Qualys VMDR
クラウドプラットフォーム & ソリューション概要

Qualys Japan K.K

2023.11

目次

- VMDRとアセットインベントリ
- VMDR 2.0 with TruRisk
- CSAM +EASM
- TotalCloud (CNAPP)
- 補助資料
- マーケット情報

Qualys VMDRとアセットインベントリ

Qualys Japan K.K

2023.09

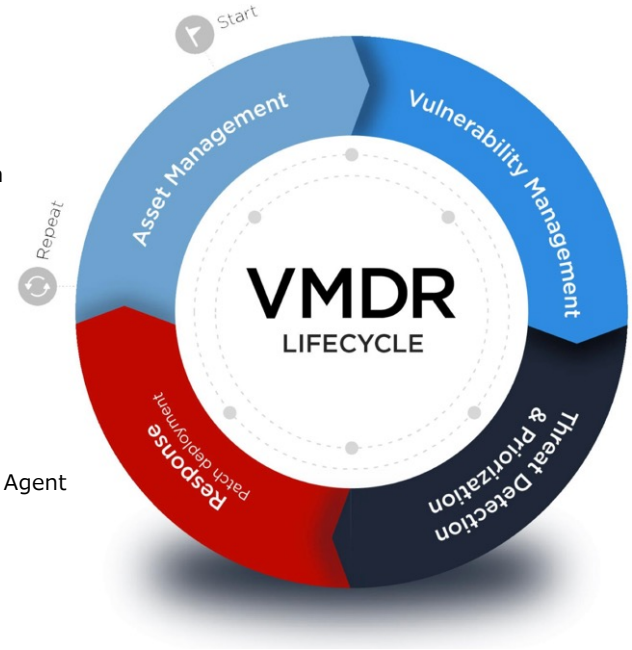
Qualys VMDRとは

Vulnerability Management Detection & Response

アセット管理、脆弱性管理、脅威による優先順位づけ、パッチ対応という脆弱性管理の
ライフサイクルに必要な４つのプロセスを一つにまとめた次世代脆弱性管理パッケージ

■ … 同梱
□ … オプション

■Asset Discovery
■Asset Inventory
-On-prem Device Inventory
-Certificate Inventory
-Cloud Inventory
-Container Inventory
-Mobile Device Inventory
■Asset Categorization & Normalization
□Enriched Asset Information
□CMDB Synchronization



■Vulnerability Management
■Configuration Assessment
■Certificate Assessment
□Additional Assessment Options
-Cloud Security Assessment
-Container Security Assessment

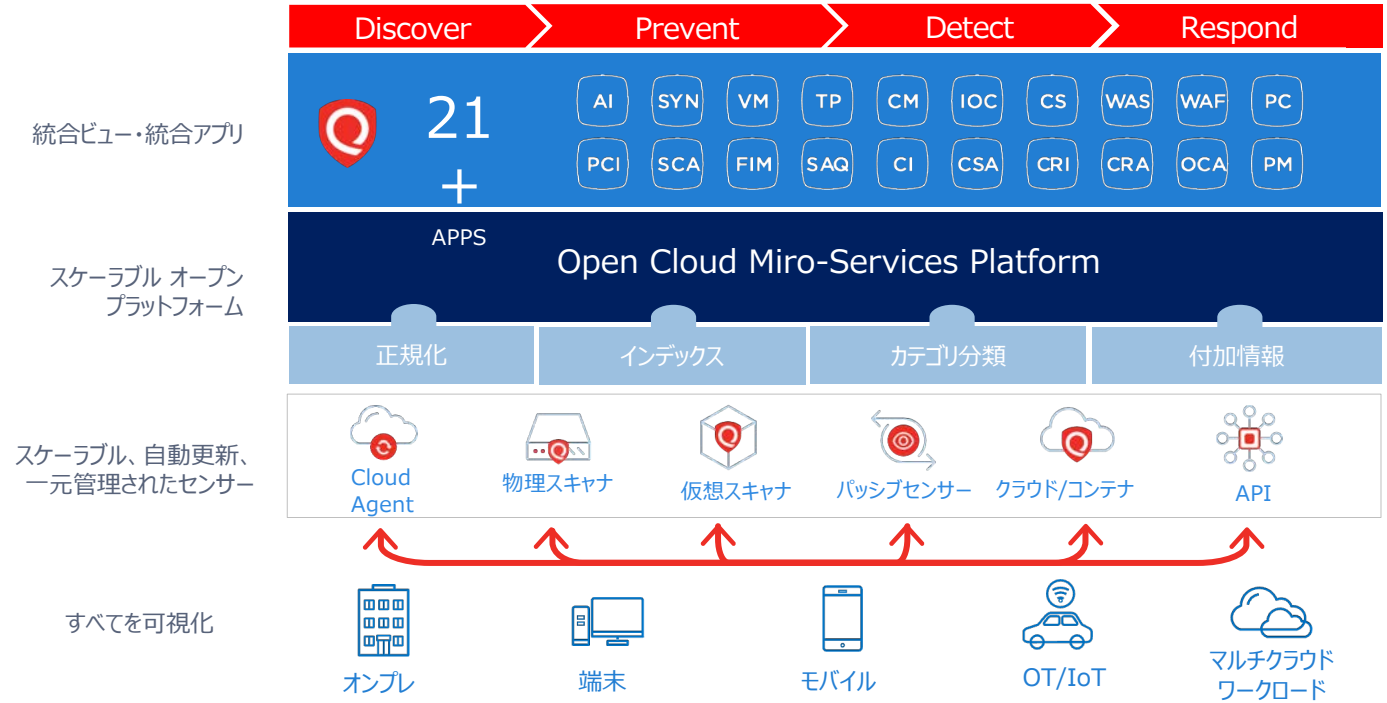
■Patch Detection
□Patch Management via Qualys Cloud Agent
□Container Runtime Protection
□Mobile Device Management
□Certificate Renewal

■Continuous Monitoring
■Threat Protection

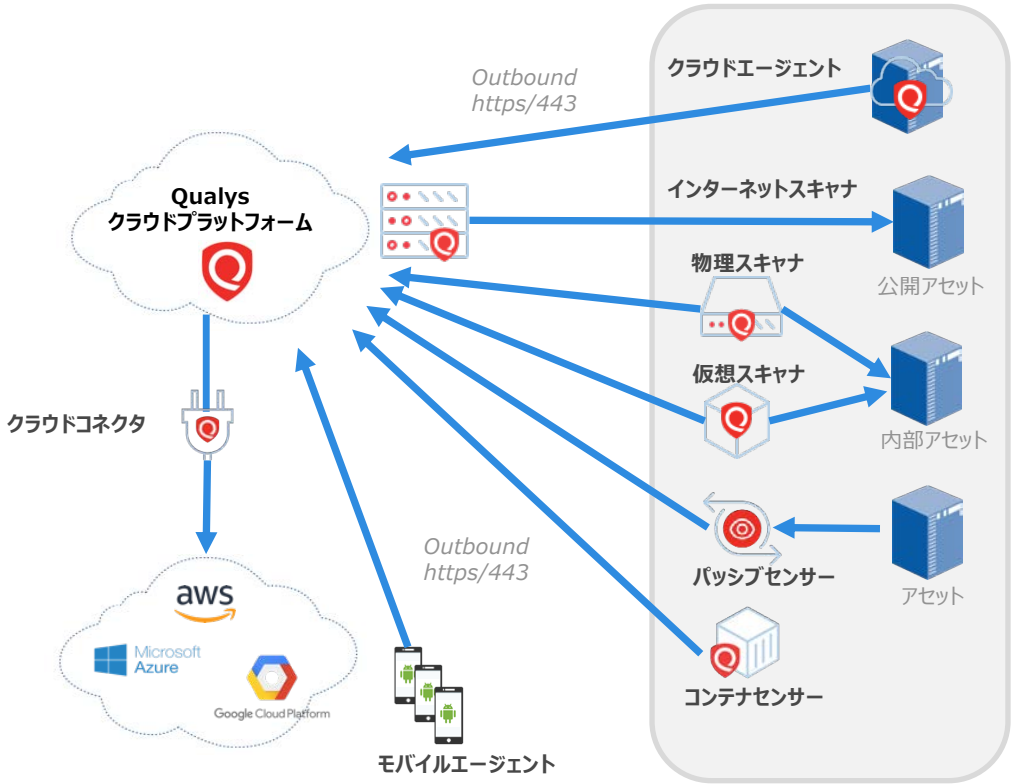
Qualys.

Qualys クラウドセキュリティプラットフォーム

IT, セキュリティ, コンプライアンスを 1 つのプラットフォームで統合管理



Asset Discovery



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。

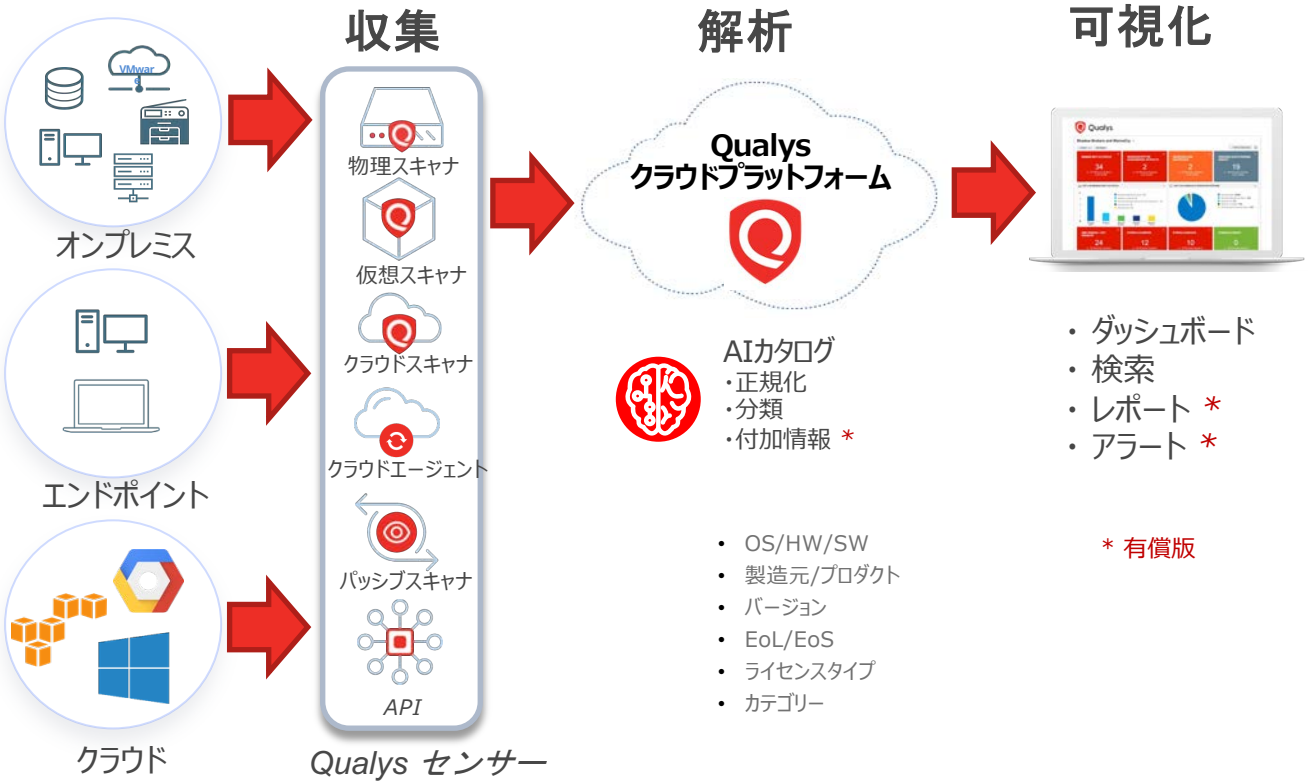
⑤ クラウドコネクタ
AWS/Azure/GCPにネイティブAPIで接続し、クラウド上のリソース情報を収集。

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。

Qualys.

Asset Inventoryとは

- 配置したセンサーからアセットインベントリー情報（ハードウェア、OS、アプリケーション）を収集



Qualys.

Qualys VMDR2.0 with TruRisk

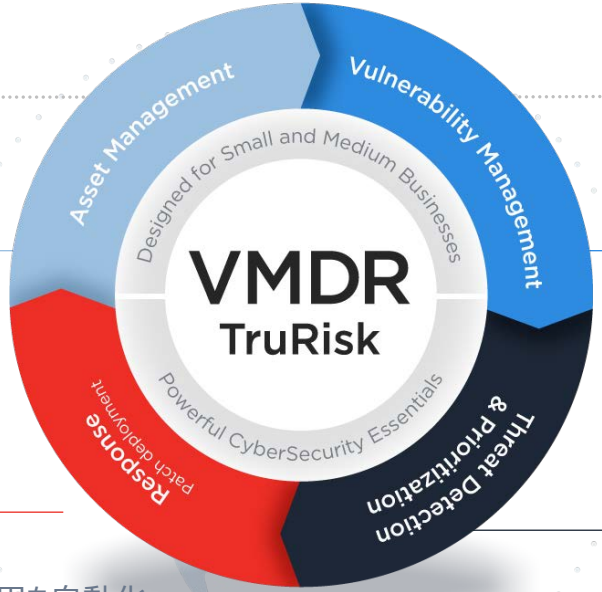
Cloud-Native Application Protection Platform　(VMDR)

VMDR TruRisk の紹介

中小企業向けのエンタープライズ グレードのセキュリティ

New!

Qualys TruRisk™
+
Automated Workflows
Risk-Based Prioritization



攻撃対象領域全体をカバー

- オンプレミスまたはクラウド上のすべての資産を把握し、OS、アプリケーション、および 100 以上の属性に基づいて分類します

脆弱性と構成評価

- 脆弱性をリアルタイムで自動検出。
- PCI,HIPAA,CISなどを含むほぼ全てのコンプライアンス管理とレポート化を実現。
- SSL 証明書の有効期限を監視。ビジネスの停止、証明書の在庫管理、期限切れの証明書の更新を防ぎます。

自動修復

- クラウドおよびオンプレミスの資産 へのパッチ適用を自動化
- ProtectITを使用し、ランサムウェアやマルウェアの感染を自動的にブロック
- 修復時間を半分に短縮。最大 40% 高速化

リスクベースの優先順位付け

- 25 を超える脅威インテリジェンス フィードを使用したリスクベースの優先順位付けを活用することで、重大な脅威を最大 5 倍の速さで検出。
- ProtectIT を使用してマルウェアやランサムウェアの感染を自動的にブロックします。

The Qualys TruRisk Platform

Asset Management

Outside-in アセットの可視化

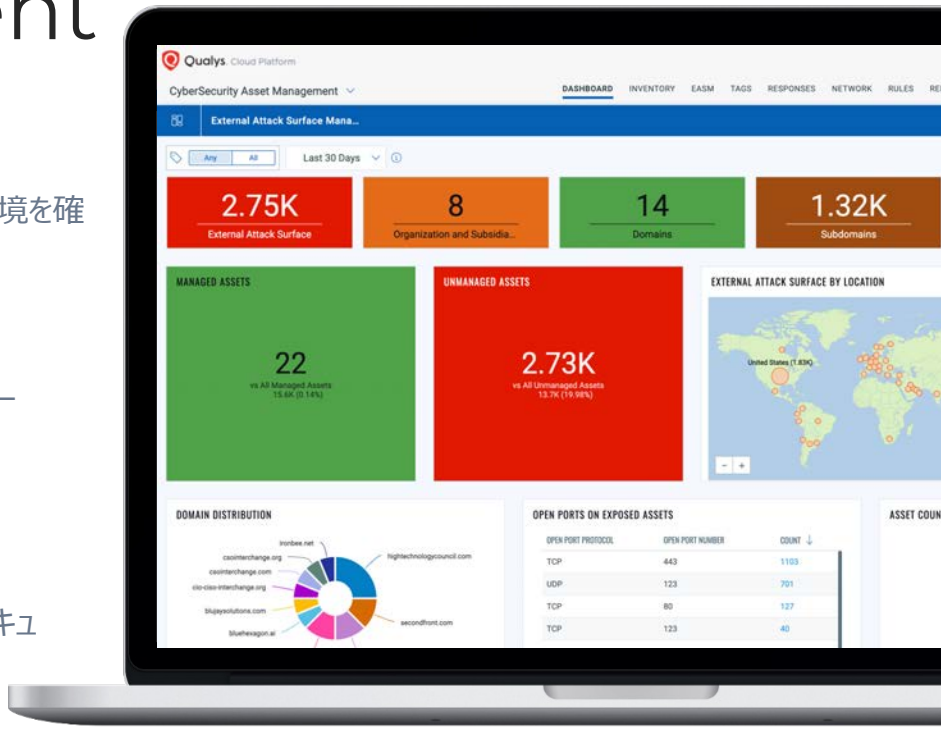
攻撃者が外部攻撃対象領域管理を使用する場合と同じように、環境を確認します。

Inside-out アセットの可視化

防御側の視点からギャップとリスクを特定することで、包括的なサイバー資産攻撃対象領域ソリューションを実現します。

シームレスに統合

ITSM、CMDB、チケット発行ツールとの双方向統合により、IT とセキュリティのギャップを埋める



The Qualys TruRisk Platform

Risk-Based VM

VM & Configuration Management

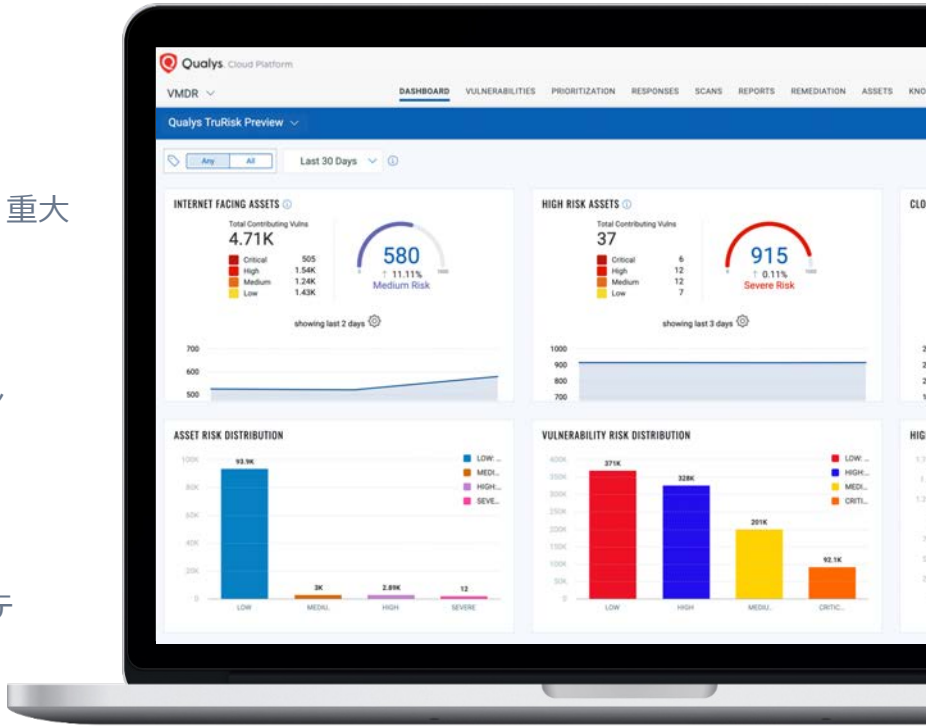
露出、悪用可能性、証拠に基づいた優先順位付けを組み合わせて、重大な脆弱性を 85% 削減します

Unified Cybersecurity Risk Score

サードパーティのセキュリティおよび IT ツールからデータを取り込み、コンテキストに基づいた実用的なリスク洞察を得ることができます。

Threat Prioritization

Qualys TruRisk スコアリング手法を補完する 25 以上の脅威インテリジェンス フィードを活用



The Qualys TruRisk Platform

Risk Remediation & Patching

Integrated Patch Management

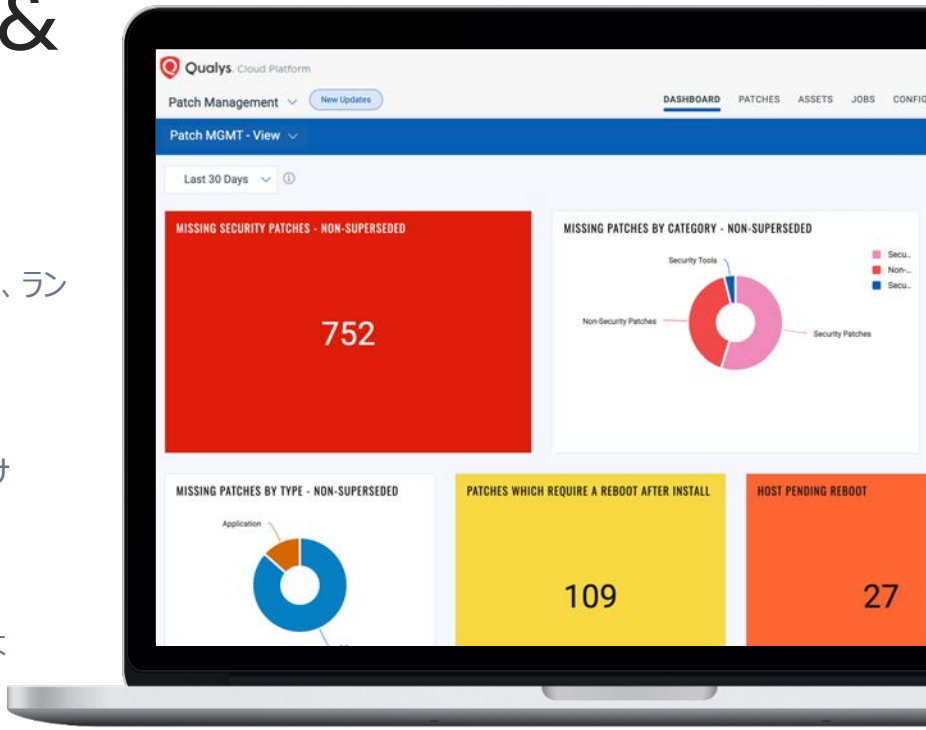
1 つのエージェントを利用して、TruRisk または脆弱性の種類 (別名、ランサムウェア、CISA など) に基づいてパッチを適用します

Patchless Protection

構成ミスの特定、スクリプトの実行、カスタム アプリの展開などにより、サイバーセキュリティ リスクを修復します。

Workflow-based Remediation

Qualys Custom Assessment and Remediation (CAR) による IT セキュリティ コラボレーションの運用化



The Qualys TruRisk Platform

Threat Detection & Response

Zero-day Protection

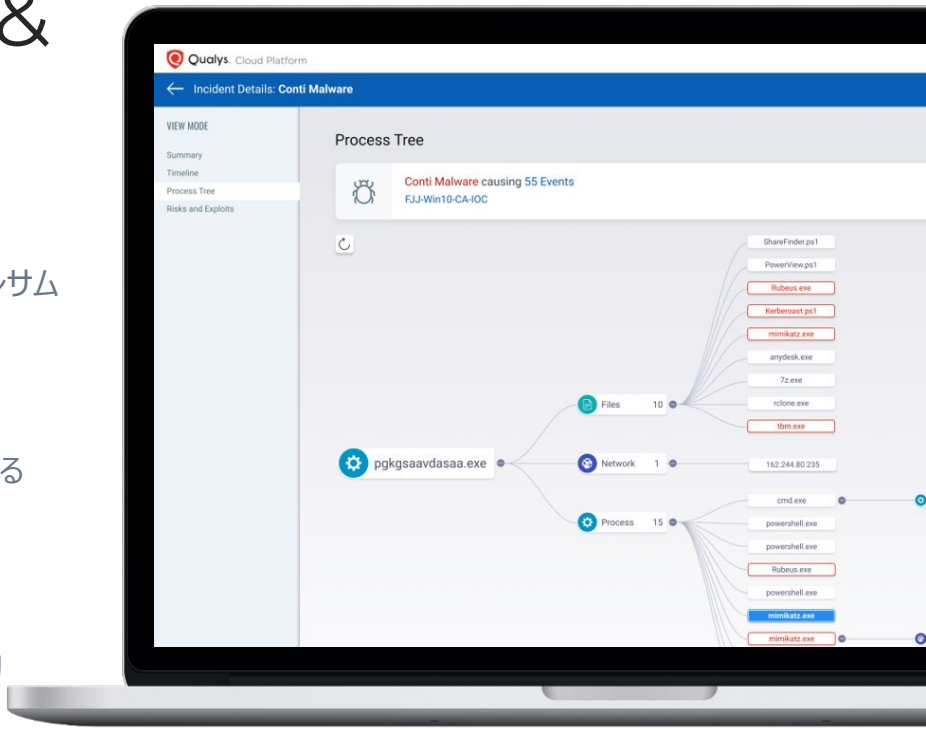
動作と ML ベースのウイルス対策機能を活用して、エクスプロイト、ランサムウェア、フィッシング攻撃、ゼロデイ攻撃を阻止します。

Multi-Vector EDR & EPP

エンドポイントの脅威を関連付けて、環境内で積極的に悪用されている脆弱性を特定します

Automation & Orchestration

エンタープライズ統合 (つまり、SIEM、ITSM、CMDB) による包括的なエンドポイント (EDR) およびクラウドの検出と対応



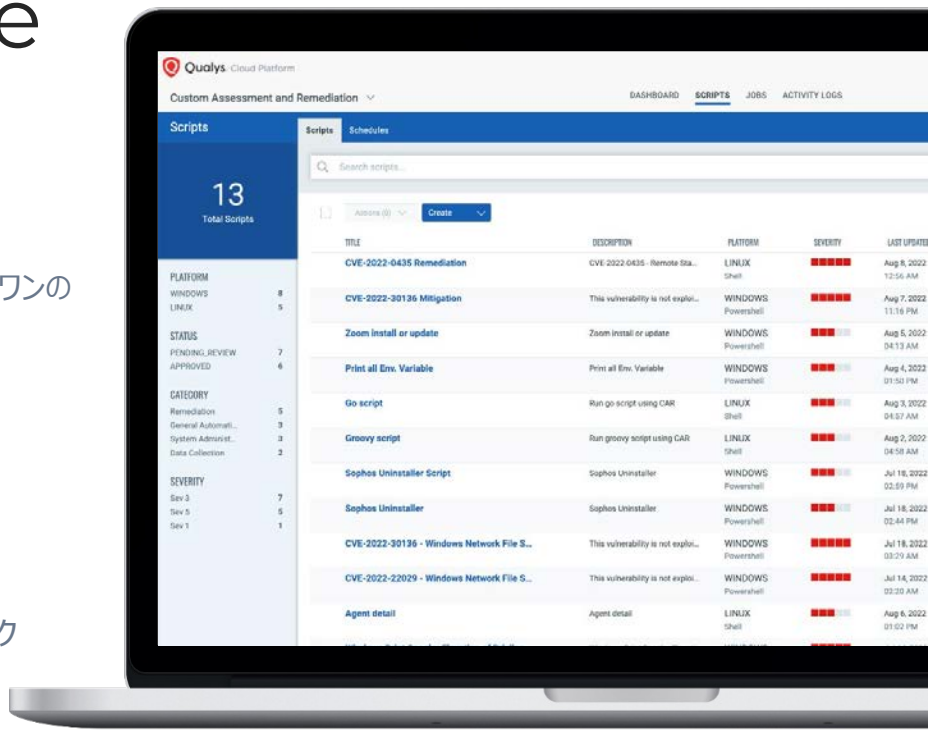
The Qualys TruRisk Platform

Policy Compliance & Configuration

Always Audit-Ready
VM と ASM をコンプライアンス管理とシームレスに統合するオールインワンのリスク プラットフォーム

Continuous Posture Management
何百もの政策および規制の枠組みにマッピングされた管理

Compliance-to-Risk Measurement
データ保護、RDP、暗号化、アクセス制御、不正なサービスなどのリスクに対する CIS の構成ミスの優先順位付け



Qualys CSAM +EASM

Cybersecurity Asset Management（CSAM）

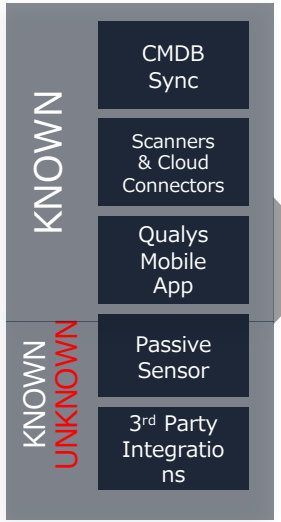
CSAM 2.0特長

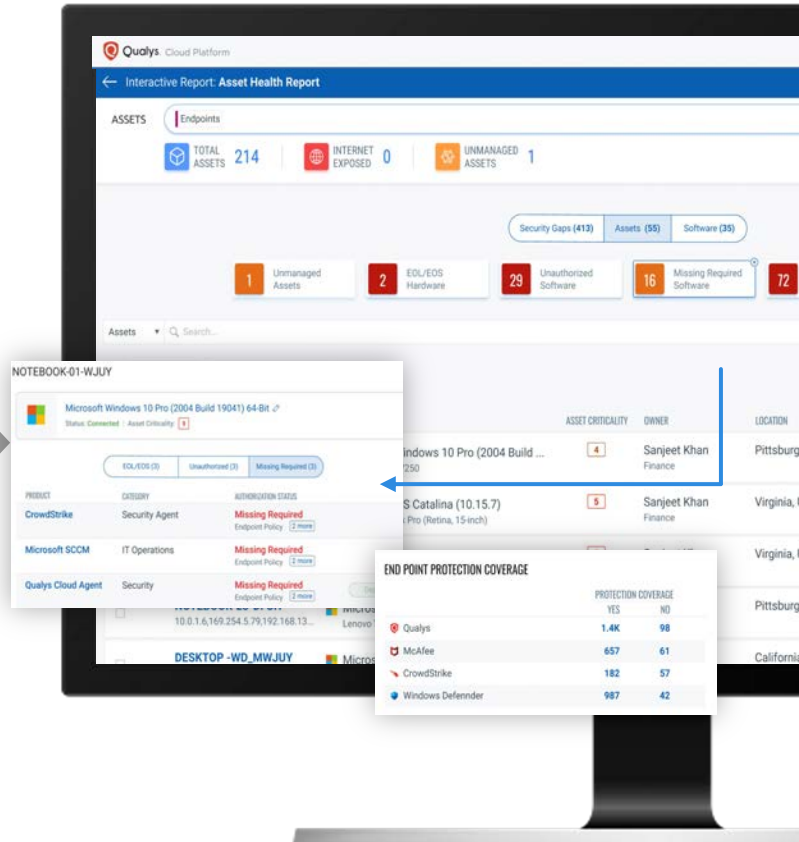
1. ビジネスコンテキストを使用した資産検出とインベントリ

2. 資産集約とインテリジェンスのためのサードパーティ統合
   - Jira, ServcieNow, Active Directory, bmc helix, webhooks

3. セキュリティギャップの検出と資産の健全性の監視
   - EoL/EoS を管理する
   - エージェントカバレッジの検索
   - 許可されていないソフトウェア

4. Qualys TruRisk によるリスクベースの優先順位付けと修復ワークフロー



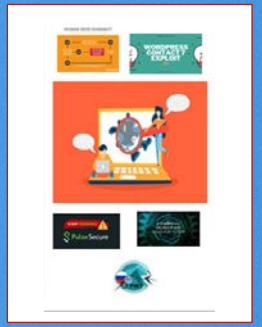


+ External Attack Surface Management (EASM)

- 「これまで知られていなかった」資産を検出
- 不明なアセット、ドメイン、サブドメインが見つかったときにアラートを出す
- ビジネスコンテキストとリスクを備えた充実した資産データを活用
- VM のワンクリック オーケストレーションで迅速に導入

ネイティブに統合された外部攻撃対象領域管理 (EASM) を備えた Qualys CSAM 2.0 により、お客様は、攻撃者が使用するものと同じ実用的なインテリジェンスを使用して、オンプレミス、クラウド、およびハイブリッド ネットワーク全体のサイバーセキュリティ体制を継続的に検出、分類、修復し、測定可能な形で改善することができます。

エンティティの検出/監視 ▸ サービス / 脆弱性発見 ▸ リスク/攻撃の予測



ドメイン、関連ドメイン、およびサブドメイン

WHOIS レジストラ

ドメインの作成日と有効期限を含む DNS レコード

生きているIP

追加のトップレベルドメイン (TLD)

ホスティングプロバイダー

シャドーIT

忘れられたアプリケーション

レガシーサービス

Qualys TotalCloud の概要

Cloud-Native Application Protection Platform （CNAPP）

Cloud Securityの課題

大規模かつ動的な攻撃対象領域

クラウドは、マルチクラウドにわたる一時的なワークロードを伴う一時的な環境です

可視化の欠如

クラウド環境の全体像を把握することは困難

新しいコンプライアンス/ベンチマーク

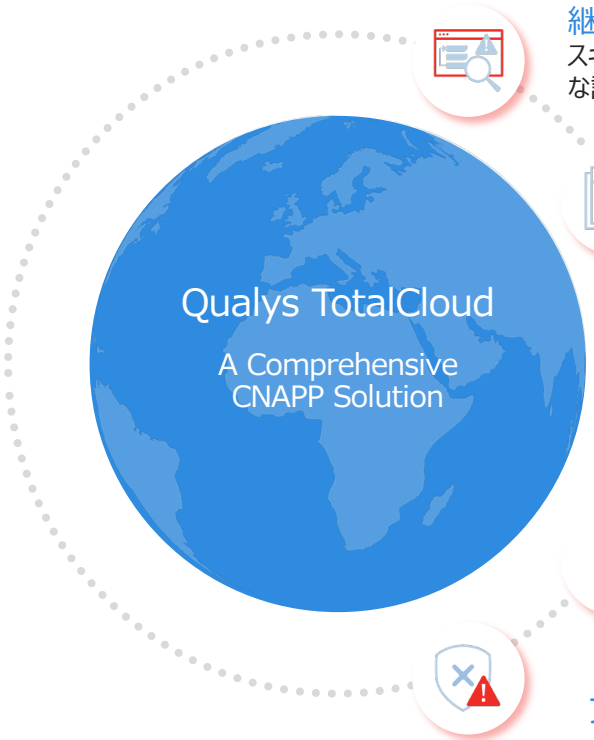
クラウドでは新しい脅威や脆弱性が絶えず出現しており、組織は常に最新の状態を維持する必要があります

手間のかかる修復プロセス

脆弱性が重大かどうかについてのコンテキストがなく、複数のダッシュボードを調べるのに膨大な時間が費やされる

Qualys.

Qualys TotalCloud の優位性



継続的で柔軟なスキャン
スキャン方法 (スナップショット、API、エージェント、ネットワーク) を選択して、最適な範囲と継続的な評価を取得します

最高レベルの検知精度
Qualys カスタム DB、調査およびリスクの優先順位付けに基づくシックス シグマ精度

脅威のリアルタム保護
AI を使用して実行時に未知の脅威と既知の脅威を迅速に検出します

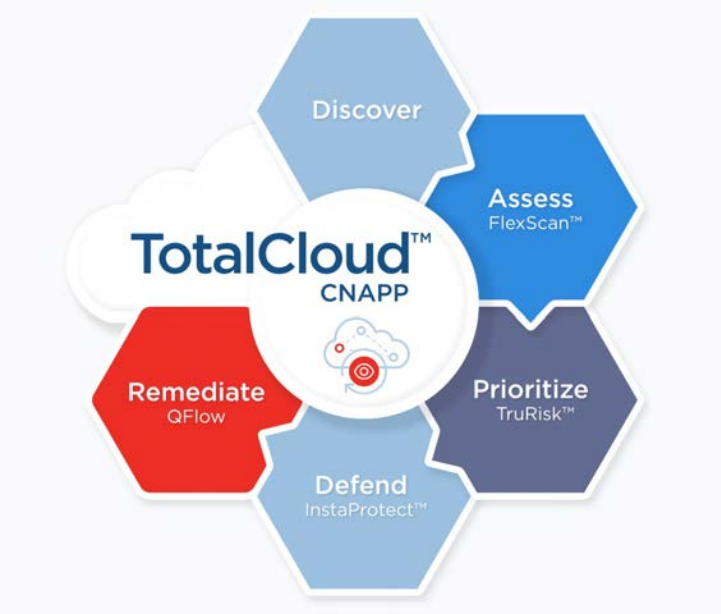
リスクの優先順位付け
ビジネスコンテキストと脅威調査データに基づいて重要なものを修正する

フレキシブルなモジュールライセンス
必要なときに必要なモジュールをデプロイし利用します

Qualys.

Qualys TotalCloud™

Qualys VMDR をクラウドネイティブのワークロードとインフラストラクチャに導入



Cloud Security Posture Management

クラウドアセットの設定ミスや非標準導入を継続的に検出、監視、分析できるため、タイムリーかつ適切な措置を講じることができます。

Cloud Workload Protection Platform

サイバー リスク コンテキストのエクスポジャーと組み合わせた広範なアセットの可視性を提供し、コンテキストとビジネス リスクに基づいて脆弱性の優先順位付けを容易にします。

Qualys TotalCloud と FlexScan は、業界で最も正確な脆弱性の検出と対応のクラウド プラットフォームを使用して、クラウドネイティブのセキュリティの評価、可視性、対応を大幅に簡素化します。単一のクラウド プラットフォームで、クラウド セキュリティ体制、構成ミス、脆弱性を構成、スキャン、評価、優先順位付け、修復します。

23M+	99.99966%	25+
Cloud Workloads Protected	Vulnerability Detection Accuracy	threat and exploit intelligence sources

Qualys TotalCloud

包括的な CNAPP ソリューション

開発から実行時までの統合された脆弱性、脅威、および状況の管理

TotalCloud

Cloud-Native Application Protection Platform (CNAPP)

Cloud Security Posture Management (CSPM)

パブリック クラウド リソースの包括的なインベントリ。展開されたアセットの構成ミスや非標準的の検出と修復します。

Infrastructure as Code (IaC) Security

デプロイ前に IaC コードをスキャンして構成ミスや非標準のアセットを検出することで、インフラストラクチャを保護します。

Cloud Workload Protection (CWP)

リスクベースの脆弱性管理により、リスクとビジネスの重要度に基づき脆弱性とアセットに優先順位をつけます。

Cloud Detection and Response (CDR)

アクティブなエクスプロイト、マルウェア、未知の脅威からマルチクラウド環境を継続的にリアルタイムで保護します。

Container Security（CS）

ビルドから実行時までコンテナを検出、追跡し、継続的に保護します。

Qualys. | Get More Security

Qualys 補助資料

Quaysの優位性

①インストール不要、メンテ不要

- (パブリック・プライベート)クラウドサービス
- セキュリティ業務に集中できる
- 見えにくい運用コストが発生しない

②低誤検知率と高検知率

- 創業からインターネット経由のスキャン
- シックスシグマ(99.9996%)の正確性
- クラウドサービスであるため、スキャンフィードバックが集まり、より検知が洗練される

③シングルプラットフォーム

- インフラやコア機能を共有しているため、モジュール間で管理機能が共通化されている
- １ユーザで複数モジュールをまたがって利用可
- 操作感が似ているため、教育の手間が省ける

④スケーラビリティ

- 数デバイスから多拠点にまたがる数百万デバイスまで1コンソールで管理可
- 多種多様なネットワークやデバイスに対応

⑤脆弱性情報の頻繁な更新

- 通常ほぼ毎営業日に更新がある
- 重要な脆弱性に即時対応
- 1日500件を超える更新 – 2018年実績

⑥日本語対応

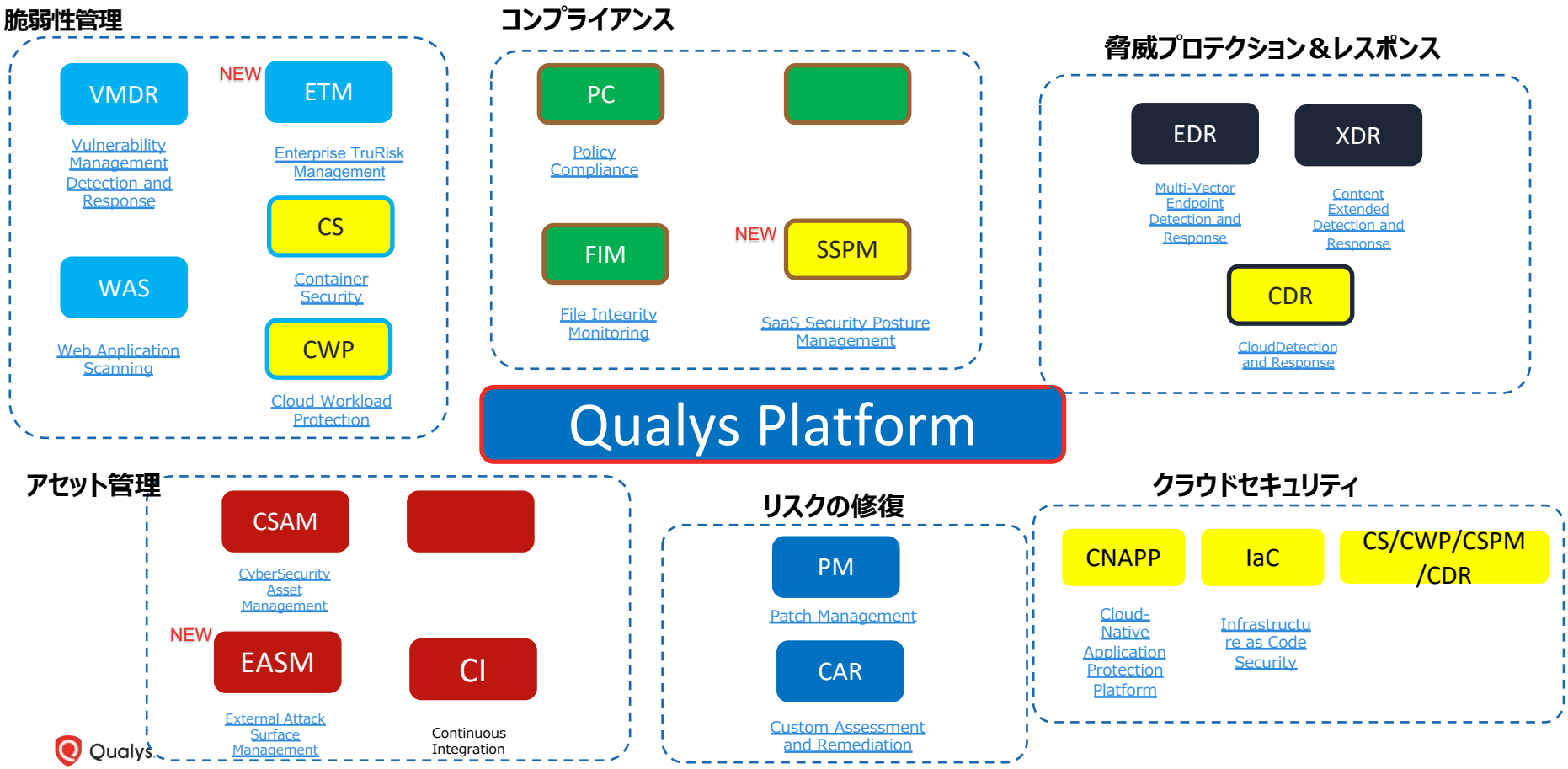
- オンラインヘルプ、バルーンヘルプ
- 脆弱性情報、レポート
- マニュアル、リリースノート
- 脆弱性情報は同日日本語対応
- パッチリンク等も日本語環境対応
- 日本語と英語をユーザ単位で切替可
- 機械翻訳は利用していない

⑦国内外で実績多数

- 19,000社超で導入済み。
- Fortune Global 100 の55%が利用
- 高い業界評価(Gartner, Frost & Sullivan 等)

Qualys.

Qualys クラウドアプリ



Vulnerability Management

- 日本語、英語で出力可
- 検知した脆弱性をQID単位で表示
- 重大度、CVSSスコアでリスクを表示
- CVE ID（例:CVE-2014-0227）、ベンダーリファレンス（例MS17-012）、Bagtraq IDなど外部情報をリンク
- 赤（確認済み）、黄（潜在）、青（情報収集）
- 対処方法をSOLUTIONSに記載
- 検出した根拠をRESULTSに表示

Continuous Monitoring

- 脆弱性の検出状況を継続的に監視し、アラートメール通知
- VMスキャン結果と連動しているため、追加スキャン不要

■アラート/監視対象
- ホスト
- 脆弱性
- 証明書
- ポート/サービス
- ソフトウェア
- チケット

Patch Management

スマート オートメーション

パッチ中心ではなく、リスク中心の自動化。顧客環境のセキュリティ リスクを分析し、現在および将来のリスクに対処するためにデバイスを自動的に修復する効率的な自動化ジョブを推奨します。

セキュリティ チームと IT チーム間の連携の強化

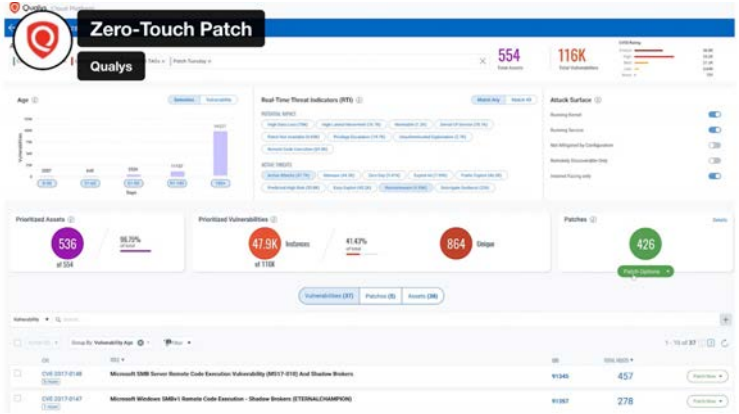
発見、評価、優先順位付け、修復が必要な資産と脆弱性について、単一の信頼できる情報源に基づいて作業します。複雑な引き継ぎプロセス、正規化されていないデータや一貫性のないデータ、最初に取り組む必要があるものに関する意見の相違はもう必要ありません。この調整により、リソースをより効率的に使用し、コストを削減し、リスクにさらされる時間を最小限に抑えることができ、組織のリスク態勢の改善につながります。

リスクベースのアプローチによる大規模な自動化の推進

Qualys VMDR と TruRisk は、組織が脆弱性の急激な増加に対応し、ビジネスに最大のリスクをもたらす資産を修復するのに役立ちます。

単一のクラウド エージェント

クラウド、サーバー、デスクトップ、ラップトップ、その他のエンドポイントの管理にかかるコスト、リスク、複雑さを軽減します。すべて単一のインテリジェントなクラウド エージェントを使用します。拡張性が高く、自動更新され、一元管理されます。



Qualys PM は、Real Time Threat Indicator (RTI)を利用して、脆弱性を利用したランサムウェア攻撃に対し Zero-Touch Patchジョブを作成し、資産の場所に関係なく自動的に展開します。

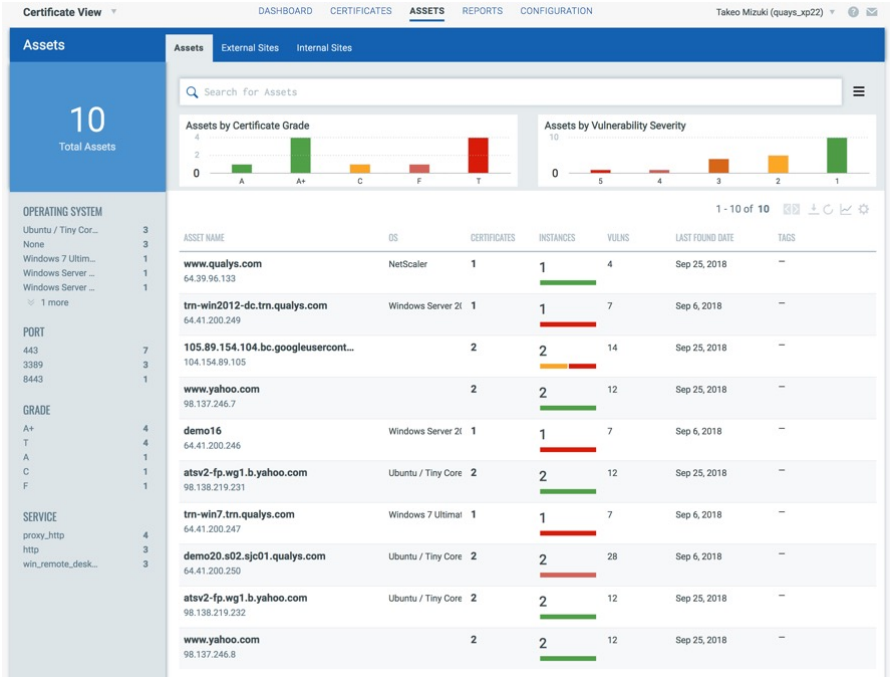
CertView

- 公開、内部、クラウド上のサーバのSSL/TLSサーバ証明書を一括監視
- 有効期限切れ、脆弱な証明書、脆弱なサーバ設定を検出

■検出項目

- 証明書が有効か
- 証明書が信頼できるか
- SSL設定は脆弱か
  - Protocol Support
  - Key Exchange
  - Cipher Strength

- A～F
- T … 証明書が信頼できない
- M … 証明書の名前が一致しない
- NA … 情報が取得できない

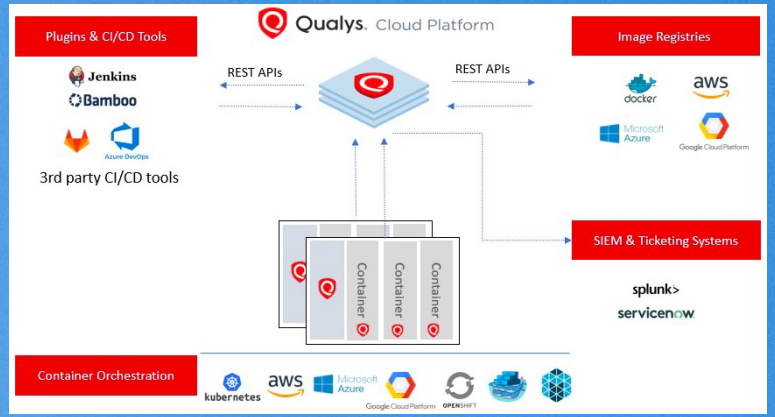


Threat Protection

- 緊急を要する脅威がどのくらい存在するか把握
- 脅威インテリジェンス・ライブフィードで脅威情報を提供
- 脅威情報は独自調査および複数の外部情報源から収集
- リアルタイム脅威指標で脆弱性の絞り込みが可能

■リアルタイム脅威指標
- Public Exploit
- Zero Day
- Actively Attacked
- High Lateral Movement
- Easy Exploit
- No Patch
- High Data Loss
- DoS
- Malware
- Exploit Kit

Container Security



Qualys Container Security プラットフォームは、ビルド フェーズからランタイムまで、コンテナー化されたアプリケーションにエンドツーエンドの保護を提供します。

このソリューションでは、Qualys 脆弱性管理機能を使用して脆弱性/資産を特定して優先順位を付け、詳細なレポートと分析を提供して、セキュリティ体制を継続的に改善します。

発見とインベントリ

多様なパブリッククラウド環境とオンプレミス ソリューションにおけるニアリアルタイムのコンテナー/イメージの検出とインベントリ

評価と優先順位付け

Dockerイメージ、コンテナの脆弱性分析と設定ミスの検出。Dockerレジストリの脆弱正分析

レポート

API、レポート、ダッシュボードによるコンテナ/イメージの脆弱性レポート。

統合

APIを使用したCI/CD プラグインとの統合。Qualys App (Splunk) を介した第三者システムへの送信

Web Application Scanning

2009 年以来、世界中で 2500 以上の顧客の Web アプリを保護

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

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

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

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

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

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

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

Qualys WAS は、Web アプリを継続的に検出し、脆弱性や設定ミスを検出するための堅牢なクラウドソリューションです。

Qualys.

PC/SCA – ポリシーコンプライアンス

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

■ 対応フレームワーク

- COBIT 4.0, ISO 17799, NIST SP800-53, SOX 404, GLBA, HIPAA, Basel II

■ 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

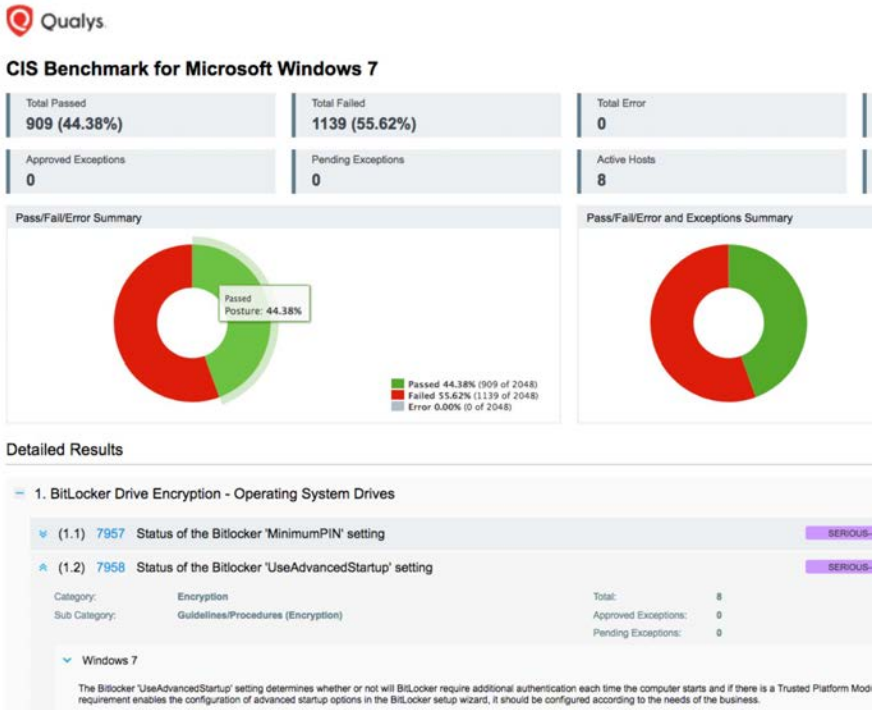
- 再スキャン不要で様々なレポートを作成可能
- ポリシーレポート、個別ホストレポート、コントロール Pass/Failレポートなど豊富なテンプレート

Security Configuration Assessment

- セキュリティ設定が業界推奨値とどの程度乖離しているか可視化
- 業界推奨値として、CIS Benchmark を利用

■SCAの特徴

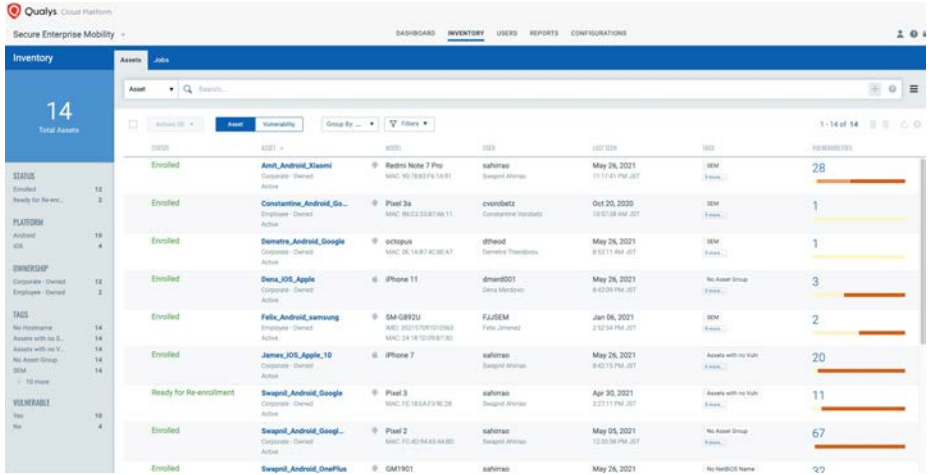
- VMアドオンとして動作
- 認証スキャンが必要
- CISベンチマークのみサポート
- 100+のOS、ミドルウェア、アプリケーションに対応
  - Windows, RHEL, CentOS, AIXなど
  - Cisco ASA, IOSなど
  - Oracle, MSSQL, PostgreSQLなど
  - Apache, Tomcat, IISなど



SEM – Secure Enterprise Mobility

モバイルデバイスの可視化、セキュリティ、継続監視

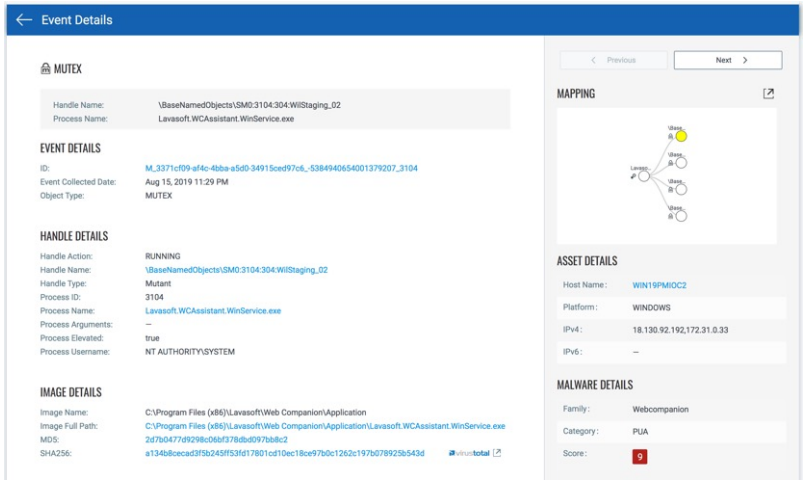
・Android 4.4.2+, iOS 9.0+, iPadOS 13.1+ 対応
・インベントリ管理（ハードウェア、OS、アプリ）
・脆弱性管理(OS,App,ネットワーク)
・設定監視(Jailbreak/暗号化無効/パスワード無効)
・アクション
　　-メッセージ
　　-スクリーンロック
・パッチ管理



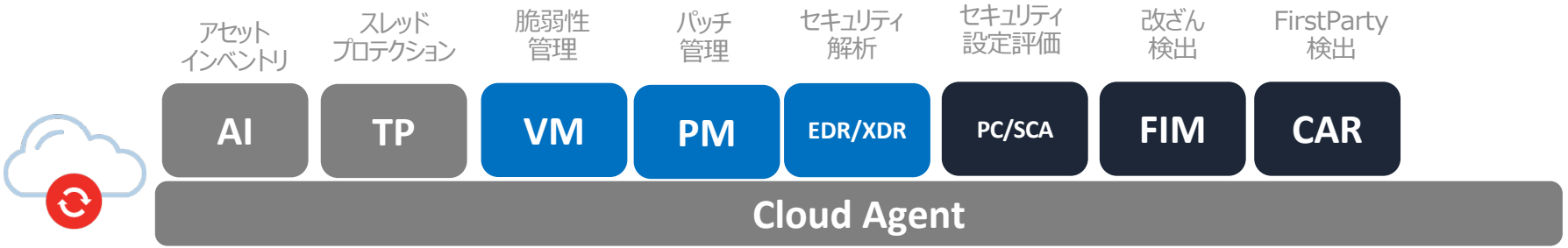
EDR – Endpoint Detection and Response

マルウェアに感染した後に、マルウェアなどがエンドポイントに残す痕跡から感染原因を特定

- ファイル、プロセス、レジストリ、ネットワーク接続などの動作を捕捉
- データをQualysクラウドへアップロードし、Qualysクラウドで解析を実施
- CPUやネットワークに制限がある環境でも考慮して動作
- ATP、CERTアドバイザリ、
  よくある怪しい動作など脅威痕跡
  検出テンプレートを提供
- マルウェアを自動検出
- Windows、Linux対応
- プロセス遮断や検疫
- アンチマルウェア機能(今後)



Cloud Agent 対応サービス



- サービス毎にインストール不要。Cloud Agentだけ一度インストールするのみ。
- AI(アセットインベントリ)、TP(スレッドプロテクション)は、デフォルトサービス。サービス購入不要。
- VM(脆弱性管理)、PM(パッチ管理)、EDR、PC/SCA(セキュリティ設定評価)、FIM(ファイル改ざん検出)から利用したいサービスを追加購入
- 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。

※ 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>

GAV と CSAMの比較

機能	概要	GAV	CSAM
アセットインベントリ	複数のセンサーを使用して、継続的に資産を検出し、インベントリを作成。サーバ、デスクトップ、ネットワーク、モバイル、IoTなど、オンプレミス環境やクラウド環境のアセット情報およびソフトウェアやコンテナの詳細情報も取得。	○	○
インベントリの正規化とカテゴリ分類	製造元、プロダクト、ハードウェアモデル、ソフトウェアの情報を標準化するため、インベントリをすっきりと整理でき、スタッフの作業時間を大幅に短縮。	○	○
動的タグとビジネスコンテキスト付加	インベントリを動的タグで整理し、ビジネス機能（例：財務）、スコープ（例：PCI DSS準拠）に関連するアセットを見つけることができます。タグに基づいて重要度を割り当てることで、最も重要なアセットに素早く注目できます。	○	○
製品ライフサイクルの把握	ハードウェアやソフトウェア製品のリリース日、EOL、ライセンス分類などのメタデータを自動的に追加。		○
未承認ソフトウェア検出	未承認ソフトウェアと承認ソフトウェアを設定し、未承認ソフトウェアがインストールされているアセットを検出し、アセットの健全性を向上。		○
EASM	External Attack Surface Management。IPアドレス、ドメイン名、組織名、証明書情報などのキーワードから自組織に関連するアセットを検出。		○
アラート・カスタムレポート	アラートを設定し、EOLや未承認ソフトウェアのインストールなど、アセットの健全性に関する問題についてアラート。PCIDSSやFedRAMPなどの業界コンプライアンスの維持のためのレポートを作成し、社内関係者に報告。		○
ServiceNow CMDB同期	インベントリをServiceNow CMDBと同期することで、ハードウェアやソフトウェアのライフサイクルや分類情報を反映した最新のインベントリを維持。 所有者、環境、ビジネスアプリケーションなどのビジネスコンテキストデータをインポートし、アセットの健全性に関する問題への対応を改善。 認定ServiceNowアプリとして提供します。		○

Qualys PC/SCA/CSA/SaaSDRの違い

PCとSCAは、オンプレあるいはパブリッククラウド上の
ネットワーク機器、OS、ミドルウェア、アプリケーション
などのセキュリティ設定評価を行う。

CSAはクラウド(IaaS)のセキュリティ設定評価を行う。
SDRはクラウド(SaaS)のセキュリティ設定評価を行う。

Qualys.

Qualys マーケット情報

GigaOMレーダー脆弱性管理レポート

What are we announcing?

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

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

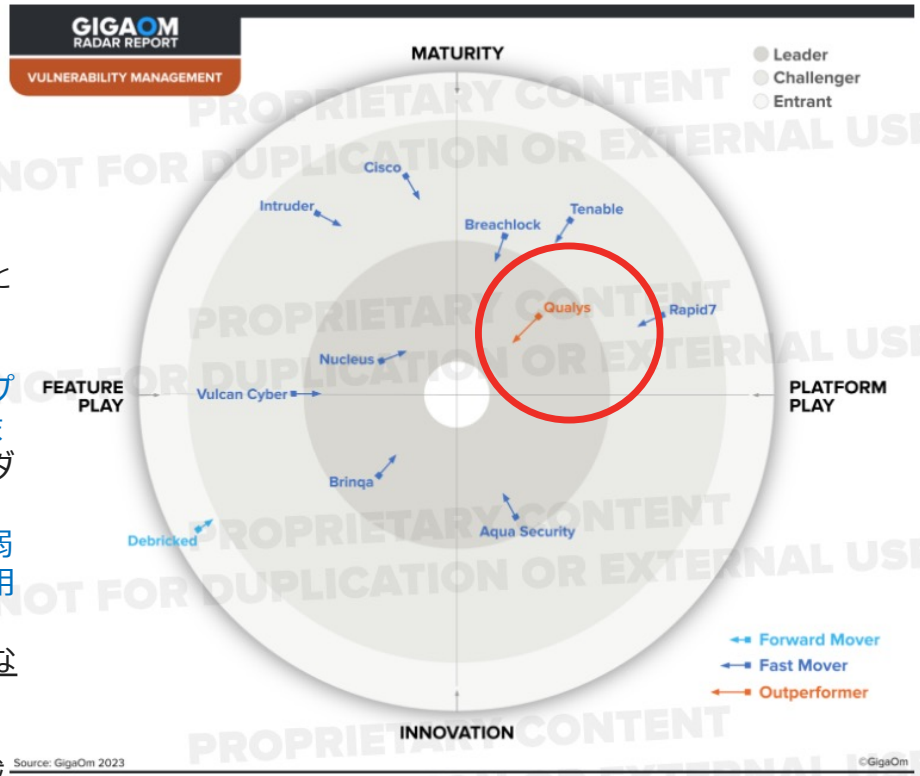


Figure 1. GigaOm Radar for Continuous Vulnerability Management

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

New!

GigaOMレーダーWASレポート

What are we announcing?

アプリケーションセキュリティテストに関する最新のGigaOmレーダーレポートにてQualys WASが「リーダー」としてタグ付けされました。

CVE フィード – 786 を超えるシグネチャを備えた Qualys WAS は、CVE および OWASP トップ 10 の脆弱性、PII、エクスポージャー、および Web マルウェアを簡単に検出できます。

API セキュリティのサポート – REST および SOAP API の動的ランタイム脆弱性を迅速かつ簡単にテストします。

統合 – サードパーティのスキャン結果を追加して、組織の全体的なセキュリティ体制のビューを強化します。

結果のフィルタリング - 重大度、資産、既知の悪用可能な脆弱性などに基づいて、スキャン結果と脆弱性をフィルタリングします。

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

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

The #1 Vulnerability Management Solution

1999 Year Founded	**130+** Countries	**5K+** Customers with cloud workloads	**2,000+** Employees
23M+ Cloud workloads protected	**75K+** CVE signatures	**6+ billion** IP scans and audits per year	**99.9996%** Six sigma scanning accuracy