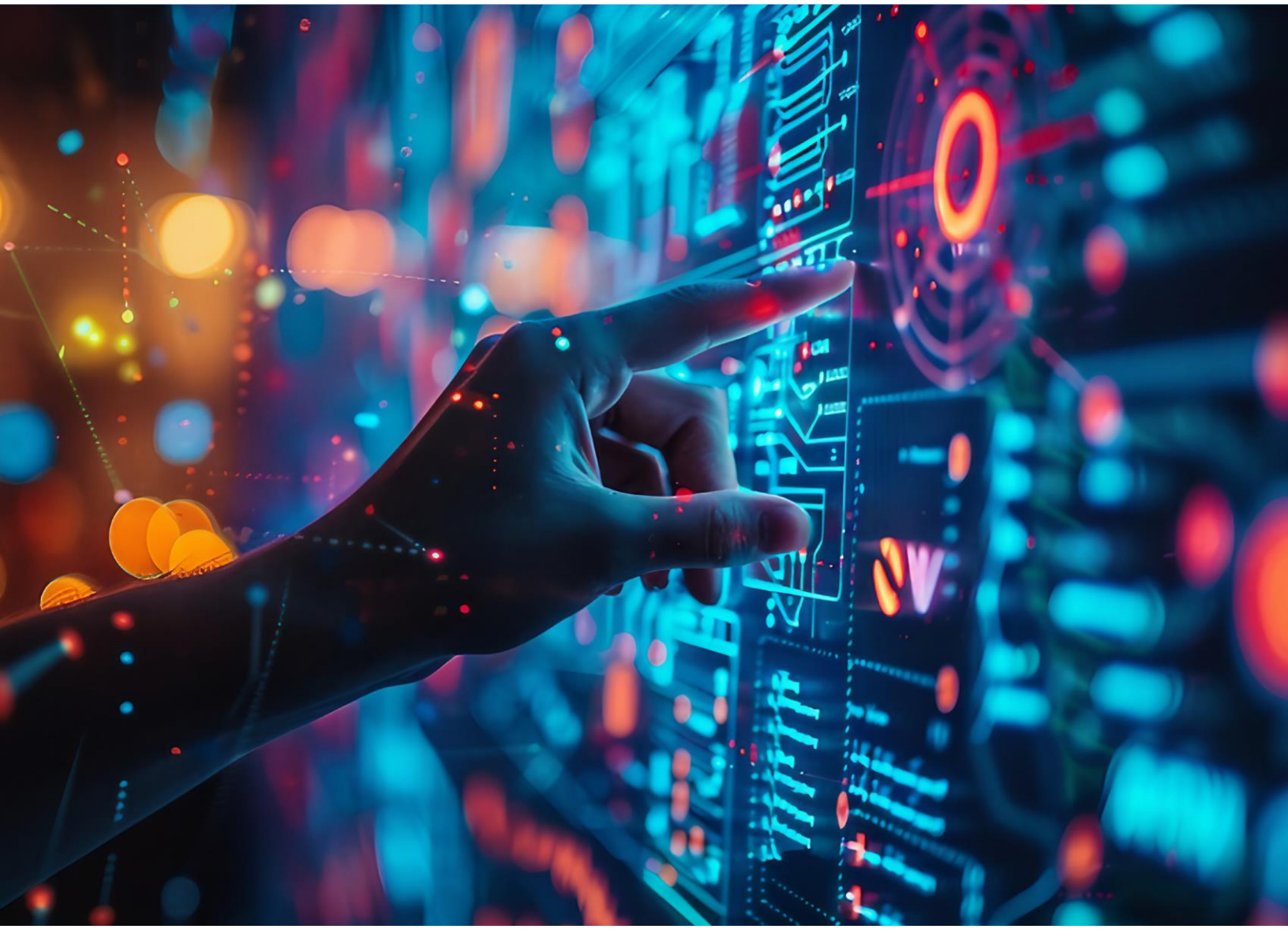
Qualys

ホワイトペーパー



TRURISK ELIMINATE

TruRisk™ Eliminate でサイバーリスク管理戦略を強化

エグゼクティブサマリー

従来のパッチ管理はソフトウェアアップデートで止まってしまいますが、今日のリスク排除にはそれ以上の対策が必要です。最新のハイブリッド環境では、ダウンタイム、アプリケーションの不安定性、パッチの入手不可といった理由から、すぐにパッチを適用できない脆弱性に直面するケースが多々あります。パッチ適用を遅らせるとシステムが脆弱な状態になり、逆に性急に適用すると重要なビジネスサービスが停止してしまう可能性があります。

Qualys TruRisk™ Eliminate は、脆弱性管理をパッチ適用にとどまらず、組織が迅速かつ的確に対応できるよう支援します。パッチ適用が遅れたり、適用にリスクが伴う場合でも対応可能です。このソリューションは、単一のリスク認識型ワークフロー内で、パッチ適用、緩和策、構成変更、制御された隔離など、リスクを軽減するための最も効果的で影響の少ない方法を継続的に判断します。

TruRisk Eliminate は、IT とセキュリティ運用を単一のプラットフォームに統合することで、脆弱性を単に管理するだけでなく、完全に排除することを保証します。柔軟な自動化、統合された変更管理、そして測定可能なリスク軽減に対する継続的な可視性により、より迅速な保護、より少ない混乱、そしてより強力なサイバーレジリエンスを実現します。

TruRisk Eliminate は、脆弱性を単に管理するだけでなく、完全に排除することを保証します。

TruRisk™ Eliminate とは？

Qualys TruRisk Eliminate は、脆弱性管理を事後対応型の特定から事前対応型のリスク排除へと変革するクラウドネイティブソリューションです。Qualys Cloud Platform 上に構築され、検出に使用されるのと同じ軽量エージェントを搭載した TruRisk Eliminate は、脆弱性を特定して優先順位付けするだけでなく、チームが脆弱性を**修正、軽減、または隔離**することを可能にします。これらすべてが、単一の統合ワークフロー内で実現されます。

TruRisk Eliminate は、エクスプロイト情報、資産の重要度、およびビジネスコンテキストを関連付けることで、あらゆる脆弱性に対して最も安全かつ効果的なアクションを決定します。パッチの適用、設定ベースの修正の適用、または Qualys 脅威リサーチユニット（TRU）が厳選した軽減策の提供など、最適なアクションが提示されます。修復がすぐにできない場合は、同じエージェントが影響を受けるシステムを一時的に隔離し、リモートパッチ適用機能を維持しながらリスクを封じ込めることができます。

TruRisk Eliminate は、複雑な環境全体にわたって保護を拡張するために、ポリシーとビジネスへの影響に基づいて継続的にパッチを適用し、脆弱性を軽減する**リスクベースの自動化機能**を提供します。これらの自動化されたワークフローにより、OS とサードパーティ製アプリケーションは手作業を必要とせずにセキュリティが維持され、組織は大規模なリスク対策、運用コストの削減、そして測定可能な継続的なリスク低減を実現できます。

TruRisk Automation は、顧客が最新のコンプライアンスに準拠した環境を維持することを可能にします。

大規模かつリスクを考慮した継続的なパッチ適用を自動化

TruRisk Eliminate が提供する自動化機能により、組織はオペレーティングシステムとサードパーティ製アプリケーションの両方を自動的にパッチ適用し、手動介入なしで継続的な保護を確保できます。設定が完了すると、自動化ジョブは定期的なスケジュールで実行され、組織のポリシーとリスク優先度に基づいて、必要な場所にインテリジェントにアップデートを展開します。セキュリティチームと IT チームは、資産の重要度に応じて適応する自動化ポリシーを定義できます。例えば、ワークステーションには最小限のテストでより頻繁にパッチを適用し、ミッションクリティカルなシステムには段階的なステージングと検証を通じて安全な展開を保証する「リングベース」の展開を適用できます。

Qualys の脆弱性検出、優先順位付け、および TruRisk スコアリングと統合することで、自動化エンジンはどの製品やアプリケーションを優先的にパッチ適用すべきかを動的に特定し、運用への影響を最小限に抑えつつ、リスクを最大限低減できるよう最適化します。
このリスクベースの自動化により、顧客は最新のコンプライアンス環境を維持しながら、すべての自動化アクションがビジネス上の許容範囲とセキュリティ目標に合致することを保証できます。

修復コックピット — セキュリティと IT の連携

TruRisk Eliminate (TRE) 修復コックピットは、セキュリティと IT 運用を単一の連携ワークフローに統合し、優先順位付けをアクションへと変換します。**セキュリティチーム**は TRE を使用して専用のコックピットビューを作成・割り当て、アプリケーション、事業部門、または資産グループごとに脆弱性をフィルタリングおよびグループ化します。これらのビューは**修復チーム**に引き渡され、修復チームは担当する脆弱性のみを、完全なコンテキスト情報とリスクベースのインテリジェンスによって強化された状態で確認できるようになります。

これらのコックピットビューから、修復チームは同じ Qualys Cloud Agent を使用して即座に対応できます。各脆弱性エントリには**豊富な選択肢が用意されており**、チームは TRE 内で最も効果的な対策を直接選択し、安全に実行できます。
環境とリスクプロファイルに応じて、チームは以下のことが可能です。

- 検証済みのアップデートが利用可能になったら、**パッチを適用します。**
- ベンダーパッチが提供されていない脆弱性に対しては、**Qualys が厳選し、すぐに適用可能な設定ベースの修正プログラムを適用します。**
- パッチ適用によって運用リスクが発生する場合は、Qualys 脅威リサーチユニット（TRU）が厳選した**緩和策を実施します。**
- 長期間にわたりコンプライアンス違反または未修正の状態にある**資産を隔離**し、リモートパッチ適用と検証のために限定的な接続を維持します。
- **修復ワークフローを** ServiceNow などの **ITSM システムと統合**し、組織のベストプラクティスに沿った確立された変更管理および承認プロセスに従ってアクションが実行されるようにします。

修復作業をさらに効率化するため、TRE は **Qualys 修復ライブラリ**へのアクセスを提供します。これは、Qualys リサーチチームが作成した検証済みのスクリプトとワークフローを継続的に拡張していくライブラリです。
このライブラリには、パッチが存在する場合でも修正が複雑な脆弱性に対処するために設計された専用スクリプトが含まれています。これらの脆弱性は、安全に修復を完了するために追加の手順や構成変更が必要となる場合があります。組織はこれらのスクリプトをそのまま実行したり、自社の環境に合わせてカスタマイズしたり、独自の修復コンテンツをアップロードしたりすることができ、大規模なリスク修復と軽減において最大限の柔軟性を実現します。

優先順位付けされたビュー、豊富な対応オプション、自動化されたワークフロー、そして Qualys エージェントによる統合実行を組み合わせることで、修復コックピットは、パッチ適用、緩和、修正、隔離など、あらゆるリスク要因が効率的かつ安全に解決されることを保証します。すべての修復活動は継続的に追跡され、TruRisk スコアリングと VMDR ダッシュボードを通じてリアルタイムで反映されるため、企業全体のリスク軽減状況を完全に可視化し、測定可能な形で証明できます。

TruRisk Eliminate は、Qualys 脅威研究ユニットが作成した検証済みのスクリプトとワークフローのコレクションである Qualys 修復ライブラリへのアクセスを提供します。このライブラリは継続的に拡張されています。

主要な機能

包括的な OS およびアプリケーション対応

Windows、macOS、幅広い Linux ディストリビューションに加え、多数のサードパーティ製アプリケーションへのパッチ適用をサポートします。

ガバナンスを伴う自動化

自動化をサポートしつつ、変更内容、実施時期、実施方法について、必要に応じて人的監視を維持します。

リスクベースの自動化

チームはリスクに基づいて自動化ポリシーを作成し、脆弱性データとビジネスへの影響度に基づいてパッチの優先順位付けとスケジュール設定を行うことができます。

ゼロタッチパッチ適用

障害発生確率の低いアプリケーションに対し、パッチ適用を完全に自動化します。ブラウザや PDF リーダー（Adobe Reader など）といった重要なソフトウェアを、手動操作なしで常に最新の状態に保ちます。これにより、広範囲にわたるアプリケーションを一貫して保護し、運用コストを削減します。

既存ソリューションの置き換えまたは拡張

既存のパッチ適用システムを置き換える、あるいは並行して運用することで、パッチ適用範囲と修復の MTTR（平均復旧時間）を向上させることができます。

適応型緩和策

パッチ適用によってリスクが生じる場合、またはパッチが提供されていない場合に、Qualys 脅威研究ユニットが厳選した非侵襲的な緩和策を推奨します。

設定ベースの修正

パッチが提供されていない脆弱性に対して、安全な設定変更とポリシー更新を提供します。

厳選スクリプトライブラリ

Qualys 脅威研究ユニットが厳選した、複雑な脆弱性や影響の大きい脆弱性に対処するための、事前に構築された修復スクリプトを提供します。

継続的なリスクフィードバック

Qualys VMDR ダッシュボードと TruRisk スコアリングを通じて、すべての是正措置をリアルタイムで反映し、リスク低減状況を測定可能な形で可視化します。

ベストプラクティスに基づいた安全な導入を実現

段階的な「リング」方式、フェーズ間の組み込みテスト、ロールバック、テストと導入を統合したワークフローなど、ベストプラクティスに基づいた導入手法を用いることで、安全かつ信頼性の高い変更実装を実現し、運用への影響を最小限に抑え、各段階での成功を検証します。

カスタムスクリプトとソフトウェア配布

組織のニーズに合わせてカスタマイズされた修復スクリプトや社内ソフトウェアパッケージの作成と展開を可能にします。

セキュリティと IT の連携

セキュリティと IT の橋渡しを行い、共有ワークフローを通じてテスト、検証、そして管理された展開を可能にします。

最終手段としての隔離

長期間にわたりパッチが適用されていない、またはコンプライアンスに準拠していないデバイスを、制御された方法で隔離できます。これにより、完全なコンプライアンスが回復されるまで、リモートパッチ適用と修復機能を維持しながら、リスクへのエクスポージャーを最小限に抑えることができます。デバイスが隔離されると、VMDR レポートでは、その資産上のすべての脆弱性が軽減済みとしてマークされ、リスクへのエクスポージャーが軽減されたことが反映されます。

変更管理と ITSM の統合

ServiceNow などの ITSM システムと統合することで、完全なコンプライアンス、トレーサビリティ、監査追跡を実現します。

TRURISK ELIMINATE

「リスクを見つけるだけでは安全は確保されない。リスクを排除することこそが安全につながる！」

Sumedh Thakar
Chief Executive Officer,
President, Qualys

結論

今日の脅威環境においては、パッチ適用だけではもはや十分ではありません。パッチ適用は依然として対策の重要な要素ですが、運用リスク、パッチ未提供、アプリケーションの依存関係などにより、多くの脆弱性に即座に対処することはできません。

Qualys TruRisk Eliminate は、従来のパッチ適用を基盤としつつ、さらに高度なインテリジェントなリスクベースの機能を追加することで、その機能を拡張しています。具体的には、パッチ適用が安全でない場合には緩和策を推奨し、パッチが存在しない場合は構成ベースの修正を適用し、長期にわたりコンプライアンス違反となっているデバイスを隔離してリスクを封じ込めます。

TruRisk Eliminate は、高度なパッチ管理、自動修復、ITSM 統合、厳選されたカスタムスクリプト、継続的なリスクフィードバックを組み合わせることで、組織がリスクを単に管理するだけでなく、真に排除することを可能にします。セキュリティチームと IT チームは、より迅速に対応し、コンプライアンスを向上させ、リスクを継続的に低減することで、安全かつ効率的に、大規模にリスクを軽減できます。

顧客の声

「私たちは今、最も重要な脆弱性、つまり実際に悪用されている脆弱性に注力し、攻撃対象領域をより迅速に縮小しています。」

Security Engineer, Children's Mercy Kansas City

「Qualys はリスクを検出し、分析し、自動的に排除します。時間と労力を大幅に節約できます。」

Security Operations Manager, Cintas.

「ハリケーン・アイダのような運用上の混乱時においても、私たちは状況を把握し、対策を講じ、脅威の範囲を縮小し続けました。Qualys は不可欠な存在でした。」

Sr. Director of IT Security & Admin New Orleans Saints

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.

v251121