opentext™ | Cybersecurity

ブローシャ

Fortify on Demand (※) 静的アプリケーションセキュリティテスト

（※）Fortify on Demandは、OpenText Core Application Securityの旧名称です。

静的アプリケーション セキュリティテスト

CyberRes Fortify on Demand はサービスとして提供される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。Fortify on Demand は、DevOps のスピードに合わせて開発者のデスクトップに継続的にフィードバックし、開発ツールチェーンに組み込まれた拡張性の高いセキュリティテストにより、安全な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にわたってアプリケーションを保護

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。リスクや脆弱性からアプリケーションを保護しなければ、ビジネスやお客様を守ることはできません。ソフトウェアセキュリティ保証プログラムを成功に導くためには、ソフトウェア開発ライフサイクル (SDLC) の全段階にわたってアプリケーションを保護しなければなりません。アプリケーションのセキュリティは、コーディングの段階から始まります。テストを通じてこのコードを検証します。ソフトウェア開発ライフサイクル (SDLC) 全体にわたって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が、ポリシーの実行、コンプライアンス、および継続的な適用を確保するための最もコスト効率に優れた方法であることが実証されています。にもかかわらず、現在のアプリケーションセキュリティプログラムがすべてのアプリケーションを対象としていると回答したテクノロジーインフルエンサーや意思決定者はわずか 13% にとどまっています。[1]

Fortify on Demand：脆弱性を検出および修正するための実証済みのソリューション

Fortify on Demand は、サービスとして提供される、実証済みの包括的なアプリケーションセキュリティソリューションです。各企業のニーズやアプリケーションロードに応じて拡張できます。Fortify on Demand により、コードを自動的にスキャンし、開発工数を最大 25% 短縮できます。Fortify on Demand の静的スキャンにより、わずか数分でリスクを特定し[2]、他社製品と比べて 2 倍の数のソースコード脆弱性を検出できます。また、誤検出を最大 95% 削減してトリアージを迅速に実行できます。また、繰り返されるコードの脆弱性を最大 40% 削減できるため、本番環境のリスクを削減すると同時にアプリケーションをより迅速に開発できます。

1. 『The State of Application Security in the Enterprise』
2. Fortify の内部評価—2020 年 10 月
3. 『Continuous Delivery of Business Value with Fortify』—2017 年 6 月

Fortify on Demand の静的評価によりコードのセキュリティを初期段階から保護

Fortify on Demand により、コーディングの段階でアプリケーションのセキュリティリスクを検出して修正できます。Fortify on Demand ソリューションは統合開発環境 (IDE) に完全に統合されているため、開発者はコードの脆弱性に関するインサイトや推奨事項をコードの記述時にリアルタイムで受け取ることができます。Fortify on Demand により、開発者は最初からより優れた安全性の高いソフトウェアを構築するためのインテリジェンスを手にすることができます。Micro Focus の包括的な静的スキャン評価により、開発者は **ソースコード、バイナリコード、バイトコード**の脆弱性を特定して排除することができます。これらはすべてビジネスにおけるより安全なソフトウェアの構築に役立ちます。**Fortify Static Code Analyzer (SCA)** を搭載した Fortify on Demand の静的評価により、781 以上のカテゴリ、27 以上のプログラミング言語、100 万以上の API で脆弱性を検出できます。

Fortify on Demand は極めて包括的で柔軟な静的評価機能を備えています。アプリケーションセキュリティ担当者が求める包括的なアプリケーションリスク管理機能と、開発者が求めるスピードと使いやすさを兼ね備えています。主な特長は以下のとおりです。

- ABAP/BSP、ActionScript、Apex、ASP.NET、C# (.NET)、C/C++、Classic、ASP (VBScript)、COBOL、ColdFusion CFML、HTML、Java (Android を含む)、JavaScript/AJAXNode.js、JSP、Kotlin、MXML (Flex)、Objective C/C++、PHP、PL/SQL、Python、Ruby、Scala、Swift、T-SQL、VB.NET、VBScript、Visual Basic、XML のサポート
- アプリケーションセキュリティを既存のアジャイルプロセスまたは DevOps プロセスに迅速に統合するための開発者ツール (IDE プラグイン、ビルドサーバーや継続的インテグレーション (CI) サーバーからのコードアップロード、バグトラッカーへのネイティブ統合など)
- Sonatype によるオープンソースのコンポーネント分析による公開済みの脆弱性およびライセンスリスクの特定
- 任意のアプリケーション (Web、モバイル、シッククライアント) のソースコード、バイトコード、オブジェクトコードにわたる包括的なスキャニングカバレッジ
- 柔軟な静的評価ライセンスモデル (シングルスキャンまたはサブスクリプション)
- Fortify Security Assistant によるリアルタイムでの脆弱性の特定とレポーティング (サブスクリプションのみ)
- 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

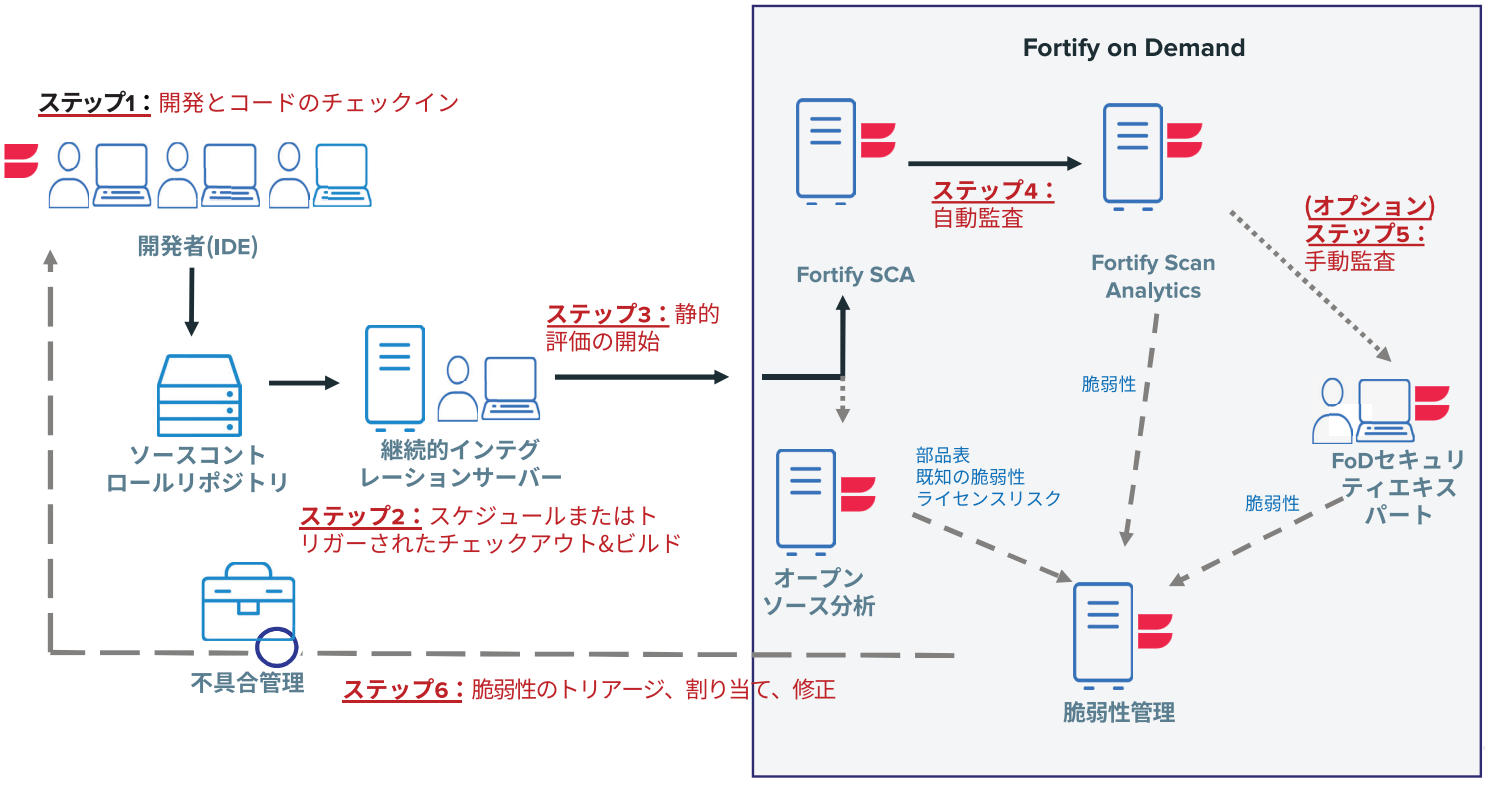

図 2. Fortify on Demand の静的アプリケーションセキュリティテストのプロセス

静的評価前 (Fortify on Demand 使用の前段階)
Fortify on Demand サブスクリプションには、DevOps のスピードとセキュリティを向上させる Fortify Security Assistant が含まれています。

Fortify Security Assistant は、コードの記述中に潜在的なセキュリティの脆弱性を開発者に通知する統合開発環境 (IDE) 内のプラグインです。Fortify Security Assistant では、特定された脆弱性を開発者が修正する方法についての推奨事項も提供します。これにより、開発者はアプリケーションのリスクを早期に把握できるほか、後の SDLC フェーズで開発者が修正に費やす時間を削減できます。

DevOps や継続的デリバリー環境において、ソフトウェアの準備が整うと、ビルドや CI サーバに渡されます。Fortify on Demand の静的評価は迅速かつ簡単に開始できます。開発者は、IDE、リポジトリ、ビルド、または CI のいずれかのサーバーから、アプリケーションのソースコード、バイナリコード、バイトコードをアップロードできます。評価対象のコードを Fortify on Demand のポータルで手動でアップロードすることも、統合エコシステムを使用して自動的にアップロードすることも可能です。

静的評価中 (Fortify on Demand 使用)
コードをアップロードすると、Fortify Static Code Analyzer (SCA) が、各アプリケーションの特性に基づいて最適な設定を選択し、アプリケーションのスキャンを即座に開始します。アプリケーションの初回送信時に、Micro Focus のセキュリティエキスパートチームが設定を調整するため、スキャンの品質を最大限まで高め、スキャンに要する時間を最小限に抑えます。最適化された設定により、開発者チームは品質を犠牲にすることなく、DevOps のスピードを達成できます。

Fortify SCA のスキャンが完了すると、Fortify Scan Analytics が優先度に従って結果を処理します。Fortify Scan Analytics は、特許申請中の機械学習技術を活用して、Fortify on Demand のエキスパートがこれまで行ってきた数百万件にも及ぶ監査関連の決定事項に基づき、最も関連性の高い脆弱性と誤検出を区別します。

新しいインテリジェンスを継続的に組み込み、予測によって大量のセキュリティ情報をわずか数秒で信頼性が高い実践的な一連の結果に変換できます。評価タイプによって、ユーザーはこれらの予測を自動的に適用して公開するか、さらにセキュリティエキスパートによる手動監査を行うかを選択します。

アプリケーションの多くはカスタムコードとオープンソースコードを組み合わせて作成されているため、静的評価にオプションでアプリケーションのオープンソース分析を含めることができます。オープンソース分析は Fortify SCA のスキャンと並行して実行されます。コードが Fortify on Demand 環境の外に出ることはありません。Sonatype のソフトウェアコンポジション分析により、各コンポーネントについて、公開されている既知の脆弱性とライセンス情報に関する部品表を取得できます。

すべての結果は、一元化された Fortify on Demand を通じて提供されます。脆弱性情報には、開発者が根本の問題を理解および修正するために必要な情報がすべて含まれています。たとえば、詳細説明、コード行、データフロー図、脆弱性の修正方法に関するガイド、修正しなかった場合の影響、コードのセキュリティを強化するためのベストプラクティスなどです。Fortify on Demand により、各チームのワークフロー (Fortify on Demand で管理されるワークフロー、またはネイティブで統合された主要な不具合管理システムで管理されるワークフロー) に修正作業を簡単に統合できます。開発チームは、主要な IDE 向けのフル機能のプラグインを使用して、トリアージ、問題の割り当て、進捗状況のトラッキング、およびコラボレーションをコーディング時にリアルタイムで実行できます。

Fortify on Demand で DevOps のセキュリティを確保

DevOps で重要なのは、新しいプロセスや組織原則を導入することだけではありません。エラーの発生しやすい、反復的なタスクを自動化し、全体的な開発効率を高めることも非常に重要です。アプリケーションのセキュリティ強化は、SDLC の作業負担や時間を増やし、DevOps モデルの妨げになるという誤解も一部に存在します。Fortify on Demand は、開発とセキュリティを一体化するために設計されたソリューションです。SDLC 内に安全なコーディングのプラクティスを確立して自動化します。

Fortify on Demand は DevOps ツールチェーンに完全統合されるため、SDLC 内での自動化と統合を推進します。開発者は、特定のリリーススケジュールか反復的なスケジュールかを問わず、またはビルドごとであっても、迅速かつ容易に SDLC にセキュリティを確立することができます。これにより、企業は AppSec プログラムの自動化、SDLC へのセキュリティの導入、本番環境のリスク削減を実現できます。現在、Fortify on Demand は、次の DevOps ツールチェーンと統合可能です。

- Eclipse、Microsoft Visual Studio、IntelliJ 開発者 IDE プラグイン
- GitHub および Atlassian Bitbucket ソースコントロールリポジトリ
- Jenkins、Microsoft Visual Studio Team Services (VSTS)/Team Foundation Server (TFS)、Bamboo、TeamCity、Travis、CircleCI を含むすべての主要ビルドおよび CI システム (ネイティブプラグインまたは Micro Focus の使いやすいユニバーサルアップロードユーティリティを使用)

- ALM Octane、Quality Center (QC)、Atlassian Jira、Microsoft VSTS/TFS、Bugzilla バグトラッキングおよび不具合管理システムを使用したアプリケーションライフサイクル管理

成熟した DevOps 環境の静的評価スキャンを数分で完了

Fortify はアプリケーションセキュリティのリーダーでもあり、イノベーターでもあります。これまで、数百もの組織と協力して、DevOps 環境におけるサービスとしてのアプリケーションセキュリティを推進してきました。成熟したセキュリティ組織は、実証済みの Fortify on Demand を活用してアプリケーションセキュリティを自動化および統合することで、静的評価を迅速に実行しています。

Fortify on Demand SCA のおおよそのスキャン時間 [4]

アプリケーションサイズ	Fortify SCA の平均スキャン時間	合計コード行数 (TLOC)
特大	12.6 時間	100 万行超
大	2.8 時間	40 万行超
中	40 分	10 万行超
小	9 分	10 万行未満

注：Fortify SCA の平均スキャン時間 (標準的なオンボーディングプロセスで新規アプリケーションの静的評価を Fortify on Demand で実行した場合)。実際のスキャン時間は、コードの構造や複雑度などの要因によって異なります。送信したアプリケーションの構造に変更があった場合は、Fortify SCA の設定を手動で再調整しなければならない場合があります。

Fortify on Demand の柔軟なライセンスモデル

Fortify on Demand 静的評価は、アプリケーションセキュリティの目的に応じて、2 つのライセンスモデルから選択できます。リスクプロファイル、アプリケーションセキュリティ成熟度、開発スケジュール、コンプライアンス要件などに基づいて、この 2 つのライセンスモデルを組み合わせて各アプリケーションに適用できます。

1. **Fortify on Demand 静的評価サブスクリプション**は、高度な自動化、スピード、機敏性を備えた、成熟したアプリケーションセキュリティ環境や DevOps 環境に最適です。オンボーディングスキャン時に当社のセキュリティエキスパートが脆弱性を手動で監査することで、高品質のベースラインを確立します。その後の自動スキャンは制限なく実行できるため、継続的な統合に最適です。
2. **Fortify on Demand 静的＋評価サブスクリプション**では、スキャンごとに手動監査を選択できます。静的＋サブスクリプションは、サブスクリプション期間中に既存アプリケーションの大幅な変更を予定している場合に最適です。また、サブスクリプション期間中にアプリケーションのベースラインを柔軟に変更したい場合にも最適です。アプリケーションセキュリティプログラムを新規に開発する場合は、誤検出の可能性を最小限に抑えながら既定のスキャンスケジュールに従ってセキュリティを強化できる、静的＋評価サブスクリプションをお勧めします。静的＋評価はビジネスクリティカルアプリケーション向けに設計されており、アプリケーションセキュリティプログラムの成熟度を問わず、あらゆる企業に適しています。財務やコンプライアンスなど、優先度の高い各種ビジネスクリティカルアプリケーションに対応しています。

Fortify on Demand では、サブスクリプションなしのアプリケーションソフトウェアセキュリティのライセンスモデルも提供されます。Fortify on Demand 単一スキャンオプションでは静的および静的＋を購入できます。これは、アプリケーションのスキャン回数が年間 2 回以下の場合、レガシーアプリケーションでコンプライアンス要件を満たす必要がある場合、または期間限定で使用するアプリケーション (業界イベントアプリやマーケティングプロモーションアプリなど) がある場合などに最適です。

4. Fortifyの内部評価—2020年10月

比較：Fortify on Demand 静的と静的 + 評価

	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
サポートするファイル	ソース、バイナリ、バイト	ソース、バイナリ、バイト
オープンソース分析	○*	○*
Fortify Static Code Analyzer	○	○
Fortify Scan Analytics	○	○
監査方法 (単一スキャン)	自動	自動 + 手動
監査方法 (サブスクリプション)	初回スキャン時は手動、その後は自動	自動 + 手動
Fortify Security Assistant (サブスクリプションのみ)	○	○

*追加の Sonatype サブスクリプションが必要

安全な開発に関するトレーニングでセキュリティを強化

Fortify はアプリケーションセキュリティに関する包括的なトレーニング、調査、インサイトを提供しています。これらのリソースには時間や場所を問わずアクセスできます。当社は、お客様にとって価値あるパートナーとなり、お客様のソフトウェアセキュリティ保証プログラムを成功に導くことを使命としています。アクセスできるリソースは次のとおりです。

- プログラマーがサイバーセキュリティに関するスキルを習得および強化するためのゲーム形式のトレーニングプラットフォーム Secure Code Warrior に Fortify on Demand からリアルタイムでアクセス
- Fortify on Demand に組み込まれたコード脆弱性の修正方法に関するガイダンスと推奨事項
- 新しいコード脆弱性の範囲、修正、知見に関する最新の Fortify Software Security Research (SSR) ルールパックの統合
- 安全なコード開発を中心とした、Fortify on Demand に関する広範なトレーニングカリキュラム

さあ始めましょう

Fortify は、静的 / 動的 / モバイルの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。

Fortify on Demand により、ソリューションをインハウスに導入することもサービスとして導入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/cyberres/application-security/fortify-on-demand

opentext™ | Cybersecurity

OpenTextグループ

jpmkt-group@opentext.com

opentext™