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9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。

アプリケーション層がサイバー攻撃の最前線となる理由

AI時代の攻撃者は、あらゆるアプリケーションを機械速度で探索し、脆弱性を狙っています。

01 Webアプリケーションとapiの全資産をマッピング

把握されていないAPI、忘れ去られたエンドポイント、野良（未承認）の連携機能――これらは、管理者よりも先に攻撃者に見つけ出されてしまいます。

02 稼働中のシステムをテスト。ソースコードは不要

- 実行時に確認できるアプリケーションの動作フロー、BOLA（認可不備）、ビジネスロジックを対象とします。
- ロジックの欠陥 + APIエンドポイントの設定不備 = アカウントの完全な乗っ取り。

03 マシンスピードで攻撃を実行。AIも標的に。

- 攻撃者は数日ではなく、わずか数時間で攻撃を仕掛けます。
- AIコンポーネントは、防御が手薄なまま急速に拡大している攻撃対象領域です。

アプリケーションは常に、攻撃の主要な標的（アタックサーフェス）でした。今や、それらは最も悪用されやすいものとなっています。

40% 全インシデントの40%は、アプリケーションの悪用から始まりました。

2x–3x AIによる高速な脆弱性発見に伴い、アプリの悪用が2～3倍に急増。

67-day 業界平均である67日というMTTR（平均修復時間）は、マイナス要因となっています。

Qualys.

TotalAppSec vs. Mythos

Mythosはソースコードを基に動作します。一方、TASは実行中のアプリケーションをテストします。
これは、攻撃者が標的とするのと同じ攻撃対象領域です。

Mythosの現実

- ソースコードが必要
- 資産の自動検出機能なし
- ビジネスコンテキストの把握なし
- AI/LLMへの対応なし

TotalAppSec

01 WebアプリとAPIの継続的な検出

- 既知・未知・忘れ去られた・シャドウ・不正なWebアプリやAPIを検出
- EASM、CSAM、Postman、MuleSoftを活用し、オンプレミス、マルチクラウド、APIゲートウェイ、コンテナ、マイクロサービスにわたる統合インベントリを実現

02 ランタイムDASTおよびAPIテスト

- 開発者が記述したコードの視点ではなく、攻撃者の視点で稼働中のアプリケーションをテスト
- AIによるスキャン最適化（アプリごと）を活用した、認証を伴う多段階かつステートフルなテスト
- AIエージェント駆動のシグネチャにより、**検出からリリースまでの時間を2倍高速化**

03 ビジネスへの影響度に基づくTruRisk™の優先順位付け

- 収益への影響、コンプライアンス適用範囲、資産の重要度によるランク付け
- OWASP Top 10およびAPI Top 10への対応、ならびにPCI-DSS、GDPR、HIPAAのコンプライアンス監視
- Claude、Mythos、Frontierモデルによる検出結果をETMに取り込み可能

04 アプリケーション内のシャドウAIを検知

- カスタムシグネチャにより、アプリ内のLLM、AIエージェント、MCPサーバーを検知
- プロンプトインジェクション、トークン漏洩、モデルの悪用に対応
- ディープラーニングによるマルウェア検知: ゼロデイ・ペイロードに対し**約99%の精度**

Roadmap

- Vuln correlation & deduplication (2H-26)
- Eliminate powered remediation of AppSec findings (2H-26)

Qualys.

Webアプリ＆API資産のディスカバリとインベントリ

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.

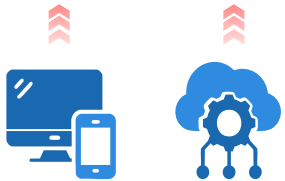
ASPM – アプリケーションセキュリティ

包括的な ディスカバリ & 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

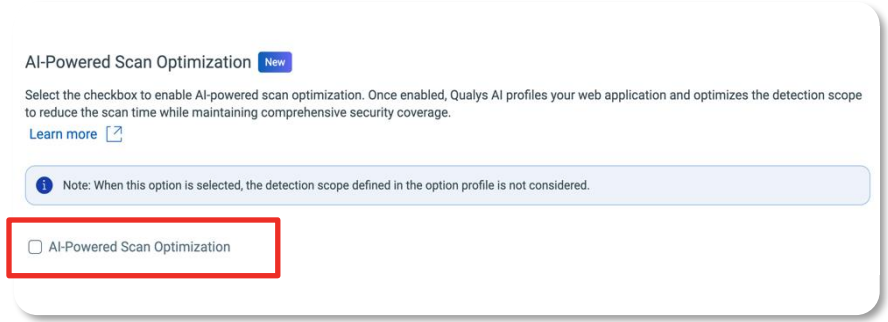
DevOpsとITSM統合による**修復ワークフロー**

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

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

- 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

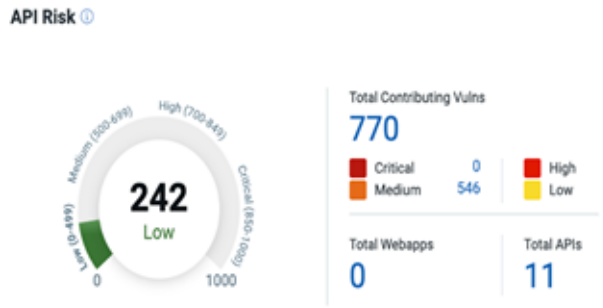
OWASP Top 10 vulnerabilities (in Web Apps)

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

- **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

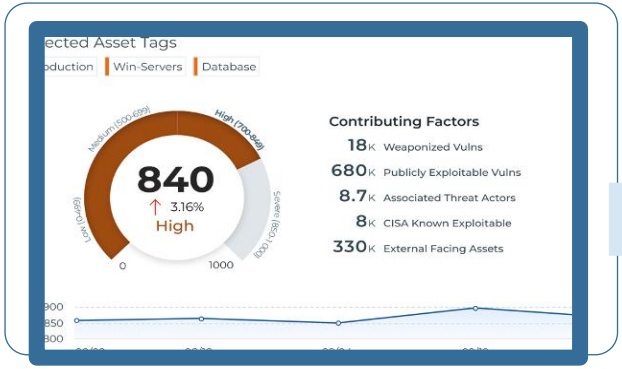
ローンチから最初の数四半期以内に

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

Qualys.

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 - アプリケーション層のセキュリティ確保

AIスピードによる高速検知、超優先順位付け、および自律的修復を運用に組み込む

AIスピードによる高速検知 (AI-Speed Detection)

マシン・スピードでの検知 ― より広範なカバレッジを実現

- 検知時間を**50%短縮**
- スキャン要求を**65%削減**
- シグネチャが存在しない**ゼロデイ攻撃**を検知

主な機能

- 攻撃対象領域の継続的な検出
- ゼロデイおよびCVEの自律的な検出
- **TTR（修復までの時間）の2倍の高速化**と、**検出機能リリースの2倍の高速化**
- ディープラーニングによるマルウェア検出
- シャドーAIの検出: LLM、AIエージェント、MCPサーバー

超優先順位付け (Hyper-Prioritization)

リスクとビジネスコンテキストに基づき優先順位付けされた、検証としてのDAST

- TruRisk™を活用し、**リスクが最も高い上位1.6%のアプリケーションを特定**
- ビジネスコンテキスト: 収益、コンプライアンス、資産の重要度

主な機能

- **25以上の脅威インテリジェンスフィード**に基づくTruRisk™
- DASTによる検証: 悪用可能性の確認
- BOLA、認証バイパス、ロジックチェーンの実際の発生を確認
- 攻撃パス分析
- Claude/Mythosの検出結果をETMに統合
- 脆弱性の相関分析と重複排除 ***Roadmap****

ゼロデイ修復 (Zero-Day Remediation)

エクスプロイト（悪用）の可能性の確認から、緩和・修復まで対応

- ITSMおよびCI/CDワークフローの活用により、**MTTRを30%短縮**
- 「TruRisk Eliminate」の活用により、**MTTRを80%短縮**
- PCI-DSS、GDPR、HIPAAへの準拠

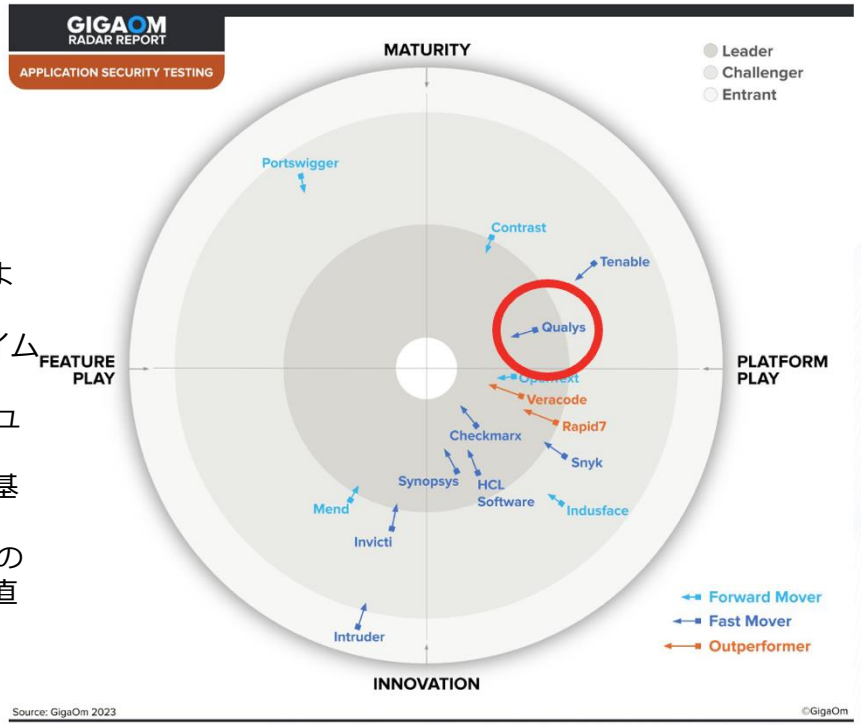
主な機能

- CI/CD: GitHub Actions、Azure DevOps、Jenkins
- ITSM: Jira、ServiceNow
- QFlow™ ノーコード・オートメーション
- TotalAppSec向けTruRisk Eliminate統合 ***Roadmap****

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。

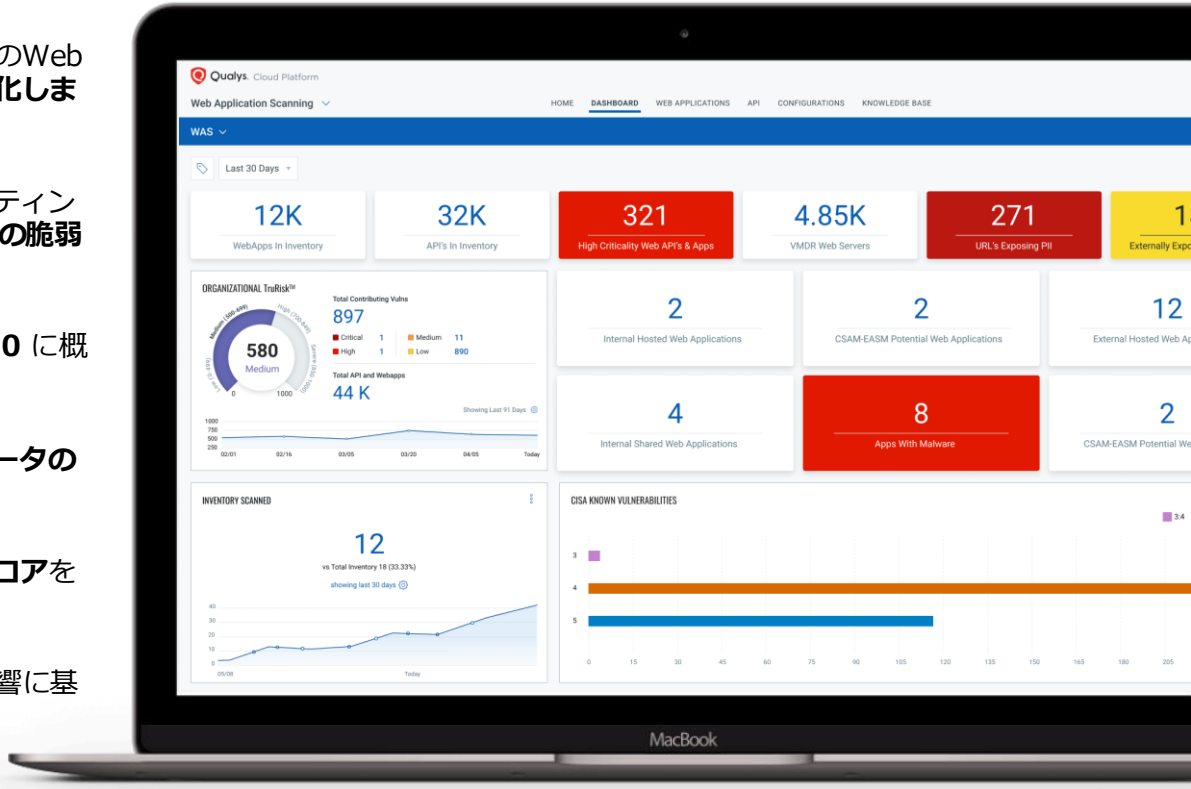
セキュリティ サービス – Qualys の統合により、チケット発行システムの自動化によって MTTR を短縮しながら、セキュリティを CI/CD 環境に直接移行できます。

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

補助資料

Webアプリケーションのセキュリティテスト

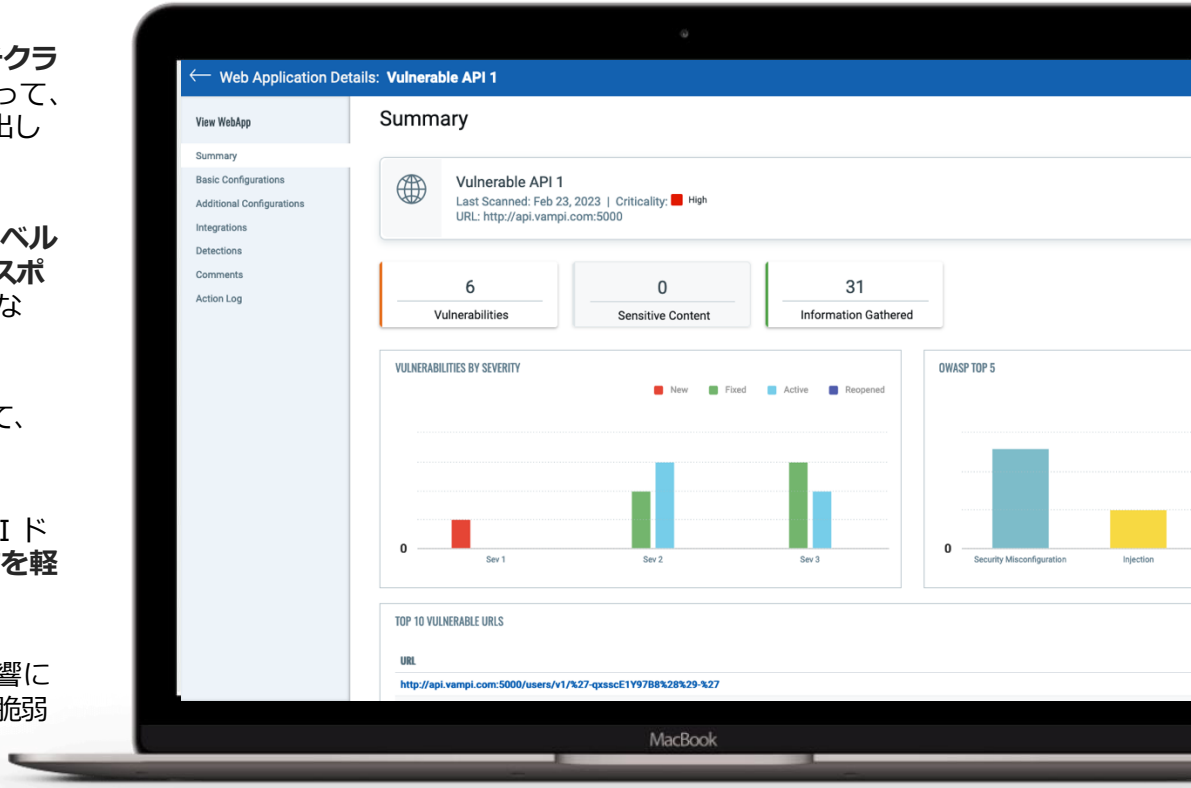
- 未知のアプリや忘れられたアプリを含むすべてのWebアプリケーションを**自動的に検出してカタログ化します**
- SQLインジェクション、クロスサイトスクリプティング (XSS)、構成ミスなどの**重大な Web アプリの脆弱性を特定します**
- 包括的なスキャンを実行して、**OWASP Top 10** に概説されているリスクに対処します
- Web アプリケーションでの **PII および機密データの露出**を検出します
- ビジネスコンテキストに合わせた**TruRisk™スコア**を脆弱性に割り当てます
- リスクの重大度、悪用可能性、ビジネスへの影響に基づいて**脆弱性の優先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

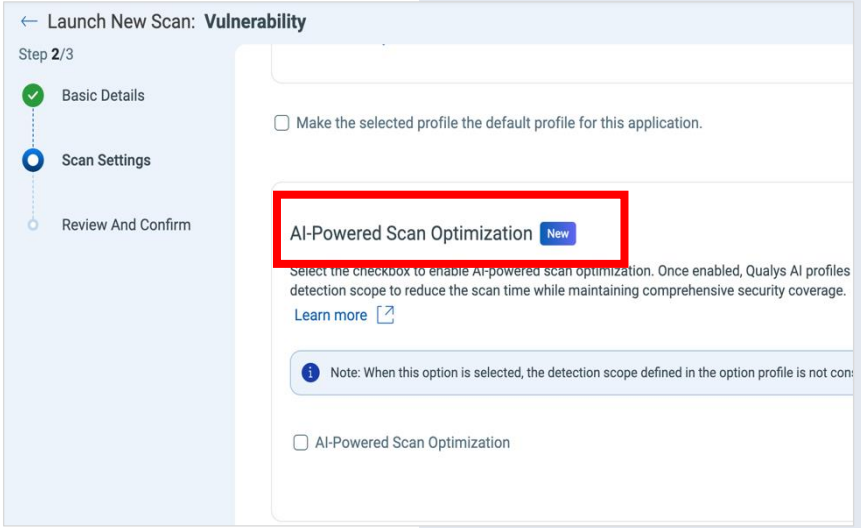
TotalAppSecはスキャン時間を80%短縮しつつ、テストの精度を維持します

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:

- 最大80%のスキャン時間短縮
- CI/CDやDevSecOpsに適した高頻度スキャンを実現
- スキャン設定・チューニングをAIが自動最適化
- リスクの高い領域を優先的に評価
- 高い脆弱性検出カバレッジを維持
- フルスキャンとの併用で効率性と網羅性を両立



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.

公式BLOG：最新のアプリケーションセキュリティを拡張する：静的プロファイルからAIを活用したスキャン最適化への移行

カスタムシグネチャ

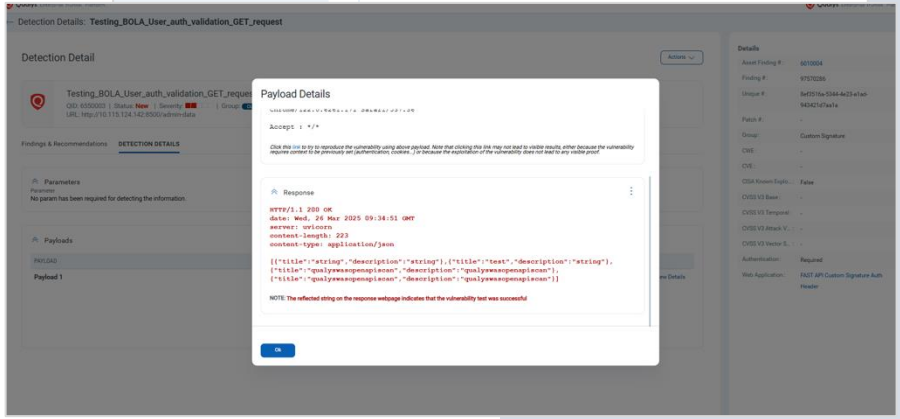
ペンテストを自動化し、従来のツールが見落としがちなBOLAの脆弱性を明らかにしましょう。

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:

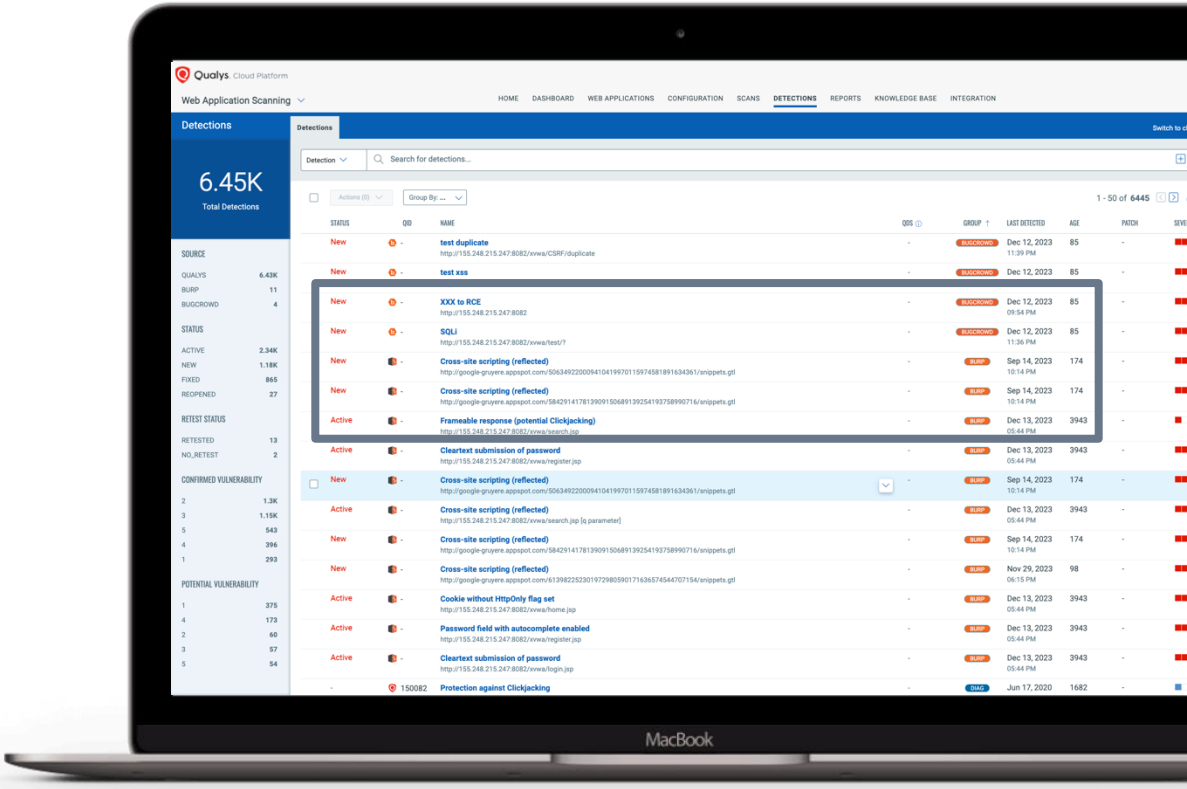
- カスタムシグネチャを定義する完全な柔軟性 (脅威、影響、解決策、署名のルール)



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

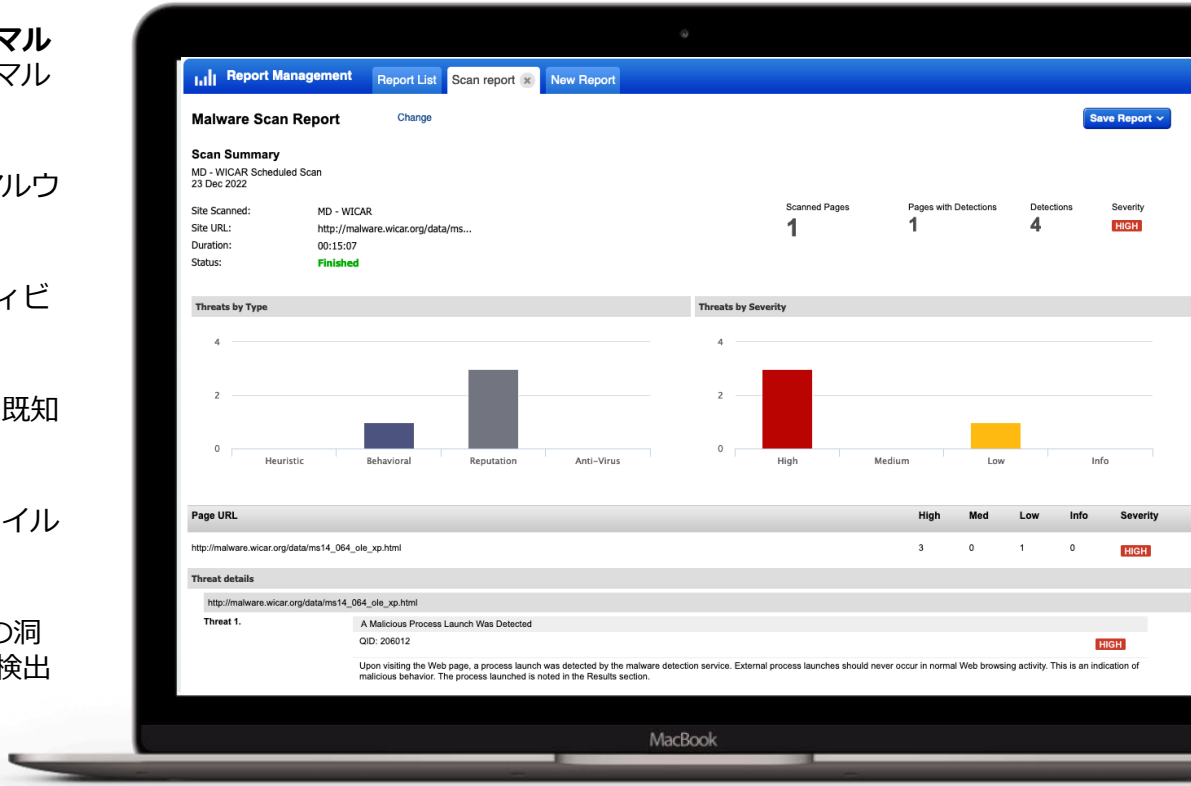


Qualys.

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

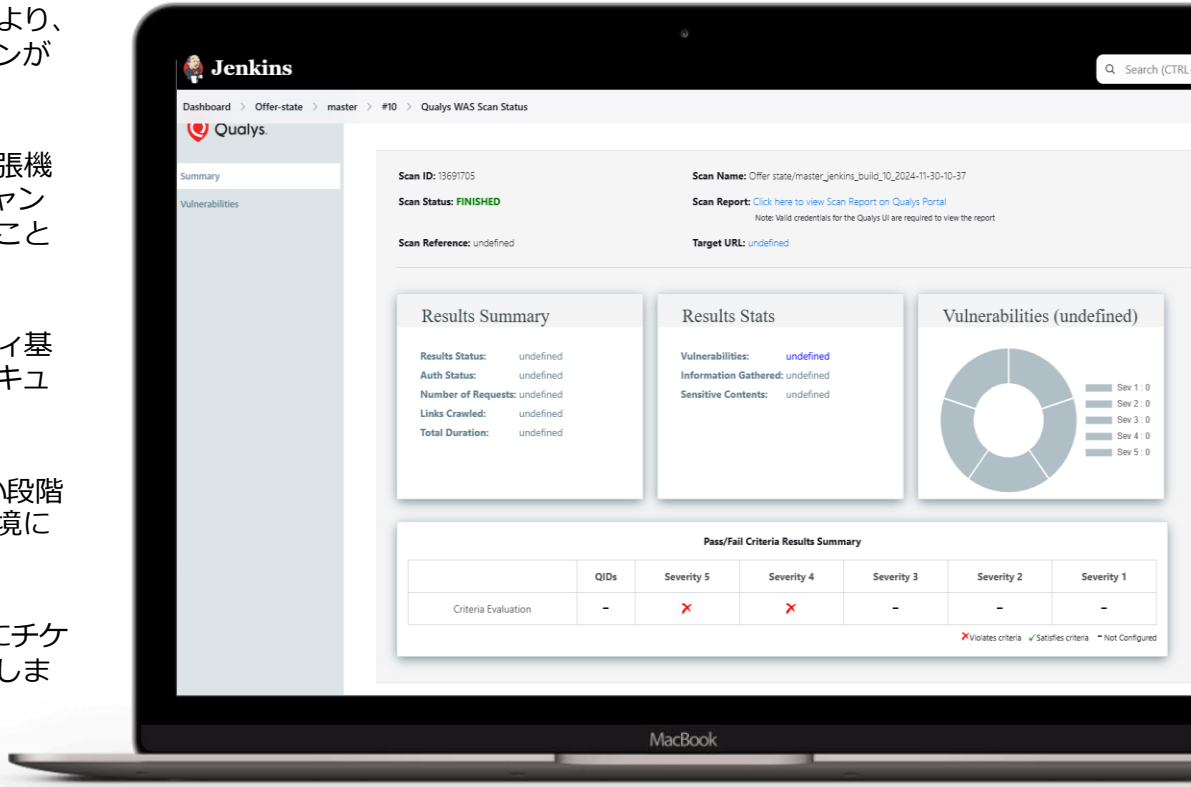
以下に基づいて優先順位を付ける

- **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

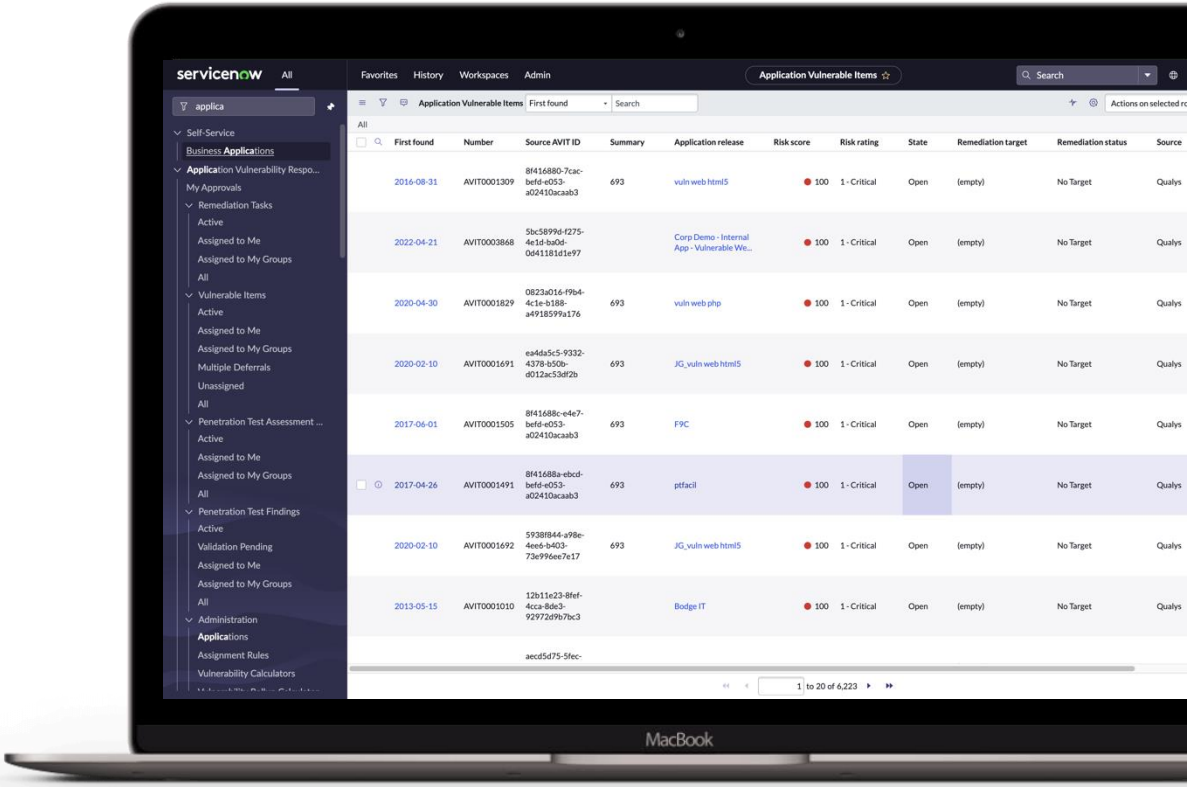
- **CI/CD パイプラインと ITSM ツールの統合**により、開発、セキュリティ、運用間のコラボレーションが促進されます
- **自動スキャン** - CI/CDツールのプラグインと拡張機能により、WebアプリケーションとAPIのスキャンをビルドとデプロイのパイプラインに組み込むことができます
- **ビルド検証** - あらかじめ定義されたセキュリティ基準に適合しないビルドを失敗させることで、セキュリティポリシーの実施を支援します
- **Shift-Left セキュリティ** - 開発サイクルの早い段階でセキュリティ・スキャンを組み込み、本番環境に到達する前に脆弱性を特定して修正し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

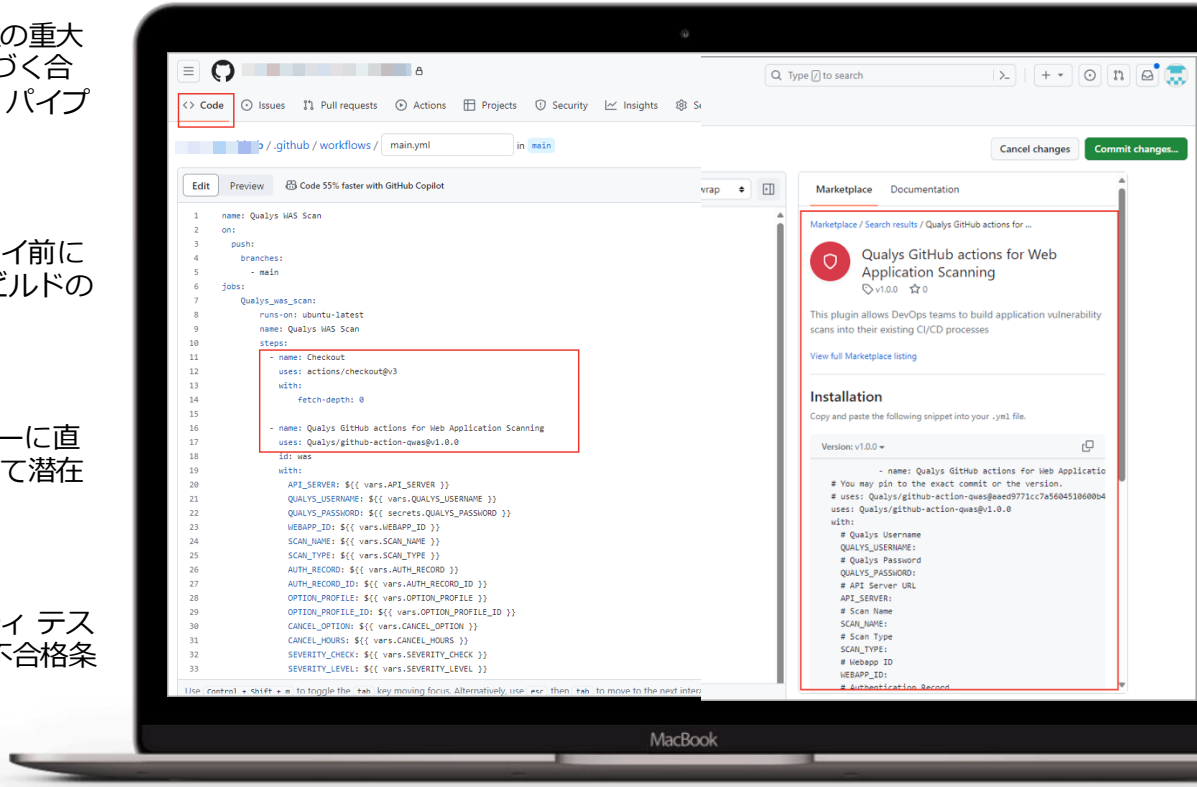
- スキャンを Azure Pipelines に統合し、デプロイ前にセキュリティ テストを実施し、ビルド検証でビルドの合格/失敗基準を構成します

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

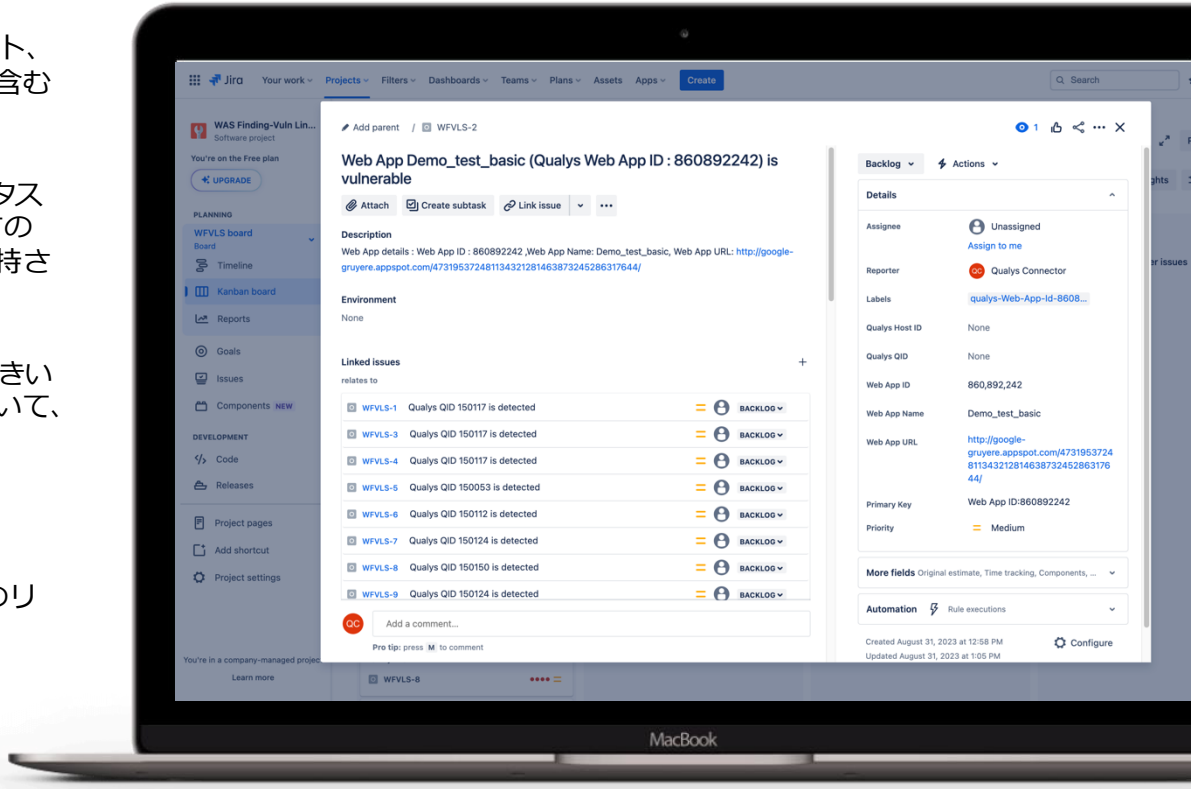
- ビルドおよび展開プロセスへの自動セキュリティ テストを有効にし、スキャン結果に基づいて合格/不合格条件を構成します



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.

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。