



TRUE SCALE APPLICATION SECURITY

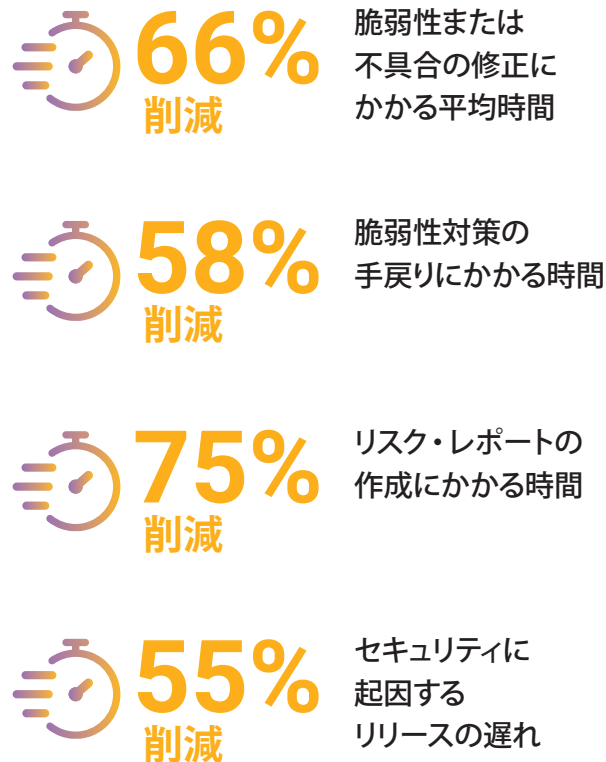
ソフトウェアの新たな時代

ソフトウェアの世界は急速に変化しています。AIの採用が急増し、その結果としてAIが生成するコードが雪崩のように押し寄せ、セキュリティに対する新たな脅威が生まれています。これと同時に、各種規制も厳しさを増しており、説明責任と透明性はビジネスを進める上での中核的な要件となっています。もはや、**ソフトウェア・セキュリティは単一の事業部門やCISOレベルだけにとどまらず、取締役会レベルの課題となっています。**高まり続けるリスクにさらされることなく、いかにビジネスのイノベーションと成長を推進していくかを、経営幹部全員が考える必要があります。

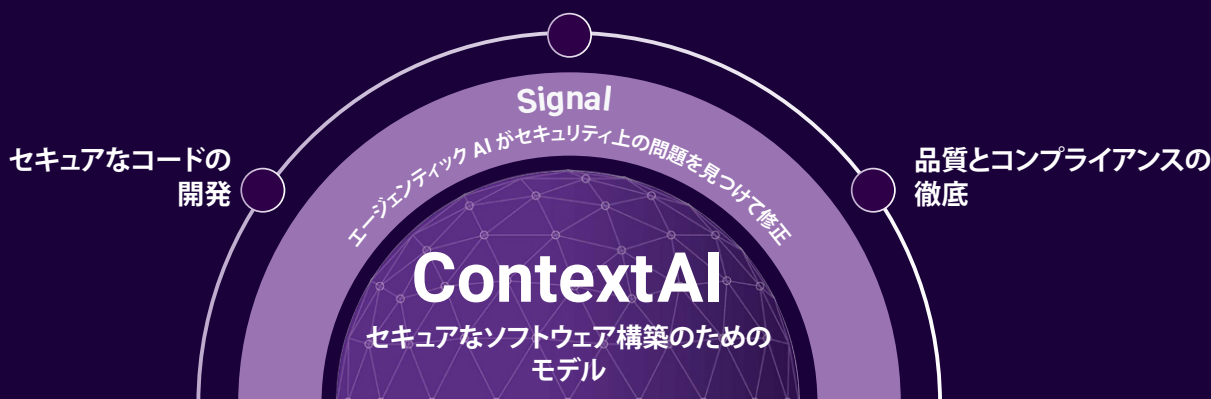
True Scale Application Security

ブラック・ダックの **True Scale Application Security** ソリューションは、セキュアなコードの開発、ソフトウェア・サプライチェーンのセキュリティ保護、およびソフトウェア製品の品質とコンプライアンスの徹底を図るための信頼できる手段として**世界中で4,000以上の組織**に採用されています。ブラック・ダックなら、開発者のエクスペリエンスかテスト結果の精度か、スキャン速度か導入の規模か、AIによる変革か規制へのコンプライアンスか、といったトレードオフの必要はありません。一切の妥協なしに大規模環境に対応できるアプリケーション・セキュリティ、それが True Scale Application Security です。

数字が物語る実績



ソフトウェア・サプライチェーンのセキュリティ保護



エンジン

SAST | SCA | DAST | コンテナ | シークレット | IaC | バイナリ | ファジング

Polaris AI AppSec プラットフォーム

ASPM | ポリシー | 解析

統合

SCM | CI/CD | IDE | リポジトリ

Signal

エージェント AI を活用したアプリケーション・セキュリティ

Black Duck Signal™ は、Claude Code や GitHub Copilot などの AI コーディング・アシスタントと連携して動作する **AI 活用型の AppSec** ソリューションで、セキュリティ上の不具合をリアルタイムに見つけて自動で修正します。LLM による解析を ContextAI™ のインテリジェンスで補強することにより、Signal は経験豊富なセキュリティ・アナリストと同じようにソフトウェアを解析できるようになっており、AI 生成コードに含まれる不具合を特定し、コードの修正を自動化すると共に、修正によって新たな問題が混入しないことも確認します。Signal には以下の利点があります。

- MCP (Model Context Protocol) によりエージェント・コーディング・ワークフローに統合
- 従来のテスト・ツールでは見つからない複雑なビジネス・ロジックのセキュリティ上の不具合を検出
- プログラミング言語の種類を問わず、あらゆるコードを迅速かつ正確に解析

Polaris

アプリケーション・セキュリティのための単一のプラットフォーム

Black Duck Polaris™ Platform は、現代の DevSecOps に最適化されたクラウド・ベース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。開発ワークフローにシームレスに統合し、リスクに優先順位を付け、スピードや精度を犠牲にすることなくポリシーへの遵守を徹底します。Polaris には以下の利点があります。

- **開発者中心のワークフローと統合。** 摩擦を起こさず効率を最大化します。
- **リスクの優先順位付けとノイズの排除。** 95% のリスクを生み出している 5% の問題に集中できます。
- **ポリシー、ガバナンス、コンプライアンス。** カスタマイズ可能なポリシーを使用し、SDLC 全体を通じてセキュリティ標準を適用します。
- **AI 駆動型のセキュリティと自動化。** リアルタイムでの問題の要約とワンクリックでの修正提案を示します。
- **深さと精度を備えた包括的なスキャン。** 業界をリードする SAST、SCA、および DAST エンジン統合しています。
- **ROI とリスク態勢を可視化して証明。** 対話型のダッシュボードとレポートにより、知見がリアルタイムに得られます。

業界をリードするソリューションを、ニーズに合わせて提供

ブラック・ダックが提供する業界で**最も包括的な一連のアプリケーション・セキュリティ・テスト・ソリューション**は、プロプライエタリ・コード、オープンソース、サードパーティの依存関係だけでなく、アプリケーションの挙動やデプロイ構成も対象として、セキュリティ、品質、およびコンプライアンスの問題を検出します。SaaS ソリューションとしてだけでなく、ホステッド環境やオンプレミス環境でも利用できるブラック・ダックのソリューションは、それぞれのカテゴリで業界リーダーとして認められています。

SAST	DAST	シークレット	バイナリ
SCA	コンテナ	IaC	ファジング

開発および DevOps との統合

ブラック・ダックは、各種の統合とセキュリティ・プラグインにより、開発スピードの低下やセキュリティ・カバレッジの妥協なしに**複雑なテクノロジー・スタックに潜むセキュリティとコンプライアンスのリスクを自動で確実に検出して軽減する仕組み**を確立します。IDE や SCM からセキュリティ・テスト、本番環境へのデプロイにまで統合することにより、リスク検出の自動化、トリアージと修正の加速、そして開発生産性の向上が実現します。

ContextAI

セキュアなソフトウェア構築に必須のモデル

ブラック・ダックのソリューションは、20年以上にわたって培ってきたセキュリティに関する知見とノウハウを凝縮した包括的なナレッジベースである ContextAI を基盤として活用しています。ContextAI によってセキュリティ・テスト結果からノイズが排除されるため、チームは AI のスピードで安心して開発に専念できます。

人間によって検証されたペタバイト級のインテリジェンスで構成される ContextAI は、数千のソースからのデータで継続的に更新および改良がなされています。これにより、開発およびセキュリティ・チーム向けに深い専門知識で AI を強化することに成功しています。



第三者機関による評価

Gartner® マジック・クアドラント™：アプリケーション・セキュリティ・テスト

ブラック・ダックは 2025 年の Gartner® Magic Quadrant™ アプリケーション・セキュリティ・テスト (AST) 分野において、8 年連続でリーダーに選出されました。Gartner が評価した 16 社の中で、6 年連続で「実行能力」において最高位を獲得しています。

Forrester Wave™ ソフトウェア・コンポジション解析

ブラック・ダックは、5 回にわたりリーダーとして評価されており、評価項目 25 のうち、コンポーネントの識別、ライセンス検出、SBOM (ソフトウェア部品表) の生成、ポリシー管理、イノベーションを含む 9 項目で最高評価を獲得しています。

ブラック・ダックについて

ブラック・ダックは、True Scale Application Security によって、モダン・ソフトウェアの経営レベルのリスクに対応し、規制された、AI を活用した世界におけるソフトウェアの信頼性を保証します。ブラック・ダックのソリューションは、セキュリティ、規制、ライセンスに関するリスクを排除しつつ、組織のスピード、精度、コンプライアンスのトレードオフから解放します。クラウドでもオンプレミスでも、コードが実行されるあらゆる場所でミッション・クリティカルなソフトウェアを保護するには、ブラック・ダックこそが選択肢となるのです。ブラック・ダックを活用することで、セキュリティ・リーダーはよりスマートな意思決定を行い、自信を持ってビジネス・イノベーションを推進することができます。詳しくは、www.blackduck.com/jp をご覧ください。

©2026 Black Duck Software, Inc. All rights reserved. Black Duck® は Black Duck Software, Inc. の米国およびその他の国における登録商標です。その他の会社名および商品名は各社の商標または登録商標です。2026 年 4 月