リスク重視のCNAPP

Qualys Total Cloud（TC）

*Total Cloudライセンスは VMライセンスから移行できます。
*Qualys Unit 単位でのライセンス計算となります。

Qualys Cloud Security （TotalCloud）による課題解決

<table>
<tr><th>課題</th><th>解決アプローチ</th></tr>
<tr><td>マルチクラウド環境での資産の可視化が困難</td><td>AWS, Azure, GCP, OCI を一元管理し、リアルタイムでインベントリを自動取得</td></tr>
<tr><td>クラウド構成ミス（misconfiguration）による
リスク増加</td><td>各クラウドサービスプロバイダーによるベストプラクティスとCISベンチマーク準拠を含む1000以上の構成チェックや誤設定の自動検出</td></tr>
<tr><td>クラウド上の脆弱性やマルウェアを管理しきれない</td><td>FlexScanによるOSやアプリの脆弱性検査及び、CDRによるマルウェアを継続監視</td></tr>
<tr><td>サーバーレスやKubernetesのセキュリティ対策
が遅れている</td><td>
<table>
<tr><th>保護領域</th><th>主なセキュリティ対策</th><th>ユースケース</th></tr>
<tr><td>Kubernetes</td><td>構成監査、RBAC分析、Admission Controllerによるセキュリティポリシー違反ブロック</td><td>・脆弱性を含んだイメージのデプロイを拒否
・セキュリティ要件を満たしていない構成（特権モード、rootユーザー）の禁止</td></tr>
<tr><td>コンテナ実行時</td><td>ランタイム監視、脆弱性検知、ポリシー適用</td><td>・予期しない動作（不審なプロセス、ファイル変更、ネットワーク接続）を検出</td></tr>
<tr><td>サーバーレス</td><td>構成監査、脆弱性検知（間接的）</td><td>・AWS Lambda、Azure Functionsなどの構成評価
・Lambda関数のコードが含まれるS3やイメージ（OCI準拠）の脆弱性評価</td></tr>
</table>
</td></tr>
<tr><td>クラウドリソースのリスクを経営層に説明しづらい</td><td>TruRiskスコアによるリスクの定量化とレポーティングに対応</td></tr>
</table>

Qualys TotalCloud の優位性

項目	Qualysの優位性	他社との比較ポイント
エージェント技術	高機能クラウドエージェントを活用し、**OSレベルまで深く可視化**	他社などはエージェントレス中心で深い内部情報が取得しづらい場合もある
統合プラットフォーム	**WAS、EASM、CSAM**とのシームレスな統合	単体製品で分断されている他社ソリューションより連携性が高い
コスト効率	**同一プラットフォーム**で多機能を実装 → TCO削減	他社製品を複数組み合わせる場合、ライセンスや運用コストが増大しやすい
コンプライアンス対応	**PCI DSS, ISO 27001, NIST**など **30以上**のフレームワークに対応	コンプライアンステンプレートとレポート出力が標準装備
クラウド脆弱性管理とリスク評価	TruRisk(**Insight**や**Attach Path**)による優先順位付け	通常のCVSS中心より実用的で、経営判断に直結しやすい
修復の自動化	- 300以上の**Playbook（修復自動化）**により、クラウド間のミスコンフィグや脆弱性を修復 - **ノーコード/ローコード対応**で非エンジニアでも操作可能	他社製品は自動修復に弱く、ノーコードは提供していない場合がほとんど

Qualys TotalCloudを推奨する理由

企業タイプ	お勧め理由
マルチクラウド（AWS, Azure, GCP,OCI）を活用する中堅～大企業	一元管理とセキュリティの統合により、管理負荷とリスクを削減
金融・製造・通信など高コンプライアンス業種	継続監査、証跡管理、コンプライアンスレポートが強力
DevSecOpsに力を入れている開発組織	IaCスキャン、パイプライン連携、Kubernetes監視が充実
CSAM/VMDRを既に導入済みのQualysユーザー	既存インフラと統合しやすく、迅速に展開可能
サイロ化されたツールを統合したい企業	Webスキャン、脆弱性スキャン、EASM (External Attack Surface Management)をひとつに集約可能

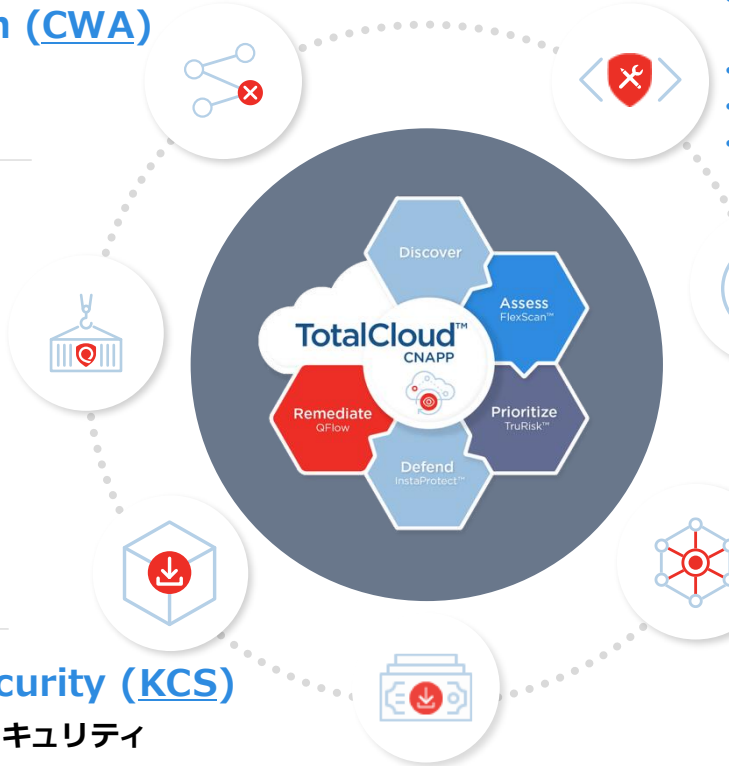
Qualys TotalCloud CNAPP

Cloud Workflow Automation (CWA)
- カスタムコントロール
- 自動修復

SaaS Security Posture Management (SSPM)
- SaaSアプリの保護
- コンプライアンス

Runtime Threats Detection (CDR)
- ランタイムの脅威の検出
- ディープラーニングAI

Kubernetes and Container Security (KCS)
開発からランタイムまでのコンテナセキュリティ



Cloud Security Posture Management (CSPM)
- マルチアカウント統合監視
- ベンチマーク準拠チェック（CIS, NIST, PCI他）
- AWS/Azure/GCPの設定ミス検出
- シフトレフト IaC スキャニング
- TruRisk Insight とAttack パス

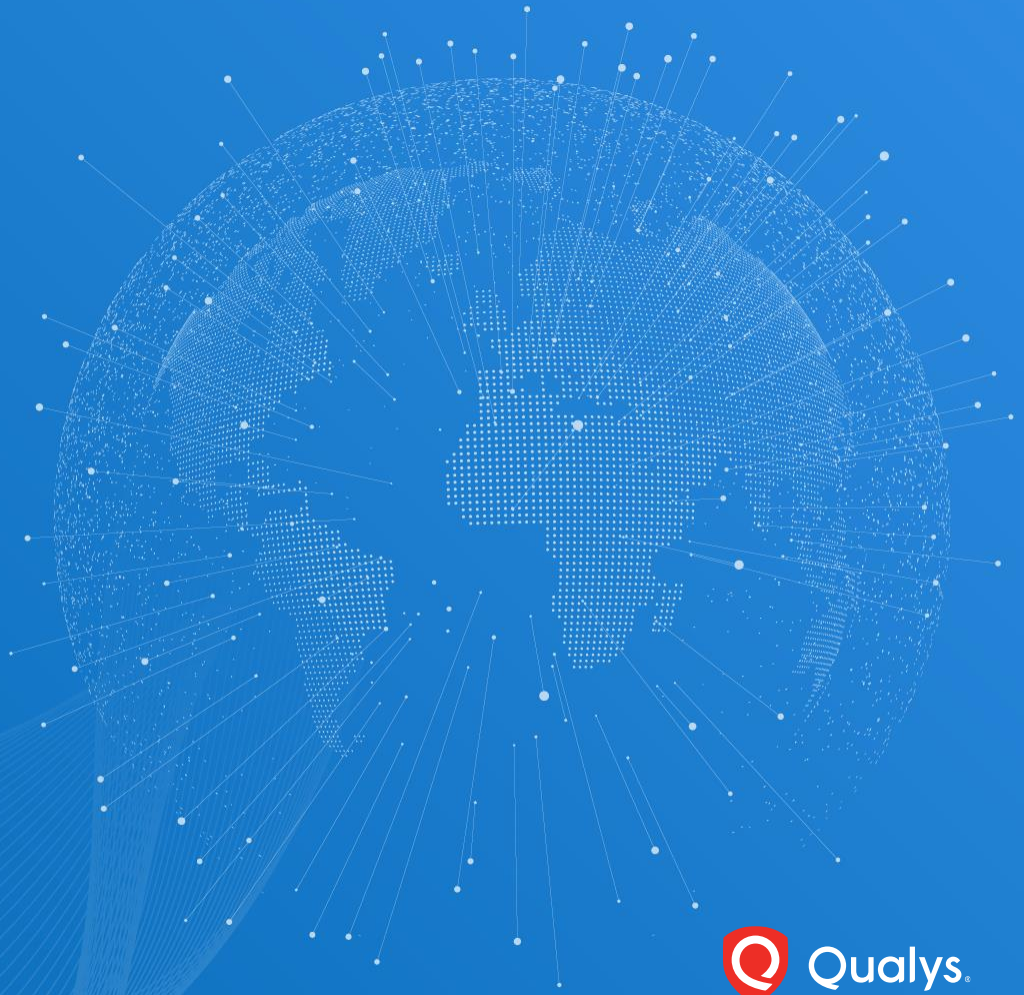
Cloud Infrastructure and Entitlement Management (CIEM)
- 過剰な権限の検出
- IAMポリシーの可視化・最適化

Application Security (ASPM)
- ウェブアップ、API、LLMの保護

Qualys. aws Azure Google Cloud ORACLE Cloud

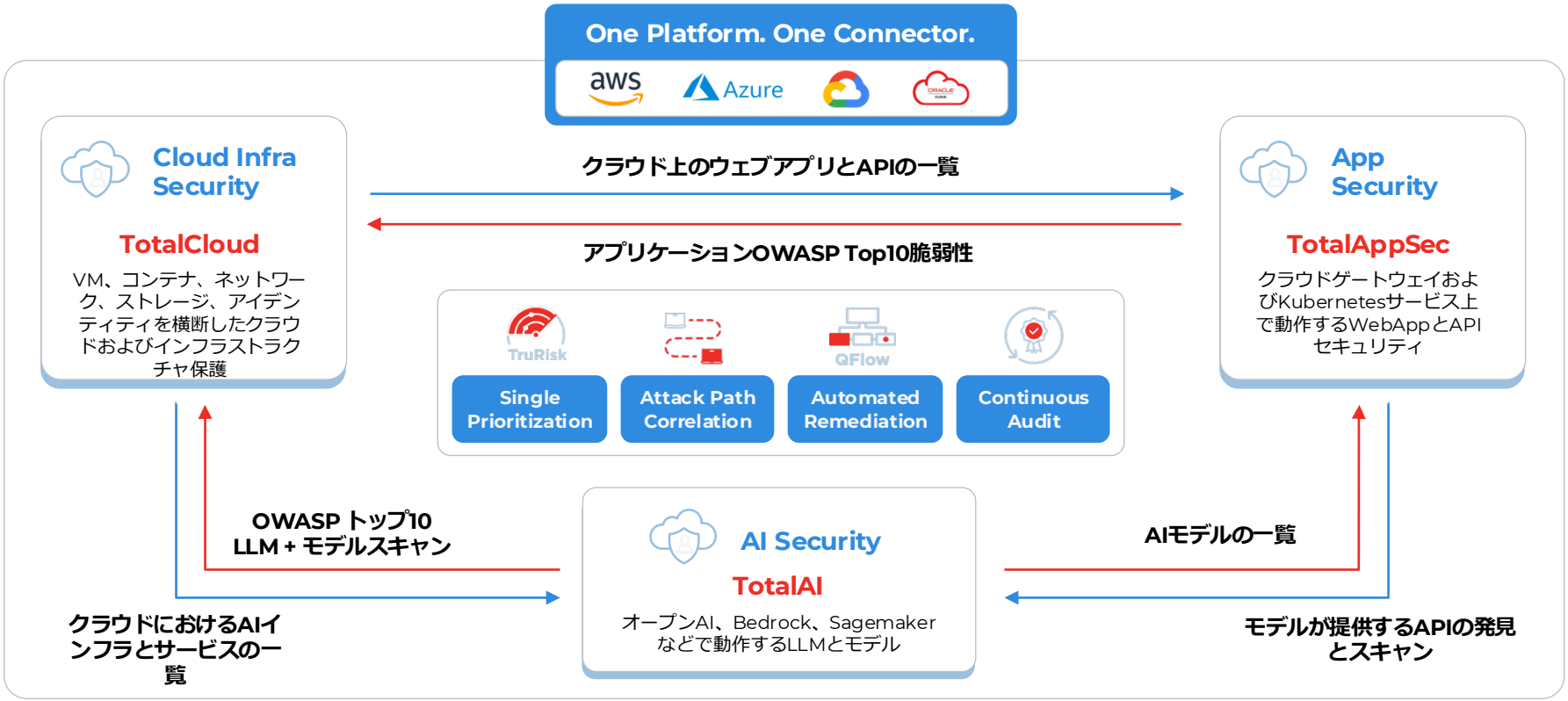
Qualys

Total Cloud
補助資料



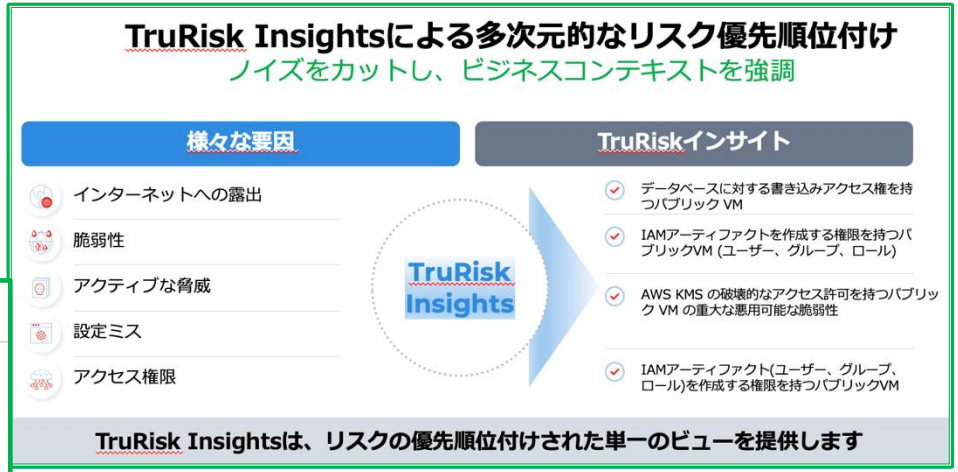
Qualys

ワン・クラウド・コネクターですべてのセキュリティ結果



Qualys.

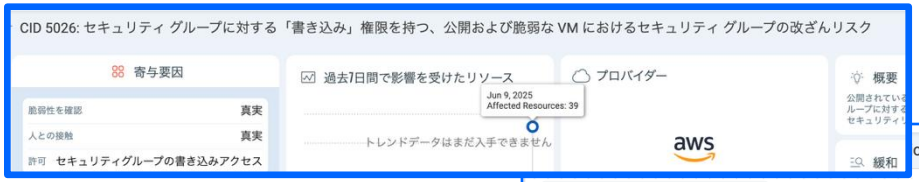
優先順位付け：TruRisk Insights



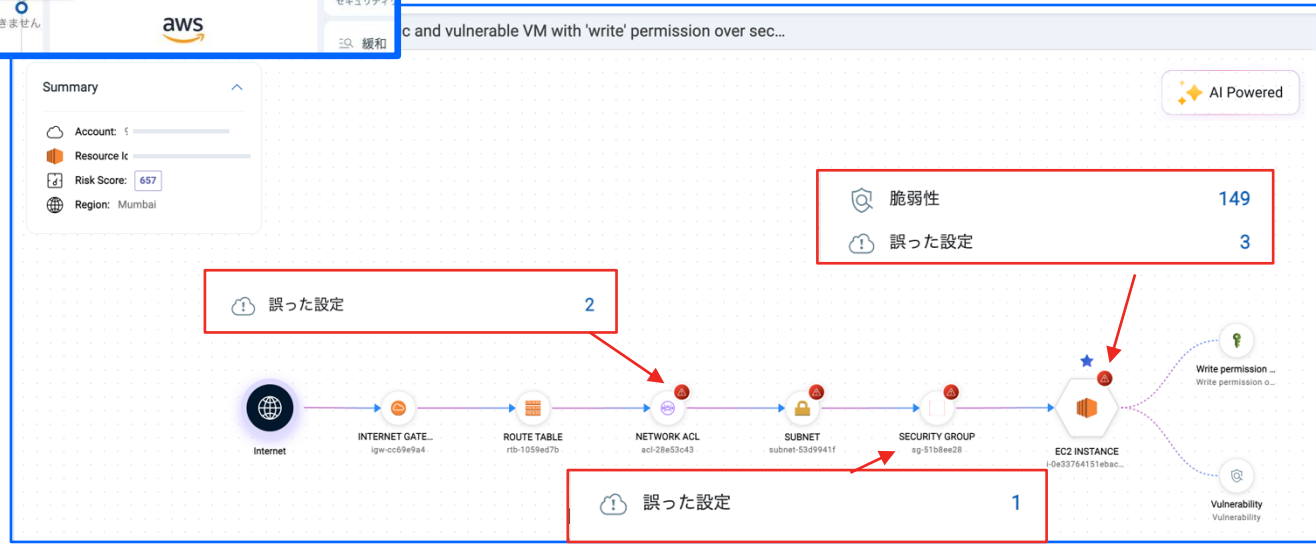
TotalCloud Attack Path

TotalCloud Attack Path(攻撃経路) は、Qualys TotalCloud プラットフォームにおける **クラウド環境の攻撃経路分析機能** です。クラウドインフラの中で、脆弱性・設定ミス・アイデンティティ・ネットワーク接続性などを基に「攻撃者がどのように重要資産へ到達できるか」を視覚的に把握するための機能です。

ユースケース	説明
クラウドセキュリティのリスク可視化	数千のアラートの中から「本当に危険なルート」を特定可能に。
脆弱性・設定ミスの優先順位付け	攻撃可能性のあるパスに関連するリスクを優先して修復。
セキュリティ対策の効果測定	攻撃経路の断絶によって防御強化を定量的に確認可能。
監査・コンプライアンス対応	攻撃パスに基づいたリスク説明が可能になる。



[外部攻撃者]
↓
[公開中の脆弱なEC2インスタンス]
↓
[権限昇格によりRole切替]
↓
[S3バケットやRDSなどの機密資産へアクセス]



BLOG: [Qualys、TotalCloud Attack Path、クラウドワークフロー自動化、そしてCNAPP向けの合理化された3ステップのユーザーオンボーディングを発表]

Qualys.

TotalCloud(Qflow)

クラウドリスクの修正を自動化し、効率的なセキュリティ運用を実現

No Code / Low Code QFlows
コーディング不要で簡単にワークフローを構築可能。

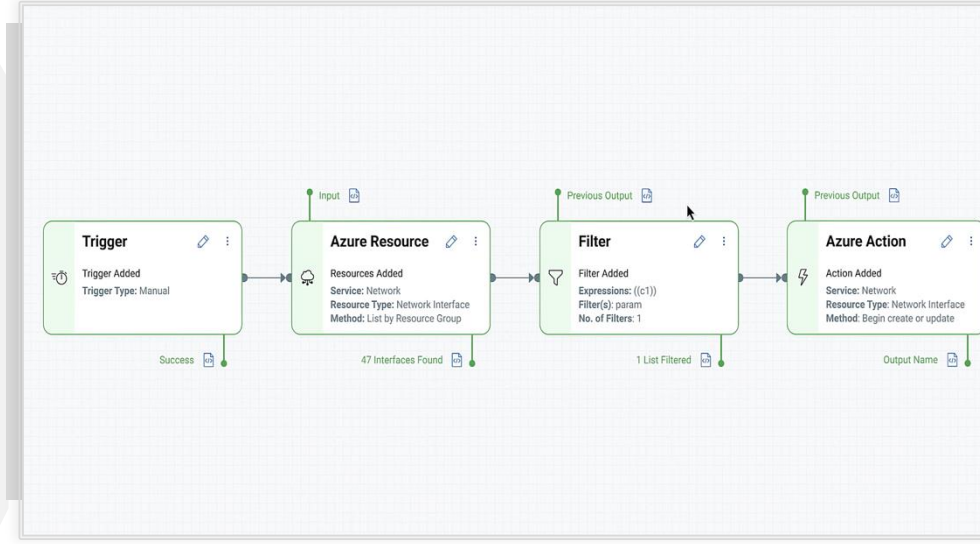
300以上の標準プレイブック
多様なリスク修正シナリオに対応する豊富なテンプレート。

ワークフローのオーケストレーション
DevOpsやITSMツールと統合し、修正プロセスを自動化。

ドラッグ&ドロップで簡単構築
ビジュアルノードを使った直感的な操作でワークフローを作成。

カスタマイズ可能なセキュリティ制御
組織の要件に合わせて柔軟に調整。

セキュリティチームの効率化
自動化により、人的リソースを削減し、対応スピードを向上。



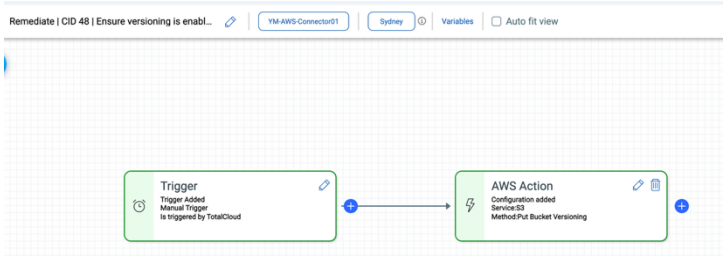
300以上の豊富な修復プレイブック

クラウドワークフロー自動化は、**リスク修正の迅速化・効率化・スケーラビリティ**を実現し、セキュリティ体制を強化するための重要な要素。

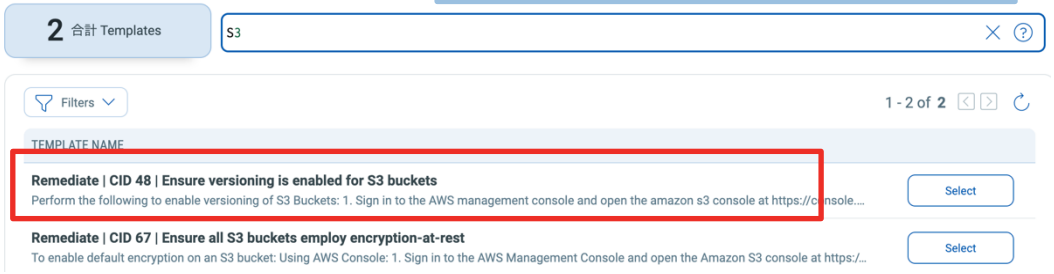
Qualys Flow

Qualys Flow は、Qualysプラットフォーム上で提供される**ノーコード自動化オーケストレーションエンジン**です。ワークフロー（Flow）を視覚的に構築でき、Qualys製品や外部サービスとの連携を通じて、**脆弱性管理やポリシー違反の修復を迅速・一貫して実行**できます。QFlow は、イベント、データ、アクションの論理フローであり、インサイト、コンプライアンスチェック、レポート、修復、アクションなどの特定の出力を取得します。Qualys Flow は、クラウド管理プロセスの自動化に役立ちます。

使用例）「AWS S3 バケットのバージョン管理が有効になっていることを確認する」。有効でなければAWS CLIで有効化する。



すぐに使える167のテンプレート



[Get Started with QFlow]

Blog: [Use Qualys Flow to Automate Detection & Remediation with No-code Workflows]

TotalCloud CIEM Secures Cloud Identities

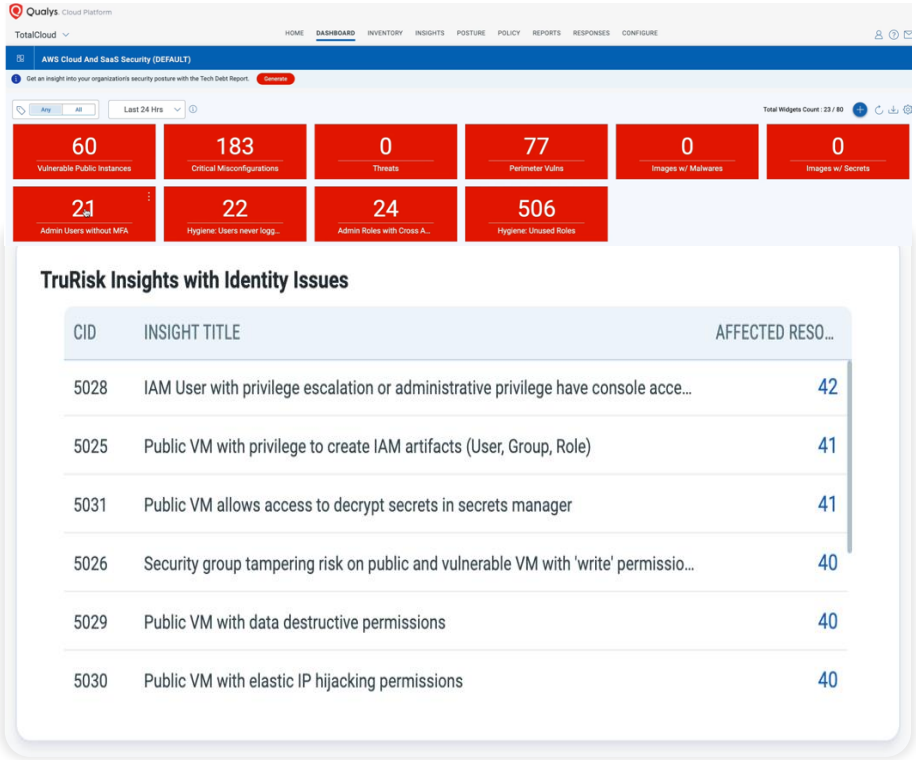
※Blogは[こちら]

クラウドアイデンティティ管理は、権限の過剰付与や設定ミスによるリスクを防ぐために不可欠。**CIEM（Cloud Infrastructure Entitlement Management）**を活用し、リスク評価と優先順位付けを自動化することで、セキュリティ体制を強化します。

完全なインベントリの取得
ユーザー、グループ、ロール、ポリシーなど、クラウドアイデンティティと権限の全体像を把握。

リスクのあるアイデンティティの特定
管理者権限やIAMロール作成など、危険な権限を持つアイデンティティを分析。

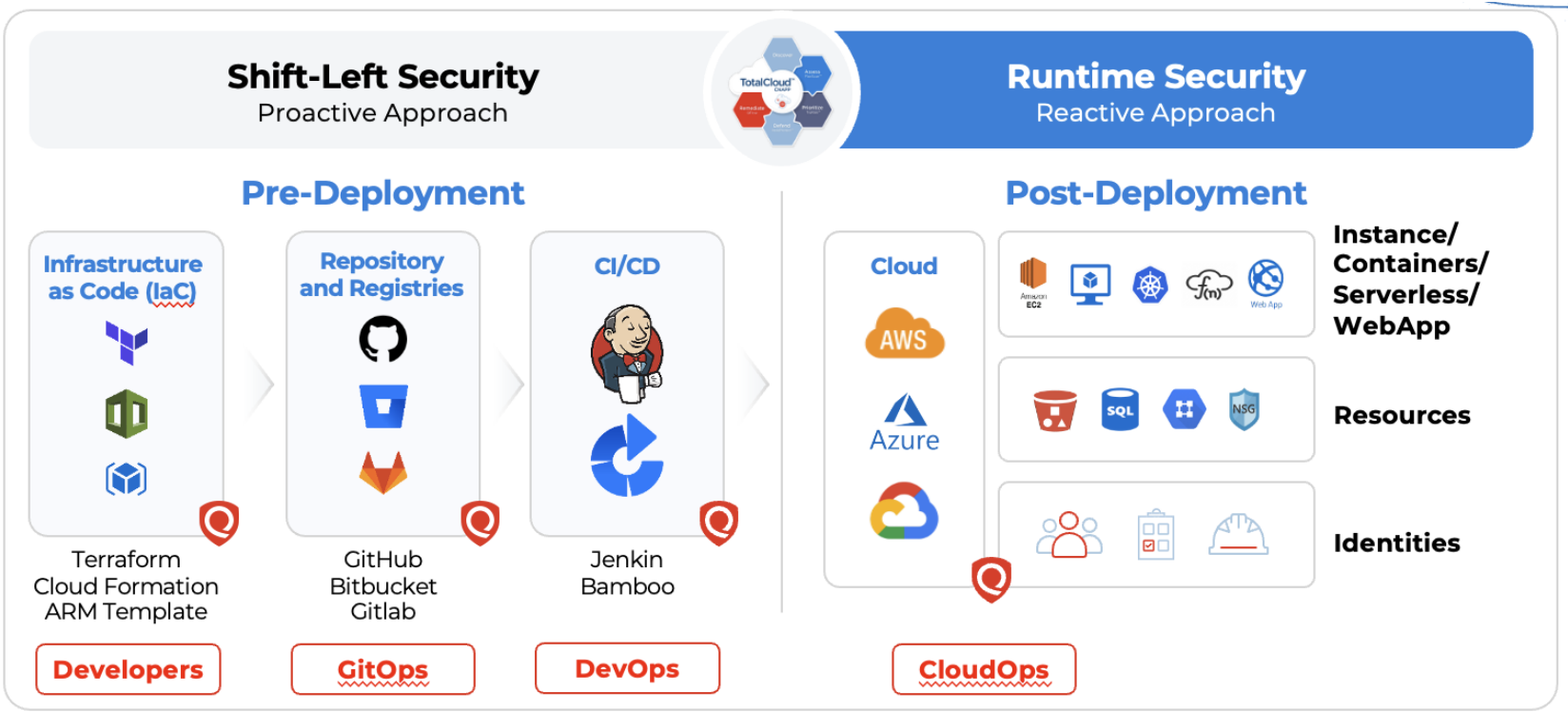
TruRisk Insightsとの統合
リスクのあるアイデンティティをTruRiskスコアに組み込み、優先度付けを強化。



TruRisk Insights with CIEM

クラウドセキュリティにおけるシフトレフト

セキュリティを後工程ではなく、開発初期（コード段階）で実装することで、リスクを未然に防ぐ。
開発ライフサイクル全体でセキュリティを組み込み、継続的にリスクを低減。



TotalCloud

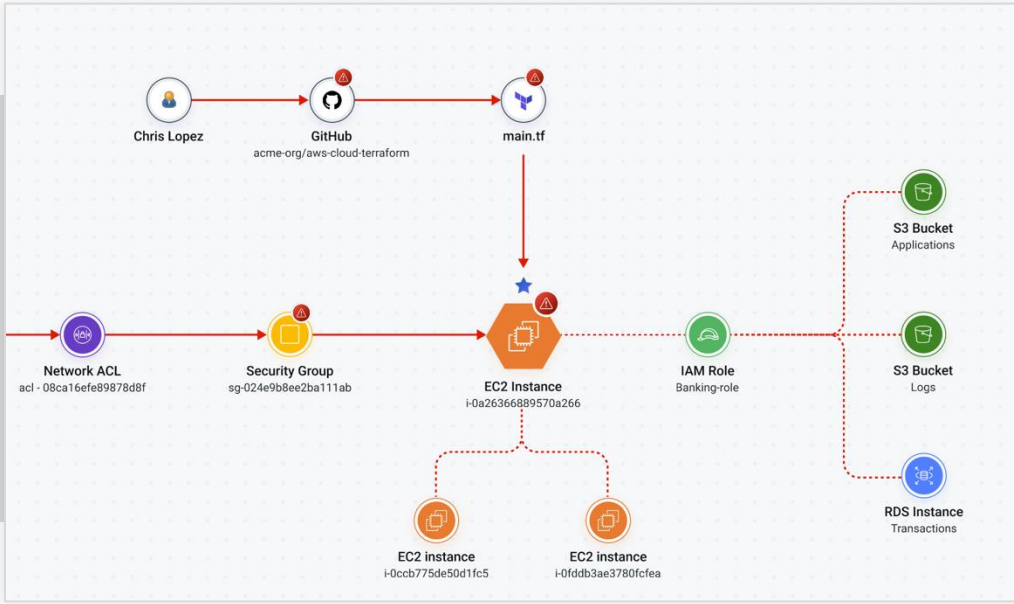
コードにランタイムリスクのコンテキストを提供

実行時リスクをコードに関連付け、開発者が優先的に修正できるようにします

Shift Left and Fix Left を実現することで、クラウドリスクをコードレベルで迅速に解決し、セキュリティ対応を開発プロセスに組み込む。

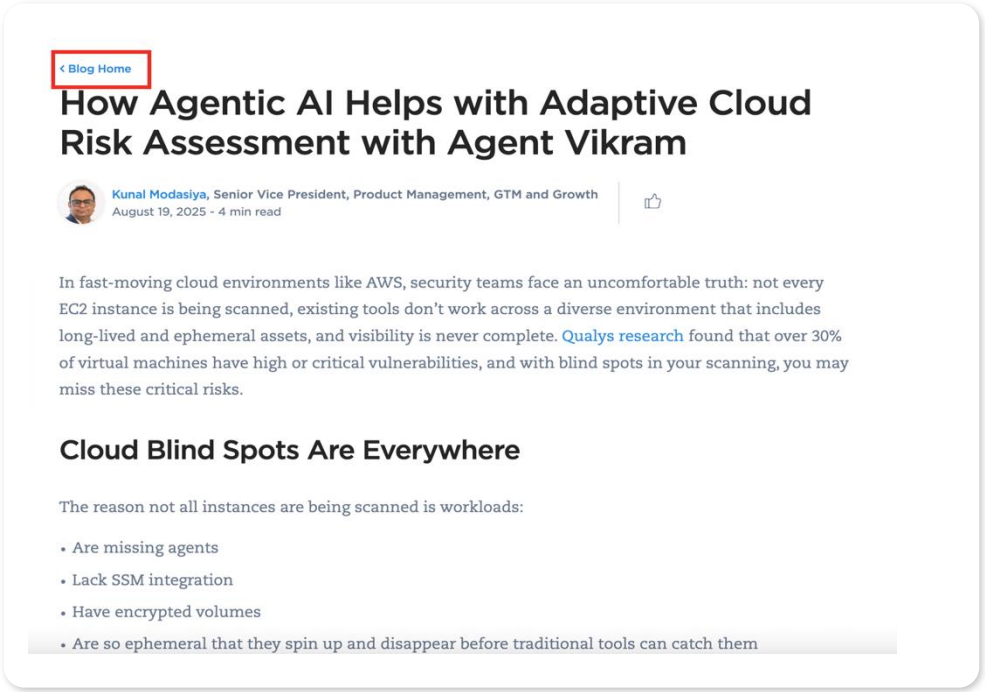
開発者は優先された調査結果とコンテキストを受け取り、まず重要な課題に取り組むことができます。

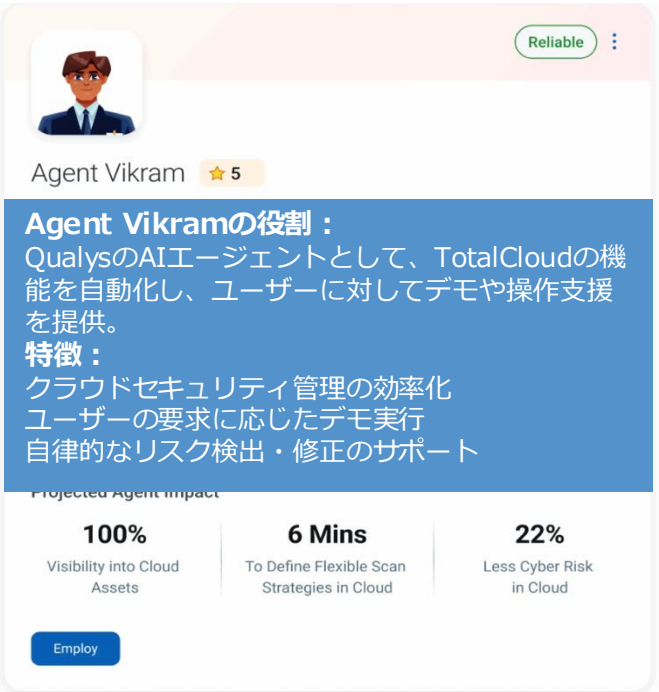
- **開発者を支援する仕組み**
  セキュリティを開発ワークフローに統合し、プロアクティブな対応を可能にする。
- **リスクとコードの関連付け**
  実行時に検出されたクラウドリスクを、原因となるコードにトレース。
- **自動化とスケーラビリティ**
  セキュリティ修正を自動化し、大規模環境でも効率的に対応。
- **優先度付きの情報提供**
  開発者に「どの問題を先に修正すべきか」を明確に提示。
- **戦略的なセキュリティ強化**
  コードからクラウドまで一貫したリスク管理を実現し、セキュリティ体制を強化。



AIエージェント「Vikram」によるTotalCloudの自動化とデモ機能

Blogはこちらから





ServiceNowと統合

ServiceNowとの統合による脆弱性・設定不備の管理と修正を効率化

レスポンスSLAを遵守

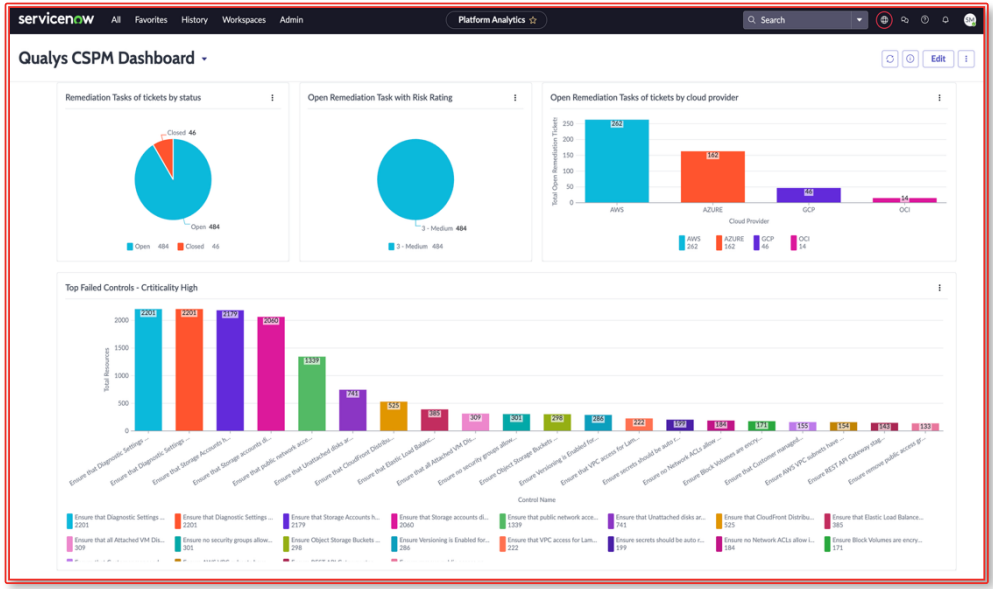
包括的なトラッキングとアクション
ITチームが発見された問題を効率的に追跡し、タイムリーに対応可能。

自動化された脆弱性割り当て
資産所有者に基づいて、修正タスクを開発者へ自動的に割り当て。

幅広い機能の採用
脆弱性管理や設定不備管理を強化するための主要機能を活用。

ServiceNow Modules

脆弱性対応
コンテナ脆弱性対応
構成コンプライアンス



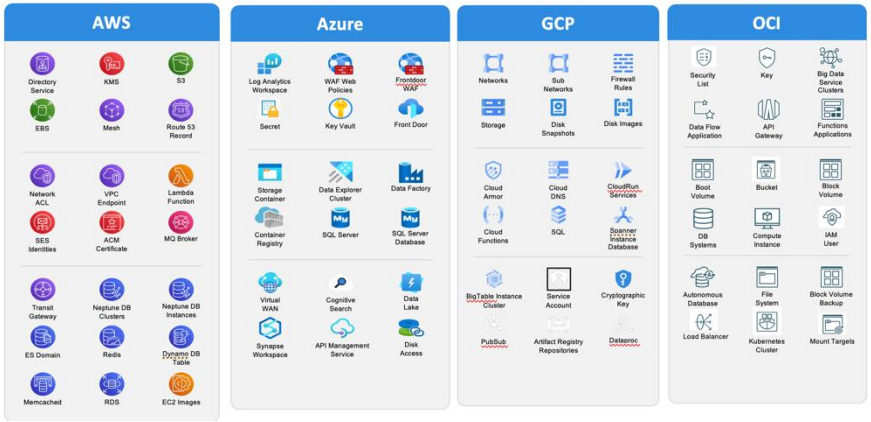
オンプレミスとマルチクラウド

オンプレミスとマルチクラウドを統合し可視化とリスク管理を実現

すべての環境
すべてのクラウド、コンテナ、ハイブリッドワークロードに対応

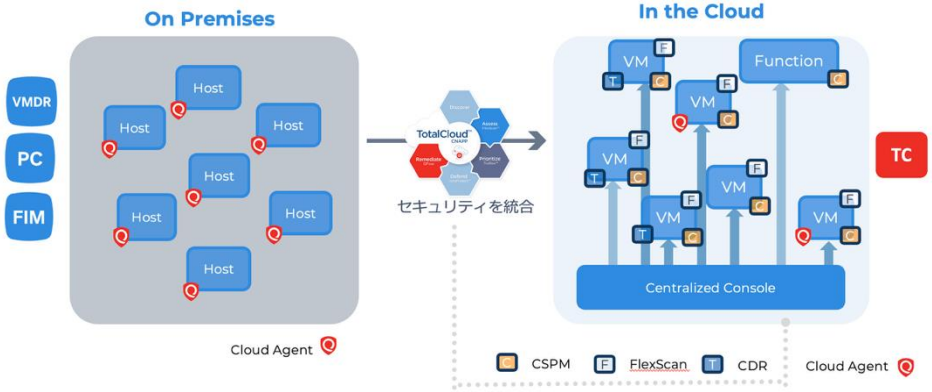
包括的なインベントリ
100%インベントリと
リソースタイプカバレッジ

導入の迅速化
簡素化された迅速なオンボーディングにより、数分で可視性を実現



主な特徴

- オンプレ＋マルチクラウドの両方をシームレスに可視化
- クラウド資産の100%カバレッジ
- ビジネスに即したリスクインサイトを提供
- ノーコード・ローコードによる修復の自動化



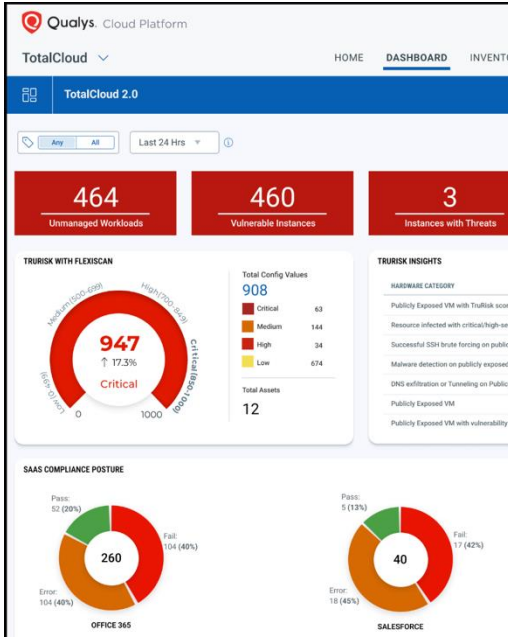
一歩先を行く
統合リスク可視化・自動修復ソリューション

Qualys.

Total Cloud Flex Scan特徴とメリット

FlexScanとTotalCloudで実現できること

1. **クラウド環境に応じた「柔軟なスキャン方式」**：APIベース、スナップショットベース、エージェントベース、ネットワークベースのスキャンを組み合わせて、クラウド環境全体のセキュリティ評価を継続的に実施
2. **ゼロタッチ評価**: エージェントレスでのスキャンにより、システムへの影響を最小限に抑えつつ、迅速な評価が可能
3. **リスクの優先順位付け**: 検出された脆弱性や構成ミスに対して、ビジネスへの影響度を考慮したリスク評価を行い、対応すべき資産の優先順位を明確にする
4. **自動化された修復ワークフロー**: QFlowなどのツールを活用して、検出された問題に対する修復作業を自動化し、対応時間を短縮する（脆弱性と設定ミスを修復する300+のプレイブック）
5. **統合環境によるコスト最適化**：分断されたツールを統合し、CNAPPとして一元的に運用可能
6. **運用負荷の軽減**：自動化・スケーラブルなスキャンによりセキュリティチームの負担を軽減する

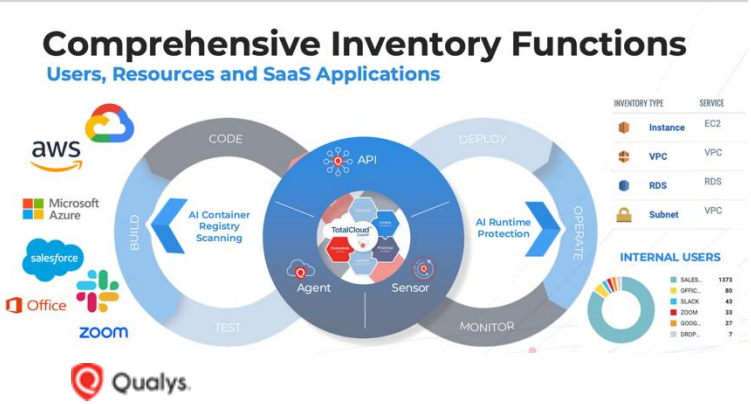


スキャン方式	特徴	利用シーン
APIベース	クラウドサービスプロバイダーのAPIを利用して、継続的なインベントリ収集と構成評価を実施。エージェントレスで迅速なセットアップが可能。	AWS、Azure、GCPなどのクラウド環境での継続的な監視。エージェントの導入が難しい環境。
スナップショットベース	ワークロードのスナップショットを取得し、オフラインで脆弱性評価を実施。一時停止中のインスタンスも評価可能。	M&Aやクラウド移行時の一括評価。定期的なセキュリティチェックを実施したい環境。
エージェントベース	クラウドエージェントを導入し、リアルタイムでの脆弱性、構成、セキュリティ評価を実施。ランタイムの脅威検出も可能。	長期間稼働するワークロード。高精度な脆弱性カバレッジが求められる環境。
ネットワークベース	ネットワーク経由での脆弱性評価を実施。ワークロードの停止不要で導入が容易。	エージェントの導入が難しい環境。ネットワークアクセスが可能な環境。

※各フレックススキャンを利用するための前提条件はこちらをご確認下さい。

SaaS活用を安全に！Qualys SSPMによるセキュリティ構成の最適化

Qualys SSPMは、クラウドファースト・SaaSファーストな環境における**セキュリティ構成の見落としを防ぎ、企業全体のセキュリティポスチャを標準化・強化**するための有効なソリューションです。多拠点・多部門でSaaS活用が進む企業や、ゼロトラストを推進する組織において強く推奨します。



主な機能	概要
SaaS設定の継続的監査	Microsoft 365, Google Workspace, Salesforceなどの設定項目を継続的にチェックし、リスクを検出
セキュリティ設定のベンチマーク評価	CIS Benchmarksや業界ベストプラクティスに基づいたコンプライアンス評価
過剰アクセスや特権アカウントの検出	不要または過剰な権限を持つユーザーや公開設定を特定
リスクベースの優先順位付け（TruRisk）	リスクの重大度をスコア化し、修正の優先順位を明確化
自動修復・ガイド付き修復	修正案の提示またはAPI連携による自動修復機能で対応を迅速化
統合レポートと可視化	ダッシュボードで全体のポスチャ状況を把握し、監査対応用レポートを生成

サポートされているコネクター

- Microsoft Office 365 (Azure AD, Sharepoint, Onedrive, ExchangeOnline, Teams service for Office 365)
- Salesforce(SFDC)
- Zoom
- Google Workspace
- Slack
- Dropbox

※詳細はスタートガイドをご参照下さい。

クォリスによるコンテナセキュリティ

Container Security

*Container SecurityはTotal Cloudライセンスが必須です。また、
Qualys Unit という単位でのライセンス計算となります。

Kubernetes & Container Security カバレッジ

Build
開発ビルドをスキャンする

GitHub
GitLab
Jenkins
Bamboo
Azure DevOps

CI/CDスキャン
脆弱性とシークレットのスキャン
シフトレフトのポリシー制御

Release
リポジトリをスキャンする

sonatype nexus repository
JFrog CONTAINER REGISTRY
Red Hat Quay
HARBOR
docker hub

レジストリのスキャン
(レジストリセンサー)
脆弱性
ゼロデイマルウェア
シークレット検出

Deploy
本番環境をスキャンする

Cluster	Host	Serverless
	docker, aws	

AttackPath分析機能を備えたコンテナ向け VMDR
脆弱性検査とコンプライアンス監査
アドミッションコントロール
(ゼロトラスト展開のブロック)
ランタイムセンサー
脅威の検出と対応(コンテナへのFIM&EDRの利用)

servicenow Jira との緩和策(Remediation)の連携

Qualys.

KCS

Kubernetes &Container Security

AI搭載のコンテナリスクオペレーションセンター

リスクを定量化し、**攻撃経路**と**完全なコード**からクラウドへのコンテキストで修復します。

01

エージェントレスオンボーディング、即時の洞察

eBPFでリスクの高いコード、ビルド、デプロイメント、ランタイム権限をブロックします。

02

DevSecOpsの包括的なコントロール

Kubernetesコントロールプレーンを保護するためにCISベンチマークを強制します。

03

Kubernetesコントロールプレーンを安全に保つ

自動チケット作成のワークフローに加え、自動割り当て、**EOL/EOSの追跡**も可能です。

04

ServiceNowでワークフローを自動化

ノイズを抑え、脆弱性を検証し、仮想パッチを適用するために**リスクの高い資産に集中**します

05

リスク重視の検知と対応

「**eBPF**」は、**Extended Berkeley Packet Filter**の略で、Linuxカーネル上で安全にカスタムプログラムを実行できる仕組みです。もともとはネットワークパケットフィルタリングのために開発されましたが、現在ではセキュリティ、観測、パフォーマンス監視など幅広い用途に使われています。

Qualys.

コンテナセキュリティの評価項目　①

脆弱性検出機能の概要

1. コンテナレジストリのスキャン

スキャン対象: AWS ECR, Docker Hub, GCR, Artifactory などのリモートレジストリをQualysに登録して自動またはオンデマンドスキャンを実施

2. CI/CDパイプラインとの統合

スキャン対象: Jenkins、BambooなどのCI/CDツールと連携し、ビルド時に自動的に脆弱性スキャンを実行します。スキャン結果に応じてビルド停止やチケット起票も可能です。

3. リアルタイムの脆弱性監視

スキャン対象: コンテナセンサーを使用して、実行中のコンテナの脆弱性をリアルタイムで監視し、新たな脆弱性が発見された場合には即座に通知します。

4．ローカルマシンのスキャン

スキャン対象:開発中のローカルDockerイメージへqualys-container-scanner CLIを使ってローカルイメージを直接スキャンします。

5．サーバレスコンテナベースのワークロード（ECS/Fargate）

スキャン対象: FargateタスクやECSのイメージ

マルウェア検査（Malware Scanning）

スキャン対象と検出内容:

1. **コンテナイメージ(Docker Image, OCI形式 Image)**へコンテナレジストリセンサーによる静的マルウェアスキャンを実施。
2. **実行中のコンテナワークロード**（K8s Pod， Docker コンテナ）へコンテナセンサーによるランタイムの不審な挙動をモニタリングし検出。例）マルウェアによる不審なファイル作成、実行、ネットワーク通信
3. **CI/CDパイプラインでビルド生成されたイメージ内**のマルウェアや不正ファイルの検出。

コンテナセキュリティの評価項目　②

セキュリティ構成評価（Compliance Scanning）

スキャン対象と検出内容：

1．**コンテナイメージをスキャンし、** CIS Docker Benchmark、非推奨な設定（rootユーザー使用、ポート開放、特権モード）などを評価。コンテナセンサーもしくは、Scannercliツールによるスキャンを利用。
2．**実行中のコンテナ**（Kubernetes やDocker Swarmなどのオーケストレーション環境で稼働しているコンテナ）をうスキャンし、実行ユーザー、ファイルシステムの設定、実行中のプロセスなどを評価。センサーがDeamonSetでクラスタに配置されている場合、自動的に監視します。
3．**ホストノード**にCloud Agentを導入し、Policy Auditモジュールで評価する。

Secret 検出

スキャン対象と検出内容:

コンテナイメージ内のコンテナイメージ内のパスワード、APIキー、その他の資格情報などの機密情報の存在を発見するための一連のルールを作成し検出します。

Kubernetesのポスチャ管理（KPM）

機能内容：Kubernetesクラスター内のすべてのコンテナ資産（イメージ、コンテナ、レジストリなど）を自動的に検出し、継続的に追跡します。Cluster Sensorと連携し、様々なクラウドプロバイダーが提供するCISベンチマークに基づく**ポリシー評価**をサポートします。これにより、コントロールの脆弱性を特定し、セキュリティ強化ポリシーを適用し、ハイブリッドKubernetes環境とマネージドKubernetes環境の両方で継続的なコンプライアンスを維持できます。

- マニフェスト（YAMLファイル）やクラスタ設定のセキュリティベストプラクティスとの比較
- CIS Kubernetes Benchmark準拠のチェック
- Role-Based Access Control（RBAC）や認証設定の確認
- ポリシー違反のアラート通知

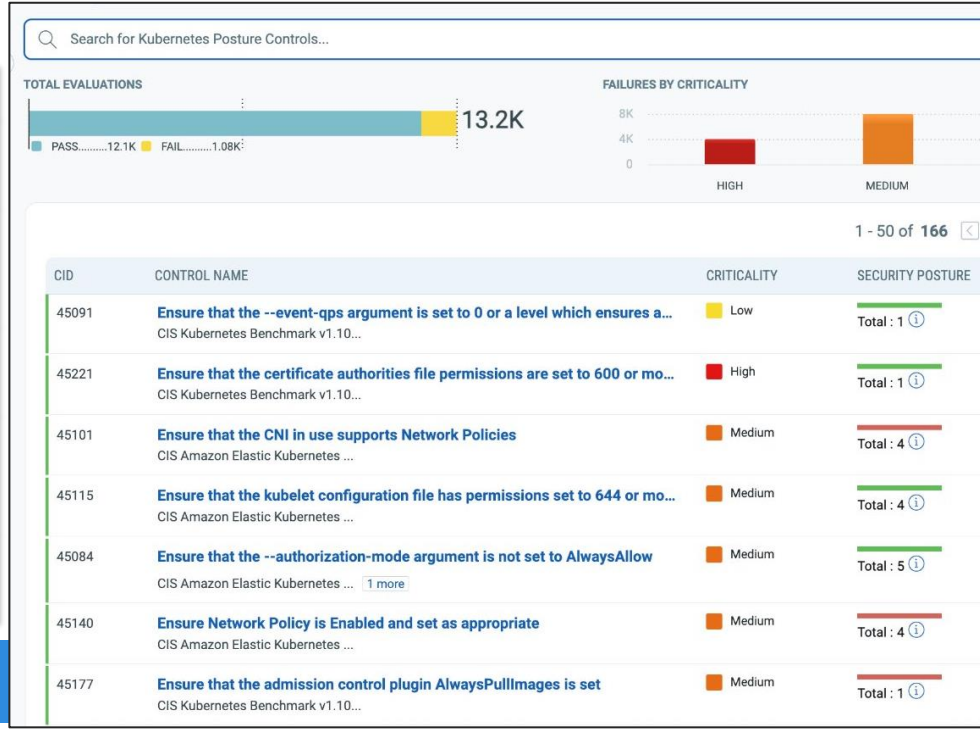
Kubernetes Posture (KSPM) + Admission Controller

Kubernetes環境の**設定監査と脅威ブロックを一体化**して提供。セキュリティとコンプライアンスを”開発段階”から“運用中のクラスタ”まで包括的にカバーし、**DevSecOpsの強化と運用コストの削減**を実現。

Policy Audit ※機能強化による利便性

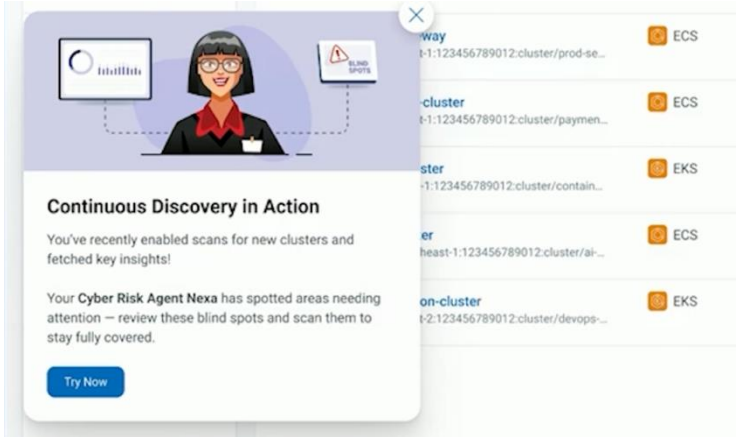
改善点	内容
Kubernetes特化のポリシーテンプレート追加	CIS Kubernetes Benchmarkの自動適用やカスタムポリシー対応。
構成ファイルレベルの監査	kube-apiserver.yamlやkubelet-config.yamlなどの設定ファイルを対象に検証。
スケジュールされた自動監査	定期的に構成監査を実行し、継続的な準拠状況を確認。
コンプライアンスレポートの自動生成	視覚的にわかりやすい形式で、経営層向け／技術担当向けの両方に適した出力。
リスクの優先度付けと対応支援	ポリシー違反ごとのリスクスコア表示や是正ガイド提示。

Over 200+ CIS-Certified Controls

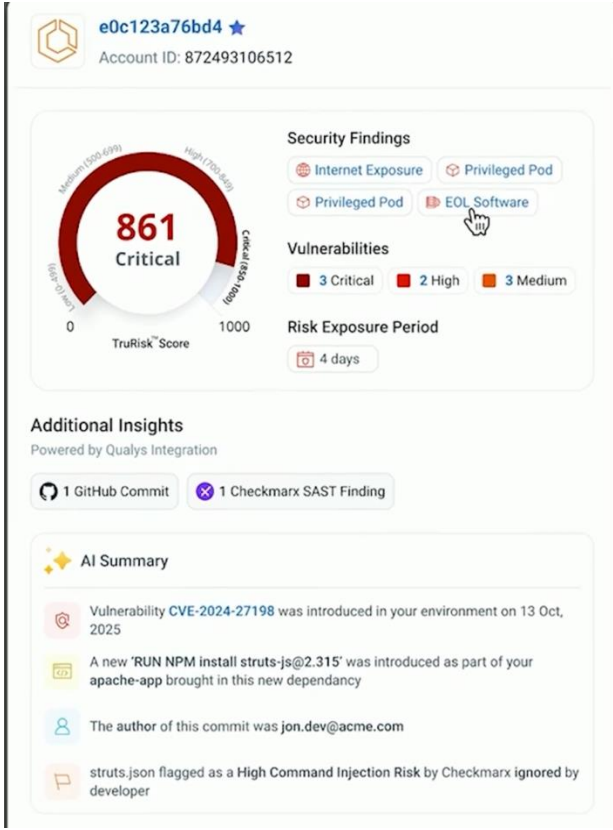


※Policy Auditは有償モジュールです。

コンテナのAttack Pathによる優先的な修正対応

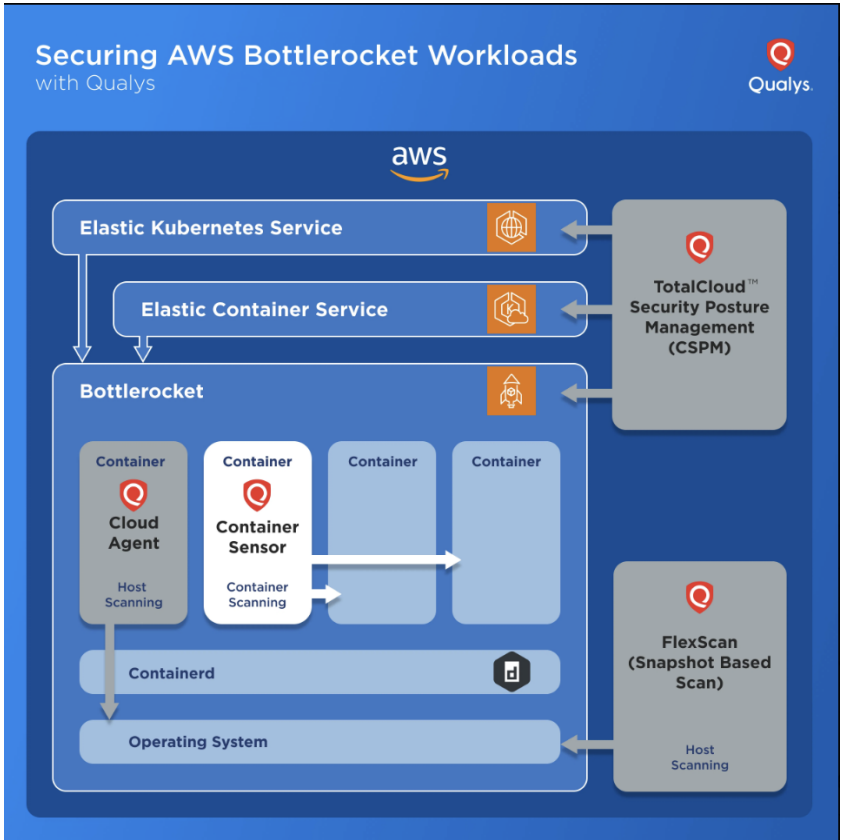


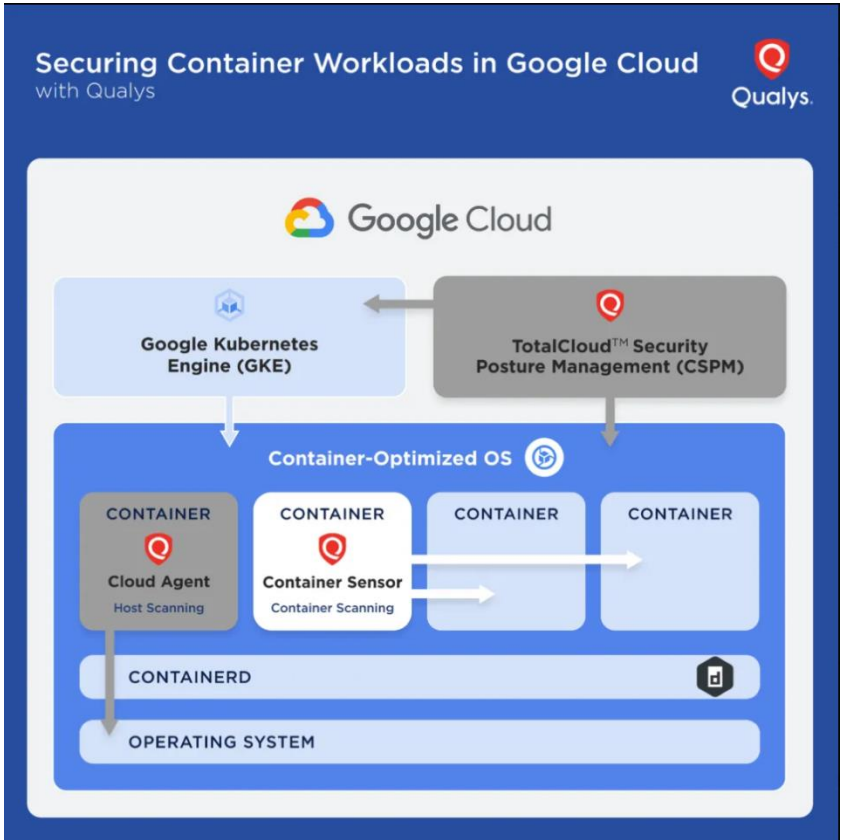
Cyber Risk Agent NexaはROCの中核として機能し、ゼロタッチの自律的なリスクオペレーションをサポートします。



Qualys.

AWSとGCP上のQualys導入構成図





Shift LeftからShift Fixへリスクオペレーションの自動化を実現

KCS(ROC)

市場背景

- 2028年までに95%の企業がコンテナ化アプリを利用する見込み（Gartner）
- 新しいKubernetesクラスタは作成後18分以内に攻撃される（Kubernetes Security Report 2025）

課題

- ✓ 短命な資産だがリスクは持続。
- ✓ 脆弱性やアラートが過剰で優先度が不明確。
- ✓ 所有権の不明確さや再構築によるチケット断絶。
- ✓ リスク基準が常に変化するため、メトリクスが不安定。
- ✓ 「Shift Left」だけでは不十分 →「Fix Left」が新しいマントラ。

大手金融機関での導入例：

- 200万コンテナをスキャン。
- 50万のリスクエクスポージャーを検出。
- 3万のビジネスクリティカル資産、300の攻撃パスを特定。

Qualys最新のアプローチ

- Risk Operations Center (ROC)：リスクを定量化し、攻撃パスを可視化。
- TruRiskスコアと攻撃パス分析で、ノイズの多い攻撃面をリスク面に変換。
- **ガイド付き**リスクチェーン分解で迅速な対応。

ソリューションの特徴

- エージェントレスで即時リスク可視化（クラスタ、レジストリ、サーバレス対応）
- コードからクラウドまでのコンテキスト提供
- Kubernetes Security Posture Management (KSPM)：CISベンチマーク準拠、構成ドリフト検出
- ServiceNow連携でチケット管理を自動化し、MTTRを短縮
- eBPFによるランタイム保護と脅威検出
- PCI-DSS 4.0対応のコンテナFIM

Total Cloud 評価

Qualys®

業界をリードするCNAPP

すべての主要分野における確立されたリーダーシップと信頼

2025年カスタマーボイス
ストロング・パフォーマー

CNAPP マーケットスペース 2025
能力のトップ5
主要選手として認められた

ベストクラウドセキュリティ(TotalCloud)
最優秀Vuln Managementを3年連続で獲得
(VMDR)

製品および市場でのリーダーシップ
クラウドセキュリティ、CTEM、そして
ハイブリッドクラウドエコシステム

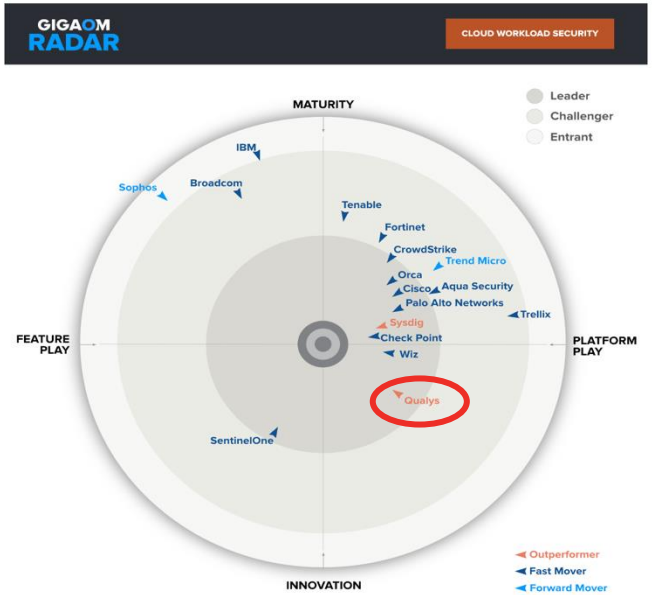
CNAPPのリーダー
コンテナセキュリティ、クラウドワークロード
セキュリティ、CIEM

Qualys.

TotalCloud – クラウドセキュリティ市場の認知度

アナリストによる評価

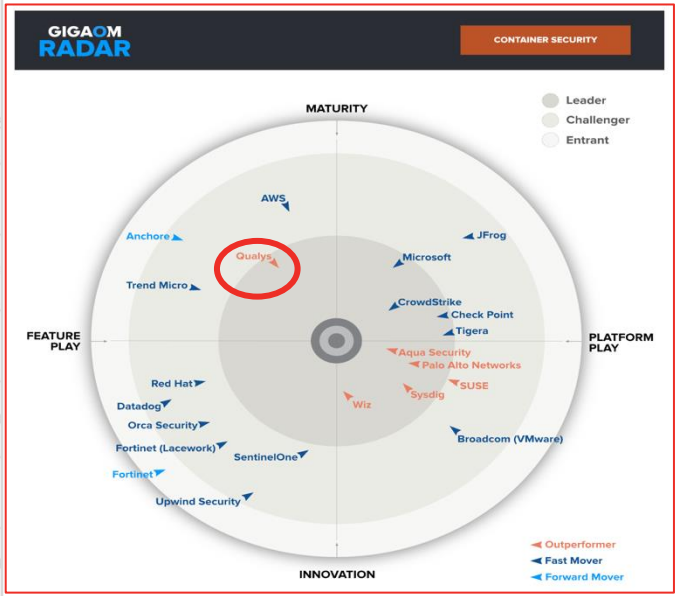
2025 Leader - Cloud Workload Security Radar



「ベンダーの積極的な開発ロードマップにより、クラウド ワークロード保護機能が大幅に進歩しました。」

企業からの信頼

2025 Leader - Container Security



「Qualys は、継続的なイノベーション、頻繁なリリース頻度、将来を見据えた製品ロードマップにより、アウトパフォーマーに分類されました。」

Qualys.

TotalCloud - クラウドセキュリティ市場の認知度

アナリストによる評価

"AI と ML を活用してリスクを検出してランク付けし、セキュリティ体制を強化するための調整のための修復を行います"

企業からの信頼

「ビジネスの重要度とリスクに基づいて、構成ミス、脆弱性、資産に優先順位を付けます。」

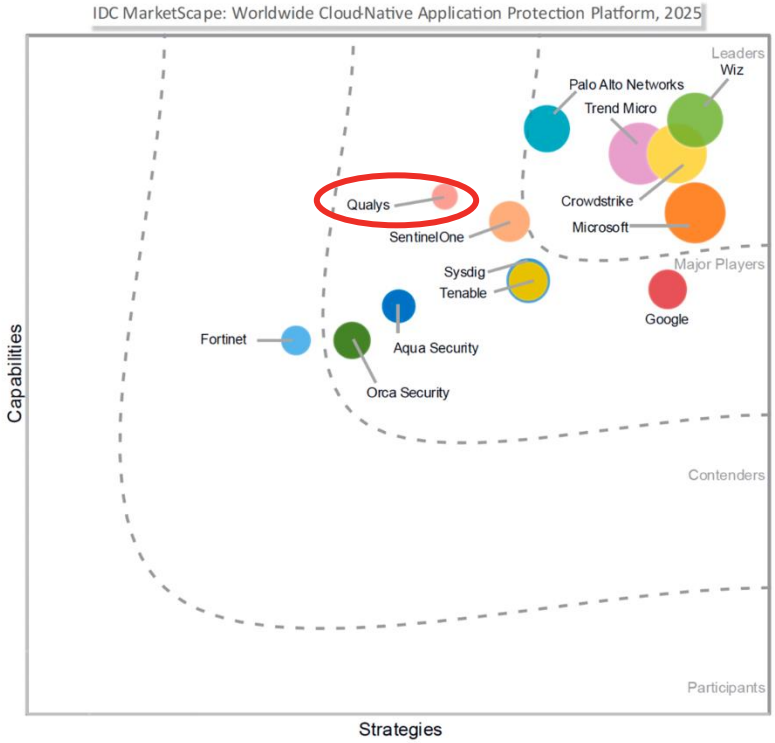
Qualys.

TotalCloud - クラウドセキュリティ市場の認知度

アナリストによる評価

企業からの信頼

2025 年の主要企業 – IDC MarketScape ワールドワイド クラウド ネイティブ アプリケーション保護プラットフォーム



***Qualys* は、*CNAPP* 機能の市場でトップ *5* のベンダーにランクされました。**

***IDC*によると:**

- 「Qualys は革新的なソリューションと顧客の成功への取り組みを提供します。」
- 「シンプルさにより価値実現までの時間が大幅に短縮され、顧客は導入後ほぼすぐに実用的な洞察を導き出すことができました。」
- 「すべてのクラウドプロバイダーで標準化できることは大きな利点であり、管理が簡素化され、一貫したセキュリティ体制が確保されます。」
- 「Qualys の自動化されたワークフローにより、修復が加速され、重大な問題の MTTR が短縮されます。」

エンタープライズグレードの規模:

- **4,500 万**のマルチクラウド ワークロードが TotalCloud Flexscan テクノロジーを使用してスキャンされます。
- **4,500 万**のマルチクラウド ワークロードが TotalCloud Flexscan テクノロジーを使用してスキャンされます。
- **800社以上の顧客から40,000のクラウドアカウント**があり、TotalCloudによって保護されています

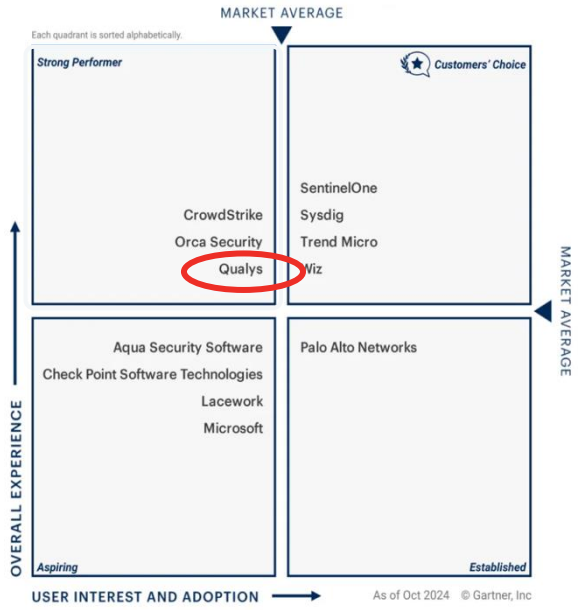
Qualys

TotalCloud - クラウドセキュリティ市場の認知度

アナリストや顧客から認められる

Gartner

2024 Strong Performer - Peer Insights
Voice Of The Customer - CNAPP



PeerSpot

Qualys TotalCloud

Reviews, Tips and Advice from Real Users

April 2025

"I appreciate TotalCloud's real-time protection and remediation features. The remediation options include automated one-click remedies and custom changes that help manage vulnerabilities efficiently."

HASHIM JUNAID

Service Manager, Security Operations at CDA IT SOLUTIONS

"TotalCloud has yielded significant cost savings by reducing manual effort by 20 to 30 percent and generating overall savings of 30 to 40 percent across various departments.."

Verified user

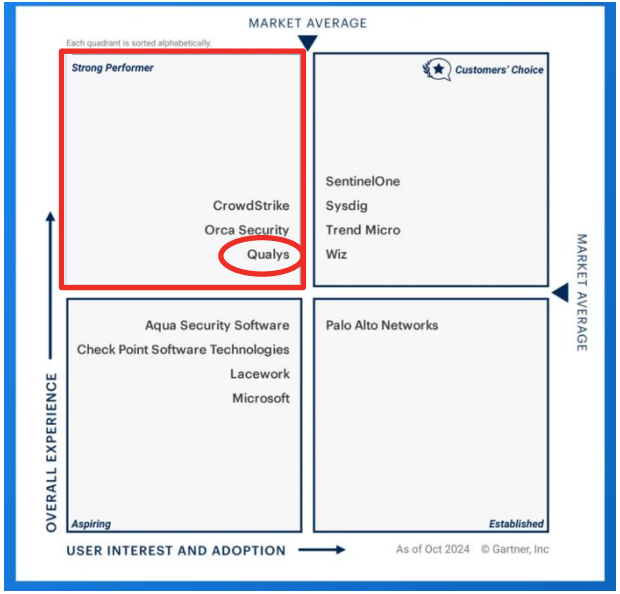
Security Manager at a consultancy with 10,001+ employees

Read full review

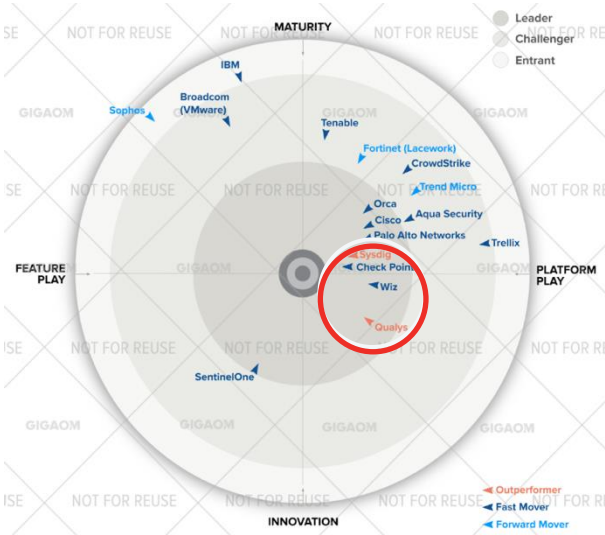
Qualys TotalCloud CNAPPのポジショニング

KuppingerCole
2024 Leadership Compass for CSPM

Gartner
2024 Peer Insights Voice Of The Customer - CNAPP



GigaOm
2025 Cloud Workload Security Radar



kuppingercole ANALYSTS

Gartner

GIGAOM

Qualys

Qualys®

Enterprise TruRisk™ Platform

Measure, communicate, and eliminate cyber risk.

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。