超優先順位付けと自律的修復の運用化

(Operationalize Hyper-prioritization and Autonomous Remediation)

「ポスト・ミュトス時代」における
脆弱性の急増への対処

クォリスジャパン株式会社
更新日：2026年9月1日

サイバーセキュリティの転換点:

サイバー兵器としてのフロンティアAIの台頭

フロンティアモデルの能力

専門家が見落としたソースコード内の脆弱性を発見します。

数分でエクスプロイトを開発し、複数の脆弱性を組み合わせて攻撃経路を特定します。

組織への影響

脆弱性情報の公開数が急増する一方、**NVDによる情報拡充が追いついていない**

悪用までの時間は**数時間**にまで短縮されています。一方、平均MTTR（平均修復時間）は30日を超えています。

QualysによるGlasswing経由のMythosへのアクセス

ソースコードの強化と脅威調査

Claude Mythos

Qualysは、AnthropicのProject Glasswing（第2期）およびOpenAIのTrusted Access for Cyberプログラムに参加しました。

Glasswingパートナーのユースケース

1. **製品のセキュリティ強化**
   Mythosを使用して自社のソースコードをスキャンし、これまで発見されていなかった脆弱性を検出・修正します。
2. **脅威調査**
   脆弱性調査、マルウェア分析

Glasswingのパートナー企業は、顧客環境でMythosを使用することは禁止されています。上記のとおり、Mythosは社内でのみ使用できます。

非対称性:
AIの速度で迫る脅威と、手動による修復プロセス

6倍

2026年7月の「Microsoft Patch Tuesday」におけるMythos以降のCVE件数

0.74%

2025年に公開された4万8000件のCVEのうち、攻撃に悪用されたもの。

30日間以上

脆弱性が完全に解消されるまでの期間の中央値

攻撃者のサイクル — 数時間 — 発見 → 武器化 → 悪用

レガシーなディフェンダー(脆弱性管理)サイクル — 数週間から数ヶ月 ― スキャン期間、手動でのトリアージ、承認、四半期ごとのサイクル

両者の間の時間差が、エクスポージャーウィンドウとなります。

脆弱性悪用は、最も多いアクセス経路です

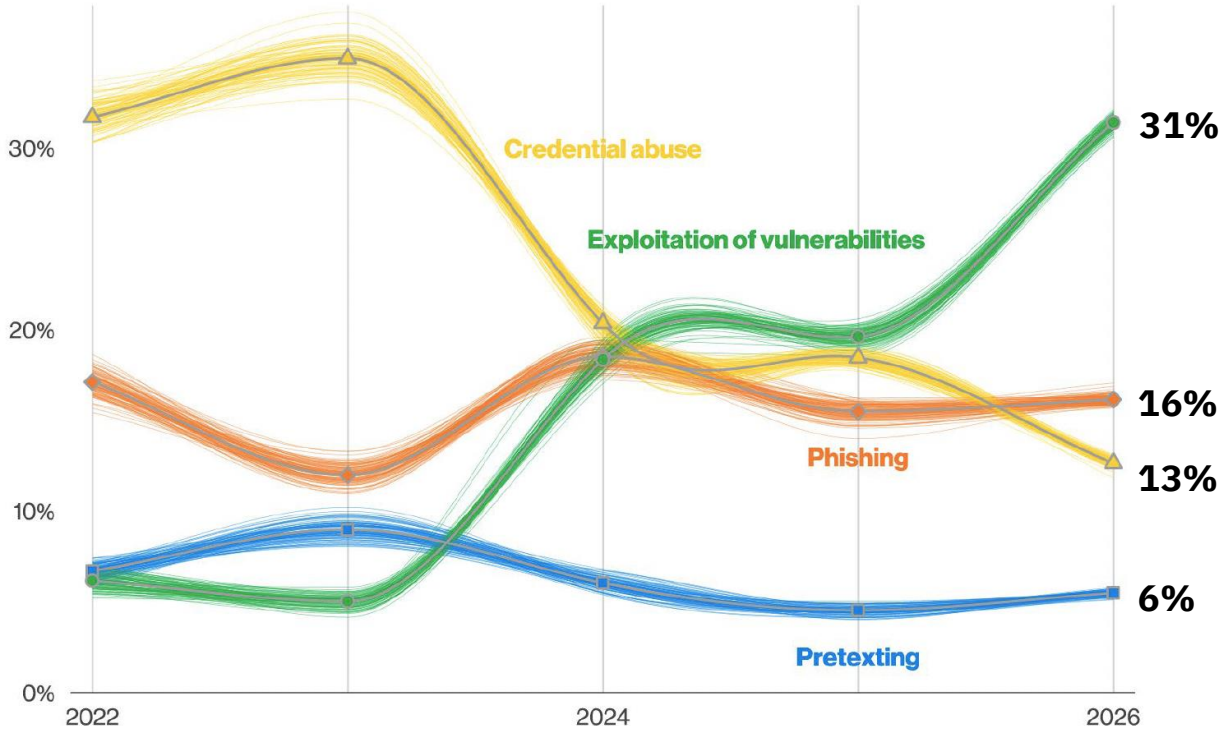


図5. エラーや不正使用以外の侵害における既知の初期アクセスベクトルの推移
（2026年のデータセットの数n=19,905）

今後の展望

攻撃者は情報公開後の数時間以内に悪用するため、環境内の悪用可能な脆弱性に対する修復速度は、マシンの速度と同等でなければなりません。

必要なソリューション:

Autonomous Remediation (自律的な修復)

AIネイティブのRisk Operation Center（AI-ROC）

自律的修復を運用可能にする

自律的修復を運用可能にするためのステップ

AIスピードによる高速検出

- 情報開示速度の迅速な脆弱性検出
- 構成（コンフィギュレーション）の評価
- オンプレミス、クラウド、アプリケーション、コンテナへの対応

超優先順位付け

- 統合された資産インベントリ
- 脅威、ビジネス、および資産のコンテキストに基づいて優先順位を決定
- 補完的コントロールを考慮した上で、エクスプロイト（悪用）の可能性を検証

ゼロデイ修復

- パッチ適用型およびパッチレス型の修復策を提供する
- 設定の不備を修正する
- 運用上のレジリエンスを確保しつつ、自動化を実現する

自律的な修復

Qualys AI-ROCを搭載

AIスピードによる高速検出

- 情報開示速度の迅速な脆弱性検出
- 構成（コンフィギュレーション）の評価
- オンプレミス、クラウド、アプリケーション、コンテナへの対応

Agent Insta

超優先順位付け

- 統合された資産インベントリ
- 脅威、ビジネス、および資産のコンテキストに基づいて優先順位を決定
- 補完的コントロールを考慮した上で、エクスプロイト（悪用）の可能性を検証

Agent Val

ゼロデイ修復

- パッチ適用型およびパッチレス型の修復策を提供する
- 設定の不備を修正する
- 運用上のレジリエンスを確保しつつ、自動化を実現する

Agent Sara

AIスピードの検出
(AI-Speed Detection)

Qualys®

AIスピードによる高速検出のケース

検知のギャップに注意

攻撃者は数時間単位で動く

業界は依然としてスキャン・ウィンドウ（定期的スキャン）に依存している

「スキャンレス・スキャン」の登場

InstaScan

Agent Instaが提供

数十分以内に検知

アドバイザリの公開から
数十分以内に、新しいCVEが
ETMに反映されます

再スキャンは不要

既に収集済みのテレメトリと
インベントリ情報を活用します

常時監視・検知

アドバイザリや資産の変更を
トリガーとして実行される、
AI駆動の継続的な評価

Qualys Blog　　Video

新たな資産やエクスポージャーを、発生したその瞬間に把握する

フロンティアAIがゼロデイの脅威を検知した際、経営層は数分以内に以下の情報を把握する必要があります。

影響を受けるシステムは何か、その所有者は誰か、そしてそれらがミッションをどのように支えているか。

~hours

ゼロデイ・シグネチャの中央値
（優先ベンダー：6時間）

99%+

CISA KEVカバー範囲
— 業界最高水準

Six Sigma

検出精度、10年以上

Minutes

InstaScanで新たなCVEを検出
— 再スキャンは不要

あらゆる領域を網羅する単一のインベントリ

オンプレミス、クラウド、コンテナ、OT（港湾、空港、国境）、そして外部攻撃対象領域（EASM）にわたり、継続的に資産を可視化・把握します。各資産は、所有者、業務上の役割、重要度、SBOM（ソフトウェア部品表）、および補完的コントロールと紐付けられます。**外部に存在する「未知の資産」は全体の20～25%に過ぎませんが、攻撃の70%はこれらを起点として発生しています。**

スキャン不要の常時稼働型シグナル

InstaScanは、すでに収集済みのテレメトリを評価します。新たなCVE情報は、アドバイザリの公開から数十分以内にROC（リスク・オペレーション・センター）に反映されるため、新たなスキャンジョブの実行やエージェントによるシステムへの負荷は発生しません。スケジュールではなく、アドバイザリや資産の変更をトリガーとして動作します。

InstaScan導入前と後の比較

導入前 ー 業界の現状	導入後 ー InstaScan活用時
シグネチャー・パイプラインの所要時間：平均12～24時間	**60分以内**の検知
日次バッチリリース	**CVE単位**の継続的デリバリー
スケジュール化されたスキャンおよびポーリング	**イベント駆動型**評価

超優先順位付け
(Hyper-Prioritization)

Qualys®

徹底的な優先順位付けを行うべき理由

0.74%

2025年の武器化されたCVE

上記のなかで、貴社の管理策を考慮した際、本番の運用環境において実際に悪用可能なものはその一部に過ぎません。
それらを優先的に対処できていますか？

数字で見る脆弱性ノイズ

年	開示済み	武器化済み	割合
2022	25,043	131	**0.52%**
2023	28,816	185	**0.64%**
2024	39,964	218	**0.55%**
2025	48,172	357	**0.74%**

The Broken Physics of Remediation, Research Report from Qualys TRU

Qualys ETM が Agentic AI で CTEM を運用可能

統合資産インベントリ (CSAM)

外部および内部の攻撃対象領域全体をリスクコンテキストとともに包括的に可視化します。技術資産を、重要度および関連リスクとともに、ビジネスエンティティに自動的にリンクします。

TruRisk: ビジネスにおけるサイバーリスクの定量化

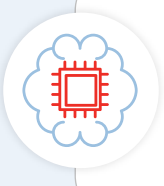
脅威、資産、ビジネスコンテキストに基づいて優先順位付け。
ビジネスへの影響に基づいて**定量化**。
環境要因とリスク軽減策に基づいて**リスクをカスタマイズ**。

エクスポージャーの集約

Qualysおよびサードパーティ製セキュリティツールから得られたセキュリティ検出結果を集約、正規化、重複排除することで、リスクの統合ビューを実現します。

TruLens: 脅威ベースのリスク優先順位付け

QualysのTruLensモバイルアプリを使えば、**業界における新たな脅威やトレンド**を常に把握し、リスクの優先順位付けと軽減計画を可視化することで、常に先手を打つことができます。外出先でも状況を把握可能です。



サイバーリスク・エージェントのマーケットプレイス

TruRiskのインサイトを活用したQualysの**「サイバーリスク・エージェント」**および**「サイバーリスク・アシスタント」**は、すぐに利用可能であり、セキュリティチームを戦略的なオーケストレーターへと変革します。

TruConfirm: 脆弱性の悪用可能性を検証

セキュリティ対策を検証しながら、**脆弱性の悪用可能性を確認**します。
悪用可能性が確認された脆弱性を優先的に処理することで、脆弱性の修復を迅速化します。

TruConfirm と Agent Valによる、実環境での悪用可能性の検証

TruConfirm

実証に基づく、本番環境でも安全なエクスプロイト検証

実際の構成やセキュリティ対策が適用された稼働中の資産を対象に、エクスプロイトの可否を検証します。

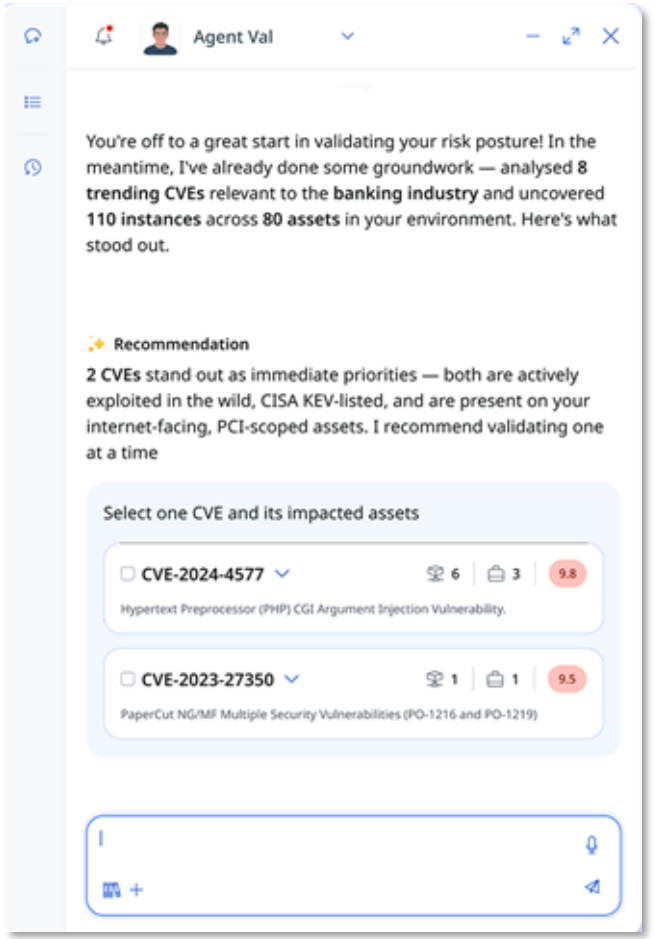
以下の**3つ**の結果を生成します:

A. 悪用可能
B. セキュリティ対策によりブロック済み
C. 到達不能

Agent Val

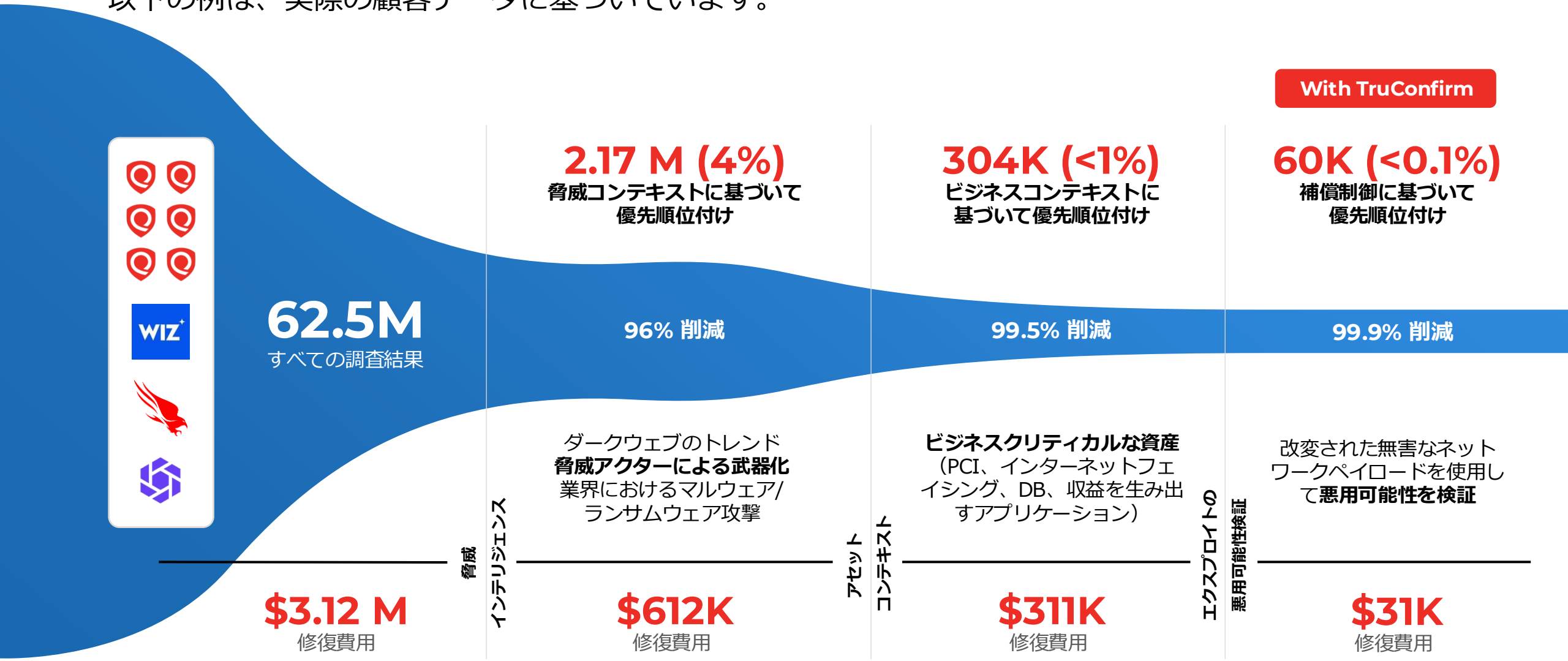
業界初の、エクスプロイト検証のためのエージェント型AI

継続的に次の対象を選定し、本番環境で安全にTruConfirmを実行して修正を推進し、完了の再検証を行う。



検出から優先順位付け、そして超優先順位付けへ

以下の例は、実際の顧客データに基づいています。



ゼロデイ修復
(Zero-day Remediation)

Qualys®

Qualys TruRisk Eliminate は、サイバーセキュリティの修復ソリューションです。

**ITパッチ適用における
スピードギャップを埋めるための
サイバーセキュリティ対策ソリューション
があることを、経営陣に確信させましょう。**

自律的な修復に対する信頼を築く方法

運用のレジリエンスへの確信を支える機能

パッチが上手く適用されるかどうか、どうすれば分かりますか？	**パッチ信頼性スコア**
パッチが利用できない場合、またはパッチが信頼できない場合は、どのように対処すればよいですか？	**パッチレスの修復**
重要度の低いマシンから重要度の高いマシンへと段階的にデプロイすることは可能ですか？	**段階的なデプロイ**
異常な動作が発生した場合、修復措置を元に戻すことはできますか？	**ロールバック機能**

TruRisk Eliminate: シックスシグマ精度で修復する

AIベースのレコメンデーションエンジン

脆弱性を最適な修復オプションにマッピングする

パッチ

- Windows、macOS、Linux
- サードパーティ製アプリ
- ゼロタッチパッチ自動化
- **AIベースのパッチ信頼性スコア**

アンインストール

- 脆弱性のある未使用のソフトウェアをアンインストールする

緩和

- パッチが利用できない場合や危険な場合は、エクスポージャーを減らす

カスタム

- 複雑なケースに対応する、すぐに使えるスクリプト
- ファーストパーティアプリ向けに独自のスクリプトを作成

隔離

- 最終手段としての封じ込め
- 高リスク機器を封じ込め、遠隔でパッチを適用する

TruRisk Eliminate: 最高水準の実績

世界中で実証され、信頼されている

5億件以上
パッチ展開数

#1
GigaOm
ランキング

機能する自動化

1億以上
自動化による
パッチ適用済み数

0.1%未満
ロールバック率

AIを活用した パッチ信頼性スコア

ウェーブ
段階的な
ロールアウト

98.2%
初回成功率

パッチ適用不要の修復に関する顧客事例

40K
サポートが終了した.NETの脆弱性、**16日間**で**アンインストール**により解消

27K
WinVerifyTrustの脆弱性、わずか**3日**で修正

10K
Birthday 攻撃の脆弱性、**6日**で**修正**

TruRisk Eliminateによる顧客への影響

80%

修復にかかる
平均時間の短縮

1日未満

エクスプロイトが確認
された脆弱性の修復に
かかる時間

0.1%未満

自動パッチ適用にお
けるロールバック率

クラウドネイティブスタックのリスク軽減

Qualys TotalCloud + TotalAppSec + TotalAI

フルスタックディスカバリ

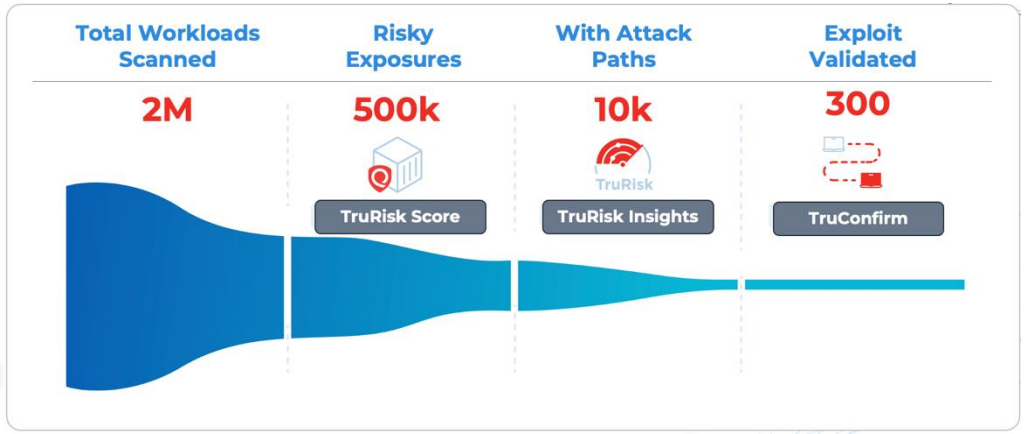
Flex スキャニング
エージェント &
エージェントレス

フルスタックディスカバリー
– Cloud, API, AI

コードからランタイム
コンテキストへ

**相互接続された
攻撃対象領域を発見する**

ランタイムコンテキストで優先順位付け



**エージェンティック技術を活用したエクスプロイト検証により、
実際に悪用可能な少数のリスクに焦点を当てる**

自律的に修復

脆弱性対応
Qscanner 自動パッチ- コードからクラウドへ
カスタム緩和策のためのCAR

リスク対応
QFlowを活用したクラウドスタック全体に
わたるノーコードプレイブック

脅威への対応
ランタイム駆動型コンテインメント

**リアルタイムで対応しましょう!!
チケット管理や手動での対応は、
もはや選択肢にはなりません。**

包括的かつ柔軟なプラットフォームAI戦略

各ユースケースに最適なモデルを採用し、推論能力とコスト効率を最大化します。

現在のプラットフォームにおけるマルチモデル統合

エージェント型AIおよびサイバーリスクエージェントフレームワークで活用

- オープンソースモデル
  (Llama, Mistral)
- カスタマイズされたSLM
  (Phi-4 Mini from Microsoft)
- Anthropic社のLLM
  (Claude Haiku / Sonnet / Opus)

脅威の調査・防御のためのモデル

研究および防御能力に関する既存のパートナーシップ

- Anthropic社のGlasswingおよびサイバー検証プログラム（CVP）。
  Mythos, Opus 4.8
- OpenAI社のサイバー向け信頼アクセス（TAC）。
  GPT-5.5-Cyber
- ユースケース:
  脆弱性調査、ゼロデイ脆弱性の発見、エクスプロイト開発、マルウェアのリバースエンジニアリング、レッドチーミング

SASTのユースケースに向けたモデルとの統合

ファーストパーティアプリの脆弱性に対するClaude Securityの統合

- ソースコードの検出結果をQualys ETMに取り込む
- Qualysを活用し、ランタイムコンテキストを適用して優先順位を決定する
- 優先順位付けされた脆弱性にパッチを適用する

ANTHROP\C　Mistral AI　OpenAI　Microsoft　Meta

統合プラットフォームによるフロンティアAI時代のリスク管理

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、クラウド、およびコンテナインフラストラクチャ全体にわたる、高精度な脆弱性検出。
- リスク管理およびコンプライアンス・ワークフローの基盤。

主要な機能

- 13万件以上のCVEを網羅し、業界トップクラスのカバー率を実現
- CISA KEVの99.4%をカバー
- デジタル証明書の評価
- 設定評価（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

超優先順位付け
ETM

Agentic AIによる運用可能なCTEM

価値

- 攻撃者に狙われる前に最もリスクの高いエクスポージャーに対処し、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倍に強化
- ビジネスへの影響に基づいた、リスクの統合的な可視化

主要な機能

- 統合アセットインベントリ (CSAM)
- QualysおよびQualys以外のセンサーによる統合リスクビュー
- アセットと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・ワークフロー向けAIエージェント

カテゴリリーダー

ゼロデイ修復
Eliminate + Audit Fix

パッチ適用とパッチレスによる修復

価値

- マシン・スピードで修復
- セキュリティとIT部門の連携を円滑化
- 運用レジリエンスを確保

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を活用したパッチの信頼性スコアと段階的展開
- 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
- ランサムウェアに対する100%の網羅性

ソリューション紹介やデモのご依頼はsales-jp@qualys.comまでお問い合わせください。

Qualys®

Additional Slides as Needed

Qualysプラットフォームを基盤とするAI-ROC

AIスピードによる高速検知

RBVM VMDR	• CISA KEVの99.6%をカバー • CISA KEVの45日前から優先的に検出 • 15,000件以上の非CVEを検出
ASPM TotalAppSec	• WebアプリおよびAPIの検出とスキャン • WebアプリおよびAPIの脆弱性、設定ミス、コンプライアンスの検出
CNAPP TotalCloud	• 市場をリードするCNAPP • 対応時間を70%短縮
AI-SPM TotalAI	• すべてのAI/LLMワークロードのインベントリを検出 • AIとLLMのリスクを軽減
ISPM ETM-Identity	• 人間と機械のIDのリスクを低減し、ID主導型攻撃の対象領域を縮小

超優先順位付け

CTEM + CRQ + Agentic AI

Enterprise TruRisk Management

統合資産インベントリ (CSAM)
エクスポージャー集約
サイバーリスク定量化
優先順位付け (TruRisk & TruLens)
悪用可能性検証 (TruConfirm)
サイバーリスクアシスタントおよび
AIエージェント

サードパーティースキャナーによる検出結果

ゼロデイ修復

修復 / RemOps

Eliminate

- パッチ適用、緩和、隔離機能を内蔵
- MTTR（平均復旧時間）を80%削減
- 業界トップクラス
- AI搭載パッチ信頼性スコア

コンプライアンス

Policy Audit

- 政府および業界標準に準拠する
- ファーストパーティアプリの脆弱性を検出する（CAR）
- ファイル変更を監視する（FIM）

Mythos、プロジェクト Glasswing、そしてその影響

Anthropic Claude Mythos プレビュー

Mythos: ソースコード内の未知の脆弱性を発見し、エクスプロイトを開発できるフロンティアモデル。

Glasswing: Mythos ― 広範な導入実績を持つ特定のベンダーに対し、ソースコード内の脆弱性を特定・修正するためのプレビュー・アクセスを提供します。

43% CISA KEVの 43%は Glasswingのローンチパートナーの製品に起因している。

Qualys製品はCISA KEVには掲載されていません

Mythosとその他のモデルの影響

1. 脆弱性の爆発的な増加
2. NVDによるCVE情報の大部分の拡充が困難に
3. 悪用までの時間が数時間単位に短縮

修復の壊れた物理学
The Broken Physics of Remediation

6.5倍	過去4年間における重大な脆弱性の件数
67日	MTTRの中央値
1%未満	武器化された脆弱性

Source: Qualys TRU Research

10億件のCISA KEVデータに基づく、この種の研究としては最大規模の調査。
4年間にわたる1万の組織における修復記録を分析。

レポートをダウンロードする

Qualys Research Unit - 修復における理論の限界 (日本語翻訳)
https://cdn2.qualys.com/docs/mktg/jp/qualys-tru-the-broken-physics-of-remediation-japanese.pdf

[Blog] **Threat Research Report: The Broken Physics of Remediation**
https://blog.qualys.com/vulnerabilities-threat-research/2026/03/23/the-broken-physics-of-remediation
(その他上記関連Blogはこちら)

従来のCTEMツールは、
AIのスピードで動く攻撃者についていけない

検知の集約に時間がかかりすぎて、即時の確認すら困難

データの集約には24時間以上を要します——攻撃者がすでに武器化しているものを含め。

あくまで理論上のリスク

悪用可能性の裏付けがない数千件もの「クリティカル（重大）」な脆弱性——攻撃されることなどまずない（99%以上を占める）それらのために、無駄にリソースが費やされている。

ダッシュボードツーリズムやチケット管理にとどまる

従来のCTEMはリスクを評価するだけで、決して解決には至りません。
修復作業は依然として手動で行われ、数週間の遅れが生じます。

修復までの時間の短縮には寄与しない

最適な修復方法（パッチ適用または緩和策）に関する知見が得られない。
修復の迅速化にはつながらない。

完全自動化された検出

平均検知時間：6時間

TECHNOLOGIES

62

62種類の製品がサポートされており、
署名の自動化も完全に行われています。

実行スケジュール

6 AM / 12 PM
6 PM / 12 AM IST

35	**Linux ディストリビューション** RHEL, Debian, Ubuntu, SUSE, CentOS, Alpine, Fedora, Oracle, Amazon, Rocky, Alma, Photon, Mariner...
11	**ベンダーのアプリケーション** Adobe, Mozilla, Google Chrome, Apple (Safari/Xcode/iTunes/macOS), Wireshark, Foxit, PDF-XChange...
6	**サーバーとミドルウェア** Apache Tomcat, Red Hat JBoss Web Server, JBoss Core Services, Mattermost, Couchbase, FreePBX
8	**ネットワーク／セキュリティ＆クラウド** PAN-OS, FortiOS (4 products), Dell BIOS, NetApp ONTAP, VMware ESXi/Workstation/Fusion, Aruba ECOS

部分的に自動化された検出

シグネチャは自動的に生成され、その後手動レビューによって検証されます。

TECHNOLOGIES

32

以下の製品では署名作成は完全に自動化されていますが、品質保証テストは手動で行われます。

6	**Atlassian Suite** Jira, Confluence Server, BitBucket, Bamboo, Jira Service Mgmt (JSMD), Jira Server & DC
5	**ネットワークおよびセキュリティ機器** F5 BIG-IP, Palo Alto GlobalProtect, Aruba AOS, Aruba CX, Juniper Junos OS
5	**CiscoエコシステムとSplunk** Cisco IOS / IOS XE, Cisco Nexus (NX-OS), Cisco ISE, Splunk Enterprise, Splunk Universal Forwarder
16	**その他のベンダー製品** Microsoft Office, Edge Chromium, VLC, WordPress, Drupal, Zoom, GitLab, SolarWinds, Liferay, IBM AIX, Joomla, Sitecore, MongoDB, Octopus, Jenkins...