



ビジネス

Qualys TruConfirm: 脆弱性の推測に終止符を

QUALYS TRUCONFIRM: 脆弱性の推測に終止符を

セキュリティチームは日々、不可能とも思える課題に直面しています。

脆弱性スキャナーは、数千件、時には数百万件もの「重大な」脆弱性を検出します。経営陣は明確な回答を求め、監査担当者は確固たる証拠を要求します。チームがダッシュボードを精査し、優先順位を議論している間に、攻撃者は既に実際に有効なごく一部の脆弱性を悪用し始めています。

現実には厳しい。重大な脆弱性と分類された脆弱性のうち、実際に悪用されるのは1%未満に過ぎない。にもかかわらず、従来のスキャナーはそれらすべてを同等に緊急性の高いものとして扱い、チームをノイズで圧倒し、真に重要な脆弱性を覆い隠してしまう。

その結果は容易に想像できる。高度なスキルを持つセキュリティエンジニアは、実証済みの攻撃経路を排除するのではなく、理論上のリスクを追いかけることに時間を費やす。修復作業の滞留は増大し、信頼は失われる。そして、侵害は依然として発生し、平均488万ドルの損失につながる。

では、別の質問を考えてみましょう。 **攻撃者があなたの環境で実際に悪用できる脆弱性を、今すぐにでも確実に知ることができるとしたらどうでしょうか？**

TruConfirmのご紹介:

Qualys TruConfirmは、推測ではなく証拠に基づいてリスクを評価することで、リスク管理のあり方を根本から変革します。ソフトウェアのバージョンや静的な深刻度スコアからリスクを推測するのではなく、TruConfirmは、脆弱性が実際の運用環境で悪用される可能性があるかどうかを検証します。

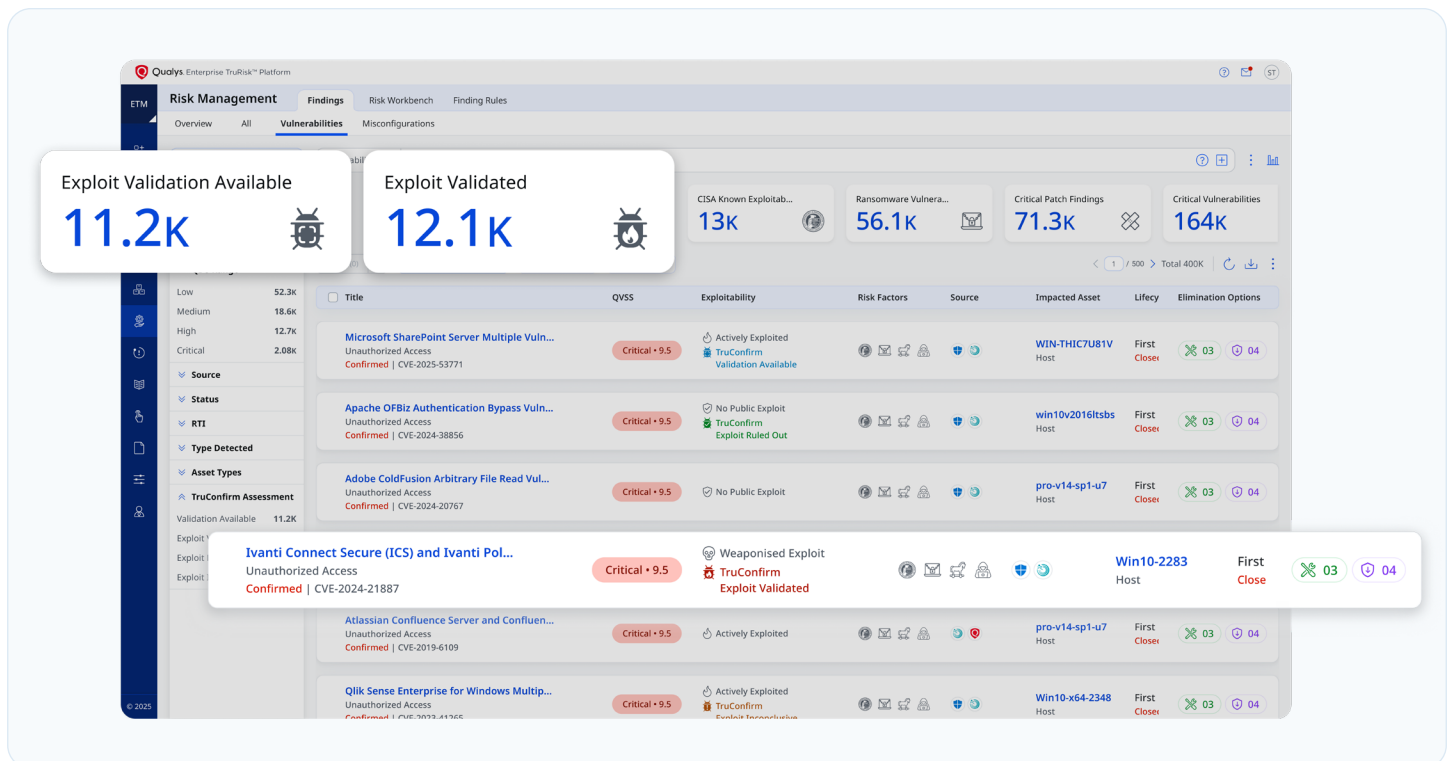
従来のスキャナーは、狭い範囲の質問しか投げかけません。

「このバージョンは潜在的に脆弱性があるか？」

TruConfirmは、より重要な質問に答えます。

「攻撃者は、私の環境で、今すぐにこの脆弱性を悪用できるのか？」

この違いは漸進的なものではなく、根本的なものです。TruConfirmは、リスク管理を確率的推論から決定論的証明へと移行させることで、リスクの優先順位付け、議論、そして最終的な排除の方法を変革します。



TruConfirmは、悪用可能性を直接検証することで、両方の失敗モードを排除します。つまり、仮定を証明に置き換えるのです。

バージョンベースの検出が失敗する理由

従来の脆弱性スキャナーのほとんどは、単純で根本的に欠陥のある前提に基づいています。それは、ソフトウェアのバージョンが既知のCVEと一致する場合、それは悪用可能なリスクを示すというものです。

しかし、この前提は現実の環境では成り立ちません。バージョンベースの検出は、攻撃者が実際に攻撃を成功させるかどうかを決定づける条件を無視しているのです。

到達可能性	
脆弱なコードが存在する	脆弱なコードパスは実行される可能性があるか？
エクスポージャー	
サービスが稼働している	サービスは現在稼働しており、アクセス可能であるか？
コントロールの有効性	
この脆弱性は悪用可能です。	WAF、ファイアウォール、IPSなどの既存の防御策は、この攻撃経路を阻止できていますか？

これらの疑問に対する答えがなければ、深刻度は推測の域を出ません。

このギャップは、2つの深刻かつコストのかかる障害モードを生み出します。

誤検知: チームは、ロードされない、アクセスできない、あるいは既に補償制御によって緩和されているライブラリのパッチ適用に何週間も費やします。

見落とされた脅威: ブラインドSSRFや非同期RCEといった、影響度の高いブラインド脆弱性は、攻撃者が密かに悪用しているにもかかわらず、目に見えるスキャナー出力がないため見過ごされがちです。

TruConfirmは、悪用可能性を直接検証することで、これらの見落としを解消します。つまり、推測ではなく証明によって検証を行うのです。

TruConfirmの特長: 攻撃者が見ているものと同じ視点から監視

TruConfirmはリスクを推測するのではなく、検証します。倫理的ハッカーやレッドチームが使用する実行パスとテクニックをそのまま適用しますが、エンタープライズ規模での安全かつ自動化された運用を実現するために再設計されています。推論に頼るのではなく、TruConfirmは3つの決定論的な検証方法によって確実性を確立します。

確実性を支える3つの柱

01 直接応答検証

従来のソフトウェアスキャナーは、ソフトウェアのバージョンに脆弱性があるかどうかに基づいてリスクを推測します。TruConfirmはさらに一歩進んで、実行を直接検証します。安全で非破壊的なペイロードを配信し、システムの実際の応答を評価します。

コマンドが実行されれば、その証拠は明確かつ観測可能です。解釈の余地も、バージョン照合も、曖昧さも一切なく、脆弱なコードパスに到達可能で悪用可能であるという監査可能な証拠のみが得られます。

02 暗号検証

コードインジェクションのシナリオにおいて、TruConfirmは脆弱な文字列照合ではなく、数学的な確実性に基づいています。検証ペイロードは、ターゲットシステムに対し、固有のシードから導出された暗号学的ハッシュを計算するよう指示します。このハッシュは、注入されたコードが正常に実行された場合にのみ生成されます。

これにより、なりすまし、リフレクションによるアーティファクト、誤検出が排除されます。結果として得られるのは、ヒューリスティックな推測ではなく、実行の決定論的な証明です。

03 帯域外検出 (サイレント検証)

目に見える反応を示さないため、ブラインド脆弱性は最も高いリスクをもたらします。TruConfirmは、サイレント検証アーキテクチャによってこの種の脆弱性に対処します。

攻撃者がシステムを強制的に操作して、攻撃者のインフラストラクチャへのアウトバウンド接続を開始させた場合、TruConfirmは、Qualys TruConfirmセキュアクラウドへの制御されたコールバックを誘発することで、悪用可能性を証明します。コールバックがない場合は、悪用経路が実行不可能であることを意味します。コールバックを受信した場合は、実行が行われ、アウトバウンド制御がそれを許可したという反論の余地のない証拠となります。

本番環境向けに構築。信頼性を追求した設計。

アクティブエクスプロイト検証に対する最も一般的な反対意見は、単純かつ正当なものです。 **本番システムを危険にさらすことはできないからです。**

TruConfirmは、この懸念を完全に解消するために設計されました。安定性、パフォーマンス、データ整合性が絶対条件となる本番環境向けに、最初から設計されています。すべての検証方法、ペイロード、実行パスは、中断なく検証を優先する安全第一の制御によって制約されています。

その結果、運用リスクを伴わずに確実なエクスプロイト検証を実現し、従来のツールでは推測に頼らざるを得なかった検証を、証明可能な形で実現します。

5つの安全原則

TruConfirmの脆弱性検証は、5つの譲ることのできない安全原則に基づいています。これらの原則は、本番環境において中断なく検証結果を確実に得るために設計されています。

01 事前照会検証

TruConfirmは、ペイロードを送信する前に、ターゲットサービスの存在と脆弱性の有無を確認します。検証は正確かつ意図的に行われ、決して無差別に、あるいは「手当たり次第に」行うことはありません。

02 無害なペイロードのみ

攻撃者が破壊的なコマンドを実行する場合、TruConfirmは無害な検証アクションに置き換えます。ペイロードは、「hello」のような制御されたネットワークコールバックなど、無害な操作を要求し、影響を与えることなくエクスプロイトパスが存在することを証明します。

03 ゼロフットプリント

エージェントはインストールされません。ファイルの書き込みや変更も行われません。

設定も変更されません。すべてのやり取りは一時的なものであり、検証完了後には痕跡は一切残りません。

04 ノンブロッキング操作

すべての検証は非同期で実行されます。主要なアプリケーションスレッドは影響を受けず、ユーザーは遅延を感じることなく、テスト中も本番システムは通常どおり動作し続けます。

05 プライバシー・バイ・デザイン

脆弱性の検証は、顧客データではなく暗号学的ハッシュ値に基づいて行われます。万が一ログが検査された場合でも、機密性の高いアプリケーションロジック、コンテンツ、または専有情報が漏洩したり保持されたりすることはありません。

TruConfirmのペイロードはすべて、**Qualys脅威調査ユニット（TRU）**によって、リリース前に隔離されたサンドボックス環境で作成、検証、およびストレステストされています。各検証手法は、有効性だけでなく、安全性、再現性、および本番システムへの影響ゼロの実行についても評価されます。その結果、エンタープライズレベルのリスクを導入することなく、エンタープライズレベルの確実性を提供するエクスプロイト検証が実現します。

ビジネスへの影響: バックログからアクションへ

TTTruConfirmは、手作業と議論をエビデンスに基づいた実行に置き換えることで、脆弱性管理の経済性を変革します。その結果、単なる量的管理から真のリスクの排除へと、目に見える形で移行が実現します。



攻撃者が実際に悪用できる脆弱性に**焦点を絞る**



手動によるトリアージを**自動化検証**に置き換える



実際に悪用可能な脆弱性に基づいて優先順位付けされた**リスクベースの修復対策**

運用上の影響: TruConfirm導入前と導入後

対象領域	TruConfirm導入前	TruConfirm導入後
アラート発生件数	明確なシグナルがないまま、数千件もの「重大な」検出結果が報告されていた	悪用が実証された脆弱性を絞り込んだリスト
検証作業	手動による検証と再検証に数週間を費やしていた	自動化されたエクスプロイト検証により、手動によるトリアージを代替
優先順位付け	CVSS、バージョン一致、スキャナースコアに基づいて検証を行っていた	検証済みの悪用可能性と攻撃経路に基づく
セキュリティ部門と運用部門の連携	深刻度と緊急度に関する議論が継続中	エビデンスに基づいた連携と迅速な意思決定
修復の重点	理論上のリスクに対する広範なパッチ適用	確認された脅威に対する精密な修復
コンプライアンス遵守の証拠	前提条件と推測される深刻度	悪用可能性とコントロール効果の監査可能な証明
MTTR (平均修復時間)	対応が遅く、一貫性がなく、バックログに左右される	リスクを大幅に軽減する脅威に対するMTTR (平均修復時間) の短縮



セキュリティ、運用、コンプライアンスの要件を満たす証拠に基づいて**行動できる自信**



最も重要な脅威に対する
MTTR（平均復旧時間）を短縮する

動的リスクスコアリング

TruRisk™スコアは、TruConfirmの検証結果に基づいて動的に調整されます。悪用可能性が確認されると、スコアは即座に引き上げられ、優先順位付けは理論上の深床度ではなく、**実際のエクスポートジャーリスク**を反映したものとなります。

時間の経過に伴うリスクスコアの上昇

検証済みの脆弱性は、常に変化します。確認された脆弱性が未対策のまま放置されると、TruRiskは経過時間に基づいたリスク上昇係数を適用します。放置時間が長くなるにつれてリスクも上昇し、対策が講じられて脆弱性が解消されるまで、緊急性が高まります。

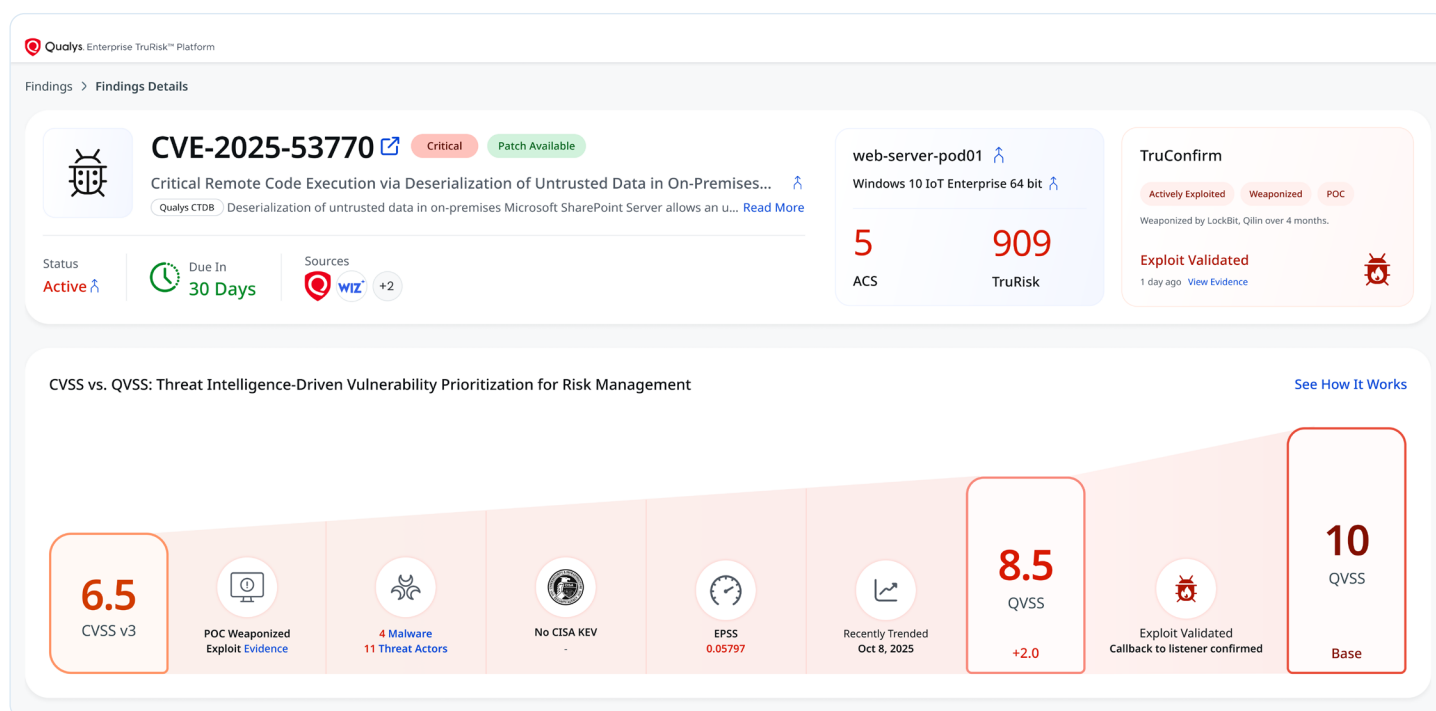
継続的な脅威インテリジェンス統合

脆弱性スコアは、EPSSの更新、CISA KEVの追加、ダークウェブの活動、新たに出てくる概念実証(POC)エクスプロイトなど、最新の脅威インテリジェンスを用いて継続的に更新されます。

TruConfirmによるスコアリングは、初期検出時のスコアではなく、常に**現在のベーススコア**を参照するため、優先順位付けは最新の攻撃者の実態を反映します。

影響

検証済みの脅威は即座に顕在化します。未解決の脆弱性は予測可能な形で拡大します。リスクが低減されるまで、優先順位付けは現実世界での悪用可能性に継続的に連動します。



攻撃対象領域全体を網羅する 包括的なカバレッジ

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。

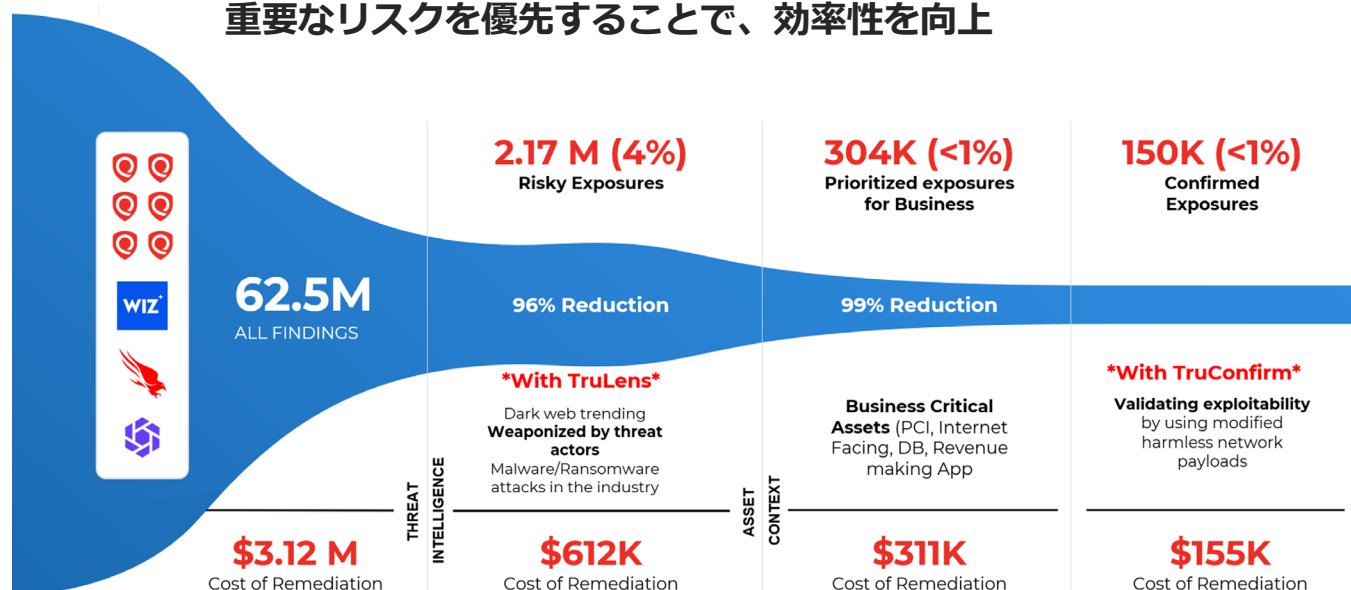
検証ライブラリは、**最近の脅威と継続的な脅威**の両方を網羅しています。

- 検証済みのCVEの**60%**は**2020年から2025年**の間に発生したものです。
- **40%**は**2020年以前に発生した脆弱性**で、現在も悪用されています。

このバランスは、実際の攻撃者の行動を反映している。既存の脆弱性は依然として確実な侵入経路として機能しており、新たな情報開示のみに焦点を当てると、既知の悪用可能な脆弱性が検証されないままになってしまう。

Qualysの脅威調査ユニットは、脆弱性が悪用されたり、高リスクのCVEが出現したりするたびに、新たな検証を優先的に実施することで、カバレッジを継続的に拡大しています。アップデートでは、実際に攻撃が行われていることが確認された場合、その年に公開された脆弱性を重点的に取り上げ、検証が攻撃者の実際の活動に遅れをとらないようにしています。

重要なリスクを優先することで、効率性を向上



Qualys ETMによる最新のエクスポージャー管理

TruConfirmは、断片化されたセキュリティシグナルを決定的なリスク軽減へと変換するために設計されたプラットフォーム、**Qualys Enterprise TruRisk Management (ETM)**の中核機能です。TruConfirmは、検出レイヤーを一つ増やすのではなく、エクスプロイト検証をETMの優先順位付けおよび対応ワークフローに直接組み込むことで、リスク管理をエビデンスに基づいたものにします。

TruConfirmは、企業向けに

1,600以上のCVE

の検出機能を提供します。

Qualys ETMに統合されているTruConfirmを活用することで、組織は以下のメリットを享受できます。

1. **攻撃者コンテキストの明確化:** どの脆弱性が実際に攻撃可能な経路であるかを明確に把握できます。
2. **精密な修復:** 悪用が実証された脆弱性にのみリソースを集中させることができます。
3. **リスク軽減の迅速化:** 検出から排除までを、議論や遅延なく迅速に進めることができます。
4. **取締役会に提出可能な証拠:** 推測される深刻度や理論上の脆弱性ではなく、検証済みのリスク状況に基づいたレポートを提供します。

リスク運用向け自律型エクスプロイト検証ツール「Agent Val」

Agent Valは、Qualys ETMのTruConfirmを支える意思決定およびオーケストレーションエンジンです。Agent Valは、AI駆動型のサイバーリスクエージェントとして、エクスプロイト検証を優先順位付け、検証、修復、再検証という継続的なクローズドループプロセスへと変革します。TruRisk、脅威コンテキスト、資産エクスプロイトプロファイル、ビジネス上の重要度、CISA KEVアライメント、エクスプロイトの可用性といった要素に基づき、テストすべきエクスプロイトを継続的に選択します。



Agent Val ?

Safe Exploit Validation with Proof

Safely validates whether high-risk exposures are exploitable in production using attacker-technique testing. It removes theoretical risk, proves control effectiveness, and gives Security and IT Ops shared evidence to minimize change friction with suppressed noise, reduce c...

Exploit Validation
Risk Prioritization
CISA KEV Analysis
+1

90%
Reduction in Remediation noise

55%
Reduction in TruRisk Score

70%
Manual Effort Reduction

What this agent does and when to use it
Onboard

優先順位が付けられると、Agent ValはTruConfirmを呼び出し、修正された無害なペイロードと、ターゲット資産およびCVEに適した検証方法（直接応答検証、暗号化検証、帯域外コールバック検出など）を使用して、本番環境における実際の悪用可能性を安全に検証します。

悪用可能性が確認されると、その結果はETMにフィードバックされ、リスクを高め、次を取るべき最適な行動を促し、対象を絞ったパッチ適用、緩和策、または補償制御を支援します。

修復後、Agent Valは同じエクスプロイトパスに対して検証を再実行し、脆弱性が実際に解消されたことを確認することで、仮説に基づく優先順位付けを証拠に基づいたリスク軽減に置き換えます。

エクスポート管理の未来は、その証拠によって示される

セキュリティ業界は長らく、何が脆弱で、何が悪用可能で、何が本当に重要なのかという点について、憶測に基づいて運営されてきた。しかし、攻撃者がパッチ適用サイクルよりも速いスピードで脆弱性を悪用する現代において、このモデルはもはや通用しない。

TruConfirmは、推測に頼る時代を終わらせます。確率を確実性へと変え、エクスポート管理を単なる量的作業から、確証に基づく規律へと変革します。

あらゆる修復判断がコスト、リスク、そして業務への影響を伴う現代において、確実性こそが最も価値のある管理手段となります。TruConfirmは、組織のリスク箇所とリスクのない箇所を明確に示し、その確実性を提供します。

Qualys TruConfirm

潜在的なリスクの山積み进行管理するのはもうやめましょう。
実証実績のあるリスクに絞り込み、排除に取り組みましょう。

Qualys Enterprise TruRisk ManagementとTruConfirmを体験し、監査、役員会、そして実際の攻撃者にも通用する証拠に基づき、環境内のどの脆弱性が実際に悪用可能であるかを確認しましょう。

デモを依頼する

qualys.com/etm



About Qualys

Qualys, Inc. (NASDAQ: QLYS) is a pioneer and leading provider of disruptive cloud-based security, compliance and IT solutions with more than 10,000 subscription customers worldwide, including a majority of the Forbes Global 100 and Fortune 100. Qualys helps organizations streamline and automate their security and compliance solutions onto a single platform for greater agility, better business outcomes, and substantial cost savings. For more information, please visit qualys.com. Qualys, Qualys VMDR® and the Qualys logo are proprietary trademarks of Qualys, Inc. All other products or names may be trademarks of their respective companies.