Qualys Trurisk Enterprise Management 概要

Qualys Japan K.K

更新日2026年3月

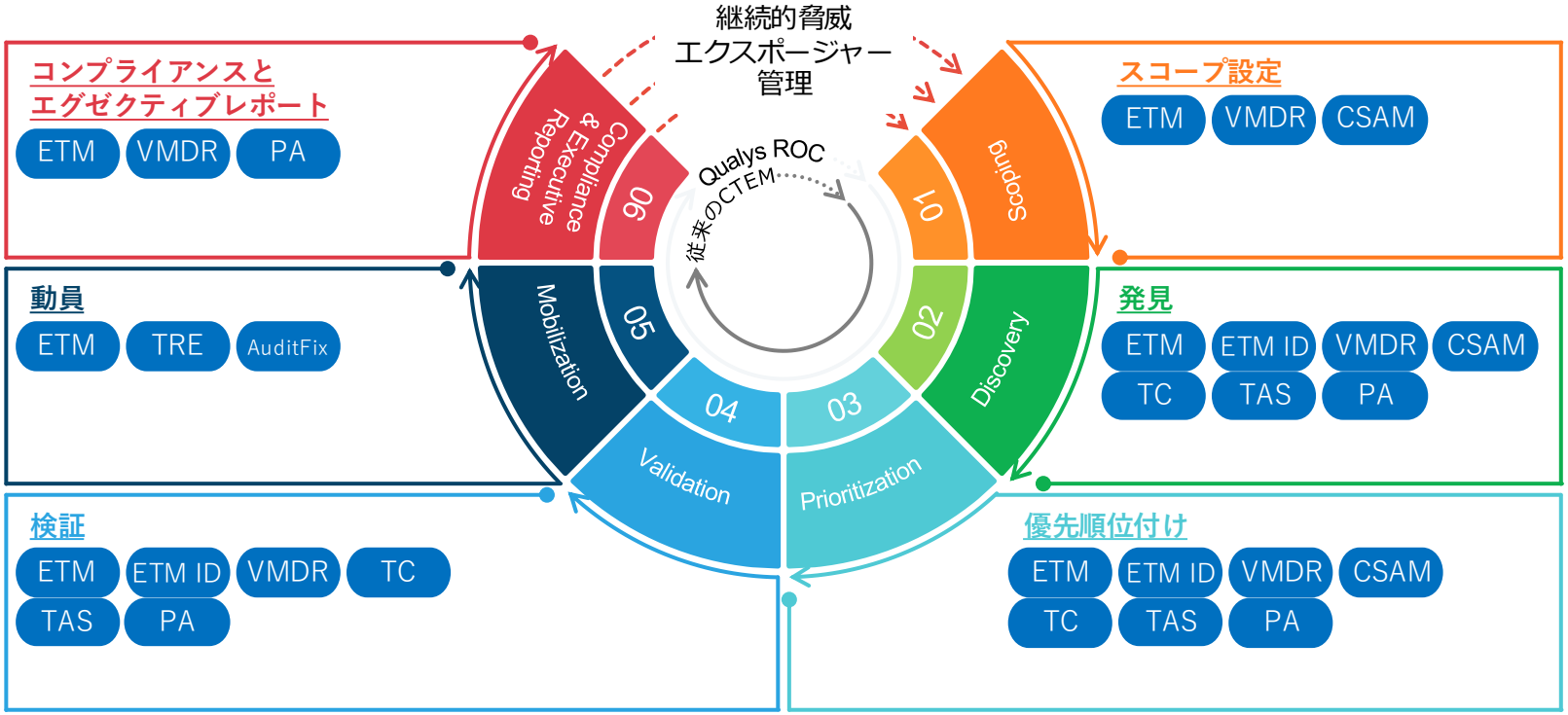
定期的脆弱性管理から継続的脆弱性リスク管理へ

定期的脆弱性管理	継続的脆弱性リスク管理
組織内の申請情報、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.

Qualys継続的脅威エクスポージャー管理

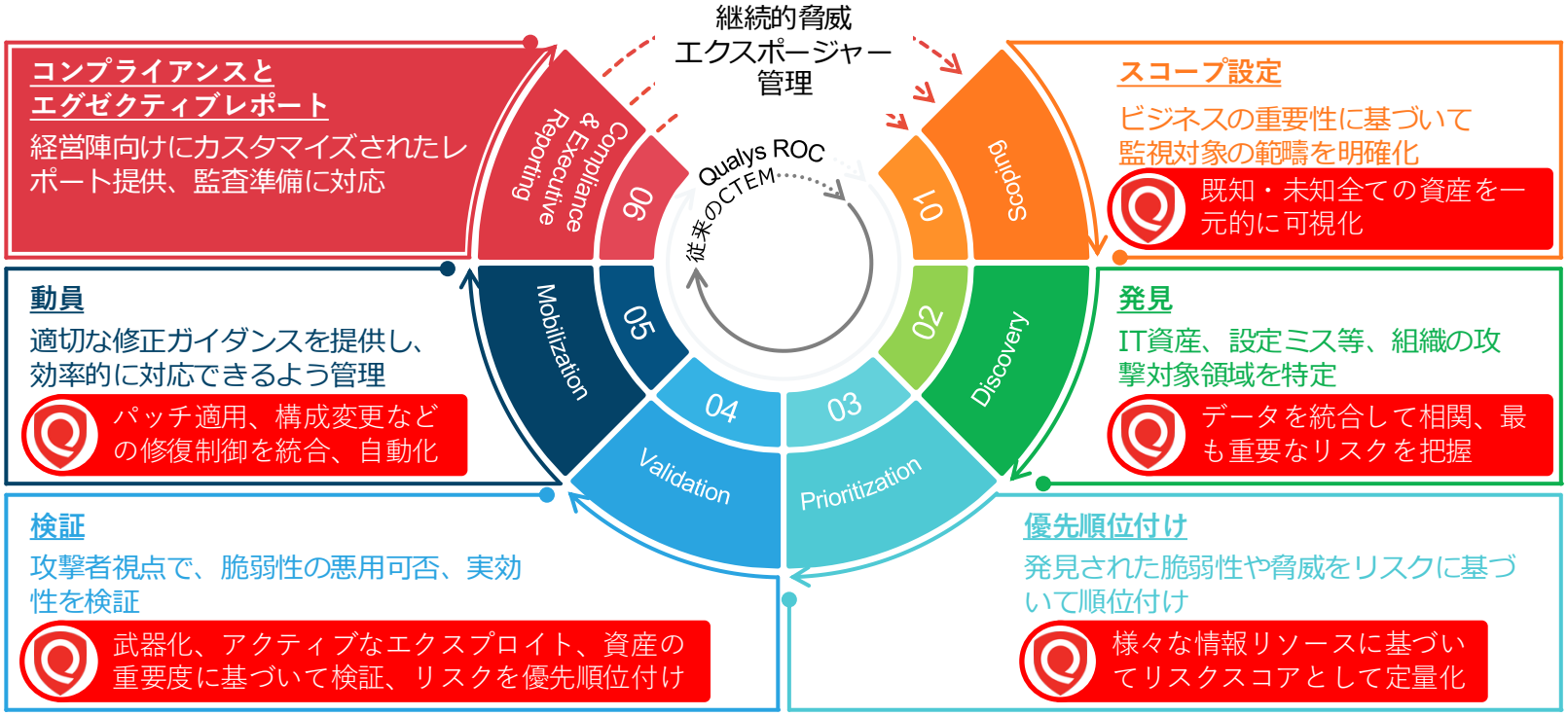
Qualysソリューションマップ



Qualys.

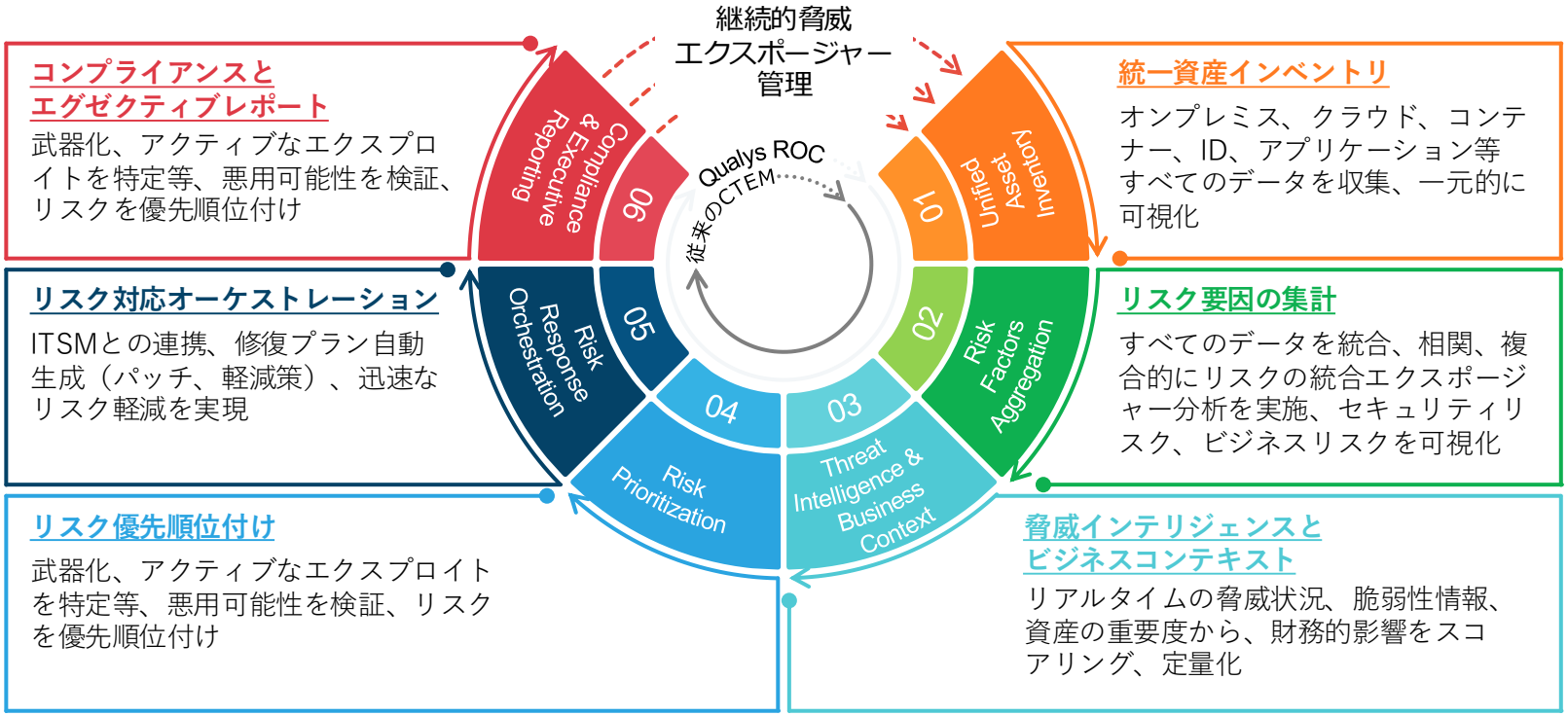
Qualys継続的脅威エクスポージャー管理ライフサイクル

QualysはCTEMを自動化、強化することにフォーカス



Qualys Enterprise TruRisk Management

CTEMを実現するためのコアコンポーネント



コンプライアンスと
エグゼクティブレポート

武器化、アクティブなエクスプロイトを特定等、悪用可能性を検証、リスクを優先順位付け

統一資産インベントリ

オンプレミス、クラウド、コンテナー、ID、アプリケーション等すべてのデータを収集、一元的に可視化

リスク対応オーケストレーション

ITSMとの連携、修復プラン自動生成（パッチ、軽減策）、迅速なリスク軽減を実現

リスク要因の集計

すべてのデータを統合、相関、複合的にリスクの統合エクスポージャー分析を実施、セキュリティリスク、ビジネスリスクを可視化

リスク優先順位付け

武器化、アクティブなエクスプロイトを特定等、悪用可能性を検証、リスクを優先順位付け

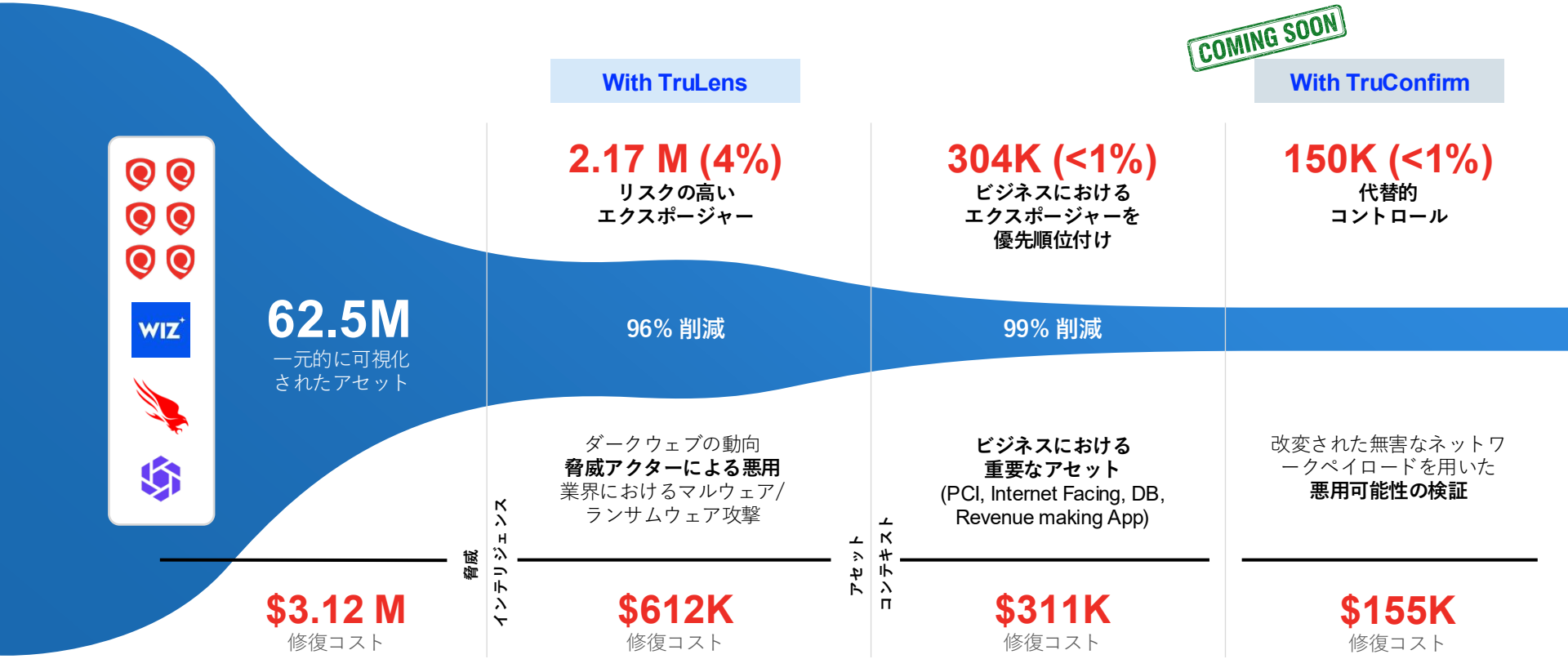
脅威インテリジェンスと
ビジネスコンテキスト

リアルタイムの脅威状況、脆弱性情報、資産の重要度から、財務的影響をスコアリング、定量化

Qualys.

ETM導入効果 – 重要なリスクを定量化、効率性向上

組織にとって重要なリスク、影響を理解



Qualys.

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。

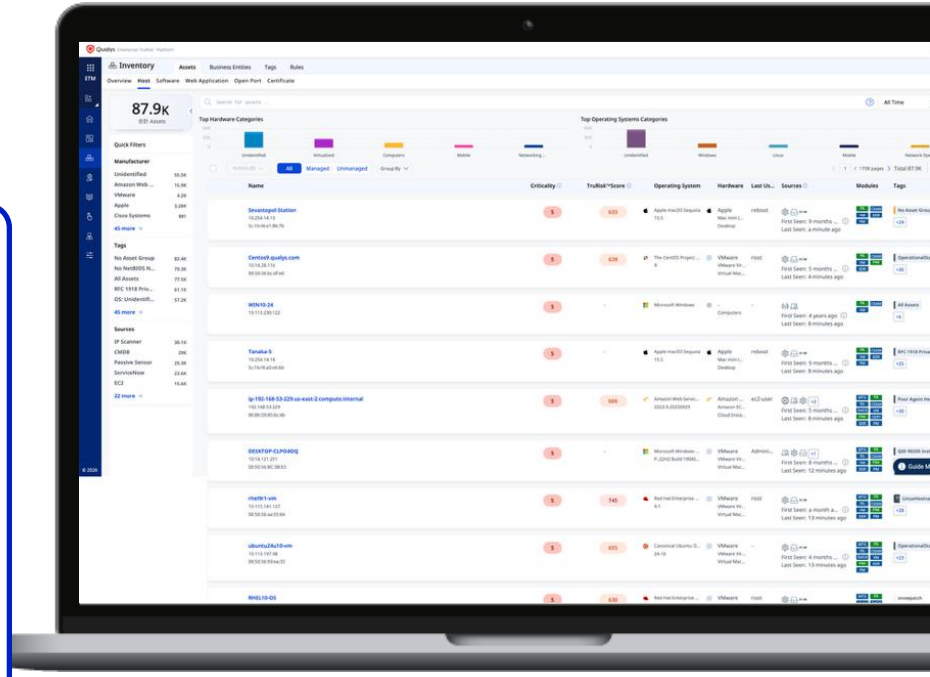
包括的な範囲: オンプレミス、クラウド、ハイブリッド環境、IoT/OT、ソフトウェアの脆弱性をカバー。

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

様々な方法によりデータを収集、統合、分類

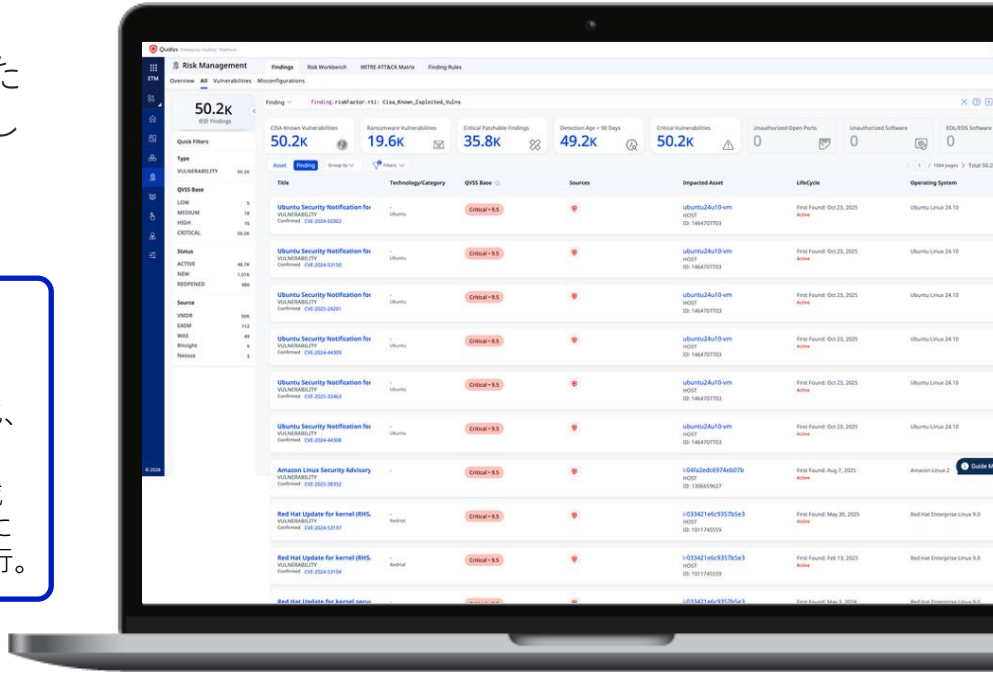
攻撃対象領域全体にわたる脆弱性、構成ミス、およびID露出データを統合、発見し定量化したすべてのリスク（脆弱性、設定ミス）を整理して可視化、結果を管理、優先順位付け。

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。

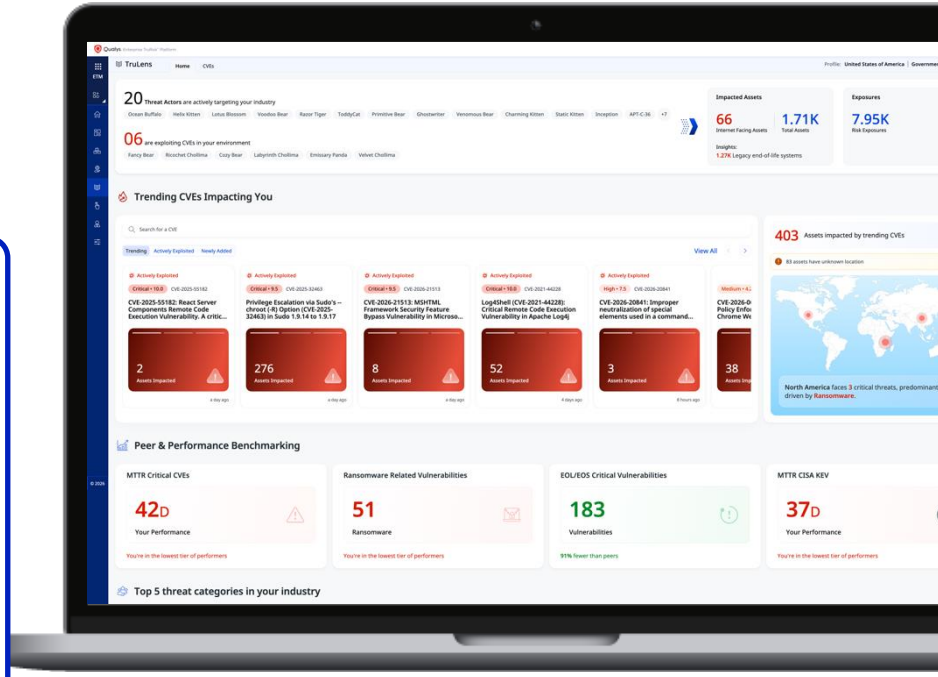


Qualys.

ETM – TruLens 統合化された脅威インテリジェンスハブ

テーラード脅威インテリジェンスによる現実のリスクを定量化

「洞察力の向上」を目的に、グローバル脅威データ、業界固有のベンチマーク、資産のコンテキストを組み合わせ、AIを使用して最も大きい脆弱性を定量化。



TruLensの主な機能と利点

カスタマイズされた脅威インテリジェンス: 組織の環境とお客様の業界に基づいてカスタマイズされた洞察を提供。

コンテキスト化されたリスク: ライブ脅威分析（CISA KEV等）とビジネスコンテキストを組み合わせて、脆弱性を動的に定量化。

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。

実質的な洞察: AIを使用してリスクの優先順位付けと可視化、セキュリティチームが事後対応型から事前対応型のセキュリティ運用に移行できるよう支援。

統合ビュー: 脅威、脆弱性、資産データを単一のプラットフォームに統合。

Qualys.

ETM – 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

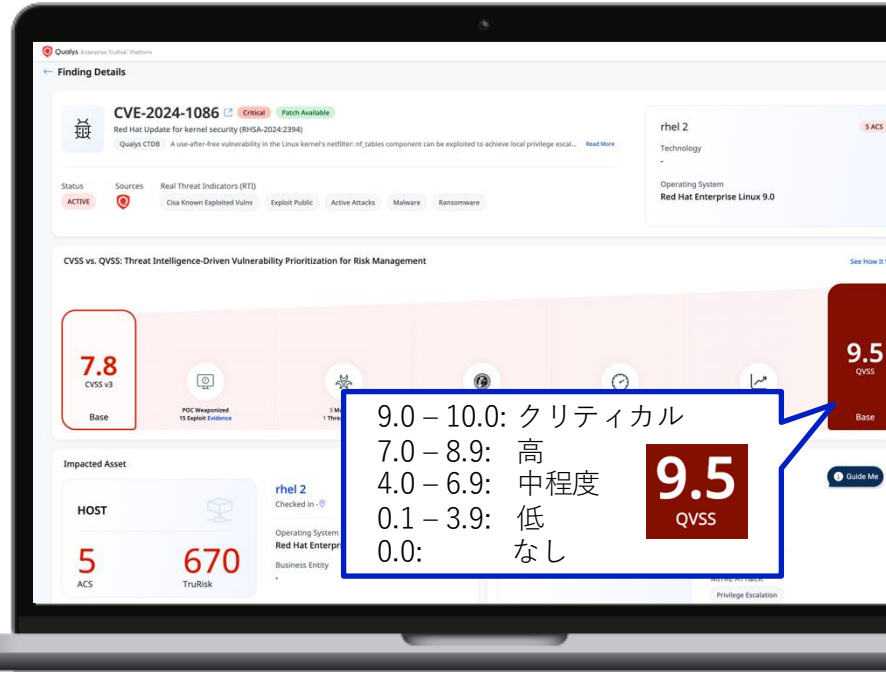
0.00 – 10.00の一般的なスケールを使用して脆弱性、構成ミスの重大度を評価。理論上の脅威ではなく実際のリスクに基づいて深刻度スコアを決定。

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。

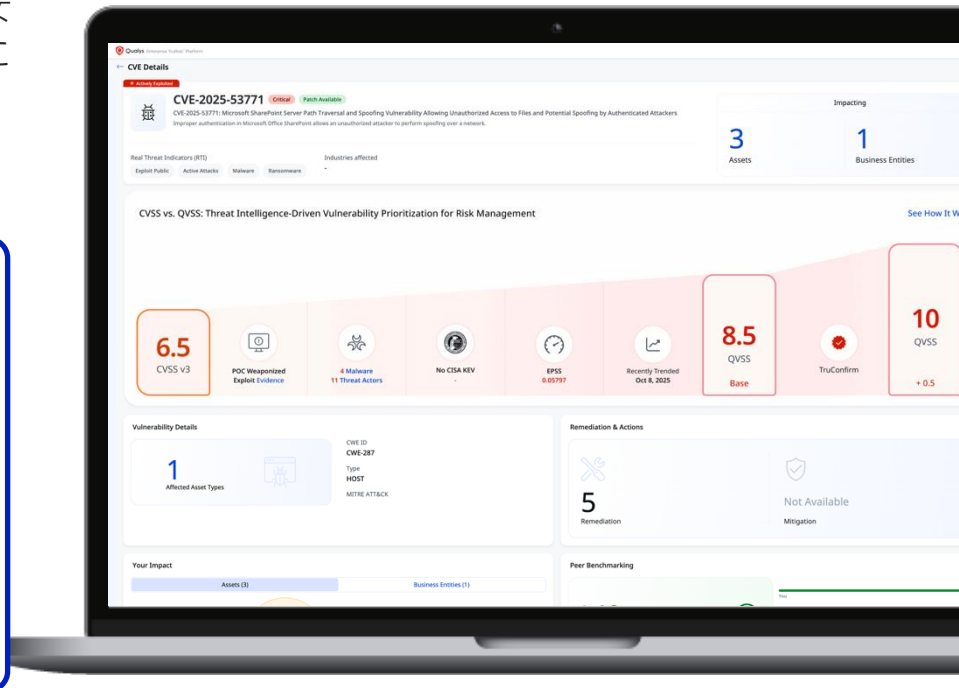


COMING SOON

ETM – TruConfirm 自動エクスポージャー検証

自社環境における悪用可能性検証

エクスポージャー管理を理論上のリスクから安全なエクスプロイトを本番環境で実行、証拠に基づく検証結果によりリスクを定量化。



ETM TruConfirmの主な機能と利点

本番環境で安全な、確定的な検証: シミュレートされた環境ではなく安全なエクスプロイトによる本番環境に対し直接アクティブな検証を実施、悪用可能性を確認。

リスク判断を直接的に促進: ETMが持つリスクコンテキスト（脅威インテリジェンス、ビジネスコンテキスト等）を活用し、高リスクのエクスポージャーを特定。悪用可能性が特定されると、自動的にQVSS、TruRiskスコアを増幅、関連したリスク軽減推奨作事項を生成。

エビデンスに基づく検証: 安全なエクスプロイトによる検証が失敗した場合、FW/WAFルール、ネットワークポリシー制御等の防御層を正確に記録。

Qualys.

ETM Identity – アイデンティティリスクの定量化

ID関連のリスクを検知、ゼロトラスト戦略を支援

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。

Qualys.

補助資料

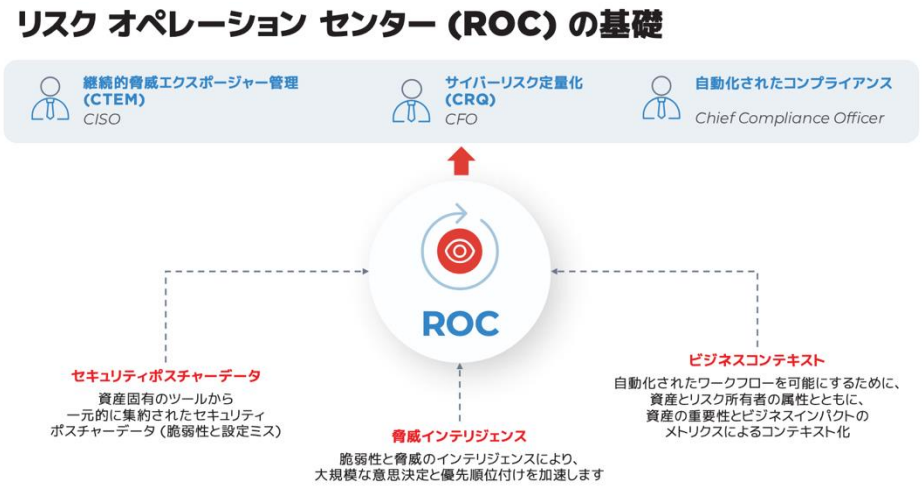
世界初のクラウド型リスクオペレーションセンター

リリース済み

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

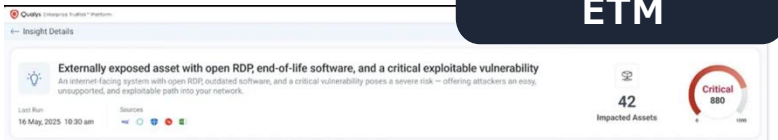
従来、複数ツールにまたがる断片的なセキュリティ対策では、冗長作業、見落とし、優先順位のズレなどが課題となっていました。ETMはこれらを一元化し、CISOや経営層が戦略的にサイバーリスクを管理できるよう設計されています。

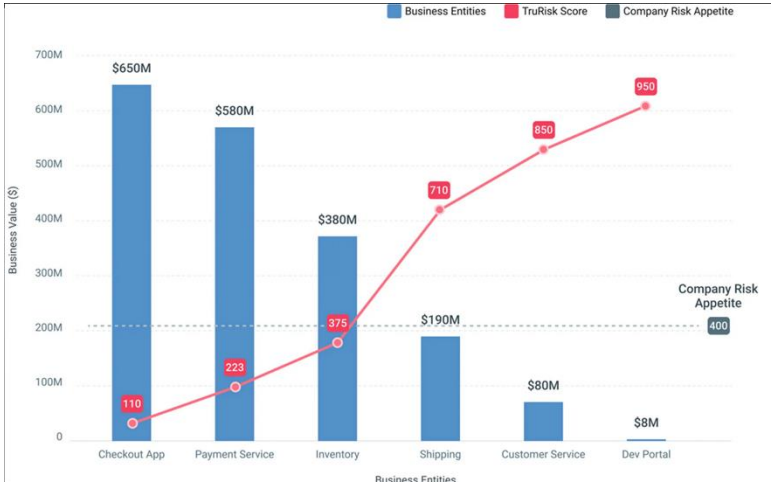


ホワイトペーパーはこちらです。
リリースノートはこちらです。

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
リスク対処の自動化	パッチ適用、チケット発行、リアルタイムアラートなど、AIドリブンの自動ワークフローによりリスク対応を迅速化（「パッチレス修復」も含む）
監査対応と経営層向け報告	詳細な監査用ログや、経営層にも伝わる一貫性のあるリスク報告機能を備え、コンプライアンス対応を支援
多様なデータソースとの統合	Qualysおよびサードパーティ製ツール（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種多様なデータを集約



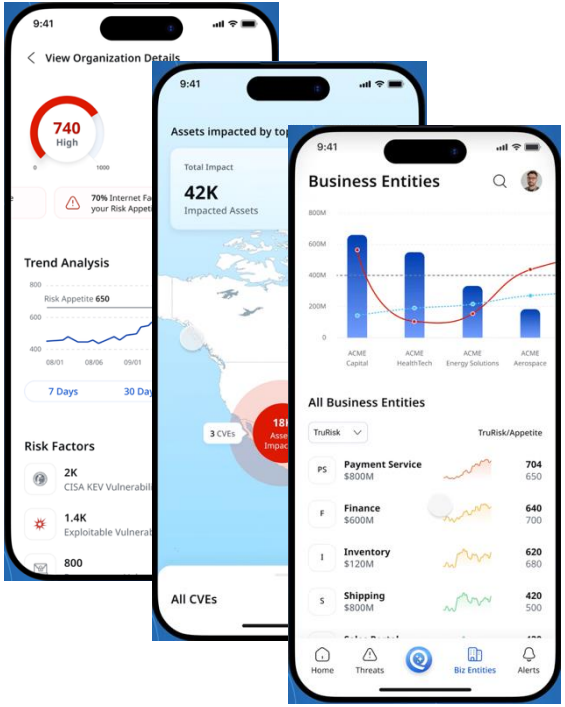


Qualys.

TruLens

ETMの機能としてプレビュー提供中

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

ETMの機能としてプレビュー提供中

ETM

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

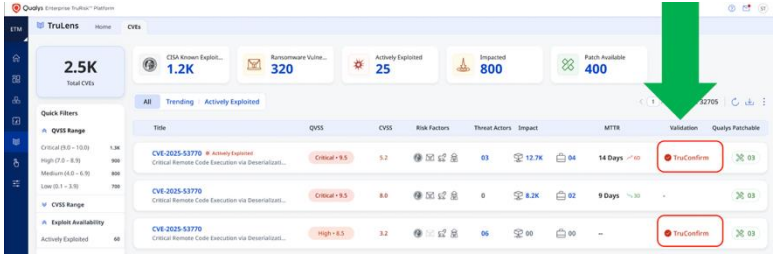
悪用可能性を確認することで、不要なアラートを減らし、対応すべき脆弱性を絞り込みます。結果として、平均修復時間（MTTR）が短縮されます。

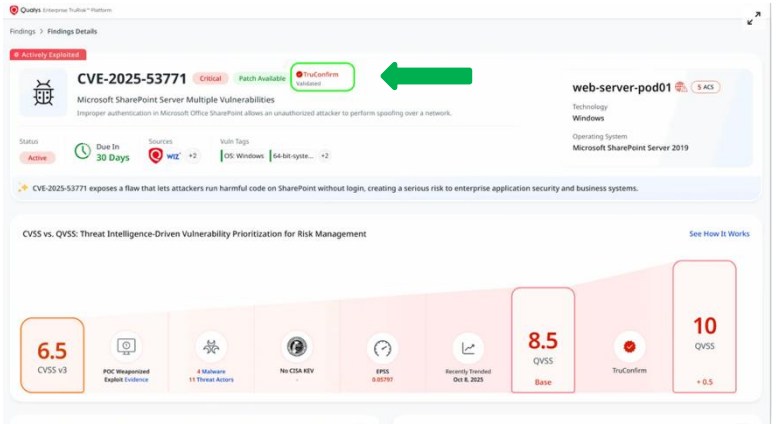
③ETMワークフローとの統合

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。





※2025年10月公開のBlogは[こちら]

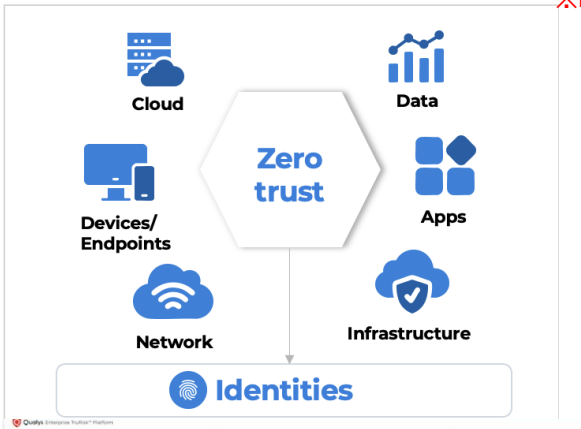
Qualys ETM Identity

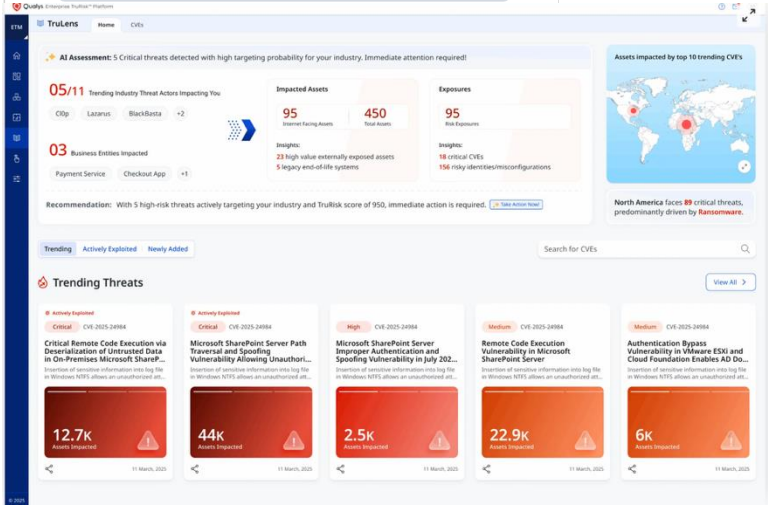
ETMの機能としてプレビュー提供中

ETM(Identity)

※ETMの有償オプション

Qualys 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

BLOG: エージェント型AIの力を活用してアイデンティティリスク、適応型脅威の優先順位付け、エクスポージャーの悪用可能性検証を実施

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)

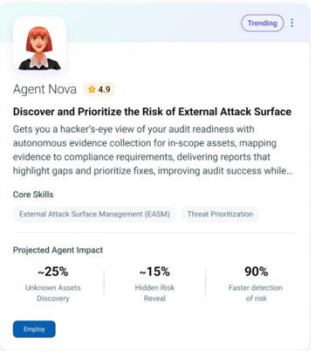
ETM機能の一部としてリリース済み

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 Saraのユースケース

利用例）

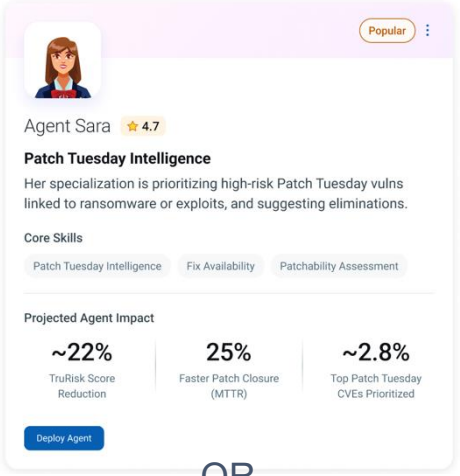
1. リスク評価の開始
- ユーザーがCyber Risk Assistantにプロンプト入力（例：「最も重大な脆弱性を修正して」）。
- AI Fabricが指示を解析し、関連する資産・脆弱性・ビジネスコンテキストを取得。

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。

Qualys.

リリース済み

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

2025年11月公開ブログはこちら

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）

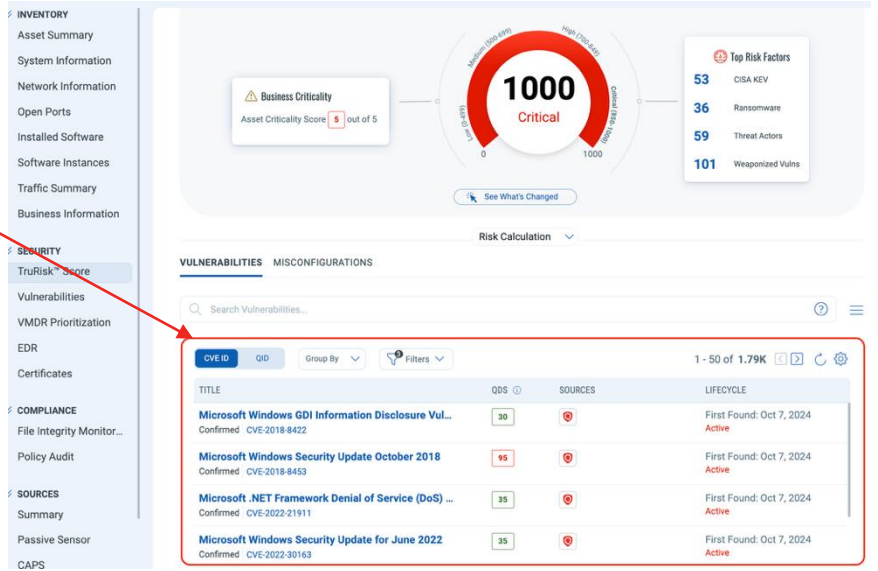
最も**深刻な脆弱性**と**発生件数**に注目。
平均値方式で起こりうる誤ったリスク感の増加を防止。

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。**

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。