



Qualys Trurisk Platform ソリューション概要

Qualys Japan K.K
更新日2025年12月



目次

- What's new!
- クオリスプラットフォームの紹介
- クオリスによる資産管理
- クオリスによるリスク管理とリクス修復
- クオリスによるAppSecセキュリティ
- クオリスによるクラウドセキュリティ
- クオリスによるコンプライアンス
- クオリスによるリスクベース優先順位付け
- クオリスによるAI,LLMセキュリティ
- クオリスによるコンテナセキュリティ
- クオ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



What's New!

Enterprise TruRisk Management (ETM)のご紹介





クラウドセキュリティの未来

Qualysが描く新しいリスクオペレーション

市場背景と課題

クラウド環境の複雑化：コード、クラウド、ランタイム、SaaS、AIまで広がる攻撃面

ツールの分散と運用負荷：平均3種類以上のツールを利用、運用が複雑化

予算制約：65%以上のCISOが「予算は横ばいまたは減少」と回答

結果：脆弱性管理の難化、アラート過多、攻撃経路の見落とし

Latio Techの提言

CNAPPの限界：「万能プラットフォーム」から脱却
注力領域：

- アプリケーションセキュリティテスト
- ユニバーサル脆弱性管理
- 高度なワークロード保護

CTEM (Continuous Threat Exposure Management) への移行

Qualysのソリューション

Enterprise TruRisk Management (ETM) :

- リスクオペレーションセンター (ROC) を構築
- 脆弱性、脅威、資産価値を統合したリスクスコア

Qualys TotalCloud :

- 攻撃経路分析 (Blast Radius、ID、ランタイム)
- FlexScanによるハイブリッド環境保護
- QFlowによるクラウドネイティブ自動修復

Qualys TotalAppSec :

DAST、SCA、APIスキャンでコードからクラウドまで可視化

Qualys 導入効果

140M以上のパッチ適用実績：大規模な修復を実現

リスクをビジネス価値に変換：経営層への説明力強化

AIによる自動化：トリアージ、調査、レポート、ワークフローを効率化

世界初のクラウド型リスクオペレーションセンター

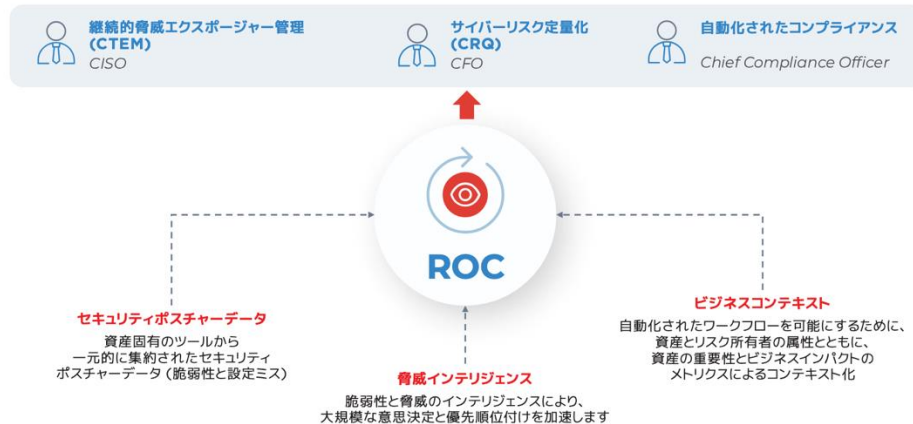
Qualysが提供する **Enterprise TruRisk™ Management (ETM)** は、セキュリティや脆弱性に関するデータを集約し、企業におけるサイバーリスクの可視化と管理を支援する クラウドベースのリスクオペレーションセンター (ROC) です。

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。



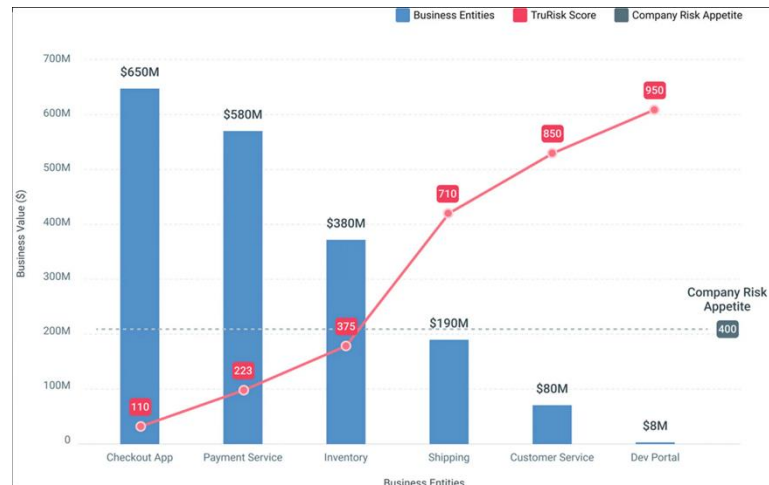
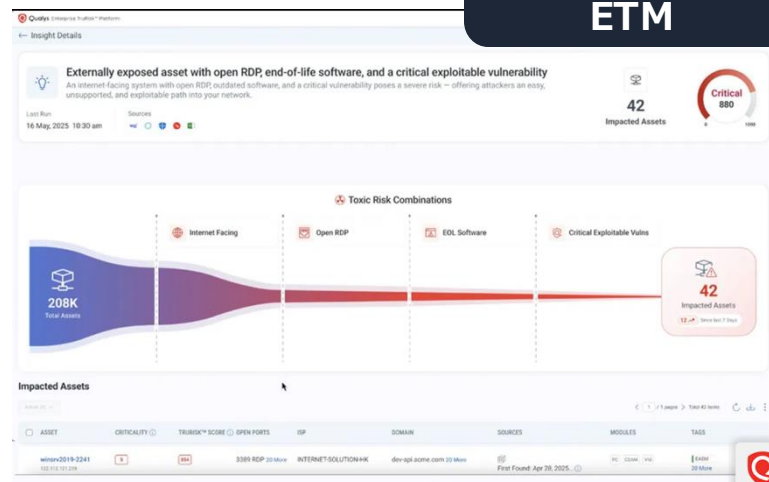
リスク オペレーション センター (ROC) の基礎



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財務上の影響度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
リスク対応の自動化	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製ツール（たとえば Microsoft Defender、Wiz、Okta など）とのリアルタイム連携により、クラウド、オンプレミス、ハイブリッド環境にまたがる多様なデータを集約



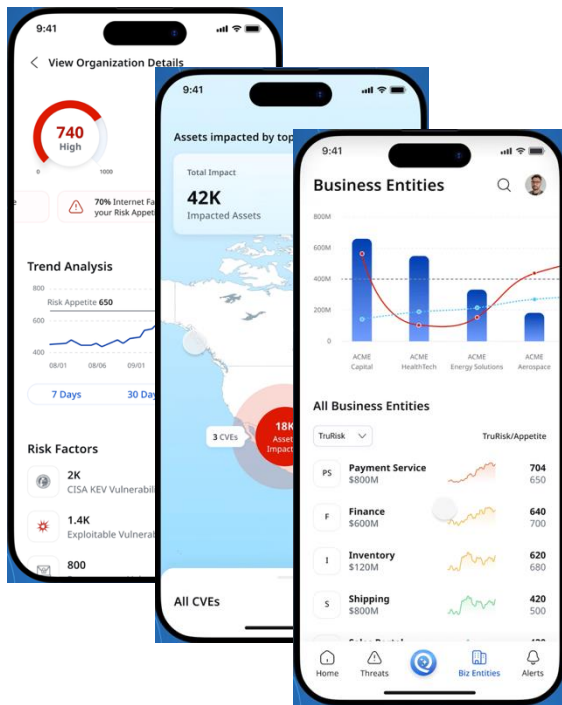


TruLens

ETMの機能としてプレビュー提供中

ETM

TruLensは、ETMプラットフォームに統合された、**業界特化型の脅威インテリジェンスとリスクコンテキストを提供する機能**です。



CISO専用モバイルアプリ

※2025年10月公開のBlogは[こちら](#)



1. 経営判断を支援する統合インテリジェンス

- グローバル脅威をビジネスインパクトに結び付けることで、単なるセキュリティ指標ではなく、経営層が理解しやすい「リスクと影響」を提示。
- 業界ベンチマークを活用し、自社のMTTR（平均復旧時間）を同業他社と比較可能。
→「当社は業界上位25%、MTTRは12日短縮」というように、取締役会や投資家に響く成果を示せる。

2. モバイルファーストでCISOを支援し、意思決定を加速

- 脅威インテリジェンスをデスクトップやSOCに閉じ込めず、経営層が必要な時と場所で利用可能とするためモバイルアプリを提供。
- 取締役会で直接表示でき、推奨修復ステップを提示し、チームに割り当てる機能で「インテリジェンスからアクションまでのループ」を短縮する。

3. リソース配分と投資判断を最適化

- TruLensは、どこに予算や人員を投入すべきかを明確化し、遅れている領域を特定。
- 「修復後の再修復」を支援し、競争力を維持。

4. コンテキストで数字を価値に変換

- 「四半期で10,000件修正」ではなく、「業界比較でランキング、重要なエクスポージャーウィンドウを競合より○日早く閉じた」というストーリーを提供。
- 取締役会・投資家・規制当局に響くレポートを簡単に生成・共有。

5. 既存ETMとのシームレス統合

- 既存のETM顧客は自動的にワークフローに統合され、追加の導入負担なし。
- Agentic AIによる迅速な修復支援で、脅威対応を加速

TruConfirm

TruConfirmは、脆弱性が実際に悪用可能かどうかを**自動で検証**し、**誤検知を減らし**
て本当に危険なものだけを優先的に対応できるようにする機能です。

TruConfirmの主な機能

①実際の悪用可能性を検証

脆弱性スコアだけでなく、環境をシミュレーションやプローブして「本当に攻撃可能か」を確認します。これにより、理論上のリスクではなく、現実的な脅威に集中できます。

②誤検知を排除し、対応を迅速化

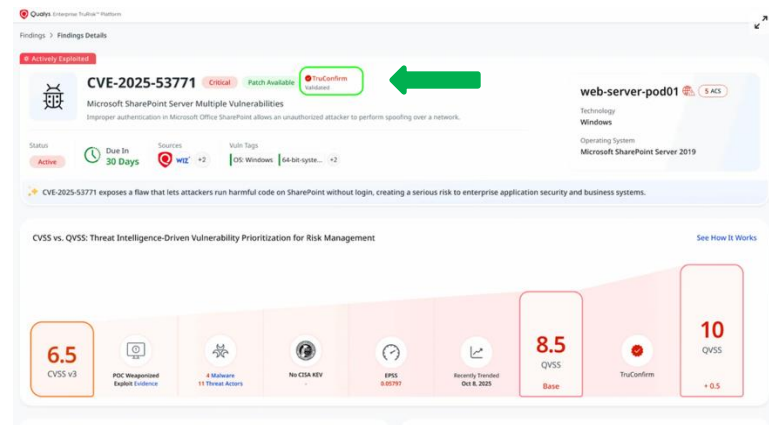
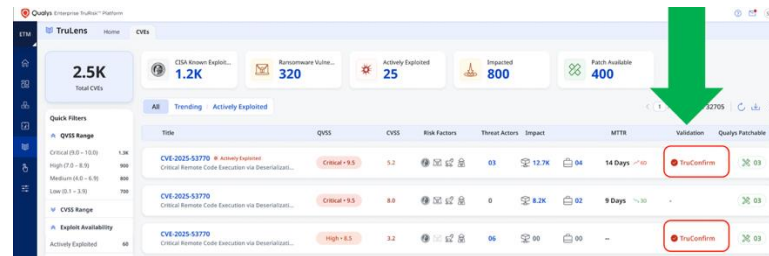
悪用可能性を確認することで、不要なアラートを減らし、対応すべき脆弱性を絞り込みます。結果として、平均修復時間（MTTR）が短縮されます。

③ETMワークフローとの統合

Enterprise TruRisk Management (ETM) の一部として、リスクスコアや修復プロセスと連携し、効率的な運用を実現します。

④セキュリティチームへの実用的な情報提供

「どの脆弱性が実際に悪用可能か」を明確に提示し、優先度付けと即時対応を支援します。



Qualys ETM Identity

Qualys ETM内に構築された**Qualys ETM Identity**は、アイデンティティセキュリティとActive Directoryの態勢を**単一の優先順位付きリスクビュー**に統合し、アイデンティティ攻撃対象領域全体にわたる**アイデンティティリスクの測定、伝達、排除**を実現



測定 AD、Entra ID、IDaaS、IdP全体にわたるアイデンティティの完全なインベントリを備えたアイデンティティ・ポスチャ



伝達 単一のTruRisk™スコアに統合されたアイデンティティリスクを評価し、対応策の優先順位付けを実現

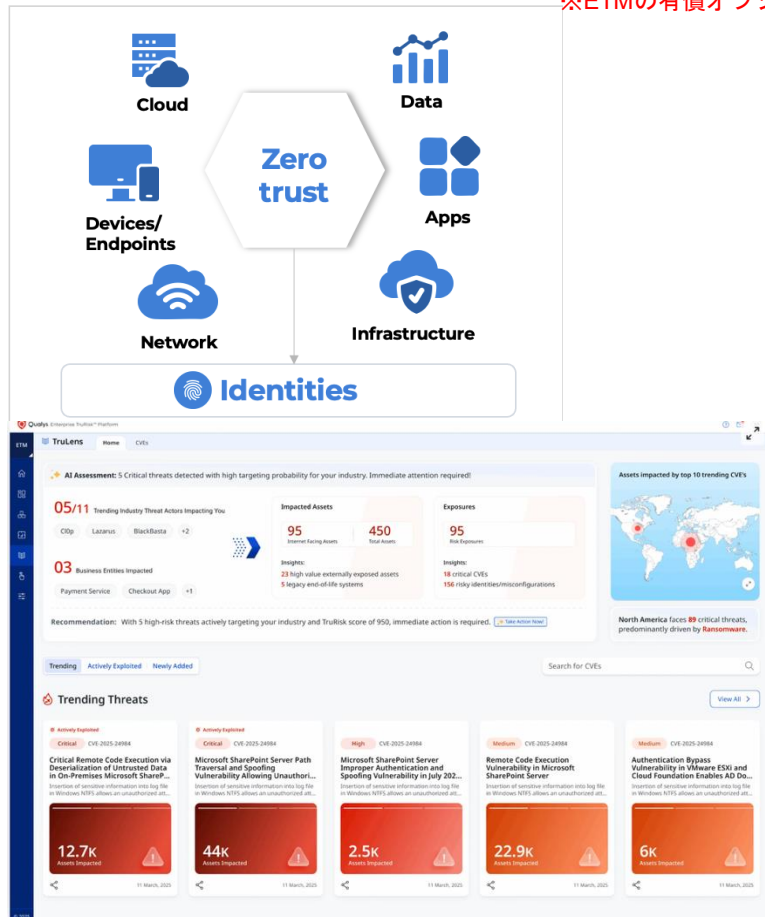


排除 ポリシー適用と自動修復による高リスク攻撃経路の防御

ETMの機能としてプレビュー提供中

ETM(Identity)

※ETMの有償オプション



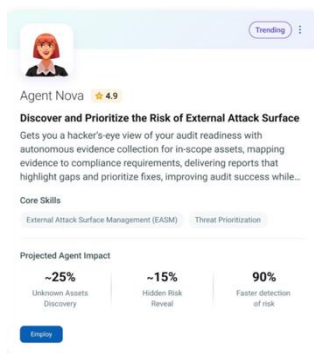
Qualys、業界初となるAgentic AI搭載リスクオペレーションセンターを発表、自律型サイバーリスク管理を実現

詳細 : [Blog](#)
[Demo Video](#)

この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、リスクポスチャーを劇的に改善し、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
- ✓ 自律的な脆弱性修正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。

Agent Saraのユースケース

利用例)

1. リスク評価の開始

- ・ ユーザーがCyber Risk Assistantにプロンプト入力（例：「最も重大な脆弱性を修正して」）。
- ・ AI Fabricが指示を解析し、関連する資産・脆弱性・ビジネスコンテキストを取得。

2. 優先順位付けとアクション計画

- ・ Agentic AIがTruRiskスコアを使って、修正すべき脆弱性をランク付け。
- ・ 修正計画を自動生成（どのパッチを適用するか、どのシステムに影響するか）。

3. 自動修正 (Remediation)

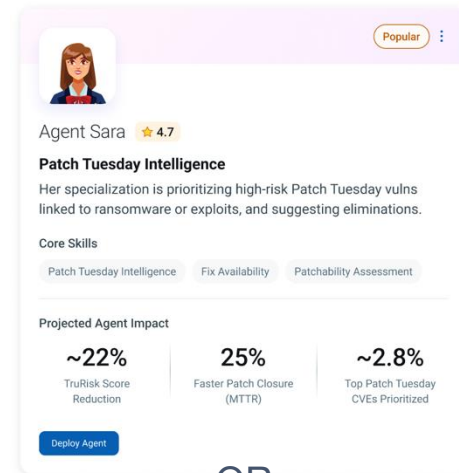
- ・ エージェントがパッチ適用や設定変更を実行。
- ・ 「Remediate the remediation」* 修正後の検証をAIが自動で行う。（計画→実行→検証→再修正）

4. 検証とレポート

- ・ 修正結果を確認し、リスクスコアを再計算。
- ・ ダッシュボードに「Before/After」比較を表示。
- ・ モバイルアプリで即時確認できる。

5. 自律的な次のアクション

- ・ AIが残存リスクを検出し、次の修正タスクを提案。
- ・ ユーザーは「承認」するだけで、AIが継続的に対応。
- ・ AI Fabricによる複数エージェントの協調動作



OR



自分だけのエージェントを作る

割り当てられたタスクを自律的に遂行できる必要なスキルを持つAIエージェントを訓練・構築する

* 「Remediate the remediation」とは？

最初に行った修正（remediation）が不完全、誤っている、または新たな問題を引き起こした場合に、その修正を再度修正すること。

主な原因：

- パッチ適用後に別の脆弱性や互換性問題が発生。
- 設定変更で予期せぬ影響が出る。
- 修正が正しく適用されなかった、または検証不足。

TruRisk2.0で進化するサイバーリスク管理

ETM(TruRisk)

※ブログは[こちら](#)

CVE標準化と新スコアリングで精度・スピード・対応範囲をETMで実現！

TruRisk 2.0の主な強化ポイント

1.脆弱性追跡をCVEベースに移行

CVEとQID両方を扱い、定量・定性ペアのアグリゲーションが可能。

2.新スコアリング手法（最大+頻度）

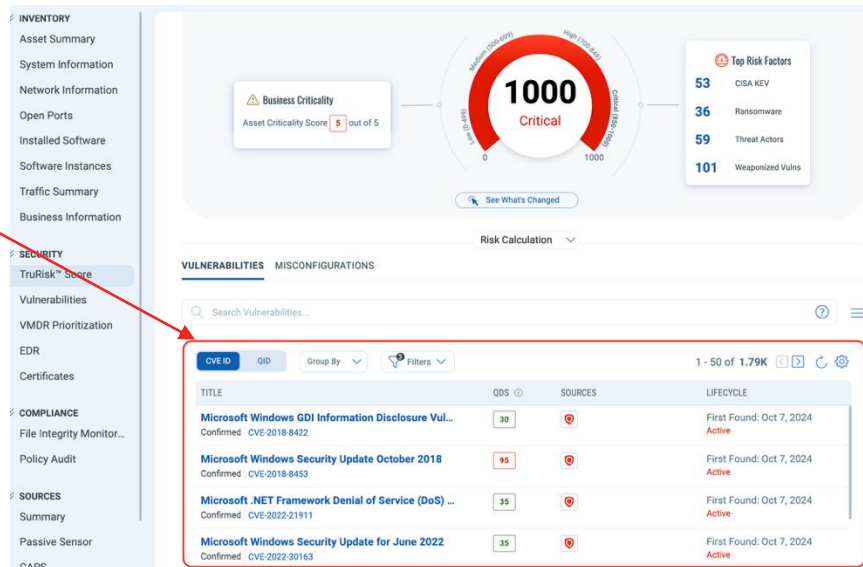
最も深刻な脆弱性と発生件数に注目。
平均値方式で起こりうる誤ったリスク感の増加を防止。

3.スコアキャッピング&動的更新

最大1000点までのスコアキャップを維持。
低・中リスクも誤ってスコアをつり上げない処置。
リスクスコアは1時間ごとにリアルタイム更新。

4.リスクファクタ対象の拡大

従来のITホストに加え、クラウドリソースやコンテナ、Webアプリ、GenAI/LLMなど、多様なリスクファクターを評価可能に。



移行プロセスとサポート体制

- ETM導入済顧客 → TruRisk 2.0に自動移行。
 - ETM未導入の既存顧客または新規顧客 → プラットフォーム内でETMを有効化すると移行可能。
- ※ご質問・ご相談は担当TAMへご連絡ください。

TruRisk1.0ではQualys Detection ID (QID) をベースに重み付けの平均値を用いたが、2.0ではCVE標準化と「最大スコア+発生件数」による新アルゴリズムを採用し、セキュリティ脅威をより正確にスコアへ反映します。
また、ETMではサードパーティからのリスクを集約するため、業界標準のCVE IDを採用致しました。



クオ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
TruRisk™

Measure (計測)

ビジネスコンテキストによる
内部および外部のインベ
ントリとリスク管理

脆弱性の検出、優先順位
付け、設定ミス

Communicate (伝達)

脆弱性や設定ミスを自動化
とインテリジェントなワーク
フローで修正

Eliminate (排除)

リスク、ビジネスコンテキスト
による脅威の監視、検出、
対応、防止

コンプライアンスの推進 業
界の規制、標準の監視、レ
ポート作成

資産管理

脆弱性と構成管理

リスクの修復

脅威検出対応

コンプライアンス



API



Lightweight Agent

Platform Services



Sensors



3rd Party Data

First-Party OSS

Applications



Operating Systems



Cloud / Containers / VMs



IT / Workstations / Servers



IOT



External Devices



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



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

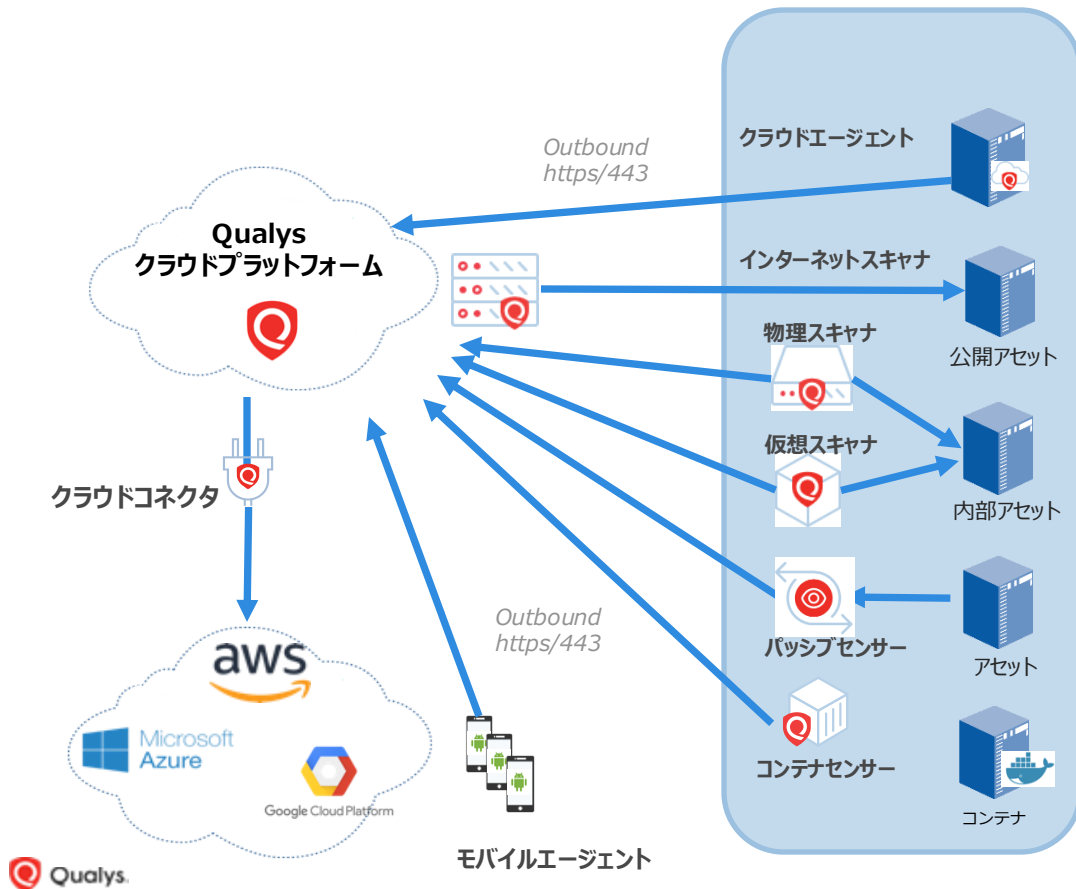
Qualys導入メリット

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/GCPI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。

クオ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

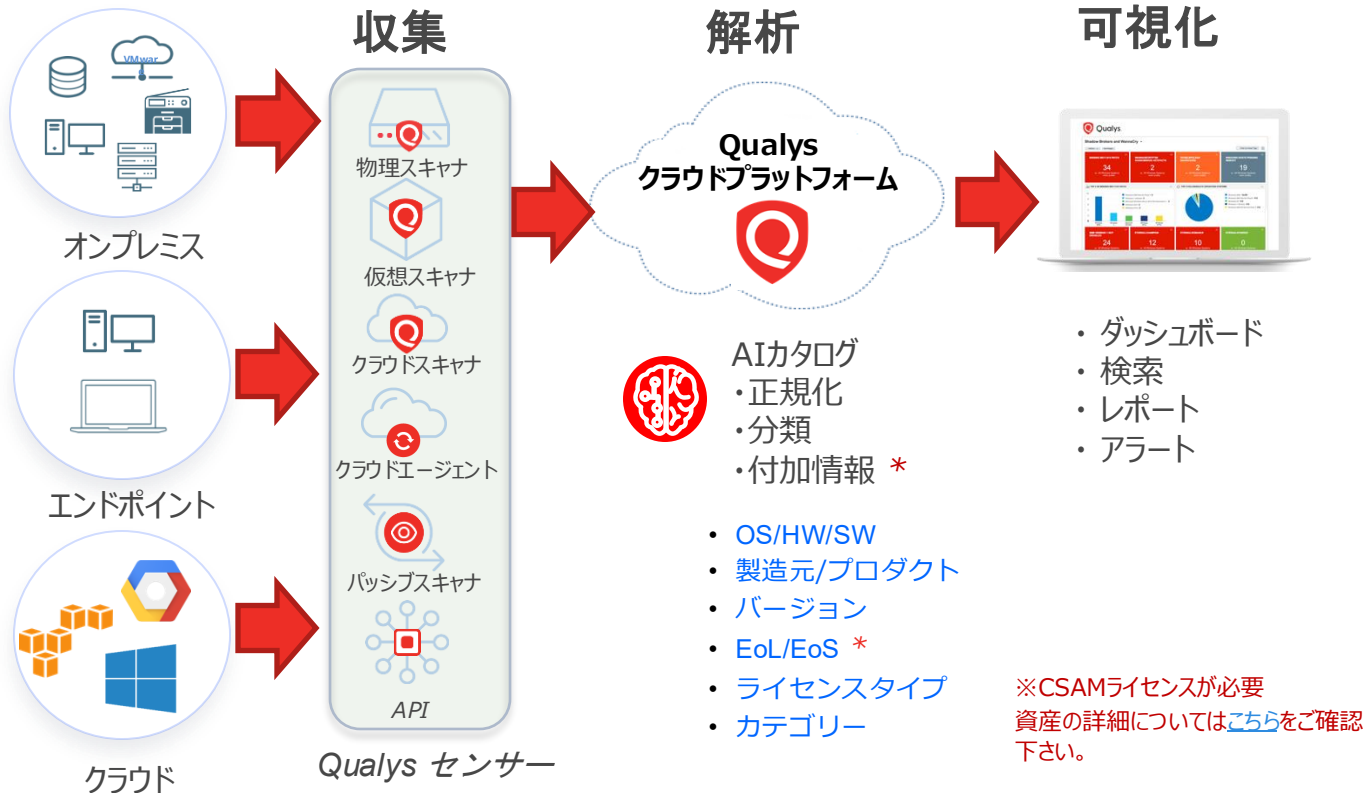
基本情報: ホスト名、IPアドレス (IPv4/IPv6)、FQDN、NetBIOS名など。
ハードウェア仕様: CPU、メモリ、ディスク容量、GPU、LPAR ID (AIX環境) など。
ネットワーク情報: MACアドレス、ネットマスク、ネットワークインターフェースの詳細。
地理的位置情報: パブリックIPに基づくアセットの地理的な位置

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。



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。

Technical Report - Host based

File View Help

- 3 WordPress Front-end Editorに任意のファイルアップロードの脆弱性 (WordPress Front-end Editor Arbitrary File Upload Vulnerability)
- 3 WordPress Front-end Editorに任意のファイルアップロードの脆弱性 (WordPress Front-end Editor Arbitrary File Upload Vulnerability)
- 3 Apache Tomcatの入力検証にセキュリティ回避の脆弱性 (Apache Tomcat Input Validation Security Bypass Vulnerability)

First Detected: 06/24/2015 at 02:30:38 PM (GMT+0900)

Last Detected: 12/01/2016 at 06:22:11 PM (GMT+0900)

Times

07/30/2015 at 11:34:47 AM (GMT+0900)

6.4

QID: 87272

CVSS Base:

CVSS Temporal:

Category: Web server

CVSS3 Temporal:

CVE ID: CVE-2014-9227

CVSS Environment:

Vendor Reference: Tomcat 6.0, Tomcat 7.0, Tomcat 8.0

Asset Group:

Bugtraq ID: 72717

Collateral Damage Potential:

Service Modified: 01/27/2016

Target Distribution:

User Modified:

Confidentiality Requirement:

Edited: No

Integrity Requirement:

PCI Vuln: Yes

Availability Requirement:

Ticket State: Open

THREAT:

Apache Tomcat は、Apache Software Foundation によって開発された、オープンソースの Web サーバおよびサーブレットコンテナです。Tomcat に、入力検証の脆弱性があります。このエラーの原因は、HTTP リクエストが正しくフィルタリングされないことにあり、ユーザがリクエストを影響を受けるバージョン:

Apache Tomcat 6.0.43, 7.0.55, 8.0.9 のいずれかより前のバージョン

IMPACT:

これらの脆弱性の悪用に成功したリモートの攻撃者は、セキュリティ制限を回避することができます。

SOLUTION:

この脆弱性が修正され、入手可能なバージョンの Apache Tomcat にアップデートしてください。

Patch:

Following are links for downloading patches to fix the vulnerabilities:

[Apache Tomcat 6.x \(英語\)](#)

[Apache Tomcat 7.x \(英語\)](#)

[Apache Tomcat 8.x \(英語\)](#)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

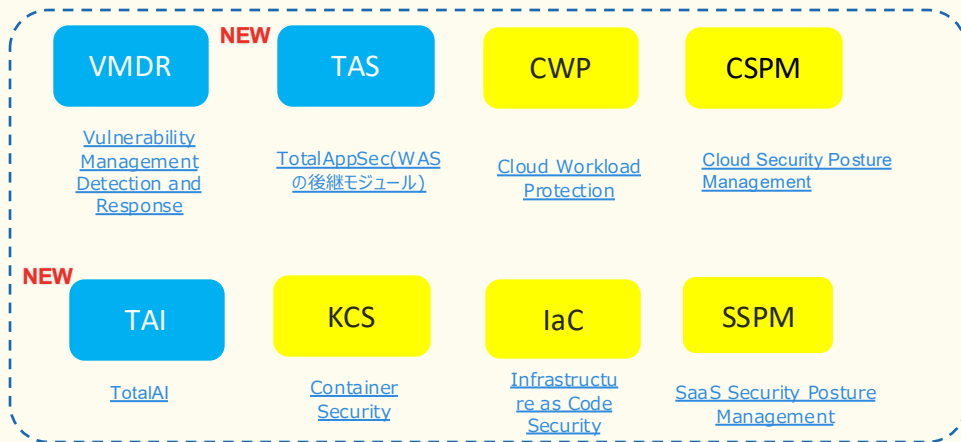
There is no malware information for this vulnerability.

RESULTS:

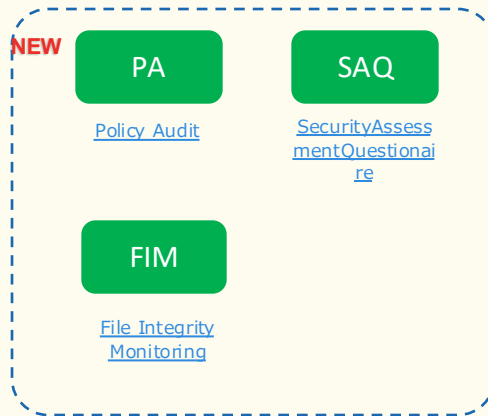
Apache Tomcat Input Validation Security Bypass Vulnerability detected on 8080 port.<title>Apache Tomcat/7.0.26 - Error report</title>

Qualysモジュール全体図

脆弱性管理&設定管理



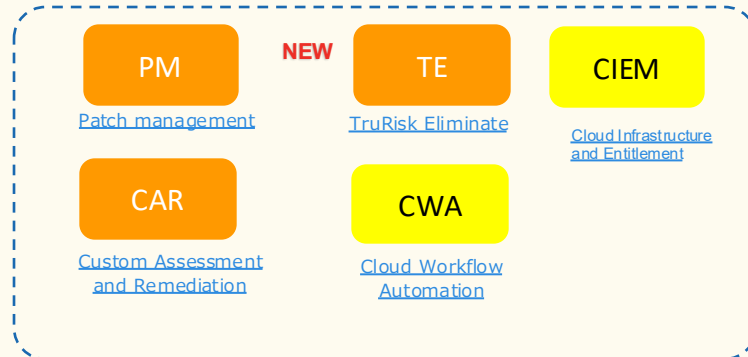
コンプライアンス



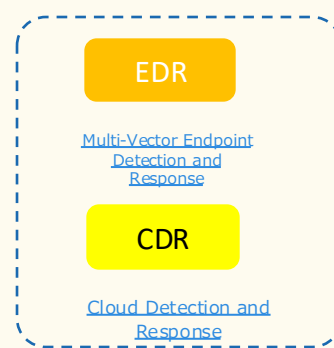
資産管理



リスクの修復

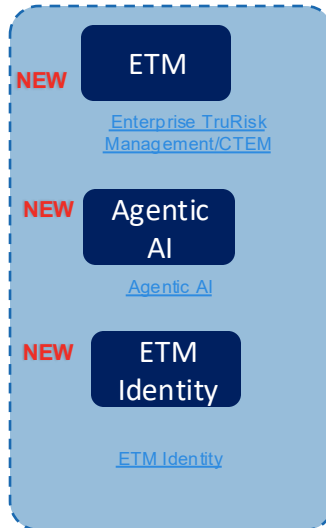


脅威の検出と応答



Update!

リスクオペレーションセンター





クオ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



※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。

内部資産

Agent, Scanner, Sensors



外部資産

Open-source Tech & Qualys Internet 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



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

リモートのための脆弱性と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



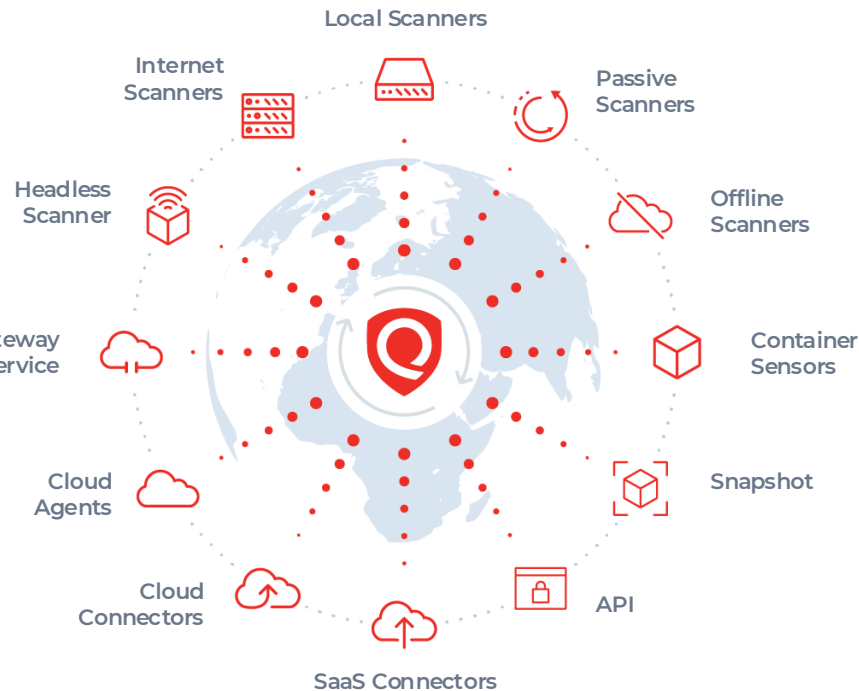
CISベンチマーク

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

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。

管理アセット

CMDB
Sync

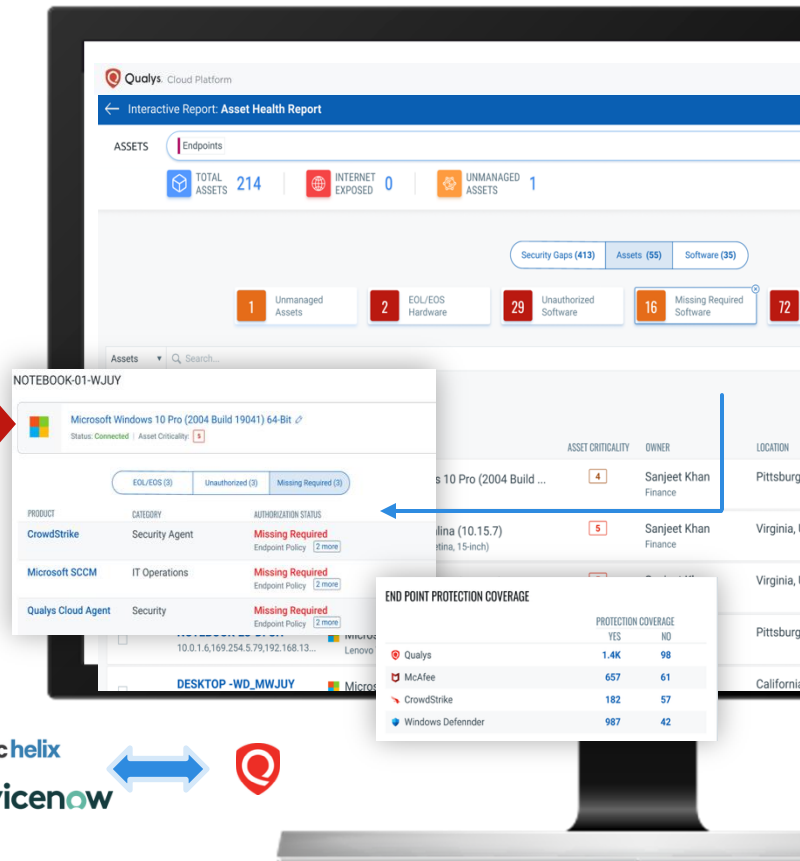
スキャナー
& クラウド
ネクター

Qualysモ
バイルアプリ

既知のアセット
未知のアセット

パッシブセンサー

サードパーティ
統合



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



高リスク

20%

重要な資産の 20% に、「高」または「重大」の脆弱性を含む EoS ソフトウェアが存在します。

48%

CISA の悪用可能な既知の脆弱性の 48% が EoL/EoS ソフトウェアおよび OS に存在します。

4x

EoS ソフトウェアに関連する脆弱性の武器化率



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。

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

外部攻撃対象領域管理(EASM)の特徴

CSAM (EASM)

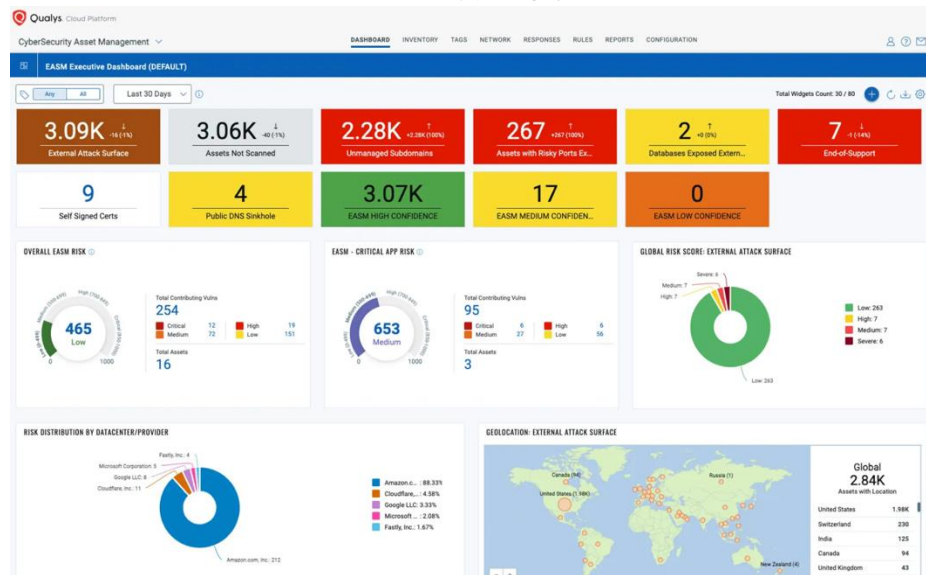
カテゴリ	機能名	説明
アセット検出	インターネット資産の自動検出	WHOIS、DNS、SSL証明書、公開リポジトリ、クラウドメタデータなどから外部資産を継続的に自動発見
アセットインベントリ	外部アセットの統合ビュー	検出されたドメイン、サブドメイン、IPアドレス、クラウド資産などを一元管理
リスク評価	脆弱性・誤設定の可視化	外部公開されたサービスやアプリケーションの脆弱性・設定ミス（例：未承認のソフトウェア、有効期限切れSSL/TLS証明書など）を検出
ブランド保護	なりすまし・フィッシング監視	自社ブランドやドメインを悪用した偽サイトや類似ドメインの発見
脅威インテリジェンス連携	攻撃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: qualys.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**

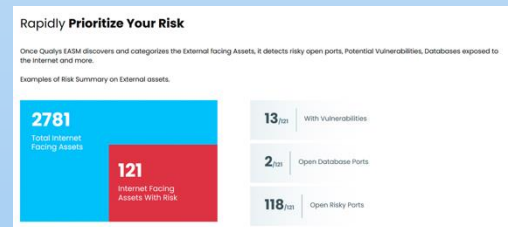
類似ドメインの検出 → **ドメインの買収・差し止め対応**

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



Top Risky Domains			Top Risky Subdomains		
ASSET DOMAIN	ORGANIZATION NAME	ASSET COUNT	ASSET SUBDOMAIN	ORGANIZATION NAME	ASSET COUNT
		4			5
		4			5
		4			5
		4			5
		4			5
		3			5



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。

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 （パ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

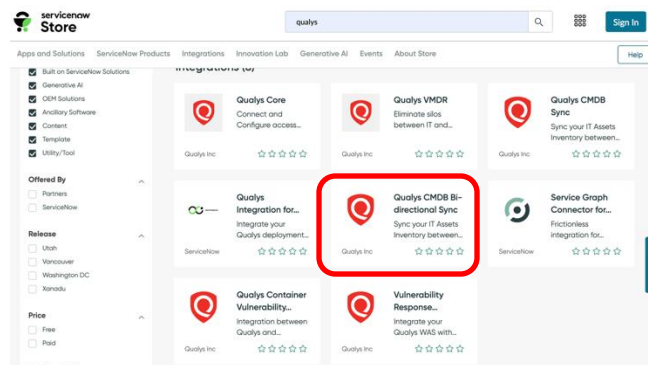
Qualys×ServiceNow連携で資産管理をスマートに自動化！

CSAM(SNOW)

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。

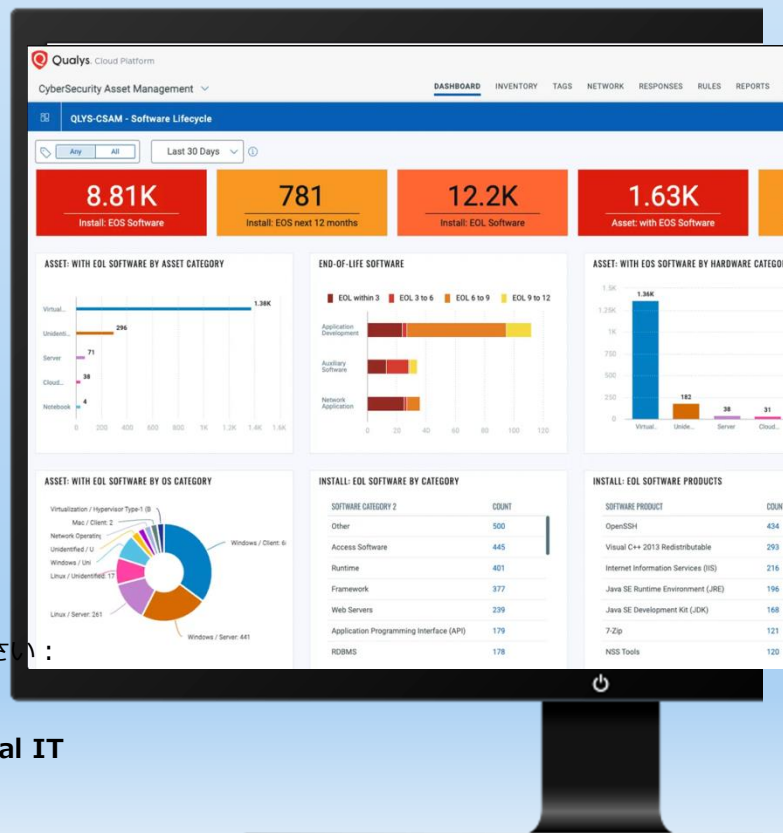
コスト最適化：**延長サポート費用の削減**や、**不要な資産の整理**に貢献。

※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。





クオリスによるリスク管理とリスク修復

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。



脆弱性のリスクに素早く対応

Eliminate

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。

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](#)

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

Eliminate機能概要



Eliminate

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

PM

OSパッチ

3rd パーティ
パッチ

ゼロタッチ
オートメーション

リスクベース
オートメーション

SCCM/Intune
との統合

カスタム
Mitigation (緩和策)
)/Remediation (修復)

Mitigate
(緩和策)

Remote
Shell

TRE

Cloud
Remediation
(クラウド
上の修正)

ServiceNow
や
ServiceNow
VRとの統合

古いバージョンの
ソフトウェアの発見と削除(java)

パッチがない場合の修復

面倒な脆弱性を
解決するライブ
リ

パッチ適用とコン
フィグの変更

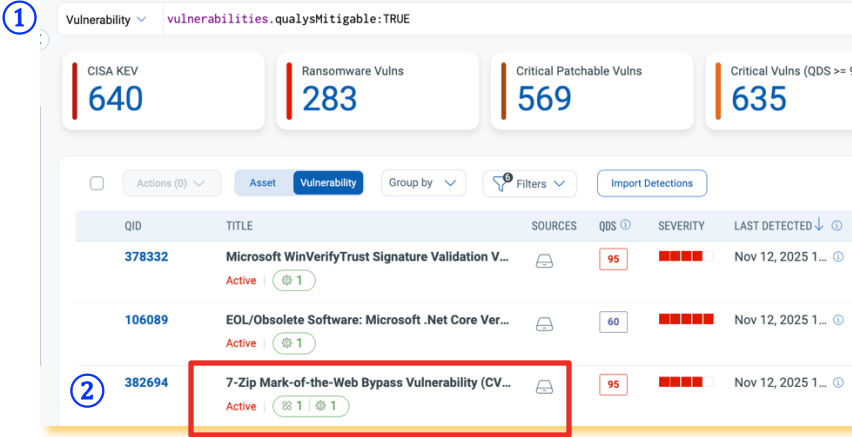
Isolate
(隔離)

ソフトウェアのイ
ンストールとアン
インストール

TruRisk Eliminate UIの紹介

緩和策とは、悪用されるリスクを軽減または排除するために講じられる措置を指します。

Eliminate



Elimination Details

Take action when vulnerabilities are detected in your environment. Vulnerabilities can be removed entirely from the environment to ensure they cannot be exploited or mitigated to an acceptable level.



Elimination Details

Take action when vulnerabilities are detected in your environment. Vulnerabilities can be removed entirely from the environment to ensure they cannot be exploited or mitigated to an acceptable level.



① Vulnerability `vulnerabilities.qualysMitigable:TRUE`

軽減できる脆弱性を検索するには、軽減に関連するQQLクエリを使用できます。



マウスをホバーすると、RemediationとMitigationの候補数が表示されます。

④

緩和策はCVE単位で案内されます。お客様の環境や状況に最も合う対策を選定できます。

Partially Applied Mitigations
Mitigations have not been applied to all CVEs.

MITIGATION TITLE	DESCRIPTION	CVE/QID ASSOCIATED	STATUS
Stop Service	This script terminates and d...	CVE-2025-29841	Pending Mitigation
Registry Update - Block RDP	Disable Windows Remote De...	CVE-2025-29831	Mitigated
Enforce App Hardening	This PowerShell script provid...	CVE-2025-30397	Pending Mitigation
Enforce System Hardening	This mitigation enables Netw...	CVE-2025-30394	Mitigated
Registry Update - Block RDP	Disable Windows Remote De...	CVE-2025-30394	Pending Mitigation
Enforce System Hardening	The provided mitigation scrip...	CVE-2025-32706	Pending Mitigation
Enforce System Hardening	This mitigation enables Netw...	CVE-2025-26677	Mitigated

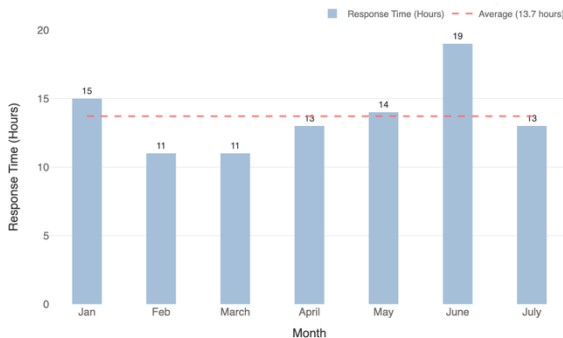
Close

軽減方法の情報は、「軽減オプション」に基づく優先順位付けに活用できます。例えば、パッチがすぐに利用できない場合は、ファイアウォールルールやサービスの無効化などの回避策を適用してリスクを軽減できます。重大なCVEにまだパッチがリリースされていないものの、ベンダーがServer Message Block v1の無効化を推奨している場合は、恒久的な修正を待つ間、迅速にリスクを軽減できます。

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。



2025 Microsoft Patch Tuesday: Response Time

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。

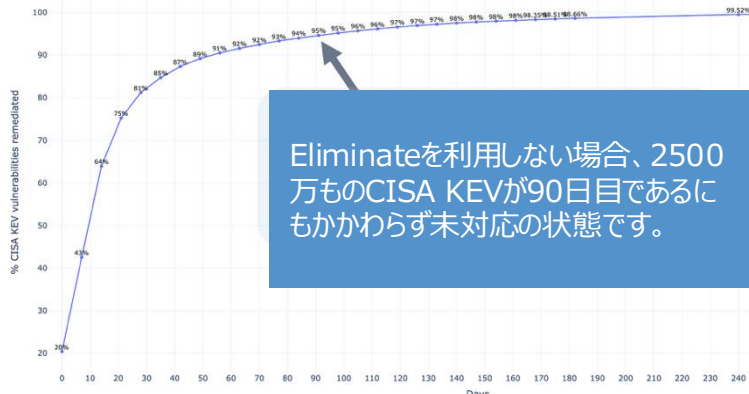
Qualys は業界をリードする CISA KEV カバレッジを持っています

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。

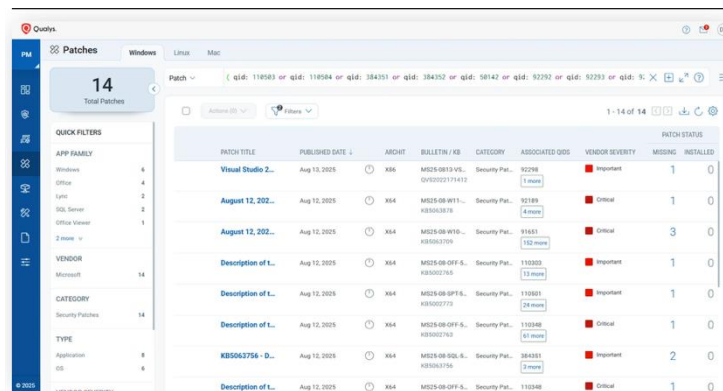
CISA KEV: TruRisk Eliminate: パッチ不可能な CISA KEV を分離、軽減、修復します



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](#)





UPDATED!

クオリスによる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。



既知および未知のウェブ資産の統合資産インベントリ

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

サードパーティインポート

Swagger, Postman, Burp Suites

API Gateways

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

トラフィック解析

トラフィック解析でAPIを発見

AI と API の発見

DiscovererのSwaggerファイル、
API呼び出し、ウェブアプリスキャン
中のAI使用状況

ウェブアプリおよびAPI 攻撃面の発見

広範囲な攻撃面の発見
既知 + 未知/忘れられた
資産

インターネット露出と内部

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

マルチクラウド環境

AWS、GCP、Azure 環境からウエ
ブアプリケーションを発見

ソースコード

ソースコードからAPIを発見する



APIスキャンによるリスク評価

さらに、必要に応じてAIリスク評価を行う能力も備えています

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

~600

QIDs for APIs

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

100%

Coverage

OWASPのAPIトップ10

5000+

API Endpoints tested

ローンチから最初の数四半期以内に

API Risk ①



Total Contributing Vulns

770

Critical 0
Medium 546
High
Low

Total Webapps

0

Total APIs

11

OWASP API Top 10 for Internet Exposed APIs

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

ウェブアプリスキャンとマルウェア検出によるリスク評価

さらに、必要に応じてAIリスク評価を行う能力も備えています

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

AI-Powered Scan Optimization New

Select the checkbox to enable AI-powered scan optimization. Once enabled, Qualys AI profiles your web application and optimizes the detection scope to reduce the scan time while maintaining comprehensive security coverage.

[Learn more](#)

Note: When this option is selected, the detection scope defined in the option profile is not considered.

☐ AI-Powered Scan Optimization

4600+

customers

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

~3300

QIDs for web apps

OWASPトップ10および機密データ漏洩チェックを含むQIDの数

~99%

Accuracy

ディープラーニングによるウェブマルウェア検出と監視の正確度

OWASP Top 10 vulnerabilities (in Web Apps)

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

統合ワークフローによるリスクレスポンスオーケストレーション



優先順位付けの自動化

優先順位付け

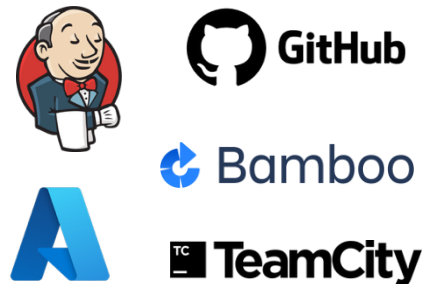
事業資産のコンテキスト
脆弱性検出と相関した脅威コンテキスト



トリアージの自動化

自動チケット作成

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



再テストの自動化

自動化されたセキュリティ検査

展開前にスキャン結果に基づく合格・不合格基準で。

Manage risk with Roc



統合資産
インベントリ

リスク要因の集約

脅威インテリジェンス

ビジネスコンテキスト

リスク優先順位付け

リスクレスポンス・オー
ケストレーション

TotalAppSecへのアップグレード

TAS

新しい機能をフル活用する

ウェブアプリケーションセキュリティ検査

ウェブマルウェア検出

WAS



発見とインベントリ

広範なAPIセキュリティ検査

高度スキャン
AI駆動のスキャン
カスタムQID

リスクオーケストレーションとレスポンス



TAS

API Vulns By Category



Total Contributing Vulns

770

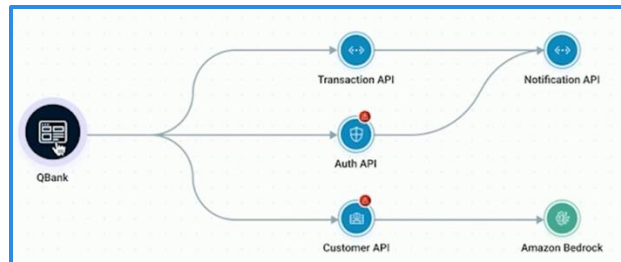
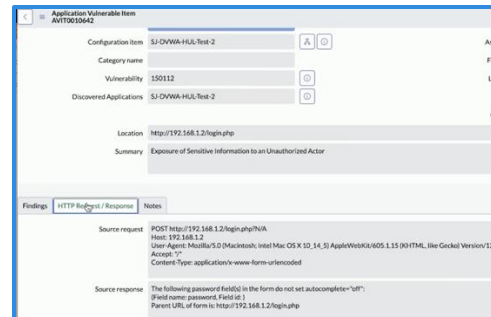
Critical 0
Medium 546

Total Webapps

0

High Risk API

APPLICATION NAME	TRURISK™ SCORE ↓	VULNERABILITY COUNT
Corp Demo - External API - ...	365	424
UAT_API_Collection	336	63
vuln-bank	333	117
API_Collection_2	330	57
VMAPI	325	45
PS_NOAPIKEY	318	6



Qualys TotalAppSec 2.4

※リリースノートは[こちら](#)

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

主な新機能（TotalAppSec 2.4）

1. APIセキュリティの強化

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

2. AIによるマルウェア検出

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

3. クラウド環境との統合

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

こんな企業様におすすめ！

APIの利用が増加し、セキュリティ管理が複雑化している企業

クラウドネイティブなアプリケーションを多数運用し、セキュリティ統制が求められる企業

開発と運用の連携を強化し、セキュリティを開発プロセスに組み込みたい企業

コンプライアンス対応を強化し、規制遵守を徹底したい企業

チケットによるタスクの管理や自動修復機能を活用して運用を効率化したい企業

導入メリット！

攻撃対象領域の可視化：隠れたWebアプリや非文書化APIの自動検出によって、脆弱性スキャンの対象が漏れません

運用の透明性・信頼性向上：コネクタ運用ログの記録機能により連携の不具合を即時把握可能

認証付きアプリの精度向上：失敗時の自動リトライ機能でスキャンの成功率が向上

TotalAppSec:攻撃面の把握からリスク管理へ進化

→ ノイズやコスト、時間を削減するためにリスク管理を自動化

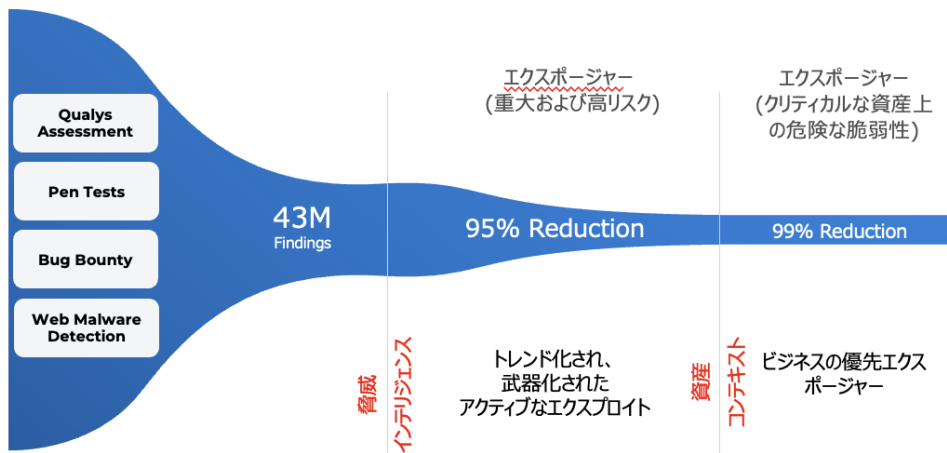
アプリケーションの全攻撃
対象を可視化

包括的発見:

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

456K
Assets

多角的なコンテキストでリスクを評価し優先順位付け



統合的修復対応

リスクへのリアルタイム
自動化対応:

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

1000+

組織はローンチから1年以内に私たちに信頼してくれました

4.4*/5

Gartner
Peer Insights™

4*/5

PeerSpot

AI時代におけるアプリケーションセキュリティの重要性

背景

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



AI時代のアプリケーションはAPIがネットワーク化し、セキュリティポスチャの把握が困難になっています。

TotalAppSecは、攻撃対象領域からリスク対象領域へ視点を転換し、ノイズ・コスト・時間を削減します。

ASPMを次のレベルへ進化させるための統合プラットフォームを提供します。

ROCによるリスク管理

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

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

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

2026年度リリース予定！

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

Manage risk with ROC



統合資産
インベントリ

リスク要因の集約

脅威インテリジェンス

ビジネスコンテキスト

リスク優先順位付け

リスクレスポンス・オー
ケストレーション

Agentic AIでAppSecをスケールアップしましょう

サイバーリスクアシスタント

会話型AIインターフェース



自然言語クエリインターフェースで AppSecプログラムを管理

ウェブアプリを全部見せてください

全てのウェブアプリの結果を見せてください

トップの有害な組み合わせを見せてください

サイバーリスクエージェント

繰り返されるワークフローのための
デジタルコラボレーター



エージェント型AI搭載のヘルスチェック

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

最適かつ包括的なテストのために**設定変更を推奨します**

ASPM – アプリケーションセキュリティ

TAS(ASPM)

2026年リリース予定

包括的な 発見 & インベントリ

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

リスクの測定と優先順位付け

Enterprise TruRisk™ Platform



Web Apps



APIs



Web Malware

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



Prioritize with
TruRisk™

リスク・オーケストレーション および修復



基盤となるインフラの自動
パッチ適用



サーバー、APIエンドポイント、
ホストの分離



ウェブアプリおよび
APIの緩和手法



DevOpsとITSM統合に
よる修復ワークフロー

顧客成果

360°視界

アプリセキュリティ・ポスチャーマネジメント

リスク優先順位付け

リスク修復



クオ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。

*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



課題

解決アプローチ

マルチクラウド環境での資産の可視化が困難

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

クラウド構成ミス（misconfiguration）によるリスク増加

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

クラウド上の脆弱性やマルウェアを管理しきれない

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

サーバーレスやKubernetesのセキュリティ対策が遅れている

保護領域	主なセキュリティ対策	ユースケース
Kubernetes	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	・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
コンテナ実行時	ランタイム監視、脆弱性検知、ポリシー適用	・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
サーバーレス	構成監査、脆弱性検知（間接的）	・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

クラウドリソースのリスクを経営層に説明しづらい

TruRiskスコアによるリスクの定量化とレポートニングに対応

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	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 CNAPP

Cloud Workflow Automation (CWA)

- ・ カスタムコントロール
- ・ 自動修復

SaaS Security Posture Management (SSPM)

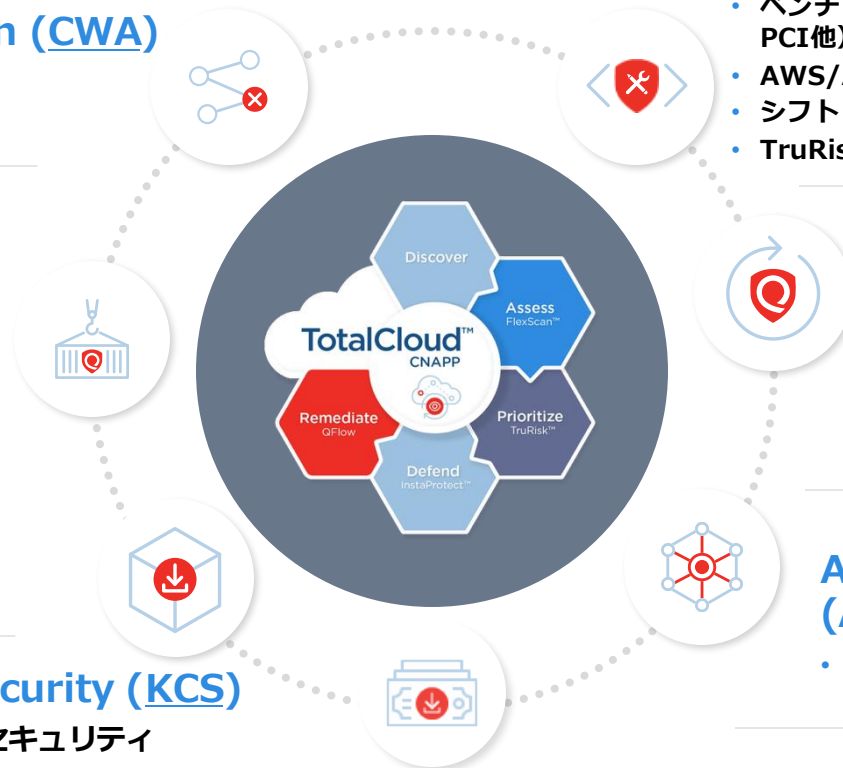
- ・ SaaSアプリの保護
- ・ コンプライアンス

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 スキャン
- ・ 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

優先順位付け : TruRisk Insights

- 資産レベルリスクスコア
- 脅威インテリジェンスによる完全な360度コンテキスト

TruRisk
Score

- 多くのソースからの信号を関連付け
- 有害な組み合わせ

TruRisk
Insight

- 攻撃経路の露出を視覚化
- 攻撃による影響度を解析

Attack
Path

Cloud Workloads
Scanned

2M

Risky Exposures

500k



VMDR Score

Business Critical

30k



TruRisk Score

With Attack Paths

300



TruRisk Insights

最重要課題に焦点を絞る

1 Month

TruRisk Insightsによる多次元的なリスク優先順位付け ノイズをカットし、ビジネスコンテキストを強調

様々な要因

- インターネットへの露出
- 脆弱性
- アクティブな脅威
- 設定ミス
- アクセス権限

TruRiskインサイト

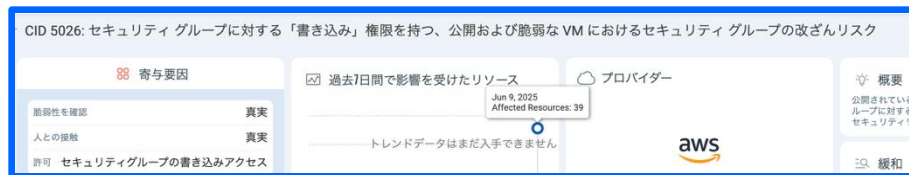
- データベースに対する書き込みアクセス権を持つパブリック VM
- IAMアーティファクトを作成する権限を持つパブリック VM (ユーザー、グループ、ロール)
- AWS KMS の破壊的なアクセス許可を持つパブリック VM の重大な悪用可能な脆弱性
- IAMアーティファクト(ユーザー、グループ、ロール)を作成する権限を持つパブリック VM

TruRisk
Insights

TruRisk Insightsは、リスクの優先順位付けされた単一のビューを提供します

TotalCloud Attack Path

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](#)



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

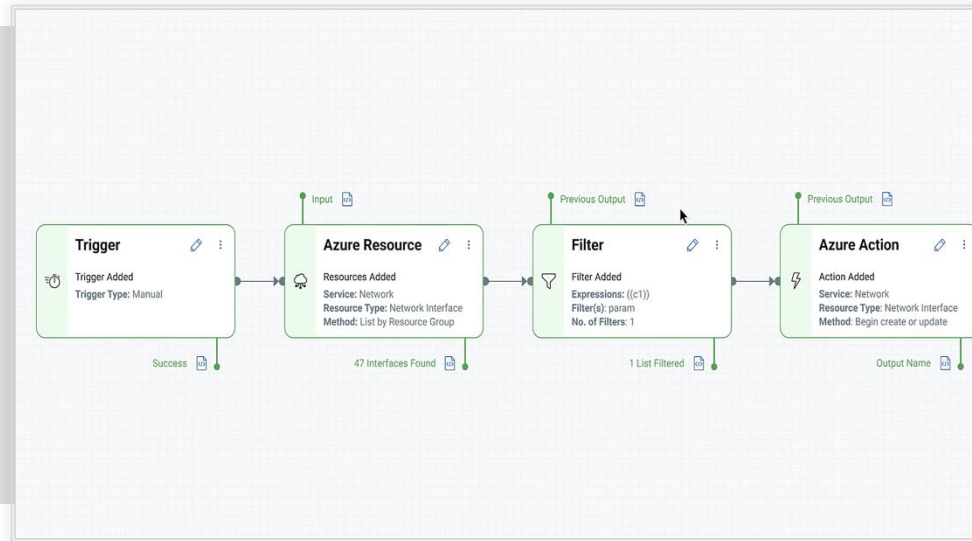
組織の要件に合わせて柔軟に調整。

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**。

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。

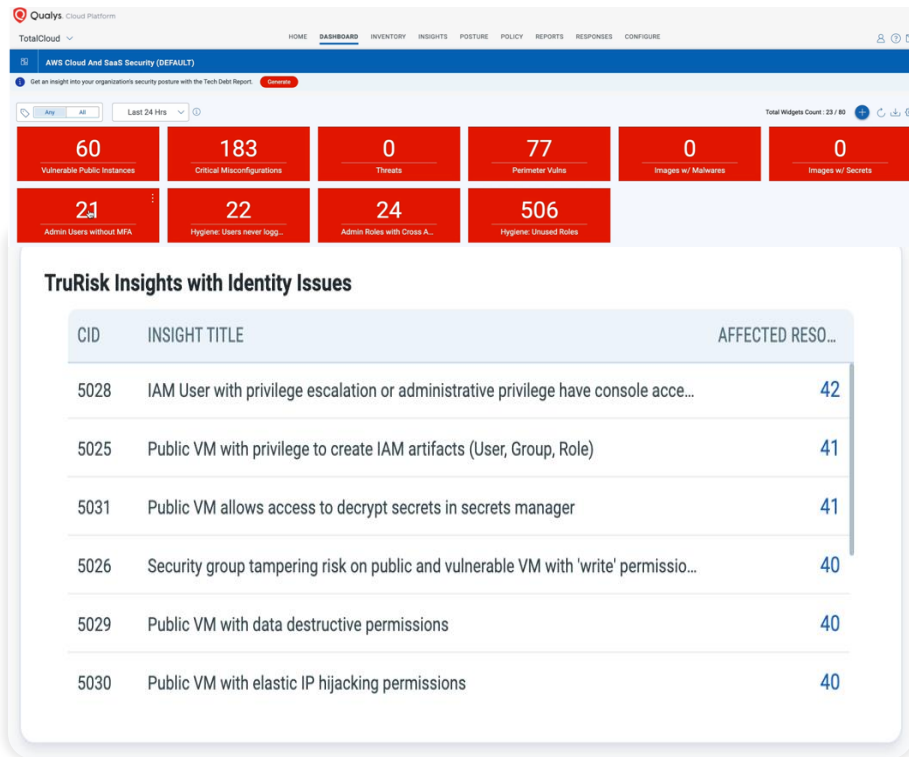


リスクのあるアイデンティティの特定

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

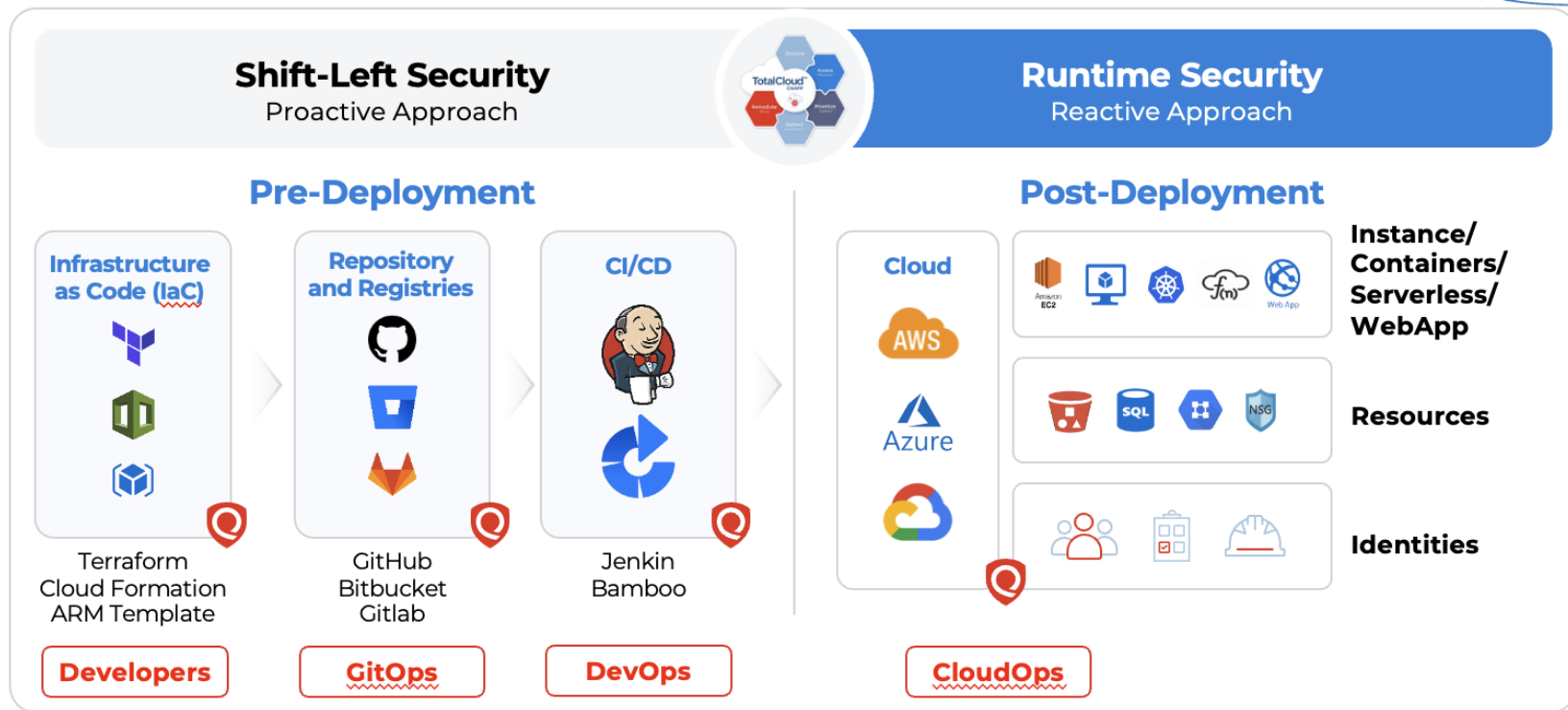
リスクのあるアイデンティティをTruRisk スコアに組み込み、優先度付けを強化。



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。



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

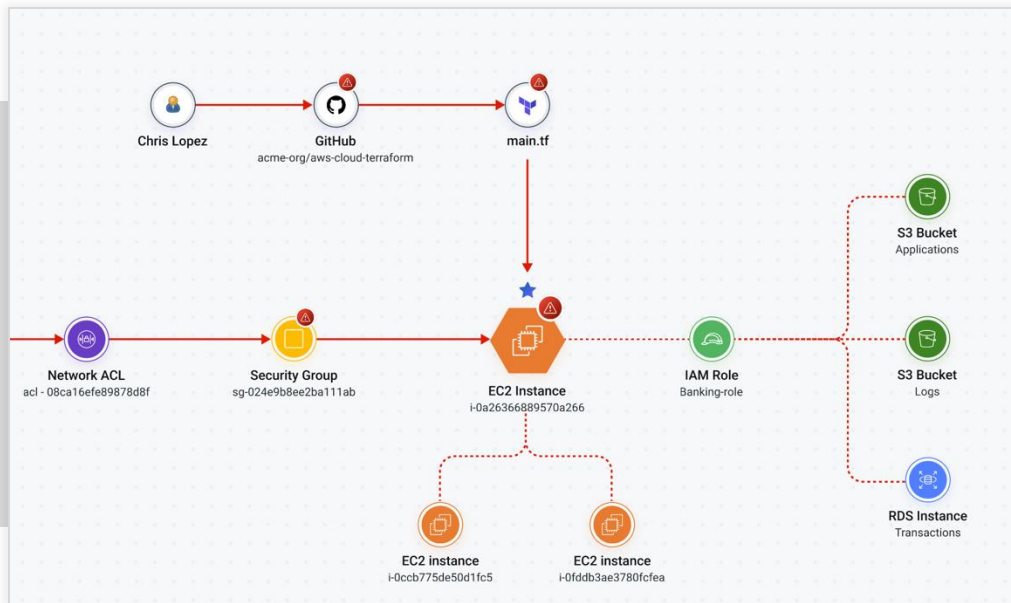
Shift Left and Fix Left を実現することで、クラウドリスクをコードレベルで迅速に解決し、セキュリティ対応を開発プロセスに組み込む。



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

[← Blog Home](#)

How Agentic AI Helps with Adaptive Cloud Risk Assessment with Agent Vikram



Kunal Modasiya, Senior Vice President, Product Management, GTM and Growth
August 19, 2025 - 4 min read



In fast-moving cloud environments like AWS, security teams face an uncomfortable truth: not every EC2 instance is being scanned, existing tools don't work across a diverse environment that includes long-lived and ephemeral assets, and visibility is never complete. [Qualys research](#) found that over 30% of virtual machines have high or critical vulnerabilities, and with blind spots in your scanning, you may miss these critical risks.

Cloud Blind Spots Are Everywhere

The reason not all instances are being scanned is workloads:

- Are missing agents
- Lack SSM integration
- Have encrypted volumes
- Are so ephemeral that they spin up and disappear before traditional tools can catch them



Reliable

Agent Vikram ★ 5

Agent Vikramの役割：

QualysのAIエージェントとして、TotalCloudの機能を自動化し、ユーザーに対してデモや操作支援を提供。

特徴：

クラウドセキュリティ管理の効率化
ユーザーの要求に応じたデモ実行
自律的なリスク検出・修正のサポート

Projected Agent Impact

100%

Visibility into Cloud Assets

6 Mins

To Define Flexible Scan Strategies in Cloud

22%

Less Cyber Risk in Cloud

Employ

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。



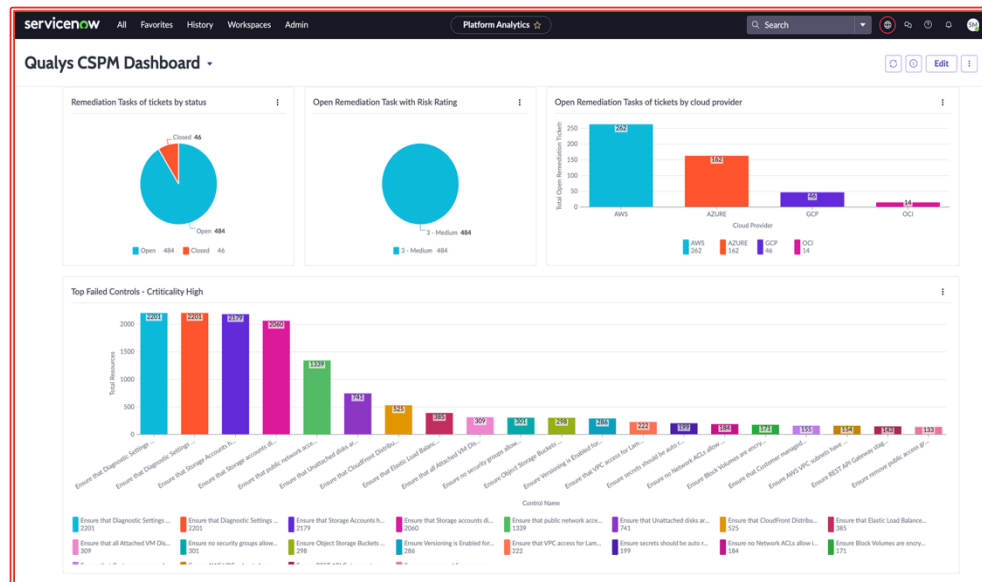
自動化された脆弱性割り当て
資産所有者に基づいて、修正タスクを開発者へ自動的に割り当て。



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



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



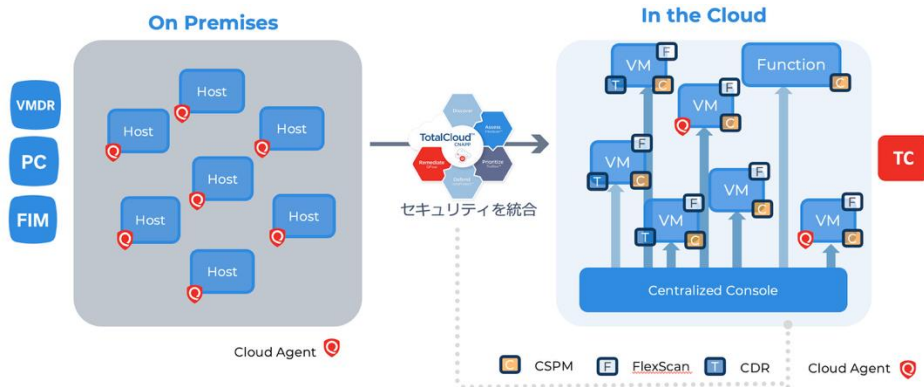
100%インベントリと
リソースタイプカバレッジ



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

AWS	Azure	GCP	OCI
 Directory Service  KMS  S3  EBS  IAM  Route 53  Record	 Log Analytics Workspace  WAF Web Protection  Frontdoor  Secret  Key Vault  Front Door	 Networks  Sub Networks  Storage  Disk Snapshots  Firewall Rules  Disk Images	 Security List  Key  Big Data Service Clusters  API Application  API Gateway  Functions Applications
 Network ACL  VPC Endpoint  Lambda Function  EBS  IAM  MQ Broker	 Storage Container  Data Explorer Cluster  Data Factory  Container Registry  SQL Server  SQL Server Database	 Cloud Armor  Cloud DNS  Cloud Functions  Cloud SQL  CloudRun Services  Spanner  Cloud SQL	 Boot Volume  Bucket  Block Volume  DB Systems  Compute Instance  IAM User
 Transit Gateway  Elasticsearch  ES Domain  Memcached	 Virtual WAN  Cognitive Search  Data Lake  Synapse Workspace  API Management Service  Disk Access	 BigTable Instance Cluster  Service Account  Cryptographic Key  PubSub  Artifact Registry  Datastore	 Load Balancer  Autonomous Database  File System  Kubernetes Cluster  Block Volume Backup  Mount Targets
 Neptune DB Instance  Neptune DB Instance  Dynamo DB Table  RDS  EC2 Images			

- ・ 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

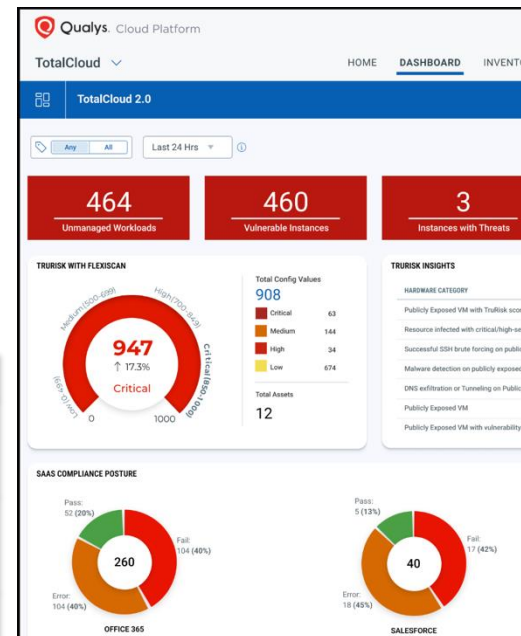


**一歩先を行く
統合リスク可視化・自動
修復ソリューション**

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、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。

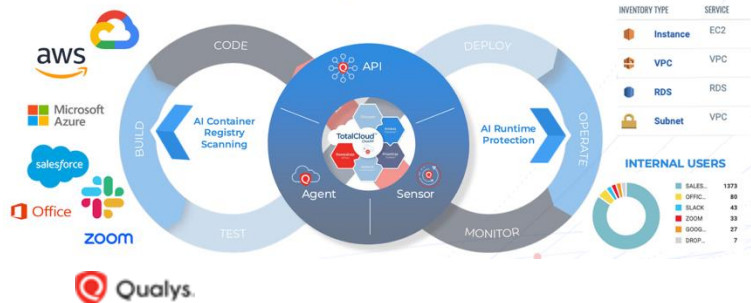
※各プレックススキャンを利用するための前提条件は[こちら](#)をご確認下さい。

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、監査対応レポートを生成

Comprehensive Inventory Functions Users, Resources and SaaS Applications



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。



クオ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

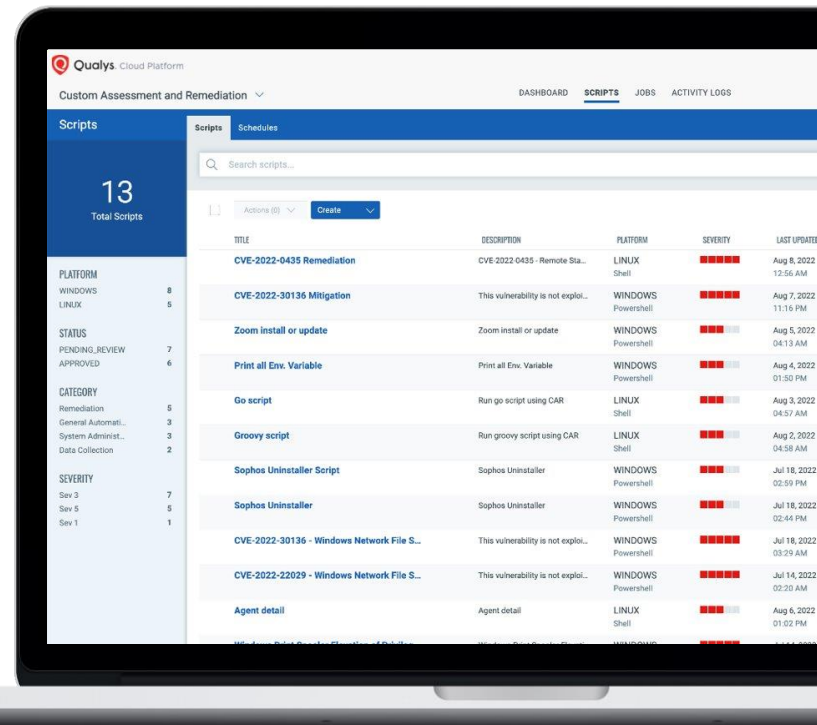
定期的な手動監査やチェックの工数を大幅に削減でき、効率的なコンプライアンス管理が実現します。これにより、監査対応やレポート作成の負荷が軽減されます。

• 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 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 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



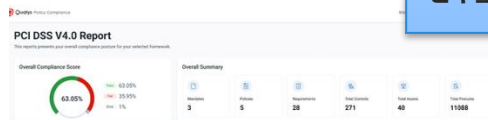
監査業務を効率化

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

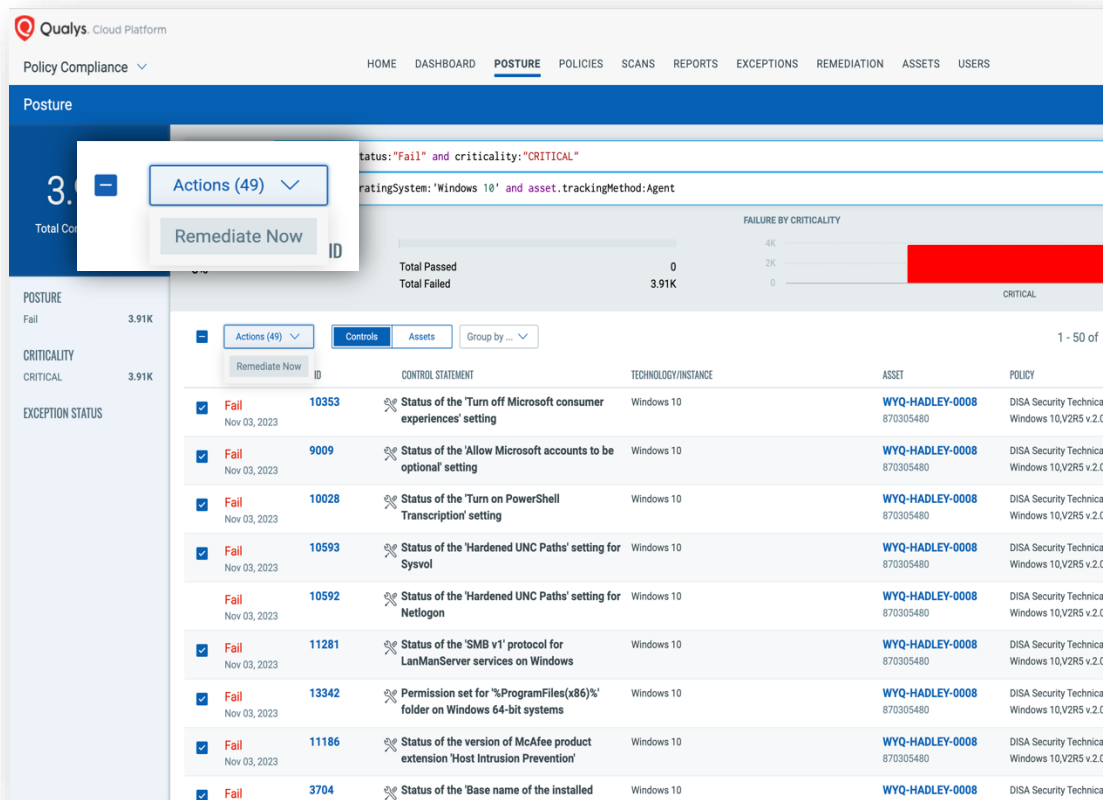
※詳しくは[Blog](#)をご覧ください

Audit Fix - 自動修復ワークフロー

※Policy Auditとは別の有償オプションです

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 Cloud Platform

Policy Compliance ▾

HOME DASHBOARD **POSTURE** POLICIES SCANS REPORTS EXCEPTIONS REMEDIATION ASSETS USERS

Posture

3. Total Controls

Actions (49) ▾

Remediate Now

POSTURE: Fail 3.91K

CRITICALITY: CRITICAL 3.91K

EXCEPTION STATUS

status: "Fail" and criticality: "CRITICAL"

OperatingSystem: 'Windows 10' and asset.trackingMethod: Agent

FAILURE BY CRITICALITY

Total Passed: 0

Total Failed: 3.91K

4K 2K 0

CRITICAL

1 - 50 of

	ID	CONTROL STATEMENT	TECHNOLOGY/INSTANCE	ASSET	POLICY
Fail	10353	Status of the 'Turn off Microsoft consumer experiences' setting	Windows 10	WYQ-HADLEY-0008 870305480	DISA Security Technical Windows 10, V2R5 v.2.0
Fail	9009	Status of the 'Allow Microsoft accounts to be optional' setting	Windows 10	WYQ-HADLEY-0008 870305480	DISA Security Technical Windows 10, V2R5 v.2.0
Fail	10028	Status of the 'Turn on PowerShell Transcription' setting	Windows 10	WYQ-HADLEY-0008 870305480	DISA Security Technical Windows 10, V2R5 v.2.0
Fail	10593	Status of the 'Hardened UNC Paths' setting for Sysvol	Windows 10	WYQ-HADLEY-0008 870305480	DISA Security Technical Windows 10, V2R5 v.2.0
Fail	10592	Status of the 'Hardened UNC Paths' setting for Netlogon	Windows 10	WYQ-HADLEY-0008 870305480	DISA Security Technical Windows 10, V2R5 v.2.0
Fail	11281	Status of the 'SMB v1' protocol for LanManServer services on Windows	Windows 10	WYQ-HADLEY-0008 870305480	DISA Security Technical Windows 10, V2R5 v.2.0
Fail	13342	Permission set for '%ProgramFiles(x86)%' folder on Windows 64-bit systems	Windows 10	WYQ-HADLEY-0008 870305480	DISA Security Technical Windows 10, V2R5 v.2.0
Fail	11186	Status of the version of McAfee product extension 'Host Intrusion Prevention'	Windows 10	WYQ-HADLEY-0008 870305480	DISA Security Technical Windows 10, V2R5 v.2.0
Fail	3704	Status of the 'Base name of the installed	Windows 10	WYQ-HADLEY-0008	DISA Security Technical

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

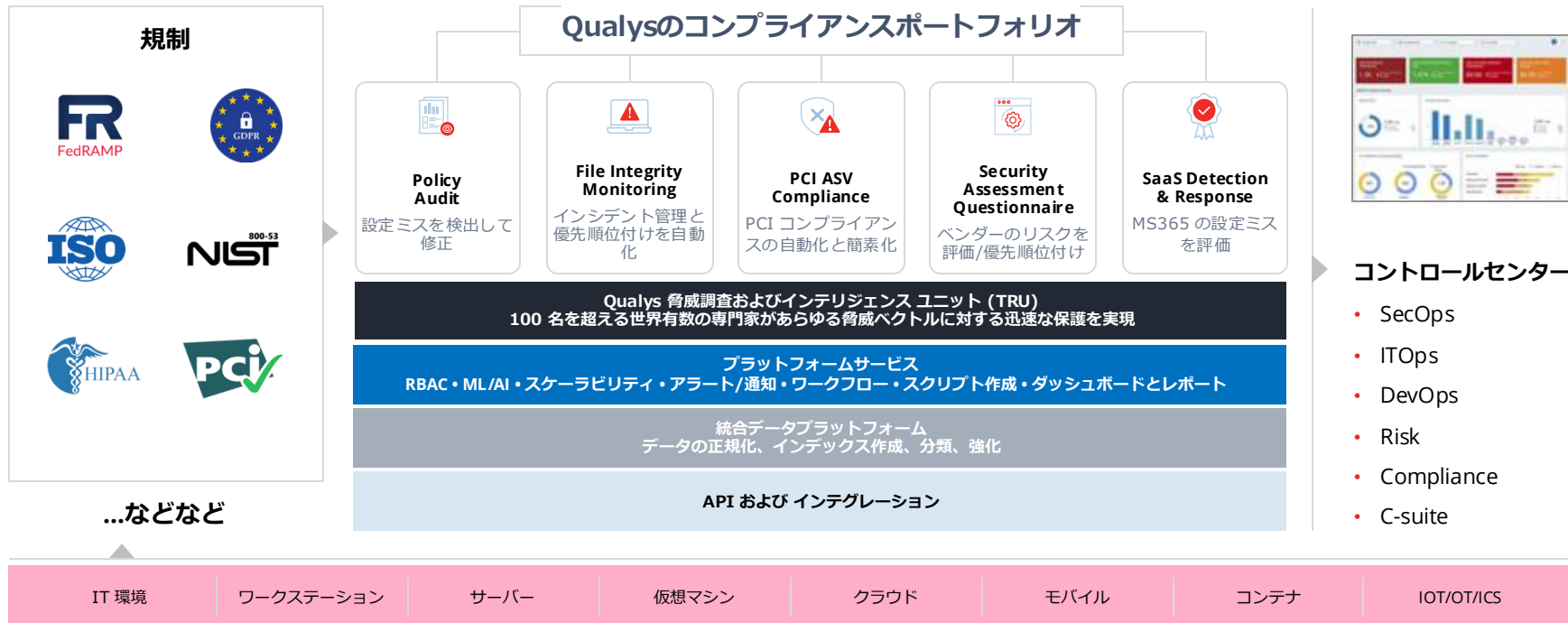
課題カテゴリ	具体的な課題内容	Policy Auditでの解決アプローチ
構成ミス・設定不備の放置	重大なポート開放、不要なサービス稼働などの設定ミスが属人的対応	CIS/NISTなどのベンチマークで継続的な設定監視・是正支援
内部統制・監査対応の負荷	設定確認・スクリーンショット取得が手作業で非効率	自動化された証跡付きレポートで監査に即対応可能
ガイドラインの整備不備	自社セキュリティポリシーが明文化されていない/徹底されていない	カスタムポリシー作成と違反検出で統制を強化
マルチOS・マルチクラウド環境の一元管理が困難	Windows、Linux、クラウドVMごとに設定がバラバラ	エージェント 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

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





クオリスによるリスクベースの優先順位づけ

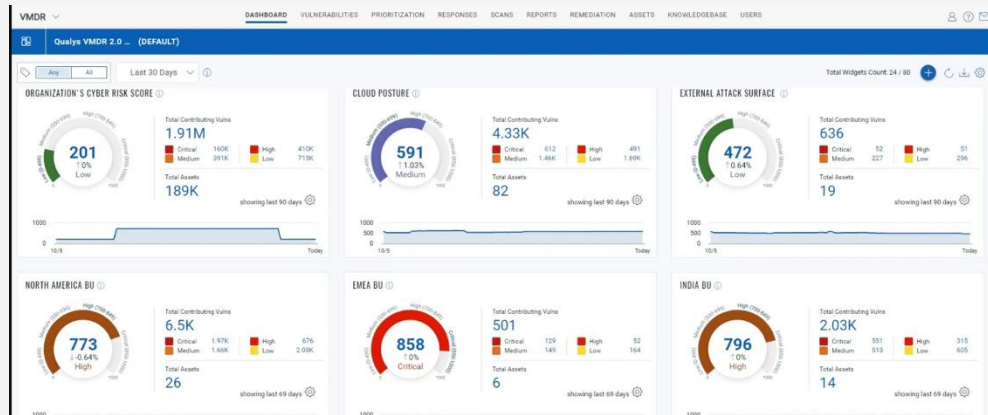
VMDR(脆弱性管理)とCSAM (資産管理)

*CSAMはVMDRライセンスとの併用が必須です。

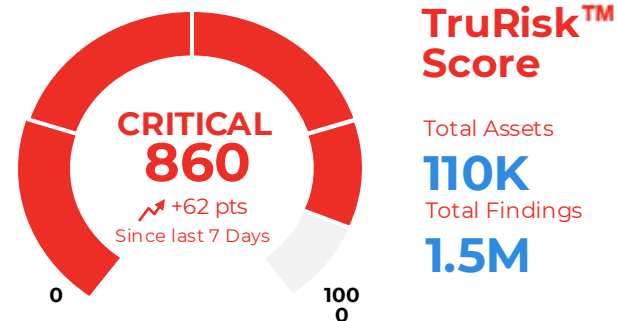


TruRisk™ 2.0による優先順位付け

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



Top Risk Factors

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

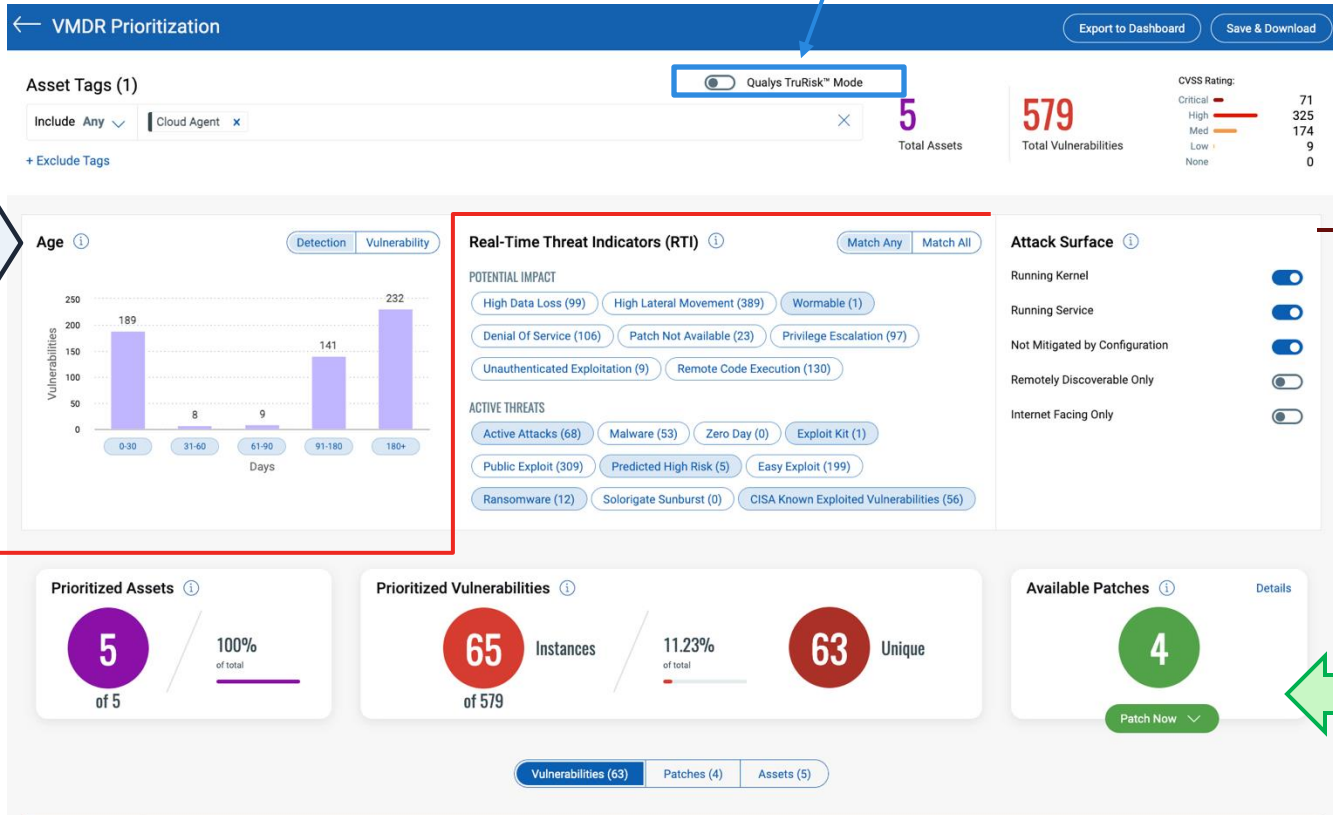
Qualys Tru RiskModeをオンにすると脅威インテリジェンスが有効になり、選択した資産のネットワーク上で最もリスクの高い脆弱性が優先順位付けされます。

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は潜在的な影響またはアクティブな脅威からインジケータを選択します。
MatchAny（いずれかに一致）とMatchAll（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。



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

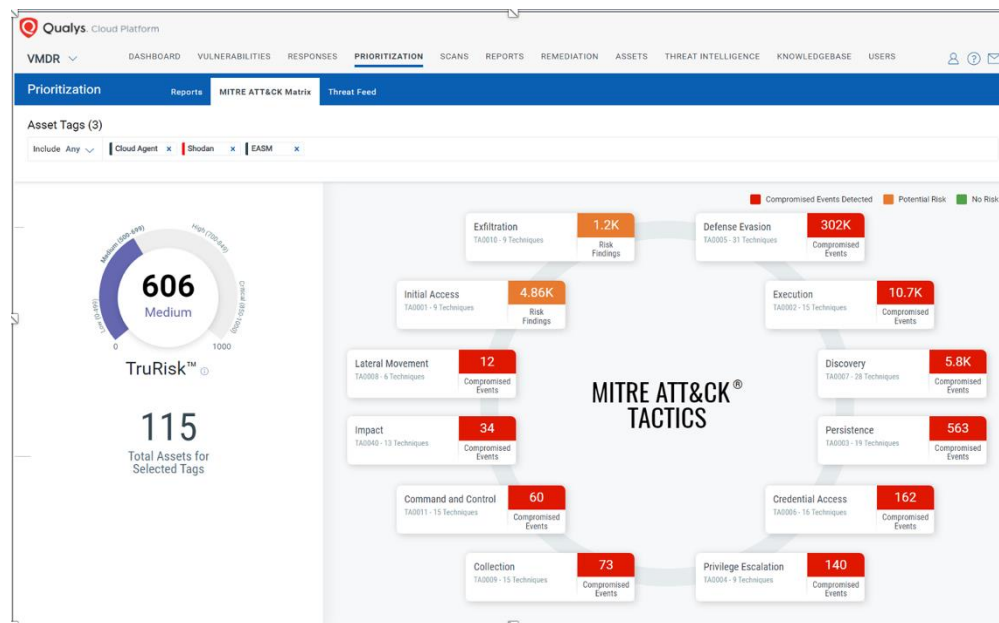
VMDRからの脆弱性、PCからの設定ミス、EDRからのインシデント、CSAMからの資産詳細（外部向け資産の識別やRDPポートの詳細など）を統合したATT&CKビューを提供します。



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マトリックスは、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を組み合わせることでフィルタを作成し、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。



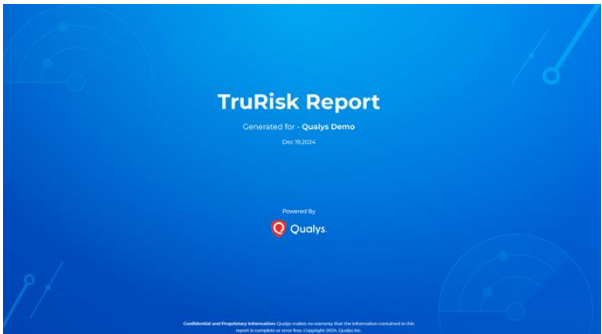
アクティブな脅威（Active Threats）

- **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 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。

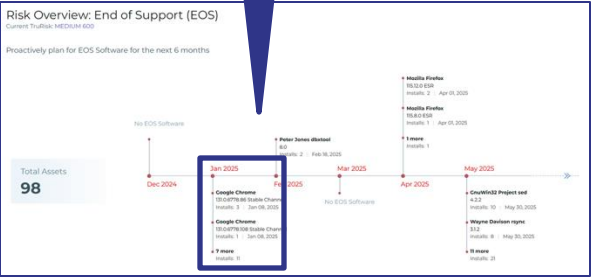
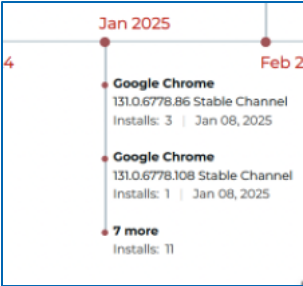


Risk Overview: EOS
2025年1月 Google Chromeのいくつかのバージョンと他のアプリケーションがEOSを迎えます。バージョンアップの計画を推奨します。

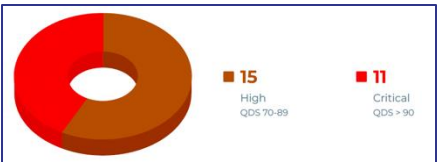
2025年6月4日 詳細は[こちら](#)

※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

Weekly Insights Vulnerabilities: Top 5
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。



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



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-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 Tunes	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+

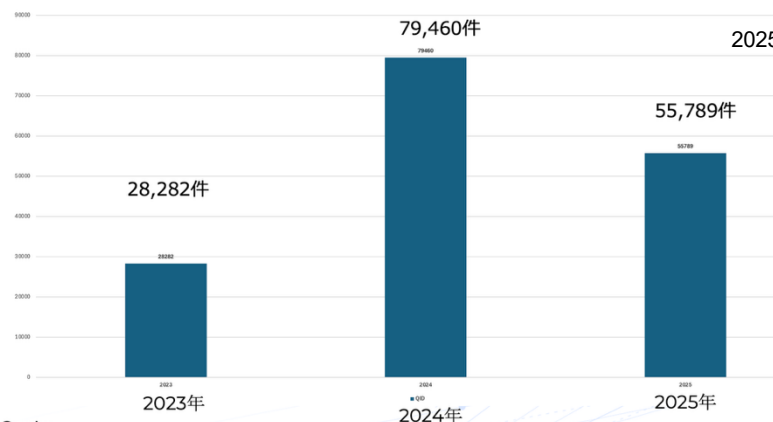
脅威研究ユニット(TRU)の専門家



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

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。



クオリスによる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？

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？

モデルとデータの損失

攻撃対象領域の増加

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？

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？

低い可視性

セキュリティサイロ

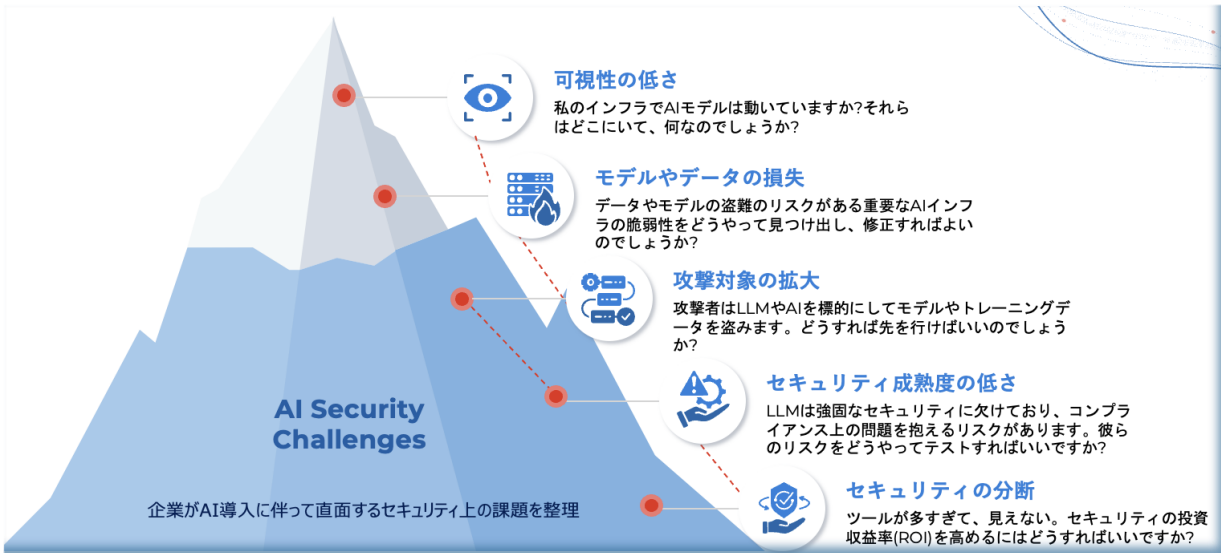
ツールが多すぎるにもかかわらず、可視性が欠如しています。セキュリティ投資からより高い ROI を得るにはどうすればよいですか？

LLMのセキュリティ課題

生成AIのワークフローにおけるリスクの存在

Total AI

生成AIのライフサイクル全体にリスクが分散しているため、包括的なセキュリティ対策が不可欠



AI導入におけるセキュリティの複雑さと、統合的なリスク管理の必要性



Qualys TotalAIの紹介

※ブログは[こちら](#)

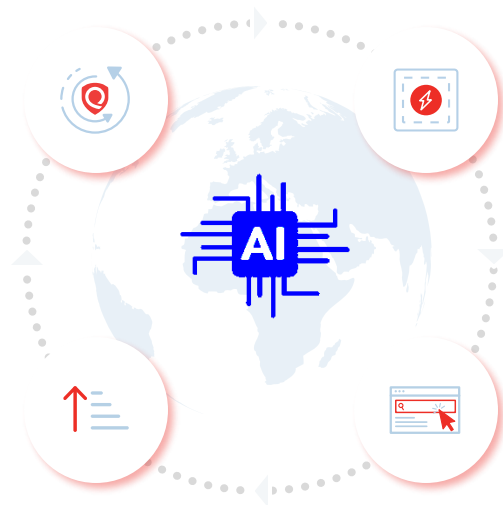
LLM リスク、AI ワークロード、AI 脆弱性を総合的に可視化します

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

レポートニ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

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。



AI ソフトウェア & パッケージの検出

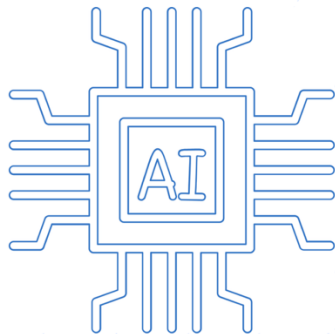
オンプレ及びマルチクラウド

- 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 Courneau 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
- Squirrel 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)



AI関連の検出実績

100万件以上のAIベースの検出をすでに実施済み。



LLMの脆弱性

テストされた大規模言語モデルの91%がプロンプトインジェクション攻撃に脆弱であることが判明。



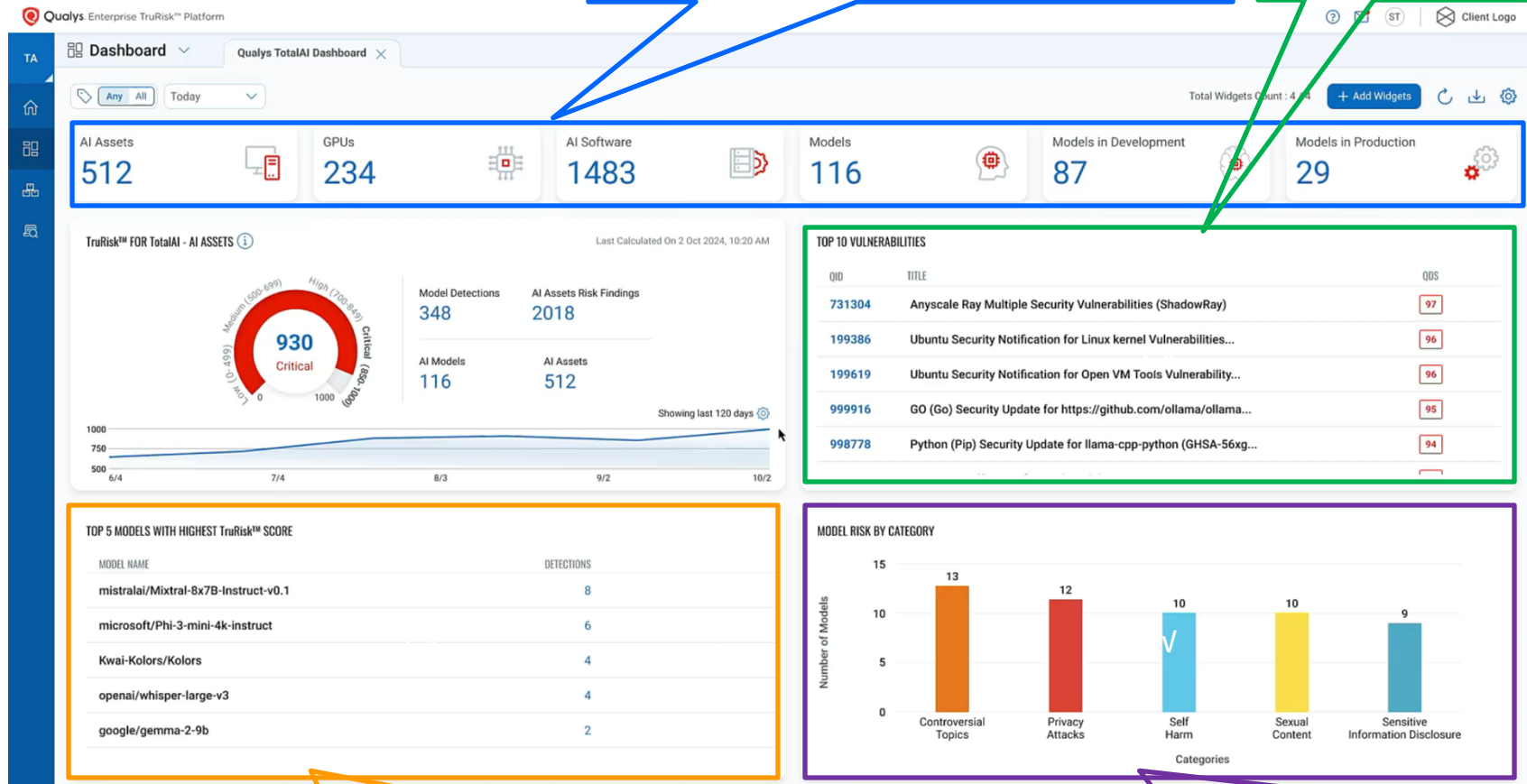
具体的なモデルの結果

DeepSeekは半数以上のJailbreakテストに失敗。

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



Qualys TruRiskスコアに基づくTop5モデル

リスクカテゴリ(論争的となるトピック、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)



UPDATED!

クオ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。



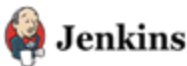
Kubernetes & Container Security カバレッジ

Build

開発ビルドをスキャンする



Bamboo



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



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



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)

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

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DaemonSet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

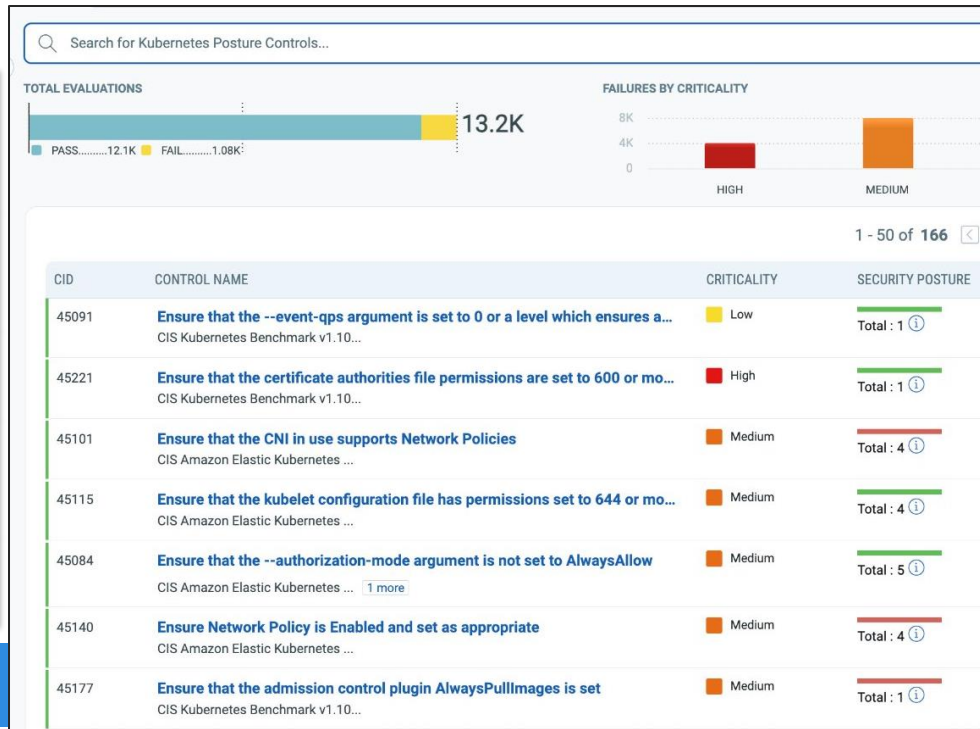
Kubernetes Posture (KSPM) + Admission Controller

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“運用中のクラスター”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



Continuous Discovery in Action

You've recently enabled scans for new clusters and fetched key insights!

Your **Cyber Risk Agent Nexa** has spotted areas needing attention — review these blind spots and scan them to stay fully covered.

[Try Now](#)

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。

e0c123a76bd4 ★
Account ID: 872493106512

Security Findings

- Internet Exposure
- Privileged Pod
- Privileged Pod
- EOL Software

Vulnerabilities

- 3 Critical
- 2 High
- 3 Medium

Risk Exposure Period

4 days

TruRisk Score

861 Critical

Additional Insights

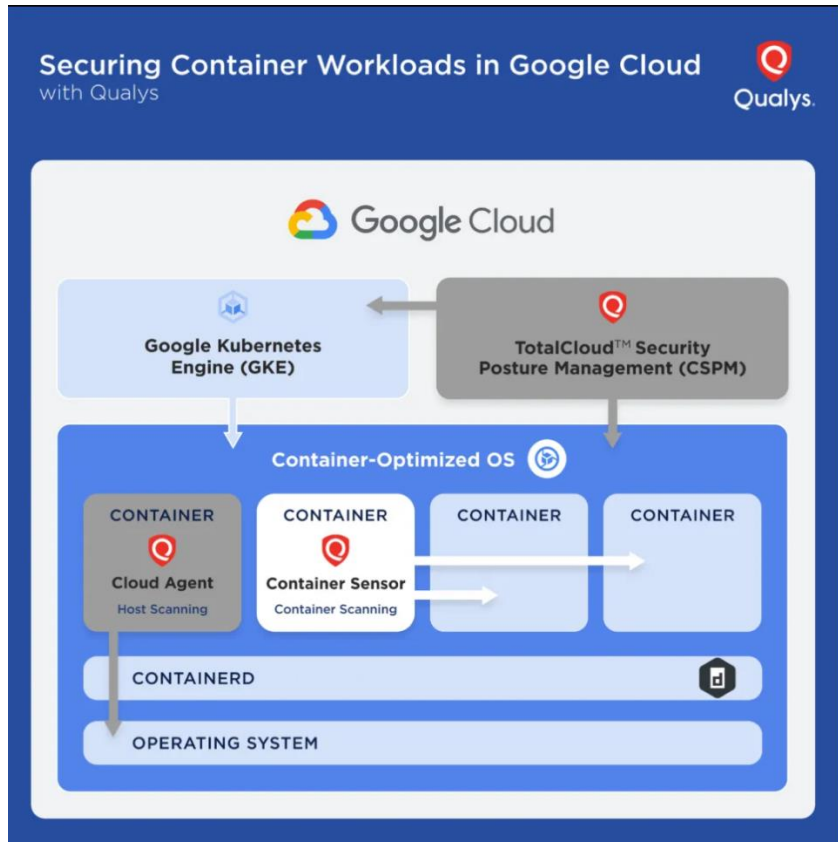
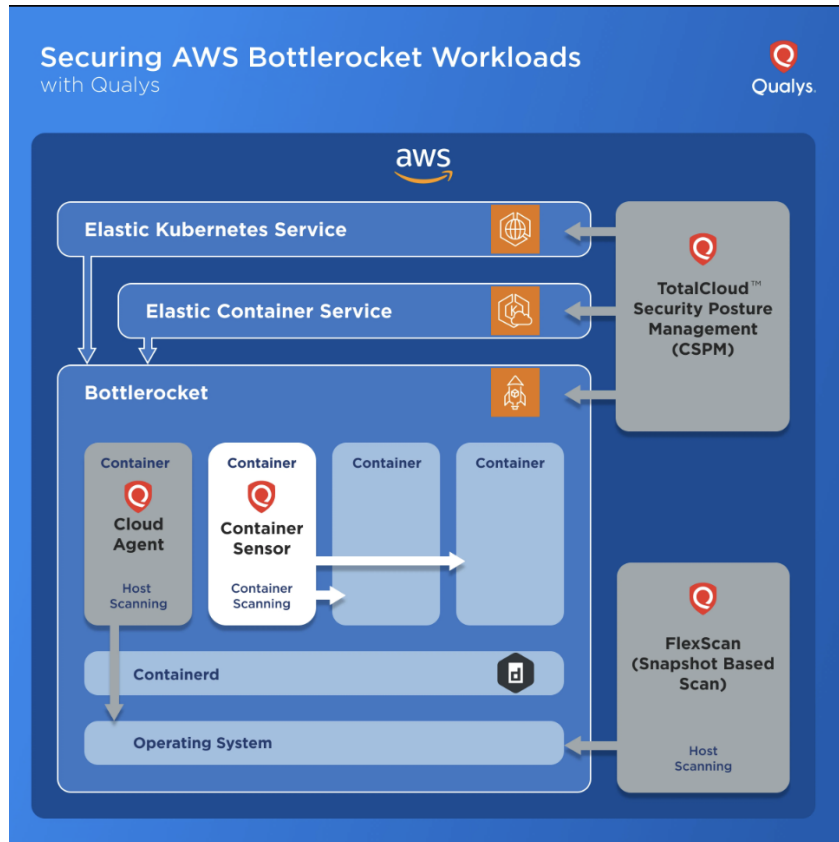
Powered by Qualys Integration

- 1 GitHub Commit
- 1 Checkmarx SAST Finding

AI Summary

- Vulnerability **CVE-2024-27198** was introduced in your environment on 13 Oct, 2025
- A new **'RUN NPM install struts-js@2.315'** was introduced as part of your **apache-app** brought in this new dependency
- The author of this commit was **jon.dev@acme.com**
- struts.json flagged as a **High Command Injection Risk** by Checkmarx ignored by developer

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

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**



クオリスクラウドエージェントの特徴

Cloud Agent

*Cloud AgentはVMDRライセンスが必要です。



Cloud Agent 対応サービス

サイバーセキュリティ
アセット管理

脆弱性
管理

オープンソフト
ウェア検出

セキュリティ
設定評価

修復、緩
和、分離

FirstParty
のリスク評価

ファイル
改ざん検出

セキュリティ
解析

パッシブ
センシング

CSAM

VM

SwCA

PA/
SCA

MTG/
ISL/PM

CAR

FIM

EDR

CAPS

インベントリ

脆弱性管理

コンプライアンス

修復

検知と応答

管理外アセット検出

Cloud Agent

- ・ 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>>

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)		

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, PowerShell, 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を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 スマートチケット連携

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。



SCA Security Configuration Assessment

VM

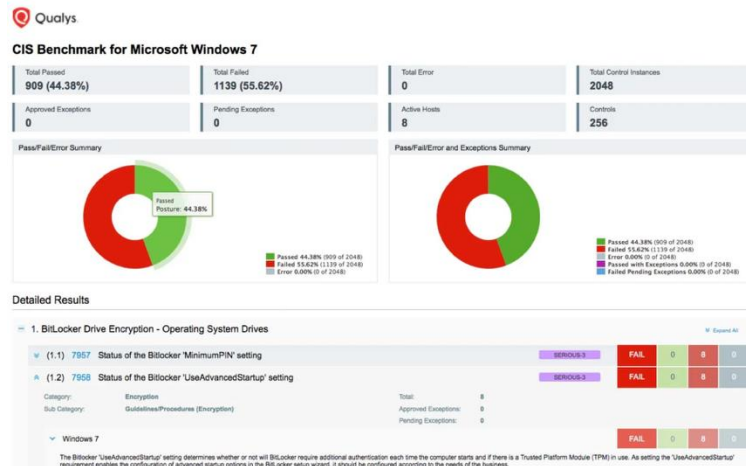
クラウドベースの構成管理とセキュリティ強化を実現する、統合型VM拡張ソリューション

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。



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バ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Clop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。

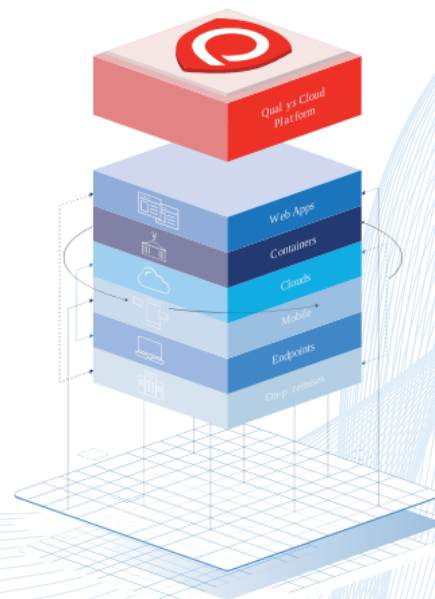


カーネル モードのアプリ: Windows OS で実行される EDR および FIM の場合のみ、カーネルドライバが必要です。検出、コンテンツ、署名、およびデータ収集は非侵襲的であり、リソースを大量に消費しません。Linux および Mac OS では、カーネル モードは呼び出されません。Qualys は、コンテンツの更新を通じてカーネル ドライバを変更しません。ドライバの変更はすべて、Microsoft による認定後に新しいエージェント バージョンとしてリリースされます。



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)。



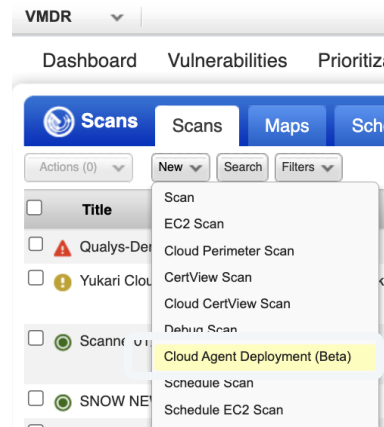
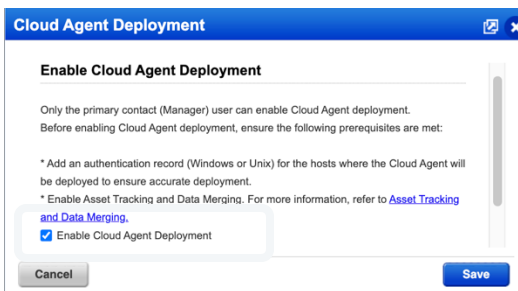
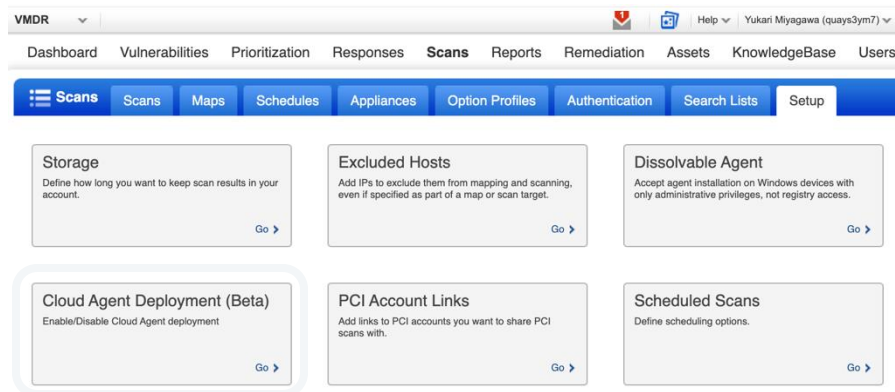
仮想スキャナーを利用したCloud Agentの展開

Qualys スキャナーを使用すると、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。スキャナーは、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。



Qualys 補助資料

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

Qualys Cloud Platform

← View Details: SUDOERS

Event Alert: File Read

sudoers

Changed On: 15 days ago Jan 25, 2024 at 11:44:42 AM

Category: PCI

By User: jerry

File Path: /etc/sudoers

By Process: /usr/bin/grep

Command Executed: grep --color=auto -i jerry /etc/sudoers

Audit User Name: root (0)

Success Status: no

sudoers was Read

Triggers

Monitoring Profile: Linux Monitoring Profile for PCI DSS - DO NOT DELETE

Section and Rules: Rule-7

Continuous Monitoring

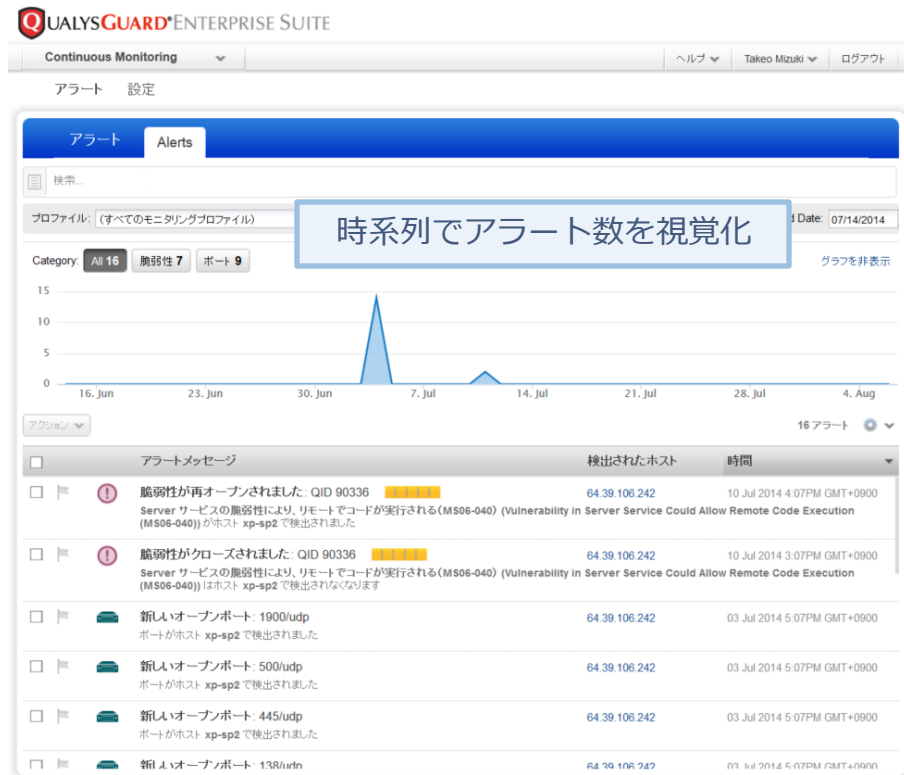
CM

■ 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



具体的なアラートメッセージを表示

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

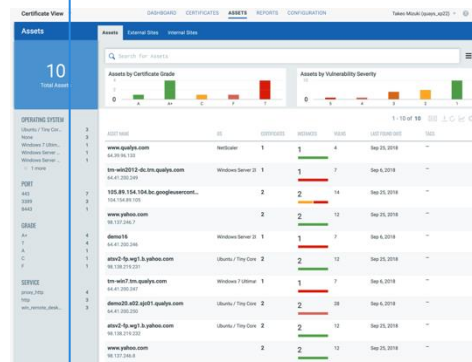
リスクのある証明書や期限切れ証明書を一目で確認できるレポート・可視化機能

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

VMDR Mobile

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

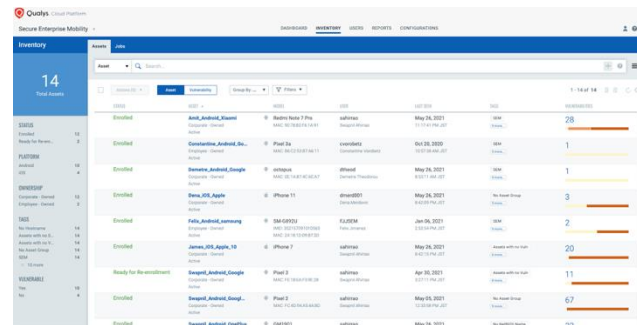
アプリ、OS、構成の情報を統合し、リスクスコアを算出

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

2 合計 Templates

S3

Filters

1 - 2 of 2

TEMPLATE NAME

Remediate | CID 48 | Ensure versioning is enabled for S3 buckets

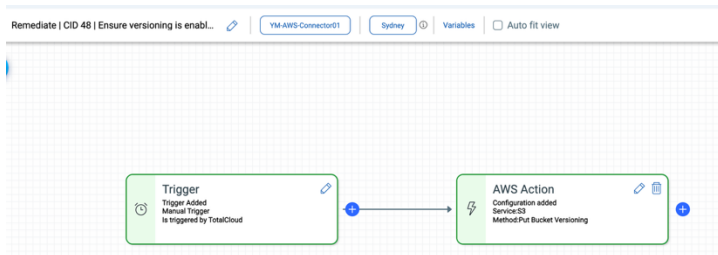
Perform the following to enable versioning of S3 Buckets: 1. Sign in to the AWS management console and open the amazon s3 console at https://console...

Select

Remediate | CID 67 | Ensure all S3 buckets employ encryption-at-rest

To enable default encryption on an S3 bucket: Using AWS Console: 1. Sign in to the AWS Management Console and open the Amazon S3 console at https://...

Select



[Get Started with QFlow](#)

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

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

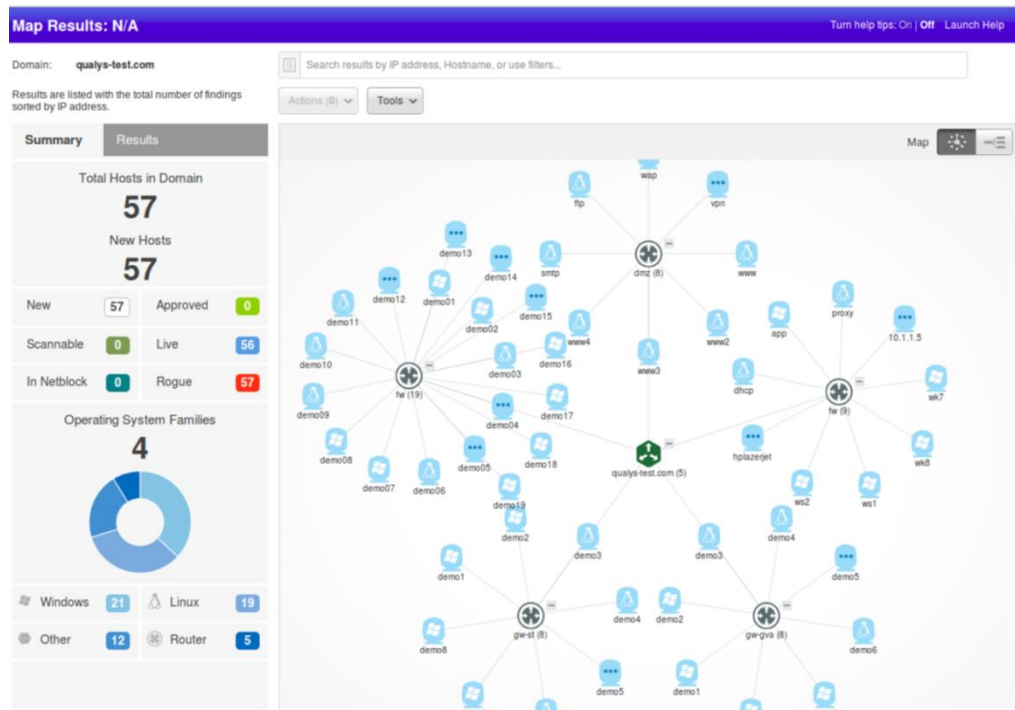
主な機能：自動資産検出、動的マップ生成、VMDRやTASへのスキャン連携、継続的な探索スケジュール、探索対象、探索範囲、除外対象、など細かく設定可能です。

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。

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 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。



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



* CAPSを使用するにはCSAMライセンスが必要です。

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、証拠を保ちながらリスク管理を強化

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

Enterprise TruRisk Platform in numbers

**9+
trillion**

データポイント
elastic search
clusterをインデ
ックス化

**2+
trillion**

年間のセキュリ
ティイベントの
保護数

**6+
billion**

年間のIPスキャ
ン数と監査数

**5+
billion**

1日あたりの
Kafkaメッセー
ジデータを安全
に高速処理

**20+
apps**

統合されたIT、
セキュリティ、
コンプライアンス
アプリ数

99.99966%

シックス・シグ
マスキャン精度
で誤検知を完全
に排除します

世界中で10,000を超えるサブスクリプション
顧客がQualysを信頼しています

70%

Forbes Global 50

54%

Forbes Global 500

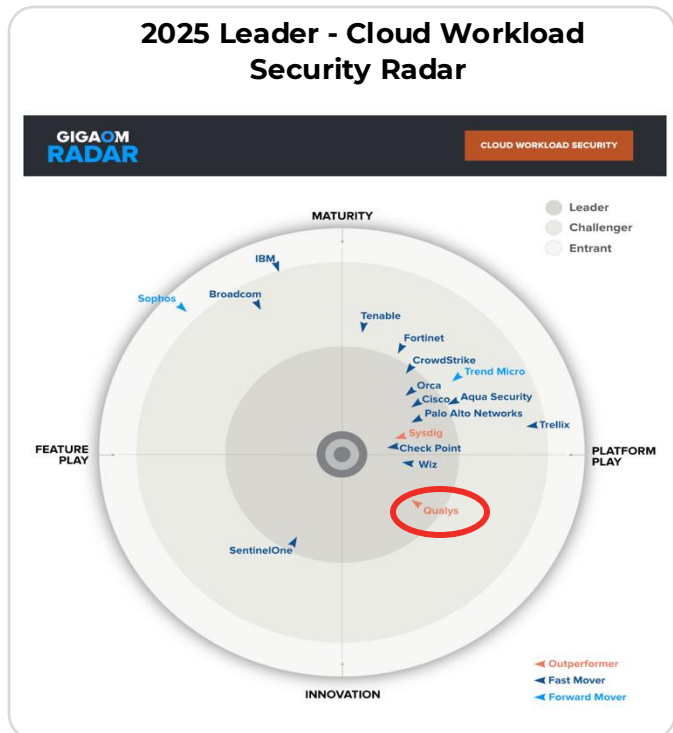
32%

Forbes Global 2000

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

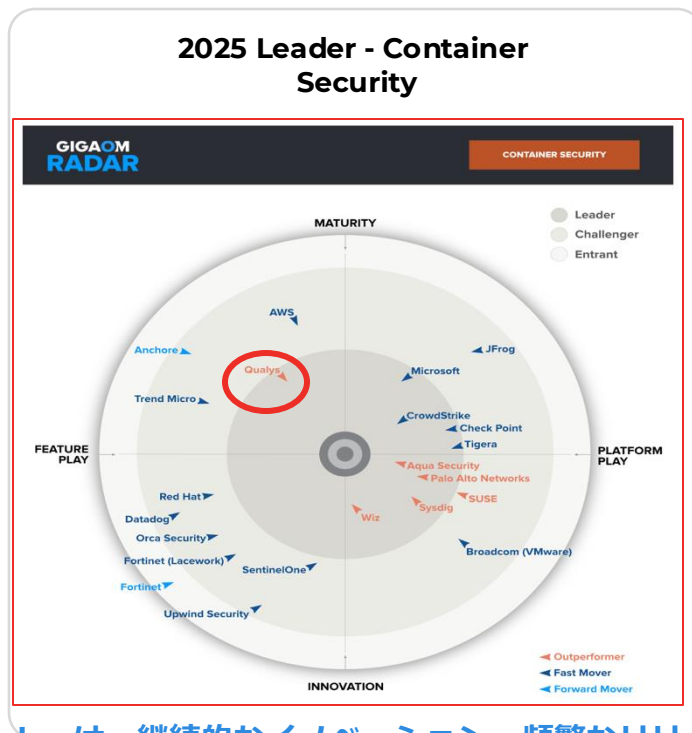
TotalCloud - クラウドセキュリティ市場の認知度

アナリストによる評価



「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



「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、アウトパーフォーマーに分類されました。」

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



"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"

「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。」

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

IDC MarketScape: Worldwide Cloud-Native Application Protection Platform, 2025



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:

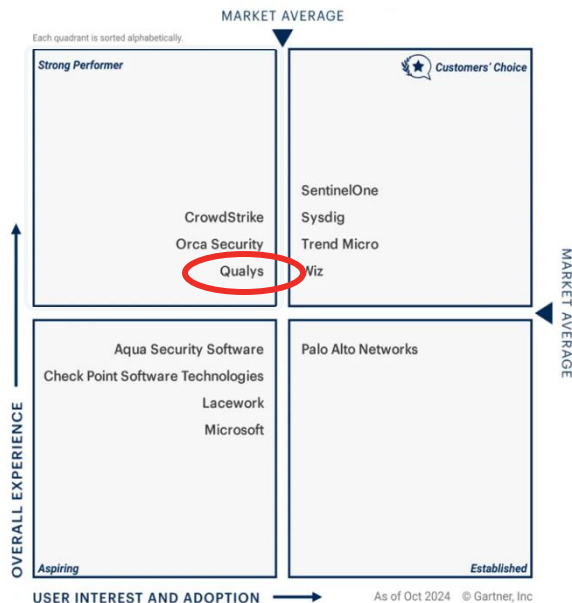
- 4,500 万のマルチクラウド ワークロードが TotalCloud Flexscan テクノロジーを使用してスキャンされます。
- 4,500 万のマルチクラウド ワークロードが TotalCloud Flexscan テクノロジーを使用してスキャンされます。
- 800社以上の顧客から40,000のクラウドアカウントがあり、TotalCloudによって保護されています

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



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](#)

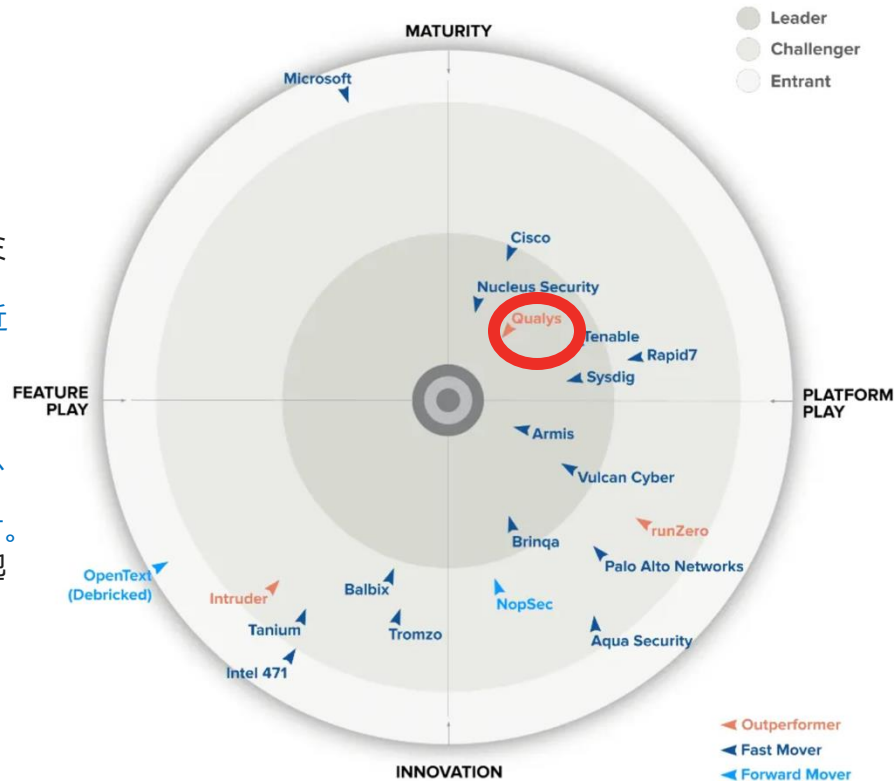
GigaOMリーダー脆弱性管理(VM)レポート

What are we announcing?

第3回年次VMリーダーレポートで、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。



Qualys TotalCloud CNAPPのポジションニング

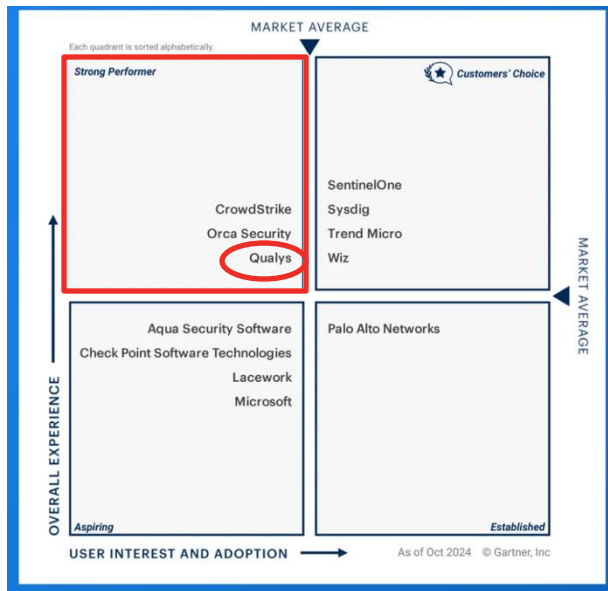
KuppingerCole

2024 Leadership Compass for CSPM



Gartner

2024 Peer Insights Voice Of The Customer - CNAPP



GigaOm

2025 Cloud Workload Security Radar



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。

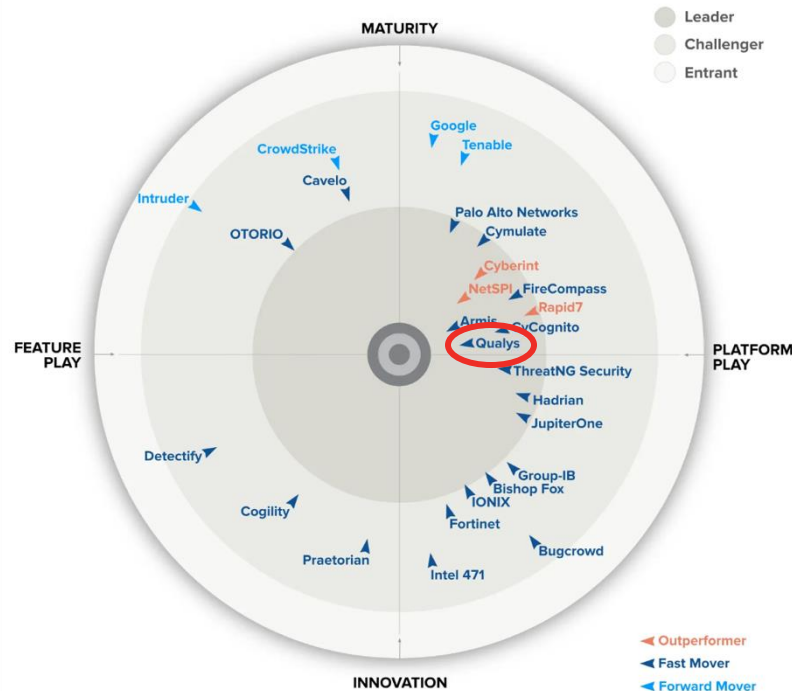
Qualys サイバーセキュリティ資産管理(CSAM)の優位性

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。



Source: GigaOm 2023

©GigaOm

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

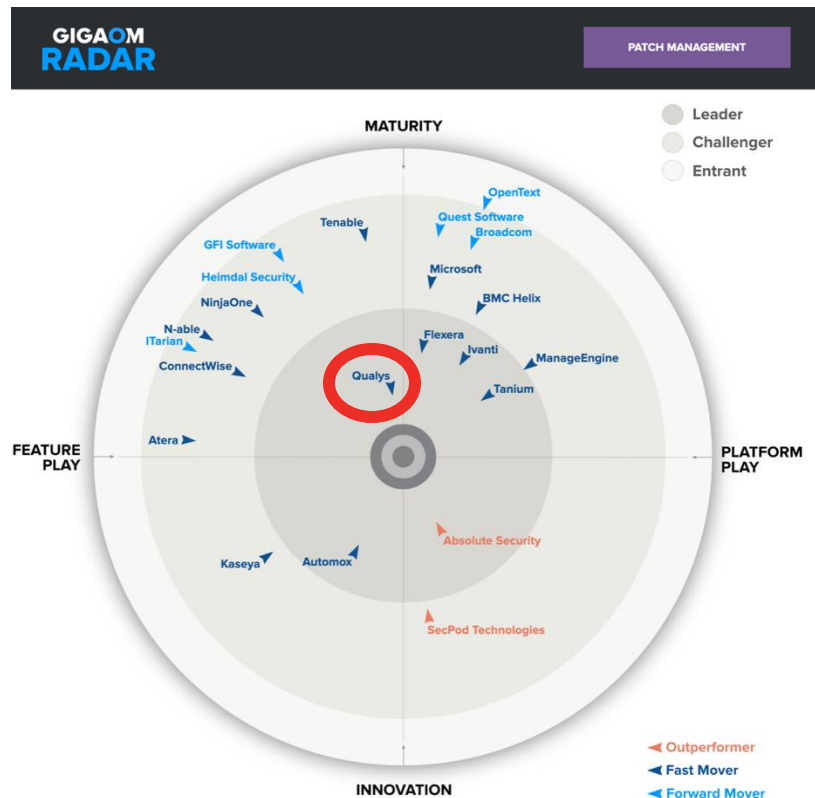
GigaOMレーダーパッチ管理(PM)レポート

Qualysは、2025年版 GigaOM パッチ管理ソリューション部門レーダーで「総合価値No.1リーダー」に選出されました。

業界による検証： GigaOMは、パッチ管理ソリューションを評価するための最も信頼性が高く包括的なリソースの1つです。この市場に特化した唯一の独立分析レポートである最新のレポートにおいて、アナリストはQualysを他のすべてのベンダーと比較して総合価値が**最も高いリーダー**として評価しました。

競争優位性： アナリストは、パッチ管理において「**リスクベースの優先順位付けと脆弱性管理ソリューションとの統合が基本的な期待値になりつつある**」ことの重要性を特に指摘しています。TREは、明確な優位性を持つ最有力候補として認識されています。「このプラットフォームは、幅広い機能と統合性において優れています。TREの修復コックピット、リスクベースの自動化ワークフロー、そしてQualys TruRiskエンジンによる動的な優先順位付けは、堅牢で拡張性の高いアーキテクチャに貢献しています。」

注： 本レポートでは、**TruRisk Eliminate (TRE)** を修復ソリューションとして位置付けています。



FedRAMP High ATO 取得

Qualys Government Platform が「FedRAMP High ATO (Authorization to Operate)」を取得
米国政府・重要インフラ機関が利用できる最高レベル (NIST SP 800-53 High準拠) の認証基準に合格。

- クラウド・オンプレ・ハイブリッド環境を問わず、**国際的に信頼されるセキュリティ基盤**を提供
- 「**最も厳格な認証を通過したクラウドサービス**」として、公共・金融・防衛分野でも採用可能
- 400超の技術的コントロールに**基づく継続的モニタリングと自動修復**を実現
- TruRisk™ によるリスクベース管理を含む統合的**サイバーリスク削減**

Qualys FedRAMP High ソリューション

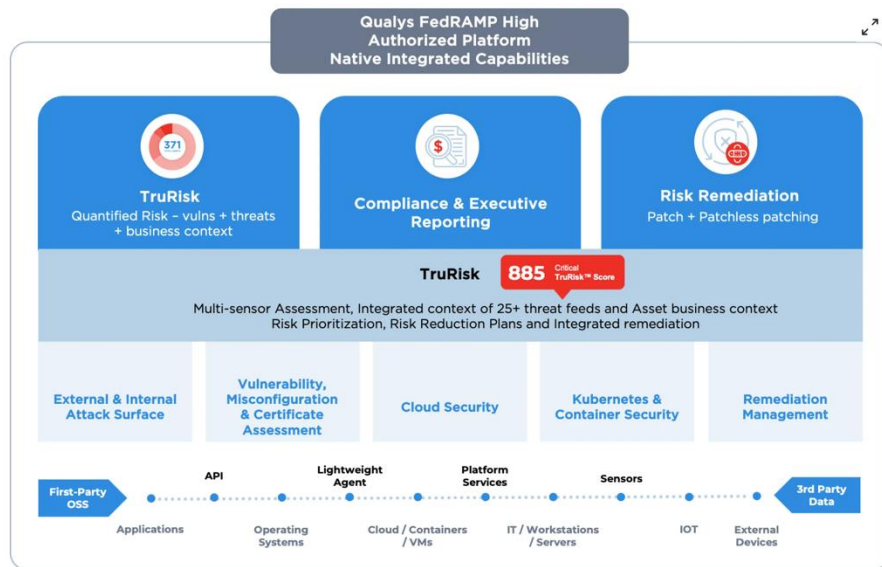
当社の統合プラットフォームは、お客様がコストと運用の非効率性を削減しながら、優先順位を付けてリスクを軽減するのに役立ちます。

初期のFedRAMP High認定ソリューション

- VMDR (Vulnerability Management, Detection & Response) – No Asset View
- Policy Audit
- Patch Management (Eliminate coming soon – Q1 2026)
- CSAM (Cyber Security Asset Management)
- Container Security (Full TotalCloud suite coming soon – Q1 2026)
- Web Application Security
- File Integrity Monitoring

主な差別化要因

- 業界唯一のFedRAMP High VMリスク管理プラットフォーム
- ゼロトラスト、BOT、エグゼクティブオーダーの上位要件に1つのプラットフォームで対応
- 柔軟なライセンス(Q-Flex)による運用の複雑さの軽減
- #1 FedRAMP MOD認証を延長



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