクリプション**には、モバイルバイナリ評価の他に、バックエンドWebサービスのWebInspect DAST評価と追加の手動テストが含まれます。自動スキャンソリューションでは利用できないFortifyのエキスパートによる包括的なセキュリティレビューが提供されるため、モバイル+のサブスクリプションは、ビジネスクリティカルなモバイルアプリケーションをサポートするのに最適です。

モバイル評価およびモバイル+評価のどちらも、ライフサイクルが限定されたアプリケーションやリリース頻度の少ないアプリケーションでは、単発のシングルスキャンとしても利用できます。

モバイル評価とモバイル+評価の違い

モバイル評価およびモバイル+評価のどちらを使用しても、アプリケーションのセキュリティ状況に関する有益な分析情報を得ることができます。これらの2つのモデルの主な違いは、所要時間とモバイル+では追加で手動確認が行われる点です。以下は、モバイルとモバイル+を簡単に比較したものです。

	Fortify on Demandのモバイル評価	Fortify on Demandのモバイル+評価
サポート対象プラットフォーム	iOS、Android	iOS、Android
自動バイナリ評価	○	○
エンドポイントレピュテーション分析	○	○
セキュリティエキスパートレビュー(誤検出の除去を含む)	任意指定	○
WebサービスのWebInspect DAST評価	×	○
バイナリ、ネットワーク、およびWebサービスの手動脆弱性テスト	×	○
一般的な所要時間	24時間以内(エキスパートレビューあり) 分(エキスパートレビューなし)	3～5日(エキスパートレビューあり)

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。

Fortifyアプリケーションセキュリティソリューションは、オンプレミスまたはFortify on Demandでサービスとして導入すれば、拡張性が高く、迅速な対応を可能にするアプリケーションセキュリティプログラムを構築することができ、今日の進化し続けるIT組織のニーズに応えることができます。

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