Qualys Trurisk Enterprise Management 概要

Qualys Japan
更新日2026年9月

定期的脆弱性管理から継続的脆弱性リスク管理へ

定期的脆弱性管理	継続的脆弱性リスク管理
組織内の資産台帳、単一システムのみに頼った対象領域の把握	外部情報リソース、他製品連携により対象領域を把握 – リスクが潜む領域を一元管理（サイロ化をなくす）
定期的な脆弱性スキャン（年2, 4回）- 脆弱性のみ把握	自動化された継続的な脆弱性スキャン – 資産を絶えずモニタリング、最新の攻撃手法や脆弱性情報を把握
CVSSスコアによる優先順位付け	リスクベース優先順位付け – 重要度、悪用性だけでなく財務影響を利用した優先順位付け
MDM等ツールを利用した当該パッチのみの適用	自動化された修復ワークフロー – パッチ適用、軽減策適用、構成変更等の修復アクションを統合し自動化
スキャン結果、パッチ適用結果等、事後処理的なレポート生成	リアルタイムの精度で即時かつ実用的なレポート生成と監査準備を実現

Qualys.

世界初のクラウド型リスク運用センター（ROC）

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

ETMの目的と導入背景

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

Qualys.

リスクオペレーションセンター(ROC)

ROCでCTEMの運用化と拡張を支援する

Risk Operation Center

01 Scoping — CSAM

デジタル攻撃面全体にわたる統一可視性:オンプレミス、クラウド、ハイブリッド資産による**自動分類**と**統一インベントリ管理**

02 Discovery — ISPM

包括的なリスクテレメトリ管理のための**ネイティブスキャン**および**サードパーティコネクター**(脆弱性、設定ミス、外部エクスポージャー)

03 Prioritization — TruLens / TruConfirm

TruRiskスコアは、QDS/QVSS脅威インテリジェンスデータとビジネスコンテキストを組み合わせ、正確なリスクランキングを実現します。**TruRisk**のカスタマイズは、**有害な組み合わせ**のスコアリングを上げ、**補償対照**が利用可能な場合にノイズを抑制するリスク因子を提供します

04 Validation — TruConfirm

TruConfirmは**安全なエクスプロイト評価**でリスクを検証し、ビジネスの混乱なしに実際の悪用可能性を確認します。展開されたセキュリティ制御が効果的かどうかを検証します

05 Mobilization — TruRisk Eliminate

TruRisk Eliminateはネイティブのパッチ管理および軽減機能を提供します。ITSMプラットフォームやサードパーティパッチ管理ソリューションとの連携により、柔軟な緩和ワークフローが実現します。エグゼクティブダッシュボードと**リスク定量化（risk quantification）**は、取締役会レベルでのリスク状況や是正の進捗を可視化します

業界をリードするCTEMカバレッジ:Qualys ETMは、単一の統一アーキテクチャ内でガートナーのCTEMの5フェーズすべてにマッピングされる唯一のプラットフォームであり、ポイントソリューションや「ベンダーのスプロールを排除」しています。

※ETMモジュールには、CSAM, TruLens, TruConfirmがライセンスに含まれております。ISPMとEliminateは追加ライセンス料が必要です。

ETM – インベントリ すべての資産を一元的に可視化

様々な方法によりデータを収集、統合、分類

組織の攻撃対象領域全体をリアルタイムかつ包括的に把握することを目的に、ASM/EASM、サードパーティツールからのデータを統合、資産を識別。

ETM インベントリの主な機能と利点

統合された可視性: Cloud Agent、スキャン、サードパーティソースからの資産データを一つの包括的なビューに統合。

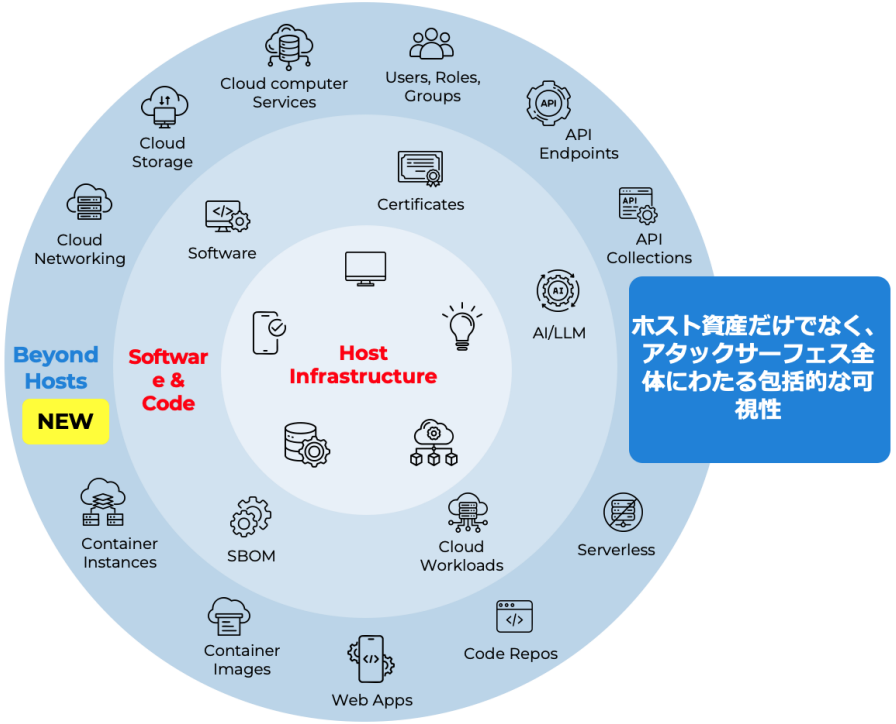
包括的な範囲: オンプレミス、クラウド、ハイブリッド環境、IoT/OT、ソフトウェアの脆弱性をカバー。

業界ベンチマーク: 組織のセキュリティパフォーマンスと修復にかかる平均時間（MTTR）を業界の同業他社と比較。

リスクの優先順位付け: TruRiskスコアを使用して、ビジネスの重要性と露出に基づいて資産の優先順位を決定。

継続的な検出: 資産をリアルタイムで追跡し、資格を減らします。

サードパーティ統合: Wiz、Microsoft、CroudStrikeなどのツールからデータを取り込んで、資産のコンテキストを充実させます。

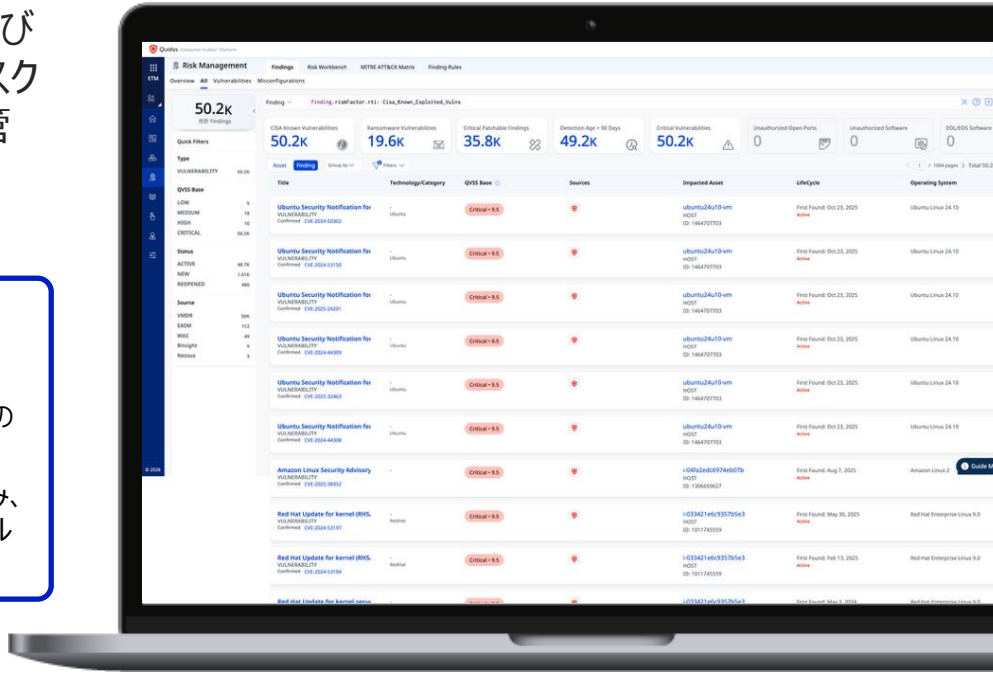


Qualys.

ETM – リスク管理 定量化したすべてのリスクを管理し優先順位づけ

様々な方法によりデータを収集、統合、分類

攻撃対象領域全体にわたる脆弱性、構成ミス、およびID露出データを統合、発見し定量化したすべてのリスク（脆弱性、設定ミス）を整理して可視化、結果を管理、優先順位付け。



ETM リスク管理の主な機能と利点

統合された可視性: 脆弱性、構成ミス、ID露出データ等、発見、調査結果としてのリスクデータを一つの包括的なビューに統合。

発見されたリスク: 脆弱性、構成ミスに分類、調査結果を可視化、実際の脅威に照らした実際のリスクを詳細表示。

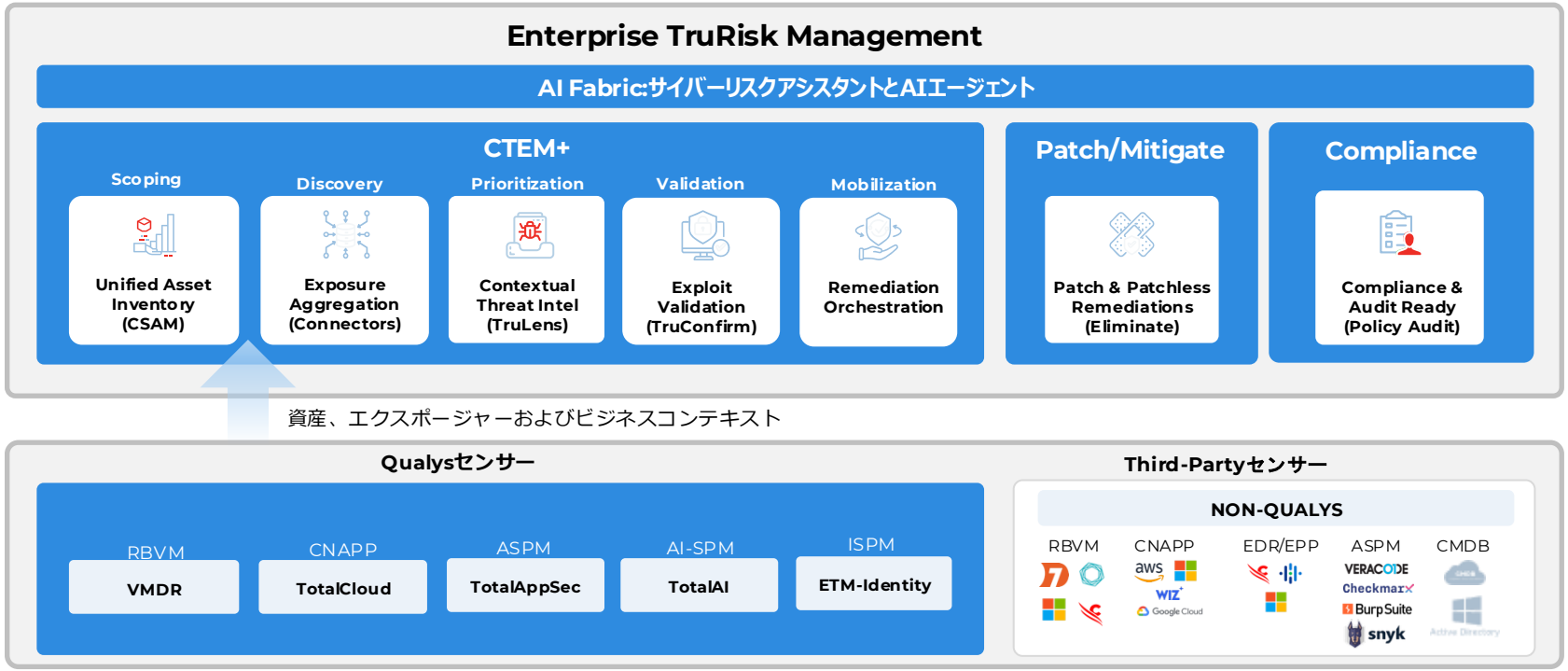
優先順位の管理: セキュリティチームがノイズを排除、重点領域の絞り込み、特定のビジネスエンティティ等最も重要なところにフォーカスするために、フィルタリングして優先順位付けを実行。

Qualys.

Qualys ETM は CTEM++

クラウドにおける初のリスクオペレーションセンター

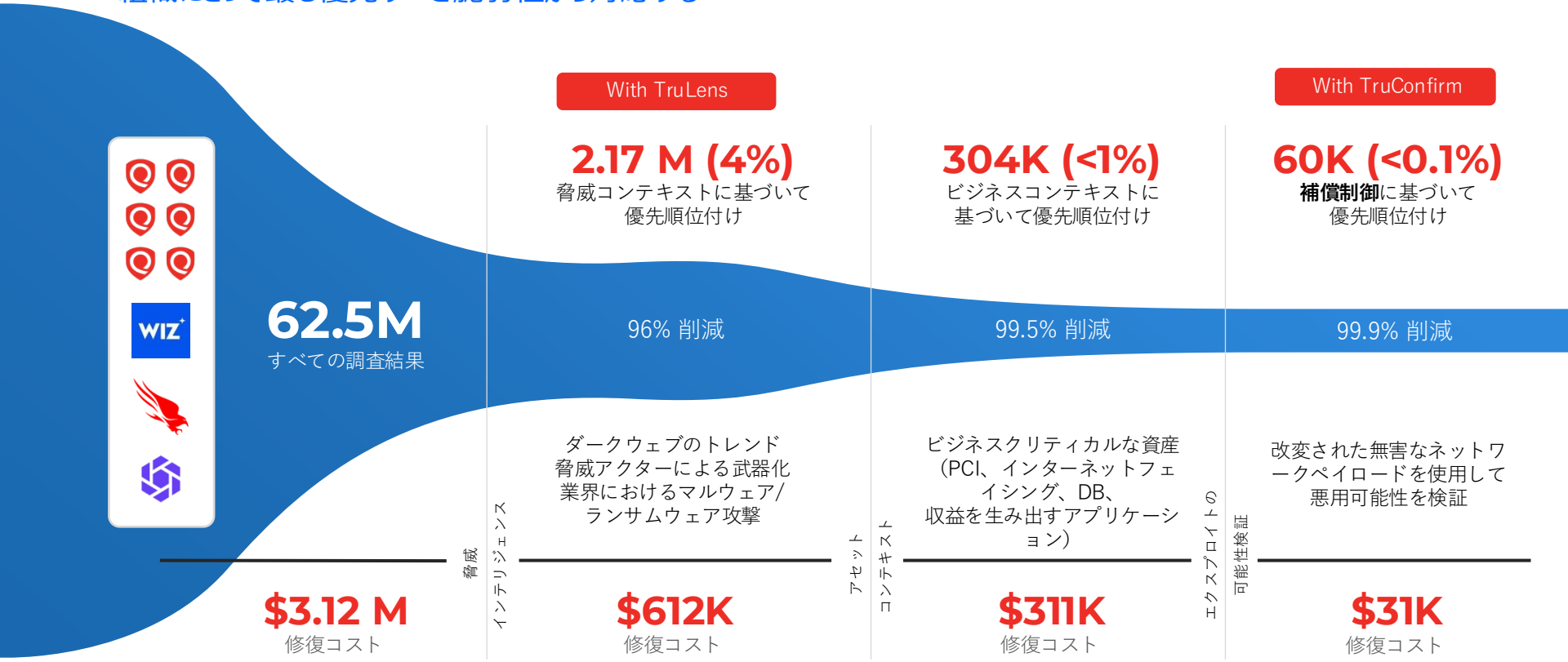
ONEプラットフォーム、**ONE**エージェント、**ONE**コンソール



Qualys.

導入効果 –リスクを定量化、確実性に基づく優先順位

組織にとって最も優先すべき脆弱性から対応する



※補償制御（compensating controls）とは、既存のセキュリティ対策によってエクスポージャーのリスクが下がっている場合に、リスクスコアを調整をします。

TruConfirm 自動エクスポージャー検証

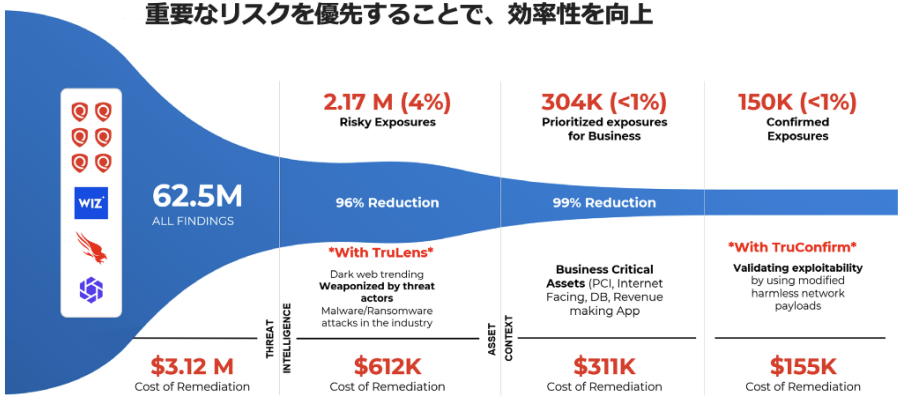
従来の脆弱性管理は、ソフトウェアのバージョンやCVSSスコアから「脆弱かもしれない」と推測していました。一方、Qualys TruConfirmは実際に攻撃経路を安全に検証し、その脆弱性が本当に悪用可能かを確認します。これにより、理論上のリスクではなく、実際のリスクに集中した脆弱性管理を実現します。

お客様の課題

- 脆弱性が多すぎて優先順位が分からない
- 誤検知の確認や手動トリアージに時間がかかる
- 修復リソースが不足している
- 本当に危険な脆弱性を特定できない
- リスク説明の根拠が不足している

TruConfirmによる解決

- 実際の悪用可能性を検証
- エビデンスベースで優先順位付け
- 修復対象を大幅に絞り込み
- MTTRを短縮
- 監査・経営層向けの説明責任を強化



TruConfirmの主な機能

1. 悪用可能性（Exploitability）の実証検証

脆弱性が存在するかどうかだけでなく、攻撃者が実際に悪用できる状態かを検証します。ソフトウェアのバージョン情報による推測ではなく、実際の攻撃経路を安全にテストして判定します。

2. Direct Response Verification

安全なペイロードを送信し、システムからの応答を分析することで、脆弱なコードが実際に実行されるかを確認します

3. Cryptographic Verification

暗号学的ハッシュを用いてコード実行の成否を検証し、文字列一致による誤検知を排除します。

4. OAST（Out-of-Band Application Security Testing）

SSRFやBlind RCEなど、通常のスキャンでは確認が難しい脆弱性について、外部コールバックを利用して安全に悪用可能性を検証します。

5. TruRiskとの連携

検証された脆弱性はTruRiskスコアへ反映され、理論上のリスクではなく、実際のエクスポージャーリスクに基づいた優先順位付けを実現します。

TruConfirmは、**1,600件以上のCVE**（共通脆弱性識別子）について悪用可能性を検証します。そのカバレッジは、単にスキャンしやすいものだけでなく、企業環境で最も頻繁に悪用されるテクノロジーと攻撃経路に意図的に焦点を絞っています。

InstaScan　スキャン不要のAI駆動型エクスポージャー検出

公式ブログはこちら

InstaScanが解決する課題

1. 脆弱性公開から検知までのタイムラグ（24～36時間）の解消

従来の定期スキャンやエージェントの再評価では、CVE（共通脆弱性識別子）が公開されてから検知までに24～36時間程度かかり、その隙に攻撃者に悪用されるリスクがありました。InstaScanは最新のアドバイザリと既存の資産インベントリを即座に自動照合することで、公開から数分以内に該当資産を特定します。

2. AIを活用した高度な攻撃スピードへの追従

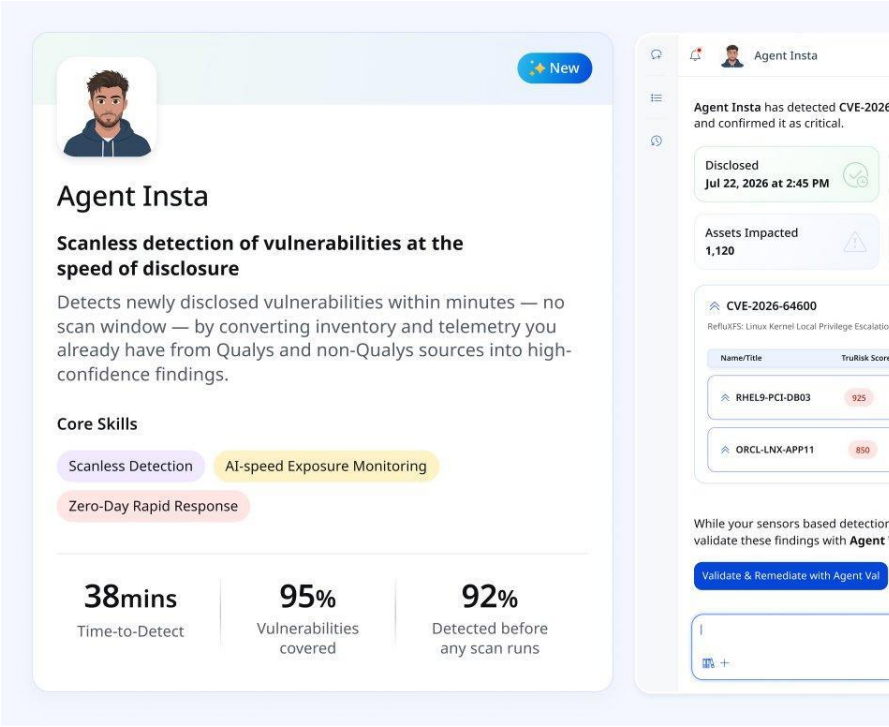
AI技術の進化により、脆弱性公開から概念実証（PoC）や攻撃コードが作成されるまでの時間が数時間に短縮されています。InstaScanはリアルタイムで脆弱性を検知することで、攻撃者のスピードに追いつくことを可能にします。

3. ネットワーク負荷やシステム停止リスク（運用摩擦）の軽減

従来のスキャン処理はネットワークやデバイスに負荷をかけたり、メンテナンスウィンドウの確保やIT部門との調整を必要としていました。InstaScanは新たなスキャンジョブを実行せずに既存のデータを解析するため、システムへの影響や手動運用の手間を抑えられます。

4. 断片化したインベントリデータの統合

エージェント、サードパーティ製ツール、CMDBなど、データ元によってソフトウェアの表記が異なる（表記揺れ）課題に対し、AIを活用してソフトウェア識別子（CPEやPURLなど）を標準化・統合することで、重複や見落としのない正確な検知を可能にします。



Qualys.

TruLens 統合化された脅威インテリジェンスハブ

従来の脆弱性管理が「何が見つかったか」を教える仕組みであるのに対し、TruLensは「今、攻撃者が狙っているものは何か」「自社は同業他社と比べて安全か」「どこから対処すべきか」をリアルタイムに示す脅威インテリジェンス基盤です。

TruLensが解決する課題

1. 脅威情報が多すぎて何を優先すべきかわからない

企業はCVE、脅威情報、攻撃キャンペーン情報、KEV、EPSSなど大量の情報を入手できますが、それらが断片的であり、自社に関係する脅威を判断するには多くの工数が必要です。

2. 脆弱性の深刻度だけでは優先順位を決められない

CVSSが高い脆弱性でも実際には攻撃されていない場合があり、一方で攻撃者が積極的に悪用している脆弱性が見落とされることがあります。

3. 自社が同業他社と比べて安全なのか判断できない

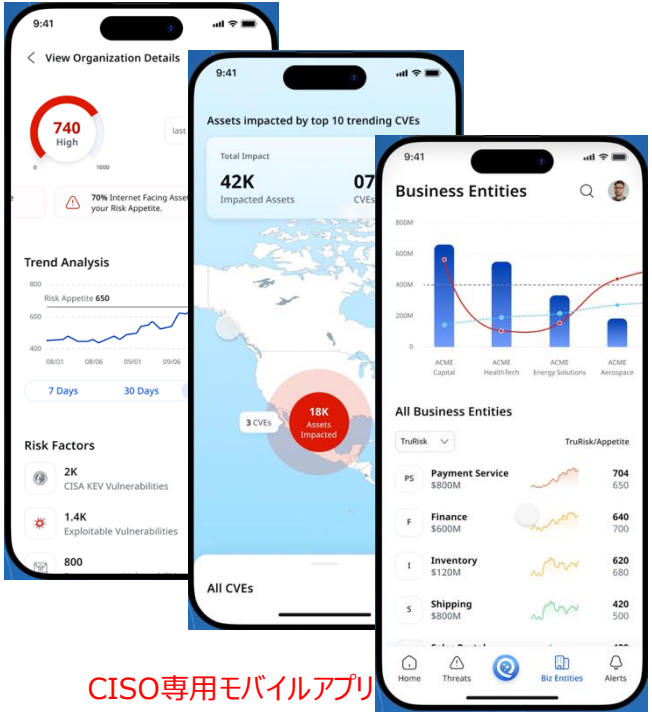
MTTRやパッチ適用速度を測定していても、それが業界平均より優れているのか遅れているのかを説明できないケースがあります。

4.「攻撃者目線」でのリスク評価が難しい

多くのツールは「何の脆弱性があるか」は示しますが、「どの攻撃グループが実際に悪用しているのか」まで結び付けて分析することは容易ではありません。

5. 経営層向けの説明が難しい

技術的な脆弱性情報をビジネスリスクや財務インパクトに変換するため、セキュリティ部門が手作業でレポート作成する必要があります。



CISO専用モバイルアプリ

※最新ブログ『TruLens for Enterprise TruRisk™ Managementのご紹介：統合脅威インテリジェンス』はこちらをご覧ください。

Qualys.

Identity　IDリスクの定量化

ID関連のリスクを検知、ゼロトラスト戦略を支援

※別途ライセンス購入が必要

デジタルアイデンティティ、アクセス権限、認証プロセスに関連するリスクを低減することを目的に、組織全体のアイデンティティ基盤の弱点を可視化。

ETM Identityの主な機能と利点

包括的なアイデンティティインベントリ: IDaaSシステム全体で人、サービス、端末のアイデンティティを検出、所有者、ライフサイクル状態、権限、変更履歴をマッピング。

統合アイデンティティリスクビュー: VMDRなどのQualysソリューション、サードパーティからのデータを統合し、アイデンティティリスクを特定、サイバーリスクポスチャー管理を実現

攻撃パスの分析: 攻撃者は目的を達成するために複数の方法で侵入します。脆弱性、設定ミス、資産間の関係性がどのように悪用されるかをを資格的にマッピング。

※最新ブログ『Qualys ETM Identity — アイデンティティ境界の真の定量化を初めて実現』はこちらをご覧ください。

Frontier AI時代のQualysの取り組み

Qualysは、サイバーセキュリティ強化に向けて、Anthropicの「Project Glasswing」とOpenAIの「Trusted Access for Cyber」に参加。AIを活用し、防御側がリスクに先行できる体制づくりを目指しています。

Qualysの自律型修復ソリューション

カテゴリリーダー

AIスピードによる高速検出
VMDR

ベースライン脆弱性管理

価値

- オンプレミス環境とクラウド環境、コンテナインフラストラクチャ全体にわたる脆弱性の高精度検出。
- リスク管理とコンプライアンスワークフローの基盤となります。

主要な機能

- No.1カバレッジ: 13万件以上のCVEをカバー
- 99.4%: CISA KEVカバレッジ
- デジタル証明書評価
- 構成評価（CISベンチマーク）
- 資産インベントリ
- 脅威ベースの優先順位付け (TruRisk)

カテゴリリーダー

超優先度設定
ETM

Agentic AIによる運用可能なCTEM

価値

- 攻撃者が攻撃を仕掛ける前に、最もリスクの高い脆弱性に対処するため、エクスポージャーノイズを98%削減します。
- セキュリティポスチャーを3倍向上
- ビジネスへの影響に合わせたリスクの統合ビュー

主要な機能

- 統合資産インベントリ (CSAM)
- QualysおよびQualys以外のセンサーからの統合リスクビュー
- 資産およびビジネスコンテキストに基づく優先順位付け (TruRisk)
- 新たな脅威 (TruLens)
- 悪用可能性の検証 (TruConfirm)
- サイバーリスクの定量化
- サイバーリスクワークフローのためのAIエージェント

カテゴリリーダー

ゼロデイ修復
TruRisk Eliminate

パッチ適用とパッチレスによる修復

価値

- 機械並みのスピードで修復
- セキュリティとIT部門の連携を円滑化
- 運用上の回復力を実現

主要な機能

- パッチ適用、修正、緩和、アンインストール、隔離。
- AIを活用したパッチ信頼性スコアとウェーブ展開
- マルチベンダー対応: Zscaler, SCCM/Intune, CrowdStrike, ServiceNow.
- ルールベースのオーケストレーション
- 100%カバレッジ: ランサムウェア対策

※最新ブログ『最先端AI時代のサイバーセキュリティの推進：QualysがProject Glasswingに参画』はこちらをご覧ください。

補助資料

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

ETM(AgenticAI)

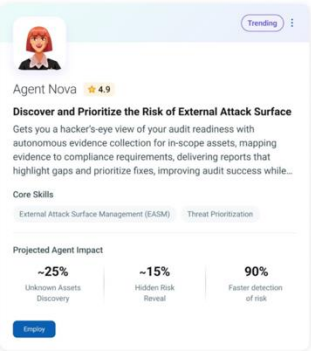
ETM機能の一部としてリリース済み

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 Valのユースケース

ETM(AgenticAI)

エージェント主導の安全なエクスプロイト検証による現実世界のリスク低減

・One Pager
・Demo Video

概要とユースケース

◎実環境でゼロインパクトのエクスプロイト検証
Agent Val は、TruConfirmを使って、実際に攻撃が成功するかを攻撃チェーン単位で安全なペイロード（書き込みなし、データ取得なし、永続化なし）で本番環境を検証。本当に危険であればTruRiskスコアを増幅し、修正の優先順位を上げる。

◎自動検証→修復→再検証（クローズドループ）
1. リスク優先度の高い脆弱性だけを選定
2. 実環境で検証
3. 修復（パッチ、コントロール追加）
4. 再検証でリスク軽減を証明

◎攻撃者目線の脅威対応
Threat intelligence（TruLensやCISA KEV）を使って、“本当に今狙われている脆弱”を抽出して対処。

こんな企業・組織へお勧め

◎高度な脆弱性管理が求められる大規模企業
CVEが年間数万件規模で発生する環境では、検証・修復コスト削減が顕著。

◎業界規制やガバナンス要件が厳しい企業
金融、ヘルスケア、公共インフラなどでは「証明できる対応実績」が非常に重要。
Agent Val の「検証⇒再検証」によるエビデンスは大きな価値に。

◎ SOC/ROC（Risk Operations Center）を運用する組織
迅速な判断・優先順位付け・自動対応が整備された環境では高ROIを発揮。ETMとの統合により、既存SOAR/SIEMとの連携も可能。

高く評価される理由

90%+	修復作業に伴うノイズの低減
70%	悪用可能な脆弱性が確認された場合の修復時間の短縮
1,600+	CVE をカバー。新たなセンサー設置は不要

Qualys.

ETM Connectors - Vision

Qualys. | De-risk Your Business

現在公開中のコネクタ と今後利用できるコネクタリスト

VM (Vulns on Host Assets)
- Qualys VMDR
- Tenable.io
- Rapid7 InsightVM
- Crowdstrike Spotlight
- Amazon AWS Inspector

End Point Security
- Qualys EDR
- Crowdstrike Falcon
- Defender for Endpoint
- Tanium Endpoint
- Palo Alto Cortex
- SentinelOne Endpoint Security
- Cybereason

CSPM & Containers
- Qualys TotalCloud/CS
- Prisma Cloud
- Wiz
- Orca
- Defender for Cloud
- AquaSec
- CS Falcon for Cloud

AppSec [DAST, SAST, SCA]
- Qualys WAS/AppSec
- Veracode
- Checkmarx One
- Snyk
- BlackDuck
- Fortify
- PortSwigger BurpSuite
- SonarQube
- GitHub
- XRay Jfrog

EASM
- Qualys EASM
- BitSight
- Security Scorecard
- Mastercard Risk Recon
- Censys
- Palo Alto Expanse
- CyCognito

CSP
- AWS
- Azure
- GCP
- Oracle

Identity
- Microsoft Active Directory
- Okta
- Microsoft Entra
- Bloodhound
- Ping Identity
- PingCastle

Ticketing
- ServiceNow Ticket/VR
- Jira (on-premise)
- Jira Cloud
- Azure DevOps
- Freshdesk (Freshservice)
- Ivanti ITSM
- BMC Helix

Asset Mgmt/CMDB
- Axonious
- ServiceNow CMDB
- Flexera
- BMC CMDB
- Cisco Collector

Patch Mgmt
- Qualys Remediate
- Trend Micro Virtual Patching
- Ivanti Neurons
- Ivanti Security Controls
- BigFix

Threat Intel
- Microsoft RiskIQ
- Mandiant
- Recorded Future
- IBM X-Force

OT / IoT
- Ordr
- Claroty
- Nozomi Network
- Armis

Technology Connectors
- CSV via multiple methods
- Public SDK
- Public APIs

Qualys On Qualys (Cross Subscription)
- CSAM
- VMDR
- WAS
- PC

DSPM
- Cyera

最新情報はこちらをご確認ください

Qualys.

Qualys脆弱性スコアリングシステム（QVSS）

様々な脅威シグナルを含んだ深刻度スコア

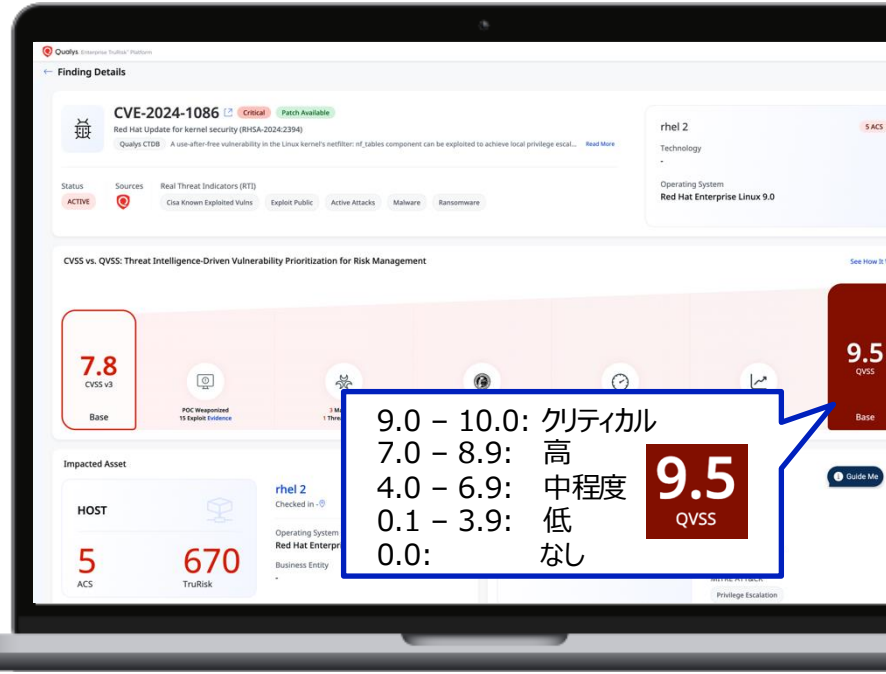
0.00 – 10.00の一般的なスケールを使用して脆弱性、構成ミスの重大度を評価。理論上の脅威ではなく実際のリスクに基づいて深刻度スコアを決定。

QVSSの主な機能と利点

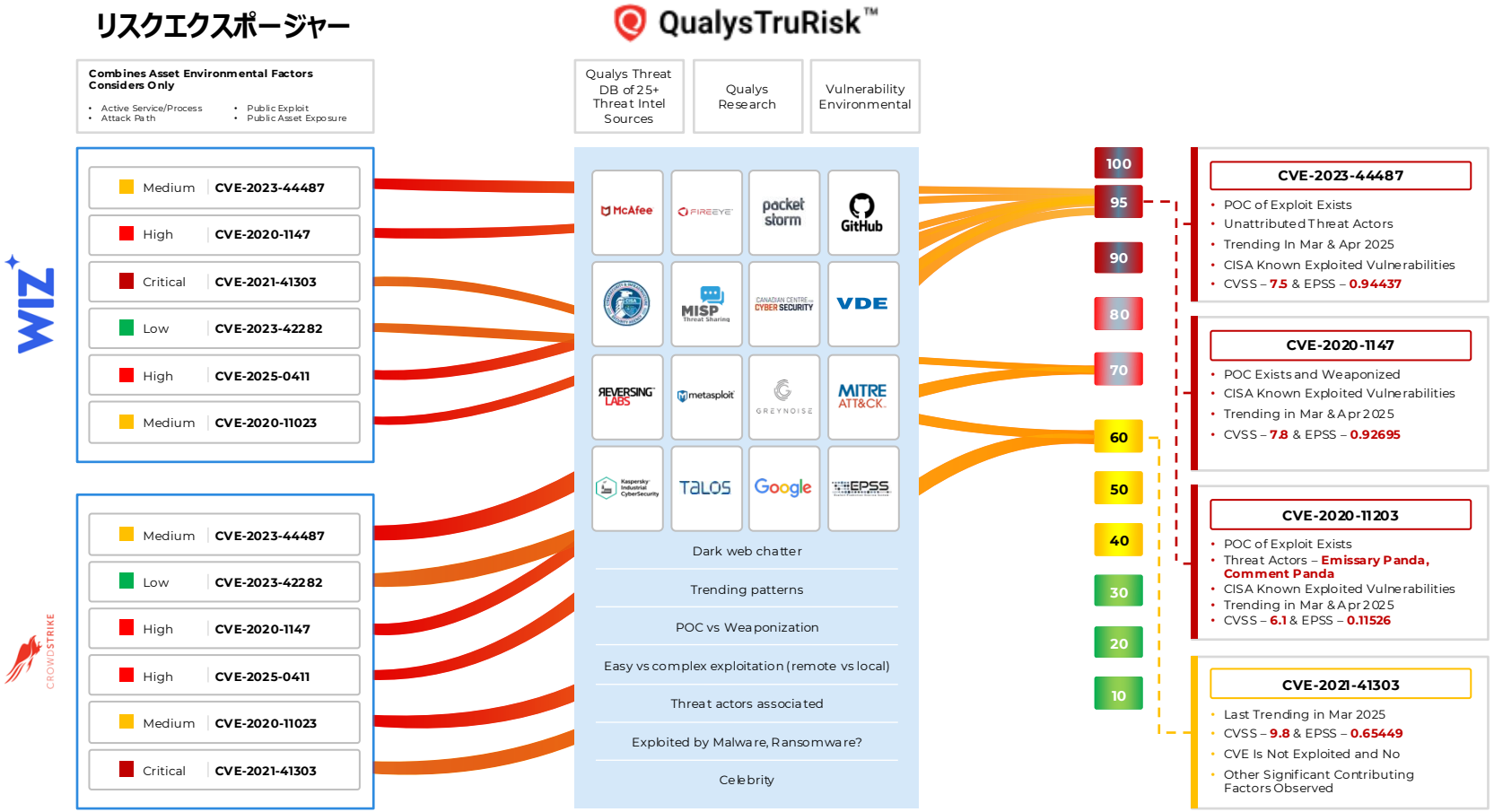
統合スコアリング: 現実の脅威リスクに基づいて下記点を考慮しスコアリング:

- CVSS属性（攻撃ベクトル、複雑さ、権限、影響）
- エクスプロイト可用性
- 搾取の証拠
- CISA KEV
- ランサムウェアとマルウェアの関連性
- 脅威アクター
- ダークウェブとトレンド
- EPSS

範囲: 脆弱性と構成ミスをカバー。



リスクエクスポージャー



Qualys.

Qualys | De-risk Your Business

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