Qualys Trurisk Platform
ソリューション概要

Qualys Japan K.K
更新日2025年9月

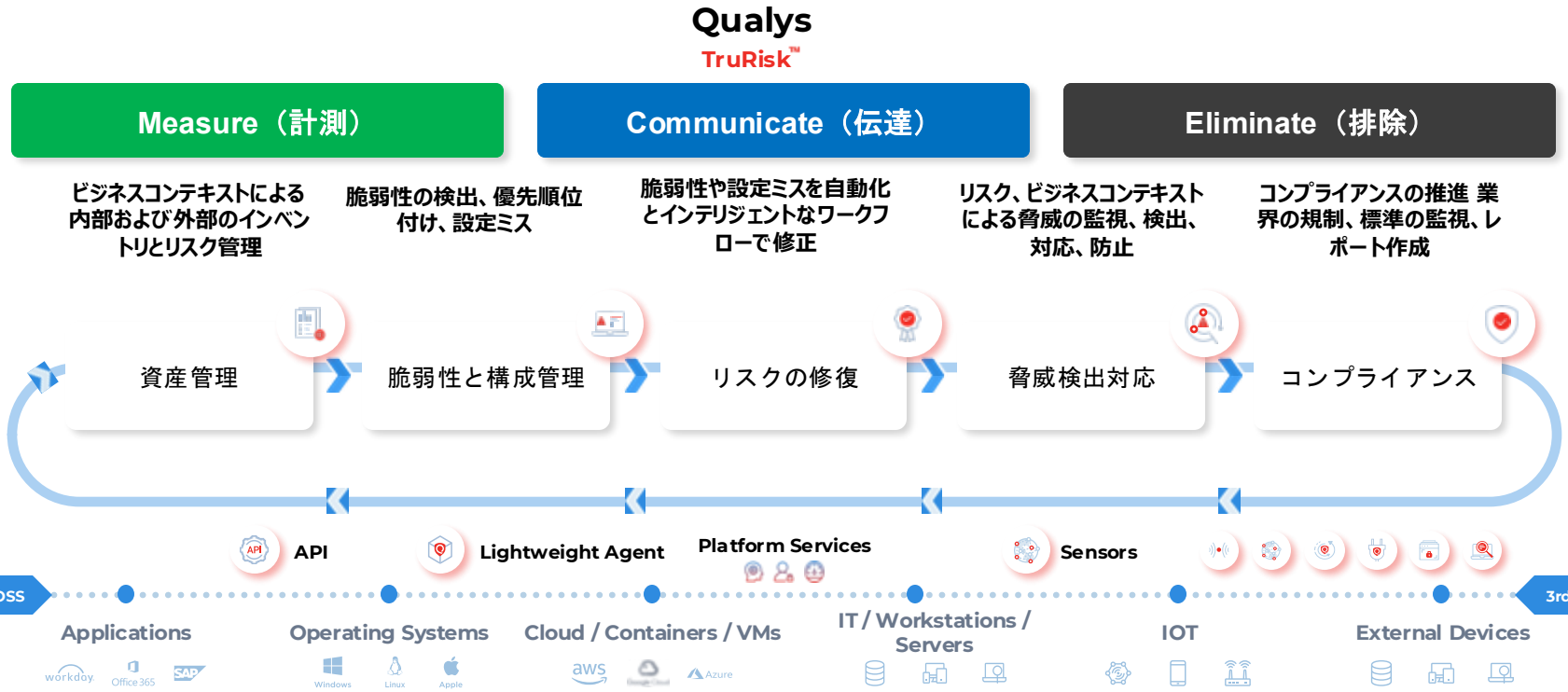
目次

- クォリスプラットフォームの紹介
- クォリスによる資産管理
- クォリスによるリスク管理とリクス修復
- クォリスによるAppSecセキュリティ
- クォリスによるクラウドセキュリティ
- クォリスによるコンプライアンス
- クォリスによるリスクベース優先順位付け
- クォリスによるAI,LLMセキュリティ
- クォリスによるコンテナセキュリティ
- クォリスクラウドエージェントの特徴
- Qualys 補助資料
- Qualys マーケット情報

クォリスプラットフォームの紹介

Enterprise TruRisk Platform
Vulnerability Management Detection and Response（VMDR）

Qualys Enterprise TruRisk Platform



Qualys VMDR with TruRisk™

最も高速、最も正確、そして最も包括的なリスクベース脆弱性管理（RBVM）ソリューション

4 修復	ワークフローの自動化	パッチ管理	緩和	
	ITSM (ServiceNow, Jira, Qflow)	脆弱性の修正	脆弱性を軽減するか資産を隔離する	
3 優先順位付け	リスクの優先順位付け	攻撃対象領域	脅威インテリジェンス	
	Qualys TruRisk スコアリング	攻撃対象領域管理（内部および外部）	25以上の脅威とエクスプロイト情報	
2 評価	資産インベントリ	証明書インベントリ	脆弱性評価	OSSと1stパーティリスク
	ネイティブに統合されたオンプレミス/クラウド資産インベントリ	有効期限切れ／期限切れ証明書の追跡	リアルタイムの脆弱性と構成の評価	20,000 件以上の脆弱性に対する OSS 評価
1 発見	脆弱性の範囲	CIS/DISA STIGS 強化	スピードと正確さ	包括的なセンサー	APIs
	10 万以上の CVE、重要な CVE を 24 時間以内にカバー	攻撃対象領域の強化（300以上のポリシー）	• 4 時間以内に脆弱性を検出 • 99.99966% の精度	エージェント、仮想/物理スキャナ、パッシブセンサー、外部スキャナ	APIファーストソリューション、サードパーティのレポートプラットフォームとの統合

企業全体のサイバーリスクを軽減
サイバーセキュリティ対策をビジネス成果に結び付ける

Qualys.

ROI: ビジネス成果の実現

統合アプローチで攻撃対象領域を削減

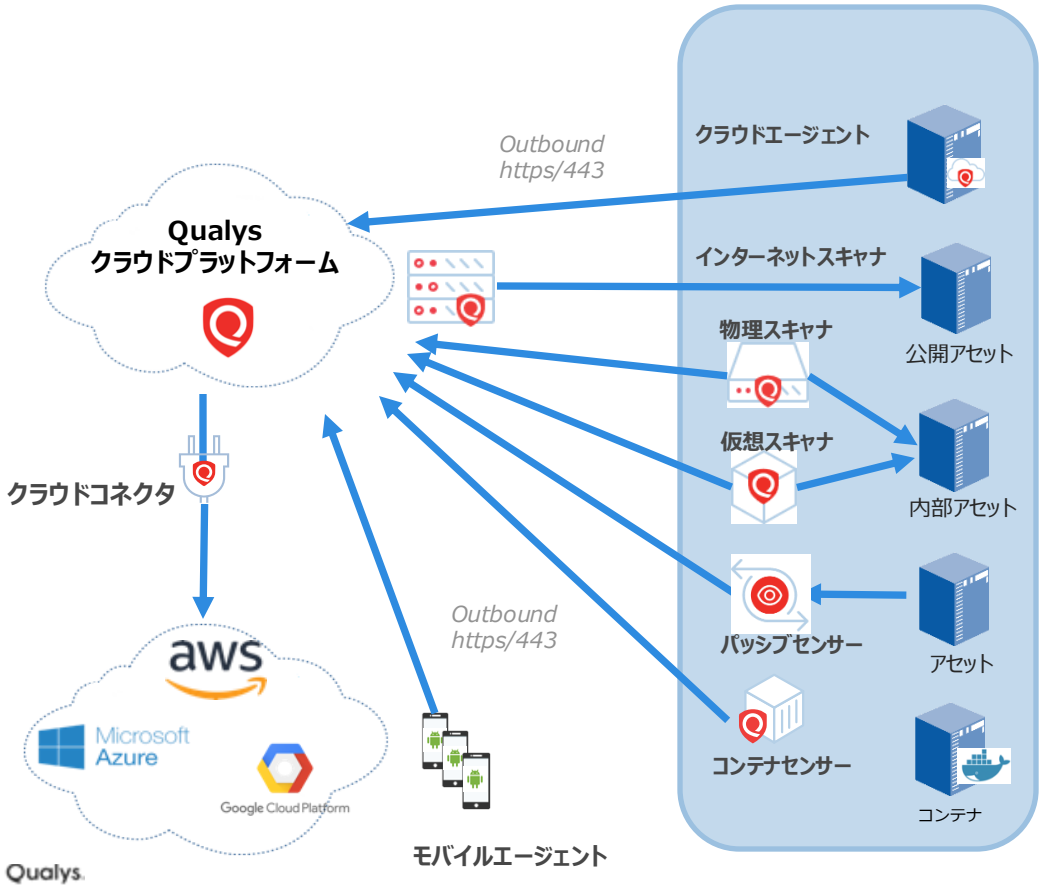
Qualys導入メリット

項目	内容
統合型プラットフォーム	アセット管理、脆弱性管理、脅威インテリジェンス、リスク評価を1つのプラットフォームに統合。エージェント／センサーも統一。
TruRisk™優先順位付け	CVSSスコアだけでなく、攻撃の可能性・資産重要度・脅威活性度を組み合わせ、ビジネスリスクに直結する脆弱性を優先。
偽陽性の大幅削減	高精度の検出エンジンにより不要なアラートを削減し、対応工数を最適化。
自動化による運用効率化	スキャン・評価・レポート・修復ワークフローの自動化し修復期間を短縮。SecOps/ITOps間の連携もスムーズに。
脆弱性管理（VMDR）	資産検出、脆弱性評価、リスクスコアによる優先順位付け、パッチ管理までワンストップで実施。
外部攻撃面（EASM）への拡張性	シャドーIT・未管理ドメインの検出とリスク評価を自動で行い、ゼロデイ脅威も含めて監視。

ROI（Return on Investment）

観点	効果
リスク削減	TruRiskにより、重要な脆弱性への対応を絞ることで **リスク23〜50%削減**（Qualys試算）
対応時間の短縮	脆弱性対応の平均時間（MTTR）を**大幅短縮**（例：30日→5日など）
人件費・ツールコスト削減	エージェントの一元化により、ツールスプロールの抑制。サイロの解消で**運用効率が向上**
コンプライアンス対応効率化	各種ガイドライン（PCI DSS, NIST, ISO等）に基づいた**継続的な監査対応の自動化**
インシデント発生コストの抑制	リアルタイムのリスク監視により、**サイバー攻撃の発見と封じ込めを迅速化**
最新情報の確認・報告対応の短縮（ダッシュボード・レポート）	役職別ダッシュボード・レポート（CISO向け・SOC向けなど）で**リスクの可視化と報告が容易**

環境に合わせた様々なスキャン方法



① クラウドエージェント
サーバ、クライアントにクラウドエージェントをインストールし、アセット情報を収集。

② スキャナ
インターネットスキャナ、物理スキャナ、仮想スキャナがリモートスキャンや認証スキャンでアセット情報を収集。

③ パッシブセンサー
ミラーポートに接続し、トラフィックからアセット情報を収集。

④ コンテナセンサー
Docker上にコンテナセンサーを配置し、コンテナ情報を収集。

⑤ クラウドコネクタ
AWS/Azure/GCPにネイティブAPIで接続し、クラウド上のリソース情報を収集。

⑥ モバイルエージェント
スマートフォンにエージェントをインストールし、スマートフォンの情報を収集。

クォリスアセットインベントリ

収集したメタデータは、Qualysのダッシュボードやレポート機能を通じて可視化され、組織のIT資産管理、セキュリティ対策、コンプライアンス遵守に貢献します。

1. ハードウェア情報

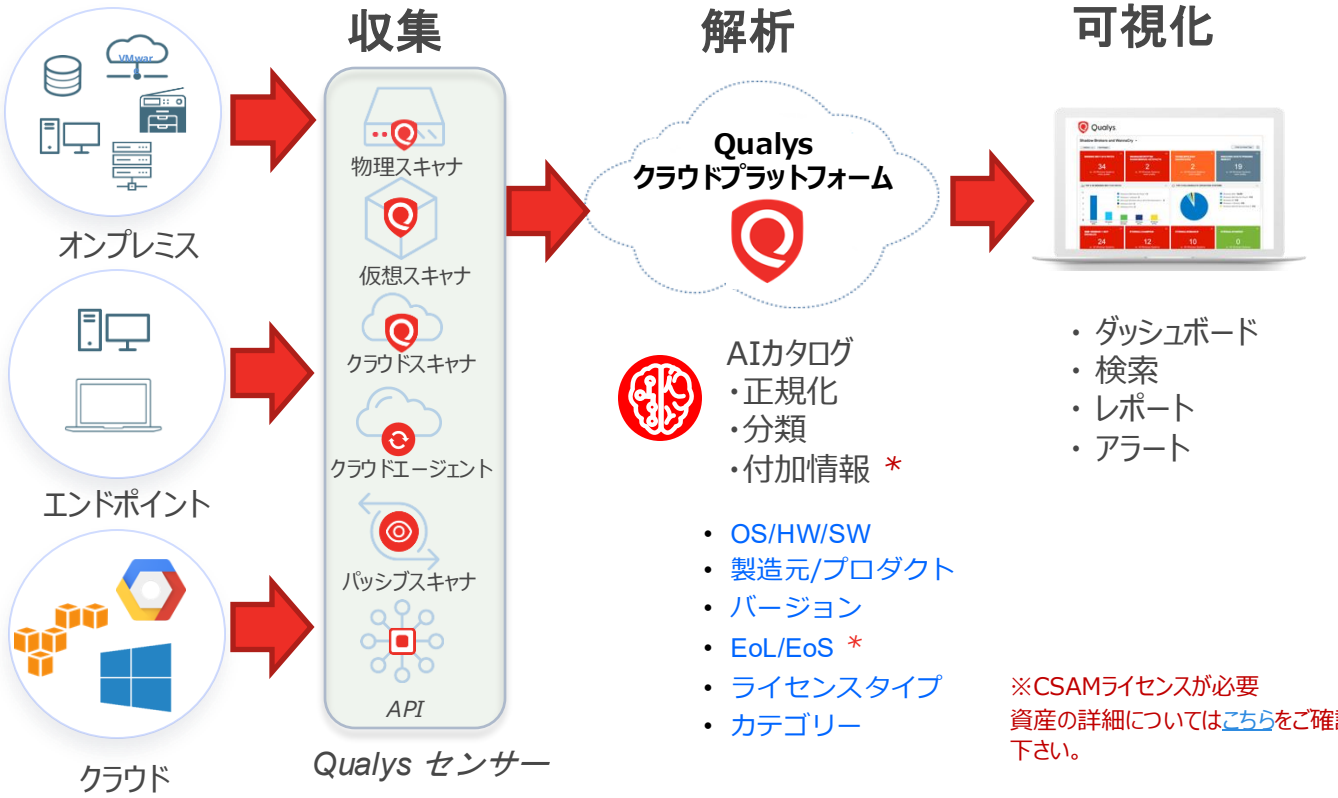
基本情報: ホスト名、IPアドレス（IPv4/IPv6）、FQDN、NetBIOS名など。
ハードウェア仕様: CPU、メモリ、ディスク容量、GPU、LPAR ID（AIX環境）など。
ネットワーク情報: MACアドレス、ネットマスク、ネットワークインターフェースの詳細。
地理的位置情報: パブリックIPに基づくアセットの地理的な位置

2. ソフトウェアおよびサービス情報

インストール済みソフトウェア: アプリケーション、OS、ドライバ、ユーティリティ、プラグインなど。
実行中のサービスとプロセス: サービス名、ポート番号、プロセスIDなど。
ユーザー情報: ログインユーザー、最終ログイン日時、ユーザーアカウントの詳細。
CPE（Common Platform Enumeration）情報: ソフトウェアやハードウェアの標準化された識別子。

3. クラウドプロバイダーメタデータ

Qualys Cloud Agentは、主要なクラウドプロバイダー（AWS、Azure、GCP、IBM、OCI、Alibaba）からインスタンスメタデータを収集します。これには、インスタンスID、リージョン、アベイラビリティゾーン、インスタンスタイプなどが含まれます。



※CSAMライセンスが必要
資産の詳細についてはこちらをご確認下さい。

脆弱性検知レポートの出力例

Qualys脆弱性検知レポートの主な特徴

◎多言語対応と詳細な情報提供

レポートは日本語と英語で出力可能です。検知された脆弱性をQID（Qualys ID）単位で表示し、関連するCVE（共通脆弱性識別子）を含めて詳細に記載します。

◎リスク評価と可視化

各脆弱性には重大度（Severity）やCVSSスコアが付与され、赤（確認済み脆弱性）、黄（潜在的な脆弱性）、青（情報収集用）などの色分けで視覚的にリスクを把握できます。

◎対処方法と根拠の明示

脆弱性の対処方法は「SOLUTIONS」に、検出の根拠は「RESULTS」に記載され、具体的な対応策とその理由を明確に示します。

◎リアルタイム脅威インテリジェンスとの連携

CISAの既知の悪用可能な脆弱性（KEV）カタログやEPSS（Exploit Prediction Scoring System）などの脅威インテリジェンスと連携し、最新の脅威情報を反映します。

Qualysレポートのメリット

◎リスクベースの優先順位付け

独自のスコアリングシステム「TruRisk」を活用し、資産の重要度（ACS）や脆弱性の危険度（QDS）を評価し、対策の優先順位を明確にします。

◎自動化と効率化

スキャンからレポート作成、通知までを自動化し、セキュリティチームとITチームの連携を強化します。

◎コンプライアンス対応

PCI-DSSやNISTなどの業界ベンチマークに準拠したレポートを提供し、監査対応を支援します。

Qualysモジュール全体図

脆弱性管理&設定管理

- VMDR — Vulnerability Management Detection and Response
- NEW TAS — TotalAppSec(WASの後継モジュール)
- CWP — Cloud Workload Protection
- CSPM — Cloud Security Posture Management
- NEW TAI — TotalAI
- KCS — Container Security
- IaC — Infrastructure as Code Security
- SSPM — SaaS Security Posture Management

コンプライアンス

- NEW PA — Policy Audit
- SAQ — SecurityAssessmentQuestionaire
- FIM — File Integrity Monitoring

資産管理

- CSAM — CyberSecurity Asset Management
- EASM — External Attack Surface Management

リスクの修復

- PM — Patch management
- NEW TE — TruRisk Eliminate
- CIEM — Cloud Infrastructure and Entitlement
- CAR — Custom Assessment and Remediation
- NEW CWA — Cloud Workflow Automation

脅威の検出と応答

- EDR — Multi-Vector Endpoint Detection and Response
- CDR — Cloud Detection and Response

- ETM — Enterprise TruRisk Management
- NEW Agentic AI — Enterprise TruRisk Management

左記モジュールの中核となるモジュール。
相互連携可能。

クォリスによる資産管理

Cybersecurity Asset Management（CSAM）

*CSAMはVMDRライセンスとの併用が必須です。

内部・外部の攻撃対象領域全般のリスク管理

資産の可視性のギャップを見つけて埋める

✓攻撃対象領域全体をカバー

✓市場で最も包括的な資産発見

30%以上の新たな資産を発見

ビジネスコンテキストでVMを高速化

✓ VM プログラムの資産カバレッジの改善

✓ 資産カテゴリ、資産構成、ビジネスコンテキストに基づいて正確なリスクの優先順位付けを推進

ACSの5倍の効果

内部資産

Agent, Scanner, Sensors

外部資産

Open-source Tech & Qualys Internet scanner

Scanner

クラウド資産 *Update!*

Monitor your Cloud environment

第三者からの資産 *Update!*

API-Based Connectors

IoT/OTと不正な資産

Passive Network Sensing & CAPS

※Asset Criticality ScoreとはQualysが提供しているお客様による資産の重要度スコア。詳しくはこちらを御覧ください。

環境適したスキャン手法で包括的にリスクを可視化

脆弱性の検出と評価
リモートのみの脆弱性とSSLベースの脆弱性を検出

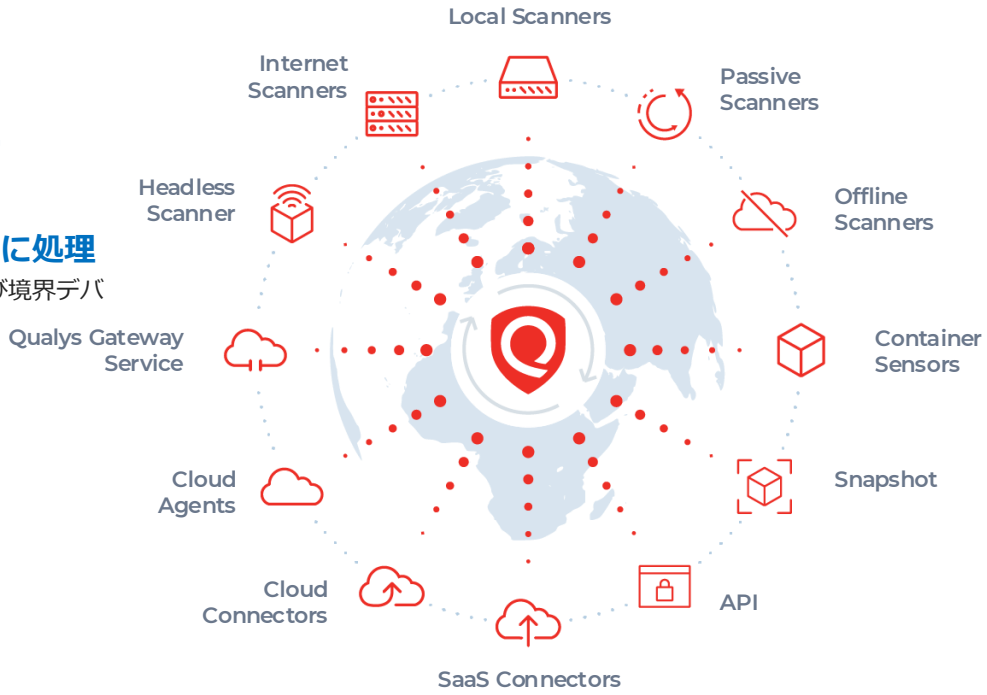
ダイナミックハイブリッド環境のリスク軽減
エージェントを配備できないクラウド資産を防御

武器化されたエクスプロイトコードを優先的に処理
エンドポイントエージェントが見逃したネットワークおよび境界デバイス上で悪用されたCISA KEVの21.7%

デジタル証明書の評価
リモートスキャンで不足している証明書を特定

CISベンチマーク
CSP全体でベンチマークの50%が失敗しています。クラウドコネクタ、API、スナップショットスキャンで可視性を高めましょう。

AIとLLMのリスク評価
ネットワークトラフィックパターンを使用してLLMモデルを検出およびスキャンします



Qualysはエージェントをインストールできない環境でも柔軟な方法でアセットの脆弱性や評価を行います

Qualys.

CyberSecurity Asset Management の特長

内部および外部の攻撃対象領域の可視性

防御側と攻撃側の両方の視点から環境を可視化防御します。これには外部攻撃対象領域管理（EASM）も含まれます。この可視性をCMDBに反映することで、IT部門に最新の実用的なインベントリを提供します。

リスクベースの脆弱性管理プログラムの改善

100% の資産可視性と完全なビジネス コンテキストを使用して VM プログラムを拡張および強化し、リスクを測定して優先順位を付けます。

技術的負債の削減

サポート終了（EoS）およびサポート終了（EoL）のハードウェア、アプリケーション、およびオペレーティングシステムを特定し、削減します。 技術的負債の重要なカテゴリを調査・特定します。 優先順位を付けて迅速に修正することで、技術的負債によるリスクを軽減します。

CSAMは、Active Directory、Webhook、ServiceNow、BMC Helixなどとのネイティブ統合を活用し、不足している資産を追加します。データは正規化されるため、資産にタグを付け、クエリを実行し、追跡することで、リスクに基づく優先順位付けが可能になります。

bmc helix
servicenow

脆弱性を超えたリスク要因

自信を持って優先順位を付ける

01 **技術的負債 (EoL/EoS)**
サポートが終了したテクノロジーには、パッチ適用できない脆弱性が含まれています。 log4shell や WannaCry などの注目度の高い攻撃によるダメージ倍率

02 **危険なポートまたは未承認のポート**
インターネットに接続するポートが正しく構成されていないと、バックドアが環境に公開される可能性があります

03 **セキュリティアップデートが不十分なソフトウェア**
不足している EDR エージェントまたはその他の必要な IT/セキュリティ ソフトウェアを特定し、リスクを事前に軽減します

04 **未承認のソフトウェア**
このソフトウェアは環境内にあるべきではありません。さらに、不正ソフトウェアの 40% は EoL/EoS です。

高リスク

Qualys TRUによるEOL/EOSコンテンツ強化

- ✓ カタログは毎日更新されます
- ✓ SW: 5500 のパブリッシャーと 30万のS/Wバージョン
- ✓ HW: 1400 の製造元および 21万のモデル
- ✓ CPE、CVE、脅威インテルにマッピング
- ✓ 検出スコアを割り当てて重大度を強調します

*Qualys Threat Research Unit (TRU) は、あらゆる規模および業界の企業にわたる 5,200 万件の資産と 450 億件を超えるインストールされたソフトウェアを分析

Qualys.

参考BLOGはこちらを御覧ください。

CSAM 3.0 には、TruRisk のすべてのリスク要因が含まれています。

外部攻撃対象領域管理(EASM)の特徴

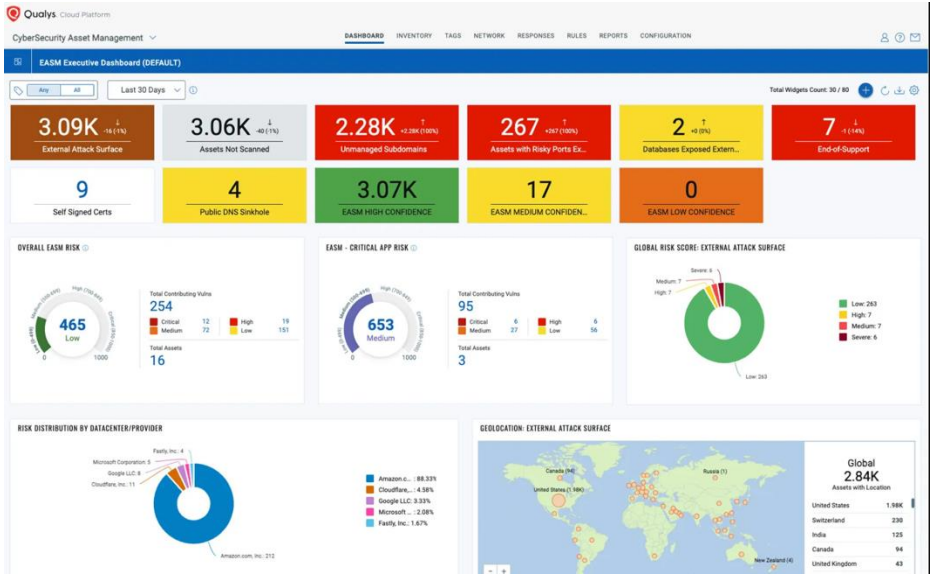
カテゴリ	機能名	説明
アセット検出	インターネット資産の自動検出	WHOIS、DNS、SSL証明書、公開リポジトリ、クラウドメタデータなどから外部資産を継続的に自動発見
アセットインベントリ	外部アセットの統合ビュー	検出されたドメイン、サブドメイン、IPアドレス、クラウド資産などを一元管理
リスク評価	脆弱性・誤設定の可視化	外部公開されたサービスやアプリケーションの脆弱性・設定ミス（例: 未承認のソフトウェア、有効期限切れSSL/TLS証明書など）を検出
ブランド保護	なりすまし・フィッシング監視	自社ブランドやドメインを悪用した偽サイトや類似ドメインの発見
脅威インテリジェンス連携	攻撃者視点の優先順位付け	既知の脆弱性、攻撃キャンペーン、マルウェアとの関連性などの脅威インテリジェンスと連携して、重要度の高いアセットと脅威を特定
リスクスコアリング	TruRiskによるリスク評価	各外部資産のビジネスリスクを数値化し、優先順位付け可能
統合と自動化	Qualys VMDR/CSAMとの連携	内部資産と外部資産を統合したサーフェス管理、チケットシステムやSOAR連携も可能
アラートとレポート	継続監視と通知	アセットの新規発見や変更、重大なリスクに対するリアルタイム通知とレポート機能

EASM Lightweight Scan搭載　新機能!

スキャンの目的: インターネットに公開された外部資産（ドメイン、サブドメイン、IPアドレスなど）を自動的に検出し、脆弱性を特定します。VMのライセンスは消費されません。

スキャンの特徴:

- EASM Discoveryの完了後、24時間以内に自動的にスキャンが開始されます。
- スキャン対象には、SSL証明書の問題や既知のCISA（米国サイバーセキュリティ・インフラストラクチャ庁）によって報告された脆弱性が含まれます。
- スキャンは毎日実行され、継続的なリスク評価が可能です。
- IPv6アドレス、プライベートIPアドレス、予約済みIP範囲、CDN資産など、一部のIPアドレスはデフォルトでスキャン対象外となります。



EASMによる「なりすまし・フィッシング」監視

機能カテゴリ	対応内容
ドメイン監視	**・類似ドメイン（タイポスクワッティング、同音異綴など）**を自動検出。フィッシングサイトや偽ブランドサイトの発見に有効。例: qual1ys.com や qualys-security[.]net **・誹謗中傷に関わるドメイン**により組織の評判を傷つける目的のコンテンツや商標権侵害のリスクのあるサイトの発見。
証明書監視	公開SSL/TLS証明書を解析し、**自社ブランド名を含む証明書の不正使用**を検出可能。
Web資産検出	未知のWebサイトやホスティングされた偽ページを自動で検出。攻撃者によるブランド**なりすましの兆候を早期発見**。
外部リポジトリ監視	GitHubやS3などの公開リソースにおける**ブランド・社名の誤用や漏洩**の兆候を検知可能。
アラートと可視化	ダッシュボードやアラートにより、なりすましの**リスクをリアルタイムに可視化・通知**。

活用例

偽ブランドサイトの早期発見 → **フィッシング被害の予防**
類似ドメインの検出 → **ドメインの買収・差し止め対応**
ブランド保護部門や法務部門と連携し、**ブランド毀損対策の迅速化**

ESAMレポート

すぐに使えるESAMレポートで検出データを自動集計しレポート化できます。資料はこちらからダウンロード下さい。

注意）Qualys EASM は「**検出と可視化まで**」が主な対応範囲です。テイクダウン対応（削除要請）やフィッシングメールの封じ込めは行いません。
注意）外部レポジトリ監視は、公開されている場合のみ検出します。

New Feature

EASM 新機能と改善点

CSAM2.18.0.0

CSAM強化により「外部攻撃面管理」「資産可視化」「リスク評価」がさらに高度に！

1. EASMプロファイルの複数作成が可能に

これまで1つのEASM（External Attack Surface Management）プロファイルしか作成できませんでしたが、バージョン2.18.0.0からは複数のプロファイルを作成できるようになりました。これにより、グローバルな組織やM&Aの評価など、異なる外部攻撃面を個別に管理することが可能になります。

2. EASMプロファイルのインポートとエクスポート機能

EASMプロファイルの設定をJSONファイルとしてインポートおよびエクスポートできるようになりました。これにより、設定のバックアップや他の環境への移行が容易になります。

3. EASMプロファイルの変更履歴の表示

EASMプロファイルの変更履歴を表示できるようになりました。これにより、過去の設定へのロールバックや変更内容の追跡が可能になります。

4. EASMの軽量スキャンのIPアドレス管理

VMDRスキャンが実行されていないVMアクティブなパブリックIPアドレスに対して、EASMの軽量スキャンを実行するための設定が追加されました。

5. ビジネスエンティティと関連資産の可視化

CSAMのUIに「ビジネスエンティティ」タブが追加され、ビジネスエンティティとそれに関連する資産の情報を表示できるようになりました。これにより、組織内の資産管理がより効率的になります。

6. タグのスコープ外の可視性向上

サブユーザーが自分のスコープ外のタグを閲覧できるようになりました。これにより、タグの重複作成を防ぎ、タグ管理が効率化されます。

7. 新しいQQLトークンの追加

以下の新しいQualys Query Language（QQL）トークンが追加され、資産の検索やフィルタリングが強化されました：

•asset.isolated：ネットワークから隔離された資産の検索
•domain.ip：指定したIPアドレスに関連するドメインの検索

EASM軽量スキャンの利点

項目	内容
高精度な脆弱性検出	最新スキャナーにより、**外部資産の重大リスクを正確に把握**
偽陽性の削減	他社EASMツール比で**60%の偽陽性を削減**（バナースキャン依存回避）
検出精度の向上	従来手法と比べ、**・重大な脆弱性検出数：3倍** **・無関係な脆弱性：60%減**
SSL証明書の継続監視	SSL Labsを活用し、**毎日スキャンして弱い暗号化レベルの証明書を可視化・警告**

Qualys.

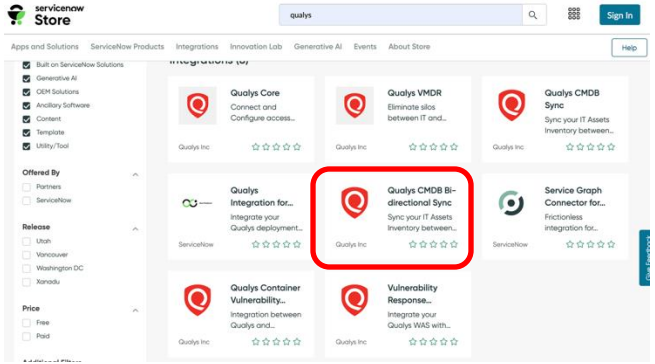
※リリースノートはこちらをご覧ください。

Qualys×ServiceNow連携で資産管理をスマートに自動化！

このアプリは、Qualys CSAMによって継続的に監視されているグローバルITリソースに関する包括的な情報を自動的にSNOWと同期します。

主な機能

機能名	説明
資産自動同期	Qualys CSAM（CyberSecurity Asset Management）で収集したIT資産情報を、ServiceNow CMDBなどに自動で同期します。
インテリジェントなマッピング	IPアドレス、ホスト名、MACアドレスなどの属性で、Qualys資産とCMDBレコードを正確にマッチング。
リッチなメタデータ提供	ハードウェア情報、OS、ソフトウェアインベントリ、脆弱性ステータスなど、Qualys側で検出した詳細データをCMDBに反映。
双方向同期（一部機能）	CMDBからの属性情報をQualys側へ連携可能な設計（構成により）
カスタム同期ポリシー	スケジューリング、フィルタリング、タグベースの同期制御などが可能。
ServiceNow認定アプリ	ServiceNow Storeで提供され、ITOM、ITSM、SecOpsの拡張に対応。



「CMDBが最新ではない」「セキュリティとIT資産管理が分離している」「資産オーナーが不明」 といった課題を抱えるお客様に対して、Qualys CMDB Sync は **自動化・正確性・一元化** による明確な価値を提供します。

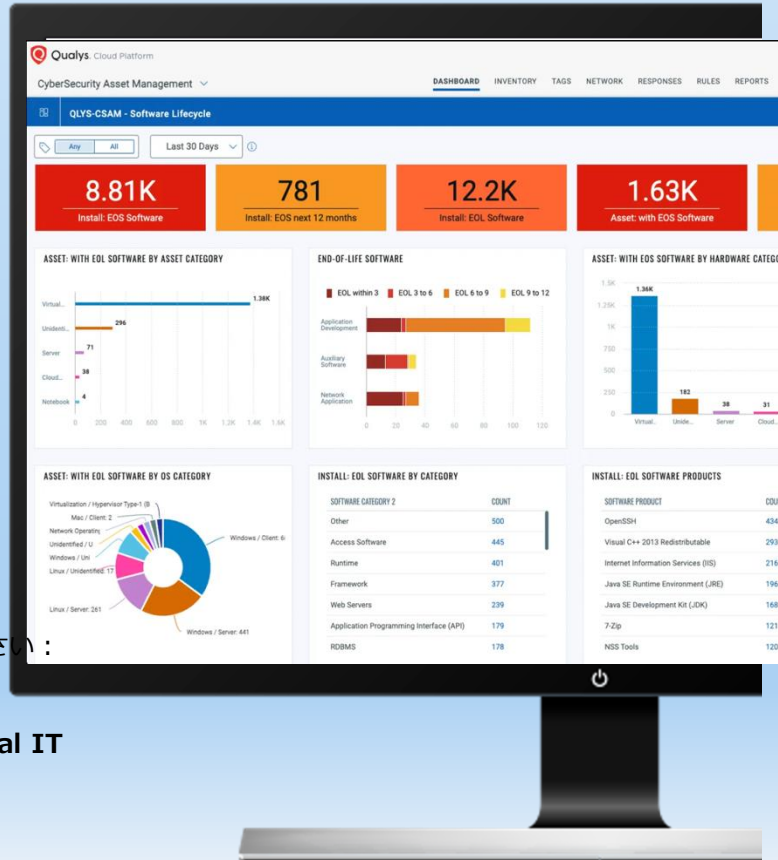
導入に適した業種・組織の例

- **大企業・グローバル企業**：多数の拠点・IT資産を保有し、CMDBの維持が困難。
- **金融・保険業界**：コンプライアンスが厳格で、資産の可視性と正確性が求められる。
- **製造業・インフラ系**：ITとOTの融合で新たな資産が増加、統合管理が必要。
- **公共機関・教育機関**：資産が多様・分散しており、集中管理に課題がある。

技術負債を一目で把握！

Qualysでリクスの見える化と評価を同時にレポート

Qualys Tech Debt Report は、組織内の技術的負債（Tech Debt）を可視化し、特に**サポート終了（EoL）やサポート終了予定（EoS）**の**ハードウェア**や**ソフトウェア**に関連するサイバーリスクを評価するレポートです。



主な目的と特徴

セキュリティリスクの可視化と経営層への報告：CIOやCISOが、技術的負債の現状を共有し、予算やリソース配分の根拠とする。
IT資産のライフサイクル管理：今後12か月以内にEoL/EoSを迎える資産を予測し、計画的な更新を支援 。
脆弱性管理の強化：パッチが提供されないソフトウェアに依存している資産を特定し、攻撃対象領域を縮小。
コンプライアンス対応：規制や監査において、技術的負債の管理状況を証明する資料として活用。
コスト最適化：延長サポート費用の削減や、不要な資産の整理に貢献。

※詳細な情報やサンプルレポートについては、以下のQualys公式ドキュメントをご参照ください：
•Technology Debt Report - Qualys Documentation
•Tech Debt Report - サンプル
※このレポートは、**Qualys CyberSecurity Asset Management（CSAM）** または **Global IT AssetView（GAV）** のユーザーが生成可能で、PDF形式で提供されます。

クォリスによるリスク管理とリスク修復

Enterprise TruRisk Management (ETM)

Trurisk Eliminate(TRE) – Patch Management, Remediation, Isolation

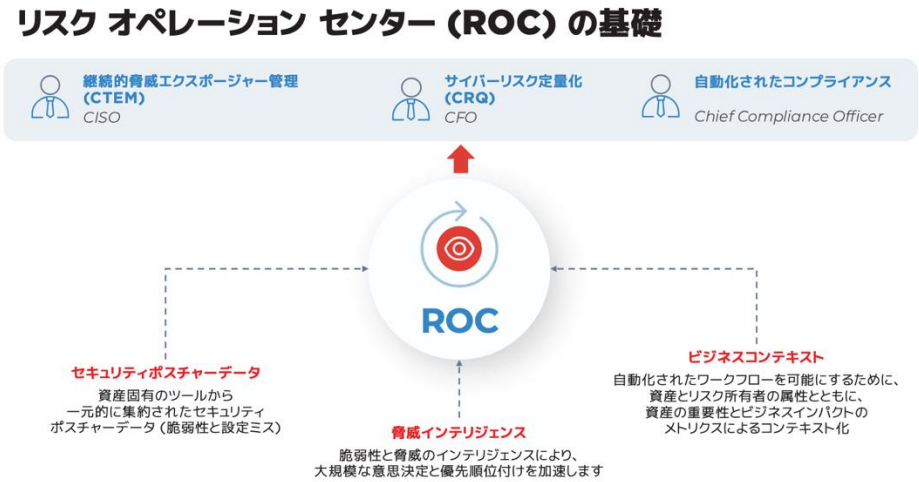
*TRU EliminateはVMDRライセンスとの併用が必須です。
また、Patch ManagementはTREに含まれていますが、単体機能としてVMDRと併用してご利用いただけます。

世界初のクラウド型リスク運用センター（ROC）

Qualysが提供する Enterprise TruRisk™ Management（ETM） は、セキュリティや脆弱性に関するデータを集約し、企業におけるサイバーリスクの可視化と管理を支援する クラウドベースのリスク運用センター（ROC） です。

ETMの目的と導入背景

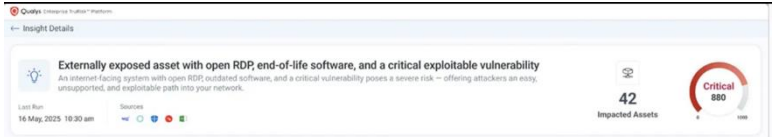
従来、複数ツールにまたがる断片的なセキュリティ対策では、冗長作業、見落とし、優先順位のズレなどが課題となっていました。ETMはこれらを一元化し、CISOや経営層が戦略的にサイバーリスクを管理できるよう設計されています。

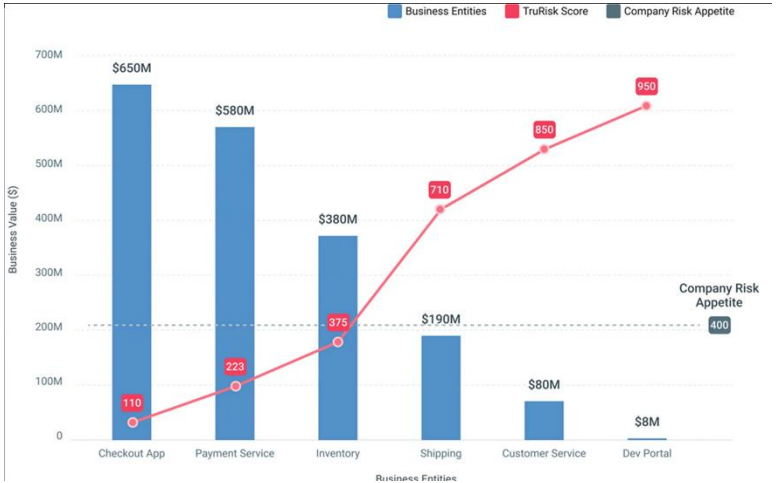


ホワイトペーパーはこちらです。
リリースノートはこちらです。

ETMの特徴

主な特徴	説明
データの統合と正規化	Qualys製品やサードパーティ製ツールからのセキュリティデータを集約し、重複排除や標準化を行って一元管理を実現
脅威インテリジェンスとビジネスエンティティの付与	MITRE ATT&CK、Talos、Qualys独自など25以上の脅威インテリジェンスを活用し、さらに業務重要度や金銭的影響などのビジネスエンティティを加えることで、リスクの優先順位付けを強化
TruRisk™ スコアによる定量評価	脆弱性の深刻度、悪用可能性、資産の重要性、ビジネスへの影響などを考慮したスコアリングで、対応すべきリスクを明確に可視化
リスク対処の自動化	パッチ適用、チケット発行、リアルタイムアラートなど、AIドリブンの自動ワークフローによりリスク対応を迅速化（「パッチレス修復」も含む）
監査対応と経営層向け報告	詳細な監査用ログや、経営層にも伝わる一貫性のあるリスク報告機能を備え、コンプライアンス対応を支援
多様なデータソースとの統合	QualysおよびサードパーティツールとのリアルタイムAPI連携により、クラウド、オンプレミス、ハイブリッド環境にまたがる多種多様なデータを集約





Qualys.

Qualys、業界初となるエージェント型AI搭載リスクオペレーションセンターを発表、自律型リスク管理を実現

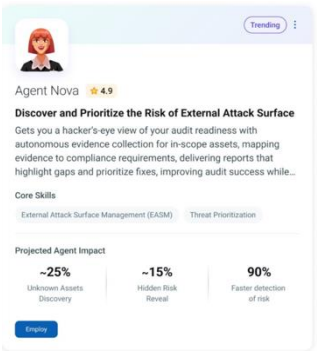
詳細：Blog
Demo Video

近日リリース予定

新しいアプローチでは、サイバーリスクオペレーションのあらゆるステップを自律的に実行するサイバーリスクAIエージェントのマーケットプレイスを導入し、リスク態勢を劇的に改善し、運用コストを削減します。

主な機能：

- ✓ リスクインサイトと優先順位付けの自動化
- ✓ 適応型修復によるセキュリティ強化
- ✓ カスタムAIエージェントの構築



主なユースケース：

1.Agent Nova: インターネットに接続された資産を自動的に検出し、攻撃者の視点からリスクを優先順位付けして報告します。

2.Agent Vikram: マルチクラウド環境（AWS、Azure、GCP）での未監視の仮想マシンを自動的にスキャンし、適切なスキャン手法を適用します。

3.Agent Chang: コンプライアンス監査の準備を自動化し、ISO、NIST、PCI-DSSなどのフレームワークに基づく証拠収集とレポート作成を行います。

4.Agent Nyra: 業界固有の脅威インテリジェンスを活用し、リスクを優先順位付けして対策を提案します。

5.Agent Sara: MicrosoftのPatch Tuesdayで公開された脆弱性を自動的に検出し、優先順位付けして修復計画を立案します。

6.Agent Sophia: 仮想マシンの脆弱性を自動的に管理し、修復作業を人手を介さずに実行します。

これらのエージェントは、Qualysの「Enterprise TruRisk Management（ETM）」に統合され、組織固有のリスク状況に基づいて自律的に行動します。また、「Cyber Risk Assistant」は、自然言語でのクエリに応じてリスク情報を提供し、意思決定をサポートします。

このように、Agentic AIは、サイバーリスク管理の効率化と自動化を実現し、セキュリティチームの負担を軽減します。

脆弱性のリスクに素早く対応

主な機能

1. **リスク優先度に基づく修復提案**
   TruRiskスコア（**脆弱性の重大度**、**資産の重要度**、**脅威のアクティビティ**など）をもとに、**修復優先度が高いアセットと脆弱性を自動抽出。**
2. **自動修復アクション（Auto-remediation）**
   Qualys Patch Managementと連携し、対象アセットに対して**自動でパッチ適用が可能。修復用のFixItチケット**やワークフローを**作成・実行**できる。
3. **影響評価とリスク削減効果の可視化**
   修復後に**リスクスコアがどれだけ下がったか**をダッシュボードで可視化。
4. **統合された作業キュー管理（Remediation Queue）**
   各チームが取り組むべき修復タスクを統一管理。
   JIRA / ServiceNowなどのITSMと**連携**し、チケット発行から対応追跡まで自動化。

TRE導入メリット	説明
セキュリティ運用の自動化	対応すべき脆弱性が自動的に抽出・修復され、手作業を削減
対応優先順位の明確化	リスクに直結する脆弱性から修復できるため、ROIが高い
監査・証跡対応	対応の実績・履歴が可視化され、金融監査や内部統制にも有効
SecOpsとITOpsの橋渡し	セキュリティチームと運用チーム間の作業分担を効率化

TruRiskの削減に対処する

パッシブおよびアクティブな対応を推進してリスクをより迅速に軽減します

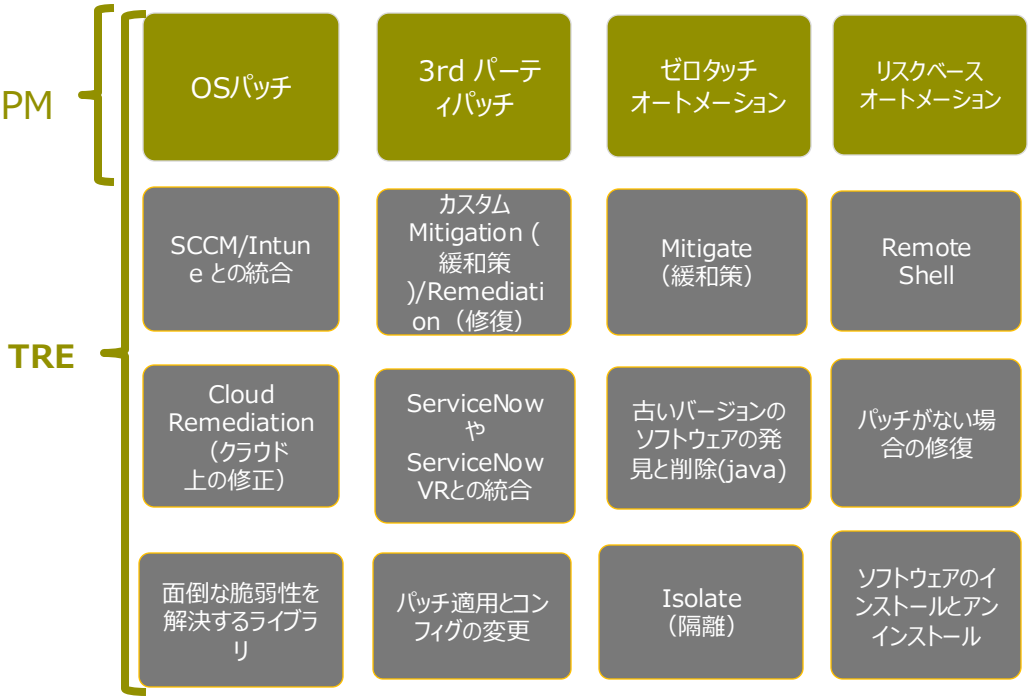
- Qualys TruRisk Eliminateサイト
- Qualys TruRisk Eliminate ブログ

Qualys.

Eliminate機能概要

TruRisk Eliminate(TRE)は 、従来のパッチ適用を超えて、統一された Qualysプラットフォームを通じて脆弱性を修正、軽減、アンインストール、および分離する機能を提供します。

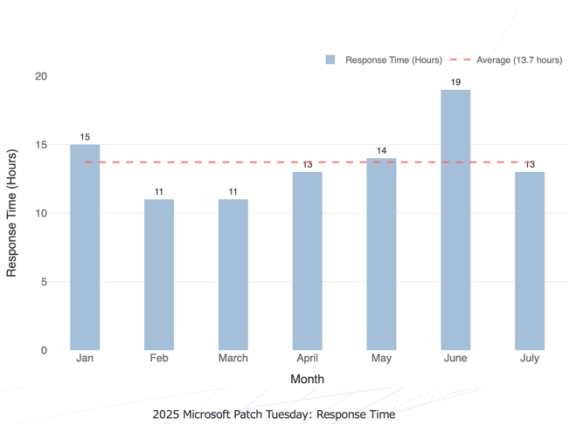
機能一覧
✓ パッチ 適用(Windows/Linux/Mac)
✓ パッチなしで脆弱性を修正
✓ カスタム修復スクリプトの作成
✓ SCCM/Intune との統合 (ロードマップ)
✓ 緩和策(MIT)の適用
✓ EOL/EOSおよび未使用のソフトウェアのアンインストール (ロードマップ)
✓ 重要なソフトウェアパッケージの配布
✓ アセットの動作をリモートで分析
✓ デバイス分離(ISL)機能
✓ オペレーショナルリスクスコア
✓ キュレーションされたスクリプトとソフトウェアインストールカタログへのアクセス
✓ リミディエーション(修復)コックピット



Qualys.

迅速なQIDリリース：CISA KEVとMS Patch Tuesday

Tuesdayパッチの
Vulnは平均14時
間でリリースされます。



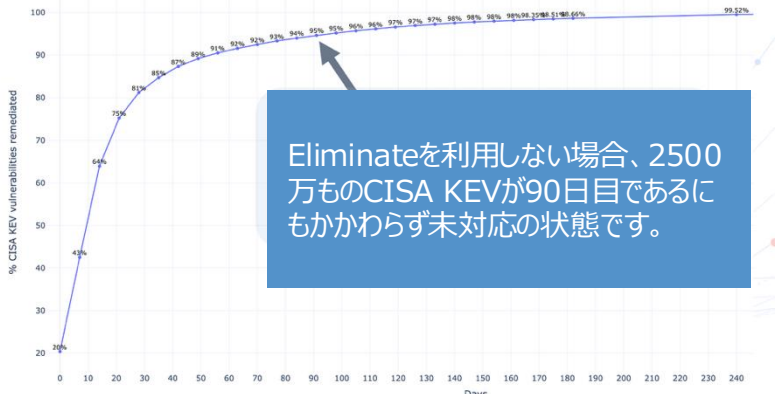
CISA の既知の悪用された脆弱性カタログのカバレッジ

- CISAの既知の悪用されたCVE(1,360/1,379)を~99%カバーして企業を保護します。
- Qualys は業界をリードする CISA KEV カバレッジを持っています

Qualys ユーザーの20%は、これらの CVE が CISA KEV カタログに追加される前に修正しています。

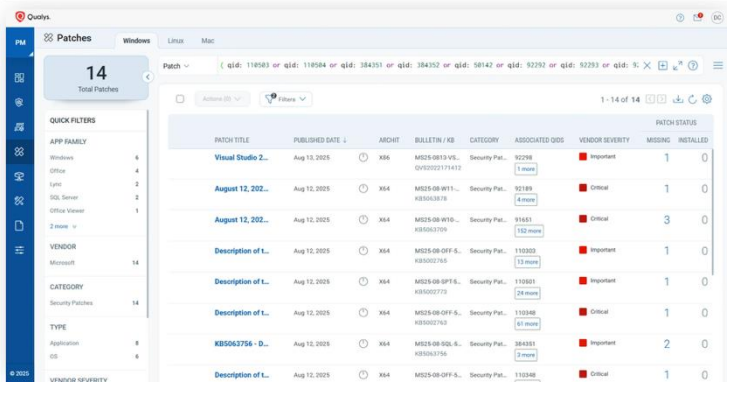
残りの1%(19のCVE)は、ほとんどがレガシー/オフマーケットテクノロジーであり、企業へのエクスポージャーは限られています。

CISA KEV: TruRisk Eliminate: パッチ不可能な CISA KEV を分離、軽減、修復します



Eliminateを利用しない場合、2500万ものCISA KEVが90日目であるにもかかわらず未対応の状態です。

パッチ管理：Patch Tuesday August 2025 blog



クォリスによるAppSecセキュリティ

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

*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。

Webアプリケーション &APIスキャニング

2009 年以来、世界中で 2500 以上の顧客の Web アプリを保護

包括的なディスカバリー
インターネットに公開されている内部、外部、およびこれまで知られていなかった Web 資産や忘れ去られた Web アプリケーションを発見します。

PII 収集と露出検出
PII データの盗難や罰金による経済的損失を防ぎます。

第三者脆弱性の統合
サードパーティの手動侵入テストから脆弱性をWAS検出とともにインポートして、Webアプリケーションのセキュリティを包括的に表示します。

API スキャン
REST API および SOAP API の実行時の脆弱性は、攻撃者が悪用する前に特定できます。

マルウェアの検出
マルウェアによるデータ盗難による経済的損失を防ぎながら、企業の名前と評判を保護します。

CICD インテグレーション
カスタマイズされたビルドの合否基準により、開発チームはソフトウェアの脆弱性を持たずにアプリケーションを確実に展開できます。

チケット発行の統合
チケット発行の自動化を活用すると、スキャンが完了するとすぐに修復を開始できるため、MTTR が短縮されます。

Qualys.

Qualys TotalAppSec概要

Qualys TotalAppSecは、2025年4月にリリースされたアプリケーションリスク管理ソリューションの最新版で、Webアプリケーションと APIのセキュリティを統合的に管理し、AIを活用したマルウェア検出機能を備えています。

主な新機能（TotalAppSec 2.0）

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

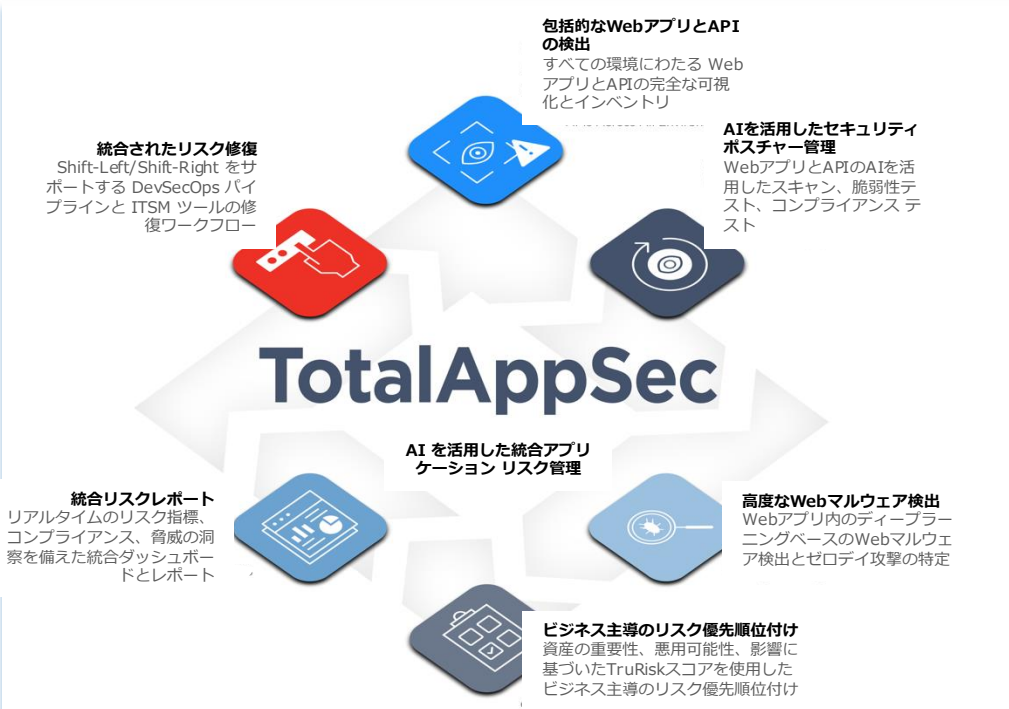
開発と運用の連携を強化し、セキュリティを開発プロセスに組み込みたい企業

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

Qualys.

TotalAppSec 2.0

New Release



Qualys TotalAppSec

2025年4月にリリースされたアプリケーションリスク管理ソリューションの最新版で、WebアプリケーションとAPIのセキュリティを統合的に管理し、AIを活用したマルウェア検出機能を備えています。統合されたアプリケーションリスク管理を提供し、マルチクラウド、オンプレミス、APIゲートウェイ、コンテナ化された環境にわたるミッションクリティカルな **WebアプリケーションとAPIのサイバーリスクを監視および軽減**します。

特徴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。

特徴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。

特徴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。

※リリースノートはこちらをご覧ください。
※WASの新規販売は終了し、TotalAppSecでの販売となります。
※WASでの更新はできずTotalAppSecでの更新となります。

クォリスによるクラウドセキュリティ

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。また、
Qualys Unit という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・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>

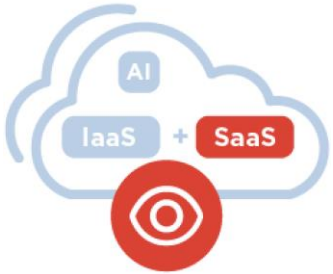
Qualys TotalCloud の優位性

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	**VMDR、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）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	EASMやDR、Webスキャン、脆弱性スキャンをひとつに集約可能

Qualys TotalCloudによるクラウドリスクの測定、伝達、排除



クラウドインフラストラクチャーとSaaS環境向けのAI搭載CNAPPソリューション

TotalCloud
with TruRisk Insights

Cloud Security Posture Management (CSPM)
パブリッククラウドリソースのインベントリ。Infrastructure as Code(IaC)セキュリティを含む、設定ミスや非標準展開の検出と修復

Cloud Workload Protection (CWP)
OSSを含むクラウド環境(VMDR with FlexScan)の脆弱性のスキャン。

Cloud Detection and Response (CDR)
マルチクラウド環境を、活発なエクスプロイト、マルウェア、未知の脅威から継続的にリアルタイムに保護します。

Kubernetes & Container Security (KCS)
コンテナを検出、追跡し、ビルドから実行まで継続的に保護します。

Cloud Infrastructure Entitlement Management (CIEM)
クラウド環境におけるIDと権限の検出、追跡、継続的な管理

SaaS Security Posture Management (SSPM)
SaaSアプリケーションスタック全体のセキュリティ体制とリスクを管理

Qualys.

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)

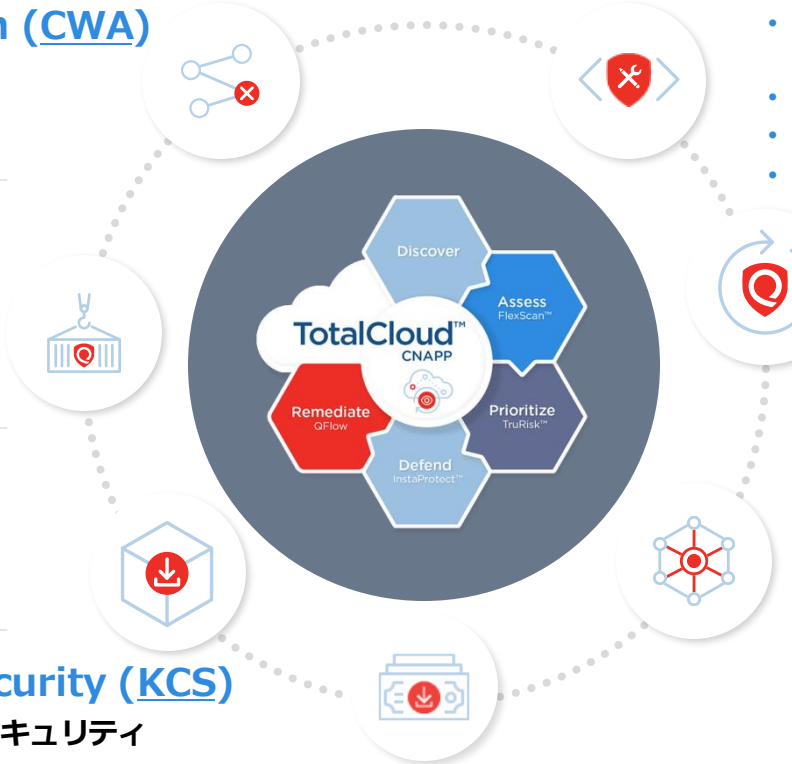
- SaaSアプリの保護
- コンプライアンス

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

Qualys. aws Azure Google Cloud ORACLE Cloud

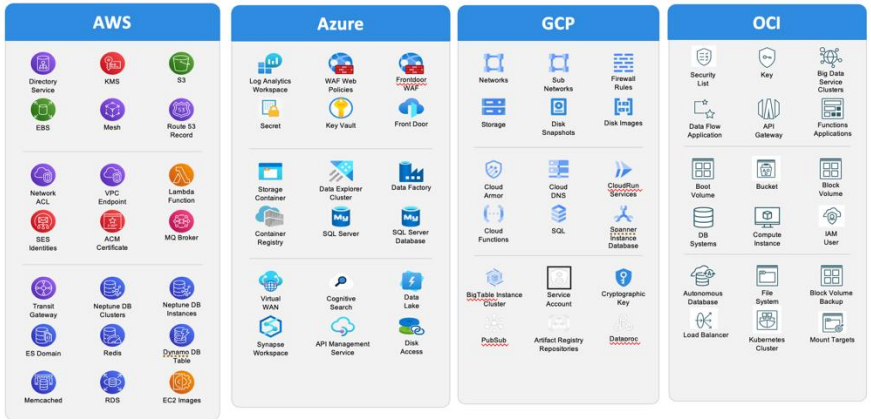
オンプレミスとマルチクラウド

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

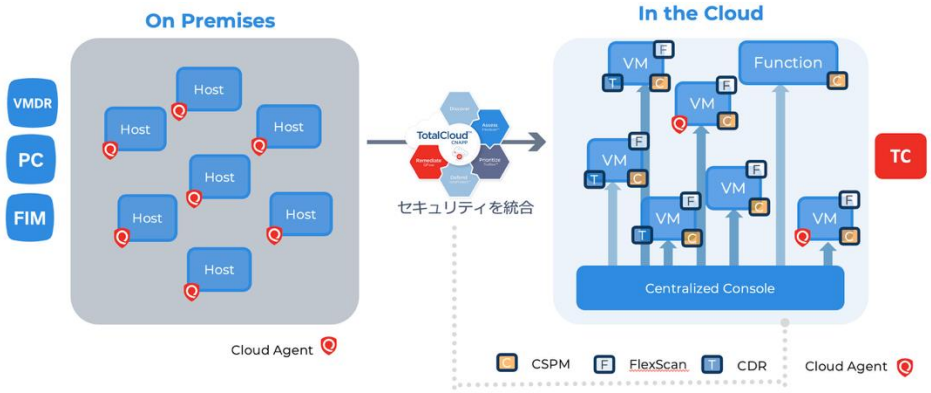
包括的なインベントリ
100%インベントリと
リソースタイプカバレッジ

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



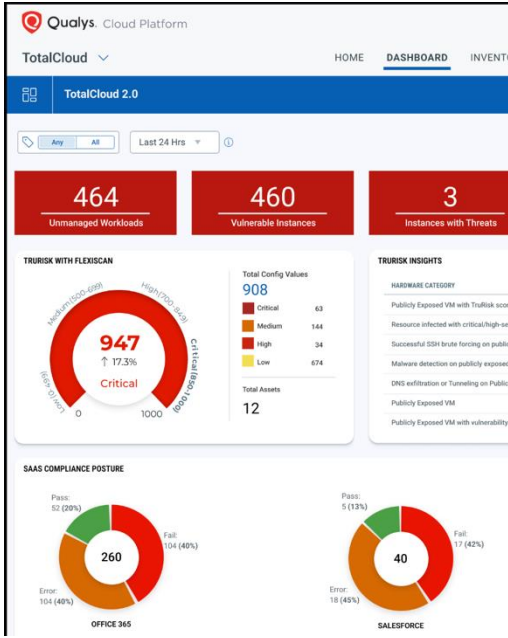
一歩先を行く
統合リスク可視化・自動修復ソリューション

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

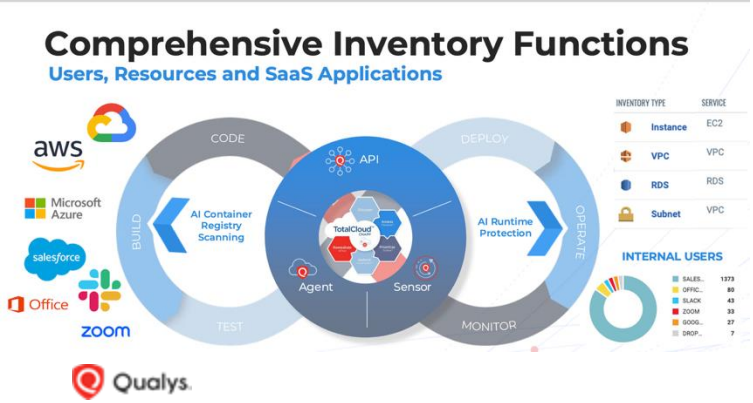


スキャン方式	特徴	利用シーン
APIベース	クラウドサービスプロバイダーのAPIを利用して、継続的なインベントリ収集と構成評価を実施。エージェントレスで迅速なセットアップが可能。	AWS、Azure、GCPなどのクラウド環境での継続的な監視。エージェントの導入が難しい環境。
スナップショットベース	ワークロードのスナップショットを取得し、オフラインで脆弱性評価を実施。一時停止中のインスタンスも評価可能。	M&Aやクラウド移行時の一括評価。定期的なセキュリティチェックを実施したい環境。
エージェントベース	クラウドエージェントを導入し、リアルタイムでの脆弱性、構成、セキュリティ評価を実施。ラン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。



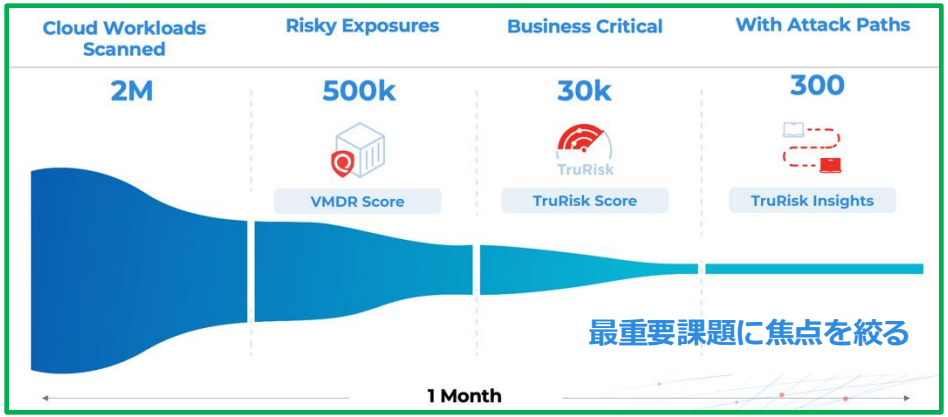
主な機能	概要
SaaS設定の継続的監査	Microsoft 365, Google Workspace, Salesforce,などの設定項目を継続的にチェックし、リスクを検出
セキュリティ設定のベンチマーク評価	CIS Benchmarks や業界ベストプラクティスに基づいたコンプライアンス評価
過剰アクセスや特権アカウントの検出	不要または過剰な権限を持つユーザーや公開設定を特定
リスクベースの優先順位付け（TruRisk）	リスクの重大度をスコア化し、修正の優先順位を明確化
自動修復・ガイド付き修復	修正案の提示またはAPI連携による自動修復機能で対応を迅速化
統合レポートと可視化	ダ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

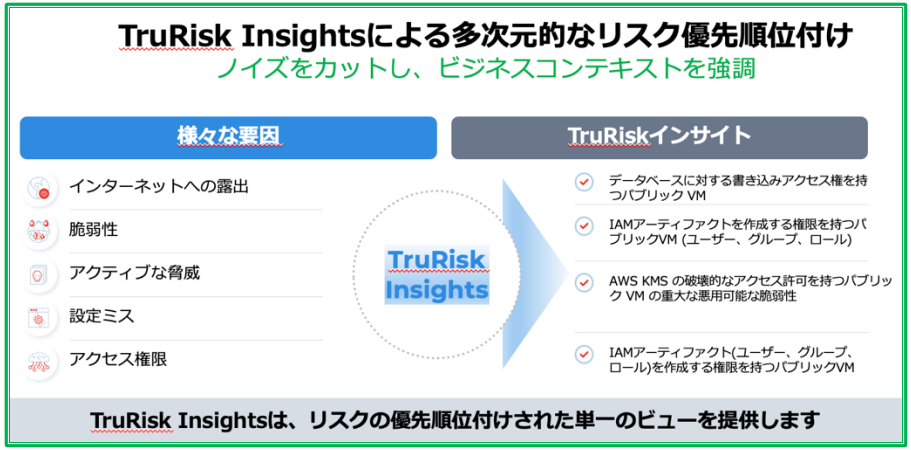
サポートされているコネクター

- 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。

優先順位付け：TruRisk Insights





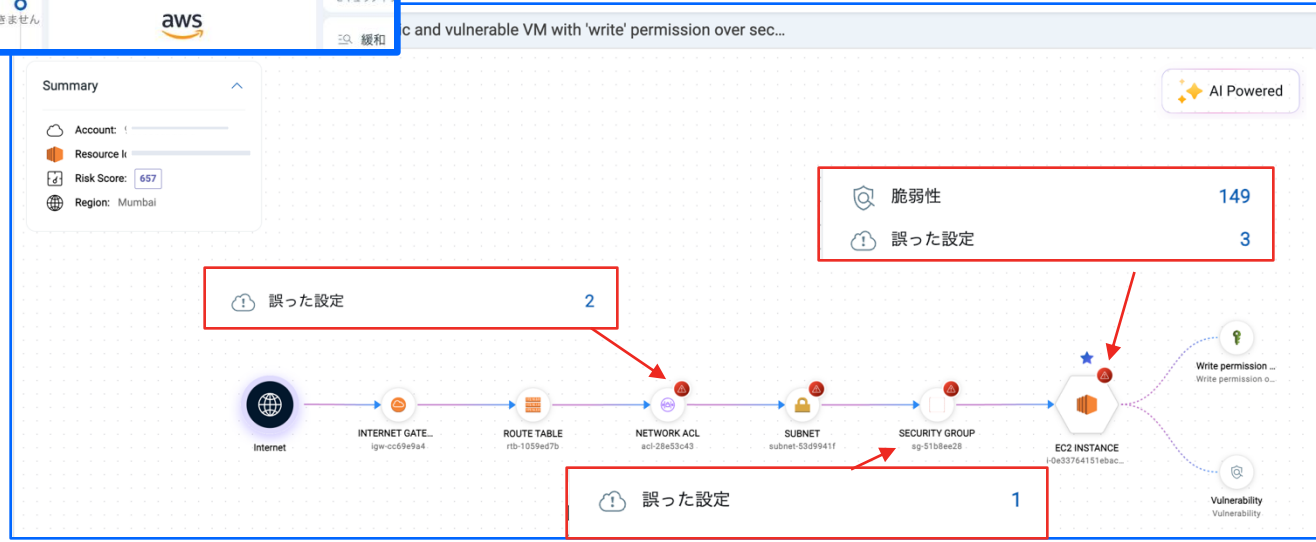
TotalCloud Attack Path

New Release

TotalCloud Attack Path 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.

クォリスによるコンプライアンス

Policy Audit

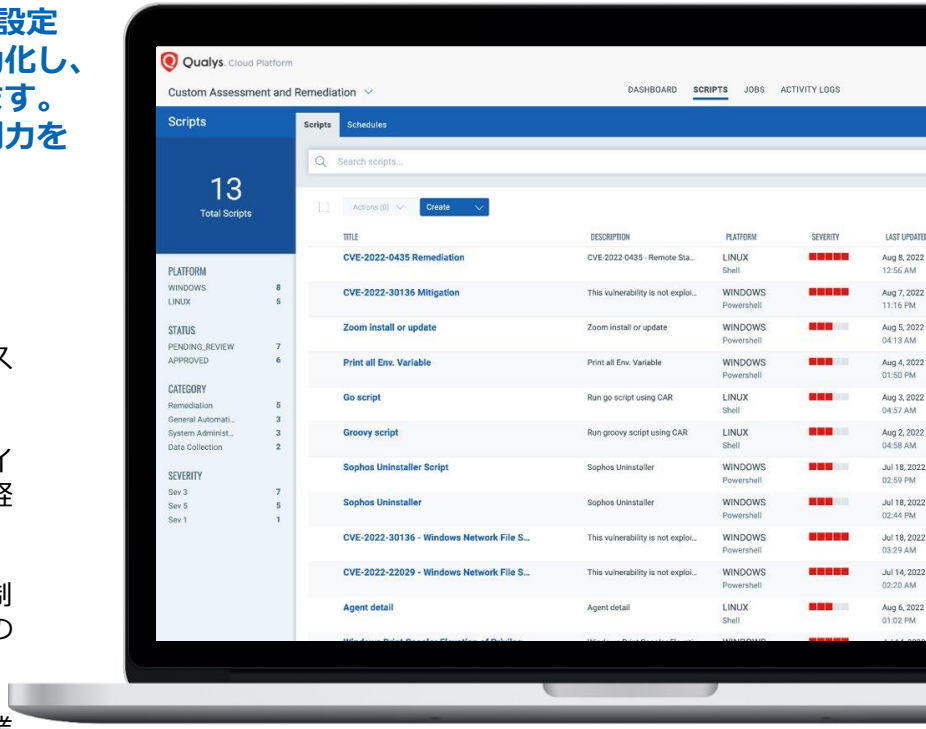
*Policy AuditはVMDRライセンスとの併用が必須です。
また、Audit Fixは別途ライセンスが必要です。

コンプライアンスと構成管理

Qualys Policy Audit（前名称：Policy Compliance）は、「設定の見える化」「違反の早期検出」「標準との整合性確認」を自動化し、企業のセキュリティ・コンプライアンス運用を大幅に効率化します。特にグローバルやマルチクラウド環境において高い柔軟性と統制力を発揮します。

主なメリット

•リスク低減と迅速な対応
自動化されたチェックにより、潜在的なセキュリティ上の脆弱性や設定ミスを早期に発見できるため、重大なセキュリティ事故のリスクを削減します。
•コンプライアンスコストの削減
定期的な手動監査やチェックの工数を大幅に削減でき、効率的なコンプライアンス管理が実現します。これにより、監査対応やレポート作成の負荷が軽減されます。
•内部統制の強化
組織内のセキュリティポリシーやガバナンスの整備を促進し、内部統制体制の強化に寄与します。また、経営層への報告や監査にも利用可能な信頼性の高い情報を提供します。
•柔軟な適応性
カスタマイズ可能なポリシー設定や各種業界標準への対応により、様々な業界や規模の組織に合わせた柔軟なコンプライアンス管理が可能です。



Qualys.

Qualys Policy Audit によるセキュリティ評価

ポリシーの推奨/設定値と実際にシステムに設定されている値を比較し、設定に対するセキュリティ評価を実施します。

■幅広いテクノロジーに対応

- 100種類超のテクノロジーに対応
- AIX, HP-UX, Linux RHLE, Oracle, Solaris, Windows など

■ 多様な業界規制への対応

- COBIT 4.0, ISO 17799, **NIST** SP800-53, SOX 404, GLBA, HIPAA, Basel II, **PCI-DSS**, FISC, **GDPR**など

■ ポリシー定義

- CIS Benchmark, Microsoft SCM Baseline, SANS/CIS Top 20 Critical Controls などのポリシーライブラリ利用可
- 対話型エディタやゴールデンイメージからカスタムポリシー作成可
- XMLインポート・エクスポート

■コントロール

- 15,000超のコントロールライブラリ
- プログラミング不要の**カスタムコントロール作成**

■評価

- クレデンシャルを用いた認証スキャンによる内部評価
- オンデマンド、スケジュールスキャン

■レポート

- 再スキャン不要で様々なレポートを作成可能
- ポリシーレポート、個別ホストレポート、コントロール Pass/Failレポートなど豊富なテンプレート

1,200＋のポリシー、20,000のコントロール、70＋の規制、450＋のテクノロジーをサポート

Qualys.

New Release

Qualys Policy Audit

Qualys Policy Audit は、450 以上のテクノロジー、1,000 以上のすぐに使用できるポリシー、90 以上のフレームワークを包括的にカバーし、継続的なコンプライアンスと監査の準備を確保し、監査失敗のリスクを最大95%削減します。

Policy Compliance から Policy Auditへ追加費用なしでシームレスなアップグレード

継続的な監査準備
自動化されたコンプライアンス監視により、組織は常に監査に対応できる状態を維持します

プロアクティブなギャップ分析
コンプライアンス上のギャップを早期に特定し、対処することで、土壇場での問題を回避します

リスクに基づく優先順位付け
継続的なリスク分析を必要とする規制要件を遵守することで、監査への準備を確実に整えます

監査業務を効率化
ServiceNowとの連携により監査上の問題を解決し、シームレスなオンボーディングとエンドツーエンドの運用化により、価値実現までの時間を短縮します

自動化された監査対応レポート
常に監査準備の整ったレポートで手作業を削減

分類	ユースケース例
ガバナンス/監査	内部監査や外部監査（PCI DSS/ISO 27001/NIST/CISなど）への対応
セキュリティ運用	セキュリティ設定の継続的な確認（例: 無効なアカウントや不要なサービス）
インフラ運用	新規サーバ構築時のベースライン準拠チェック
クラウドセキュリティ	クラウドVMの構成がCISベンチマークに準拠しているかの評価
セキュリティ強化	設定不備による攻撃経路の早期発見と是正

※詳しくはBlogをご覧ください

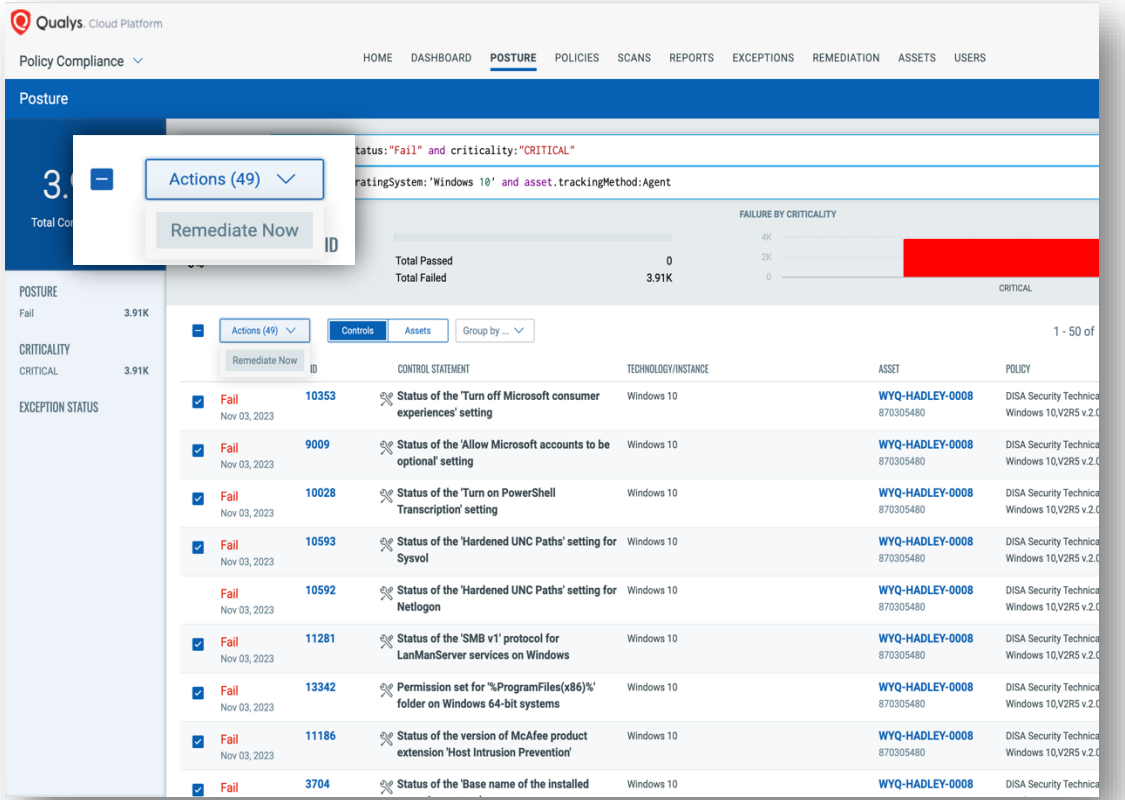
NIST 800-53 ISO FedRAMP GDPR PCI HIPAA

New Release

Audit Fix - 自動修復ワークフロー

監査ギャップを効果的かつ迅速に埋め、侵害リスクを大幅に削減

- 自動修復機能により、監査上の問題になる前に監査の発見事項を修正します
- すぐに使えるスクリプトの事前定義ライブラリ
- CI/CD パイプラインによる自動修復のためのゴールデン ポリシー
- カスタマイズ可能な修復



Qualys.

New Feature

Audit Fix & CAR　ポリシー監査向け自動修復機能

※Audit Fix およびCARはどちらも有償モジュールとなります。

Qualysの「Audit Fix」と「Custom Assessment and Remediation（CAR）」機能は、コンプライアンスの自動化とリスクの軽減を目的として、2025年5月に重要なアップデートが行われました。

Audit Fix リリース10.34 主な特徴

•**自動修復スクリプトの活用**：事前定義されたスクリプトライブラリを使用して、検出されたコンプライアンス違反を自動的に修復します。
•**CI/CDパイプラインとの統合**：修復スクリプトをCI/CDパイプラインに組み込むことで、開発プロセス中にコンプライアンス違反を事前に修正します。
•**カスタマイズ可能なレポート**：90以上の規制要件に対応したレポートを生成し、継続的なコンプライアンス監視を可能にします。
これにより、手動での対応が必要だった監査プロセスを自動化し、効率的なコンプライアンス管理が実現します。

参照：Audit Fix リリースノート

CAR リリース2.5.1主なアップデート

•**タグベースのユーザースコープ設定**：管理者は、ユーザーに対して特定のタグが付与された資産のみへスクリプト実行権限を設定できます。これにより、スクリプトの実行範囲を制限し、セキュリティを強化します。

•**ライセンスベースの機能アクセス制御**：CARの機能はライセンスに基づいて制御され、例えばAudit Fix/AutoRライセンスを持つユーザーは特定の修復スクリプトを実行できます。
これらの機能強化により、CARはより柔軟でセキュアなカスタムスクリプトの実行をサポートします。

参照：CAR2.5.1リリースノート

導入を勧める企業の課題と解決のアプローチ

課題カテゴリ	具体的な課題内容	Policy Auditでの解決アプローチ
構成ミス・設定不備の放置	重大なポート開放、不要なサービス稼働などの設定ミスが属人的対応	CIS/NISTなどのベンチマークで継続的な設定監視・是正支援
内部統制・監査対応の負荷	設定確認・スクリーンショット取得が手作業で非効率	自動化された証跡付きレポートで監査に即対応可能
ガイドラインの整備不備	自社セキュリティポリシーが明文化されていない/徹底されていない	カスタムポリシー作成と違反検出で統制を強化
マルチOS・マルチクラウド環境の一元管理が困難	Windows、Linux、クラウドVMごとに設定がバラバラ	エージェント or 認証スキャンで統一的に可視化
部門ごとのセキュリティばらつき	各拠点や部門で設定準拠状況に差があり全体最適化が難しい	グループ単位の準拠率表示・改善指標で横断管理が可能

推奨導入企業の特徴

- 金融・保険・官公庁・製造業など、**規制遵守が厳しい業界**
- 数百～数万台規模の**マルチプラットフォームを保有する企業**
- SOC運用やIT統制に力を入れる**CISO主導のセキュリティ体制**がある企業

Qualys.

コンプライアンス ソリューションのポートフォリオ

単一プラットフォーム | 単一エージェント | 単一コンソール | 監査対応

規制

FedRAMP / GDPR / ISO / NIST 800-53 / HIPAA / PCI

...などなど

Qualysのコンプライアンスポートフォリオ

- **Policy Audit** — 設定ミスを検出して修正
- **File Integrity Monitoring** — インシデント管理と優先順位付けを自動化
- **PCI ASV Compliance** — PCI コンプライアンスの自動化と簡素化
- **Security Assessment Questionnaire** — ベンダーのリスクを評価/優先順位付け
- **SaaS Detection & Response** — MS365 の設定ミスを評価

Qualys 脅威調査およびインテリジェンス ユニット (TRU)
100 名を超える世界有数の専門家があらゆる脅威ベクトルに対する迅速な保護を実現

プラットフォームサービス
RBAC • ML/AI • スケーラビリティ • アラート/通知 • ワークフロー • スクリプト作成 • ダッシュボードとレポート

統合データプラットフォーム
データの正規化、インデックス作成、分類、強化

API および インテグレーション

コントロールセンター

- SecOps
- ITOps
- DevOps
- Risk
- Compliance
- C-suite

IT 環境 | ワークステーション | サーバー | 仮想マシン | クラウド | モバイル | コンテナ | IOT/OT/ICS

Qualys.

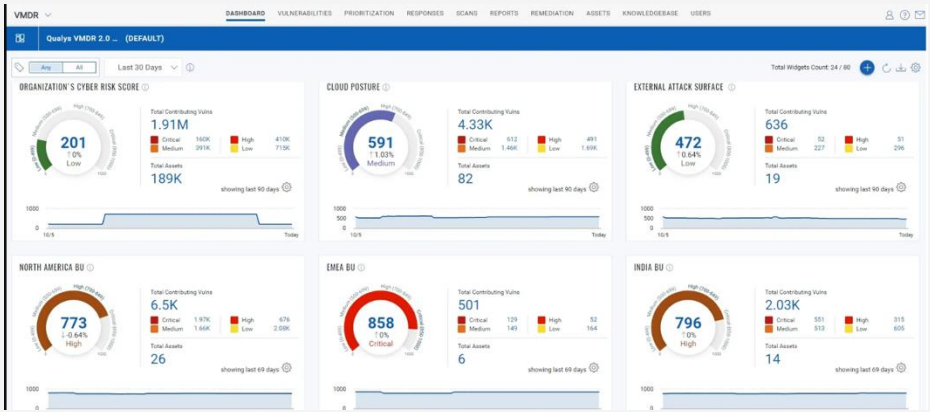
クォリスによるリスクベースの優先順位づけ

VMDR(脆弱性管理)とCSAM（資産管理）

*CSAMはVMDRライセンスとの併用が必須です。

TruRisk™ 2.0による優先順位付け

主な特徴	詳細
① ビジネスリスク連携の強化	資産の「ビジネスコンテキスト」（例：業務影響、場所、所有チーム、規制対応要件など）を取り込み、単なる脆弱性スコアではなく**“ビジネスリスク”**に基づく優先順位を算出。
② TruRiskスコアの高度化	CVSSスコアだけでなく、以下を複合的に加味してスコアを算出：• 攻撃可能性（Exploitability）• 外部脅威インテリジェンス（Threat Intel）• 資産重要度（Asset Criticality）• 修復状態（Remediation Status）
③ クロスプラットフォーム統合	クラウド、オンプレミス、コンテナ、モバイルなど、**すべての環境のリスク評価を一元化**。Qualys EASM や TotalCloud との統合により、攻撃面全体をカバー。
④ 脆弱性以外のリスク要素も可視化	OS設定不備、ソフトウェア構成エラー、ポリシー違反、外部露出（例：シャドーIT、公開S3バケット）など、**非脆弱性リスク**もスコアに反映。
⑤ サイバーリスクの金額換算（TruRisk Budget）	経営層向けに、サイバーリスクを「ドル／円ベースのリスク」として可視化。**ROI計算**や**リスク低減投資の効果測定**にも使用可能。
⑥ 組織全体での役割別可視化	CISO、SOC、IT運用など、**ロールベースのダッシュボード**が強化。チームごとに最適な意思決定支援を提供。
⑦ ServiceNowなどとの連携強化	TruRiskスコアに基づいたチケットの自動起票、優先度連動のワークフロー管理など、**セキュリティOpsとITOpsの統合**がより緊密に。



TruRiskスコア構成要素

TruRisk™ Score

Total Assets
110K
Total Findings
1.5M

Top Risk Factors

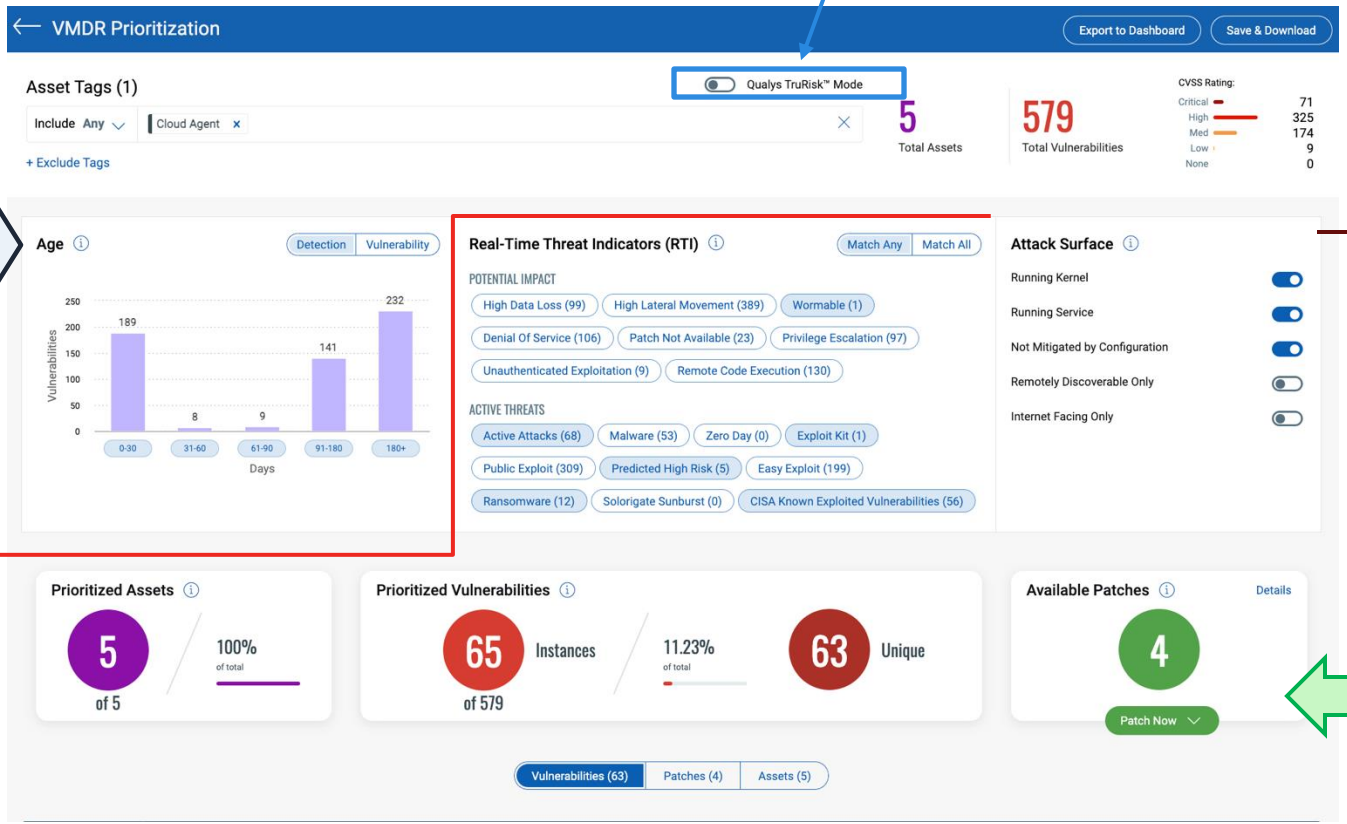
CISA/NCSCの脆弱性
143.2K
インターネットに公開されたアセット
20.4K
設定ミス
92.4K
インシデント
19

Qualys VMDR ：脆弱性スキャン + TruRisk優先順位
Qualys CSAM ：資産インベントリ × ビジネスリスク
Qualys Policy Audit：構成・設定のリスクをTruRiskスコアに反映
Qualys EASM：外部露出をトリガーとしたリスクスコア強化

脅威ベースの脆弱性対応と優先順位付け

Qulays TruRiskModeをオンにすると脅威インテリジェンスが有効になり、選択した資産のネットワーク上で最もリスクの高い脆弱性が優先順位付けされます。

Detection: 脆弱性が最初に検出された時期に基づくデータ。環境内で一番長くアクティブになっている脆弱性は１８０＋に表示されます。
Vulnerability: 脆弱性が公開されてからの日数。最近公開された脆弱性は0-30に表示されます。



RTIは滞在的な影響またはアクティブな脅威からインジケーター　を選択します。MatchAny（いずれかに一致）とMatch All(全てに一致)からフィルタを選択でき、優先順位付けされます。

Running Kernel: 同じLinuxホストで複数のカーネルが検出される場合があります。オンにすると、悪用される可能性のある実行中のカーネルに絞る事ができます。
Running Service:フィルターをオンにすると、悪用される可能性のある実行中のサービスに絞る事ができます。
Not Mitigated by Configuration:フィルターをオンに切り替えると、ホスト構成により悪用できない構成関連の脆弱性が除外されます。
Remotely Discoverable Only: このフィルターをオンに切り替えると、リモート (認証されていない) スキャンを使用するスキャナーによって検出できる脆弱性のみが含まれます。
Internet Facing Only： このフィルターをオンに切り替えると、悪用される可能性のある IP アドレスを持つ資産が含まれます。

適用可能なパッチの数が表示され、直ちに対策を取ることが出来ます。

Qualys.

MITRE ATT&CK マトリックスによる優先順位

攻撃者中心の視点を実現

攻撃者の視点から主要なATT&CK戦術と手法を把握し、脅威情報に基づく防御を導入してリスクを軽減します。

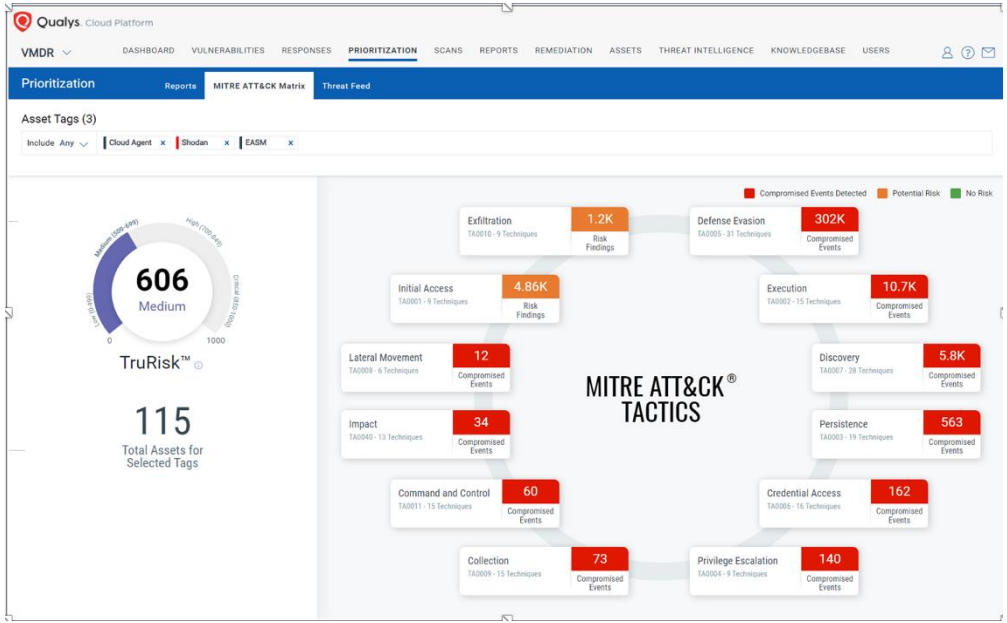
包括的なATT&CKビュー

VMDRからの脆弱性、PCからの設定ミス、EDRからのインシデント、CSAMからの資産詳細（外部向け資産の識別やRDPポートの詳細など）を統合したATT&CKビューを提供します。

攻撃経路の排除

MITRE ATT&CKのインサイトを活用し、攻撃経路を特定、優先順位付け、排除し、統合パッチ管理を使用してキルチェーンをプロアクティブに断ち切ります。

VMDRの「Prioritization」タブにあるMITRE ATT&CKマトリクスは、攻撃者の視点から脆弱性や設定ミス、EDR（Endpoint Detection and Response）イベントを戦術（Tactics）・技術（Techniques）・サブ技術（Sub-Techniques）にマッピングします。これにより、攻撃のライフサイクルにおけるリスクの位置づけを明確にし、優先的な対策が可能となります。



Real-Time Threat Indicatorsによる優先順位

組織の課題

検出される脆弱性の数が膨大で、どれから対応すべきか分からず、重要なリスクが埋もれてしまう。**実際に悪用されている脆弱性（Active AttacksやCISA Exploitedなど）に絞って対応優先度を決められる。**

RTIの活用方法

優先順位付け：RTIを使用して、組織内で検出された多数の脆弱性（QID）の中から、**最もリスクの高いものを特定**し、優先的に対策を行うことができます。

フィルタリング：複数のRTIを組み合わせてフィルタを作成し、**特定の条件に一致する脆弱性を抽出**することで、効率的な対策が可能になります。

代替防御策の提供：パッチが利用できないが、アクティブな攻撃が確認されている脆弱性に対しては、**回避策や代替の防御策を提供**することができます。

潜在的な影響（Potential Impact）

- **High Data Loss**：成功した悪用により、ホスト上で大量のデータ損失が発生する可能性があります。
- **High Lateral Movement**：攻撃者がネットワーク内の他のマシンを侵害する可能性が高いです。
- **Wormable**：ユーザーの介入なしに自己拡散するマルウェア（ワーム）によって悪用される可能性があります。
- **Denial of Service**：成功した悪用により、サービス拒否が発生します。
- **Patch Not Available**：ベンダーから公式の修正が提供されていません。
- **Privilege Escalation**：成功した悪用により、攻撃者が特権を昇格させることができます。
- **Unauthenticated Exploitation**：この脆弱性の悪用には認証が不要です。
- **Remote Code Execution**：成功した悪用により、攻撃者がターゲットシステムまたはプロセスで任意のコマンドやコードを実行できます。

アクティブな脅威（Active Threats）

- **Active Attacks**：実際の攻撃が観測されています。
- **Malware**：この脆弱性に関連するマルウェアが存在します。
- **Zero Day**：実際の攻撃が観測され、ベンダーからのパッチが存在しません。
- **Public Exploit**：既知の悪用コードが公開されています。
- **Predicted High Risk**：機械学習を活用して、悪用されていない脆弱性の優先順位付けを行います。
- **Easy Exploit**：攻撃の実行が容易で、特別なスキルや詳細な情報が不要です。
- **Exploit Kit**：この脆弱性に関連するエクスプロイトキットが存在します。
- **Wormable**：ワームによって悪用される可能性があります。
- **Solorigate Sunburst**：FireEyeのRed Teamツールによって使用されるすべてのCVEと関連付けられています。
- **Ransomware**：この脆弱性は、ランサムウェアが配置された攻撃ベクトルによって悪用されています。
- **CISA Exploited**：CISAが管理する、実際に悪用されていると一般に知られている脆弱性のカタログに関連付けられています。

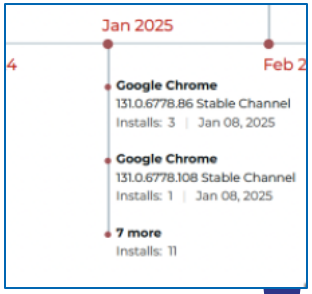
Qualys.

Qualys TruRisk レポート

リスクに基づく脆弱性管理と戦略的なセキュリティガイダンス

Qualys TruRisk™レポートは、**企業のセキュリティ体制を**明確かつ実用的な方法で**評価**し、**重要な脆弱性とリスクを浮き彫り**にするとともに、それらの**軽減に向けた戦略的なガイダンス**を提供します。脆弱性と資産は、インフラに及ぼす**リスクに基づいて優先順位付け**されます。サイバーリスクを正確に定量化することで、**エクスポージャーの低減、リスク軽減の傾向の追跡**、そして**サイバーセキュリティプログラムの有効性向上を実現**します。

※レポート出力条件：VMDRライセンスがありマネージャーユーザー権限を持つこと

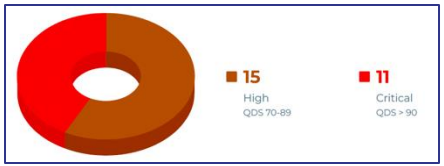


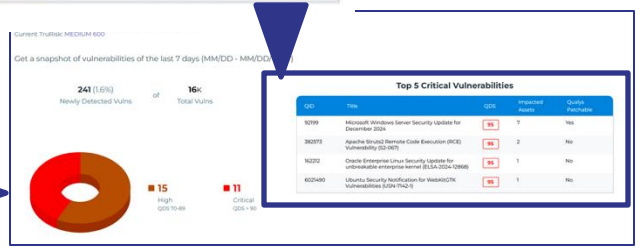
Risk Overview: EOS
2025年1月　Google Chromeのいくつかのバージョンとその他アプリケーションがEOSを迎えます。バージョンアップの計画を推奨します。

2025年6月4日 詳細はこちら

QID	Title	QDS	Impacted Assets	Qualys Patchable
92199	Microsoft Windows Server Security Update for December 2024	95	7	Yes
382573	Apache Struts2 Remote Code Execution (RCE) Vulnerability (S2-067)	95	2	No
162212	Oracle Enterprise Linux Security Update for unbreakable enterprise kernel (ELSA-2024-12868)	95	1	No
6021490	Ubuntu Security Notification for WebKitGTK Vulnerabilities (USN-7142-1)	95	1	No

Weekly Insights Vulnerabilities: Top5クリティカルな脆弱性
優先度の高いクリティカルな脆弱性があります。パッチ提供の有無も確認できます。





Qualys Threat Research Teamの主なハイライト

ディスカバリー&アワード

Qualys TRU はサイバーセキュリティ研究において一貫して優れた成績を収めており、Best Privileged Escalation Bug と Most Under-Under-Hyped Research の 2 つの名誉ある Pwnie Awards を獲得しています。

Qualys TRU Zero-Day Research/Discovery & Awards

Recognition and awards received by Qualys TRU:

Secured two Pwnie Awards: Best Privileged Escalation Bug and Most Under-Hyped Research (12+ Pwnie Award Nominations)

Nomination for discovering RenderDoc vulnerabilities marks fifth year of recognition in cybersecurity research contributions.

Qualys TRU 脆弱性の発見例:

CVE Identifier	CISA KEV	Named Vulnerabilities	Component Affected	Description
3 CVEs/Vulnerabilities	No	NA	GNU C Library's syslog()	heap-based buffer overflow syslog
CVE-2024-6387	No	regreSSHion	OpenSSH server	Remote Unauthenticated Code Execution Vulnerability in OpenSSH server
5 CVEs/Vulnerabilities	No	NA	needrestart	Privilege Escalation Vulnerabilities
CVE-2023-6779	No	NA	glibc	Off-by-one heap-based buffer overflow in the _vsyslog_internal (function).
CVE-2023-6780	No	NA	glibc	Integer overflow issue in the _vsyslog_internal (function).
CVE-2023-4911	Yes	Looney Tunables	glibc (ld.so)	Local Privilege Escalation.
CVE-2023-38408	No	NA	OpenSSH (ssh-agent)	Remote Code Execution in forwarded ssh-agent.
CVE-2023-33865	No	NA	RenderDoc	Local symlink vulnerability allowing attackers to gain RenderDoc user privileges.
CVE-2023-33864	No	NA	RenderDoc	Integer underflow causing a heap-based buffer overflow, exploitable remotely
CVE-2023-33863	No	NA	RenderDoc	Integer overflow leading to a heap-based buffer overflow, potentially exploitable remotely.
CVE-2022-41974	No	Leeloo Multipath	multipathd	Authorization bypass and symlink attack.
CVE-2022-41973	No	Leeloo Multipath	multipathd	Authorization bypass and symlink attack.
CVE-2021-44731	No	Oh Snap! More Lemmings	snap-confine	Local Privilege Escalation Vulnerability.
CVE-2021-4034	Yes	PwnKit	polkit's pkexec	Local Privilege Escalation Vulnerability.
CVE-2021-33910	No	NA	systemd	Denial of Service (Stack Exhaustion).
21 CVEs/Vulnerabilities	No	21Nails	Exim Mail Server	Multiple Critical Vulnerabilities.
CVE-2021-33909	No	Sequoia	Linux's Filesystem	Local Privilege Escalation Vulnerability.

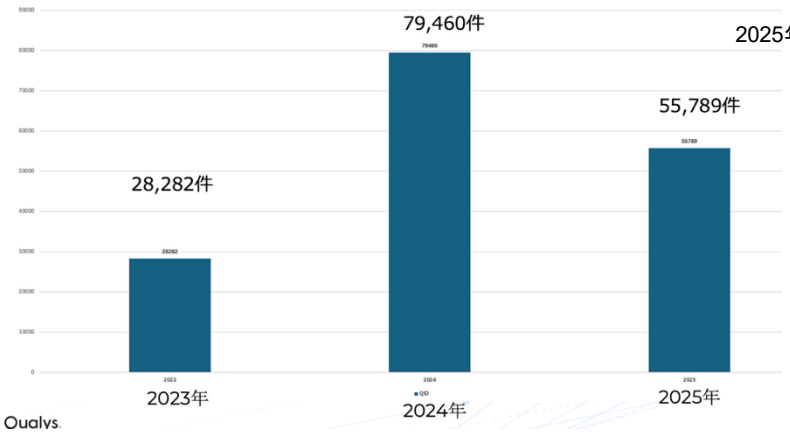
120,486
特定された脆弱性/CVE

269,890
検出シグネチャ(QIDs)

120+
脅威研究ユニット(TRU)の専門家

16 hrs
応答時間の中央値

QID リリース数(2023–2025 YTD)



2025年6月時点

2025年6月時点

ThuRiskを推奨する企業タイプ

企業タイプ	理由
SOC・CSIRTを保有し、**膨大な脆弱性を抱える**大手企業	Truriskによる優先順位付けと自動分析で運用効率化が可能
サイバーリスク可視化と**定量評価を強化**したい企業	TruRiskとの連携で、経営視点での意思決定を支援
セキュリティアナリストが不足している中堅企業	TruRiskがアナリスト支援・代替となり、少人数でも高度な分析が可能
複数セキュリティ製品を使っているが**相関分析に課題**がある企業	Qualys ETM※が異なるデータソースを統合し、知見を抽出
従来のダッシュボードでは**迅速な判断が難しい**	カスタマイズが簡単なウェジェットを作成し、様々なデータをダッシュボードで確認できる
経営層への**レポーティングに時間がかかる**	すぐに使えるテンプレートで現場レベルからCISO、経営者層へのレポート作成が可能

※Qualys Enterprise TruRisk Management（ETM）は、世界初のクラウドベースのリスクオペレーションセンター（ROC）として、組織のサイバーリスク管理を統合・自動化するプラットフォームです。

Qualys.

クォリスによるAI、LLMセキュリティ

Total AI

*Total AI は単体でご購入いただけます。

組織の課題

AI と LLM は企業に増大するリスクをもたらします

攻撃対象領域の増加

攻撃者は LLM と AI インフラストラクチャをターゲットにして、モデル (守るべき重要資産) とトレーニング データ (PII) を盗んでいます。
攻撃者に先んじて対処するにはどうすればよいですか?

モデルとデータの損失

AI パッケージと AI インフラストラクチャ関連の CVE は、データとモデルの盗難につながる可能性があります。
AI インフラストラクチャの重大な脆弱性を発見し、修正するにはどうすればよいですか?

セキュリティの成熟度が低い

LLM には堅牢なセキュリティ対策が欠けていることが多く、コンプライアンス違反や罰金につながる可能性があります。
リスクを理解するためにモデルをテストするにはどうすればよいですか?

低い可視性

セキュリティ チームは、AI のワークロードとモデルに盲目になっていませんか?
インフラストラクチャにモデルはありますか? それらはどこで稼働しているのでしょうか?

セキュリティサイロ

ツールが多すぎるにもかかわらず、可視性が欠如しています。
セキュリティ投資からより高い ROI を得るにはどうすればよいですか?

Qualys.

Qualys TotalAIの紹介

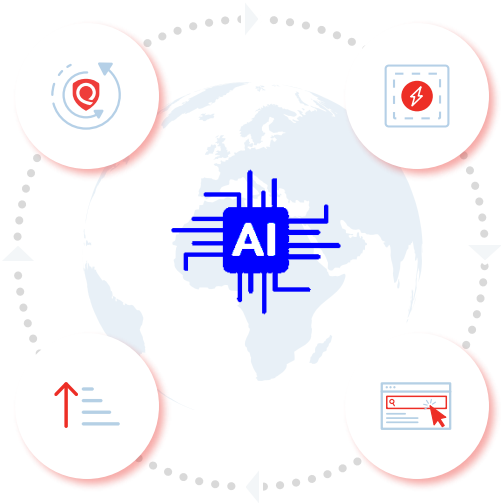
LLM リスク、AI ワークロード、AI 脆弱性を総合的に可視化します

スタック全体の完全な可視化

- すべての AI ワークロードを発見する
- AI パッケージ、AI ソフトウェア、AI ハードウェア (GPU) のインベントリを取得する

モデルのリスクを評価する

- LLM エンドポイントをスキャンする
- LLM に OWASP LLM TOP 10およびMitre Atlasのマッピング プロンプトを表示し、データの漏洩、バイアスの表示、ジェイルブレイク攻撃の可能性がないことを確認します



脆弱性評価

- TruRisk の脅威と相関する 1,000 以上の AI 固有の脆弱性検出結果
- 脆弱性リスクにパッチを適用し、モデルやデータの盗難からインフラを保護

レポーティングとコンプライアンス

- コンプライアンス違反 (GDPR、PCI など) による罰金の回避
- 管理者向け LLM セキュリティ レポート

既存の Qualys Agent と Scanner を使用

Qualys.

TotalAI導入のメリット

LLM リスクを発見、監視、軽減します

可視性と制御の強化: AI インフラストラクチャを完全に可視化します。AI モデルがどこに存在するかを把握します。

プロアクティブなインフラストラクチャ強化: モデル盗難とデータ損失を防止するため、リアルタイムでCVEを継続的に特定し、優先順位を付けます。

コンプライアンス罰金の回避: 定期的なモデル スキャンにより、関連するデータ保護およびプライバシー規制へのコンプライアンスを確保できます。モデルがデータを漏洩していないことを確認します。

リスクの優先順位付けと排除: セキュリティ ツールのサイロを排除する TruRisk を使用して、AI スタック全体でリスクに優先順位を付けます。

対象を絞った LLM セキュリティ: LLM 固有の最も重大なセキュリティ リスクに焦点を当てるための LLM 固有のスキャン。

Qualys.

AI ソフトウェア＆パッケージの検出

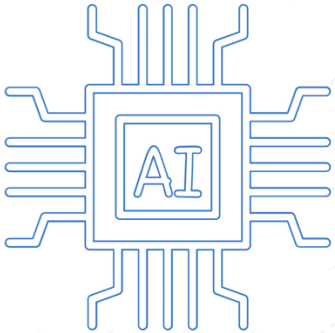
オンプレ及びマルチクラウド

- Altair Engineering RapidMiner
- Altair Engineering RapidMiner Studio
- Alteryx Intelligence Suite
- Anaconda
- Anaconda Jupyter Notebook
- Anaconda Miniconda
- ANSYS STK Integrated Jupyter Notebooks
- Anyscale Ray
- Apache Airflow
- Apache PySpark
- Azure Machine Learning Workbench
- BUNDLAR BUNDLAR
- DataRobot
- David Cournapeau scikit-learn
- Element Labs LM Studio
- ExplosionAI spaCy
- fast.ai
- Gael Varoquaux Joblib
- Google TensorFlow
- Guolin Ke LightGBM
- Homebrew Jan
- Hugging Face
- Hugging Face Transformers
- IBM Watson Content Analytics
- IBM Watson Studio
- Intel oneDAL and Intel Extension for Scikit-learn
- Iterative.ai DVC
- Jupyter Notebook
- KNIME KNIME Analytics Platform
- KPMG LLP KPMG Bridge
- Kubeflow
- libboost-numpy
- Logitech Logi AI Prompt Builder
- Matplotlib
- Microsoft Azure AI Machine Learning Studio
- Microsoft Azure Machine Learning Workbench
- Miniconda
- MLflow Project Mlflow
- NLTK Team NLTK
- Nomic GPT
- Numpy
- NumPy Developers NumPy
- NVIDIA CUDA
- NVIDIA CUDA Toolkit
- NVIDIA TensorRT
- NVIDIA Triton Inference Server
- Ollama
- OpenAI ChatGPT
- Opencv
- Pandas
- Jupyter Notebook
- Python
- python-matplotlib
- python-numpy
- Radim Rehurek GenSim
- SAS Institute SAS Viya
- Sebastian Ramirez FastAPI
- Squirro Joblib
- The Eclipse Deeplearning
- The Kubeflow Authors Kubeflow
- The Matplotlib development team Matplotlib
- The XGBoost Contributors XGBoost
- Travis Oliphant SciPy
- Wes McKinney Pandas

モデルエンドポイントの検出とインベントリ

包括的な AI セキュリティで AI パイプラインをエンドツーエンドで保護

包括的な検出のためのQIDを使用して、MCP(モデルコンテキストプロトコル)サーバーを完全に可視化します。



1500+ 検出シグネチャ (QID)

Azure Foundry	AWS Bedrock	GCP AI Studio
Azure AI services	AWS Bedrock Serverless	Vertex Model Endpoints
Azure OpenAI services	AWS Sagemaker	Vertex Models
Azure Machine Learning		

Qualys.

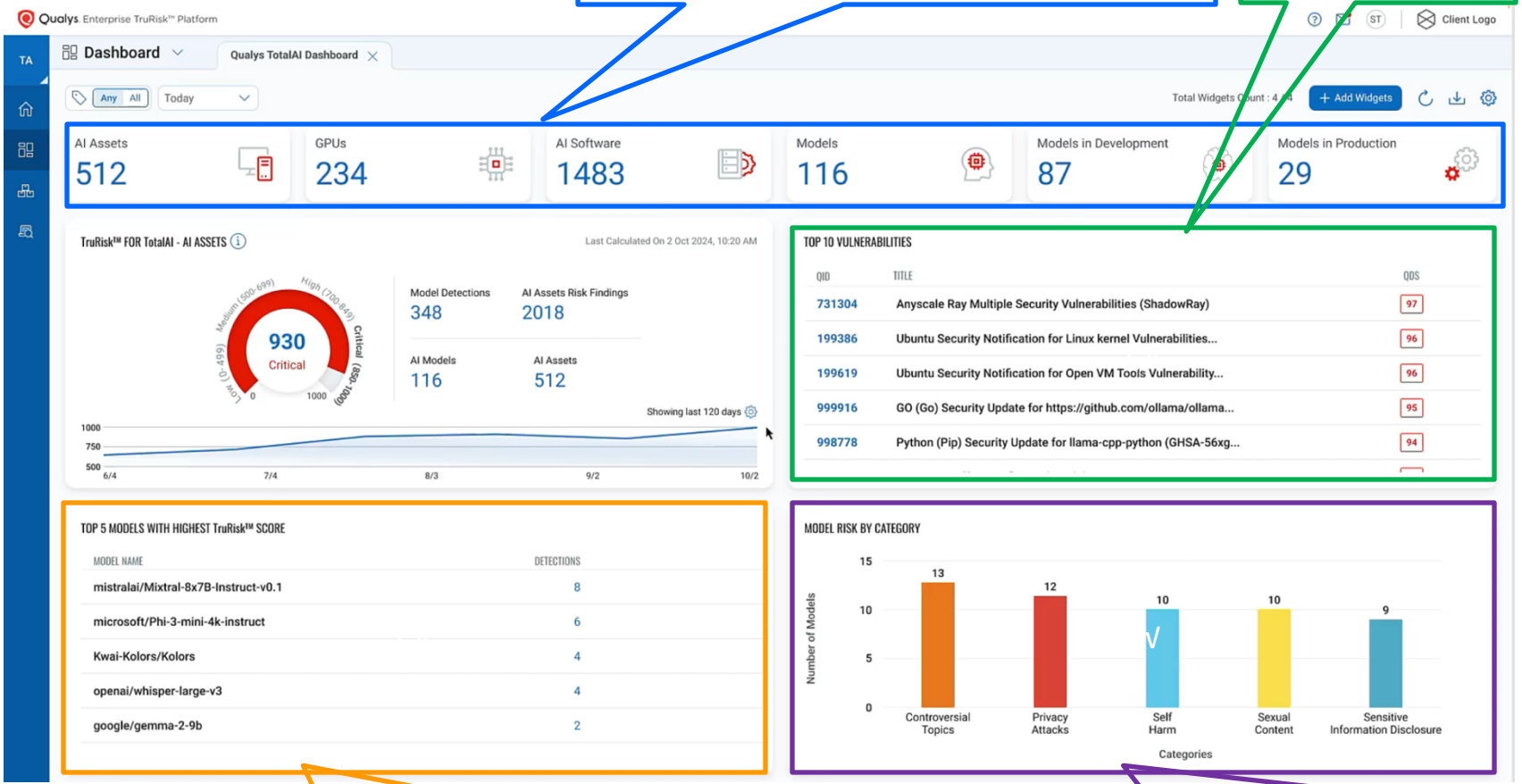
マルチクラウド環境でのモデルの発見

Qualys.

TotalAIダッシュボード

AI パッケージ、AI ソフトウェア、AI ハードウェア (GPU) の発見とインベントリ

検出された脆弱性のTOP10とリスクスコア



TruRiskスコアに基づくTop5モデル

リスクカテゴリ(論争の的となるトピック、プライバシー攻撃、自傷行為、性的コンテンツ、センシティブな情報の開示)

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 & コンテナセキュリティ全般

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

本番環境のスキャン

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.

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。

Qualys.

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

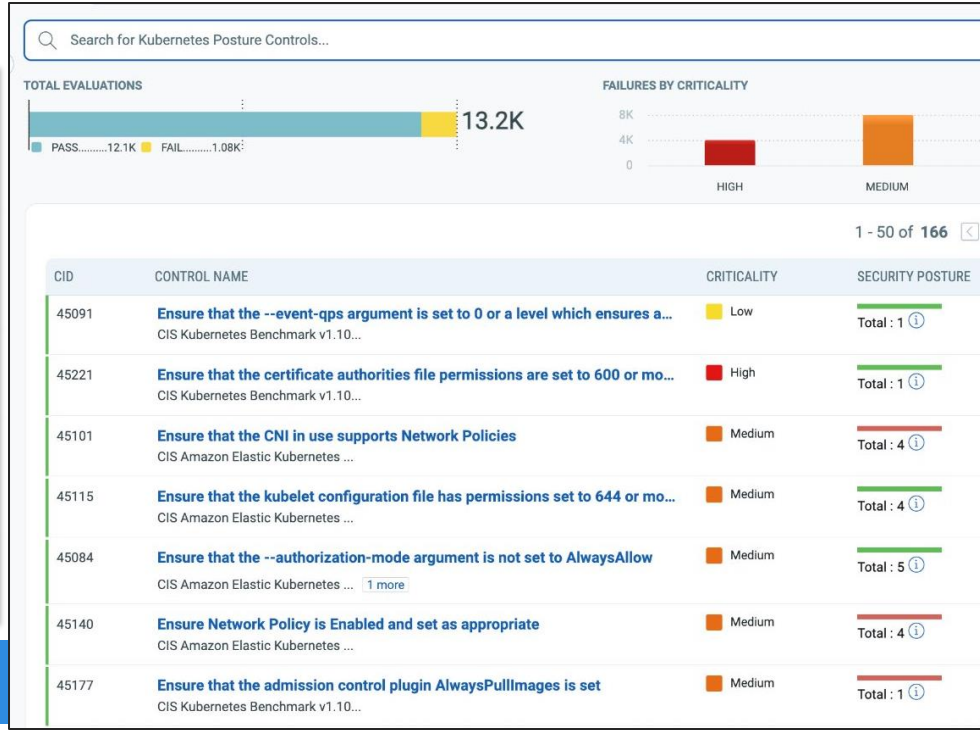
Kubernetes Posture (KSPM) + Admission Controller

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

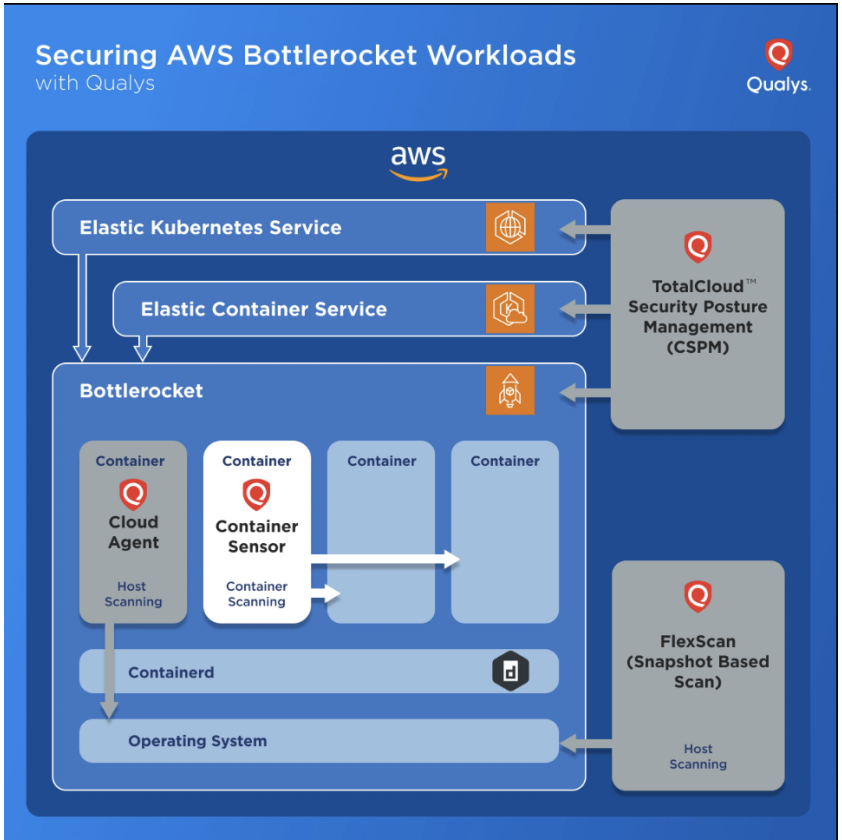
改善点	内容
Kubernetes特化のポリシーテンプレート追加	CIS Kubernetes Benchmarkの自動適用やカスタムポリシー対応。
構成ファイルレベルの監査	kube-apiserver.yamlやkubelet-config.yamlなどの設定ファイルを対象に検証。
スケジュールされた自動監査	定期的に構成監査を実行し、継続的な準拠状況を確認。
コンプライアンスレポートの自動生成	視覚的にわかりやすい形式で、経営層向け／技術担当向けの両方に適した出力。
リスクの優先度付けと対応支援	ポリシー違反ごとのリスクスコア表示や是正ガイド提示。

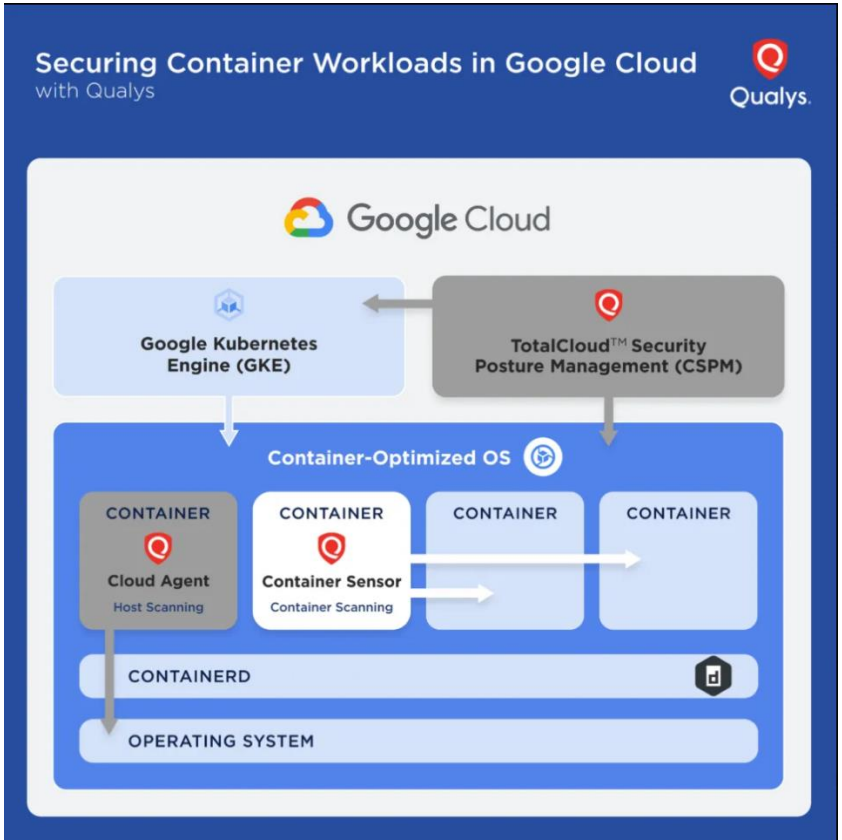
Over 200+ CIS-Certified Controls



※Policy Auditは有償モジュールです。

AWSとGCP上のQualys導入構成図





クォリスクラウドエージェントの特徴

Cloud Agent

*Cloud AgentはVMDRライセンスが必須です。

Cloud Agent 対応サービス

- ライセンスごとにCloud Agentのインストールは不要。Cloud Agentを一度インストールするのみ。
- 管理者は、購入したサービスを管理画面からアクティベートするだけで、エンドポイントに適用出来ます。
- VM(脆弱性管理)、PM(パッチ管理)、EDR、PA(コンプライアンス評価)、CAR(FirstPartyリスク評価)FIM(ファイル改ざん検出)、CSAM(サイバーセキュリティアセット管理)から利用したいサービスを購入。
- SwCA(オープンソフトウェア検出および脆弱性管理)はVMライセンスの購入が必要。SwCA自体のライセンスは不要。
- CAPS(Cloud Agent as Passive Sensor)はCSAMライセンスの購入が必要。CAPS自体のライセンスは不要。

※ 対応OSプラットフォームは以下をご参照下さい。
<https://success.qualys.com/support/s/article/000006675>

Qualys.

Cloud Agent 対応プラットフォーム

業界で最も広範なカバレッジ

Windows
.exe (x86_64)

Windows
.exe (ARM64)

Linux
.rpm (x86_64)

Linux
.rpm (ARM64)

Linux
.rpm (ppc64le)

Linux
.deb (x86_64)

Windows
.exe (x86_64)

zSystems LinuxONE
.rpm (s390x)

zSystems LinuxONE
.rpm (s390x)

Mac
.pkg (x86_64)

Mac
.pkg (Apple Silicon)

BSD UNIX
.txz (x86_64)

AIX
.bff (POWER)

Solaris
.pkg (x86_64,SPARC)

CoreOS
.tar (x86_64)

ChromeOS
.apk (x86_64)

SQL Server

Oracle Database

- Qualys Only

Bottlerocket OS
.tar (x86_64)

Container-optimized OS by Google
.tar (x86_64)

GenToo
.tar (x86_64)

※ 対応OSプラットフォームはこちらをご参照下さい。

CAR– カスタムシグネチャによる検知と応答

今日、多くの組織は、80%がオープンソースのコンポーネント上に構築されたプロプライエタリまたは「ファーストパーティ」ソフトウェアを使用してビジネスを運営しています。Qualys Custom Assessment and Remediation を利用すると次の事が実現できます。

■カスタムQIDを作成できます

- お客様にてFirst Partyアプリケーション(独自に開発したプログラム)検知用にQID(カスタムシグネチャ)をお好みのスクリプト言語(Python, PoweShell, LUA、その他)を使用し、独自のロジックを記述する事で作成できます。
- Qualys スクリプトライブラリの事前定義されたテンプレートまたはスクリプトを使用し、ニーズに合ったQIDを作成する事ができます。

■対優先対応による修復対応

- VMDR TruRisk を使用して結果に優先順位を付ける事ができます。
- 独自のカスタムスクリプトを使用して脆弱なアセットを修復できます。

■ユースケース

事例１：侵入テストチームは、何千ものアセットにデプロイされている自社開発のアプリケーションに脆弱な jar を見つけました。カスタム QID を作成し、すべてのアセットでこの脆弱な jar を探します。すべての脆弱な資産が表示され、VMDRから直接管理できます。

事例２：カスタムアプリケーションは、設定ファイルやログファイルのシークレットを誤って共有する可能性があります。CARを使用し、組織は、プレーンテキストの秘密鍵やアクセスキーなど、安全でないシークレットの使用をすべて見つけるためのクイックスクリプトを作成できます。

事例３：新しいゼロデイ通知が発生し、多くのファーストパーティおよびサードパーティアプリケーション(log4jなど)に組み込まれた一般的なライブラリに影響を与える可能性があります。ワンクリックワークフローを活用して、これらのコンポーネント(Runtime SCA Scanによって収集)を統一された方法で検索することにより、ゼロデイの範囲を理解します。

事例４：カスタム QID を作成し、未承認の Chrome アドオンがインストールされている脆弱なアセットや、未承認のプラグインを含む環境内の他のアプリとしてフラグを設定します。

SwCA（Software Composition Analysis）ソフトウェア構成分析 VM

可視化からアクションへ

SwCAの機能強化によるソフトウェアサプライチェーンのセキュリティの向上

「開発とセキュリティをつなぎ、SBOM導入による“常駐型”サプライチェーン防衛ツール」

① リアルタイム製品・実行環境連携

CI/CDや運用環境、実行中プロセスと脆弱性情報を統合し、「リアルタイムに脆弱性を可視化」。

② Software Atlas：アプリ ↔ コンポーネントの関係把握 CSAM

どのOSSがどのアプリに使われているかを明確化。顧客関連アプリなど重要性に応じた優先順位付けが可能 。
修正までの所要時間を最大60%短縮。

③ C/C++バイナリ解析対応

静的リンクされたライブラリなど、従来スキップされていたC/C++領域の脆弱性を検出し、TruRisk™スコアによる一元管理が可能に。

④ スマートチケッティング連携

JiraやServiceNowと連携し、オーナー別に脆弱性を自動でタスク化。問題の所在と責任者を明確化 。

⑤ SBOM（CycloneDX形式）の自動出力

UIおよびAPI経由でCycloneDX v1.4／v1.6形式のSBOMを生成。常に最新の構成情報と脆弱性情報を反映。

⑥ ランタイム可視化

インストール済みではなく「稼働中の」OSSコンポーネントを識別し、対応の優先度を最適化 。

⑦ エンタープライズ規模の対応力

1つの資産で20,000以上のOSSコンポーネントを扱える規模と柔軟なクエリ・API機能を備えています。

Qualys.

6月16日ブログはこちら

SCA Security Configuration Assessment

VM

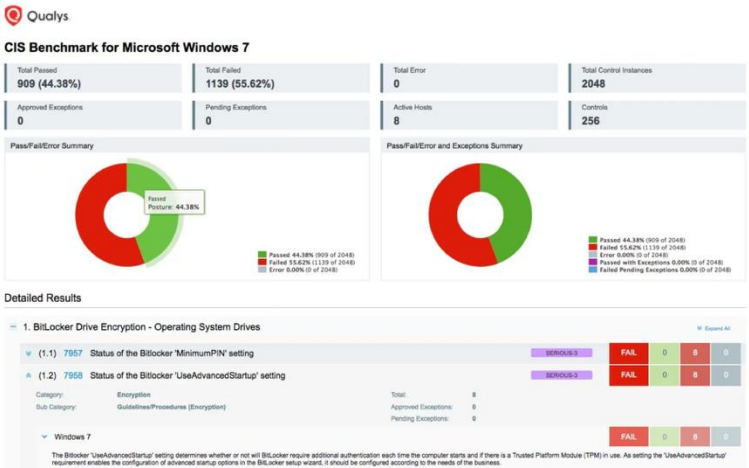
クラウドベースの構成管理とセキュリティ強化を実現する、統合型VM拡張ソリューション

SCA（Security Configuration Assessment）とは

ソフトウェアのセキュリティ設定を通じて、セキュリティの強化を図る手法です。例えば、オペレーティングシステムがファイルに対するユーザーのアクセス権を設定するアクセス制御リスト（ACL）を提供したり、アプリケーションが保存される機密データの暗号化を有効または無効にする設定を提供したりします。これらのセキュリティ設定が誤って構成されると、ソフトウェアのセキュリティに悪影響を及ぼす可能性があります。SCAのような優れたセキュリティ構成プログラムは、攻撃者がこのような構成上の脆弱性を悪用することを困難にします。

SCAの導入手順

1.アセットの追加: VMでスキャン済みのアセットにSCAを有効化。
2.CISポリシーのインポートと構築: 200以上の事前設定されたCISポリシーから選択し適用。
3.設定データの収集: スキャンを開始し、CISポリシーに基づくデータを収集。
4.レポートの生成: CISベンチマークに基づいた最新のコンプライアンス状態をレポート化。



Qualys.

EDR – Endpoint Detection and Response

強化された機能

1. MITRE ATT&CKフレームワークとの統合
Qualys EDRは、**MITRE ATT&CKフレームワークと統合**され、**脆弱性や誤設定、EDRインシデントを攻撃者の視点で分析で**きるようになりました。これにより、潜在的な脅威を予測し、優先順位を付けて迅速に対応することが可能です。

2. カスタムおよびシステム生成クエリの強化
EDR 3.7では、システム生成クエリとカスタムクエリの管理機能が強化され、**詳細の閲覧、クローン作成、編集が可能**になりました。これにより、**脅威ハンティングやインシデント対応の柔軟性と効率性が向上**しています。

3. ランサムウェア対策機能の追加
EDR 3.4.1では、**ランサムウェアの検出と防止、暗号化されたファイルの復旧、ローカルプロセスやリモートアクセスされたネットワークパスの保護機能が追加**されました。特定のフォルダーやプロセス、リモートIPアドレスを**監視対象から除外**することで、**重要な領域にセキュリティリソースを集中**できます。

4. MacOS Intel版Cloud AgentでのEDRサポート
Cloud Agent for MacOS Intel 6.0では、EDRアプリケーションのサポートが追加され、**システムファイルやプロセスの監視、ファイルの作成・更新・削除の追跡が可能**になりました。これにより、MacOS環境でのセキュリティポスチャーの監視と脆弱性の検出が強化されました。

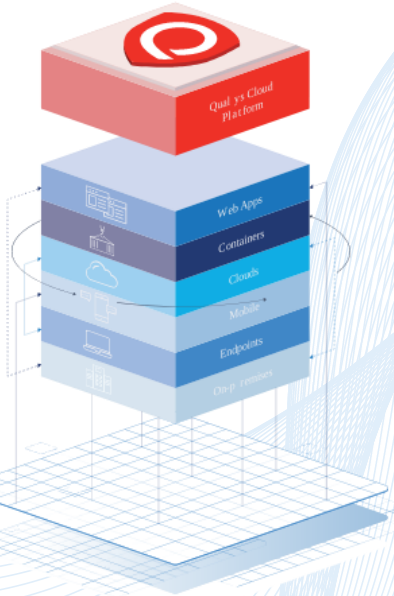
5. MITRE ATT&CK評価での高評価
Qualys EDRは、**2024年のMITRE ATT&CK評価**において、LockBitおよびCl0Pシミュレーションの主要ステップを**100%検出**し、**誤検出率も非常に低い**結果を達成しました。これにより、Qualys EDRの**高度な脅威検出能力と正確性が証明**されました。

EDR主要機能

Qualys Cloud Agentの品質、セキュリティ、安全性

ユーザー モード: VM、PC、SwCA、CAPS、CAR、Patch Management、CSAM はユーザーモードで開発されています。 このアプローチはオペレーティングシステムのカーネルに干渉せず、ブルースクリーンオブデス(BSOD) シナリオのリスクを排除します。

段階的導入: Qualys アップデート (エージェントバイナリ) は、社内の導入から始まり、潜在的な影響を最小限に抑えるために選択された顧客に段階的にリリースされます。 rm、kill、mv などの悪意のあるコマンドを防止するために、自動チェックが導入されています。



カーネル モードのアプリ: Windows OS で実行される EDR および FIM の場合のみ、カーネル ドライバーが必要です。検出、コンテンツ、署名、およびデータ収集は非侵入的であり、リソースを大量に消費しません。 Linux および Mac OS では、カーネル モードは呼び出されません。 Qualys は、コンテンツの更新を通じてカーネル ドライバを変更しません。 ドライバーの変更はすべて、Microsoft による認定後に新しいエージェント バージョンとしてリリースされます。

Qualys のテストプロトコルには次のものが含まれます (これらに限定されません) :

- 新機能と変更の静的コード、メモリ リーク、バイナリ分析。
- サポートされているすべての Windows プラットフォームでのドライバーのロード/アンロード テスト
- カスタム スクリプトを使用して、カーネル コンポーネントを切り替えてシステムとアプリケーションのパフォーマンスをテストするパフォーマンス影響評価。
- エージェントとドライバーのパッケージを承認する前に、バースト、ハイ、およびノーマル モードで耐久性とパフォーマンスのテストを行います。
- WHQL 認定テスト スイート (Microsoft によって作成され、サポートされているすべてのバージョンの Windows で実行される 4,000,000 のファイル システムとネットワークのテスト)。

仮想スキャナーを利用したCloud Agentの展開

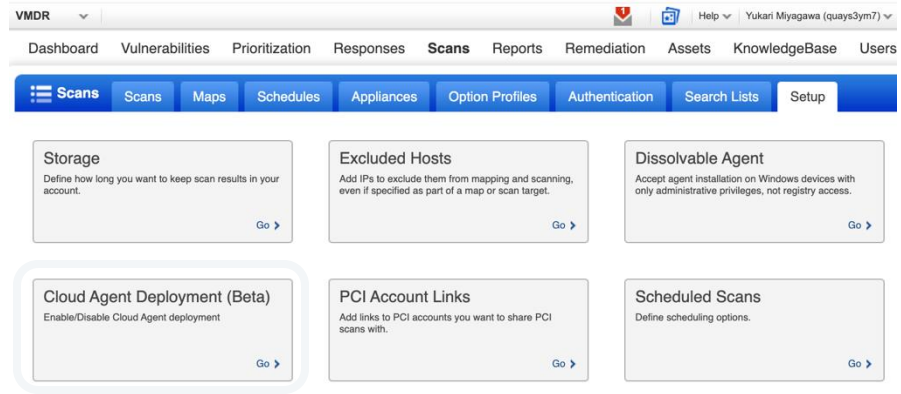
Qualys スキャナを使用すると、サードパーティのツールに頼ることなく、クラウド エージェントを展開できます。スキャナは、次のプラットフォーム タイプの Windows/Linux アセットにクラウド エージェントを展開できます。

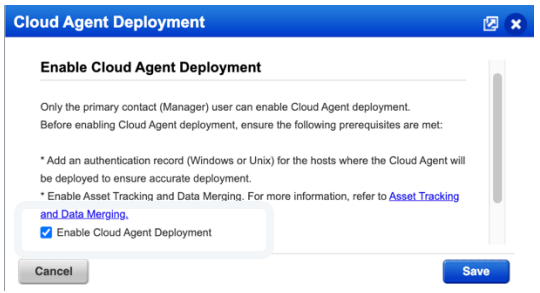
- Windows-X86-32/64
- Linux-X64-RPM
- Linux-X64-DEB

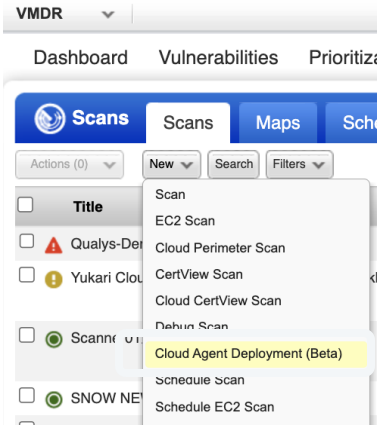
前提条件

•この機能はデフォルトでは有効になっていません。サブスクリプションでこの機能を有効にするには、Qualys サポートまたは TAM にお問い合わせください。
•スキャン中はターゲット ホストが稼働している必要があります。
•スキャン中、Unix ターゲット ホストでは SSH サービスが実行されている必要があります。
•展開中、Windows ターゲット ホストでは SMB サービスと Windows リモート管理サービスが実行されている必要があります。
•正確なデプロイメントを確実に行うには、クラウド エージェントがデプロイされるホストで PC/SCA 認証レコード (Windows または Unix) が使用可能である必要があります。
- Windows認証を設定する
- Unix認証の設定

•必ずアクティベーション キーを作成してください。
•アクティベーション キーと認証レコードが同じネットワーク内にあることを確認します。







参考資料：[Deploy Cloud Agent Using Qualys Scanner]

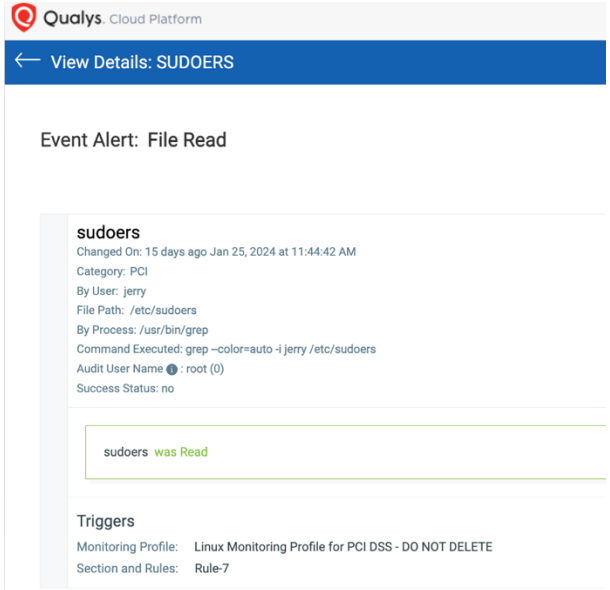
Qualys 補助資料

FIM

File Integrity Monitoring

不正なファイル、フォルダ、レジストリ、オブジェクトアクセスをリアルタイムに監視、記録し、アラート通知するコンプライアンスに不可欠な機能

カテゴリ	機能	説明
リアルタイム監視	ファイル、フォルダ、レジストリの変更を即時検出	システムファイルや設定の変更をリアルタイムで検知し、詳細を記録。
ユーザー操作の追跡	操作記録「誰が・いつ・どのように」	操作ユーザーや変更内容を詳細に記録。
アラート・レポート	自動通知と監査レポート	不正な変更の通知とコンプライアンス対応レポートを生成。
ファイルアクセス監視（FAM）	アクセス試行の記録	機密ファイル等へのユーザーアクセス履歴を詳細に記録。
エージェントレス監視	ネットワーク機器の監視	ルーターやファイアウォールなども対象。
コンプライアンス対応	規制準拠	PCI DSS、HIPAA、GDPR、NISTをなどに対応。
誤検知の削減	アラート精度向上	信頼された変更をホワイトリスト化し不要なアラートを最大90％削減。
一元管理とダッシュボード	ワンプラットフォームによる統合監視	複数環境（オンプレミス、AWS、Azureなど）を統合



PCI Security Standards Council
California Consumer Privacy Act (CCPA)
GDPR.EU
U.S. Department of Health and Human Services
NERC
NIST

Continuous Monitoring

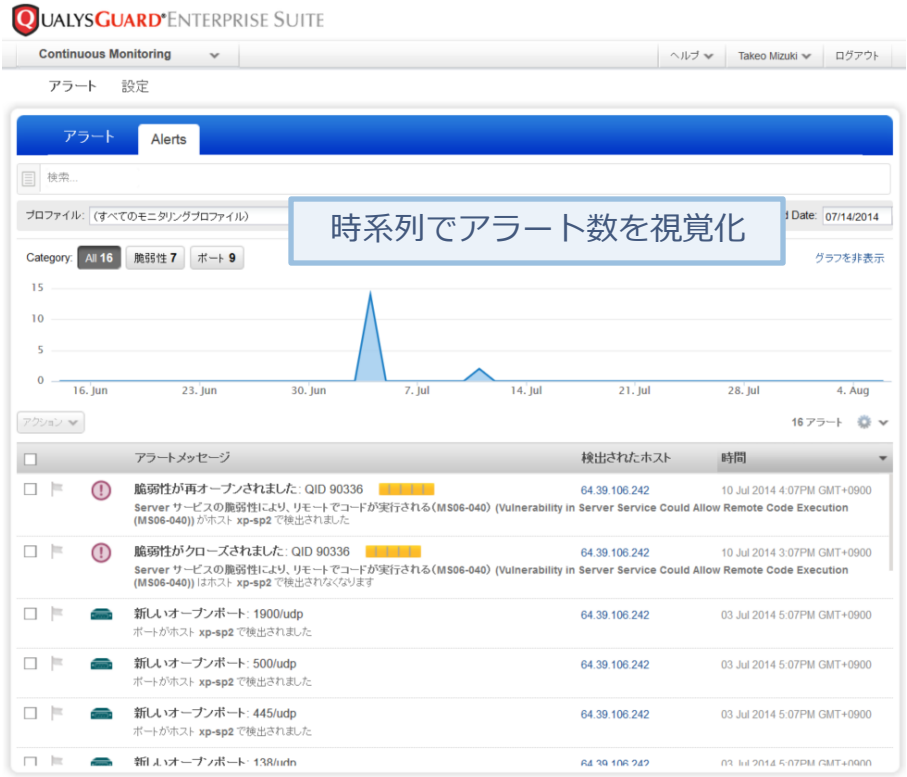
CM

■主な機能の説明

機能	内容
リアルタイム監視	IT資産に対する変更（例：新規ポート、サービス、脆弱性など）を即時検出
ポリシーベースのルール設定	資産やイベントに対して条件を設定し、特定の変化があればアラートを自動通知
資産グループの柔軟な管理	タグベースで資産グループを動的に作成・監視できる
通知の自動化	メールやAPIでのアラート通知に対応し、SOARなどと連携可能
継続的スキャンの連携	VMDRやスケジュールスキャンと組み合わせ、検出から対応までの自動化が可能

■アラート/監視対象ユースケース

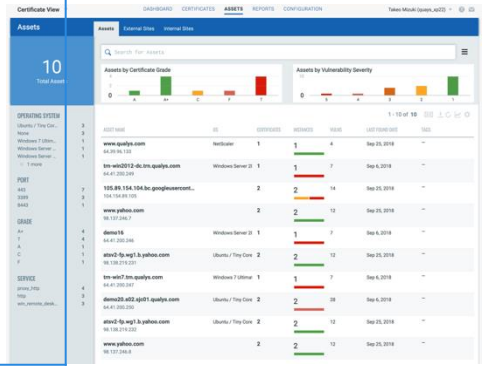
ユースケース	説明
新しい脆弱性の即時検知	公開サーバーに新しい脆弱性が追加された際に即通知、早期対応を可能に
シャドーITの検出	知らない資産がネットワークに追加された場合に検知し、管理外資産のリスクを可視化
構成変更の監視	特定ポートの開放やサービス起動など、ポリシーに違反する変更があれば即通知
攻撃対象領域の変化の把握	外部公開範囲に変化（DNS変更、新IP追加など）があった際に検出
コンプライアンス監査支援	設定逸脱や不正な変更を自動で記録・通知し、監査レポートの元データとして活用可能



CERT

CertView

機能カテゴリ	機能内容
証明書の自動検出	ネットワーク上のすべてのSSL/TLS証明書をスキャンし、自動でインベントリ化
有効期限の管理	証明書の有効期限を可視化し、期限切れ前にアラート通知
脆弱性と構成の評価	弱い暗号スイート、自己署名、古いプロトコル（例：TLS 1.0）などを検出
証明書の所有者タグ付け	アプリや部門別などに証明書をタグ付けし、管理責任の明確化
CA（認証局）の可視化	使用中のCAを一覧表示し、信頼されていないCAや方針違反を特定
レポートとダッシュボード	リスクのある証明書や期限切れ証明書を一目で確認できるレポート・可視化機能
ポリシーベース監視	自社ポリシー（有効期間、暗号強度など）に基づいた継続的監視
API連携	CMDBやITSMとの統合、証明書更新フローとの自動化連携が可能



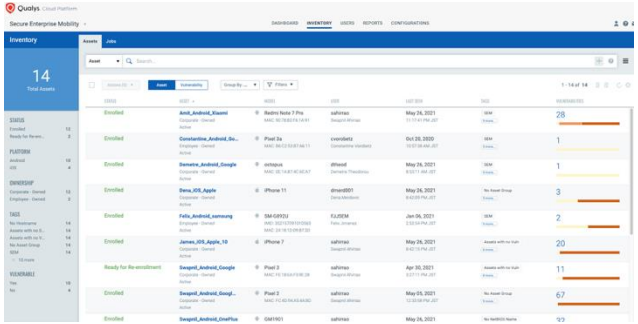
ユースケース	説明
期限切れ証明書の防止	有効期限が迫った証明書を検出し、事前に通知してサービス停止リスクを回避
シャドー証明書の特定	管理外の自己署名証明書や開発環境に残存する証明書を検出して統制強化
PCI DSS対応支援	弱い暗号スイートの使用検出により、コンプライアンス準拠を支援
ゼロトラスト環境での可視化	外部公開サービスやクラウドに設置されたSSL証明書も一括可視化し、セキュリティ強化
証明書ライフサイクル管理の最適化	所有者や用途ごとの分類により、更新・失効管理を効率化
攻撃対象領域の把握と削減	公開証明書から外部攻撃対象資産を特定し、リスクを低減

Mobile

VMDR Mobile

Qualys VMDR Mobile（Vulnerability Management, Detection and Response for Mobile Devices）は、**モバイルデバイス（iOS/Android）に対する脆弱性管理とリスク対応**を可能にするソリューションです。従業員のスマートフォンやタブレットを含むモバイル環境の可視化・セキュリティ強化に貢献します。

機能カテゴリ	機能内容
モバイル資産の自動検出	iOS/Androidデバイスを自動で検出・インベントリに追加
アプリ情報の取得	インストール済みアプリ、バージョン、許可権限の可視化
OSの脆弱性管理	OSに存在するCVE脆弱性の検出、CVSSスコアやTruRiskによる優先順位付け
設定ミス・セキュリティ状態の把握	暗号化未設定、パスコード未設定、Jailbreak検知など
コンプライアンス対応	CISベンチマークなどのモバイルポリシー準拠チェック
TruRiskによるリスク評価	アプリ、OS、構成の情報を統合し、リスクスコアを算出
アラートとレポート	リアルタイムなアラート、脆弱性一覧、対応状況などのレポート機能
統合されたダッシュボード	PCやサーバーと同一ダッシュボードでモバイルも一元管理可能



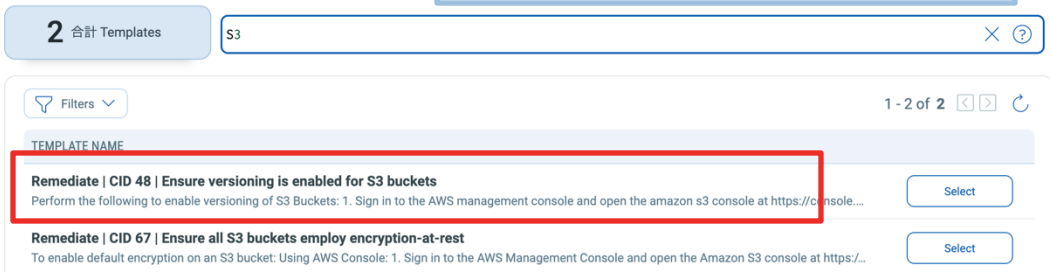
ユースケース	説明
BYOD環境のリスク可視化	私物端末の業務利用に伴うリスクを検出し、セキュリティポリシーの遵守を確認
アプリ脆弱性の早期検出	悪意あるアプリや既知の脆弱性アプリを可視化し、使用停止や通知を促す
インシデント調査支援	モバイル関連のセキュリティインシデント時に、構成・脆弱性情報から調査を迅速化
監査・レポート作成	モバイルポリシー違反の検出結果を元に、監査対応や外部報告用レポートを自動生成可能
セキュリティポスチャの統一管理	PC・サーバー・モバイルを1つのプラットフォームで横断的にリスク管理

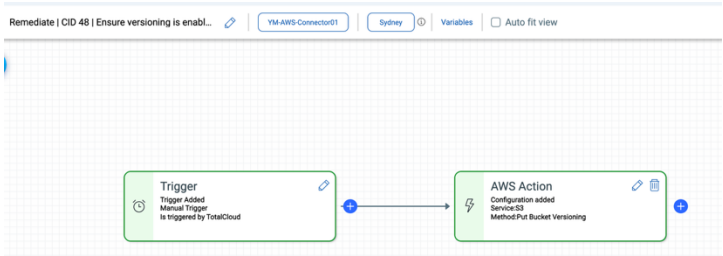
Qualys Flow

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]

Qualys.

MAP

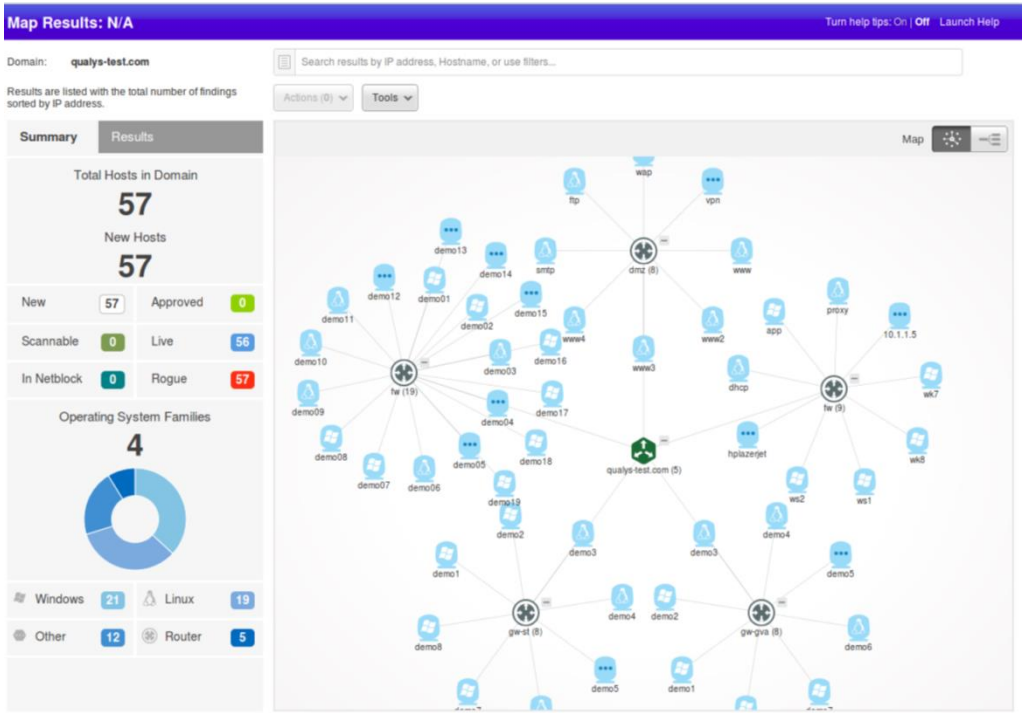
Qualys Mapping

IT資産の有無を正確に把握するための事前探索機能

Qualysの「Mapping機能（MAP機能）」とは、ネットワーク内外に存在するIT資産を自動的に検出・可視化し、攻撃対象領域（Attack Surface）を正確に把握するための資産可視化機能です。主に、脆弱性スキャンを実施する前段階として、スキャン対象の資産やサービスを特定するためのマッピング（事前探索）に使われます。

主な機能：自動資産検出、動的マップ生成、VMDRやTASへのスキャン連携、継続的な探索スケジュール、探索対象、探索範囲、除外対象、など細かく設定可能です。

ユースケース	説明
1. 未知の資産の検出（シャドーIT）	社内外に存在する未登録サーバやWebアプリを可視化
2. スキャン前の事前準備	VMDRで脆弱性スキャンを行う前に、対象資産の正確な把握
3. ネットワークセグメントの可視化	IP空間ごとに分布するホストやサービスを図で表示し、漏れや不要な公開を発見
4. リスク評価の網羅性向上	資産検出漏れによる「スキャン漏れ」を防止し、リスク管理の抜けを防ぐ
5. 脆弱性管理の自動化連携	検出資産をVMDRやWASに自動で登録し、スキャンとレポートを自動化



Qualys.

Qualys Cloud Agent パッシブ センサーの紹介

CAPS

継続的に監視し、内部の攻撃対象領域を削減する

Windows及びLinuxの
Cloud Agentにて対応

単一、軽量、拡張可能、自己更新、集中管理型エージェント

さまざまなシステム向けにカスタマイズ可能な Qualys Agent は、パブリック ネットワークまたはホーム ネットワークからのデータをフィルタリングします。

ネットワークタップの制限から逃れる

ドメインごとに自動選択されたマスター レポーターによる非侵入型のネットワーク レポート。Qualys プラットフォームの管理対象/非管理対象資産を表示します。

パッシブセンシング

データはブロードキャストとマルチキャストをリッスンすることにより、サブネット内で受動的に傍受されます。

- ARP、DHCP、SSDP、NetBios、mDNS、CDP/LLDP、LLMNR、WSD などを使用して豊富なアセット メタデータを収集します。

ユースケース	説明
シャドーITの検出	管理外のPCやIoTデバイスなど、見落とされがちな資産を把握
BYOD環境の監視	従業員の個人デバイスが業務ネットワークに接続された瞬間を検知
ゼロトラスト対応	接続デバイスの即時可視化により、動的なアクセス制御の基盤を支援
資産インベントリの拡充	Cloud Agentでカバーできない部分の可視性を向上させ、完全なCMDBを実現
コンプライアンス準拠	継続的な監視と記録により、証跡を保ちながらリスク管理を強化

センサーや新しいシステムに大規模な投資をせずに、
IoT 環境でも不正デバイスを特定

Qualys.

＊CAPSを使用するにはCSAMライセンスが必要です。

Qualys Passive Sensor の概要

Qualys Passive Sensorは、ネットワーク上を流れるトラフィックを**ミラーポートやTAP経由で受動的に監視**することで、リアルタイムで資産や通信を検出・可視化するセンサーです。

機能	説明
リアルタイム資産検出	ネットワークトラフィックを監視し、接続されたデバイスやシステムを即座に検出。非管理資産の把握にも対応。
エージェントレス監視	エージェントやクレデンシャルなしで資産情報（OS、MAC、アプリ名など）を取得可能。
通信プロトコル識別	HTTP、FTP、SSH、SMB、DNSなど多様なプロトコルを自動識別し、通信内容のメタデータを収集。
シャドーITの検出	不正にネットワークへ接続されたデバイス（BYOD、IoT等）を自動的に検出し、可視化。
他のQualysソリューションと統合	CSAM（CyberSecurity Asset Management）やVMDR、EASMと連携し、統合的なリスク管理へ展開。

ユースケース	詳細
非管理資産の発見	DHCPやIPスキャンでは見逃される一時的・未管理の資産（IoT機器やBYOD）を可視化。
ゼロトラスト対応	信頼できない資産の即時隔離や評価につなげ、ゼロトラストセキュリティの基盤として活用。
インベントリの自動補完	Active ScanやCloud Agentで収集できない資産情報を補完し、完全なアセットインベントリを実現。
セキュリティポリシー違反の検出	許可されていない通信や未承認アプリケーション利用の検知。
監査対応・可視化	ネットワーク上の全通信・資産を記録・可視化し、監査レポートやリスクレポートの精度向上。

- **設置場所**: L2スイッチのミラーポートやTAPに接続。
- **デプロイ方法**: センサは仮想アプライアンスとして提供され、オンプレミスでデプロイ可能。
- **対応プロトコル**: 約200種類以上のプロトコル識別に対応。

Unit Managerによるアクセス管理

主な機能と権限

Unit Managerには以下のような権限が付与されます

1．資産管理
- 自分のビジネスユニットにIPアドレスやドメインを追加可能
- スキャン対象の資産グループを作成・編集

2．ユーザー管理
- ユニット内のユーザーの追加・編集・削除
- ユーザータグの作成・編集・削除

3．レポート管理
- スキャン結果のレポート作成・編集・削除・配布

4．ダッシュボード管理
- 自分のダッシュボードの作成・編集・削除
- 他ユーザーのダッシュボードの編集・削除（権限がある場合）

5．スキャンと通知
- スキャンの実行とスケジュール設定
- スキャン完了後の通知受信と対応

利用シーンの例

- 部門ごとにセキュリティ管理を分担したい場合
- グローバル企業で地域別に管理者を配置したい場合

注意点

- Unit Managerは**1つのビジネスユニットにのみ所属可能**です。
- 他のユニットの資産やユーザーにはアクセスできません。
- 初めてビジネスユニットを作成する際は、**最初のユーザーは必ずUnit Managerとして登録**する必要があります。

TAGによるアクセス管理

Qualysでは、**TAG（タグ）機能を活用したアクセス管理**が可能です。これは、資産やユーザーにタグを割り当てることで、**きめ細かいアクセス制御**を実現する仕組みです。

◎ ロールベースアクセス制御（RBAC）との連携

Qualysでは、ユーザーに対して「ロール」と「スコープ」を設定できます。タグはこの「スコープ」の定義に使われ、**特定のタグが付与された資産のみを閲覧・操作可能にする**ことができます 。

例）**Readerユーザーの制限**

たとえば、Readerロールのユーザーに対して「営業部タグ」が付与された資産のみを閲覧可能にすることで、**部門ごとの情報分離**が可能になります。

使用目的	タグ例	説明
部署別管理	Finance, HR, IT	部署ごとにアセットを分類
リスク管理	Critical, Medium, Low	アセットの重要度に応じて分類
クラウド資産管理	AWS, Azure, GCP	クラウド環境別に分類
脆弱性対応	Log4Shell, QID12345	特定の脆弱性を持つアセットを抽出

TAGの種類と使い方

◆ **静的タグ** 手動で資産に割り当てる

例：Tokyo-Office, Windows-Server, Finance-Dept

◆ **動的タグ**条件に基づいて自動的に資産にタグを付与

例：OSがWindowsかつIPが特定範囲
→ Windows-Tokyo

◆ **システム定義タグ** Qualysプラットフォームにより自動で作成・管理されるタグ

例：Business Units, Asset Groups, Cloud Agent, Internet Facing Assets, Passive Sensor

◆ **Connectorタグ**Qualys TotalCloudなどのコネクタに対してもタグを付与

Qualys マーケット情報

25年以上にわたってテクノロジーのリーダーシップ、研究、イノベーションを推進

1999
年設立

130+
ヶ国以上

10K+
社以上のサブスク契約企業

2,000+
従業員数

2005-2006
継続的なコンプライアンス監視

2014
NWの継続的な監視とリアルタイムのアラート

2016
業界をリードする脅威分析と脆弱性の優先順位付け

2018
証明書のインベントリと評価

2019
Qualys がパッチ管理でクラウド プラットフォームを拡張

2021
Qualys が CyberSecurity Asset Management でクラウド プラットフォームを拡張

2024
Qualys が Qualys TotalCloud でクラウド プラットフォームを拡張

1999
初のSaaS型脆弱性管理ソリューション

2009-2013
Qualys が Web App Security ソリューションをリリース

2015
セキュリティ評価アンケート(SAQ)

2017
IOC
セキュリティ構成の評価。
ファイル整合性の監視

2018
Qualys が次世代のクラウドおよびコンテナ セキュリティ ソリューションを発表

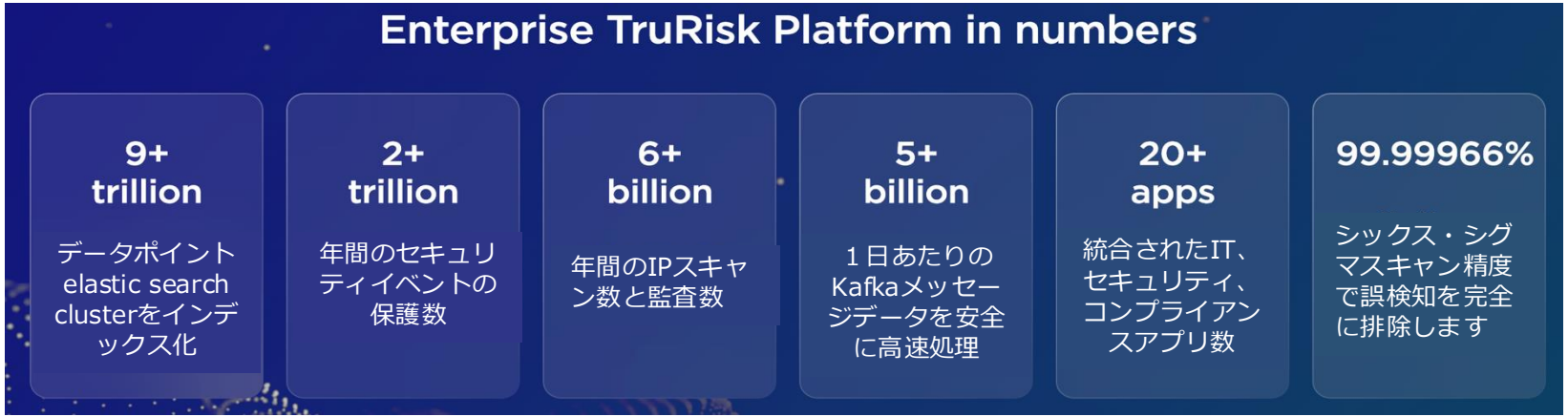
2020
Qualys は、複数のアプリケーション間で問題を関連付けるための ML 機能を備えた統合脆弱性管理プラットフォームを発表

2022
マルチベクトル EDR
コンテキストXDR
カスタム評価と修復

2024
Qualys Enterprise TruRisk Management は、TruRisk を3rdパーティ データセットに拡張

数字でみるTruRiskプラットフォーム

10,000 を超える組織が Qualys でビジネスリスクを軽減している理由



小売業 - トップ10のうち7社
テクノロジー - トップ10のうち8社
通信 - トップ 10 のうち 7 社
ヘルスケア - トップ10のうち6社
金融 - トップ10のうち8社

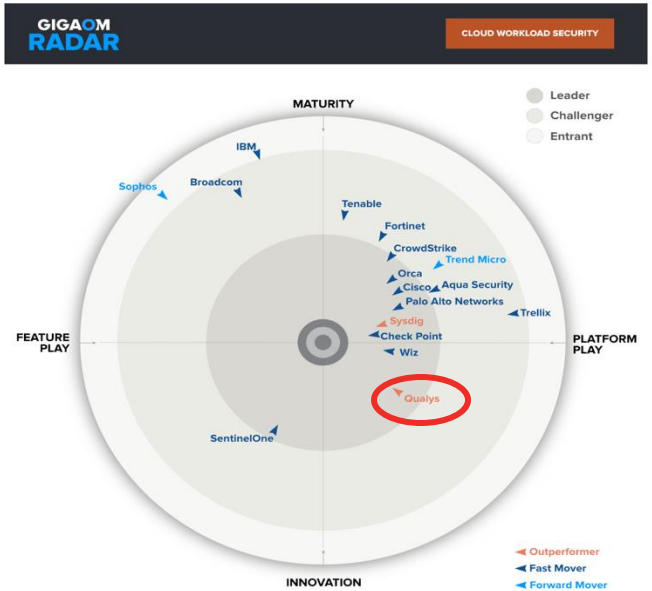
https://www.qualys.com/company/

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

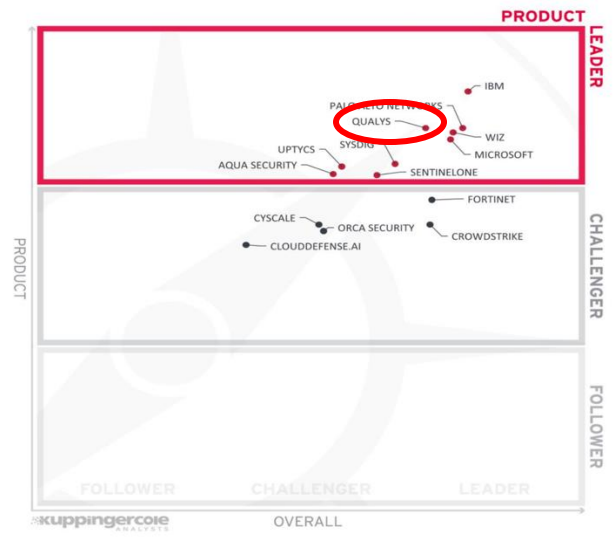
「Qualys は、継続的なイノベーション、頻繁なリリース頻度、将来を見据えた製品ロードマップにより、アウトパフォーマーに分類されました。」

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

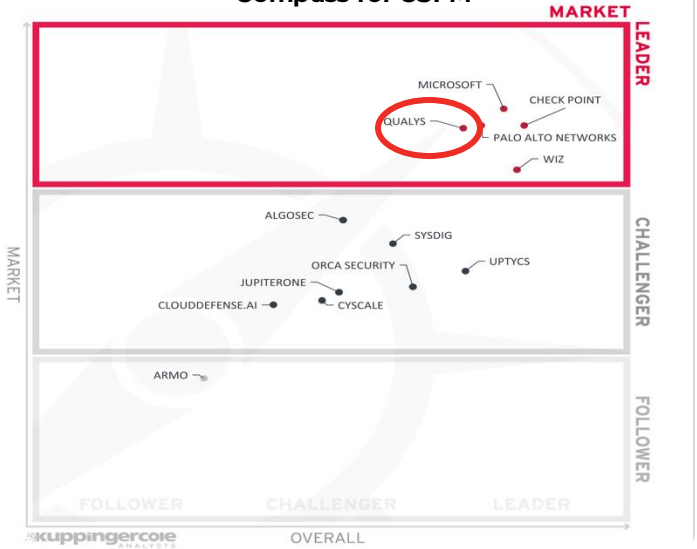
2025 Leadership
Compass for CNAPP



" 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

2024 Market Leader -
Compass for CSPM



「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

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

企業からの信頼

***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

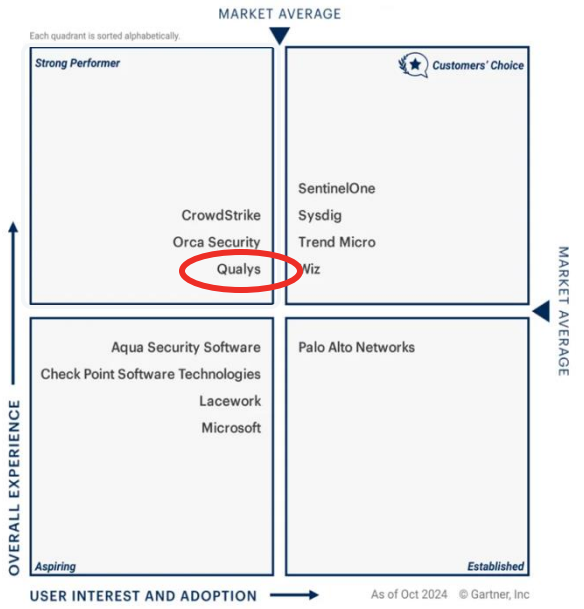
Qualys.

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

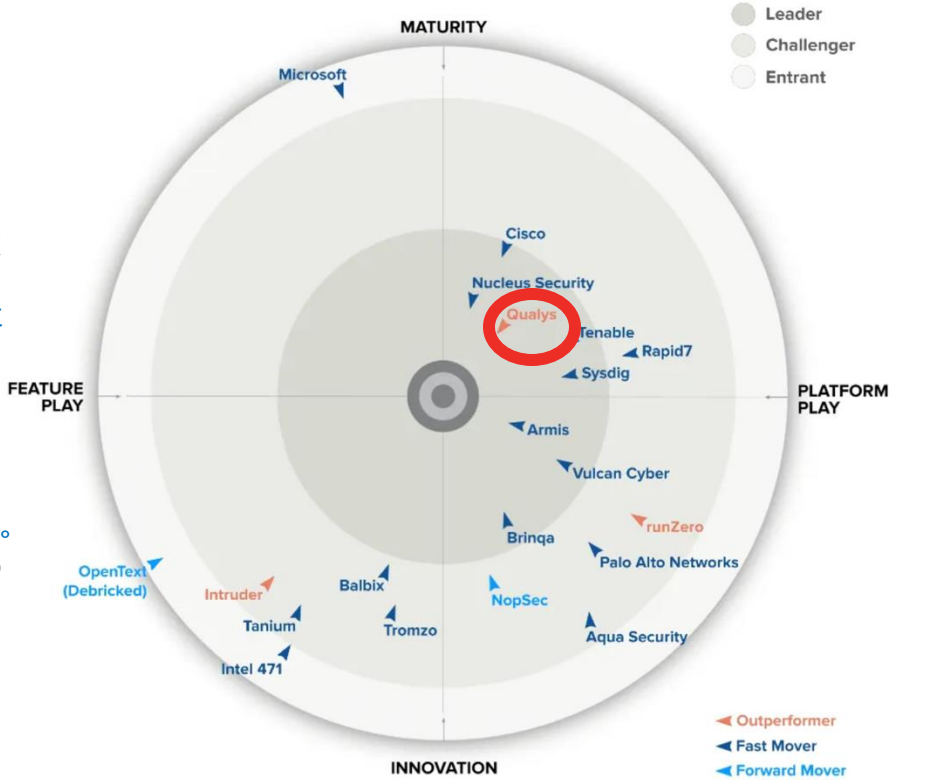
Read full review

GigaOMレーダー脆弱性管理レポート

What are we announcing?

第３回年次VMレーダーレポートで、2年連続で脆弱性管理を実装するQualys VMDRが「リーダー」としてタグ付けされました。

Qualys は、脆弱性管理の分野で定評のあるプレーヤーであり、脆弱性と構成ミスを管理するためのリスクベースのソリューションである脆弱性管理、検出、および対応 (VMDR) を提供しています。TruRisk機能を備えたVMDR 2.0への最近のアップグレードにより、プラットフォームは大幅にアップグレードされ、サイバーリスクを効果的に測定および軽減するためのさまざまな機能がSaaS提供されます。Qualys が他のすべての脆弱性管理ベンダーに対して優れていることを可能にしたこれらの差別化要因に加えて、Qualys VMDR は、ネットワーク スキャン機能、インフラストラクチャの脆弱性スキャン、AI 支援のリスク計算、エンドツーエンドのカバレッジ、相互運用性に優れた、大企業にとって「格別」としても強調されています。パッチ管理や高度な修復ソリューションを提供しないTenableやRapid7などの他の競合他社とは異なり、Qualys VMDRはエンドポイントにパッチをより効率的に展開できるため、スケーラブルなVMを必要とするだけでなく、ツールの統合を促進するのに役立ち、ほとんどの組織の労力と時間を削減します。

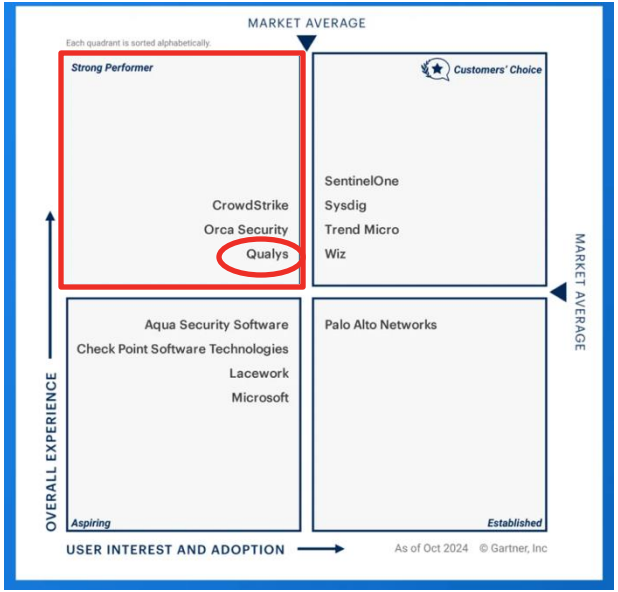


https://gigaom.com/reprint/gigaom-radar-for-continuous-vulnerability-management-237762-qualys/

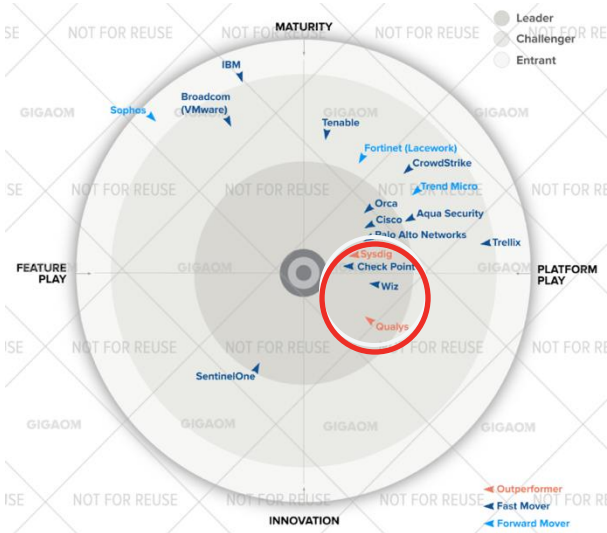
Qualys TotalCloud CNAPPのポジショニング

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.

GigaOMレーダーASMレポート

Qualys は、ASM Radar レポートの成熟度/プラットフォーム プレイ象限でリーダーおよび *Fast Mover*としての地位を獲得しました。

GigaOm は、脆弱性管理、資産検出、外部攻撃対象領域管理への統合アプローチを強調し、Qualys を**「柔軟な導入オプションを備えた包括的な資産可視性を求める組織にとって最適な市場」**と評しています。レポートでは特に、Qualys が**「詳細な資産分類とカスタマイズ可能な検出頻度を必要とする企業」**に最適であるとしています。

Qualys サイバーセキュリティ資産管理(CSAM)の優位性

1. 完全なディスカバリとインベントリ
   Qualysは攻撃対象領域全体を強力にカバーし、個々のユースケースに合わせて設計された柔軟な検出方法を用意しています。
2. リスクアセスメント
   資産の TruRisk スコア内で「100,000 を超える脆弱性シグネチャ、25 を超える脅威インテリジェンス ソース、資産の重要度、エクスポージャーメトリック、構成ミス、およびEOLステータス」がすべて考慮される、プラットフォームの差別化要因としての TruRisk™ フォーミュラに特に注目しています。

[Blog: 独立系アナリスト企業: Qualys が攻撃対象領域管理のリーダーとして認められる]

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