クォリスによるリスク管理とリスク修復

Trurisk Eliminate(TRE) – Patch Management, Remediation, Isolation

クォリスジャパン株式会社
更新日：2026年9月

*TRU EliminateはVMDRライセンスとの併用が必須です。
また、Patch ManagementはTREに含まれていますが、単体機能としてVMDRと併用してご利用いただけます。

Post-Mythos時代における対応

従来の脆弱性管理の常識が通用しなくなった時代

- 脆弱性公開から**数時間で攻撃が始まる**
- **AI**により攻撃のスピードがさらに加速
- **脆弱性の数・規模が爆発的に増加**

従来の方法の限界

- 検知・優先順位付けはすでに高度化している

一方で以下の**課題**がある
- **パッチ配布が遅い**
- インフラがボトルネック
- 手作業・人依存

88%の脆弱性が攻撃より遅れて修正

63%の重要脆弱性が1週間後も未対応

Qualysのソリューション

全プロセスを“**機械スピード**”にできる

Qualysは以下を統合：
1.検知（VMDR）→ 数時間単位で脆弱性を把握
2.優先順位付け（TruRisk + TruConfirm）→ 本当に危険なものだけに絞る
3.修正（TruRisk Eliminate）→ 自動でパッチや緩和策を適用

クォリスがポスト・ミュソス時代に優位である理由

Hyper-Prioritization

超高度な優先順位付け

ETM + TruConfirm

Hyper-Prioritizationでは、6,250万件の検出結果を約6万件まで絞り込み、99.9%のノイズ削減を実現しています。

TruRiskによりリスクをビジネス影響（ドル）で定量化し、TruConfirmが本番環境での悪用可能性を検証（800万件以上・業務影響なし）することで、対応の優先度を正確に判断します。

さらにAgent Valによって脆弱性を「悪用可能／コントロールにより阻害／到達不可能」の3つに分類し、CISA KEV掲載の約45日前から先回りして対応を可能にします。

Zero-Day Remediation

高速な修正能力

TruRisk Eliminate

Zero-Day Remediationでは、過去12か月間で150M以上のパッチを配布してきた実績があり、大規模環境でも確実に運用できることが証明されています。

また、自律的なパッチ適用におけるロールバック率は0.1%未満と極めて低く、さらに初回適用の成功率も98.2%に達しているため、高い安定性と信頼性を兼ね備えています。

対応手法としては、単純なパッチ適用にとどまらず、修正（Fix）や緩和（Mitigation）、カスタムスクリプトの実行、さらにはシステムの隔離（isolation）まで幅広くカバーしており、状況に応じた柔軟な対処が可能です。さらに、平均的な修復完了までの時間は従来と比較して80%短縮されており、ゼロデイ脆弱性に対しても平均で1日未満という非常に迅速な対応を実現しています。

AI-Speed Detection

超高速検知

VMDR

シグネチャーリリースは、重大およびゼロデイ脆弱性に対して中央値12時間という非常に短い対応時間を実現しており、特に優先度の高いベンダーについてはわずか6時間での対応が可能です。

また、10年以上にわたりシックスシグマレベルの高い検出精度を維持しており、信頼性の面でも業界トップクラスの水準を誇ります。

さらに、CISAの既知の悪用脆弱性（KEV）に対しては99%という高いカバレッジを達成しており、130,000件以上のCVEにも対応しています。これに対して、一般的な競合スキャナーでは対応に数日から数週間を要することも多く、検知スピードの面で大きな差があります。

TruRisk Eliminate 脆弱性のリスクに素早く対応

主な機能

AIを活用したパッチ信頼性スコアリング
実際のパッチ適用に関する膨大なテレメトリデータを分析してパッチの信頼性を予測し、適用前にその結果を予測・把握することを可能にします。

段階的な自動修復
エージェント「Sara」が修復案を提示します。制御された段階的ロールアウト（展開）を行うため、容易な修正からリスクの高い変更へと順次進められます。

パッチレスの修正
ベンダーからのパッチがなくても、修正、緩和、アンインストール、隔離、あるいはカスタムアクションといった手段により、脆弱性のエクスポージャーを解消します。

組み込みのロールバック機能
期待通りの動作をしなかった修復処理を元に戻すための、安全策が組み込まれています。

TRE導入メリット	説明
セキュリティ運用の自動化	対応すべき脆弱性が自動的に抽出・修復され、手作業を削減
対応優先順位の明確化	リスクに直結する脆弱性から修復できるため、ROIが高い
監査・証跡対応	対応の実績・履歴が可視化され、金融監査や内部統制にも有効
SecOpsとITOpsの橋渡し	セキュリティチームと運用チーム間の作業分担を効率化

TruRiskの削減に対処する

パッシブおよびアクティブな対応を推進してリスクをより迅速に軽減します

DE-RISK YOUR BUSINESS

- Qualys TruRisk Eliminateサイト
- Qualys TruRisk Eliminate ブログ

Qualys.

Qualys Patch Management (PM)、**Mitigation (MTG)**、**Isolation (Isolate)** はいずれも脆弱性対応のための機能ですが、目的と対応方法が異なります。Qualys ではこれらをまとめて「**TruRisk Eliminate**」として提供しています。

TruRisk Eliminate

	TruRisk Patch	TruRisk Mitigate	TruRisk Isolate
目的	脆弱性を根本的に修正	パッチ適用までのリスク低減	攻撃を即座に遮断
実施内容	OSやアプリケーションのパッチ適用	サービス停止、ポート閉鎖、レジストリ変更、スクリプト実行など	端末をネットワークから隔離（Quarantine）
利用シナリオ	ベンダーパッチが提供されている場合	ゼロデイ、業務都合でパッチ適用できない場合	侵害疑い端末や緊急対応時
説明	Patch Managementは、Windows、Linux、Macに対してベンダー提供のパッチを自動展開し、脆弱性を恒久的に解消する機能です。VMDRで検出した脆弱性に対し、対応パッチを特定して配布できます。 例: • Microsoftの月例パッチ適用 • ChromeやAdobeなどサードパーティ製品のアップデート • Linuxパッケージ更新	Mitigationは、パッチがない、またはすぐ適用できない場合の代替策です。Qualys Agent経由で設定変更やスクリプトを実行し、脆弱性の悪用経路を塞ぎます。 例: • 脆弱なサービスを停止 • 危険なポートを閉じる • レジストリ変更 • 脆弱機能の無効化 特に以下の状況下で有効 • ゼロデイ脆弱性 • 運用停止できないサーバー • パッチ未提供製品	Isolation（TruRisk Isolate）は、リスクの高い端末をネットワークから隔離する機能です。脆弱性が存在する端末や侵害の疑いがある端末の通信を制限し、横展開や攻撃の拡大を防ぎます。 例: • ランサムウェア感染疑い端末 • 公開された重大ゼロデイの影響端末 • 緊急パッチ適用前の一時隔離

TruRisk Eliminate:パッチレスの修復

パッチレス修復

パッチが存在しない場合や、適用が安全でない場合でも、TruRiskEliminateは別の方法でリスクへのエクスポージャーを解消します。

Patch

- 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**
- **各パッチの信頼性スコア**

Uninstall

修正プログラムやパッチが提供されていない場合、脆弱性のあるソフトウェアや未承認のソフトウェアを完全に削除します

Mitigate

パッチ適用が遅れる場合やリスクを伴う場合に、制御された変更を通じて脅威へのエクスポージャーを低減します

Custom

複雑な環境には標準スクリプトを提供し、自社アプリにはカスタムスクリプトで対応

Isolate

最終手段として、可視性やリモート管理機能を維持しつつ、脆弱性のある資産を隔離して脅威の拡散を防ぐ

実証済みの成果:

- **150M+** パッチ適用件数
- **40M+** 自動修復（ロールバック率0.1%未満）
- **85%** 脆弱性へのエクスポージャーを削減
- **25x** P2P配信によるパッチ配信の高速化

Eliminate機能概要

機能	内容
パッチ適用	Windows/Linux/macOSおよびサードパーティアプリのパッチを適用
パッチレス脆弱性修復	パッチが存在しない場合でもスクリプト等で脆弱性を修復
修復（Fix）	TRU提供スクリプトなどで具体的な問題を解決
緩和（Mitigation）	パッチ未適用でもリスクを低減する対策を適用
カスタムスクリプト	独自の修復・緩和スクリプトを作成可能
ソフトウェア削除	EOL/EOSや不要なアプリケーションのアンインストール
デバイス分離（Isolation）	脆弱な端末をネットワークから隔離し攻撃を防止
ソフトウェア配布	セキュリティソフトやパッケージの展開
リモート分析	パッチ適用失敗などをリモートで調査
TruRisk連携	脆弱性をビジネスリスクとして評価・優先順位付け
オペレーショナルリスクスコア	パッチ適用による業務影響リスクを評価
リミディエーションコックピット	IT/セキュリティ間のタスク共有と実行管理
タスク割当	修復タスクをチーム単位で割当・管理
SCCM/Intune連携	SCCMやIntune経由で修復やパッチ展開
TRU提供コンテンツ	修復スクリプトや緩和策を提供
マルチアクション対応	Patch/Fix/Mitigate/Uninstall/Isolateを統合して実行可能

TruRisk Eliminate(TRE)は 、従来のパッチ適用を超えて、統一された Qualysプラットフォームを通じて脆弱性を修正、軽減、アンインストール、および分離する機能を提供します。

PM

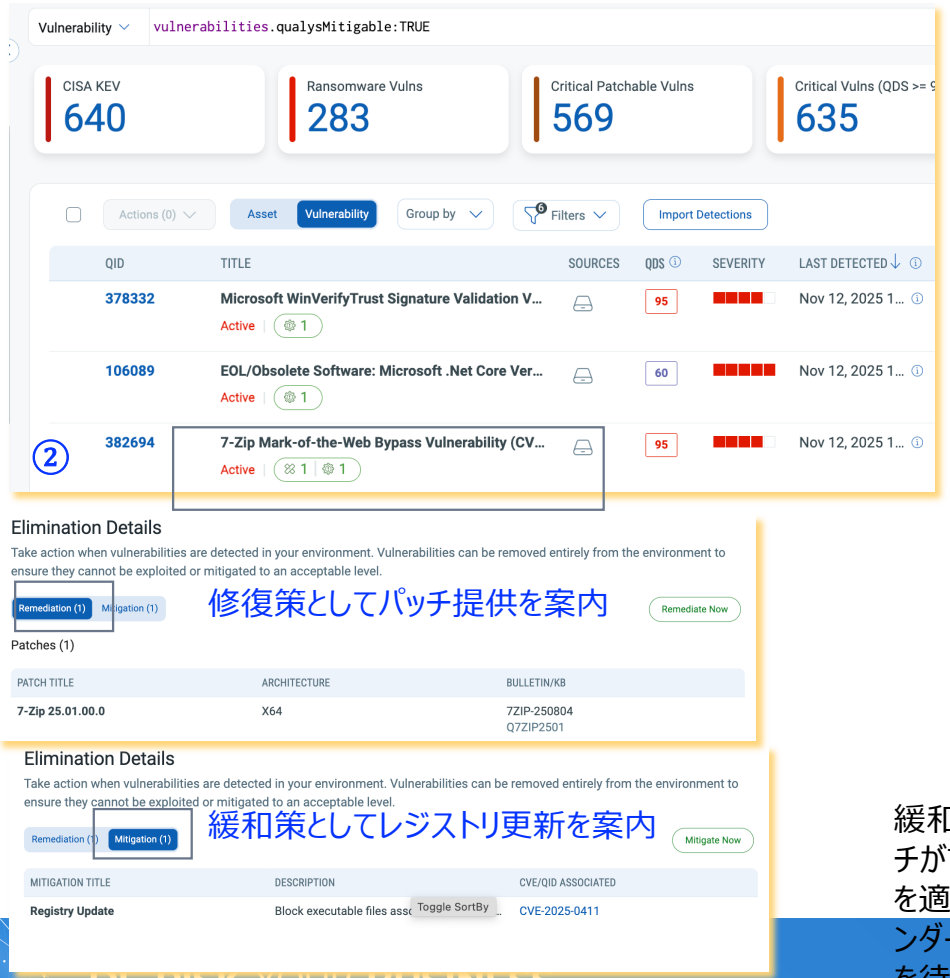
- OSパッチ
- 3rd パーティパッチ
- ゼロタッチオートメーション
- リスクベースオートメーション

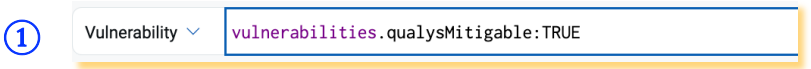
TRE

- SCCM/Intuneとの統合
- カスタムMitigation（緩和策）/Remediation（修復）
- Mitigate（緩和策）
- Remote Shell
- Cloud Remediation（クラウド上のリスク修正）
- ServiceNowやServiceNow VRとの統合
- 古いバージョンのソフトウェアの発見と削除(java)
- パッチがない場合の修復
- 面倒な脆弱性を解決するライブラリ
- パッチ適用とコンフィグの変更
- Isolate（隔離）
- ソフトウェアのインストールとアンインストール

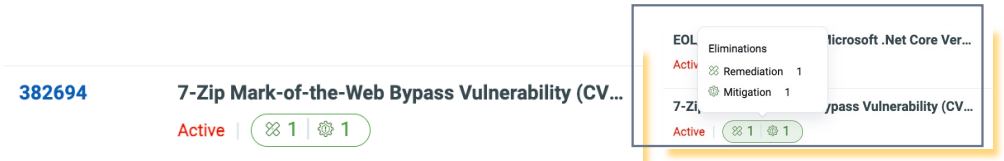
UIの紹介

緩和策とは、悪用されるリスクを軽減または排除するために講じられる措置を指します。





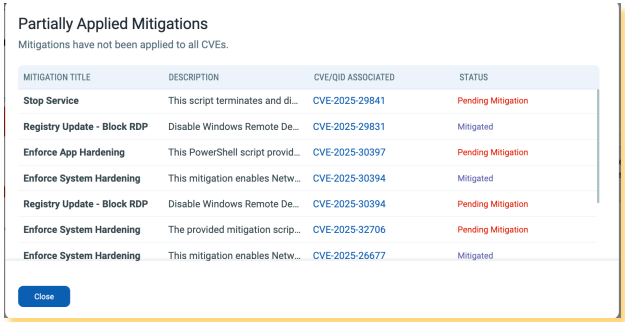
軽減できる脆弱性を検索するには、軽減に関連する**QQL**クエリを使用できます。



マウスをホバーすると、RemediationとMitigationの候補数が表示されます。

④

緩和策はCVE単位で案内されます。お客様の環境や状況に最も合う対策を選定できます。



緩和策の情報は、「軽減オプション」に基づく優先順位付けに活用できます。例えば、パッチがすぐに利用できない場合は、ファイアウォールルールやサービスの無効化などの回避策を適用してリスクを軽減できます。重大なCVEにまだパッチがリリースされていないものの、ベンダーがServer Message Block v1の無効化を推奨している場合は、恒久的な修正を待つ間、迅速にリスクを軽減できます。

次世代の標準となる自律型運用（Autonomous RemOps）

Phase 01

事後対応型のパッチ適用

2022–2024

現在、多くの組織がこの段階にある

- 目立つ問題から順番に対応
- チケットの振り分けは手作業
- CVSSスコアだけで優先順位を決定
- 修復までに60〜90日かかる

Phase 02

修復プロセスを一元管理して実行

2024–2026

これからの運用のスタンダード

- リスクを考慮した優先順位付け
- 対応状況を自動追跡・管理
- パッチ、緩和策、隔離を柔軟に使い分け
- 修復まで20〜30日かかる

Phase 03

自律型修復運用

2026–2030

Qualysが導く運用の未来

- AIによる自律的な修復実行
- 自己修復型のクローズドループ運用
- 重要な脆弱性を7日以内に修復

Competitors are here

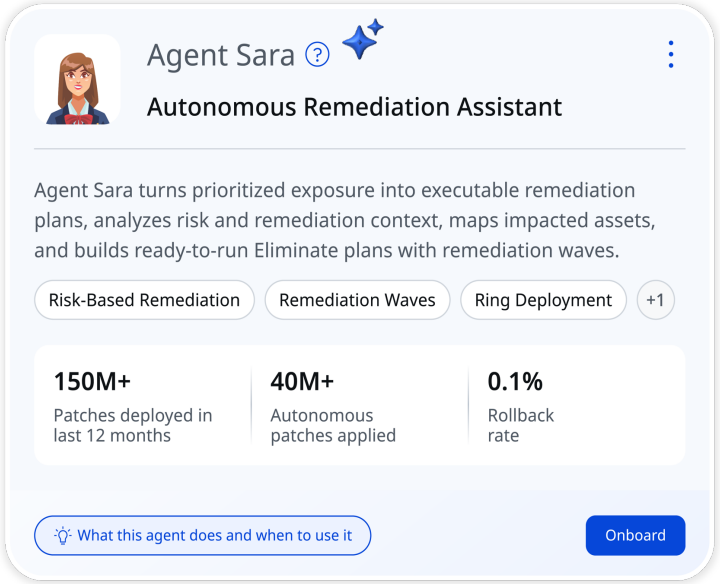
Qualys is here

DE-RISK YOUR BUSINESS

Qualys.

ETM Agentic AI

エージェント・サラによる自律的修復



Demoサイト

Your Vulnerability Backlog

エージェント・サラはあらゆる脆弱性を分析します

- パッチの入手可能性と信頼性
- 資産の種類(Server vs. Workstation)
- 再起動と依存リスク
- 現在の脅威状況(CISA KEV, Ransomware)

最適な展開ウェーブへ自動割り当て

- **Wave 1** 業務への影響が少ない
- **Wave 2** 業務への影響が大きい
- **Wave 3** 緩和策
- **Wave 4** アンインストール

パッチ配信アップデート

Qualys

より高速で、インフラに依存しない新しい配信モデルの必要性

大規模環境では、従来の中央集約型のパッチ配信が非効率かつスケールしない理由

① 帯域とネットワークの負荷

全端末が同じパッチを個別にダウンロード → **ネットワーク帯域を圧迫・混雑**

② 重複ダウンロードによる非効率

同一パッチを何度も取得 → **無駄な通信が大量発生**

③ インフラ依存・スケーラビリティの限界 → **大規模・分散環境に追従できない**

ゲートウェイやアプライアンスが必要
拠点が増えると運用負荷増大

従来の配信方式は限界に達しており、より高速で、インフラに依存しない新しい配信モデルが必要

QualysではGateway Serviceを提供しているが、課題もある

QGSの強み

キャッシュによる外部帯域の削減
•エージェント通信の簡素化
•拠点ごとのローカルキャッシュ

QGSの限界（問題点）

- 拠点ごとにアプライアンスが必要
- 多拠点では運用負荷が大きい
- インフラがない拠点では導入困難
- プロキシ設定などの構成が複雑

QGSだけでは大規模・分散環境の課題を解決しきれない
→ よりシンプルでスケーラブルな方法が必要

Peer to Peer パッチ配布でより高速展開
(P2Pパッチ配布機能)

Windows Cloud Agent
New Release

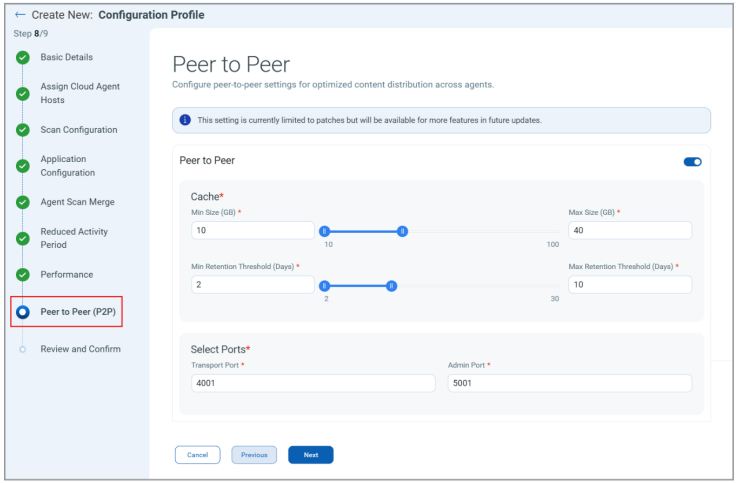
Qualys の P2P パッチ配布は、エンドポイント同士が協調してパッチを共有することで、ネットワーク負荷と配布遅延を大幅に削減します。
中央CDNへの依存を最小化し、LAN内で高速・効率的にパッチを展開することで、大規模環境でもスケーラブルかつレジリエントなパッチ管理を実現します。

UI 上での可視性
Windows Cloud Agent 6.5 リリース後：
Cloud Agent UI に P2P 設定タブが表示

本機能でできること：

- 同一 LAN 内の Cloud Agent 同士で **パッチファイルを共有**
- CDN へのアクセスを最小化
- 帯域使用量とダウンロード時間を削減

従来：約5TBの通信
P2P：約20～50GB



主な特徴	内容
LAN 限定	Peer 検出と共有は **同一 Local Area Network 内のみ**
チャンク化	パッチファイルは **複数チャンクに分割**
並列ダウンロード	複数の Peer から同時取得し高速化
CID（Content Identifier）	暗号学的 ID により **改ざん防止・整合性保証**
冗長取得	1台が失敗しても他 Peer から再取得可能

この機能の詳細については、*Peer-to-Peer Patch Distribution*をご参照ください。

Patch Tuesday: P2Pの帯域幅がいい理由

シナリオ:パッチチューズデーに合計約5GBのアップデートを1,000台のエンドポイントへ展開する

実際のデータ: 2026年5月のWindowsアップデートKB5089549ダウンロードサイズは~5GBです。

Traditional (CDN) Model

全ての端末がインターネット（DCN）から個別のダウンロード

~5 TB

消費される外部帯域幅の総量

5 GB × 1,000 台 = 1,000 GB

- WANやインターネットの帯域幅が急増
- オフィス拠点間の混雑
- 遠隔地での修復は遅い

Peer-to-Peer (P2P) Model

最初の数台だけがCDNからダウンロード

~20–50 GB

消費される外部帯域幅の総量

CDNからの初回ダウンロードはわずか5～10台。
残りの端末はLAN上でピアツーピアを伝播。

- 99%以上の外部帯域幅削減
- 高速ローカルLAN転送
- ピア間の並列分布

節約:~4950 GBの外部帯域幅削減 = パッチチューズデーサイクルあたり99%+削減

P2Pの設定オプション

Qualys Cloud Agent Configuration Profileを通じたシンプルで集中的な設定

設定オプション

Peer to Peer Toggle
設定プロファイルごとにP2Pの有効化または無効化

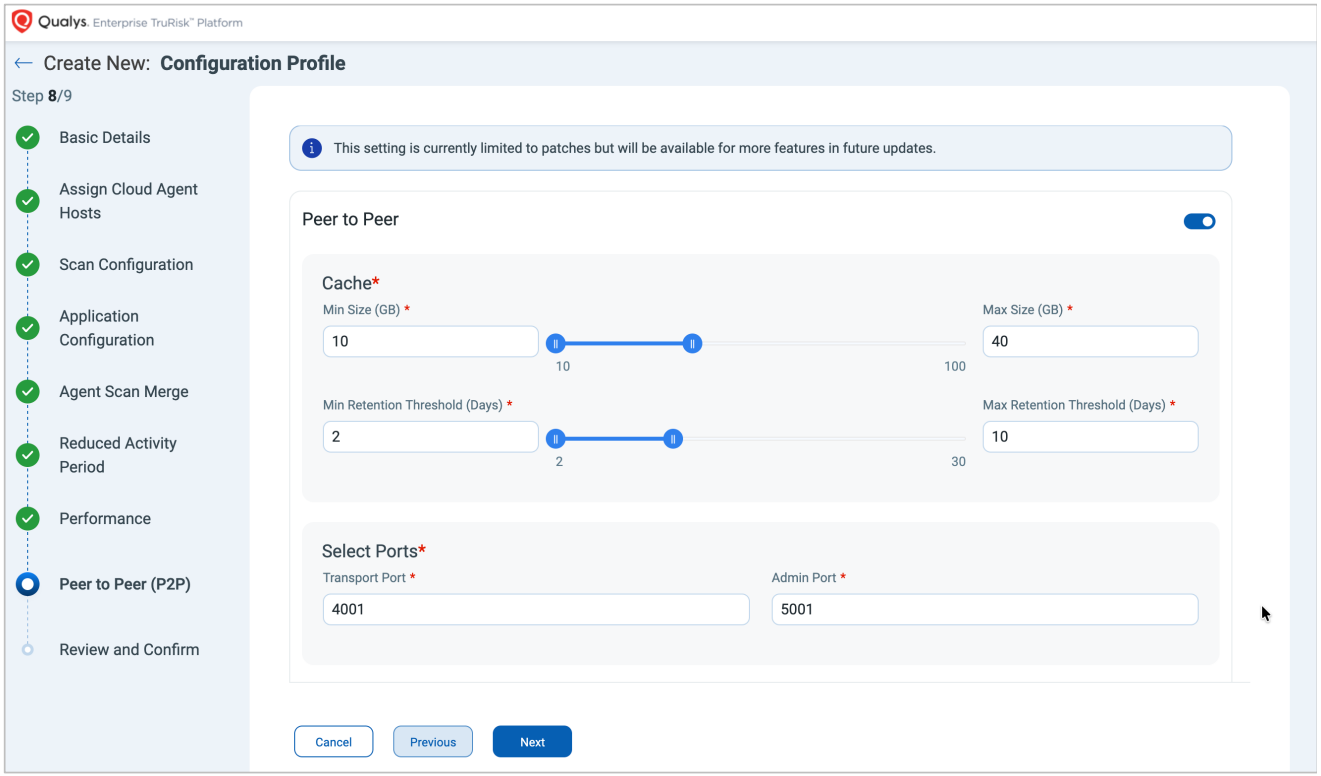
Cache Size (GB)
キャッシュパッチのディスク割り当てを制御(最小:10 GB、最大:最大100 GB)

Retention Threshold (Days)
パッチのキャッシュと共有期間を設定する(最短:2日、最大:最大30日)

Transport Port
ピアコンテンツ共有に使われるポート
(デフォルト:4001)

Admin Port
ローカルノード調整に使用されるポート(デフォルト:5001)

この設定は現在パッチ限定ですが、今後は対応可能です
今後のアップデートで、より多くの機能が利用可能になる予定です。



P2PとQualysゲートウェイサービス(QGS): それぞれの得意分野

要件/環境ニーズ	QGS	P2P	備考
Caches Resources	✅	Patches today	外部通信をQGSで制御し、内部配信はP2Pで分散可能
クラウドエージェント通信集中型	✅	❌	QGSはエージェント通信の中継
レガシーOS向けのTLSのアップグレード	✅	❌	QGSは各クライアントへQGSと通信するための証明書の配布が必要
すべてのQualysセンサータイプに対応	Yes	Windows Agent	P2Pは今後Linux,MacOSにも対応予定
展開、設定、保守の容易さ	⚠️	✅	QGSは各拠点に設置が必要
ピアツーピア通信が必要	❌	✅	
最良の複合展開	✅	✅	QGSとP2Pを組み合わせて使うのが最も効果的な構成

Rule of thumb:

QGSを集中管理とキャッシュに活用 | P2Pを活用して、高速で大規模なパッチ実行 | 最良の結果を得るには両方使う

Windows Cloud Agent
New Release

Bonus Feature

CLOUD AGENT FOR WINDOWS 6.7

近日公開予定:60秒パッチジョブ配信

Today	Cloud Agent 6.7
15分 – 3時間	< 60秒
パッチジョブを受けるまでの時間	パッチ作業開始時間

P2Pで配布自体は高速化できますが、従来はパッチ実行の指示が届くまで最大数時間かかっていました。Cloud Agent 6.7ではそれが60秒以内になり、検知から修正までをほぼリアルタイムで実行できるようになります。

フロンティアAI時代において、エクスプロイトのタイムラインは数分単位で計られており、パッチの配達も一致しなければなりません。Cloud Agent 6.7がそれを可能にします。

Coming Soon:パッチダウンロードソースの可視性

パッチジョブ詳細表の新しい列には、各パッチがどのように取得されたかが正確に表示されます

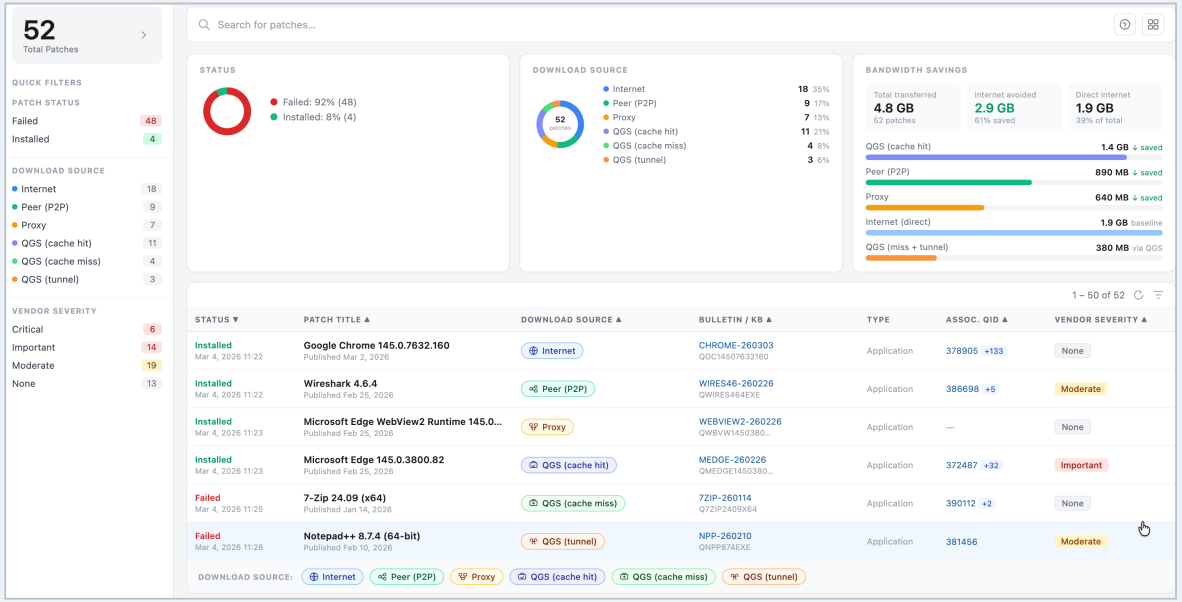
Source Visibility
すべてのパッチバイナリがどこから始まったかを正確に追跡することで、トラブルシューティングと監査準備度を向上させましょう。

Distribution Validation
展開中にキャッシュ層やP2P配信が効率的に機能しているか確認します。

Bandwidth Insight
すべての配信方法で帯域幅の使用量を測定し、パッチ配布のパフォーマンスを最適化します。

パッチの取得元を可視化

Internet	Proxy	QGS (cache miss)
Peer (P2P)	QGS (cache hit)	QGS (tunnel)

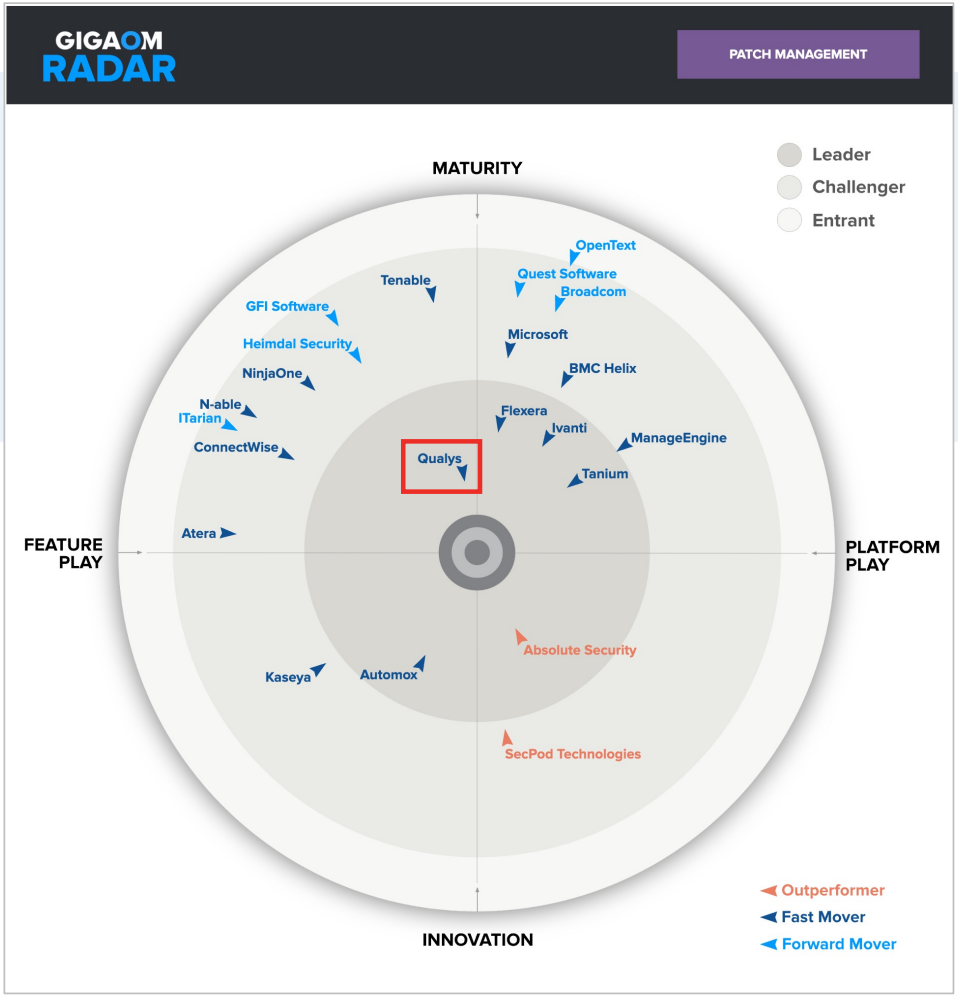


P2Pで高速化するだけでなく、実際にどこからパッチが配布されたかを可視化できるので、運用の透明性やトラブルシューティングも強化されます

September 2, 2025

GigaOm Radar for Patch Management Solutions v4

TruRisk Eliminate The Leader!



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。