

Fortify on Demand

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、拡張するために必要なセキュリティテスト、脆弱性管理、専門知識、サポートをお客様に提供します。

包括的なサービスとしての AppSec

Fortify On Demand by OpenText™ を使えば、アプリケーションセキュリティプログラムに集中できます。アプリケーションのセキュリティ評価のスケジュールを設定し、ダッシュボードやレポートを通じて結果を利用するために使用される、インタラクティブな Web ベースの管理ポータルで構成されています。また、クラウドベースのマネージドサービスであるため、インフラストラクチャの維持に気を使う必要はありません。セキュリティテスト、脆弱性管理、カスタマイズされた専門知識、およびサポートなどのあらゆる利点を、インフラストラクチャやリソースの追加なしで利用できます。

- すぐに使用できる VPN ソリューション (FoD Connect) により、イントラネットアプリケーションのスキャンがより簡単になりました。
- Fortify on Demand は、SAST、SCA、DAST、IAST、MAST をサービスとして提供する唯一の AppSec プロバイダーです。
- SAST、DAST、SCA、およびモバイル評価のための統合ソリューションです。
- 評価ユニットの購入による柔軟な使用モデルです。
- 充実したサポート / オンデマンドのエキスパートが、結果の監査 / トリアージをサポートします。
- 専任のカスタマーサクセスマネージャーが AppSec プロセスを支援します。
- ソフトウェアセキュリティ調査チーム発行のルールパックを含めて、常に最新で最良の状態を維持します。
- Fortify on Demand および Debricked (Fortify のソフトウェアコンポジション分析ソリューション) は、FedRamp 認定済みです。

DevSecOps 向けの設計

現在のソフトウェアデリバリーは、DevSecOps そのものです。早期導入者から多くのユーザーに普及が広がることで、単なる統合と自動化を超えた進化が進んでいます。Fortify on Demand によれば、AppSec を「Everything-as-code」の時代に対応させて、摩擦を生じる要素からメリットを生む要素へと変えることができ、品質を犠牲にすることもありません。

- エコシステムに広範囲で統合し拡張性を提供します。
- 次世代アーキテクチャのための包括的なシフトレフトセキュリティ。
- 正確で信頼性が高く、再現性のある結果が得られます。
- リアルタイムで、一元管理されたエンタープライズグレードのレポートとダッシュボード。

エンタープライズグレードの AppSec

現在のアプリケーションセキュリティがどんな状況であっても、Fortify On Demand には、AppSec プログラムの成熟度向上、プログラム目標の達成、アプリケーションセキュリティの統合を支援する幅広い機能があり、1つのアプリケーションから数百、数千のアプリケーションに拡張できます。

- AppSec チームと開発者間のコラボレーションを促進することで確実に導入します。
- 完全な監査証跡を提供し、義務の分離や共同監査を実現します。
- 1日に1回~数千回のスキャンをサポートします。
- 現在の企業の取り組みをサポートします。
- AppSec の成功に向けて組織を強化します。
- API を介してヘッドレス AppSec プログラムを実現します。

AppSec イニシアチブを加速

Fortify on Demand を使えば、アプリケーションセキュリティイニシアチブを1日で立ち上げ、ソフトウェアセキュリティ保証プログラムを拡張し、セキュリティテスト、脆弱性管理、カスタマイズされた専門知識、およびサポートといったすべての利点を、インフラストラクチャリソースの追加なしで利用できます。

- すぐに利用開始し、迅速に拡張できます (低い導入障壁)。
- 操作と運用が容易。
- セキュリティに関する専門知識 (24 時間 365 日のテストとサポート) を利用できます。
- AppSec プログラムの成熟度を高めつつ、コアビジネスに集中できます。

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	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	+	+
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	+
オープンソース分析	+ ³	+ ³

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
3. 追加の Debricked サブスクリプションが必要

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。Fortify Static Code Analyzer (SCA) by OpenText™ により、静的評価では 29 種の言語で 100 万を超える個別の API を対象として 1166 以上の脆弱性カテゴリを検出できます。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や革新的な **Audit Assistant** 機械学習プラットフォームによるレビューを含めることもできます。誤検出を排除し、全体的な品質が確保されるため、開発チームはソフトウェアライフサイクルの初期段階で修正作業を効率的に実施できます。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 / 継続的導入 (CI/CD)、およびバグ管理システムにより、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

- 29 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、GoLang、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。
- Fortify on Demand の Security Assistant によるリアルタイムの脆弱性特定。
- DevOps の自動化により、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。

オープンソースソフトウェアコンポジション評価

多くのアプリケーションのコードベースではサードパーティ製コンポーネントが大部分を占めています。このため、ソフトウェアコンポジション解析は「必須」の AppSec 機能です。自然言語処理を使用して、すべてのオープンソースプロジェクトへの全 GitHub のコミット、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を動的にモニターします。Fortify on Demand の Software Composition Analysis は、宣言された依存関係と National Vulnerability Database (NVD) とを単純に比較するだけではありません。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、専有の知識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、完全に統合されたエクスペリエンスとして、(セキュリティ脆弱性、提言、ライセンスの詳細を含む) 総合的な明細表が提供されます。

特長

- 1回のコード提供で静的解析 (SAST) とソフトウェアコンポジション解析の両方を実施。
- Java、.NET (テクノロジー)、JavaScript、PHP、Ruby、Go、Python、Objective-C、Swift をサポート。
- 修正、レポート、分析用に1つのプラットフォームに統合された結果を提供。
- オープンソースのセキュリティ、コンプライアンス、プロジェクトの健全性を容易に自動化。
- 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	動的+
アプリケーションタイプ	Web サイトまたは API	Web サイトまたは API
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		+

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。

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。自動ダイナミックスキャンのための Fortify WebInspect 機能を備えているので、Fortify On Demand はフルサービスのエクスペリエンスを提供します。すべてのスキャンには、認証用のマクロ作成と、誤検出を排除し、全体的な品質を保証するための当社の専門家による結果の完全な監査が含まれます。これは、他のプロバイダーでは得られないレベルのサービスです。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導入後は、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知検出について、本番環境でも安全な脆弱性スキャンを提供します。

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定義。
- IAST ランタイムエージェントによってより充実したカバレッジ、精度、および修復のための詳細情報。
- 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。
- 公開および社内向けの Web サイトおよび API 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。

Fortify on Demand Connect

Web アプリケーションが社内向けの場合、Fortify on Demand を使用してサイト間 VPN をセットアップすることができます。Fortify on Demand Connect によって OpenVPN サーバー / クライアント設定が実装され、安全なサイト間接続が構築されます。OpenVPN クライアントは Docker コンテナとして使用できます。

動的 API セキュリティ評価

OpenText Cybersecurity は、次のアクティビティで構成される単一の動的 API 評価を実行します。

- Web サービス URL、および評価する Web サービスエンドポイントを記述する顧客提供の OpenAPI JSON 仕様または Postman コレクションを検証します。
- 顧客提供の OpenAPI JSON 仕様または Postman コレクションを使用して、指定された Web サービスエンドポイントの WebInspect 評価を自動的に実行します。

モバイルアプリケーションセキュリティ評価

	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		+

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、API) 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、外部委託開発、購入を問わず、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定義。
- 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 分以内に自動モバイルバイナリ評価。
- 物理的なデバイスを用いた手動テスト。

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投資を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。1 回の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、お客様が 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 か月以内の 1 回の改善検証スキャンが含まれます。

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基礎となります。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鍵となる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 は、100 時間を超えるアプリケーションセキュリティトレーニング資料を提供します。13 のロールベースのカリキュラムで構成され、Fortify On Demand プラットフォーム上で実行されます。

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ちょうど適切なトレーニングを提供。たとえば、一般の Java 開発者はセキュアな Java コードの開発方法について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 開発者に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提供することにより、スケジューリングを容易にして開発者の生産性への影響を最小化。
- 該当する場合には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。
- 新しい脅威や技術について理解と対応ができるよう、最新のコンテンツを提供。

お客様が Fortify on Demand を選ぶ主な理由

- 包括的なサービスとしての AppSec
- DevSecOps 向けの設計
- エンタープライズグレードの AppSec
- AppSec イニシアチブを促進

お問い合わせ

www.opentext.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、プラットフォームとツールの使用に関する詳細なハウツーガイドとチャットサポートを利用できるようになっています。また、専門のサポートチームに依頼できるヘルプデスクのチケットを 24 時間年中無休で発行できます。大規模なお客様向けには、サービス導入の促進とお客様の成功を支援する CSM (カスタマーサクセスマネージャー) のサポートが含まれます。CSM はお客様の主要な連絡先となり、最初の開発チームの立ち上げ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。

Fortify on Demand は 8 マルチテナント環境ですが、これはお客様それぞれに独自のテナントが与えられるということです。このテナントでは、他のすべてのテナントからアプリケーションテストデータが分離されます。お客様は、Fortify on Demand にアクセスするためにはインターネットに接続する必要があります。

Fortify について

Fortify のアプリケーションセキュリティテストポートフォリオは、DevSecOps プラクティスにおけるチームの能力を強化します。それによってクラウドトランスフォーメーションが実現し、イノベーション、サポートの提供、世界中の組織とのコラボレーションが恒常化することでソフトウェアサプライチェーンのセキュリティが確保されます。20 年以上にわたる専門知識が詰め込まれた唯一のコードセキュリティソリューションとしてあらゆる主要アナリストから市場リーダーと認められている Fortify は、適応性、正確性、拡張性にこの上なく優れた AppSec プラットフォームを提供しており、これは最新のユースケースと機能を幅広くカバーします。優れたコードとは安全なコードであると当社は確信しており、Fortify においてはすべての活動で一貫して、お客様がその目標を達成できるように支援します。

Fortify Community にはこちらからアクセスできます。アプリケーションセキュリティ製品について技術的な不明点がある場合は、Fortify のディスカッションフォーラムをご確認ください。アプリケーションセキュリティに関するヒントや情報については、こちらから最新情報をご覧ください。

詳細はこちら：

www.microfocus.com/ja-jp/cyberres/application-security/fortify-on-demand

opentext™ | Cybersecurity

OpenText Cybersecurity は、あらゆる規模の企業とパートナー様を対象に、包括的なセキュリティソリューションを提供しています。予防から検出、復旧対応、調査、コンプライアンスに至るエンドツーエンドの統合プラットフォームにより、包括的なセキュリティポートフォリオを通じてお客様のサイバーレジリエンスの構築をサポートします。コンテキストに基づくリアルタイムの脅威インテリジェンスから得られた実用的なインサイトを活用できるため、OpenText Cybersecurity のお客様は、優れた製品、コンプライアンスが確保されたエクスペリエンス、簡素化されたセキュリティというメリットによって、ビジネスリスクを管理できます。