Qualys

ソリューションブリーフ

技術ソリューション概要: IT運用向け TruRisk Eliminate™

攻撃者が脆弱性の公開からわずか数時間でそれを悪用する手段を確立する中、確認された脆弱性や脅威を即日（同日中）に修正・対処する必要性が急速に高まっています。脆弱性の数は増え続け、対応可能な期間は短縮の一途をたどっていますが、従来の修正ワークフローはこのスピードに対応できる設計にはなっていません。Verizonの「2026年データ侵害調査報告書（DBIR）」では、脆弱性の悪用が、侵入の足掛かり（初期アクセス）となる攻撃手法としてすでに最多となっていることが指摘されています。また、実際に悪用が確認されている脆弱性の修正にかかる中央値は**43日**に達しました（前年の**32日**から増加）。たとえボトルネックが自部門になかったとしても、この修正にかかる時間の責任はIT部門が負うことになります。

ITチームには、運用のレジリエンス（回復力・継続性）を維持しつつ、自律的な機能によって継続的にリスクを低減できる、サイバーセキュリティのゼロデイ脆弱性修正専用のソリューションが必要です。

「TruRisk Eliminate」は、まさにこうしたニーズに応えるために開発されたものであり、既存の一般的なITパッチ適用ソリューションを補完する不可欠なツールとなります。

TruRisk EliminateがIT部門の運用負荷を軽減する5つの方法

1. 従来のパッチ適用が不可能な場合の修復

脆弱性の中には、適用すべきパッチが存在しないものがあります（ベンダーによる修正が提供されていない、システムがサポート終了（EOL）を迎えている、本番環境が繊細で変更を加えるのが困難、など）。こうした脆弱性は、そのまま放置されがちです。

TruRisk Eliminateは、Qualys TRUが開発・検証した「設定変更による修正」や「EOLソフトウェアの削除ワークフロー」を、既存のCloud Agent経由で展開します。修正スクリプトの作成や、新たなツール・プロセスの導入は一切不要です。

成果: **16日間**で**4万件**の.NET EOL（サポート終了）関連の脆弱性を解消。 **3日間**で**2万7,000件**のWinVerifyTrust関連の問題を解決（パッチ適用は不要）。

2. メンテナンスウィンドウを中断することなく、エクスポージャーを無効化する

セキュリティ部門から即日の修正を求められると、IT部門は緊急対応モードを余儀なくされます。計画外のCAB（変更諮問委員会）会議、深夜勤務、そして本番環境への高いリスクといった事態に直面するのです。

「TruRisk Eliminate」は、こうした状況で「時間」を確保します。安全かつ一時的な緩和策を適用して脆弱性への露出を即座に無効化できるため、恒久的なパッチ適用を次回の定期メンテナンス期間まで延期することが可能です。つまり、予定していたスケジュールを変更せずに済みます。

成果: 設定の最適化による対策でリスクへのエクスポージャーを即座に**85%削減**し、緊急の非定期的デプロイを完全に排除しました。

3. ロールバックのリスクなしにパッチ展開を拡張

パッチの適用に失敗すると、本来修正すべき脆弱性そのものよりも大きな混乱を招くことになります。ロールバックの実施、作業時間の延長、そして業務時間外の緊急対応といった負担がすべてIT部門にのしかかるからです。

TruRisk Eliminateは、AIを活用して各パッチの展開信頼性を自動的にスコアリングします。その結果に基づき、低リスクの更新は即座に展開する一方、リスクの高い更新については、既存のテスト、パイロット、本番といった各展開段階（リング）を通じて段階的に適用します。

成果: **14日間**で**25万台**のワークステーションにパッチを適用。展開サイクルの短縮と、ロールアウト時の問題の大幅な削減を実現しました。

4. チケットは適切な担当者へ直接ルーティング。推測は不要

IT部門とセキュリティ部門の間の摩擦の多くは、同じような経緯で生じます。資産に関する十分な情報がないまま修復依頼が届き、IT部門はまず、そもそも対応が必要かどうかを確認する作業に時間を費やさなければならないのです。

「TruRisk Eliminate」は、チケットが作成される前の段階で、CSAMから所有者情報を取得し、リスクインテリジェンスと資産情報を適用します。各タスクは、対応に必要な情報が事前に付与された状態で、適切なIT担当者へとルーティングされます。推測や担当者の再割り当て、部門間でのやり取りといった無駄なプロセスは発生しません。

成果: チーム間での手作業による調整を排除することで、MTTR（平均復旧時間）を**30%削減**し、応答時間を**40%短縮**しました。

5. 本番環境を停止させることなく、厳格なコンプライアンスSLAを遵守

CISA KEV（既知の悪用された脆弱性）への対応義務には遅延が許されず、期限を逃せば即座にコンプライアンス違反となります。

「TruRisk Eliminate」は、SLAの期限内にCISA KEVやゼロデイ脆弱性の修正を優先的に実行し、監査に備えてすべての操作を自動的に記録します。AI主導の優先順位付けにより、こうした脆弱性への対処スピードはさらに加速します。修正適用後にはレジリエンス（回復力）チェックを行い、本番環境に不具合が生じていないことを確認します。

成果: すべての修復経路においてCISA KEVをほぼ完全に網羅し、監査に対応可能な記録も自動生成されます。

ITおよびセキュリティチーム向けに設計

TruRisk Eliminateは、パッチ適用およびパッチを伴わない修復作業のための共通プラットフォームをIT・セキュリティ部門に提供します。これにより、緊急事態や不要なチケット対応（ノイズ）が減少し、デプロイの失敗も抑制されます。

大規模環境での実績: **1億5,000万件**のパッチをデプロイ。そのうち**4,000万件**を自動化し、ロールバック率は**0.1%未満**を達成。さらに、**100万件**に及ぶ緩和策の適用、修正、および隔離処理を実行しました。

v260702