Web アプリと API 向けの AI を活用した統合アプリケーション リスク管理

Total AppSec (TAS) - Web application Scanning & API Scanning

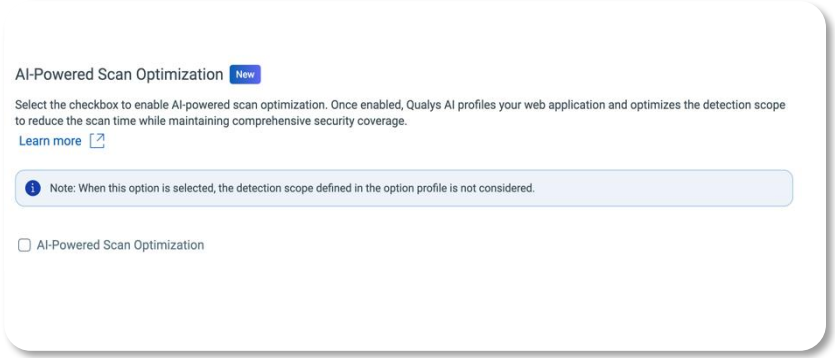
クォリスジャパン株式会社
更新日：2026年3月

*TASはLAN内のWebサーバーをスキャンする場合、VMDRライセンスとの併用が必須です。

ウェブアプリスキャンとマルウェア検出によるリスク評価

さらに、必要に応じてAIリスク評価を行う能力も備えています

- AI搭載のスキャンは**スキャン時間を半分に短縮**します
- **カスタムQID**を定義し検証します
- **AI使用を検出**し、AIコンポーネントのAIリスク評価をトリガー
- ディープラーニングスキャンによる**ゼロデイマルウェア検出**



4600+

customers

QualysのウェブアプリケーションおよびAPIリスク評価機能を信頼し利用しているユーザー数

~3300

QIDs for web apps

OWASPトップ10および機密データ漏洩チェックを含むQIDの数

~99%

Accuracy

ディープラーニングによるウェブマルウェア検出と監視の正確度

OWASP Top 10 vulnerabilities (in Web Apps)

NAME	COUNT
Injection	2341
Security Misconfiguration	1751
Broken Access Control	1711
Vulnerable and Outdated Components	686
Insecure Design	650
Cryptographic Failures	274

Qualys.

APIスキャンによるリスク評価

さらに、必要に応じてAIリスク評価を行う能力も備えています

- **OAS V3適合**のための**API検査**
- **OWASP & API Security Top 10検査**
- **TruRiskスコアによる優先順位付け**
- **「シフト・レフト」と「シフト・ライト」**のセキュリティを構築
- **AI搭載によるスキャン**で**スキャン時間を半分に短縮**

~600

QIDs for APIs

OASへの機密データ漏洩、コンプライアンスを含む、APIのOWASPトップ10のチェック

100%

Coverage

OWASPのAPIトップ10

5000+

API Endpoints tested

ローンチから最初の数四半期以内に

OWASP API Top 10 for Internet Exposed APIs

NAME	COUNT
Broken Object Property Level Authorization	472
Security Misconfiguration	369
Unrestricted Resource Consumption	178
Broken Authentication	31
Unsafe Consumption of APIs	22
Broken Object Level Authorization	14

統合ワークフローによるリスクレスポンスオーケストレーション

servicenow

Jira

GitHub

Bamboo

TeamCity

優先順位付けの自動化

優先順位付け

事業資産のコンテキスト

脆弱性検出と相関した脅威コンテキスト

トリアージの自動化

自動チケット作成

ITSMシステム内で自動的にチケットを生成し、適切なチームに割り当てて対応します

再テストの自動化

自動化されたセキュリティ検査

展開前にスキャン結果に基づく合格・不合格基準で。

Manage risk with Roc

Quc

統合資産インベントリ → リスク要因の集約 → 脅威インテリジェンス → ビジネスコンテキスト → リスク優先順位付け → リスクレスポンス・オーケストレーション

TotalAppSecへのアップグレード

新機能をフル活用する

ウェブアプリケーション
セキュリティ検査

ウェブマルウェア検出

WAS

＋

発見とインベントリ

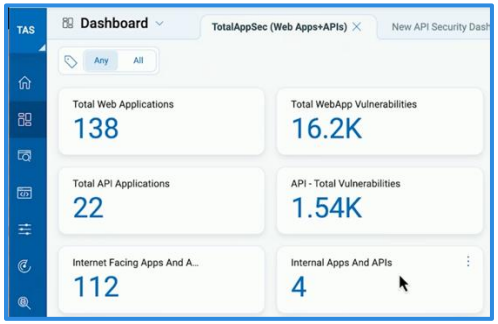
広範なAPIセキュリティ検査

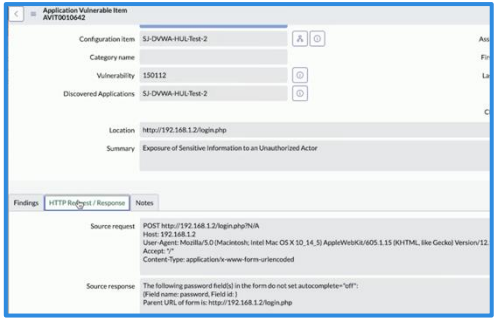
高度スキャン
AI駆動のスキャン
カスタムQID

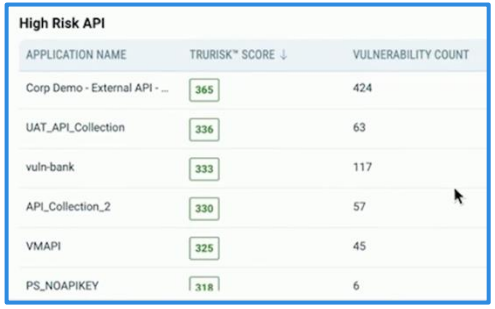
リスクオーケストレーションとレスポンス

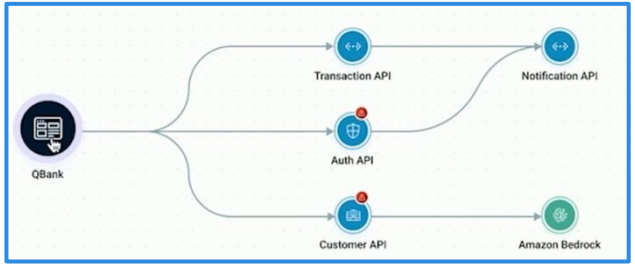
＝

TAS









AI時代におけるアプリケーションセキュリティの重要性

背景

AIの急速な普及によりアプリケーションの攻撃対象領域が拡大しています。99%のAI関連の脆弱性はAPIの欠陥に起因し、89%のAI対応のAPIが安全な認証を欠いています。アプリケーションは従来のフォーム入力から、意図駆動型のインタラクション（例：「フライト予約」「メール要約」）へ進化し、APIネットワーク化が進行しています。

AI時代のアプリケーションはAPIがネットワーク化し、セキュリティポスチャの把握が困難になっています。**TotalAppSec**は、攻撃対象領域からリスク対象領域へ視点を転換し、ノイズ・コスト・時間を削減します。**ASPM**を次のレベルへ進化させるための統合プラットフォームを提供します。

ROCによるリスク管理

ROC（Risk Operations Center）対応：リスク要因集約、脅威インテリジェンス、ビジネスコンテキストを統合し、リスク対応を自動化。

Agentic AI活用：自然言語でのAppSec管理、ヘルスチェック、設定の最適化。

スケーラブルなライセンスモデル：WebアプリとAPIに柔軟対応、SMB向け割引あり。

2026年度リリース予定！

次のTotalAppSecでは、アプリケーションセキュリティポスチャ管理（ASPM）を実現するプラットフォームへと進化します。

Manage risk with ROC

TAS(ASPM)

ASPM – アプリケーションセキュリティ

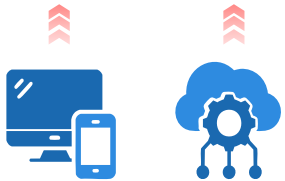
2026年リリース予定

包括的な発見 & インベントリ

- **Qualysコネクター** – VMDR、CSAM/EASM、TotalCloudなど。
- **マルチクラウド**(例:AWS、GCP、Azure、Direct Cloud APIS)
- コンテナ(例:Docker、Kubernetes、Service Mesh Arch、Istio、Kuma)
- **APIゲートウェイ**(例:Apigee、Mulesoft、AWS API Gateway)
- 外部向け/インターネット**公開資産**および**証明書**
- **サードパーティ統合**(例:Postman、Burp Suite、Swagger)
- Checkmarx、Synk、VeracodeによるSASTおよびSCA統合

リスクの測定と優先順位付け

Enterprise TruRisk™ Platform



Web Apps　APIs　Web Malware

DAST、APIテスト、AI駆動スキャン、ディープラーニングベースのウェブマルウェア検出

Prioritize with TruRisk™

リスク・オーケストレーションおよび修復

基盤となるインフラの**自動パッチ適用**

サーバー、APIエンドポイント、ホストの分離

ウェブアプリおよびAPIの**緩和**手法

DevOpsとITSM統合による**修復ワークフロー**

顧客成果

360°視界　アプリセキュリティ・ポスチャー管理　リスク優先順位付け　リスク修復

TotalAppSec:攻撃面の把握からリスク管理へ進化

ノイズやコスト、時間を削減するためにリスク管理を自動化

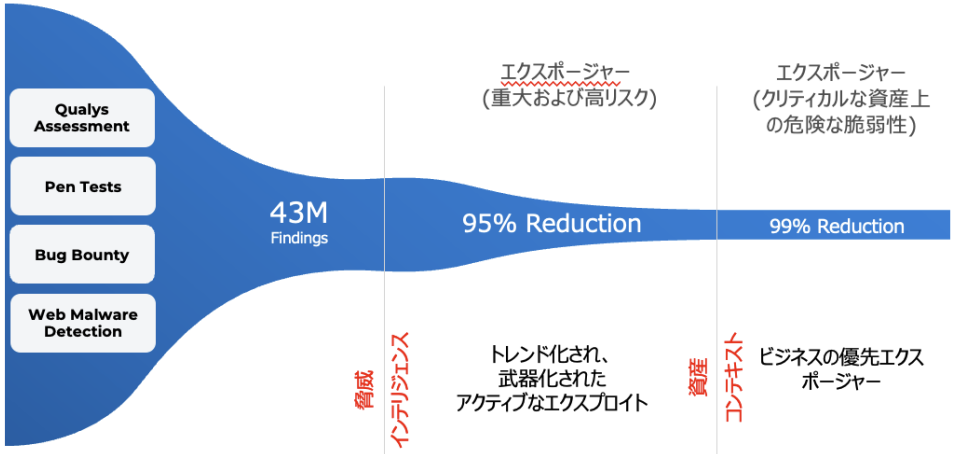
アプリケーションの全攻撃対象を可視化

包括的発見:

- ✓ クラウド環境
- ✓ APIゲートウェイ
- ✓ Webアプリケーションスキャン
- ✓ 内部およびインターネット向けスキャン

456K
Assets

多次元的なコンテキストでリスクを評価し優先順位付け



統合的修復対応

リスクへのリアルタイム自動化対応：

- ✓ TruRiskによる優先順位付け
- ✓ 自動トリアージと修正
- ✓ CI／CD統合による再テスト

1000+ 組織はローンチから1年以内に私たちを信頼してくれました

4.4*/5 Gartner Peer Insights™

4*/5 PeerSpot

Qualys.

Agentic AIでAppSecをスケールアップしましょう

サイバーリスクアシスタント

会話型AIインターフェース

自然言語クエリインターフェースでAppSecプログラムを管理

ウェブアプリを全部見せてください

全てのウェブアプリの結果を見せてください

トップの有害な組み合わせを見せてください

サイバーリスクエージェント

繰り返されるワークフローのための
デジタルコラボレーター

エージェント型AI搭載のヘルスチェック

サイバーリスクエージェントは、TotalAppSecでオンボーディングされたウェブアプリケーションやAPIを監視します。

最適かつ包括的なテストのために設定変更を推奨します

Qualys.

※*TASとETMサブスクリプションが必要*

既知および未知のウェブ資産の統合資産インベントリ

ウェブアプリケーションやAPIにおけるAI利用状況を発見する機能も含まれます

サードパーティインポート

Swagger, Postman, Burp Suites

API Gateways

Mulesoft、AWS API Gateway、Azure APIM、APIgeeのAPIを発見

トラフィック解析

トラフィック解析でAPIを発見

AI と API の発見

Discovererのスワガーファイル、API呼び出し、ウェブアプリスキャニング中のAI使用状況

ウェブアプリおよびAPI攻撃面の発見

広範囲な攻撃面の発見
既知 + 未知/忘れられた資産

インターネット露出と内部

CSAMやVMDRスキャンから、インターネット公開および内部のウェブアプリやAPIを発見

マルチクラウド環境

AWS、GCP、Azure 環境からウェブアプリケーションを発見

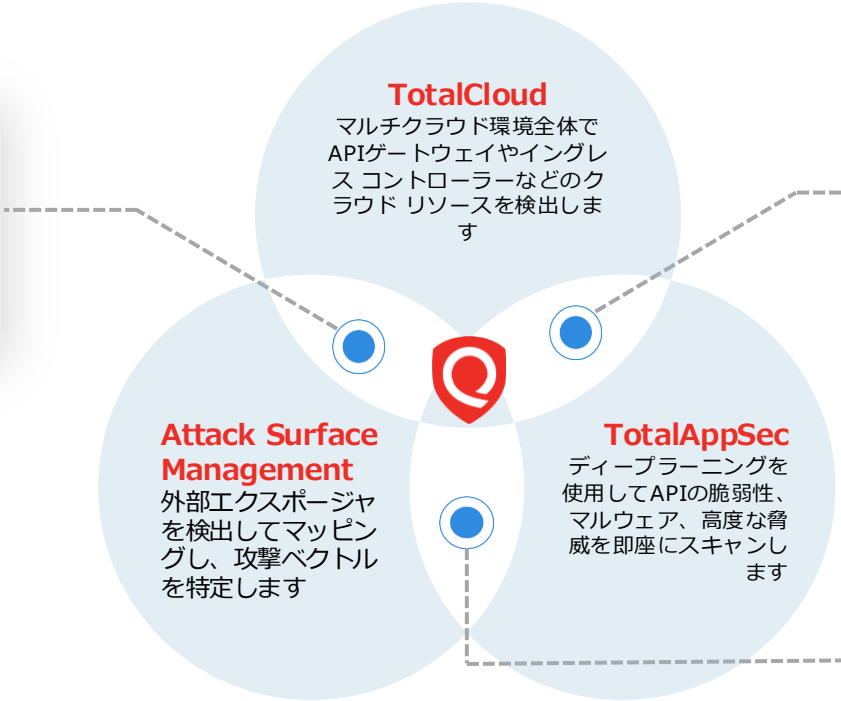
ソースコード

ソースコードからAPIを発見する

Qualys.

クラウドからAPIまでの完全なアプリケーションセキュリティ
統合された可視性、エクスポージャー、およびアクション

IT Ops、クラウド セキュリティ
マルチクラウド環境全体で、内部および外部に面したクラウド資産、API、およびシャドー IT を検出してスキャンします



クラウドセキュリティ、AppSec、 DevOps
APIゲートウェイ、イングレス コントローラー、クラウドネイティブ ワークロードの脆弱性、設定ミス、APIペイロードに挿入されたマルウェアを検出します

AppSec、IT、DevOps
インターネットに公開されたWebアプリ、API、エンドポイントを検出して、脆弱性、マルウェア、設定ミス、APIの欠陥をスキャンします

攻撃対象領域、クラウド、アプリを検出して保護する

Total AppSec 導入メリット

統合アプリケーション リスク管理 – インフラ、アプリ、API、クラウド インフラ

インフラストラクチャ、Web アプリ、クラウドにわたるアプリと API のリスクを一元化

サードパーティのツールと手動の PEN テストからの**結果を統合**する

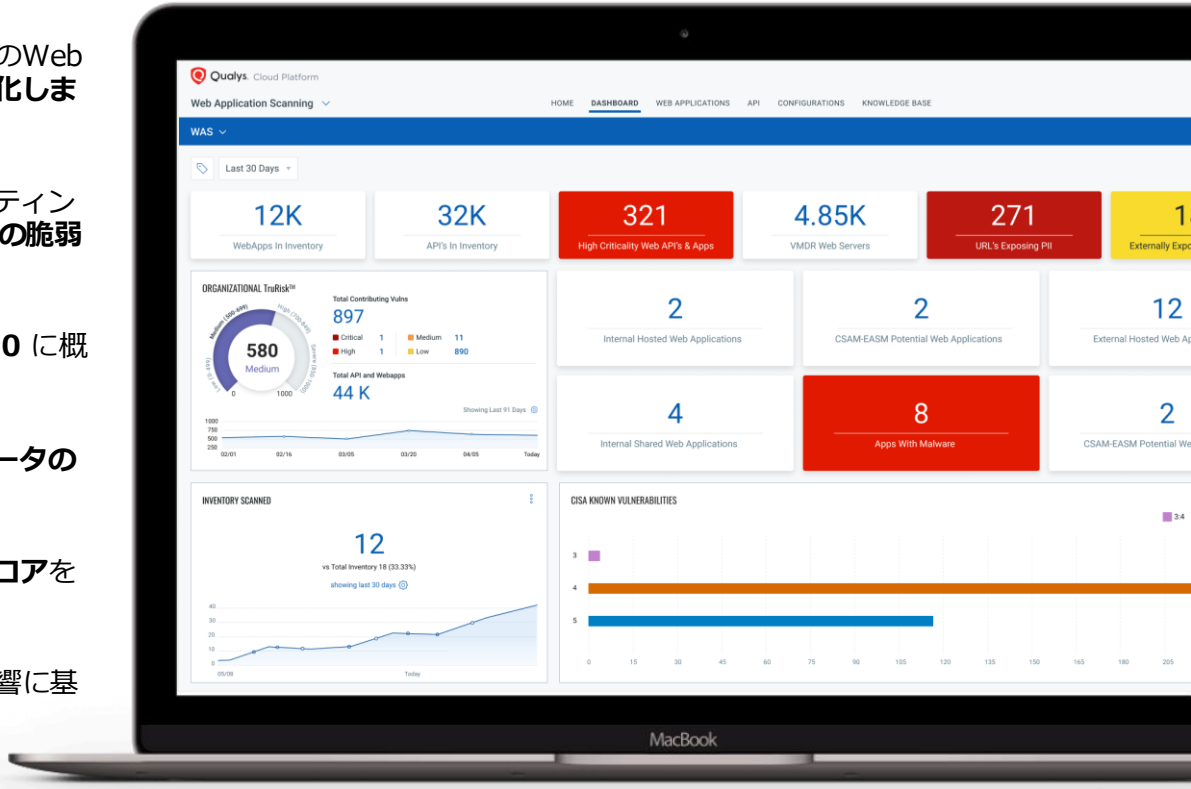
シフトレフトとシフトライトの統合ワークフローによる**リスク軽減とインシデントのトリアージ/対応の加速**

セキュリティ チームと IT チーム全体でカスタマイズされたワークフローがネイティブに統合された**一元化されたプラットフォーム**

補助資料

Webアプリケーションのセキュリティテスト

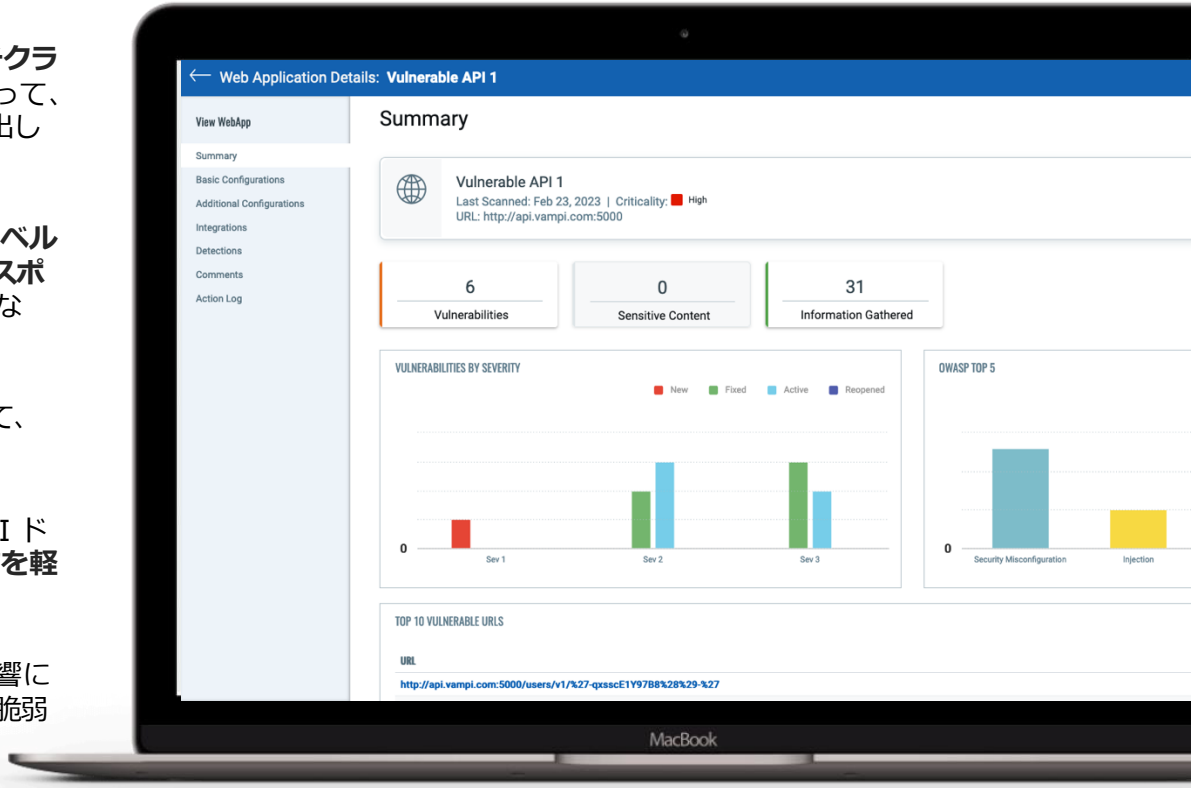
- 未知のアプリや忘れられたアプリを含むすべてのWebアプリケーションを**自動的に検出してカタログ化します**
- SQLインジェクション、クロスサイトスクリプティング (XSS)、構成ミスなどの**重大な Web アプリの脆弱性を特定します**
- 包括的なスキャンを実行して、**OWASP Top 10** に概説されているリスクに対処します
- Web アプリケーションでの **PII および機密データの露出**を検出します
- ビジネスコンテキストに合わせた**TruRisk™スコア**を脆弱性に割り当てます
- リスクの重大度、悪用可能性、ビジネスへの影響に基づいて**脆弱性の優先順位付けと修復を行う**



Qualys.

APIセキュリティテスト

- **クラウドネイティブ アプリケーション、マルチクラウド、APIゲートウェイ、コンテナ全体**にわたって、シャドウAPIを含むすべての APIを自動的に検出します
- **OWASP API Top 10、壊れたオブジェクトレベル認可(BOLA)、認証の問題、過剰なデータエクスポージャー**などのリスクに対処するための包括的なAPIスキャン
- **PIIと機密データのエクスポージャーを特定**して、データ侵害やコンプライアンス違反を防ぎます
- **OASコンプライアンス テスト**により適切な API ドキュメントを確保し、**API の設定ミスのリスクを軽減**します
- リスクの重大度、悪用可能性、ビジネスへの影響に基づいて、**TruRisk™ スコア**を使用してAPIの脆弱性に優先順位を付け、修復します



Qualys.

AI搭載スキャン最適化

TotalAppSecはスキャン時間を50%短縮しつつ、テストの精度を維持します

顧客特典:

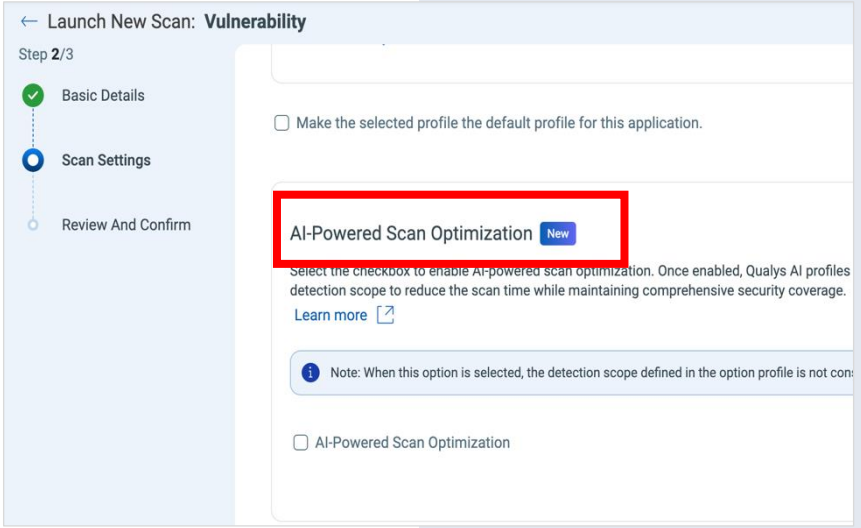
テストのカバレッジを損なうことなく、大規模で複雑なウェブアプリケーションのスキャン時間とコストを削減。

機能:

- 最も関連性の高いQIDを自動的に選択します。
- 手動でQIDを選択する必要がなくなる。
- AI搭載スキャン最適化のオン・オフを柔軟に切り替えられる。

観察された成果:

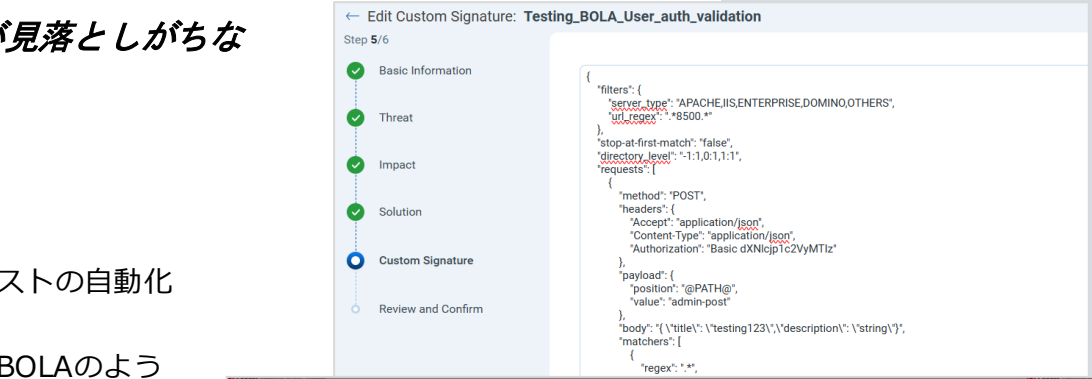
AI搭載スキャン最適化の早期導入者であるグローバルなCPG企業は、スキャン時間を50%削減し、リクエストを65%削減し、CMSのコストを大幅に削減しつつ、テストの精度を維持できます。

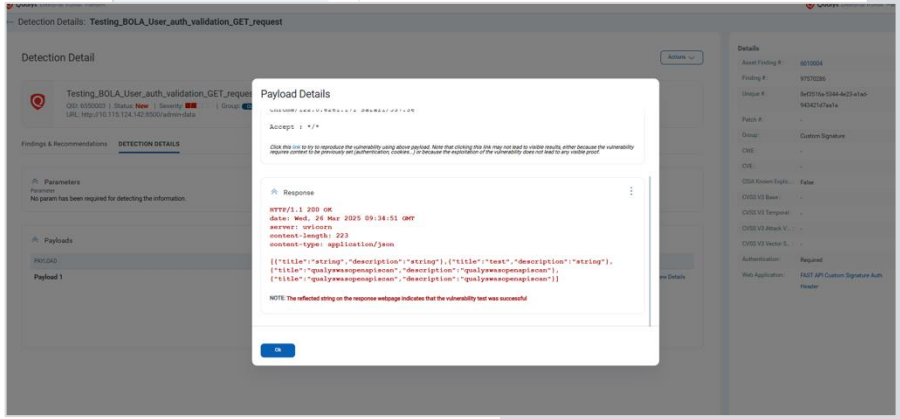


Qualys.

カスタムシグネチャ

ペンテストを自動化し、従来のツールが見落としがちなBOLAの脆弱性を明らかにしましょう。





顧客のメリット:

- カスタムシグネチャによるペンテストの自動化とスケール
- 多くのカスタム設定が必要となるBOLAのような複雑な脆弱性を検出
- Qualysが新しいQIDを公開するのを待たずに、脆弱性を検出するためのカスタムシグネチャを作成可能

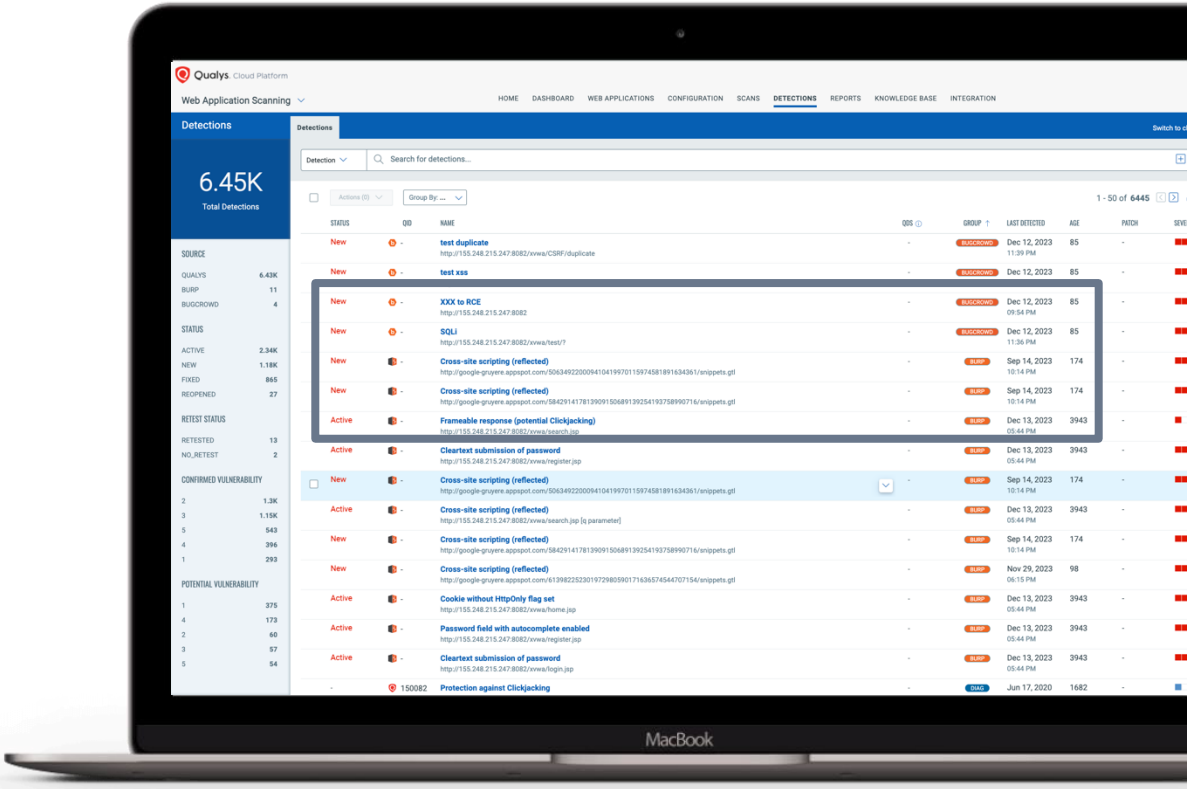
機能:

- カスタムシグネチャを定義する完全な柔軟性 (脅威、影響、解決策、署名のルール)

Qualys.

手動 PEN テストによる脆弱性の統合

- 自動スキャンと、さまざまな手動侵入テスト ソースからの検出結果の統合を通じて、**Web アプリケーションと API の脆弱性を統合**します
- **Burp Suite** - Burp Suite スキャン データのインポートと手動テスト結果の統合
- **Bug Bounty Platforms -** スキャン結果の双方向インポートおよびエクスポートのために、**Bugcrowd** などのバグ報奨金プラットフォームと統合します

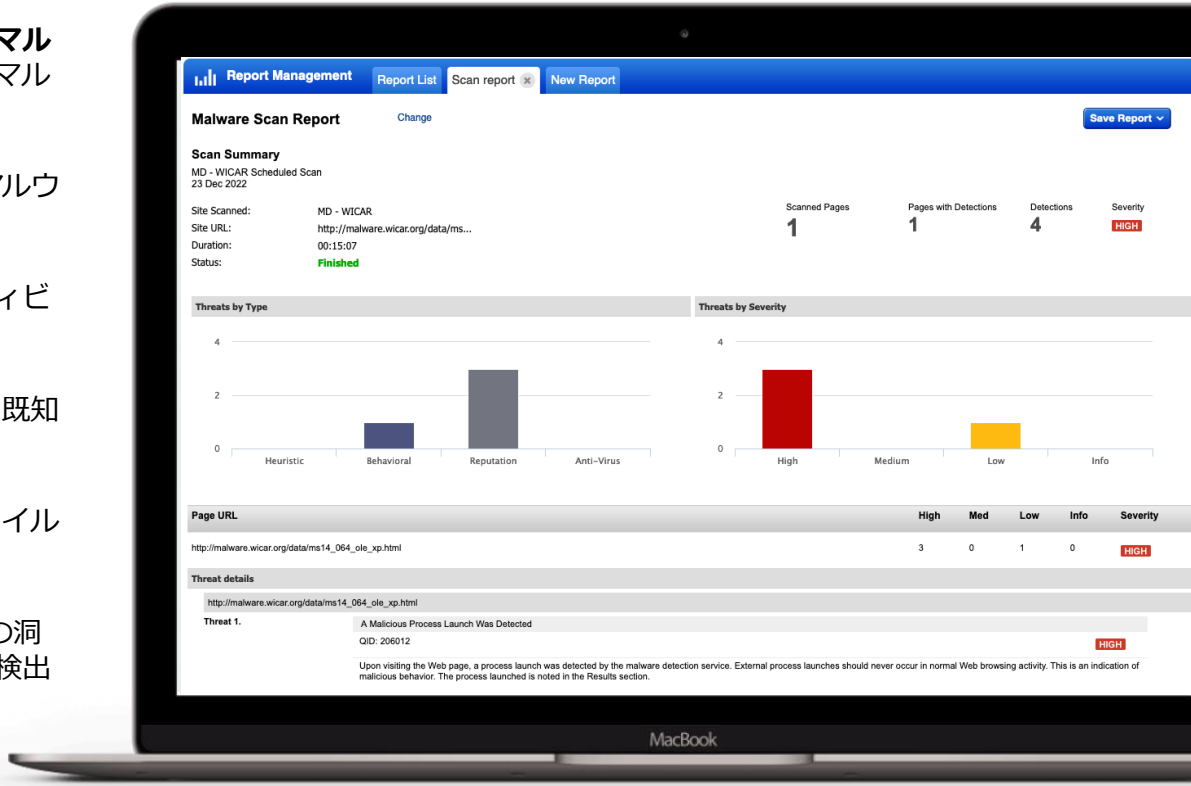


Qualys.

ディープラーニングベースのWebマルウェア検出

ディープラーニング AI を搭載

- **ディープラーニングベースのシグネチャ不要のマルウェア検出機能**により、既知、未知、ゼロデイマルウェアを特定
- **Webアプリケーションを継続的に監視**して、マルウェアの脅威が出現したときにそれを特定します
- **静的および動作分析**を使用して、不審なアクティビティについてファイルと振る舞いを分析します
- **ウイルス対策シグネチャ チェック**を使用して、既知のマルウェア シグネチャに対して検証する
- 幅広い**レピュテーション サービス**に対してファイルとソースをクロスチェックします
- **25以上の脅威インテリジェンス フィード**からの洞察を活用して、新たなマルウェアのトレンドを検出します



Qualys.

Qualys TruRiskTM スコアでリスクを定量化

包括的な指標に基づいてスコアを定量化

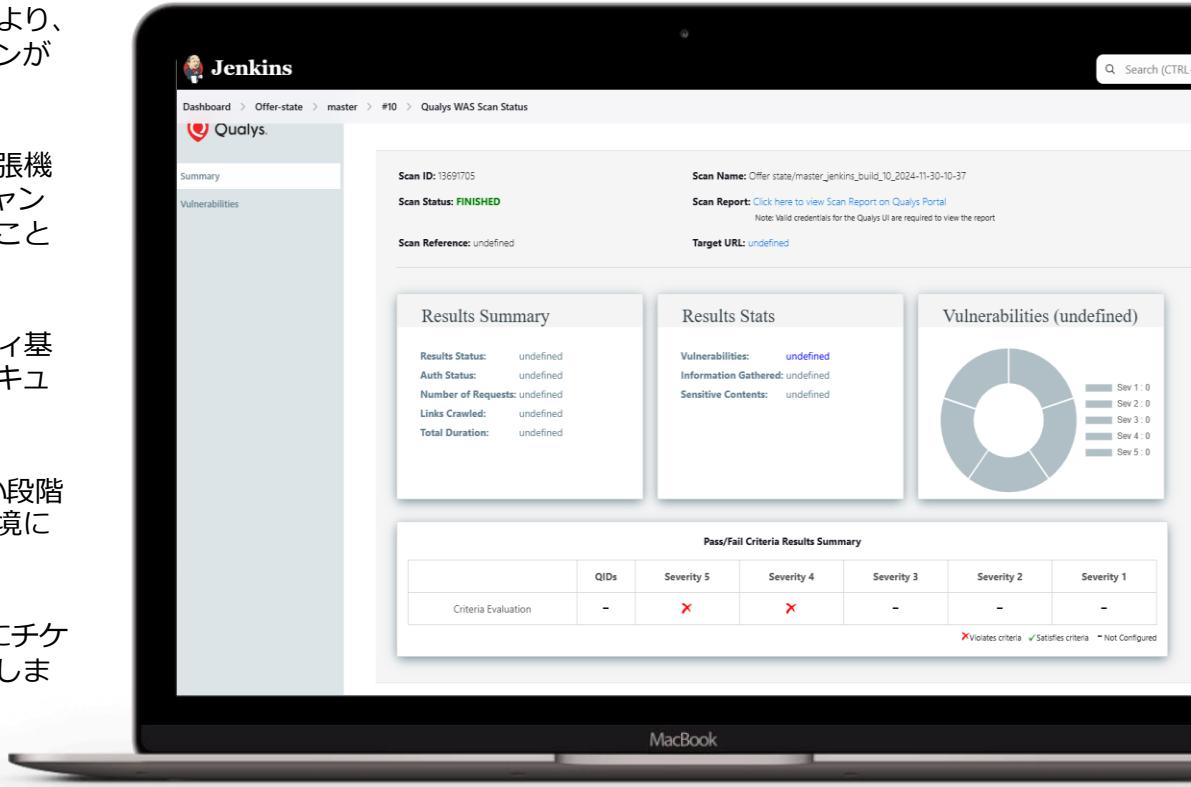
以下に基づいて優先順位を付ける

- **ビジネス資産のコンテキスト**
- **脆弱性の検出と相関する脅威コンテキスト**

Qualys.

自動修復ワークフロー

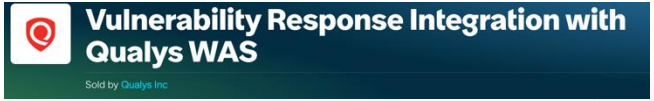
- **CI/CD パイプラインと ITSM ツールの統合**により、開発、セキュリティ、運用間のコラボレーションが促進されます
- **自動スキャン** - CI/CDツールのプラグインと拡張機能により、WebアプリケーションとAPIのスキャンをビルドとデプロイのパイプラインに組み込むことができます
- **ビルド検証** - あらかじめ定義されたセキュリティ基準に適合しないビルドを失敗させることで、セキュリティポリシーの実施を支援します
- **Shift-Left セキュリティ** - 開発サイクルの早い段階でセキュリティ・スキャンを組み込み、本番環境に到達する前に脆弱性を特定して修正します
- **チケットの自動作成** - ITSMシステムで自動的にチケットを作成し、適切なチームに割り当てて改善します



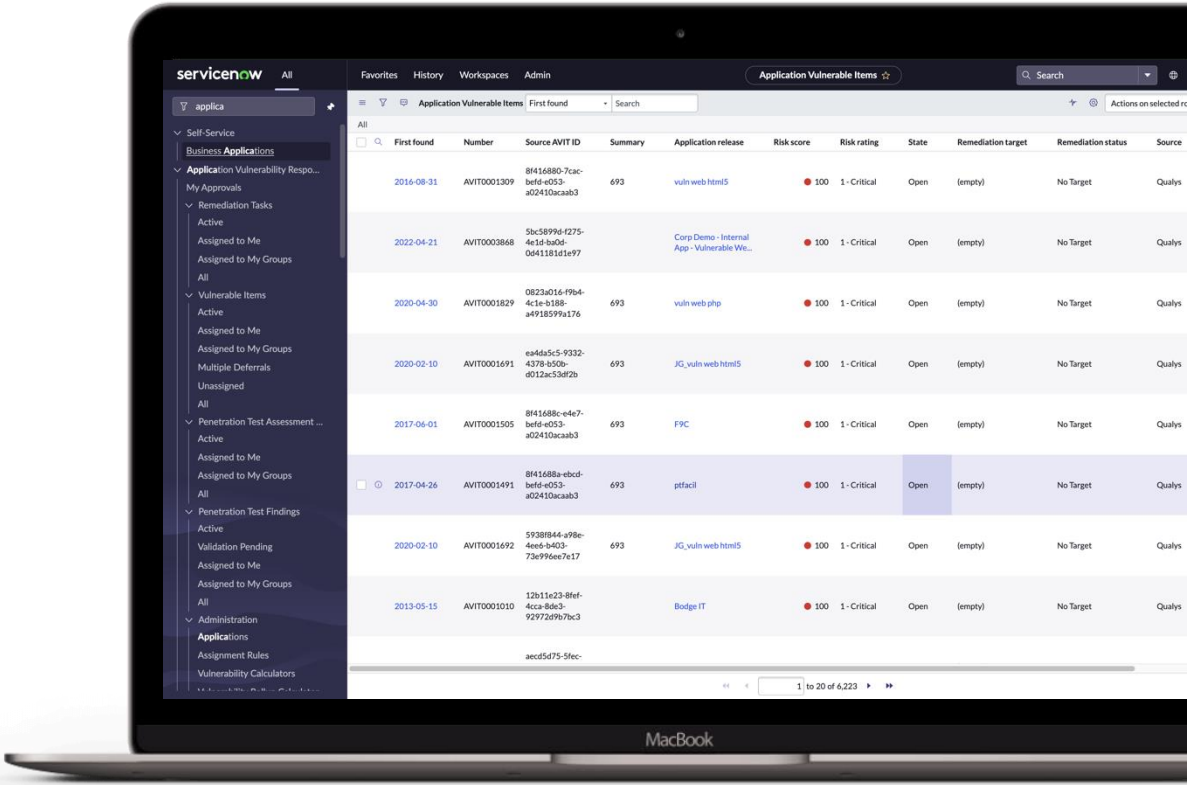
Qualys.

ServiceNow AVR インテグレーション

- **Qualys WAS**のすべてのWebアプリケーション**スキャンデータをServiceNowに統合**
- **データの自動同期** - Qualys WAS APIを利用して、スキャン結果、Webアプリケーションリスト、関連する脆弱性を**ServiceNowのVRモジュール**に自動的にインポートします
- **WAS関連のKnowledgeBase**エントリをQualysからServiceNowに同期します
- インポートされたデータは**ServiceNowのデータ構造**と整合し、正確な追跡と修復ワークフローを促進します



※詳しくは[こちら]



Qualys.

CI/CD パイプライン インテグレーション

Jenkins

- ビルド後のフェーズでの自動スキャン、脆弱性の重大度レベルまたは特定の Qualys ID (QID) に基づく合否条件の構成により、スキャン結果を Jenkins パイプラインにプッシュします

Azure DevOps

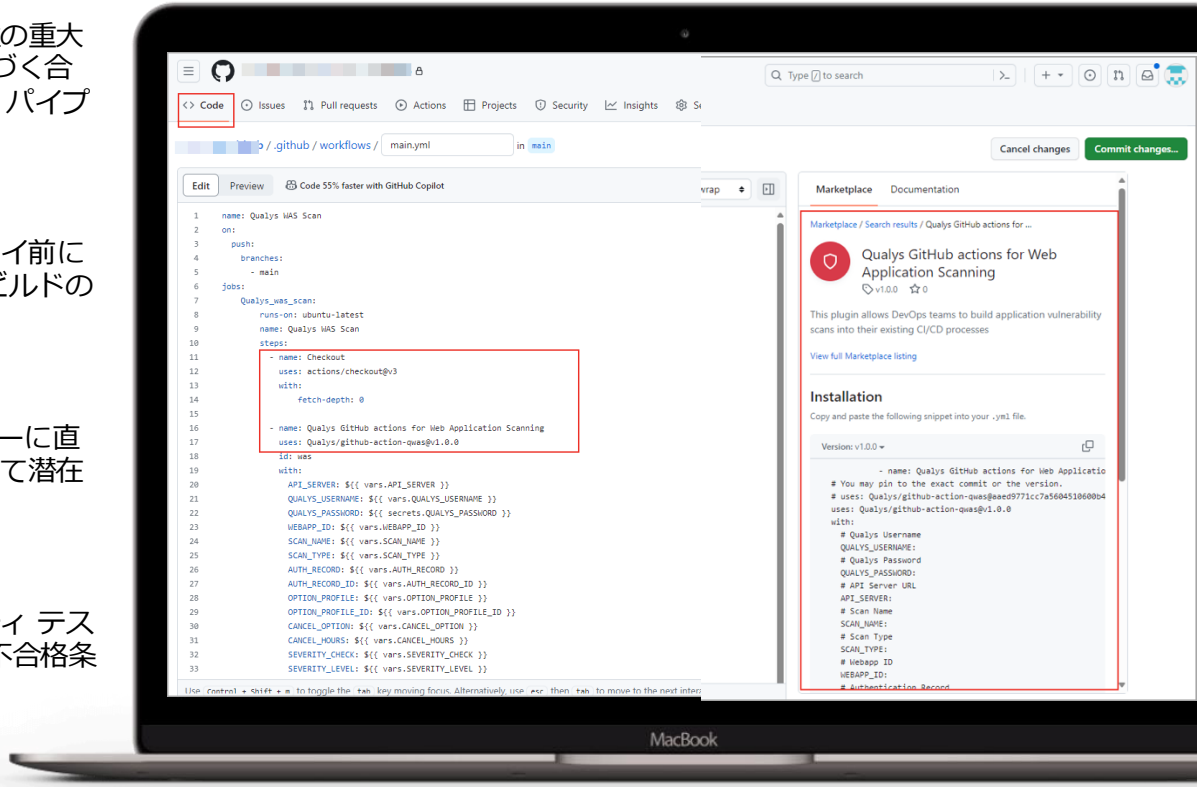
- スキャンを Azure Pipelines に統合し、デプロイ前にセキュリティ テストを実施し、ビルド検証でビルドの合格/失敗基準を構成します

GitHub Actions

- スキャンデータを GitHub Actions ワークフローに直接追加し、コードの変更を自動的にスキャンして潜在的なセキュリティ問題を特定します

BambooとTeamCity

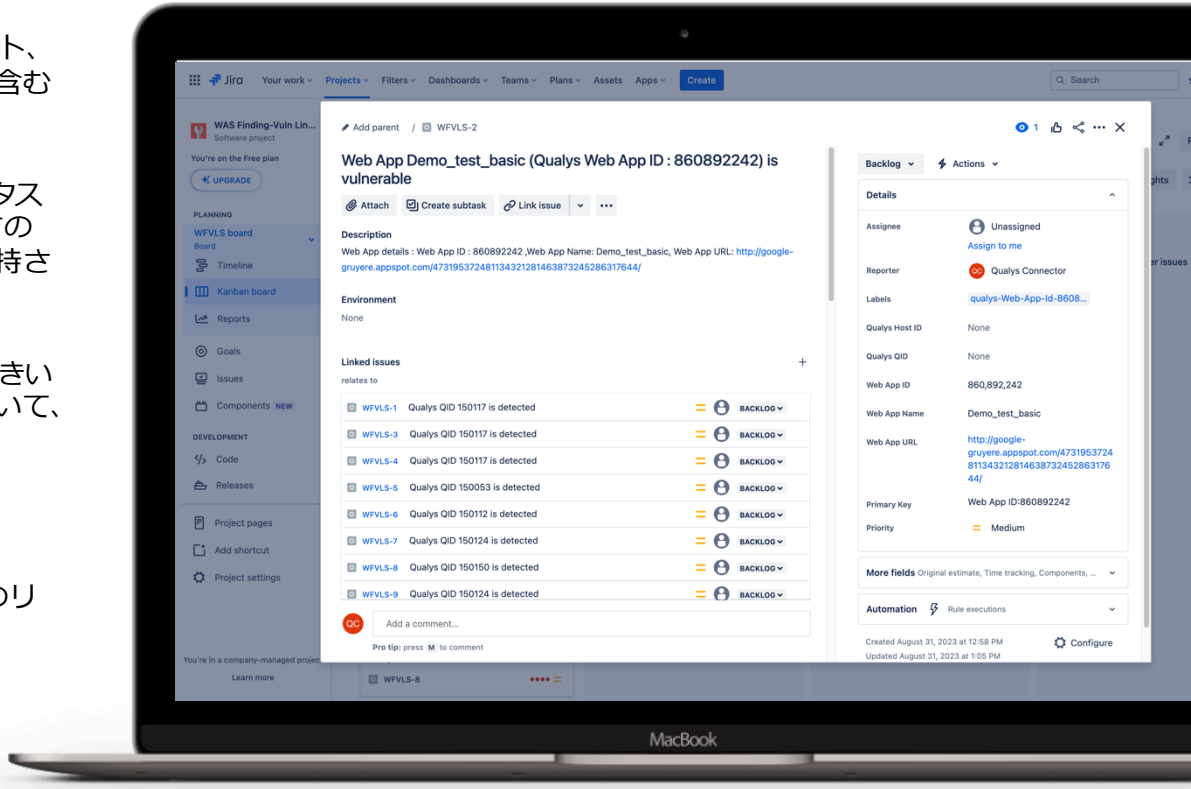
- ビルドおよび展開プロセスへの自動セキュリティ テストを有効にし、スキャン結果に基づいて合格/不合格条件を構成します



Qualys.

JIRA チケット発行 インテグレーション

- **自動チケット作成** - 問題、影響を受けるアセット、重大度レベル、修復ガイダンスに関する情報を含む詳細なチケットを Jira で自動的に生成します
- **リアルタイム同期** - Qualys 内の脆弱性ステータスの更新はすべて Jira チケットに反映され、両方のプラットフォーム間で一貫性と最新の情報が維持されます
- **カスタマイズ可能なワークフロー** - 重大度のしきい値、資産グループ、または特定の脆弱性に基づいて、チケット作成の設定ルールを調整します
- **チケット発行スキームの定義** -
  - 脆弱性ごとに個別のチケット
  - 各ホストの親チケットと、個々の脆弱性のリンクされた子チケット



Qualys.

リリースノート

Qualys TotalAppSec 2.4

November 2025

TAS

※リリースノートはこちら

TotalAppSecは、**Webアプリ**と**API**のセキュリティを**AIで強化**し、**攻撃対象領域を完全に可視化・保護する**次世代プラットフォームです。

主な新機能（TotalAppSec 2.4）

1. APIセキュリティの強化

- **OWASP API Top 10 2023**に対応し、APIの脆弱性を網羅的に検出します。
- **OpenAPI/Swagger仕様**に基づくコンプライアンスチェックを実施し、APIの設計段階からセキュリティを確保します。
- **TruRisk™スコア**により、APIごとのリスクを可視化し、優先順位を付けた対策が可能です。

2. AIによるマルウェア検出

- **ディープラーニングモデル**を活用し、ゼロデイ攻撃や高度なマルウェアを高精度で検出します。
- **99%の検出率**を実現し、従来の手法では見逃されがちな脅威にも対応します。

3. クラウド環境との統合

- **TotalCloud**との連携により、クラウドインフラ内の潜在的なWebアプリケーションを自動的に発見し、セキュリティ管理を強化します。

こんな企業様におすすめ！

APIの利用が増加し、セキュリティ管理が複雑化している企業
クラウドネイティブなアプリケーションを多数運用し、セキュリティ統制が求められる企業
開発と運用の連携を強化し、セキュリティを開発プロセスに組み込みたい企業
コンプライアンス対応を強化し、規制遵守を徹底したい企業
チケットによるタスクの管理や自動修復機能を活用して運用を効率化したい企業

導入メリット！

攻撃対象領域の可視化：隠れたWebアプリや非文書化APIの自動検出によって、脆弱性スキャンの対象が漏れません
運用の透明性・信頼性向上：コネクタ運用ログの記録機能により連携の不具合を即時把握可能
認証付きアプリの精度向上：失敗時の自動リトライ機能でスキャンの成功率が向上

Qualys.

Qualys TotalAppSec 2.5

January 2026

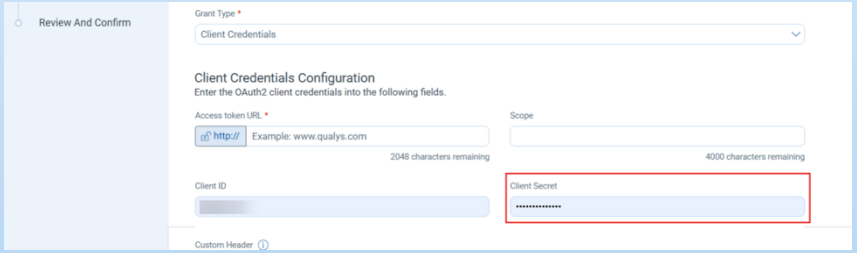
TAS

※リリースノートはこちら

主な新機能（TotalAppSec 2.5）

1. Oauth2クライアントシークレットのセキュリティ強化

機密性の高い資格情報をより適切に保護するために、OAuth2 認証レコードが強化されました。
OAuth2 認証レコードを作成または編集するときにクライアントシークレット フィールドがマスクされるようになり、機密情報の安全な取り扱いが保証されます。この機能は、新しく作成されたレコードと既存のレコードの更新の両方に適用されます。



2. RAMLサポートによる拡張API検出

MuleSoft APIコネクタは、OpenAPI（OAS）に加え、RESTful APIモデリング言語（RAML）ファイル形式をサポートするようになりました。この機能強化により、RAMLで定義されたAPIの検出が可能になり、MuleSoft標準API仕様を利用するお客様のカバレッジが拡大します。

3. ヘッダーインジェクションガイダンスの改善

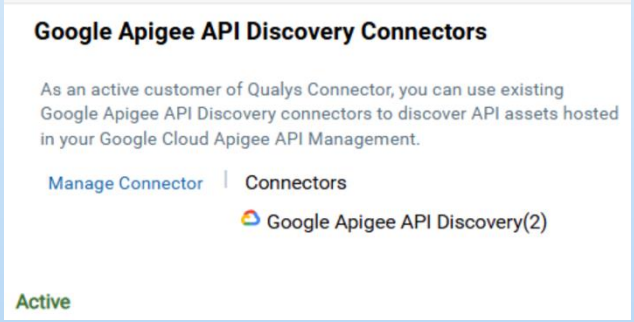
Web アプリケーションの作成時に、 [追加構成]セクションの[ヘッダー挿入]フィールドのテキスト ガイダンスを更新しました。
更新されたガイダンスでは、正しいヘッダー形式が示されており、機密性の高いヘッダーを含めないようアドバイスされています。スキャンレポートでマスキングが必要なヘッダーは、「認証レコード」 > 「ヘッダー」で設定する必要があります。

Qualys TotalAppSec 2.6

TAS

※リリースノートはこちら

主な新機能（TotalAppSec 2.6）



1. Google ApiGee API検出コネクタを使用してAPIを検出する

GCP APIコネクタを使用すると、TotalAppSecはGCP環境で公開されているすべてのエンドポイントでSwaggerファイルを検出できます。この機能強化により、TotalAppSecのAPI検出機能が強化され、セキュリティ体制全体の改善に役立ちます。GCP コネクタを作成するには、[検出] > [ソース]タブの [GCP API コネクタ] に移動し、[コネクタの作成] をクリックします。コネクタが作成されると、環境から検出されたAPI が[検出された API]タブに表示されます。これらの API をサブスクリプションに追加し、 スキャンを実行して脆弱性を評価することができます。
Google Apigee API Discovery Connector の設定の詳細については、オンライン ヘルプを参照してください。

2. KONG Gateway API コネクタを使用してAPIを検出する

TotalAppSecは、Kong Gateway Discovery APIコネクタを使用したAPIディスカバリをサポートするようになりました。この機能強化により、TotalAppSecはKong Gatewayインスタンスからすべてのエンドポイントを含むSwaggerファイルを検出できるようになり、APIの可視性が拡張され、組織のセキュリティ体制の強化に役立ちます。

3. APIコネクタ名の変更

TotalAppSecのAPIコネクタの名称を、標準化された命名規則に従って変更しました。変更された名称はベンダーブランドを明確に示し、ゲートウェイ製品を定義するため、API検出機能とターゲット環境の識別が容易になります。

Qualys

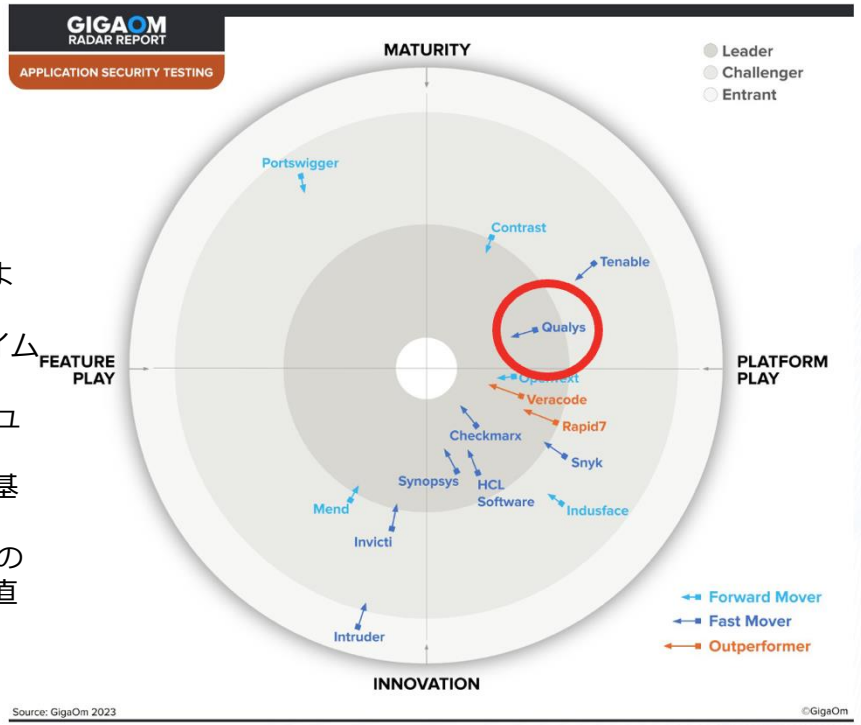
QualysTotalAppSec 評価

Qualys

GigaOMレーダーWASレポート

What are we announcing?

アプリケーションセキュリティテストに関する最新のGigaOmレーダーレポートにてQualys WASが「リーダー」としてタグ付けされました。



CVE フィード – 786 を超えるシグネチャを備えた Qualys WAS は、CVE および OWASP トップ 10 の脆弱性、PII、エクスポージャー、および Web マルウェアを簡単に検出できます。

API セキュリティのサポート – REST および SOAP API の動的ランタイム脆弱性を迅速かつ簡単にテストします。

統合 – サードパーティのスキャン結果を追加して、組織の全体的なセキュリティ体制のビューを強化します。

結果のフィルタリング - 重大度、資産、既知の悪用可能な脆弱性などに基づいて、スキャン結果と脆弱性をフィルタリングします。

セキュリティ サービス – Qualys の統合により、チケット発行システムの自動化によって MTTR を短縮しながら、セキュリティを CI/CD 環境に直接移行できます。

https://blog.qualys.com/product-tech/2023/09/28/qualys-named-a-market-leader-in-gigaom-radar-report-for-application-security-testing

Qualys | De-risk Your Business

製品およびDemoリクエストなどは
sales-jp@qualys.comまでお問い合せください。