Qualys Trurisk Platform
ソリューション概要

Qualys Japan K.K
更新日2026年3月

クォリスプラットフォームの紹介

Enterprise TruRisk Platform
Vulnerability Management Detection and Response（VMDR）

Qualys Enterprise TruRisk Platform

Qualys VMDR with TruRisk™

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

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

企業全体のサイバーリスクを軽減

サイバーセキュリティ対策をビジネス成果に結び付ける

ROI: ビジネス成果の実現

統合アプローチで攻撃対象領域を削減

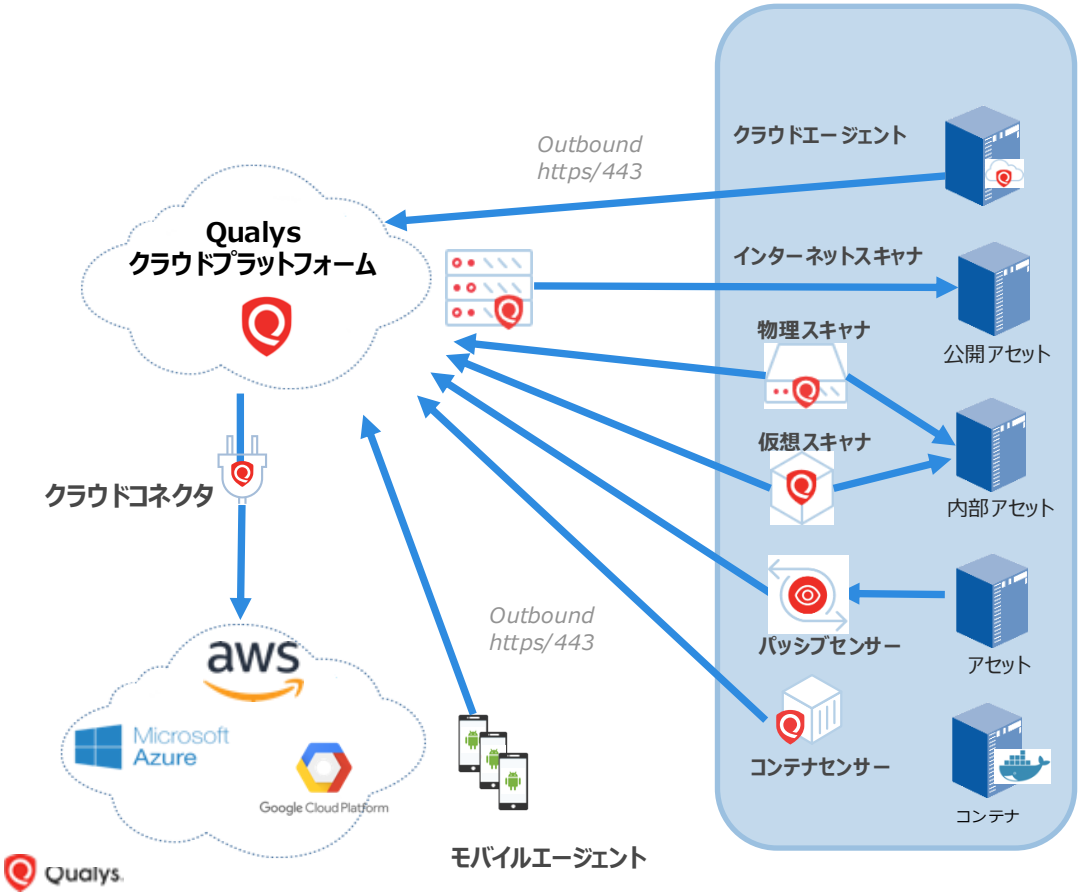
Qualys導入メリット

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

ROI（Return on Investment）

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

環境に合わせた様々なスキャン方法



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

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

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

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

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

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

クォリスアセットインベントリ

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

1. ハードウェア情報

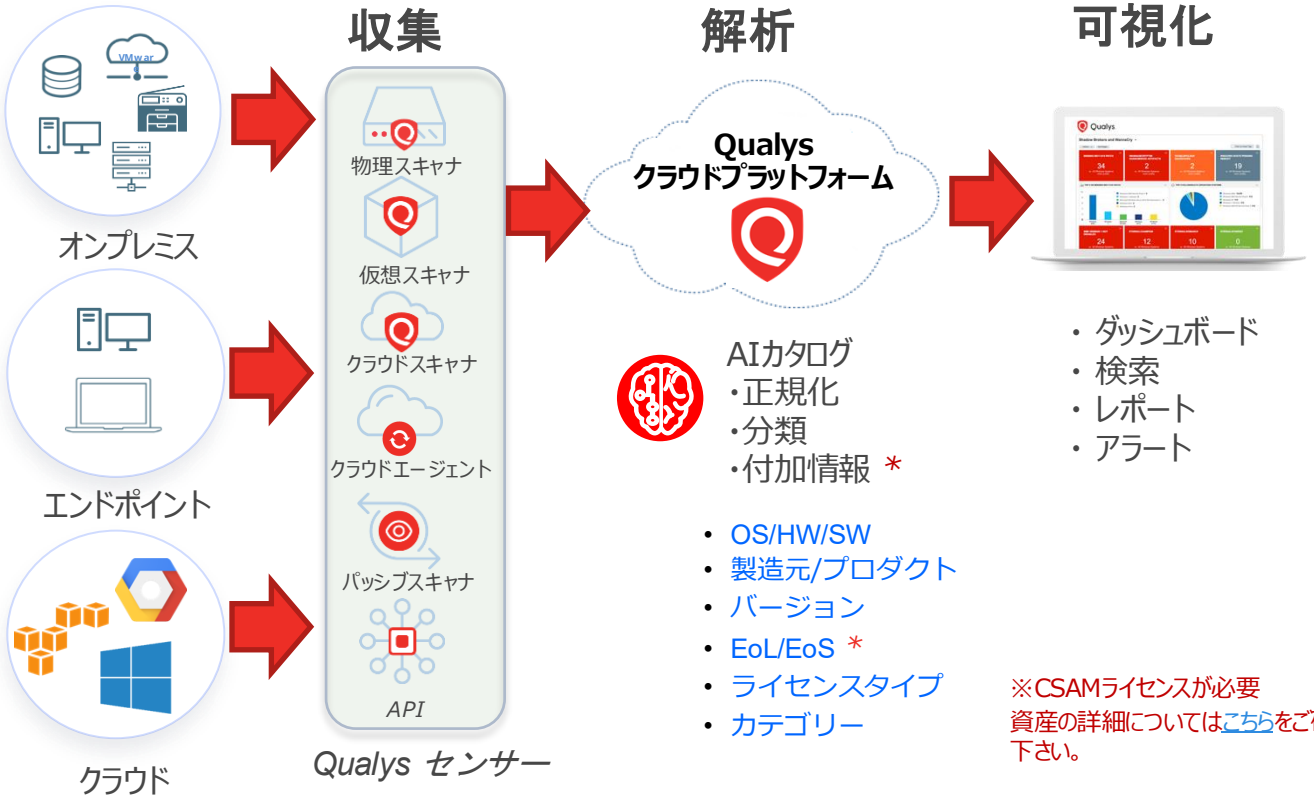
基本情報: ホスト名、IPアドレス（IPv4/IPv6）、FQDN、NetBIOS名など。
ハードウェア仕様: CPU、メモリ、ディスク容量、GPU、LPAR ID（AIX環境）など。
ネットワーク情報: MACアドレス、ネットマスク、ネットワークインターフェースの詳細。
地理的位置情報: パブリックIPに基づくアセットの地理的な位置

2. ソフトウェアおよびサービス情報

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

3. クラウドプロバイダーメタデータ

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



※CSAMライセンスが必要
資産の詳細についてはこちらをご確認下さい。

脆弱性検知レポートの出力例

Qualys脆弱性検知レポートの主な特徴

◎多言語対応と詳細な情報提供

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

◎リスク評価と可視化

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

◎対処方法と根拠の明示

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

◎リアルタイム脅威インテリジェンスとの連携

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

Qualysレポートのメリット

◎リスクベースの優先順位付け

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

◎自動化と効率化

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

◎コンプライアンス対応

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

Qualysモジュール全体図

脆弱性管理&設定管理

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

コンプライアンス

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

資産管理

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

リスクの修復

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

脅威の検出と応答

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

Update!

リスクオペレーションセンター

- NEW ETM — Enterprise TruRisk Management/CTEM
- NEW Agentic AI — Agentic AI
- NEW ETM Identity — ETM Identity

クォリスによる資産管理

Cybersecurity Asset Management（CSAM）

*CSAMはVMDRライセンスとの併用が必須です。

内部・外部の攻撃対象領域全般のリスク管理

資産の可視性のギャップを見つけて埋める

✓攻撃対象領域全体をカバー

✓市場で最も包括的な資産発見

30%以上の新たな資産を発見

ビジネスコンテキストでVMを高速化

✓ VM プログラムの資産カバレッジの改善

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

ACSの5倍の効果

Qualys.

内部資産

Agent, Scanner, Sensors

外部資産

Open-source Tech & Qualys Internet scanner

SHODAN Scanner Whois DNS

クラウド資産 *Update!*

Monitor your Cloud environment

aws Azure Google Cloud ORACLE

第三者からの資産 *Update!*

API-Based Connectors

Active Directory servicenow bmc helix vmware

IoT/OTと不正な資産

Passive Network Sensing & CAPS

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

環境適したスキャン手法で包括的にリスクを可視化

脆弱性の検出と評価
リモートのみの脆弱性とSSLベースの脆弱性を検出

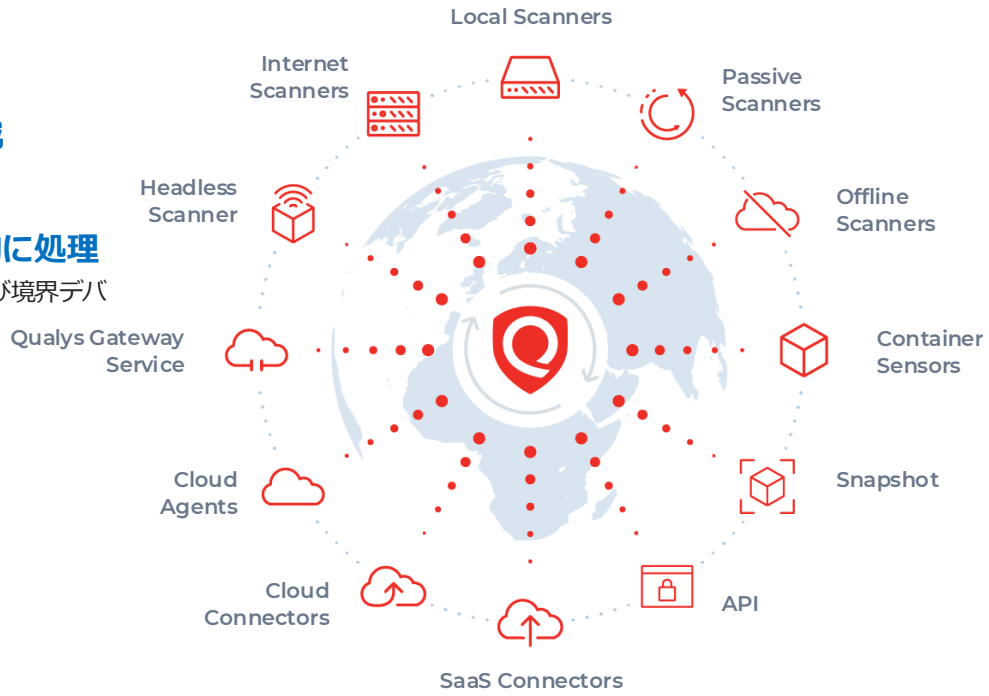
ダイナミックハイブリッド環境のリスク軽減
エージェントを配備できないクラウド資産を防御

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

デジタル証明書の評価
リモートスキャンで不足している証明書を特定

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

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



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

Qualys

CyberSecurity Asset Management の特長

内部および外部の攻撃対象領域の可視性

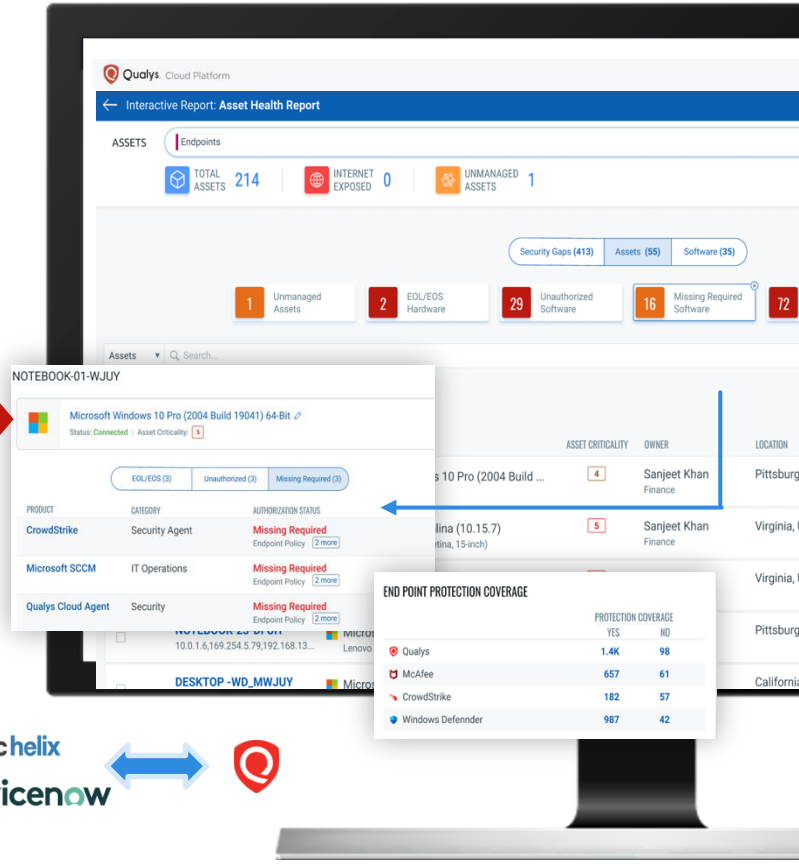
防御側と攻撃側の両方の視点から環境を可視化防御します。これには外部攻撃対象領域管理（EASM）も含まれます。この可視性をCMDBに反映することで、IT部門に最新の実用的なインベントリを提供します。

リスクベースの脆弱性管理プログラムの改善

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

技術的負債の削減

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



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

bmc helix
servicenow

脆弱性を超えたリスク要因

自信を持って優先順位を付ける

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

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

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

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

高リスク

Qualys TRUによるEOL/EOSコンテンツ強化

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

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

Qualys

参考BLOGはこちらを御覧ください。

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

外部攻撃対象領域管理(EASM)の特徴

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

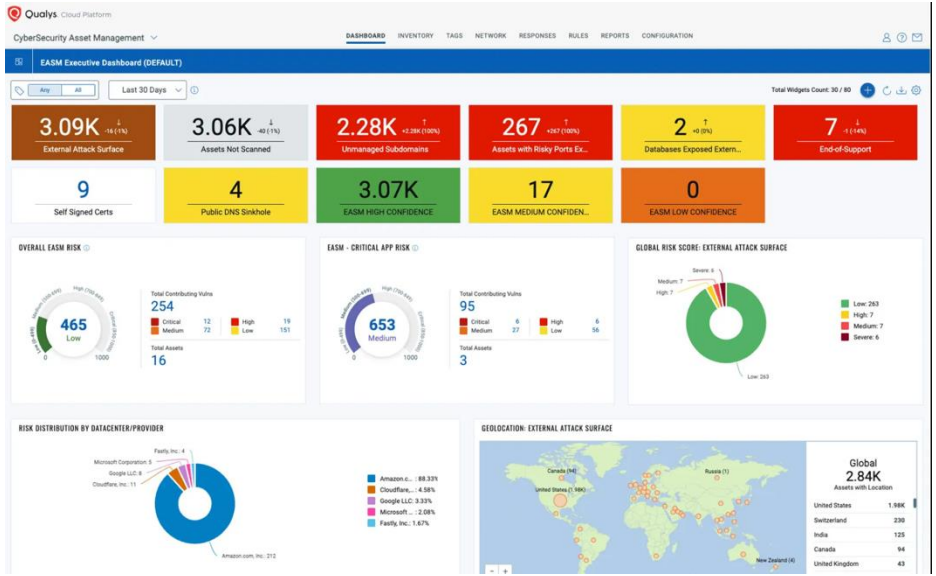
EASM Lightweight Scan搭載

新機能!

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

スキャンの特徴:

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



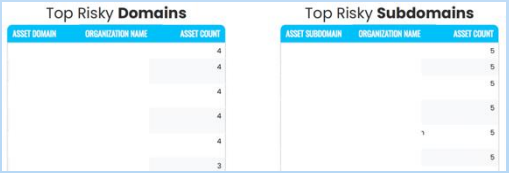
EASMによる「なりすまし・フィッシング」監視

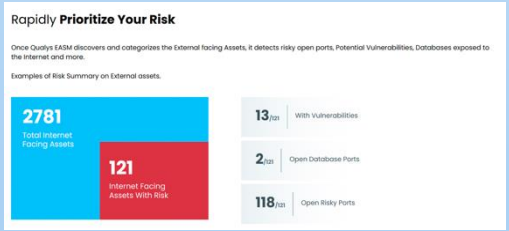
機能カテゴリ	対応内容
ドメイン監視	・**類似ドメイン（タイポスクワッティング、同音異綴など）**を自動検出。フィッシングサイトや偽ブランドサイトの発見に有効。例: qual1ys.com や qualys-security[.]net ・**誹謗中傷に関わるドメイン**により組織の評判を傷つける目的のコンテンツや商標権侵害のリスクのあるサイトの発見。
証明書監視	公開SSL/TLS証明書を解析し、**自社ブランド名を含む証明書の不正使用**を検出可能。
Web資産検出	未知のWebサイトやホスティングされた偽ページを自動で検出。攻撃者によるブランド**なりすましの兆候を早期発見**。
外部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

活用例

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

ESAMレポート





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

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

EASM 新機能と改善点

CSAM2.18.0.0

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

1. EASMプロファイルの複数作成が可能に

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

2. EASMプロファイルのインポートとエクスポート機能

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

3. EASMプロファイルの変更履歴の表示

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

4. EASMの軽量スキャンのIPアドレス管理

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

5. ビジネスエンティティと関連資産の可視化

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

6. タグのスコープ外の可視性向上

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

7. 新しいQQLトークンの追加

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

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

EASM軽量スキャンの利点

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

※リリースノートはこちらをご覧ください。

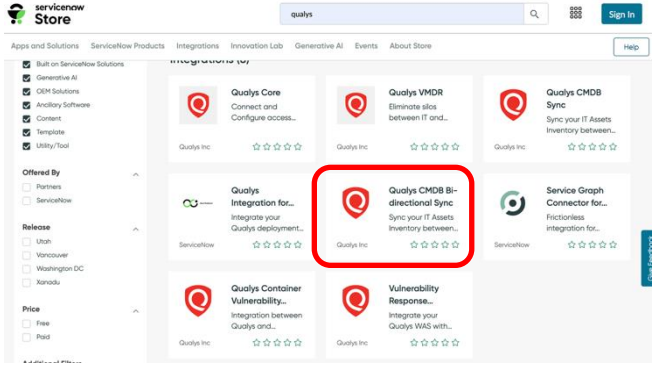
Qualys×ServiceNow連携で資産管理をスマートに自動化！

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。

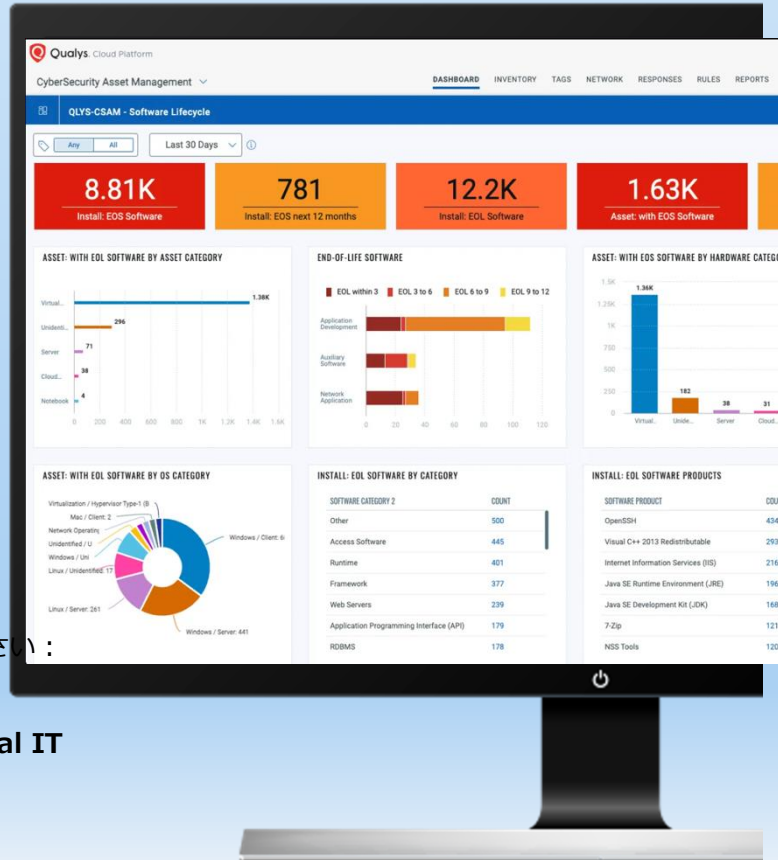
導入に適した業種・組織の例

- **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。

クォ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

主な機能

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

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

TruRiskの削減に対処する

パッシブおよびアクティブな対応を推進してリスクをより迅速に軽減します

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

Qualys.

Eliminate機能概要

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

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

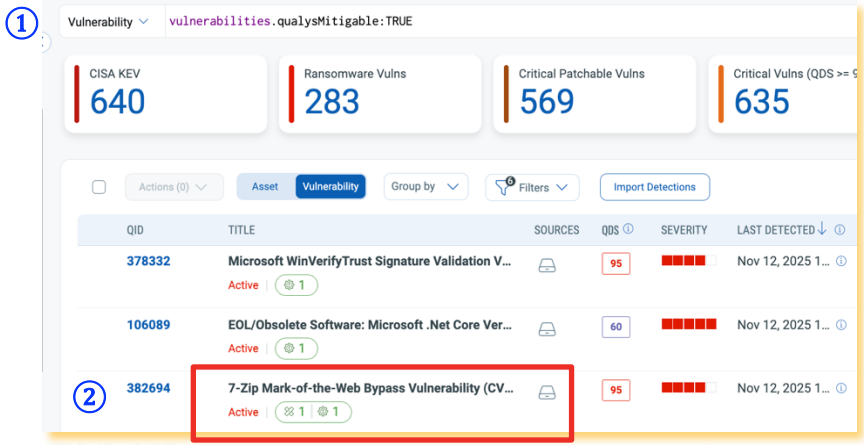
PM

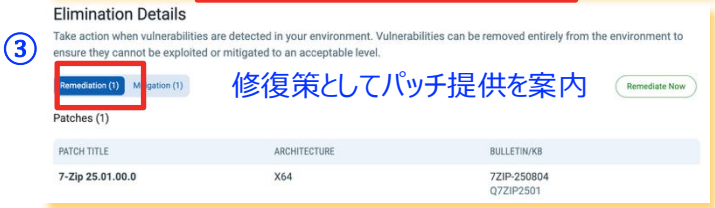
TRE

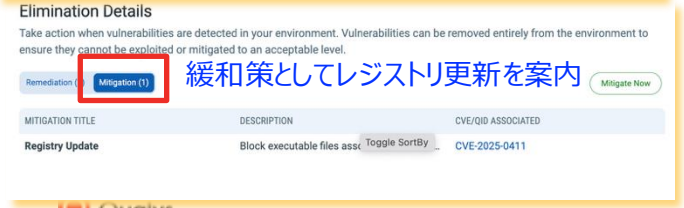
OSパッチ	3rd パーティパッチ	ゼロタッチオートメーション	リスクベースオートメーション
SCCM/Intune との統合	カスタム Mitigation (緩和策)/Remediation (修復)	Mitigate (緩和策)	Remote Shell
Cloud Remediation (クラウド上の修正)	ServiceNow や ServiceNow VRとの統合	古いバージョンのソフトウェアの発見と削除(java)	パッチがない場合の修復
面倒な脆弱性を解決するライブラリ	パッチ適用とコンフィグの変更	Isolate (隔離)	ソフトウェアのインストールとアンインストール

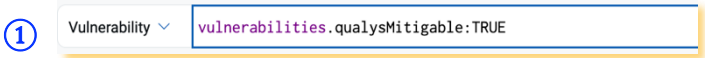
TruRisk Eliminate
UIの紹介

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。

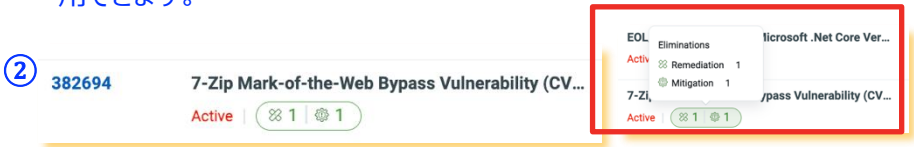








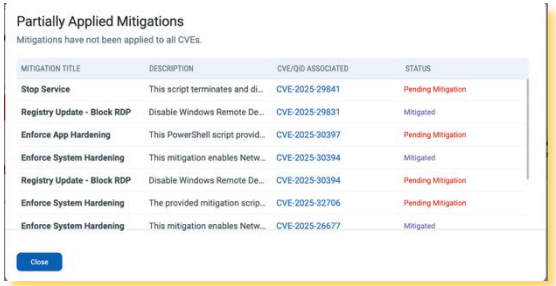
軽減できる脆弱性を検索するには、軽減に関連する**QQL**クエリを使用できます。



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

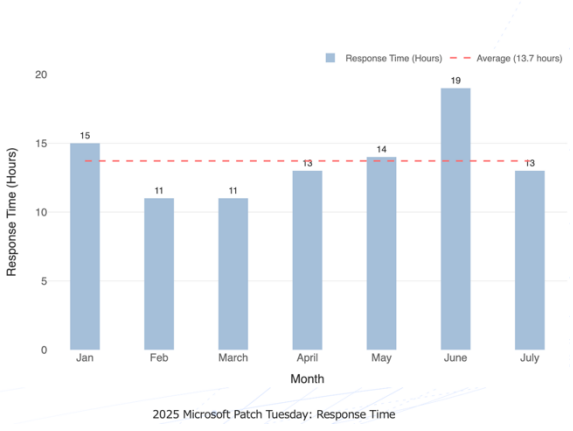
緩和策はCVE単位で案内されます。お客様の環境や状況に最も合う対策を選定できます。



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。



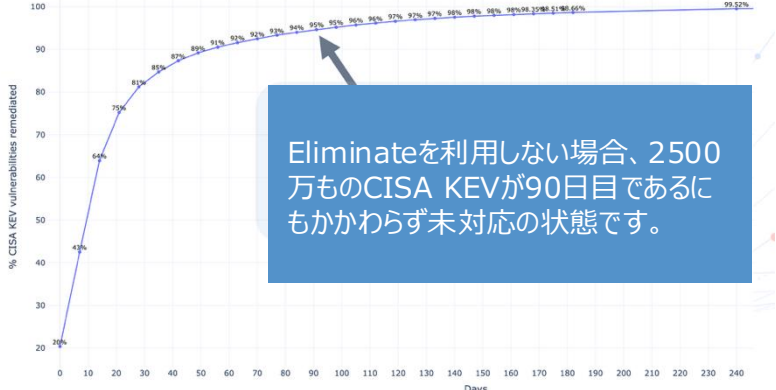
CISA の既知の悪用された脆弱性カタログのカバレッジ

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

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

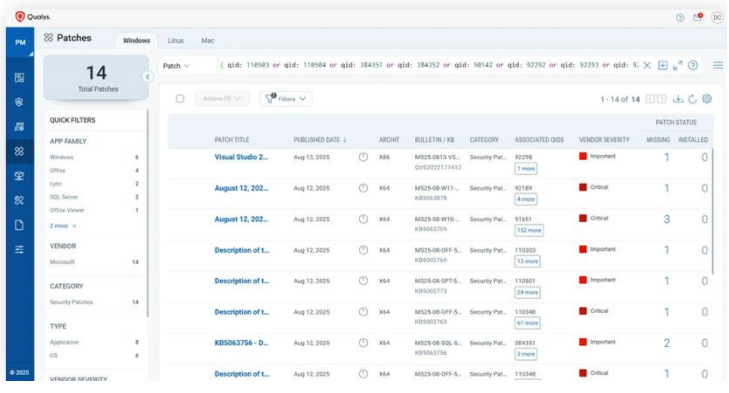
残りの1%(19のCVE)は、ほとんどがレガシー/オフマーケットテクノロジーであり、企業へのエクスポージャーは限られています。

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



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

パッチ管理：Patch Tuesday August 2025 [blog]



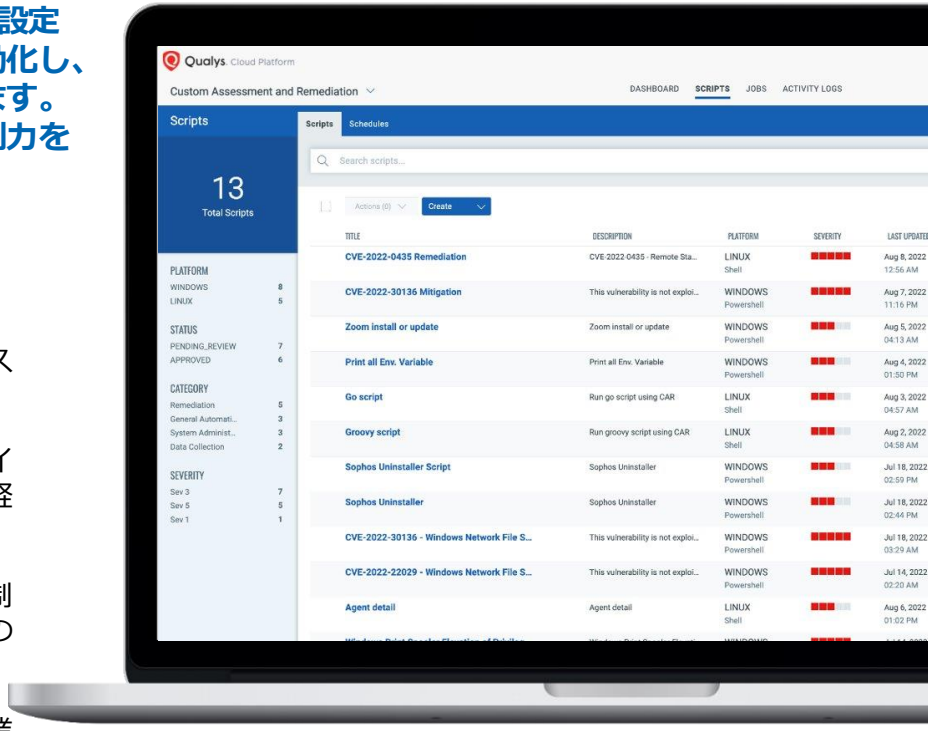
クォリスによるコンプライアンス

Policy Audit

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

コンプライアンスと構成管理

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



主なメリット

•リスク低減と迅速な対応
自動化されたチェックにより、潜在的なセキュリティ上の脆弱性や設定ミスを早期に発見できるため、重大なセキュリティ事故のリスクを削減します。

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

•内部統制の強化
組織内のセキュリティポリシーやガバナンスの整備を促進し、内部統制体制の強化に寄与します。また、経営層への報告や監査にも利用可能な信頼性の高い情報を提供します。

•柔軟な適応性
カスタマイズ可能なポリシー設定や各種業界標準への対応により、様々な業界や規模の組織に合わせた柔軟なコンプライアンス管理が可能です。

Qualys.

Qualys Policy Audit によるセキュリティ評価

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

■幅広いテクノロジーに対応

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

■ 多様な業界規制への対応

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

■ ポリシー定義

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

■コントロール

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

■評価

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

■レポート

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

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

Qualys

Qualys Policy Audit

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

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

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

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

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

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

自動化された監査対応レポート
常に監査準備の整ったレポートで手作業を削減

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

※詳しくはBlogをご覧ください

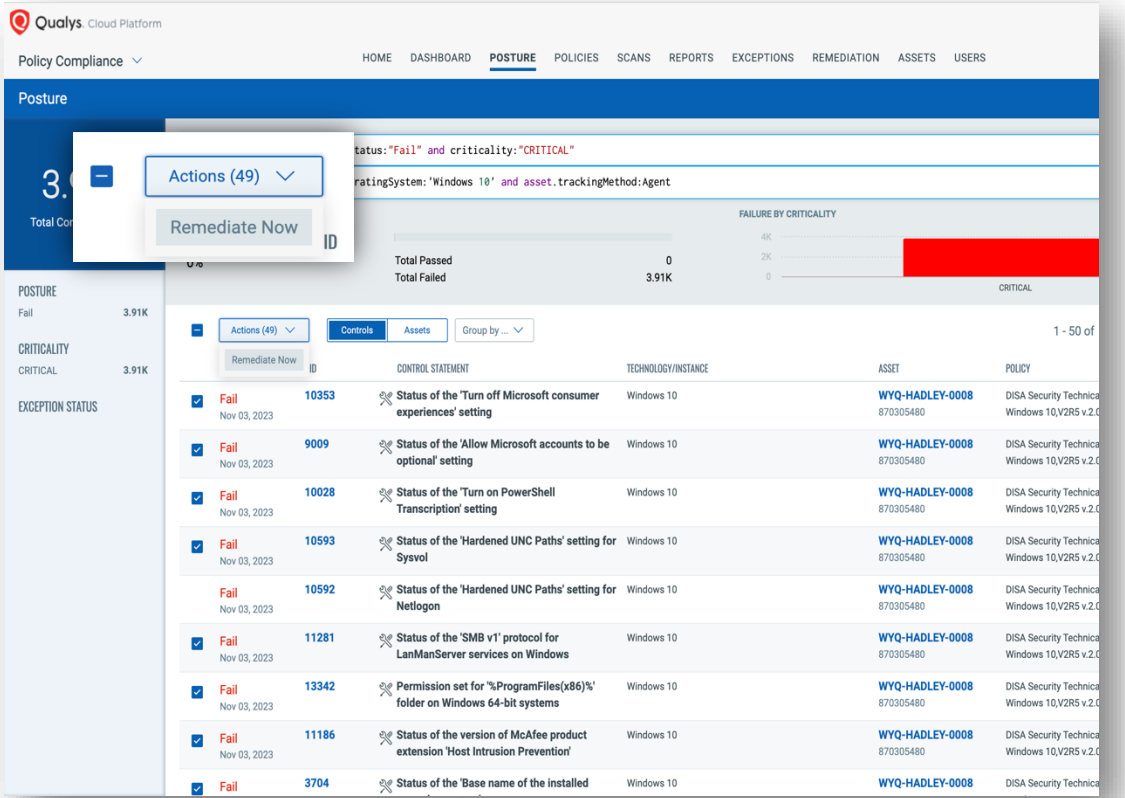
NIST 800-53 ISO FedRAMP GDPR PCI HIPAA

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.

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

規制

FedRAMP
GDPR
ISO
NIST 800-53
HIPAA
PCI

...などなど

Qualysのコンプライアンスポートフォリオ

Policy Audit
設定ミスを検出して修正

File Integrity Monitoring
インシデント管理と優先順位付けを自動化

PCI ASV Compliance
PCI コンプライアンスの自動化と簡素化

Security Assessment Questionnaire
ベンダーのリスクを評価/優先順位付け

SaaS Detection & Response
MS365 の設定ミスを評価

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

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

統合データプラットフォーム
データの正規化、インデックス作成、分類、強化

API および インテグレーション

コントロールセンター

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

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

Qualys

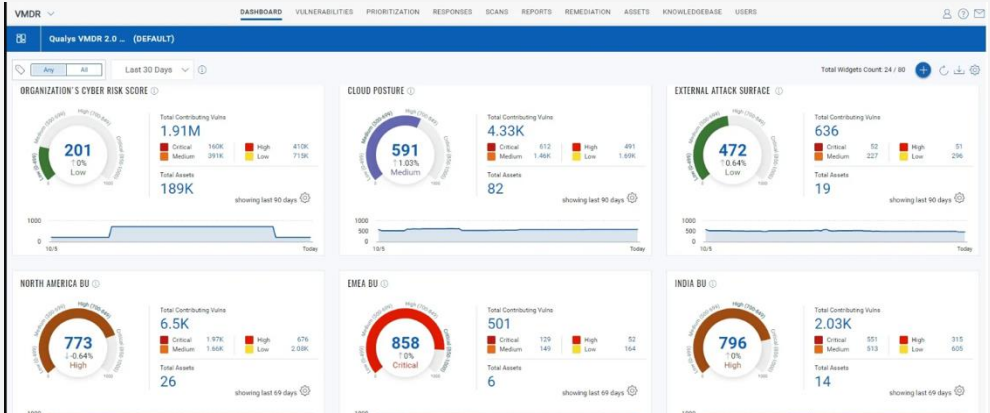
クォリスによるリスクベースの優先順位づけ

VMDR(脆弱性管理)とCSAM（資産管理）

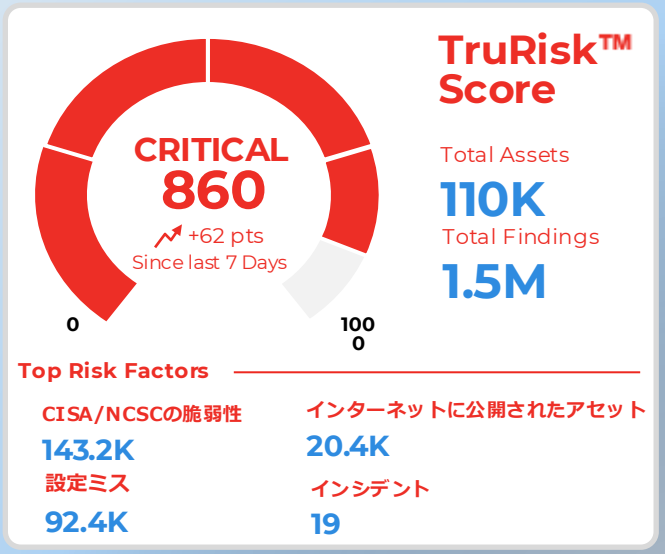
*CSAMはVMDRライセンスとの併用が必須です。

TruRisk™ 2.0による優先順位付け

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



TruRiskスコア構成要素

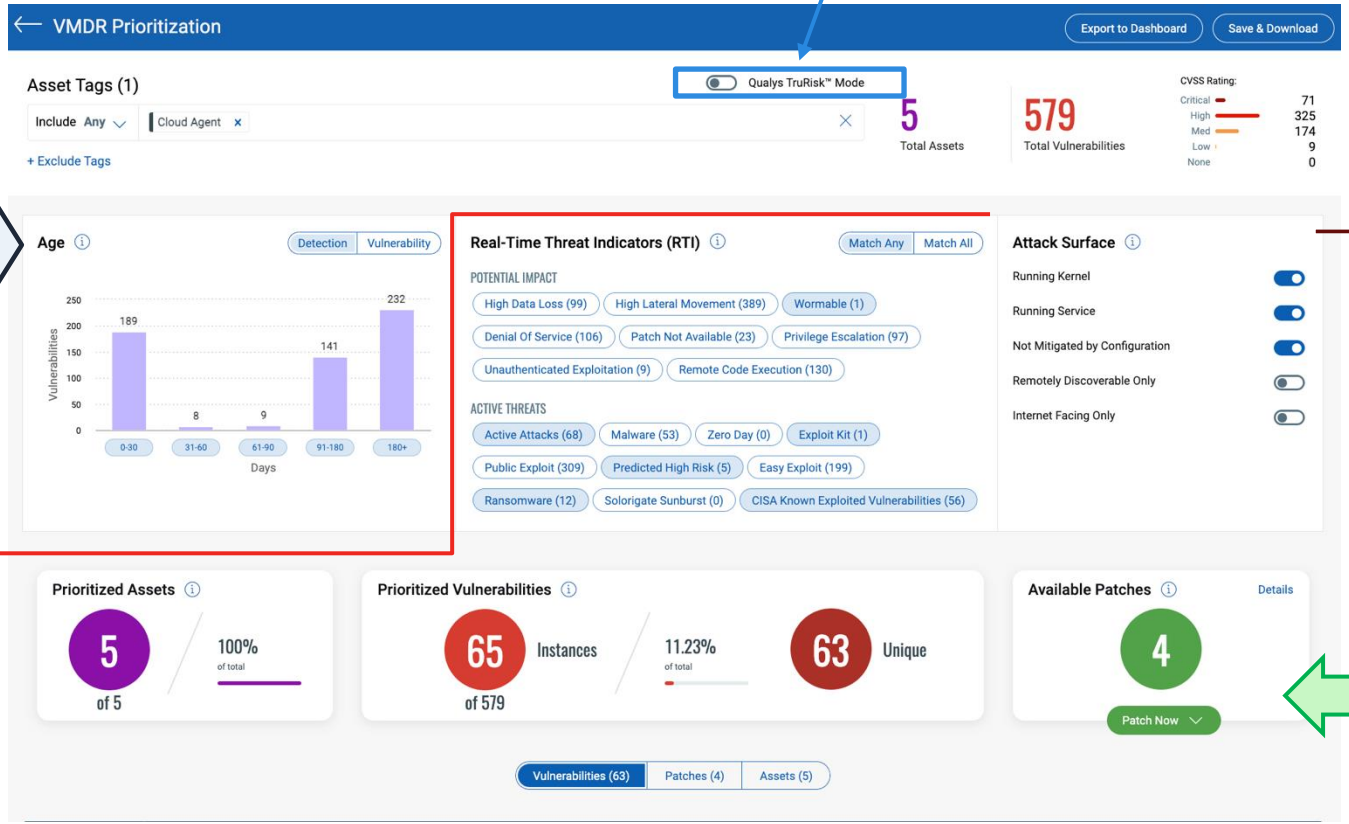


Qualys VMDR ：脆弱性スキャン + TruRisk優先順位
Qualys CSAM ：資産インベントリ × ビジネスリスク
Qualys Policy Audit：構成・設定のリスクをTruRiskスコアに反映
Qualys EASM：外部露出をトリガーとしたリスクスコア強化

脅威ベースの脆弱性対応と優先順位付け

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

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



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

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

適用可能なパッチの数が表示され、直ちに対策を取ることが出来ます。

Qualys.

MITRE ATT&CK マトリックスによる優先順位

攻撃者中心の視点を実現

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

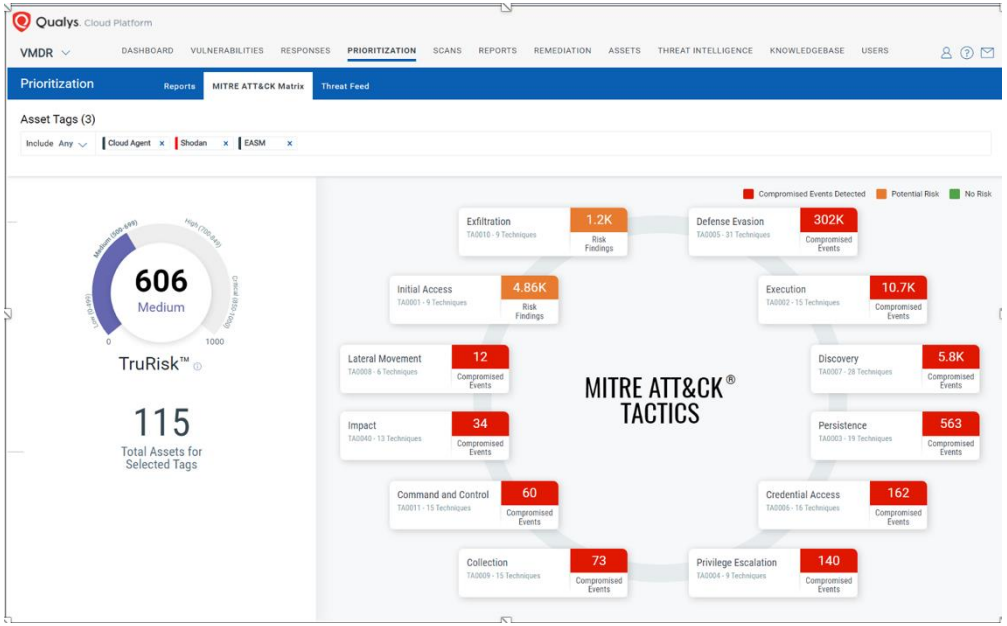
包括的なATT&CKビュー

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

攻撃経路の排除

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

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



Real-Time Threat Indicatorsによる優先順位

組織の課題

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

RTIの活用方法

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

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

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

潜在的な影響（Potential Impact）

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

アクティブな脅威（Active Threats）

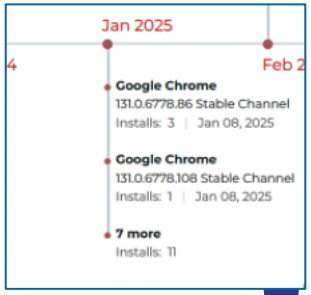
- **Active Attacks**：実際の攻撃が観測されています。
- **Malware**：この脆弱性に関連するマルウェアが存在します。
- **Zero Day**：実際の攻撃が観測され、ベンダーからのパッチが存在しません。
- **Public Exploit**：既知の悪用コードが公開されています。
- **Predicted High Risk**：機械学習を活用して、悪用されていない脆弱性の優先順位付けを行います。
- **Easy Exploit**：攻撃の実行が容易で、特別なスキルや詳細な情報が不要です。
- **Exploit Kit**：この脆弱性に関連するエクスプ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

Qualys TruRisk レポート

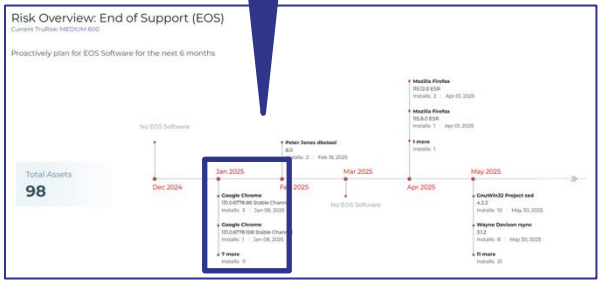
リスクに基づく脆弱性管理と戦略的なセキュリティガイダンス

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

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



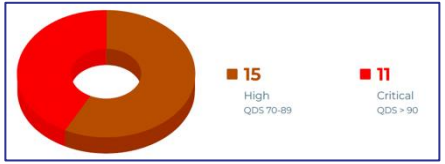
Risk Overview: EOS
2025年1月　Google Chromeのいくつかのバージョンとその他アプリケーションがEOSを迎えます。バージョンアップの計画を推奨します。

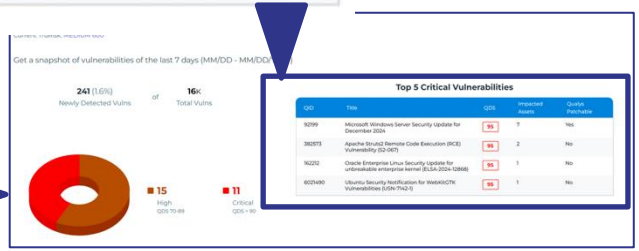


2025年6月4日 詳細はこちら

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

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





Qualys Threat Research Teamの主なハイライト

ディスカバリー&アワード

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

Qualys TRU Zero-Day Research/Discovery & Awards

Recognition and awards received by Qualys TRU:

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

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

Qualys TRU 脆弱性の発見例:

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

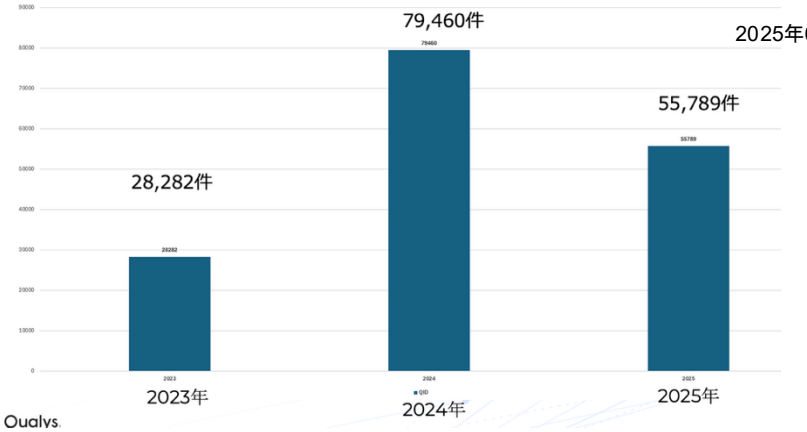
120,486
特定された脆弱性/CVE

269,890
検出シグネチャ(QIDs)

120+
脅威研究ユニット(TRU)の専門家

16 hrs
応答時間の中央値

QID リリース数(2023–2025 YTD)



2025年6月時点

2025年6月時点

ThuRiskを推奨する企業タイプ

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

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

Qualys.

クォリスクラウドエージェントの特徴

Cloud Agent

*Cloud AgentはVMDRライセンスが必須です。

Cloud Agent 対応サービス

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

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

Qualys.

Cloud Agent 対応プラットフォーム

業界で最も広範なカバレッジ

Windows
.exe (x86_64)

Windows
.exe (ARM64)

Linux
.rpm (x86_64)

Linux
.rpm (ARM64)

Linux
.rpm (ppc64le)

Linux
.deb (x86_64)

Windows
.exe (x86_64)

zSystems LinuxONE
.rpm (s390x)

zSystems LinuxONE
.rpm (s390x)

Mac
.pkg (x86_64)

Mac
.pkg (Apple Silicon)

BSD UNIX
.txz (x86_64)

AIX
.bff (POWER)

Solaris
.pkg (x86_64,SPARC)

CoreOS
.tar (x86_64)

ChromeOS
.apk (x86_64)

SQL Server

Oracle Database

- Qualys Only

Bottlerocket OS
.tar (x86_64)

Container-optimized OS by Google
.tar (x86_64)

GenToo
.tar (x86_64)

※ 対応OSプラットフォームはこちらをご参照下さい。

CAR– カスタムシグネチャによる検知と応答

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

■カスタムQIDを作成できます

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

■対優先対応による修復対応

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

■ユースケース

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

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

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

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

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

可視化からアクションへ

SwCAの機能強化によるソフトウェアサプライチェーンのセキュリティの向上

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

① リアルタイム製品・実行環境連携

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

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

どのOSSがどのアプリに使われているかを明確化。顧客関連アプリなど重要性に応じた優先順位付けが可能 。

修正までの所要時間を最大60%短縮。

③ C/C++バイナリ解析対応

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

④ スマートチケッティング連携

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

⑤ SBOM（CycloneDX形式）の自動出力

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

⑥ ランタイム可視化

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

⑦ エンタープライズ規模の対応力

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

Qualys.

6月16日ブログはこちら

SCA Security Configuration Assessment

VM

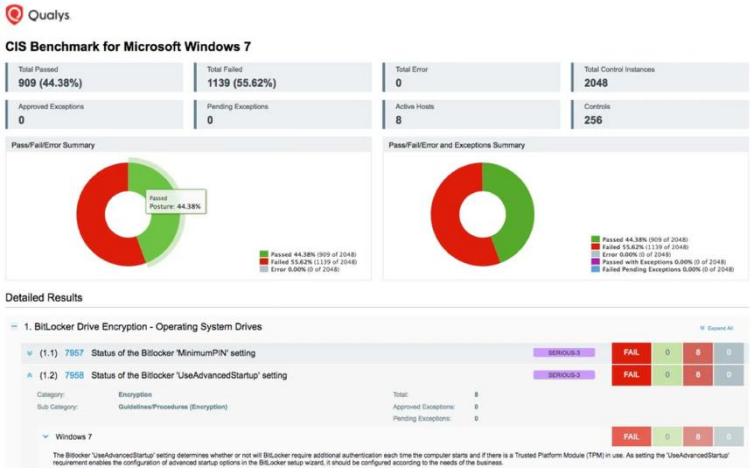
クラウドベースの構成管理とセキュリティ強化を実現する、統合型VM拡張ソリューション

SCA（Security Configuration Assessment）とは

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

SCAの導入手順

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



Qualys

EDR – Endpoint Detection and Response

強化された機能

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

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

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

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

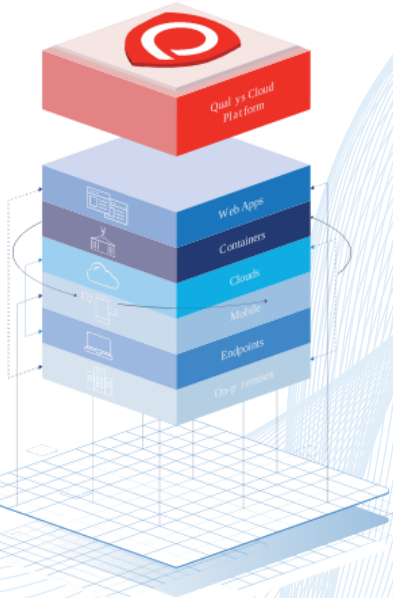
5. MITRE ATT&CK評価での高評価
Qualys EDRは、**2024年のMITRE ATT&CK評価**において、LockBitおよびCl0Pシミュレーションの主要ステップを**100%検出**し、**誤検出率も非常に低い**結果を達成しました。これにより、Qualys EDRの**高度な脅威検出能力と正確性が証明**されました。

EDR主要機能

Qualys Cloud Agentの品質、セキュリティ、安全性

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

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



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

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

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

仮想スキャナーを利用したCloud Agentの展開

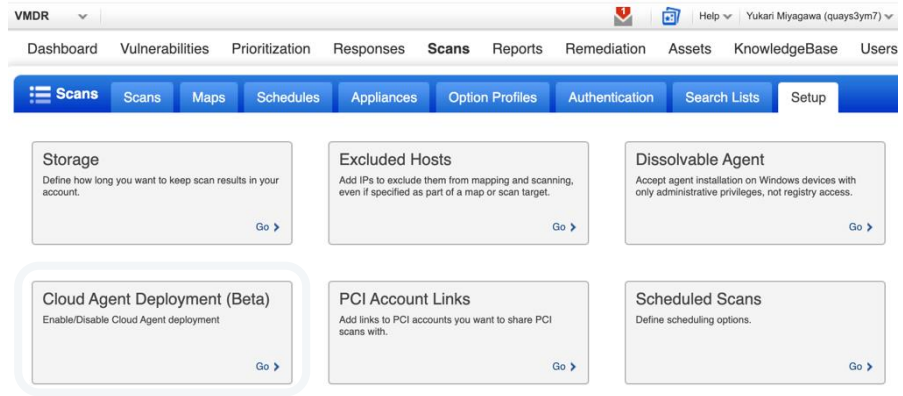
Qualys スキャナを使用すると、サードパーティのツールに頼ることなく、クラウド エージェントを展開できます。スキャナは、次のプラットフォーム タイプの Windows/Linux アセットにクラウド エージェントを展開できます。

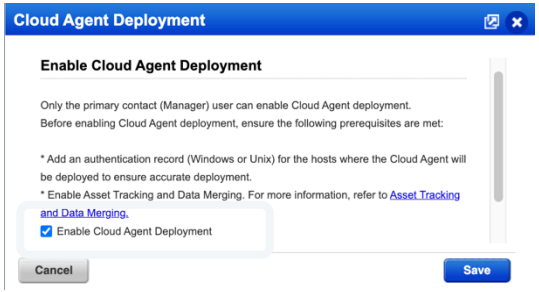
- Windows-X86-32/64
- Linux-X64-RPM
- Linux-X64-DEB

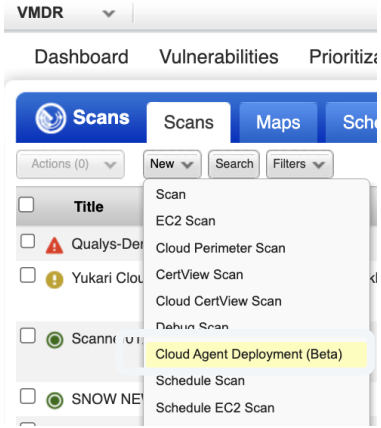
前提条件

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

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







参考資料：Deploy Cloud Agent Using Qualys Scanner

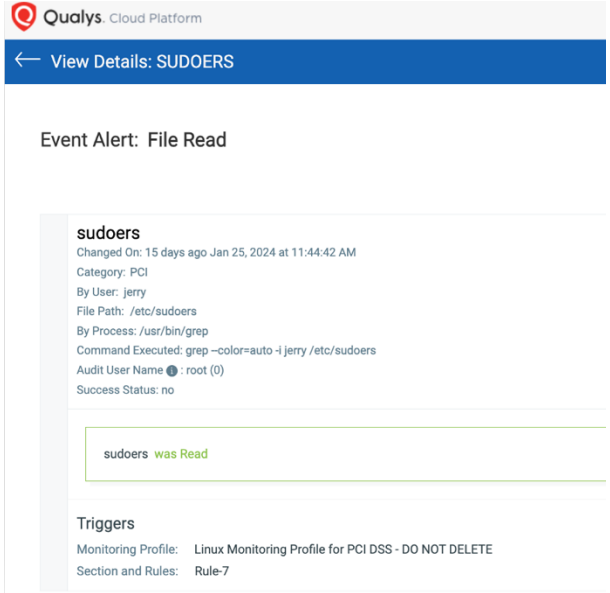
Qualys 補助資料

FIM

File Integrity Monitoring

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

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



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

Continuous Monitoring

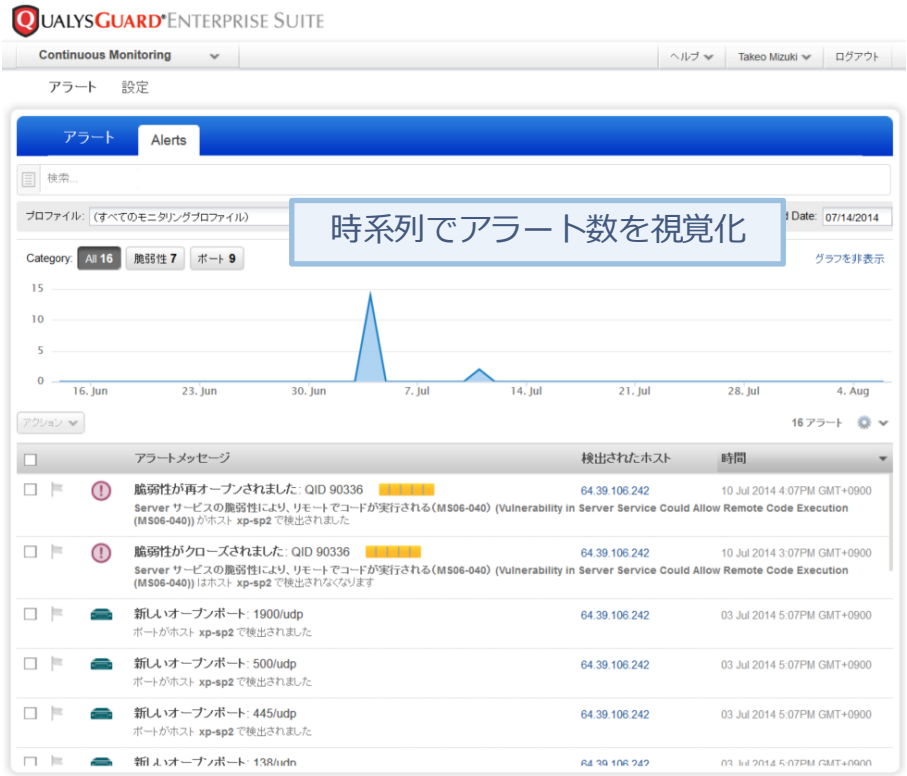
CM

■主な機能の説明

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

■アラート/監視対象ユースケース

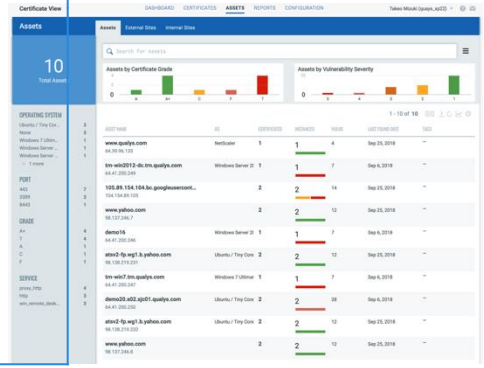
ユースケース	説明
新しい脆弱性の即時検知	公開サーバーに新しい脆弱性が追加された際に即通知、早期対応を可能に
シャドーITの検出	知らない資産がネットワークに追加された場合に検知し、管理外資産のリスクを可視化
構成変更の監視	特定ポートの開放やサービス起動など、ポリシーに違反する変更があれば即通知
攻撃対象領域の変化の把握	外部公開範囲に変化（DNS変更、新IP追加など）があった際に検出
コンプライアンス監査支援	設定逸脱や不正な変更を自動で記録・通知し、監査レポートの元データとして活用可能



CERT

CertView

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



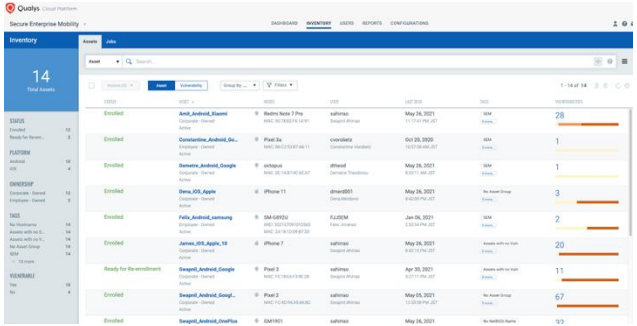
ユースケース	説明
期限切れ証明書の防止	有効期限が迫った証明書を検出し、事前に通知してサービス停止リスクを回避
シャドー証明書の特定	管理外の自己署名証明書や開発環境に残存する証明書を検出して統制強化
PCI DSS対応支援	弱い暗号スイートの使用検出により、コンプライアンス準拠を支援
ゼロトラスト環境での可視化	外部公開サービスやクラウドに設置されたSSL証明書も一括可視化し、セキュリティ強化
証明書ライフサイクル管理の最適化	所有者や用途ごとの分類により、更新・失効管理を効率化
攻撃対象領域の把握と削減	公開証明書から外部攻撃対象資産を特定し、リスクを低減

Mobile

VMDR Mobile

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

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

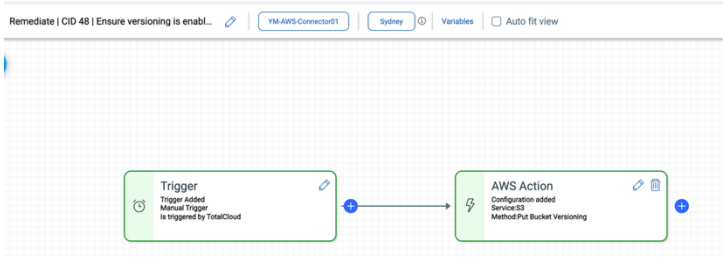


ユースケース	説明
BYOD環境のリスク可視化	私物端末の業務利用に伴うリスクを検出し、セキュリティポリシーの遵守を確認
アプリ脆弱性の早期検出	悪意あるアプリや既知の脆弱性アプリを可視化し、使用停止や通知を促す
インシデント調査支援	モバイル関連のセキュリティインシデント時に、構成・脆弱性情報から調査を迅速化
監査・レポート作成	モバイルポリシー違反の検出結果を元に、監査対応や外部報告用レポートを自動生成可能
セキュリティポスチャの統一管理	PC・サーバー・モバイルを1つのプラットフォームで横断的にリスク管理

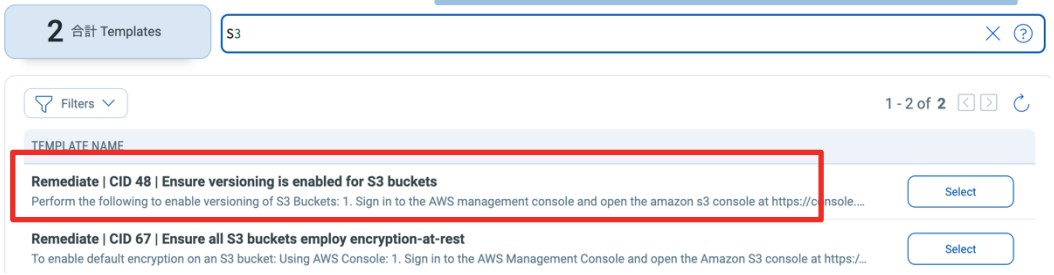
Qualys Flow

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

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



すぐに使える167のテンプレート



[Get Started with QFlow]

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

MAP

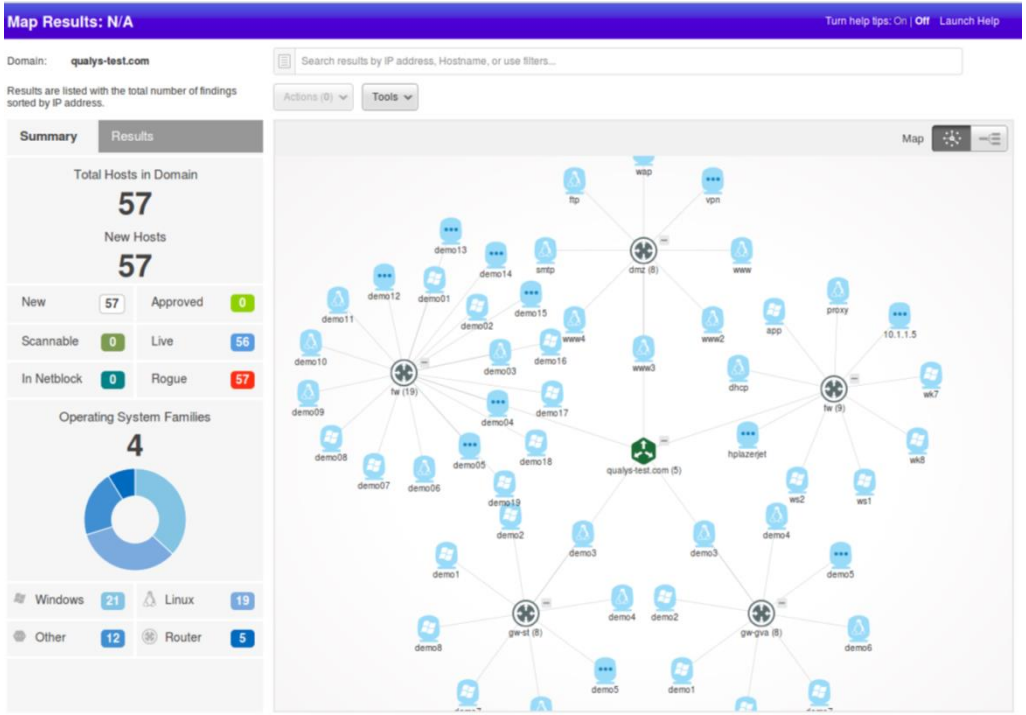
Qualys Mapping

IT資産の有無を正確に把握するための事前探索機能

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

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

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



Qualys.

Qualys Cloud Agent パッシブ センサーの紹介

CAPS

継続的に監視し、内部の攻撃対象領域を削減する

Windows及びLinuxの
Cloud Agentにて対応

単一、軽量、拡張可能、自己更新、集中管理型エージェント

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

ネットワークタップの制限から逃れる

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

パッシブセンシング

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

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

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

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

Qualys.

＊CAPSを使用するにはCSAMライセンスが必要です。

Qualys Passive Sensor の概要

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

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

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

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

Unit Managerによるアクセス管理

主な機能と権限

Unit Managerには以下のような権限が付与されます

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

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

3．レポート管理
- スキャン結果のレポート作成・編集・削除・配布

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

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

利用シーンの例

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

注意点

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

TAGによるアクセス管理

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

◎ ロールベースアクセス制御（RBAC）との連携

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

例）**Readerユーザーの制限**

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

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

TAGの種類と使い方

◆ **静的タグ** 手動で資産に割り当てる

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

◆ **動的タグ**条件に基づいて自動的に資産にタグを付与

例：OSがWindowsかつIPが特定範囲
→ Windows-Tokyo

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

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

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

受賞歴と業界からの評価

Qualys®

受賞歴と業界からの評価

2025 KuppingerCole Leadership Compass for ASM

Highest-rated Leader

CSAM

2024 Frost Radar for EASM

Leader

CSAM

2025 Gigaom Radar for Patch Management

Leader with the highest value

Eliminate

2025 KuppingerCole Leadership Compass on API Security and Management

Leader

TotalAppSec

2025 IDC MarketScape for Exposure Management

Leader

ETM/ROC/VM

2025 Gartner Magic Quadrant for Exposure Assessment Platforms

Leader

ETM/ROC/VM

2025 Frost Radar for VM

Leader

ETM/ROC/VM

2025 Info-Tech Data Quadrant for VM

Champion & Highest-rated vendor

ETM/ROC/VM

2025 Info-Tech Emotional Footprint for VM

Champion & Highest-rated vendor

ETM/ROC/VM

2025 LatioTech Cloud Security Research

CTEM Leader

ETM/ROC/VM

2025 LatioTech CTEM & Cloud Security Research

Combined Leader

ETM and TotalCloud

Qualys.

受賞歴と業界からの評価

2025
KuppingerCole Leadership Compass for CNAPP

Leader

TotalCloud

2025
Gigaom Radar for Container Security

Leader and Outperformer

TotalCloud

GIGAOM

2025 Gigaom Radar for Cloud Workload Security

Leader and Outperformer

TotalCloud

GIGAOM

2025
Gigaom Radar for CNAPP

Leader and Outperformer

TotalCloud

FROST & SULLIVAN

2025
Frost Radar for CSPM

Leader

TotalCloud

FROST & SULLIVAN

2025
Frost Radar for CWPP

Leader

TotalCloud

2025
LatioTech Cloud Security Research

Cloud Security Ecosystem Leader

TotalCloud

IDC

2025
IDC Marketscape for CNAPP

Major Player

TotalCloud

Gartner peerinsights

2024
Gartner Voice of the Customer for CNAPP

Highest-rated vendor

TotalCloud

Gartner

2025
Gartner Market Guide for CNAPP

Representative Vendor

TotalCloud

2025
Gigaom Radar for ASM

Leader

CSAM

Qualys.

受賞歴と業界からの評価

Qualys Recognized As One of 20 Coolest Cloud Security Companies Of The CRN 2025 Cloud 100 (#13)

Winner

As part of CRN's Cloud 100, Qualys was named as a top cloud security company to know about in 2025

https://www.crn.com/news/security/2025/the-20-coolest-cloud-security-companies-2025-cloud-100?page=13

Qualys TotalCloud wins Best Cloud Security Solution at SC Awards Europe 2025

Winner

Qualys TotalCloud receives the top accolade in the Best Cloud Security Solution category

https://www.qualys.com/company/newsroom/news-releases/usa/qualys-solutions-recognized-for-exceptional-performance-at-sc-awards-europe/

Qualys VMDR awarded Best Vulnerability Management Solution for third consecutive year at SC Awards Europe 2025

Winner

Qualys Solutions Recognized for Exceptional Performance

https://www.qualys.com/company/newsroom/news-releases/usa/qualys-solutions-recognized-for-exceptional-performance-at-sc-awards-europe/

Qualys TRU wins prestigious Pwnie Award for "Epic Achievement" at DefCon 2025

Winner

Qualys Honored for Groundbreaking Cybersecurity Research

https://blog.qualys.com/qualys-insights/2025/08/12/two-pwnie-awards-one-crucial-lesson-what-our-openssh-research-reveals-about-cyber-defense-in-2025

Qualys TRU wins Pwnie Award for "Best Remote Code Execution (RCE)" at DefCon 2025

Winner

Pwnie Award wins underscore Qualys TRU's leadership in cybersecurity research and commitment to responsible vulnerability disclosure

https://blog.qualys.com/qualys-insights/2025/08/12/two-pwnie-awards-one-crucial-lesson-what-our-openssh-research-reveals-about-cyber-defense-in-2025

Qualys wins Best Regulatory Compliance / Enterprise Risk Management Solution at the Italian Security Awards 2025

Winner

Award highlights the best security vendors in Italy, selected based on direct feedback from 8,500 end users

https://www.securityopenlab.it/news/5643/italian-security-awards-2025-il-premio-al-meglio-della-cybersecurity-italiana,raddoppia.html

Qualys Achieves **FedRAMP High** Authorization for Comprehensive Risk Management Platform

Recognition

Leading cyber risk management company meets the highest federal standard to serve its growing public sector customer base

https://www.qualys.com/company/newsroom/news-releases/usa/qualys-achieves-fedramp-high-authorization

25+年間業界をリード

Your Partner in Cyber Risk Management

126M+
Ransomware Detections

10,000+
Subscription Customers

12.2 B+
Vulnerabilities Detected

9B+
IP scans in a year

140M+
Patches Deployed by Qualys Customers

Qualys | De-risk Your Business

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