データシート
セキュリティ

Fortify on Demand

Micro Focus Fortify on Demand (FoD) はサービス型のアプリケーションセキュリティプラットフォームです。ソフトウェアセキュリティ保証プログラムを簡単に作成、改良、拡張するためのセキュリティテスト、脆弱性管理、専門知識、サポートを提供します。

図 1. Fortify on Demand：新しい SDLC 向けのアプリケーションセキュリティ

製品概要

企業のアプリケーションリスク管理

リスクを理解することは、アプリケーションセキュリティ対策の重要な第一歩です。企業は、ソフトウェア開発ライフサイクルの各ポイントで対策を講じてセキュリティを構築しなければなりません。Fortify on Demand は、安全な開発、運用前のセキュリティテスト、および本番環境モニタリングを含むプログラムの構築を支援します。完全なプログラムはこれらのすべての領域に全体的な「多層防御」を導入するものですが、セキュリティチームは任意のポイントから開始して強化することができます。

企業のアプリケーションポートフォリオは、規模においても、複雑性においても、急速に拡大しています。レガシーアプリケーションの保護や、カスタムコードとオープンソースコードの組み合わせを使用して社内で開発されたソフトウェア新規リリースの認証に加えて、外部委託した市販向けアプリケーションのセキュリティを確保することも重要です。サードパーティのコードを購入しているお客様向けに、Fortify on Demand は、ソースコードがなくてもベンダーがアプリケーションをテストして問題を解決し、購入者にレポートを発行することができる、使いやすいベンダーセキュリティ管理サービスを提供しています。

一元的なオンラインポータルにより、Fortify on Demand の使用を迅速に開始して、包括的なソフトウェアセキュリティ保証プログラムを段階的に構築することができます。ダッシュボードは、組織のアプリケーションセキュリティポートフォリオ全体に対する可視性を提供します。プログラムのリスクを表示して、重要なセキュリティ問題に早期に対処することを可能にするとともに、複数のチームやアプリケーションにわたる修正に高い優先度を設定することができます。

主な利点

セキュアな開発

開発中にアプリケーションのセキュリティ問題を早期に発見して修正することは、アプリケーションのデプロイ後の修正よりもはるかに低コストで済むため、開発者が初期段階から安全なソフトウェアを作成できるようにすることが極めて重要です。開発者が作業を行う IDE 内に完全に統合された静的評価は、開発者に迅速にフィードバックを提供します。マウスをクリックするだけで追加できるオープンソースコンポーネント分析により、既知の脆弱性のあるコンポーネントを回避することができます。コード行の詳細や修正のアドバイスを含む監査済みのスキャン結果は、セキュアなコーディングのベストプラクティスの促進に役立ちます。成熟が進んで DevOps の原則を

お客様が Fortify on Demand を選ぶ理由トップ 5

- 展開の柔軟性
- 操作が簡単
- 高品質な成果物
- スケーラビリティ
- DevSecOps 向けの設計

適用した組織では、継続的なビルドと統合パイプラインの自動的なステップとしてFortify on Demand の静的評価がソフトウェアツールチェーンに組み込まれるようになります。

セキュリティテスト

QA、テスト、またはステージング環境における実行中のアプリケーションの動的またはモバイル評価は、悪意を持つ者が使う実際のハッキングと攻撃の手法をシミュレーションします。Web アプリケーションおよび Web サービスの場合、動的評価では自動と手動のテスト法を組み合わせて使用します。アプリケーションを本番環境にデプロイする前に、アプリケーションの攻撃対象領域をクロールしてセキュリティホールとなる脆弱性を特定します。Fortify のランタイムエージェントを使用したインタラクティブアプリケーションセキュリティテスト (IAST) は、動的テストを強化し、より多くの脆弱性発見とより迅速な修正を可能にします。

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、コンパイルされたアプリケーションバイナリを使用して、自動と手動の手法を組み合わせます。クライアントデバイス、ネットワーク、バックエンドサービスで構成されるモバイルエコシステムの 3 つの層すべてで脆弱性を特定します。モバイル評価は、単なるレピュテーション分析や行動分析だけでなく、モバイルアプリケーションのセキュリティに真剣に取り組む企業に真のセキュリティテストを提供します。

本番環境のセキュリティのモニタリング

残念ながら、すべてのアプリケーションのすべての脆弱性を本番前に修正できるわけではありません。本番環境の誤った設定によって、本番前には存在しなかった問題が生じ、リリースサイクルの合間に新たなゼロデイ脆弱性が発生する可能性があります。強固な本番環境モニタリングには、脆弱性の継続的な動的評価とアプリケーションのセキュリティイベントのランタイム検出が含まれます。Fortify on Demand は、単一の統合された場所で、すべての本番アプリケーションモニタリングアクティビティを提供します。

主な特長

静的なアプリケーションセキュリティ評価

静的評価は、開発者がソース、バイナリ、バイトコードの脆弱性を特定して排除し、より安全なソフトウェアを構築するために役立ちます。Micro Focus Fortify Static Code Analyzer (SCA) による静的評価では、781 のカテゴリ、26 のプログラミング言語、100 万超の API にわたって脆弱性を検出できます。Fortify on Demand の静的評価には、当社のセキュリティエキスパートによるレビューと革新的な Fortify Scan Analytics 機械学習プラットフォームが含まれます。誤検出を排除し、全体的な品質が確保されるため、開発チームによるソフトウェアライフサイクルの初期段階での修正作業が効率的になります。Fortify on Demand は、すぐに使用できる IDE プラグイン、継続的インテグレーション / 継続的デリバリー (CI/CD)、およびバグ管理システムの統合により、お客様の既存のアジャイルプロセスや DevOps プロセスとシームレスに連携できます。

特長

- 26 以上の言語をサポート：ABAP/BSP、ActionScript、Apex、ASP.NET、C# (.NET)、C/C++、Classic ASP (VBScript)、COBOL、ColdFusion CFML、Go 言語、HTML、Java (Android を含む)、JavaScript/AJAX/Node.js、JSP、Kotlin、MXML (Flex)、Objective C/C++、PHP、PL/SQL、Python、Ruby、Scala、Swift、T-SQL、VB.NET、VBScript、Visual Basic、XML
- 最新のアプリケーション開発に適したマイクロサービスライセンスモデル
- Security Assistant によるリアルタイムの脆弱性特定
- DevOps 自動化により、ほとんどのアプリケーションで 1 時間以内にアクション可能な結果を提供

	静的	静的+
アプリケーションタイプ	Web、モバイル、またはシッククライアント	Web、モバイル、またはシッククライアント
Fortify SCA 分析	○	○
オープンソース分析	○	○
Fortify Scan Analytics 自動監査	○	○
Security Assistant	○ [1]	○ [1]
セキュリティエキスパートによる手動レビュー	△ [2]	○

1 **サブスクリプションのみ**
2 **セキュリティエキスパートによるレビューは初回のサブスクリプションスキャンのみのオプション**

オープンソースソフトウェアコンポジション評価

サードパーティのコンポーネントは多くのアプリケーションコードベースの重要な部分であるため、ソフトウェアコンポジション解析はアプリケーションセキュリティにおいて「必須」の機能です。Sonatype による Fortify on Demand のソフトウェアコンポジション解析は、単に宣言された依存関係を National Vulnerability Database (NVD) と照合するだけではありません。自然言語処理により、すべてのオープンソースプロジェクト、アドバイザリ Web サイト、Google 検索アラート、OSS インデックス、多数の脆弱性サイトに対するすへての GitHub の

コミットを動的に監視します。また、セキュリティ研究者の専任チームにより定期的に新しい脆弱性が発見され、専有データベースに追加されます。Fortify on Demand により、IDE でも CI/CD パイプラインでも静的分析とコンポジション解析が 1 か所に統合されるため、導入およびスキャンのプロセスが簡素化します。セキュリティのプロフェッショナルにも開発者にも、完全に統合された体験として、セキュリティ脆弱性とライセンスの詳細に関する総合的な部品表が提供されます。

特長

- 静的評価とソフトウェアコンポジション解析の両方に1回でコードを提供
- Java、.NET、Javascript、Pythonをサポート
- 統合された結果に基づいて、修正、レポート、分析に1つのプラットフォームを提供
- ファイル名とパッケージマニフェストだけではなく、6500万のコンポーネントのフィンガープリントを検証
- NVDデータベース単独の場合と比べて脆弱性の検出が70%増加

動的な Web アプリケーションセキュリティ評価

動的評価では、自動と手動両方の手法を使用して実際のハッキングおよび攻撃の手法を再現し、複雑な Web アプリケーションとサービスの包括的な分析を提供します。自動動的スキャンが可能な Fortify WebInspect を特徴とする Fortify on Demand は、他のプロバイダでは得られないサービスレベルのフルサービスエクスペリエンス（認証用マクロ生成を含む動的スキャン、弊社専門家診断結果レビューによる誤検知除去、全体的な品質）を提供します。手動テストは、認証、アクセス制御、入力検証、セッション管理、ビジネスロジックテストを含む、熟練したハッカーが悪用する脆弱性のタイプに重点を置いています。アプリケーションのデプロイ後は、継続的なアプリケーションモニタリングにより、OWASP Top 10 の最も重大な脆弱性とリスクプロファイルの変更検出について、安全な脆弱性スキャンを本番環境に提供します。

特長

- QA、ステージングまたは本番のWebアプリケーションについて250を超える脆弱性カテゴリを特定
- IASTランタイムエージェントによる、カバレッジ、精度、および修復のための詳細の拡張
- 本番アプリケーションの継続的アプリケーションモニタリングを含む
- 顧客向けおよび社内向けのWebサイトおよびWebサービスを評価
- すべての主要なWebアプリケーションファイアウォール(WAF)向けに仮想パッチを生成

	動的	動的+
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 [3]
Fortify WebInspect 分析	○	○
URL 検証と認証	○	○
セキュリティエキスパートによる手動レビュー	○	○
インタラクティブアプリケーションセキュリティテスト (IAST)	○	○
継続的アプリケーションモニタリング	○ [4]	○ [4]
手動脆弱性テスト	×	○

3 **シングルスキャンは Web サービスのみ。**
4 **サブスクリプションのみ。脆弱性およびリスクプロファイルスキャンを含む。ディスカバリは別売。**

モバイルアプリケーションセキュリティ評価

Fortify on Demand は、モバイルエコシステムの 3 層すべて（クライアントデバイス、ネットワーク、Web サービス）全体で、実際のモバイルアプリケーションセキュリティテストを使用して、包括的なエンドツーエンドのモバイルセキュリティを提供します。Web アプリケーションの動的テストと同様に、モバイル評価では、社内開発、外部委託、購入したものを問わず、コンパイルされたアプリケーションバイナリを使用して、ハッカーがモバイルアプリケーションの脆弱性を悪用する際と同じ手法を使用します。Fortify on Demand のモバイル評価は、単なるレピュテーション分析や行動分析だけでなく、モバイルアプリケーションのセキュリティに真剣に取り組む企業に真のセキュリティテストを提供します。

特長

- iOS および Android モバイルアプリケーションをサポート
- モバイルバイナリからバックエンドサービスまで、300 を超える脆弱性カテゴリを特定
- 行動分析とレピュテーション分析に加えて、セキュリティの脆弱性特定を重視
- ほとんどのアプリケーションで 5 分以内の自動モバイルバイナリ評価
- 物理的なデバイスに対する手動テスト

	モバイル	モバイル+
アプリケーションタイプ	モバイルバイナリ	モバイルバイナリとバックエンドサービス
脆弱性分析 (モバイルバイナリ)	○	○
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による手動レビュー	○	○
Fortify WebInspect 分析 (バックエンドサービス)	×	○
手動脆弱性テスト	×	○

評価ユニット

Fortify on Demand の静的、動的、モバイルアプリケーションセキュリティテストサービスは、評価ユニット (アセスメントユニット) を購入して引き換えることで利用できます。Fortify on Demand 評価ユニットは、1 回の評価またはアプリケーションサブスクリプションと引き換えることができる前払いのクレジットで、年間を通じて柔軟に配分することができます。評価ユニットの有効期間は 12 か月間で、個別に引き換えることができます。

評価またはサブスクリプションの各リクエストについて、1 つの評価タイプ (動的、静的またはモバイル) と 1 つの評価サービスレベルの組み合わせを選択します。アプリケーションサブスクリプションでは、12 か月間、1 つのアプリケーションについて回数の制限なく評価することができます。すべての評価には、評価から 1 か月以内に 1 回の改善検証スキャンが含まれます。

評価タイプ	1回の評価	アプリケーション サブスクリプション
静的	1 評価ユニット	4 評価ユニット
静的 +	2 評価ユニット	6 評価ユニット
動的	2 評価ユニット	6 評価ユニット
動的 +	6 評価ユニット	18 評価ユニット
モバイル	1 評価ユニット	4 評価ユニット
モバイル +	6 評価ユニット	18 評価ユニット

表 4. Fortify on Demand 評価ユニットの引き換え

セキュアな開発のためのトレーニング

ソフトウェア開発ライフサイクルに関わるすべての人を対象とした、セキュアな開発のためのトレーニングは、あらゆるアプリケーションセキュリティプログラムの要であり、組織がアプリケーションのセキュリティリスクに晒される可能性を減少するために役立ちます。ほとんどの組織は、セキュアな開発のためのトレーニングが、アプリケーションのセキュリティリスクを低減するために重要なセキュリティ対策であることを認識しています。しかし、多くの場合、トレーニングはアドホックでしか提供されていません。

Fortify on Demand では、13 のロールベースのカリキュラムに分類された 100 時間以上のアプリケーションセキュリティトレーニング教材を提供します。これらは Fortify on Demand プラットフォームを通じて管理されます。

特長

- アプリケーション開発プロセスへの参加を許可する前に、すべての開発担当者にトレーニングを義務化
- 個人の必要性に応じて適切なトレーニングを提供します。たとえば、通常の Java 開発者は安全な Java コードの開発方法について詳細なトレーニングを受ける必要があり、e コマースアプリケーションを担当する Java 開発者は、より高度なトレーニングが必要です。
- トレーニングをオンデマンドで利用可能なソリューションにすることで、スケジューリングを容易にし、開発者の生産性への影響を最小化
- 該当する場合、サードパーティを含め、開発に関わる全員にスケーラブルなソリューションを提供
- 最新のコンテンツを提供し、新しい脅威や新技術についての理解と対応を確立

お問い合わせ先:
www.microfocus.com

サポート

Fortify on Demand はセルフサービスのプラットフォームとして設計されており、コンテキストに沿ったヘルプ、ビデオチュートリアル、チャットサポートが含まれます。専門サポートチームを通じてヘルプデスクのチケットを 24 時間年中無休で発行することができます。大規模なお客様向けには、サービスの導入を促進し、お客様の成功を確約するためのテクニカルアカウントマネージャー (TAM) が含まれます。TAM はお客様の主要な連絡先となり、最初の開発チームのオンボーディングを積極的にサポートし、サポート問題を管理するとともに、定期的にサービスレビューを実施します。追加のオンサイトまたはリモートのサポートサービスは、追加料金でご利用いただけます。

Micro Focus Fortify について

Fortify は、静的および動的アプリケーションセキュリティテストのための包括的な技術に加え、ランタイムアプリケーションのモニタリング / 保護機能を備えており、いずれも業界先進のセキュリティ調査に裏打ちされています。当ソリューションは社内にデプロイすることもサービスとしてデプロイすることもできるため、今日の IT 組織の進化するニーズを満たす、拡張性に優れた機敏なソフトウェアセキュリティ保証プログラムを構築できます。

詳細情報はこちら：
www.microfocus.com/ja-jp/products/application-security-testing/overview

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

160-JA0278-003 | H | 08/20 | © 2020 Micro Focus or one of its affiliates. Micro Focus および Micro Focus ロゴは、英国、米国、およびその他の国における Micro Focus、その子会社、関連会社の商標または登録商標です。その他すべての商標は、該当する所有者に帰属します。