



# Contrast Assess

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)

## 課題

- 従来の静的・動的セキュリティツールは、スピードが求められるアジャイルやDevOps環境では十分に活用出来ません。
- オープンソースのソフトウェアは、ますます不正侵入に脆弱で無防備になりつつあり、格好の攻撃対象になっています。
- ベライゾンによる年間データ漏洩の調査報告書によると、ウェブアプリケーションへの攻撃がデータ漏洩の原因となっています。
- ガートナーの調査では、漏洩の84%がアプリケーション層の脆弱性悪用が原因となっています。

## ソリューション

Contrast Assessは、ソフトウェアにエージェントをインストールし、脆弱性をアプリケーションの内部から調査し、高い精度で自動的に特定する画期的なアプリケーション・テスト・ソリューションです。

Contrast Assessは、エージェント型手法によりWEBアプリケーションやAPIの開発やテスト中に自動的に脆弱性を調査します。このセキュリティテストへのパッシブアプローチにより、多大な時間を要し、効果の低い静的セキュリティスキャンを削減します。

Contrast Assessは、現行のソフトウェア開発ライフサイクル(SDLC)プロセスとシームレスに連携し、継続的な脆弱性検査をアプリケーションポートフォリオ全体に展開出来ます。

## 特徴

弊社のモダンアプリケーションセキュリティへのユニークなアプローチは、脆弱性の検出と修復に必要なリアルタイムのインテリジェンスと継続的可視化を生み出し、誤検出や検出漏れは発生しません。



### アジャイル、DevOps、DevSecOpsとの親和性

Contrast Assessは、WEBアプリケーションやAPIの開発やテストをする開発者とインタラクティブにやり取り出来る様、設計されています。DevOpsチームは、Contrast Assessを標準のメッセージングツールやビルドツール、自動プロビジョニングシステムやSlack、Maven、Docker等のコンテナと連携して、アプリケーションに内在する脆弱性を検査し報告することができます。Contrast Assessは、自動機能テスト中にセキュリティ分析を実施しJenkinsのようなCI/CD自動化サーバと連携すれば、過剰な脆弱性が発見されたビルドを失敗させることも出来ます。



### 継続的分析

Contrast Assessは、エージェント型手法を用いて正確に脆弱性分析出来るため開発チームやQA、セキュリティチームはソフトウェアの開発やテストを実施しながらリアルタイムで脆弱性を検出できるため、修正が最も容易でコスト削減を図れるSDLCの初期に脆弱性を修復することができます。



### 高精度

従来のアプリケーションセキュリティのテストツールとは異なり、Contrast Assessはアプリケーションとそのランタイム環境に自動化と可視化機能を追加しますので開発者は直ちに対応可能な脆弱性情報を得ることが出来ます。IAST、SAST、DASTのアプリケーション・テスト・アプローチを最も効果的に組み合わせ、更にオープンソースセキュリティ分析と融合させて機能します。



### スケーラブルなアーキテクチャ

Contrast Assessは、アプリケーションの内部より脆弱性情報を調査出来るので、容易にアプリケーションポートフォリオ全体に展開出来ます。実行中アプリケーション全てに並行して脆弱性検査出来ます。

## TeamServer管理コンソール



## 主な特徴

## Contrast Assessアーキテクチャの2つの主要構成要素

- 1) アプリケーションサーバ上でアプリケーションと共に実行され脆弱性検出を行うエージェント
- 2) エージェントが特定した脆弱性を収集して報告し、管理する一元管理コンソール(TeamServer)

## 脆弱性を広範囲に網羅

Contrast Securityは、一般的なアプリケーション・セキュリティ・リスクを広範囲に網羅しており、この中にはOWASPトップ10やPCI-DSSも含まれます。

## コードレベルの修正方法をガイダンス

Contrast Securityの革新的なセキュリティ・トレース・フォーマットは、脆弱性がコードのどこに存在するか？どのように機能するか？をピンポイントで特定します。Contrast Securityは開発者が理解や実装がしやすい修正方法を提示します。

## サードパーティのコード分析

最新のアプリケーションでは、氷山と同様、コードの80%が“表面に現れず”、ライブラリやフレームワーク、その他のコンポーネントの中に潜んでいます。アプリケーションは大抵、このようなライブラリを50以上持っており、その何百万ものコード行が脆弱である可能性があります。

## アプリケーション・インベントリ

シンプルに見えて、アプリケーション・インベントリはアプリケーション・セキュリティチームにとって解決が一番厄介でもあります。企業には何百、何千というアプリケーション、マイクロサービス、APIがあって、それぞれの異なるバージョンの複数のインスタンスが開発やQA環境にあり、しかもその全てが常時変更されています。Contrast Securityは、内外のwebサービスやこれらのアプリケーションとの関わりに関する情報を追跡し、継続的に統合セキュリティインベントリと部品表にフィードし、これらを最新状態に保ち管理します。

## ライブ状態のアプリケーション・アーキテクチャ

Contrast Securityは、アプリケーションのアーキテクチャ上の主要コンポーネントの略図を自動生成します。これは、開発者が迅速に脆弱性の詳細を理解するのに役立ちます。