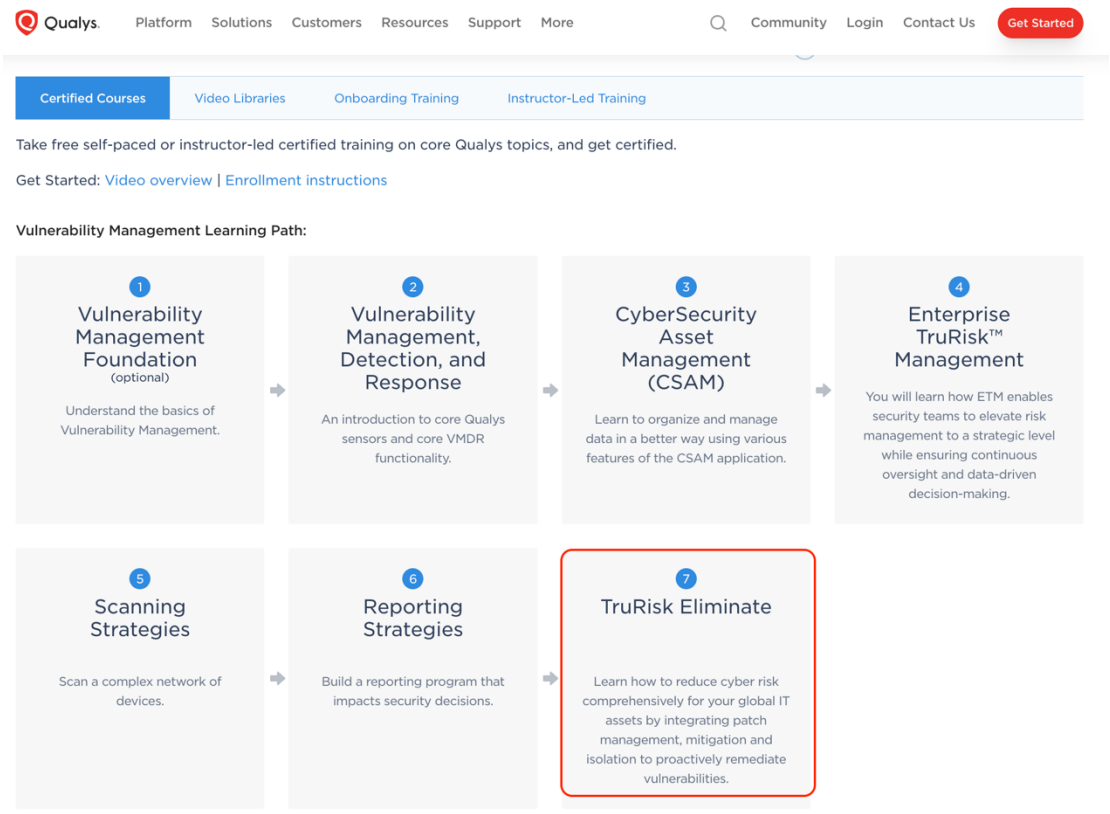
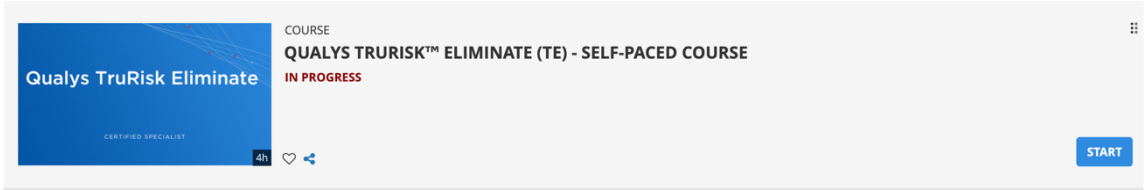
2025 年 12 月

Qualys TruRisk Eliminate トレーニングガイド

はじめに

本資料は Qualys　トレーニングサイトの TruRisk Eliminate の学習をより深く理解するための日本語ドキュメントとなります。下記サイトよりフリートレーニングにサインアップいただき、TruRisk Eliminate のトレーニングをスタートしてください。
https://www.qualys.com/training/





TruRisk Eliminate Overview

本ビデオでは、**Qualys True Risk Eliminate**（以下、TRE）が True Risk プラットフォームの機能を拡張し、**脆弱性管理のライフサイクル**の中でどの段階を担当し、どのようにリスク低減を実現するかを説明しています。
ポイントは、パッチ適用（Patch）だけでなく、緩和（Mitigate）と 隔離（Isolate）という選択肢を追加し、運用制約下でもリスクを下げられるようにしたことです。

脆弱性管理ライフサイクルの順序

資産の発見（Discover）
ネットワーク上の資産（端末・サーバ・アプリケーション等）を把握し、**可視化・棚卸**を行います。
→ 資産が見えていないと、セキュリティ状態の把握や対策が困難になります。
構成の把握（Inventory / Configuration）
各資産の **OS、適用済みパッチ、導入アプリケーション**などの構成情報を収集します。
→ この情報が後段の**脅威インテリジェンスとの突合**や、優先度付けの基礎になります。
優先度付け（Prioritize）
複数のパートナから得られる**脅威インテリジェンス**を参照し、資産の状態と突き合わせて、**どの脆弱性から対処すべきか**を決めます。
→ ここで、**True Risk エンジン**がリスク指標に基づく優先度付けに寄与します。
対処（Eliminate / Remediate） — ★TRE の主戦場
第 4 ライフサイクルの**修正の実装（パッチ等の適用）を自動化・統制します。**
→ **この「対処」フェーズを、TRE が Patch / Mitigate / Isolate** の 3 手段で拡張します。

True Risk Eliminate（TRE）の新機能と役割

Qualys は既存のパッチ適用機能に加え、**2 つの新機能**を追加しました。
Patch（パッチ適用） → ベンダー提供の**修正パッチ**を適用する、最も標準的な手段です。
ただし、依存関係、互換性テスト、停止計画（ダウンタイム）などの事情で、**即時適用が難しいケース**があります。
Mitigate（緩和） → **パッチが未提供／即時適用不可**の状況でも、**レジストリ変更**や**サービス停止**など、**ベンダーが推奨する設定変更**で**リスクを低減**します。パッチまでの「橋渡し」として、**攻撃面を狭める**実務的な選択肢。

Isolate（隔離）→ パッチも緩和も不可能な場合でも、資産を**ネットワーク的に隔離**し、**Cloud Agent 経由で管理**できるようにします。必要な作業（オフライン修復など）を実施後、**安全が確認できたら本番ネットワークに復帰**させます。事業継続とセキュリティを両立するための「最終防波堤」。
この 3 つの手段により、環境や制約に応じた**最適なリスク低減ルート**を選べます。

Risk-Based Vulnerability Management（RBVM）の考え方

RBVM は、**技術的深刻度（CVSS など）だけに依存しない**戦略で、以下を考慮して**実リスクに基づく優先度付け**を行います。

- **悪用可能性（Exploitability）**
- **資産の重要度（Asset Criticality）**
- **ビジネス影響（Business Impact）**

Qualys では、**VMDR（Vulnerability Management, Detection and Response）と True Risk エンジン**を統合することで、
識別 → 評価 → 優先度付け → 修復までを**自動ワークフロー**で支援します。
TRE はこの「修復」の部分を**現実的運用に合わせて拡張**する役割を担います。

運用イメージ

東京拠点やグローバル環境での運用を想定すると、次のような進め方が実務的です。

資産の網羅性確認 → スキャン範囲と Cloud Agent 配布状況をチェックし、棚卸の抜け漏れを塞ぐ。
重要資産のタグ付け → 事業クリティカルなサーバ／端末にタグを付与し、リスク評価時に重み付け。
優先度付けのルール整備 → Exploit 公開状況、インターネット露出、アイドル時間帯などを考慮した**修復 SLA** を定義。
対処方針の分岐（Patch / Mitigate / Isolate） → 互換性テスト済みなら **Patch** を自動適用。 テスト待ち・停止不可なら **Mitigate** で一時防御。緊急性が高く、他手段不可なら **Isolate** で封じ込め。
検証と復帰手順 → 隔離後の**動作検証**、影響評価、変更管理をクリアしてから本番復帰。
変更は**監査証跡**を残し、レポートで可視化。

Qualys Patch Management Overview

このビデをでは以下の内容について説明しています。

1．パッチ管理の課題

- どのパッチをどの脆弱性に適用すべきか判断が難しい。
- 同じアプリケーションを複数の OS でパッチ適用するのが複雑。
- 優先順位付けができても、リモートやモバイル、ハイブリッド環境ではタイムリーな展開が困難。
- ダウンタイムのスケジュール調整や IT 資産情報の最新化も課題。

2. Qualys Patch Management の特徴

- **包括的で自動化されたソリューション**で、パッチ管理を簡素化しセキュリティを強化。
- 脆弱性の検出、パッチのテスト・展開、コンプライアンス確保を効率的に実施。
- 運用負荷を軽減し、リアルタイムでパッチ状況や脆弱性の可視化が可能。

3. 主なメリット

- **セキュリティリスク低減**：脆弱性や脅威への露出を最小化。
- **運用効率向上**：ワークフローの合理化。
- **コンプライアンス強化**：規制要件を容易に満たす。
- **コスト削減**：手動パッチ作業の削減で TCO を低下。
- **時間節約**：自動化により IT チームが戦略的業務に集中可能。
- **安心感**：法的・商業的コンプライアンスを確保。

4. 脆弱性管理との連携

- Qualys Vulnerability Management と組み合わせると、脆弱性と必要なパッチを自動で関連付け。
- 高リスク脆弱性を優先的に修正可能。

5. 対応範囲と機能

- OS やアプリケーション、サードパーティ製ソフトのパッチに対応。
- インターネット接続があれば VPN 不要でどこでもパッチ適用可能（空港・カフェ・リモートオフィスなど）。
- 古いパッチ（superseded）を識別し効率化。
- 脆弱性の深刻度や既知の脅威に基づいてパッチジョブを構築可能。

資産の有効化と管理

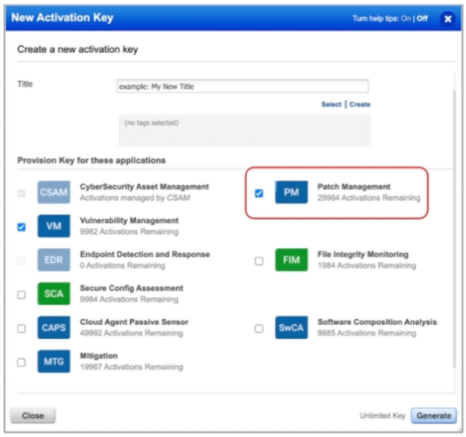
このセクションでは、複数のホストまたは特定のホストに対してパッチ管理モジュールを有効化し、パッチ展開ライセンスを活用する方法を学習します。また、ライセンス資産と評価プロファイル設定におけるタグの重要性についても理解を深めます。

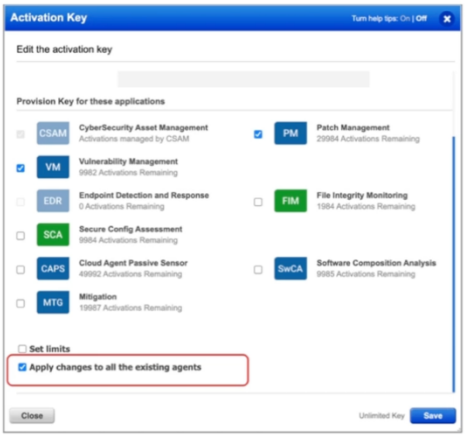
1. 全体概要

最初に「アクティベーションワークフロー」の概要を説明します。これは **クラウドエージェントの設定**と**パッチ管理モジュールの設定**という 2 つの大きなステップで構成されています。クラウドエージェントがインストールされていない場合は、まずそれを設定する必要があります。

2. クラウドエージェントのインストールと設定

クラウドエージェントはパッチ管理の前提条件です。ターゲット資産にクラウドエージェントをインストールし、パッチ管理に対応できるように設定します。Activation Key は、クラウドエージェントをインストールする際に使用する「構成プロファイル」です。このキーを資産（ホスト）に適用することで、その資産がどのモジュールやサービスにアクセスできるかを決定します。





3. パッチ管理モジュールの設定

- **アセスメントプロファイルの有効化**
  クラウドエージェントがホストの状態を確認し、ソフトウェアやパッチの有無を把握するための設定です。
- **パッチライセンスの割り当て**
  アセスメントプロファイルを設定しても、ライセンスがなければパッチ適用はできません。両方を設定する必要があります。

4. パッチジョブの作成

- OS や業務領域ごとにパッチジョブを作成します。タグを活用して資産をグループ化し、効率的にパッチを適用します。

5. アクティベーションキーの役割

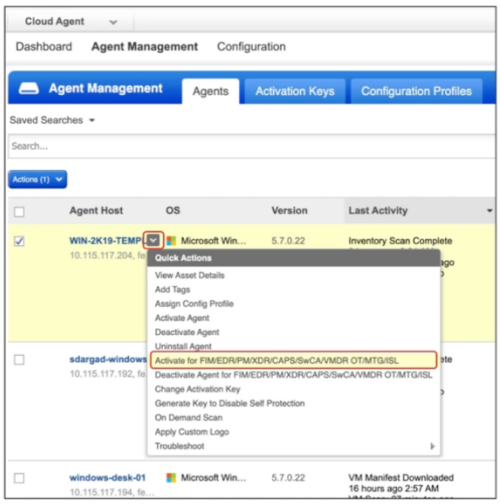
- アクティベーションキーは複数資産に適用でき、どのモジュールを有効化するかを決定します。
- **一括変更も可能**で、既存資産に新しいモジュールを追加できます。

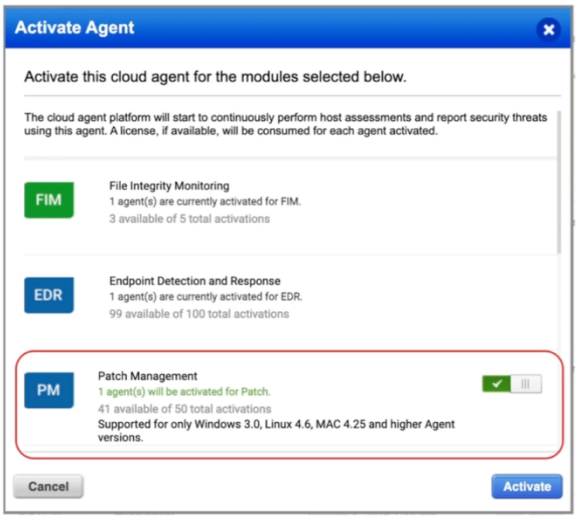
「Apply Changes to all the existing agents」チェックボックスは、クラウドエージェントの Activation Key を編集する際に表示されるオプションで、非常に重要な機能です。
このチェックボックスをオンにすると、現在その Activation Key を使用しているすべての既存エージェントに対して、変更内容が一括適用されます。

例えば、Activation Key に新しいモジュール（例：Patch Management）を追加した場合、このオプションを有効にすると、すでにそのキーで構成されている全資産に新しいモジュールが追加されます。

6. 個別ホストへのモジュール追加（例外ケース）

- アクティベーションキーに含まれていなくても、特定ホストに手動でパッチ管理を有効化できます。
- 「**Quick Actions**」からモジュールを選択し、スライダーをオンにして有効化します。





QQL でパッチ管理モジュールが適用されていないアセットを見つける

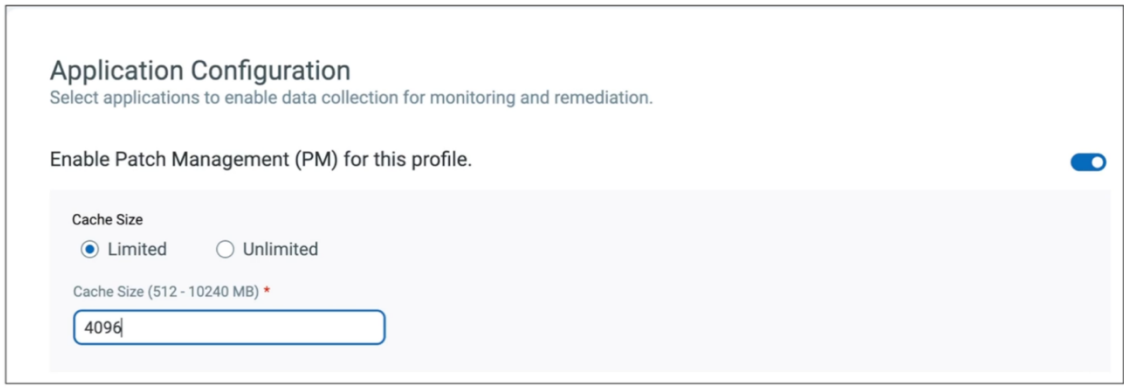
not activatedForModules: “PM”

7. キャッシュサイズ設定

- パッチのサイズに応じてキャッシュサイズを調整可能。**Windows パッチは最大 4GB** になるため注意が必要です。

Agent Configuration Profile

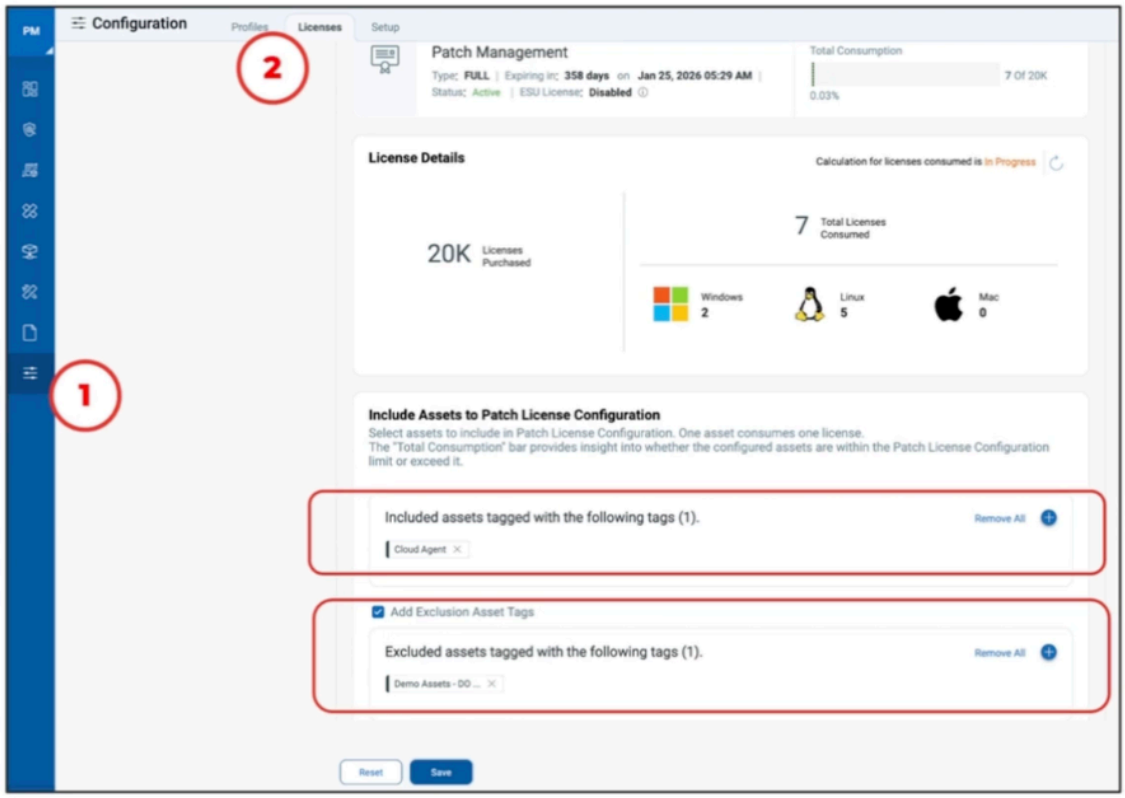
- Assign target hosts to CA Configuration Profile that has PM enabled.
- Default Cache Size is 2048 MB.
- The Recommended Cache Size is 4096 MB for Windows Assets.



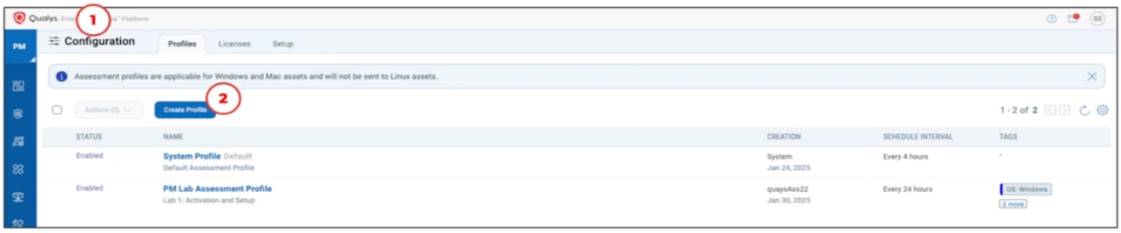
8. ライセンス設定

- パッチ管理ライセンスは必須。タグを使って対象資産を指定し、不要な資産（例：デモ環境）は除外します。
- パッチ管理モジュールを有効化していても、ライセンスがなければパッチ適用はできません。
  → アセスメントプロファイル設定 ＋ ライセンス適用が必須条件です。
- **ライセンスの設定場所**
  「Patch Management」→「Configuration」→「Licenses」タブで管理します。ここで資産にライセンスを割り当てます。
- フィルタリングで確認
  Patch Management の資産ページで QL 検索を使用します：

  `licensed:true` → ライセンスありの資産
  `licensed:false` → ライセンスなしの資産



9. アセスメントプロファイル



Patch Assessment Profile は、クラウドエージェントが資産をスキャンし、**どのパッチが不足しているか、どのソフトウェアが脆弱かを評価するためのルールセット**です。
→ パッチ適用の前提として、まず資産の状態を正確に把握するために必要です。

スキャン対象の定義 - どの OS やアプリケーションを評価するかを指定。
スキャン頻度の設定 - デフォルトでは 4 時間ごとにスキャンが実行されますが、カスタムスケジュールも可能。
タグによる適用範囲の制御 - 特定の資産グループにのみプロファイルを適用できます。

10. サブスクリプションレベル設定

- **PowerShell 実行ポリシーのバイパス**（Windows ジョブ用）

Bypass Execution Policy の意味

「Bypass」を有効にすると、**既定のポリシーを無視してスクリプトを実行可能**になります。

- **署名の有無に関係なく実行できる**
- **警告や確認メッセージなしで実行される**

パッチ管理では、OS パッチ適用時に PowerShell スクリプトを使うため、ポリシーが厳しいとジョブが失敗する可能性があります。そのため、バイパスを有効化することで、スムーズにスクリプトを実行できます。

- **クラウドエージェントスキャンの延期**（パッチジョブ優先）

Defer Cloud Agent Scans は、パッチ管理における**クラウドエージェントのスキャン動作を一時的に延期する機能**です。特に、Windows パッチのデプロイやロールバックジョブを実行する際に、スキャンとジョブが競合しないようにするために使われます。

通常、クラウドエージェントは脆弱性スキャンや資産情報収集を定期的に実行します。**Defer Cloud Agent Scans を有効化すると、パッチジョブの実行中はクラウドエージェントのスキャンを一時停止**し、ジョブが完了した後にスキャンを再開します。

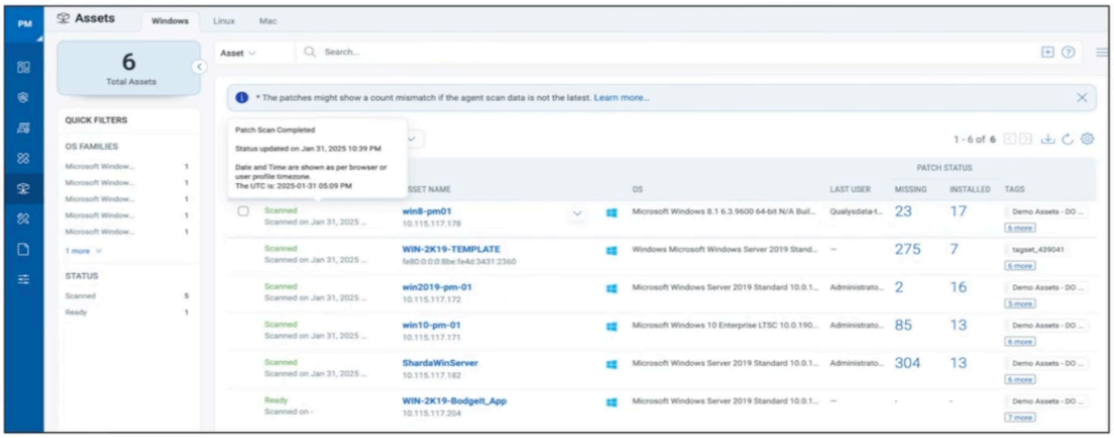
- **内部リポジトリからのパッチダウンロード**（外部取得不可時）

「Download Patches from Internal Repository」とは、パッチ管理において外部ベンダーから直接パッチを取得できない場合に、社内のリポジトリ（内部サーバ）からパッチをダウンロードするための設定です。

- 通常、パッチは OS やソフトウェアのベンダーサイトから直接ダウンロードします。
- しかし、ネットワーク制約（インターネット接続不可、セキュリティポリシー）やベンダーサイトへのアクセス障害がある場合、内部リポジトリを利用します。
- このオプションを有効化すると、クラウドエージェントは**指定された内部リポジトリからパッチを取得**します。

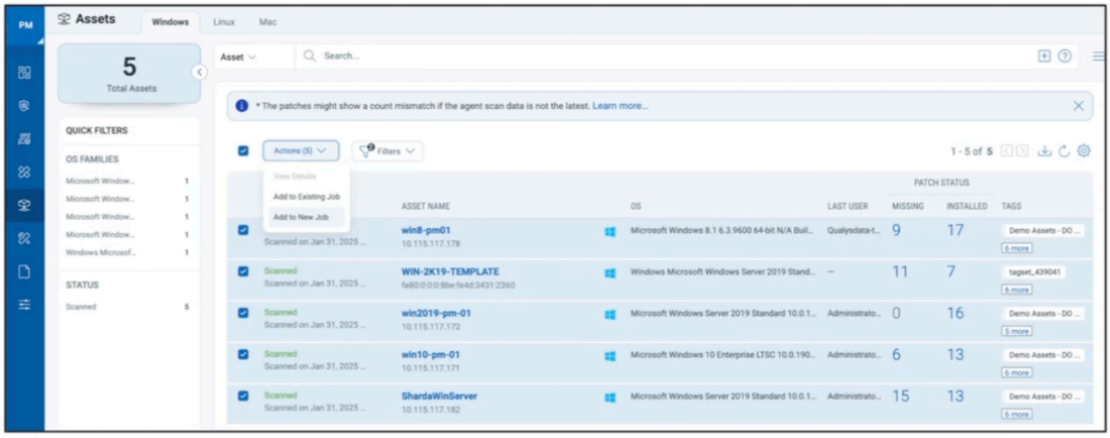
11. 資産の確認とフィルタリング

- パッチ管理が有効な資産を一覧表示。
- `licensed:true` や `licensed:false` でライセンス有無をフィルタ可能。



12. パッチジョブへの資産追加

- ライセンス付き資産を選択し、新規または既存のパッチジョブに追加できます。



Qualys Patch Source

このセクションでは、パッチ展開ジョブで使用される様々なパッチソース（ベンダーのコンテンツ配信ネットワークや社内リポジトリからダウンロード可能なパッチなど）について説明します。Windows、Linux、Mac オペレーティングシステムに関連するパッチについて解説します。

パッチ配布の準備完了後、利用可能なパッチソースを確認する

- 複数の配布元があり、それぞれの特徴を理解して活用することが重要です。

標準的な配布元：ベンダーのグローバル CDN

- OS やアプリケーションのパッチは、通常ベンダーが提供する公式ネットワークから取得します。

セキュリティ検証

- Qualys はダウンロードしたパッチを**デジタル署名とハッシュ値**で検証し、さらに **Malware Insights** で安全性を確認します。

認証が必要な場合の対応

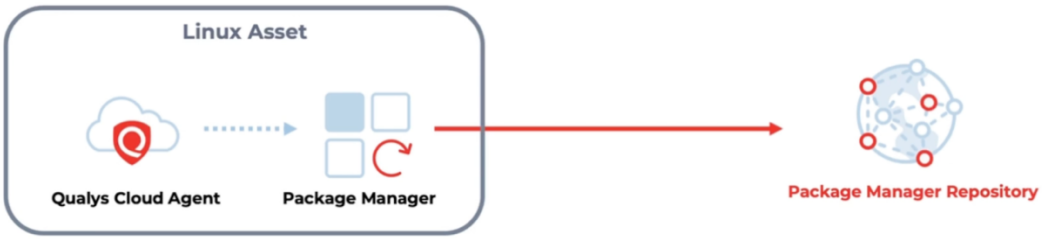
- 認証付きパッチは、管理者が手動でダウンロードし、**内部リポジトリ**に配置します。
- エージェントが内部リポジトリを参照できるよう、設定を有効化する必要があります。

Qualys Gateway Service (QGS)

- 外部パッチの**キャッシュ機能**と、認証付きパッチの**内部リポジトリ機能**を提供しています。
- ネットワーク負荷を軽減し、効率的な配布が可能です。

Linux 資産のパッチ適用

- Linux では、クラウドエージェントが OS 標準のパッケージ管理ツール（apt、yum など）を使用します。
- 内部リポジトリ利用時は、事前にパッチを配置し、参照設定を整備します。



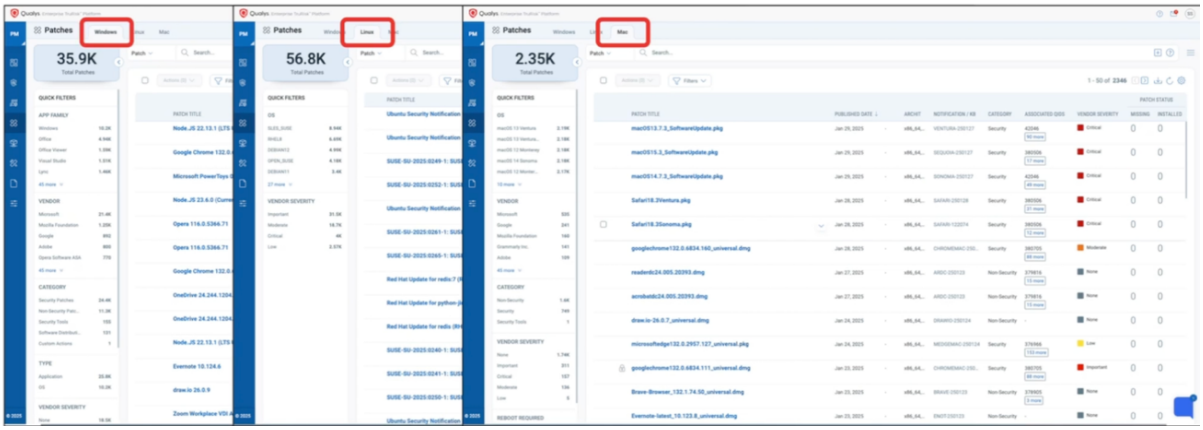
パッチジョブ実行前の準備

- 内部リポジトリに必要なパッチが揃っていることを確認してからジョブを開始することが重要です。

Qualys パッチカタログ

1. パッチ管理における「Qualys パッチカタログ」の役割

- パッチ管理の重要な要素は、Qualys パッチカタログの仕組みを理解することです。
- このカタログは、**Windows・Linux・Mac の 3 つの OS ごとに利用可能なパッチを一覧化**します。
- パッチは、**脆弱性（CVE ID）とリンクされ、QID（Qualys ID）で管理**しています。
    - QID は CVE ID がない場合は表示されない。
- この仕組みにより、**脅威の全体像を正確に把握**が可能となります。



2. Windows パッチカタログの特徴

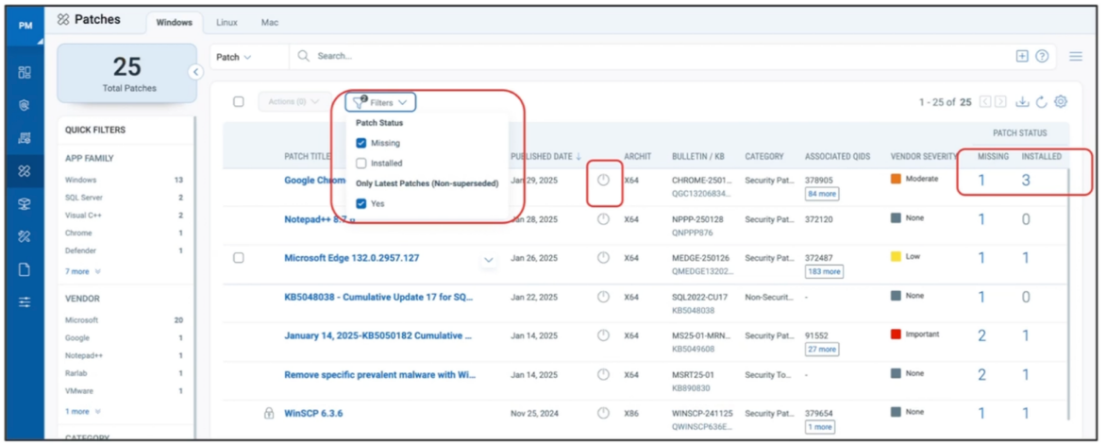
- **2 種類のパッチ**：
    - **Quality Patchable**：自由に取得可能。
    - **Acquire from Vendor**：認証情報が必要。

  ※Quality Patchable は簡単にパッチジョブに追加できるが、**Acquire from Vendor** は事前準備が必要。

- **フィルタリング機能**：
    - 「Missing」チェックで未適用パッチを表示。

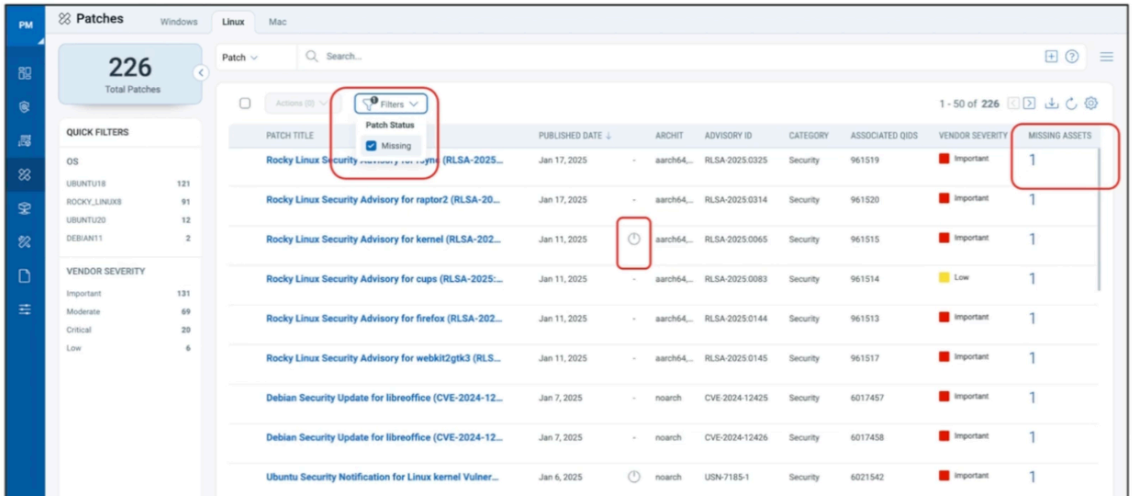
- 「Installed」チェックで適用済みパッチを表示。
- 「Non-superseded」で最新パッチのみ表示（古いパッチを除外）。

- **アイコンの意味**：
  - 鍵マーク（例：WinSCP）は「Acquire from Vendor」を示す。



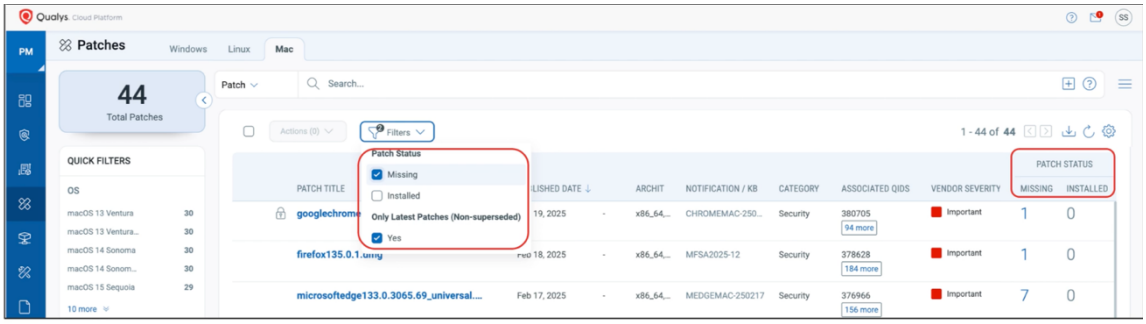
3. Linux パッチカタログの特徴

- Linux は**未適用パッチのみ表示可能**（OS の仕組みによる）。
- **優先度付けのためのソート**：
  - 公開日、カテゴリ、重大度など。
- **クイックフィルタ**：
  - 例：Ubuntu 18、Ubuntu 20、重大度別。



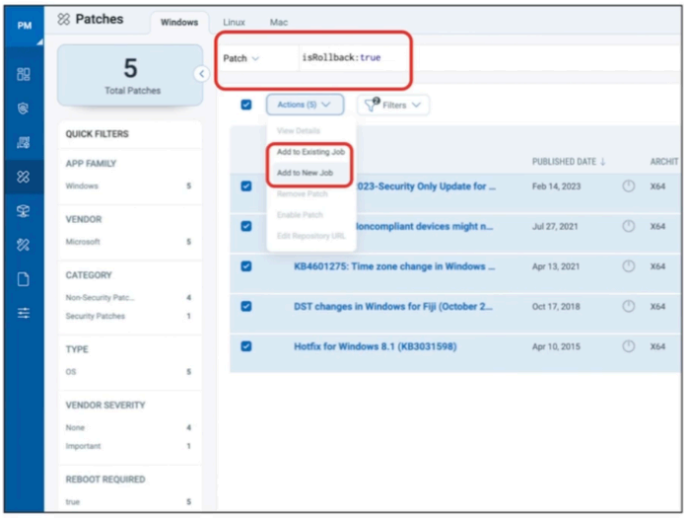
4. Mac パッチカタログの特徴

- Windows 同様、**Missing / Installed / Non-superseded** でフィルタ可能。
- 左側にクイックフィルタあり。



5. 高度なフィルタリング（クエリ言語）

- 例：
  - **再起動が必要か**　RebootRequired: (True/False)
  - **Acquire from Vendor かどうか**　DownloadMethod: (Available/AcquireFromVendor)
  - **セキュリティパッチのみ表示**　IsSecurity: (True/False)
  - **ロールバック可能なパッチ**　IsRollback: (True/False)



6. Acquire from Vendor パッチの有効化手順

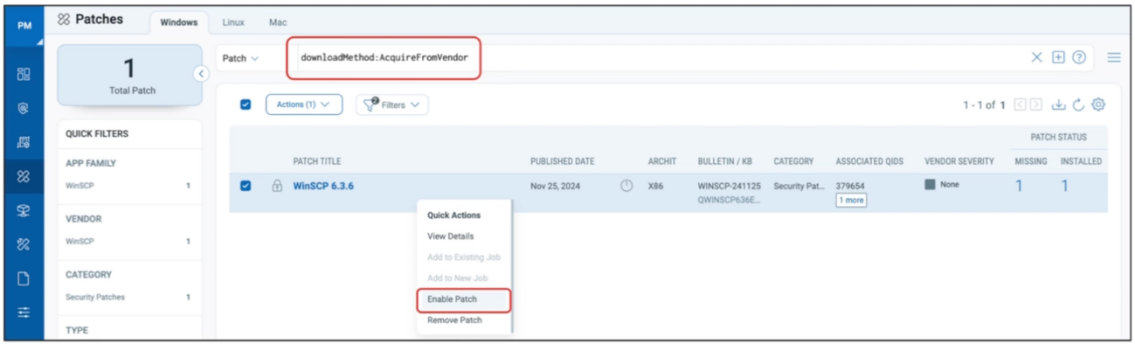
- 「Enable Patch」をクリックすると、**内部リポジトリにパッチを配置する設定画面**が表示。

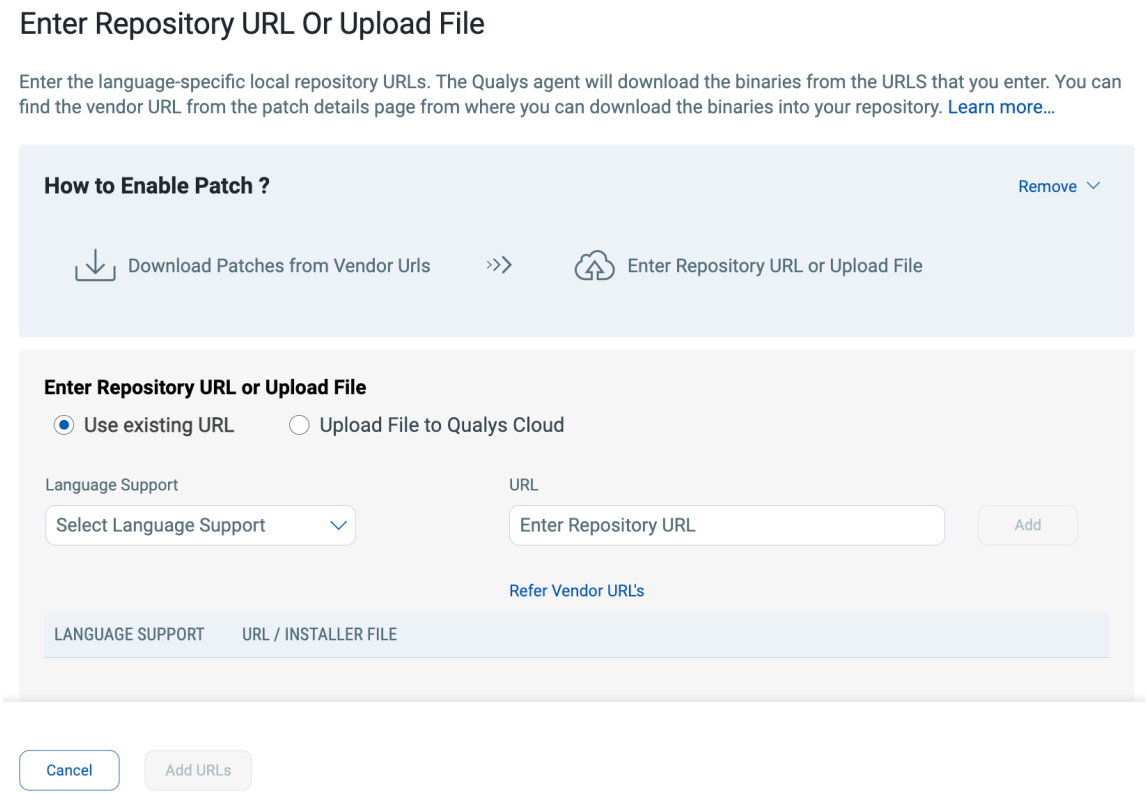
手順：

1. **内部リポジトリの URL 設定**（言語別 URL）。
2. **ベンダーからパッチをダウンロードし、内部リポジトリに配置。**

注意：

- この機能は **Windows と Mac のみ対応。**
- サブスクリプション設定で「内部リポジトリからのダウンロード」を有効化する必要あり。





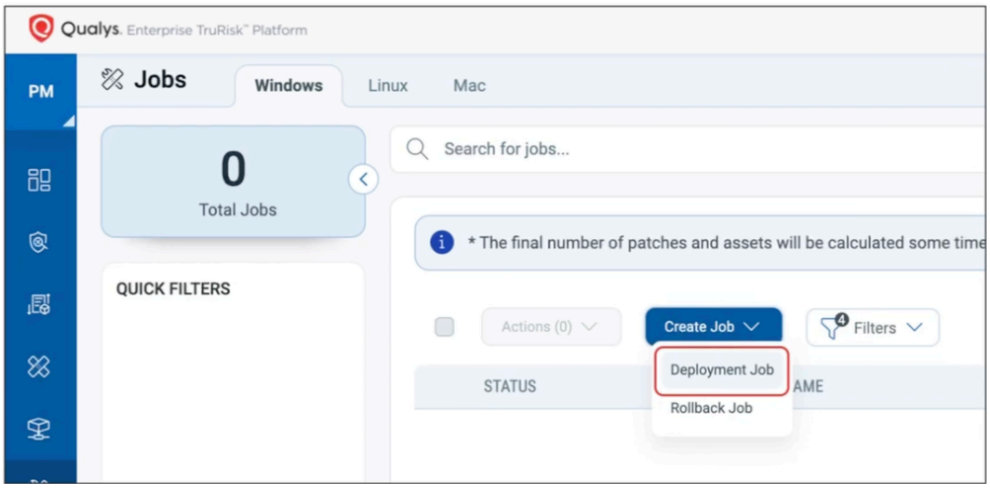
Patch Deployment Job の構成

パッチデプロイの概要

- パッチは「パッチデプロイウィザード」を使って、**パッチ管理モジュール内の 3 つの場所**からデプロイ可能です。
    1. **Jobs セクション（最も包括的）**
        - メニュー左の「Jobs」タブから開始。
        - パッチや対象資産など、ジョブの詳細をすべて設定可能。
    2. **Assets タブ**
        - 選択済みの資産にパッチを適用。
    3. **Patches タブ**
        - 選択済みのパッチを資産に適用。
- **制限事項**
    - 1 ジョブに追加できるパッチは最大 **2000 件**。
    - OS ごとに別ジョブ（Windows、Linux、Mac）で管理。

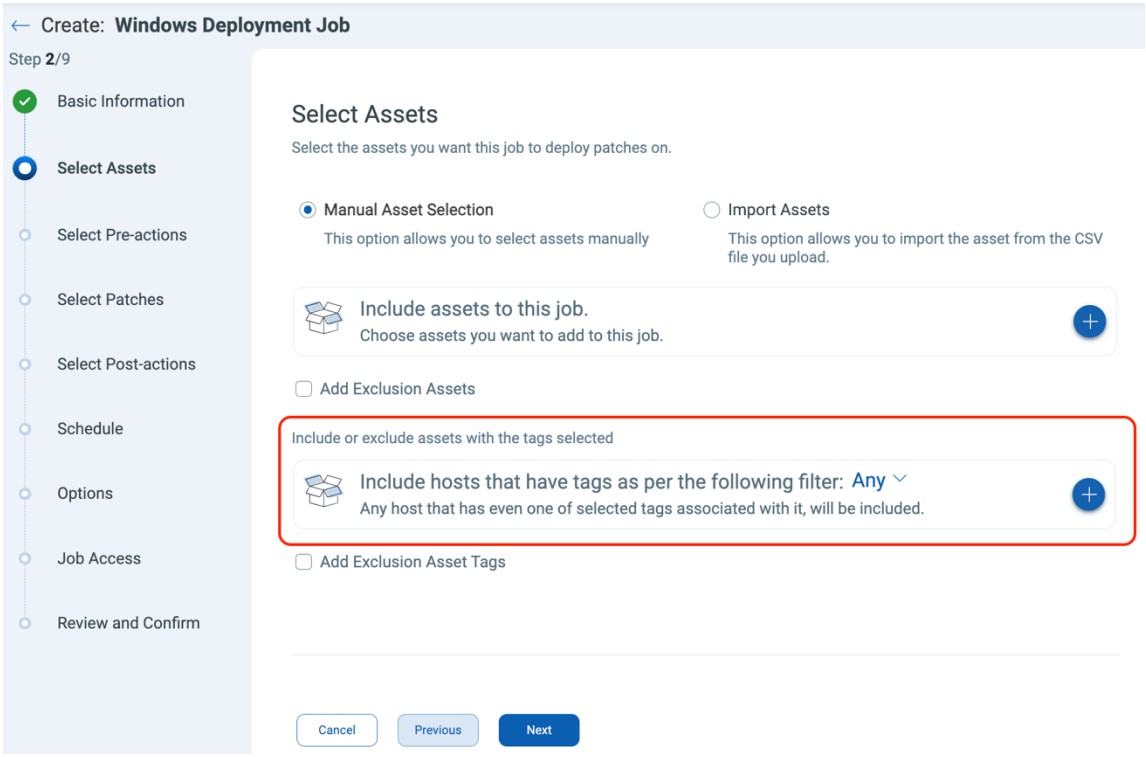
ジョブ作成手順

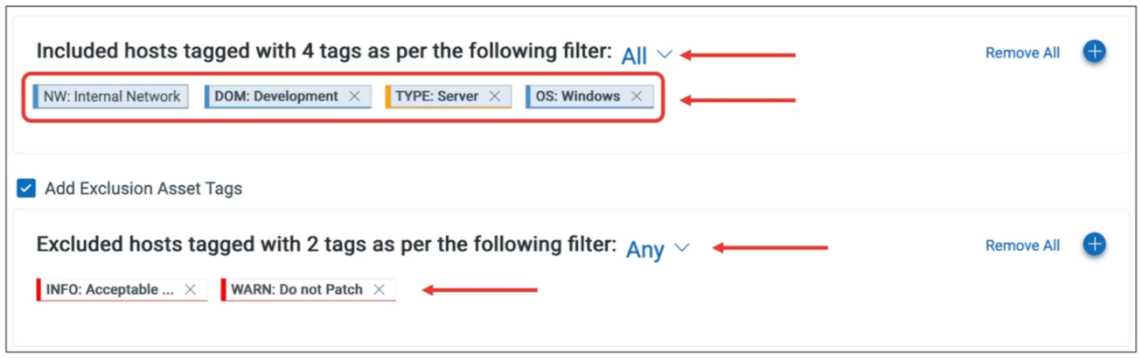
1. **Jobs ウィンドウで「Create Job」ボタンをクリック**
    - 「Deployment Job」または「Rollback Job」を選択。
    - Rollback は既存パッチを取り消すために使用。
2. **ジョブ情報入力**
    - **必須**：ジョブ名（重複不可）
    - **任意**：説明（詳細な目的を記載推奨）



資産の選択方法

- **方法 1：資産名で選択**
    - 手動で追加（チェックボックス）
    - CSV インポートも可能。
- **方法 2：資産タグで選択**
    - タグは動的または静的に付与。
    - **Any**：いずれかのタグが一致すれば追加。
    - **All**：すべてのタグが一致する資産のみ追加。
    - 除外タグも設定可能（例：「Do Not Patch」タグ）。

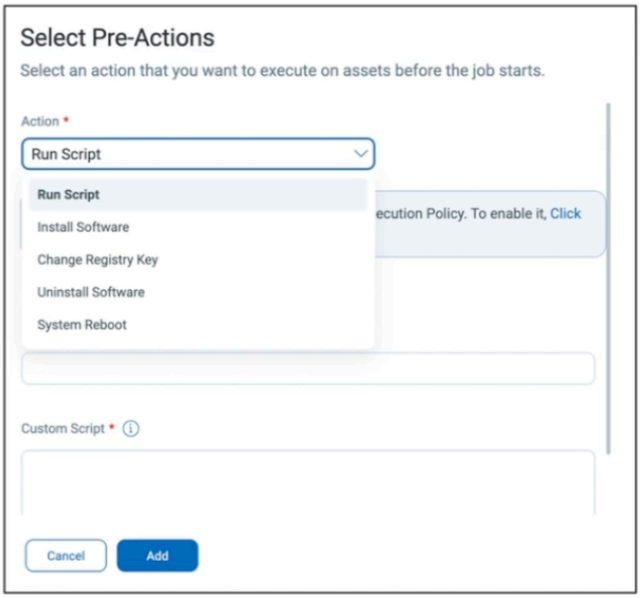




Pre／Post アクション

- 各 OS で異なるが、**最大 5 つのプリアクションと 5 つのポストアクション**を設定可能。
- 各アクションの実行時間は最大 **180 分**。
- アクション例：
  - ソフトウェアのインストール／アンインストール
  - レジストリキー変更（プリとポストで元に戻す場合あり）
  - スクリプト実行（サイズ上限：20KB、文字数上限：20,480）
  - システム再起動（選択時は他のアクションを避ける）

- **注意：**
    - スクリプトに強制再起動を含めない（再起動ループ防止）。
    - 実行結果は進捗レポートやポスト実行レポートで確認可能。



スクリプト実行と実行ポリシー

- スクリプトを実行する際、警告やメッセージを表示させないためには「**bypass execution policy**」を有効化する必要があります。
- この設定は **サブスクリプションレベルの構成**で行い、パッチ管理の設定画面で切り替えます。
- 有効化すると、署名付き・署名なしのスクリプトを警告なしで実行可能になります。

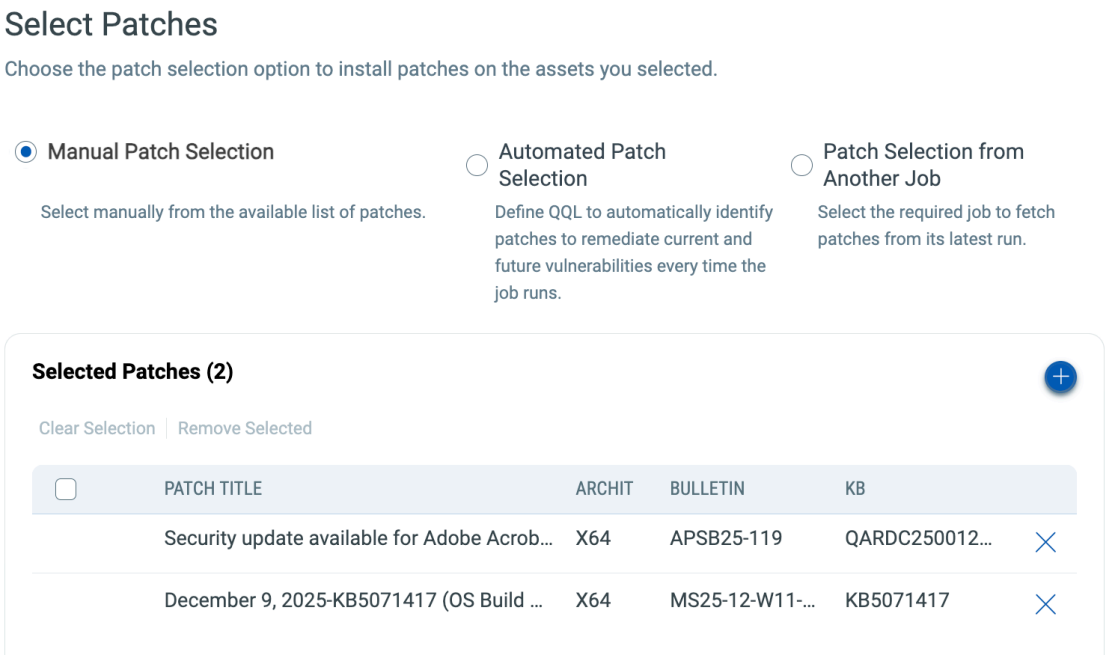
Linux でのプリ・ポストアクション

- パッチ適用前（Pre）と 後（Post）にスクリプトを実行できます。
- スクリプトには名前を付ける必要があり、**最大文字数は 20,480 文字**。
- 実行可能なスクリプトは **シェルスクリプト**や **Apple スクリプト**で、同じ文字数制限が適用されます。

パッチ選択方法

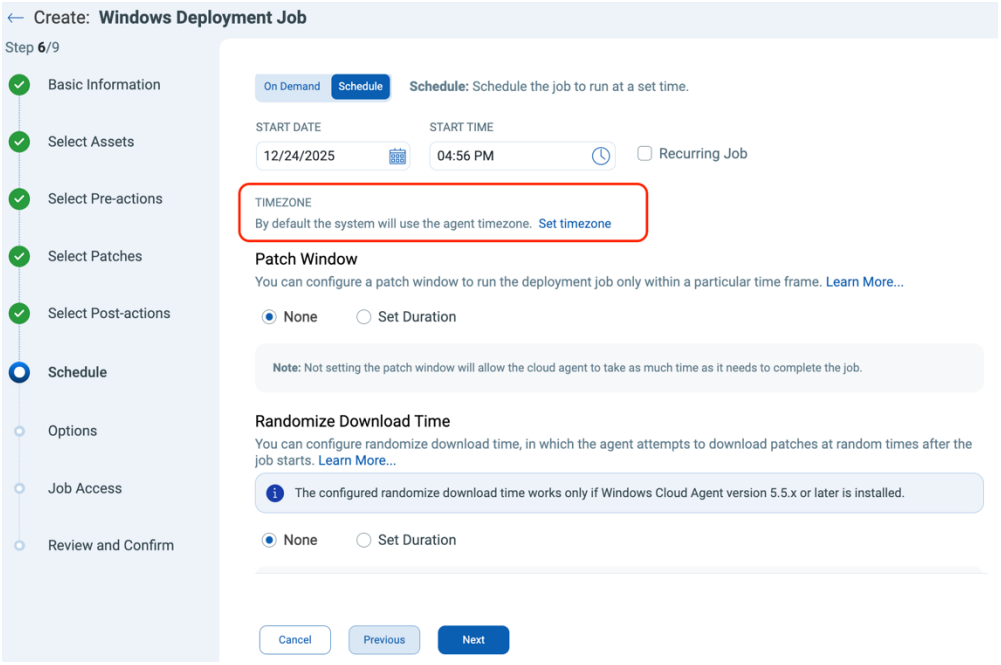
- **手動選択：**
    - 「Select patches」画面で青い「＋」をクリックし、パッチを追加。

    - デフォルトで「within scope」ボタンがオンになっており、選択した資産に関連するパッチのみ表示。
    - フィルターや検索でさらに絞り込み可能。
    - 「latest patches only」を選択すると、非推奨パッチを除外できます。
- **自動選択**：
    - パッチ選択プロファイルを設定し、脆弱性スコアや脅威情報に基づいて自動選択。
    - 例：スコア 80 以上、ランサムウェア関連、64bit 対応など。
- **過去のジョブから再利用**：
    - テスト済みパッチを本番ジョブに再利用可能。



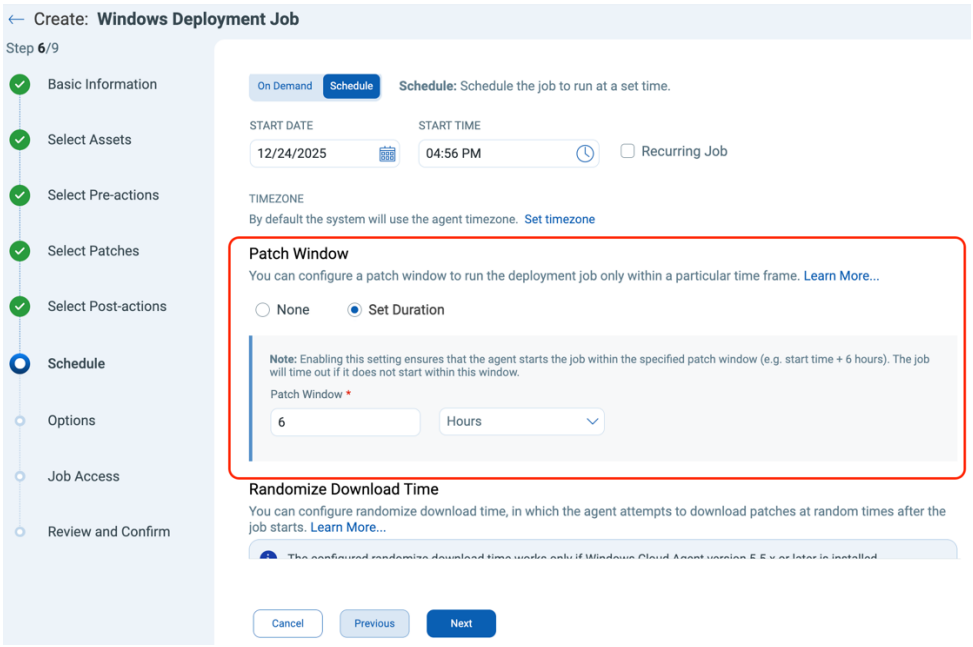
デプロイ方法

- **オンデマンド**：
    - クラウドエージェントがチェックインした時点で即時実行。
- **スケジュール**：
    - 開始日時を設定し、**一回限り**または**定期実行（毎日・毎週・毎月）**を選択。
    - **「Patch Tuesday」**などの特定日設定も可能。
    - デフォルトでは**エージェントのローカルタイムゾーンで実行**されますが、統一タイムゾーン設定も可能。



パッチウィンドウ

- パッチジョブが開始できる時間枠を設定（**30 分～168 時間**）
- ウィンドウ内に開始できない場合、次回に延期または失敗。
- エージェントがオフライン、ダウンロード時間不足などが原因になることがあります。

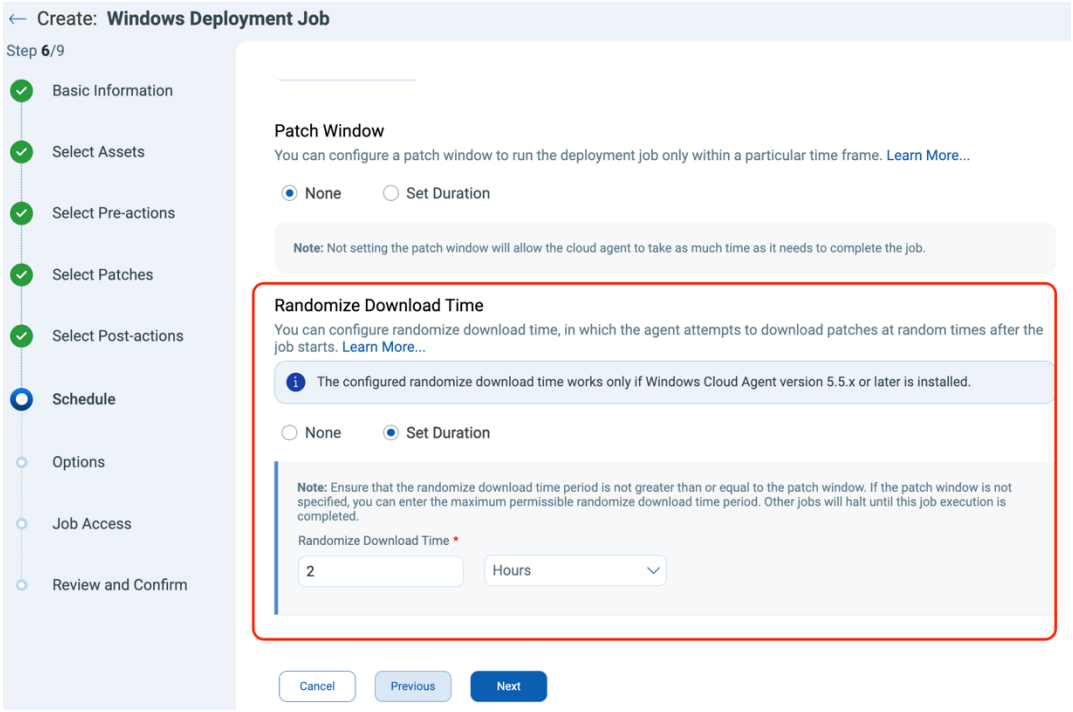


スキャンとの競合回避

- 「**Defer cloud agent scans**」オプションで、パッチジョブ中に脆弱性スキャンを遅延させることが可能です。
- ただし、スキャンが先に開始されている場合はスキャンが優先されます。

ネットワークへの影響とランダムダウンロード時間

パッチジョブ開始時に、すべての資産が同時にダウンロードを開始するとネットワークに負荷がかかります。そのため、ランダムなダウンロード時間を設定し、資産ごとに異なるタイミングでダウンロードを開始することで負荷を分散します。**最大設定可能時間は 2 時間**です。なお、この設定を行うと「**オポチュニスティックパッチダウンロード**」は利用できません。これは、ジョブ開始前にアイドル時間を利用してパッチを事前にダウンロードする機能です。**ジョブ開始まで 3 時間以上ある場合は、この機能を推奨します。**



通知とメッセージ設定

パッチジョブの実行時には、ユーザーに対して通知や再起動メッセージを表示できます。これらは個別にオン・オフ設定が可能です。Linux では再起動メッセージをデフォルトで表示しますが、抑制も可能です。再起動までのカウントダウン表示も設定できます。**通知メールは最大 50 件まで登録できます。**また、パッチインストールが一部失敗しても処理を継続するオプションがあります。Mac では、パッチ適用時に資格情報入力を促すメッセージを表示できます。

パッチジョブの共有と保存

ジョブ作成者は、他のユーザーにジョブアクセス権を付与できます。ただし、追加できる資産は作成者のスコープ内に限られます。ジョブは「保存して有効化」または「保存のみ」で管理できます。前者は即時実行可能、後者は無効状態で保存されます。

パッチジョブの例

- **パッチチューズデー対応**：テスト環境で翌日に実施し、問題なければ本番環境で数日後に適用します。
- **再起動不要のパッチ適用**：業務時間中に小規模アプリ（例：Notepad やブラウザ）を更新します。
- **即時パッチ適用**：緊急時に迅速に資産を更新します。

NCSC 推奨の 5 つの対策

1. **更新ポリシーの策定**：すべての資産を対象にします。
2. **資産の完全な把握**：発見作業を徹底します。
3. **リスクの優先順位付け**：重要資産と重大な脆弱性を優先します。
4. **更新しないリスクの認識**：組織として責任を持ちます。
5. **プロセスの定期的な見直し**：脆弱性管理を継続的に改善します。推奨サイクルは、外部公開サービスは 5 日以内、重要資産は 7 日以内、その他は 14 日以内です。

Internet-facing services and software	5 days
Operating system and applications	7 days
Internal / air-gapped services	14 days

Recommended SLA for remediation from NCSC

Patch Job Status

1. モジュールの概要

このモジュールでは、パッチジョブのステータス確認方法について説明します。パッチ管理モジュールは、パッチ適用やエンドユーザーへの通知を管理するために、別のプロセスを使用します。ターゲットホスト上で表示されるメッセージや通知は、このプロセスによって制御されます。

2. クラウドエージェントと UI の役割

Qualys Cloud Agent は、エージェント自体の実行を担当します。一方、Qualys Cloud Agent UI は、パッチ管理プロセスを実行し、パッチ適用中にメッセージを表示します。表示されるメッセージには、パッチ適用開始前、進行中、完了後の通知が含まれます。

3. パッチインストールのプロセス

パッチのインストールは「St.deployed.exe」という別のプロセスが担当します。Windows のジョブページでは、複数のジョブが表示され、進行中のジョブや完了間近のジョブを確認できます。このページでは、ジョブ名、スケジュールタイプ、対象パッチ、資産数、選択されたタグなどの情報が確認できます。

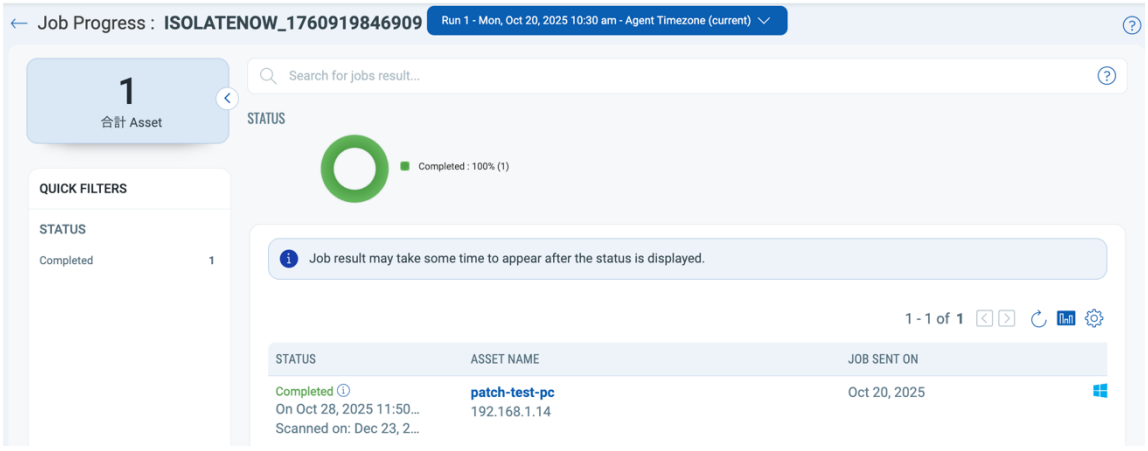
4. ジョブステータスの種類

ジョブには複数のステータスがあります。主なものは以下の通りです。

- **部分的に構成済み(Partially Configured)**：パッチのみ追加され、他の設定が未完了です。
- **無効化（Disabled）**：ジョブは実行されませんが、編集可能です。
- **有効化（Enabled）**：設定された時間に実行されます。
- **準備中（Preparing）**：ジョブ定義ファイル（マニフェスト）を作成中です。
- **準備完了（Prepared）**：マニフェストが作成され、資産にダウンロード可能です。
- **実行中（Executing）**：ジョブが開始され、資産から進捗が返されます。

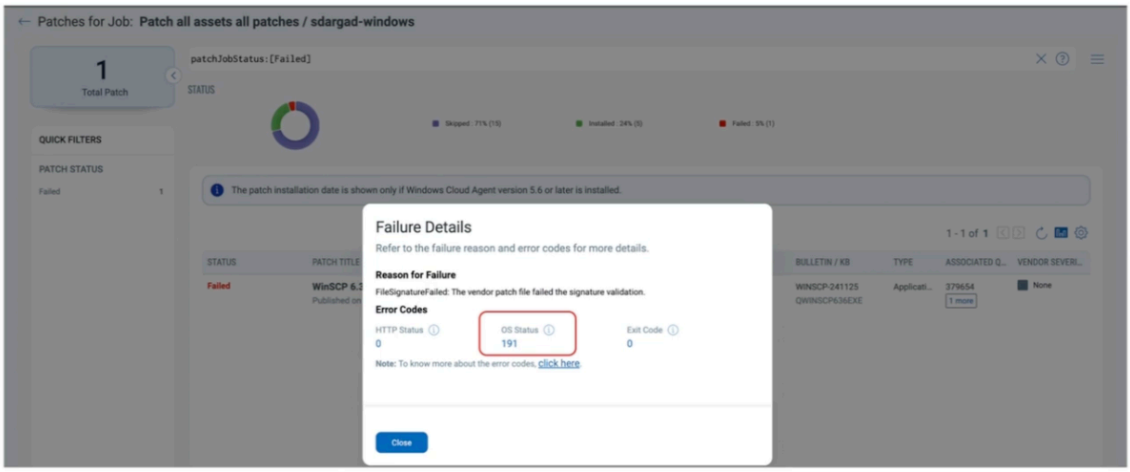
5. ジョブ進捗の確認方法

ジョブ一覧から「クイックアクション」→「進捗を表示」を選択すると、対象資産の進捗状況を確認できます。画面には、完了、保留、再起動待ちなどの状態が表示されます。上部の円グラフでは、資産のステータスが視覚的に示されます。



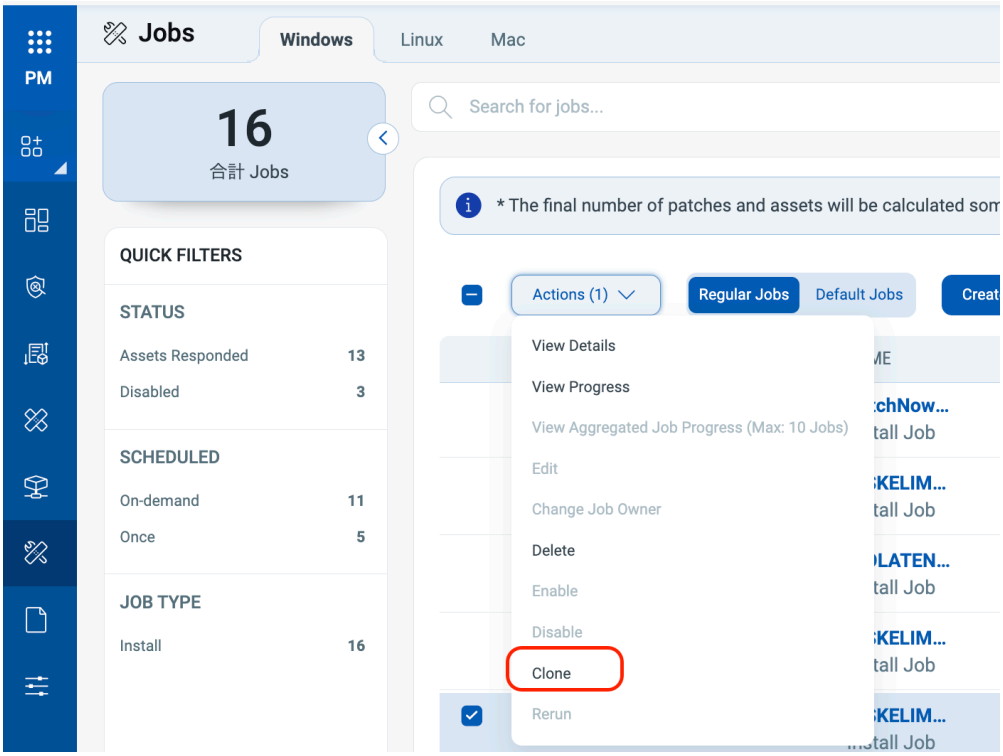
6. **詳細情報とエラーコード**

   各資産ごとに、**インストール済み、失敗、スキップ**されたパッチ数を確認できます。スキップ理由は、パッチが適用不要、既にインストール済み、または他のパッチに置き換えられた場合です。失敗したパッチの詳細は、エラーコード（HTTP ステータス、No ステータス、Exit コード）で確認できます。例として、OS ステータス 191 が原因の場合、Web で調査できます。



7. **ジョブの複製**

   ジョブページからジョブをクローンし、異なる資産セットに再展開できます。例えば、テスト環境での検証後、本番環境に適用する際に便利です。



Automated Patch Selection

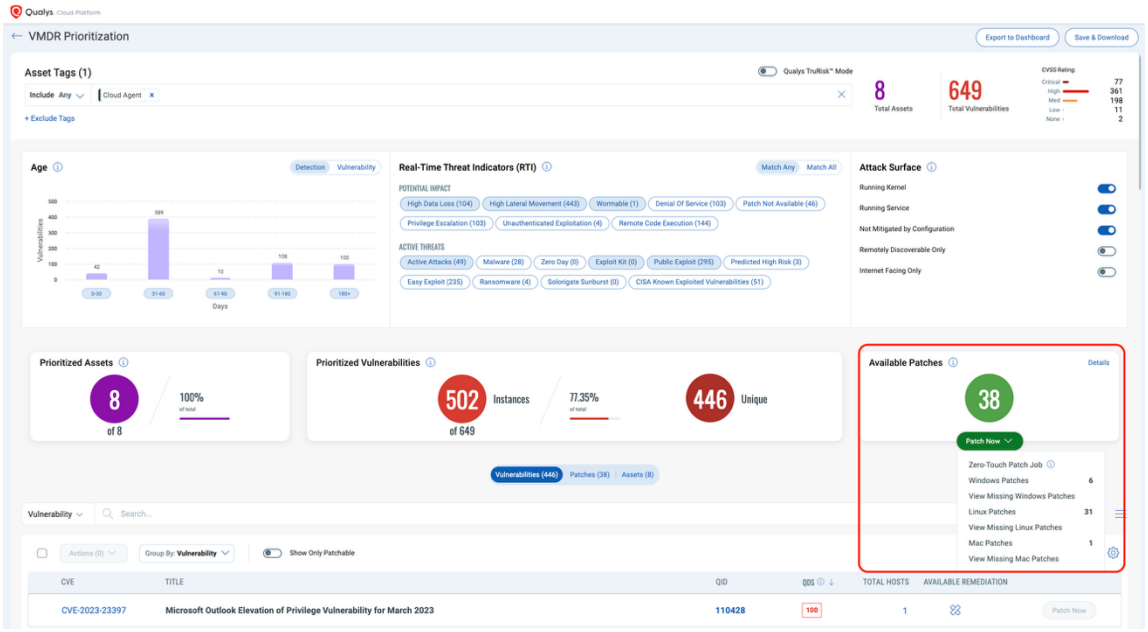
このセクションでは、**パッチ選択**をより容易にし、リスク軽減をより的確に行うための様々な手法について学びます。これは、TruRisk スコア、脆弱性の QDS、リアルタイムの脅威情報などの要素に基づいて行うことができます。

1. **スマートオートメーションの概要**

   スマートオートメーションは、環境内で最もリスクの高い製品を特定し、必要なパッチや構成変更を自動的に適用するジョブを作成する仕組みです。これにより、手動での対応よりも迅速に脆弱性を修正できます。スマートオートメーションは**「パッチ重視」ではなく「リスク重視」**のアプローチを採用しています。

2. **リスクベースのアプローチ**

   リスクを基準にすることで、資産全体を分析し、サイバーセキュリティリスクを評価します。その結果、現在および将来のリスクを効率的に軽減するための自動化ジョブを推奨します。また、運用リスクへの影響も考慮する必要があります。



3. 資産のタグ付けと優先順位付け

Qualys の機能を使うことで、資産のタグや優先度に基づき、脆弱性と資産価値を組み合わせて正しい優先順位を決定します。これにより、パッチの重大度だけでなく、資産の重要性も考慮できます。

4. 自動化の利点

「低ハードルな更新」や再起動不要のパッチを自動化することで、効率的にリスクを低減できます。また、テスト・承認・展開のプロセスを自動化することで、信頼性の高い運用が可能になります。

5. VMR モジュールの活用

VMR（Vulnerability Management and Remediation）モジュールは、パッチ管理プロセスと統合し、資産の重要度と脆弱性の重大度を関連付けて優先順位を決定します。これにより、リスクを減らすためのパッチジョブを効率的に作成できます。

6. 優先順位レポートとパッチ管理

VMR の優先順位レポートでは、最もリスクの高い脆弱性を特定し、Windows・Linux・Mac の各エージェントに対応するパッチを選択できます。ジョブ作成時には、タグやパッチが自動的に引き継がれます。

7. ゼロタッチパッチング

ゼロタッチパッチングは、最もリスクの高い資産を自動的に特定し、Windows の脆弱性を継続的に修正するジョブを作成します。スケジュール設定により、将来の脆弱性にも対応できます。現在は Windows 資産のみ対応しています。

8. 脅威インテリジェンスとの連携

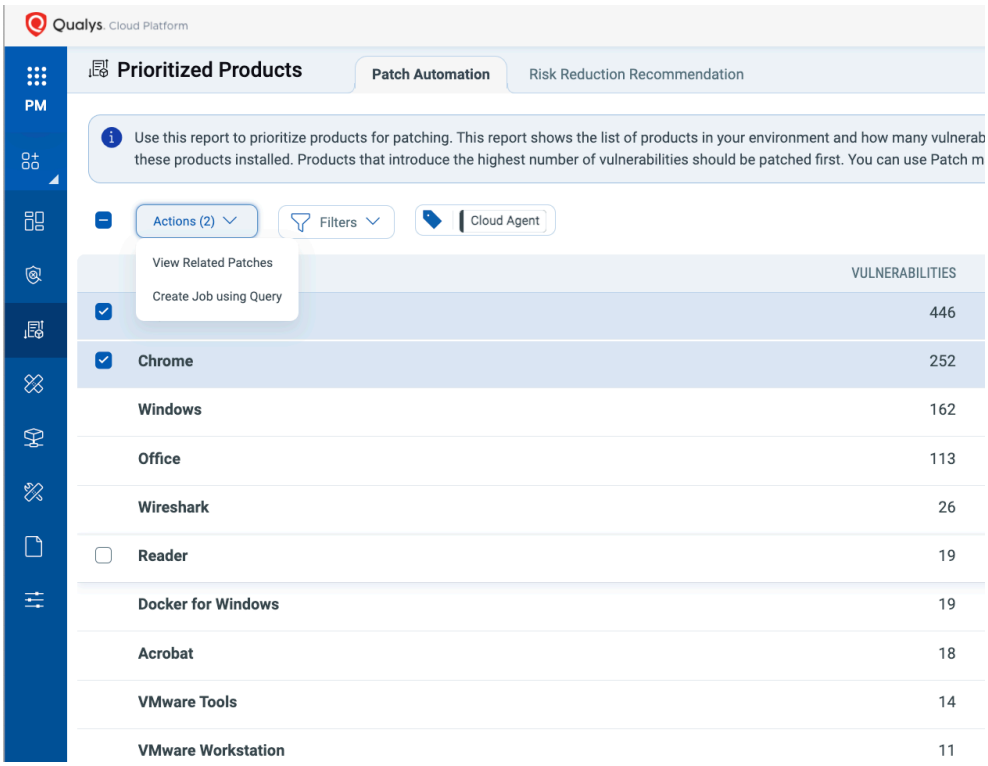
ゼロタッチパッチングでは、マルウェアやランサムウェア関連の脆弱性を自動的に修正する設定が可能です。これにより、攻撃者が脆弱性を悪用するまでの時間を短縮できます。

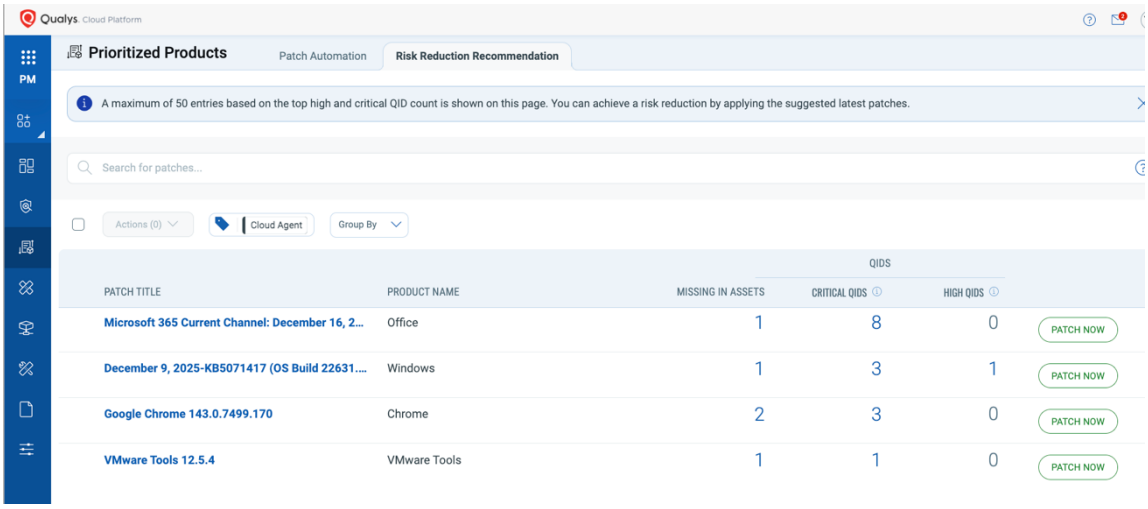
9. パッチ管理によるリスク低減

パッチ管理モジュールでは、過去の脆弱性データを活用し、特定のアプリケーションを自動化ジョブに分離できます。ブラウザなど再起動不要のアプリは特に自動化に適しています。

10. 優先製品とリスク低減推奨

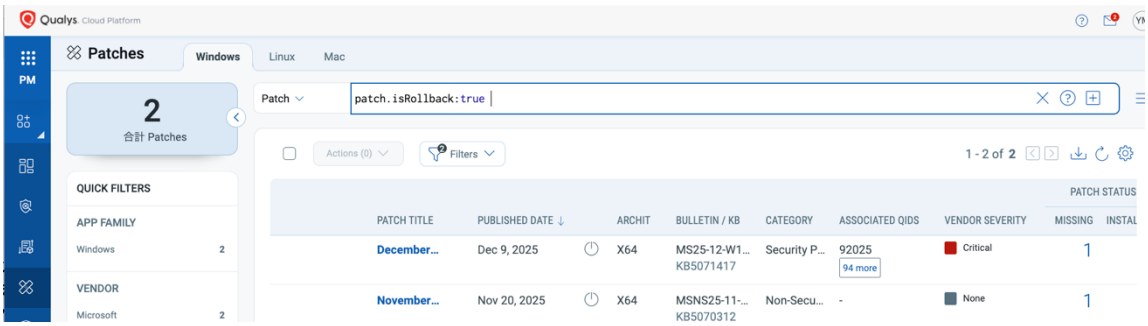
「優先製品」タブでは、脆弱性数に基づいてアプリをリスト化し、常に最新状態を維持できます。また、「リスク低減推奨」では、Windows エージェントに対して最も効果的なパッチを提示し、迅速なリスク低減を実現します。





パッチのロールバック

Windows パッチをロールバックするには、ジョブセクションの Windows タブで「ジョブ作成」ボタンをクリックし、「ロールバックジョブ」オプションを選択します。ロールバックジョブウィザードでは、パッチ適用ジョブと同様の手順で設定しますが、ロールバック可能なパッチのみが対象です。対象パッチは検索バーに「patch.isRollback:true」と入力して確認できます。



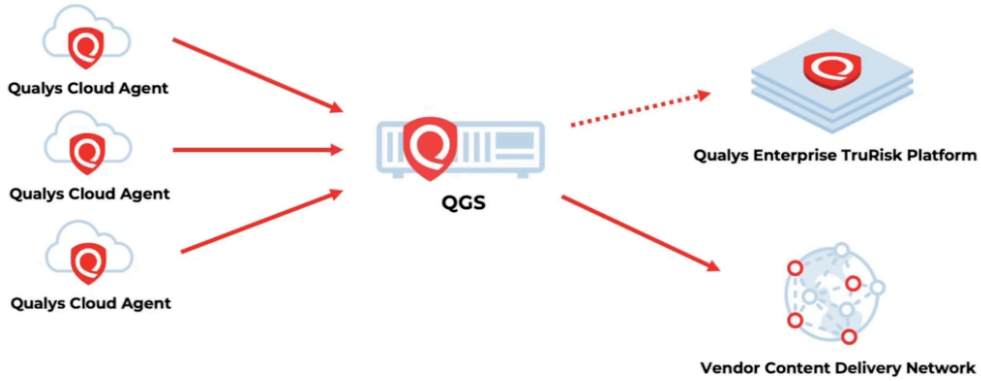
資産の選択は、特定の資産や資産タグで行えます。一度作成したロールバックジョブに、後から新しいパッチを追加したい場合は、そのジョブを「編集」することで対応できます。つまり、ジョブを再作成する必要はなく、既存のジョブにパッチを追加できます。

Linux 資産の場合はより簡単で、一覧からほぼすべてのパッチを選択できます。資産の選択はタグまたは個別選択で行いますが、管理権限の範囲内の資産のみ対象です。たとえば、特定の地域のみ管理権限がある場合、他地域の資産にはパッチ適用や解除はできません。

Qualys Gateway Service を使ったパッチ適用の最適化

このセクションでは、Qualys Gateway Service (QGS) と、それがパッチ展開ジョブの最適化にどのように役立つかについて学習します。

Qualys Gateway Service（QGS）は、Qualys Cloud Agent の展開を最適化するための仮想アプライアンスです。QGS は、プロキシサービスとキャッシュ機能を提供し、仮想スキャナーアプライアンスとは異なる役割を持ちます。対応環境は、VMware、Microsoft Hyper-V、AWS、Azure、Google Cloud Platform、OpenStack、Nutanix です。Qualys VDR の顧客は追加費用なしで利用できます。



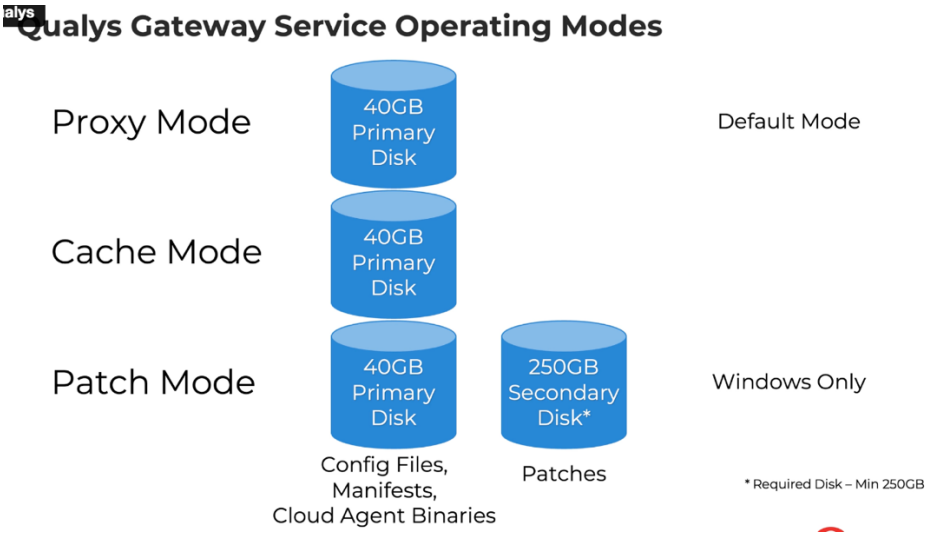
QGS には 3 つの動作モードがあります。

プロキシモード（デフォルト）：Cloud Agent が QGS を経由して必要なサービスにアクセスします。

キャッシュモード：Cloud Agent がダウンロードする構成ファイルやバイナリを QGS にキャッシュし、ネットワーク帯域を節約します。

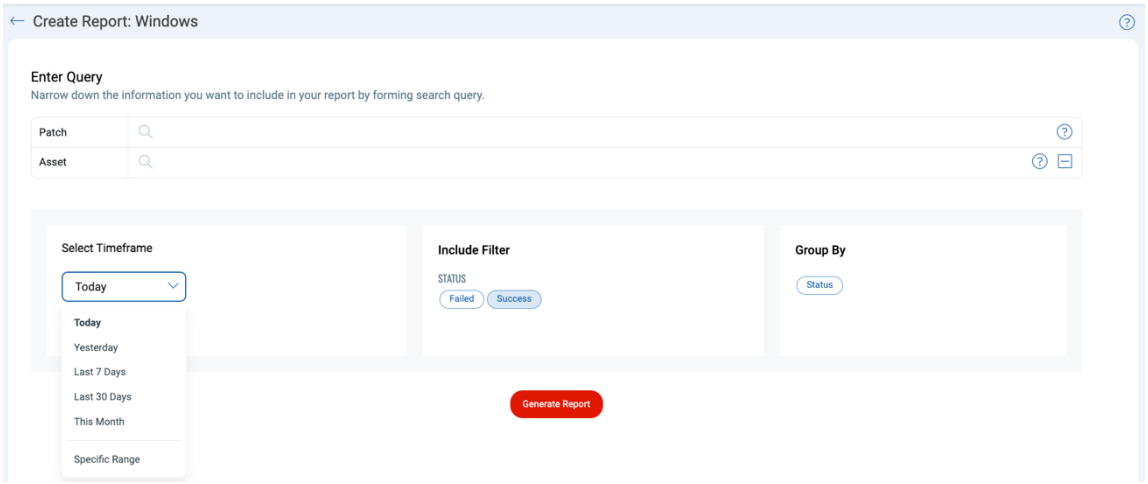
パッチモード：Windows 資産向けに、ダウンロードされたパッチを QGS に保存します。このモードには 250GB 以上の追加ディスクが必要です。

キャッシュモードとパッチモードはデフォルトでは無効であり、Qualys Enterprise TruRisk Platform の UI から設定できます。これらの機能を活用することで、ネットワーク帯域と時間を大幅に節約できます。



パッチレポート

パッチレポートについて説明します。パッチレポートは、Windows、Linux、Mac の資産に対して生成できます。レポートの設定は 4 つのステップで行います。
まず、レポートを実行する対象となるパッチを決定します。さらに、資産を指定してレポートの範囲をより詳細に絞り込むこともできます。
次に、レポートが対象とする期間を設定します。期間は「昨日」「先週」「過去 30 日間」「今月の開始から今日まで」または特定の開始日と終了日を指定できます。
3 番目に、必要に応じて成功したパッチと失敗したパッチを選択します。
最後に、レポート結果をステータスごとにグループ化するかどうかを選択できます。



画面上で利用可能なリアルタイムデータは、レポートにダウンロードされます。たとえば、フィルターや検索機能を適用した場合、選択したデータや入力した QQL トークンの結果がそのままレポートに反映されます。レポート内の日付や時刻に関する記載は、UTC タイムスタンプとして扱われます。
レポートを開始すると、データ量に応じて処理に数分かかる場合があります。完了すると「準備完了」ステータスが表示され、レポートをダウンロードできます。**ユーザーごとに同時にアクセスできるレポートは最新の 10 件までです。作成されたレポートは 7 日間保持され、その後データは削除されます。**
レポートは CSV 形式で ZIP ファイルとしてダウンロードできます。CSV ファイルには、UI に表示されているデータに加えて、UI には表示されないいくつかの列も含まれています。**レポートファイルは圧縮後で最大 1GB までとなります。**

Using Unified Dashboards To Communicate Risk

このセクションでは、パッチ管理を使用したリスク軽減の詳細と、資産、ジョブ、構成の詳細を監視するために使用できるさまざまなダッシュボードについて学習します。

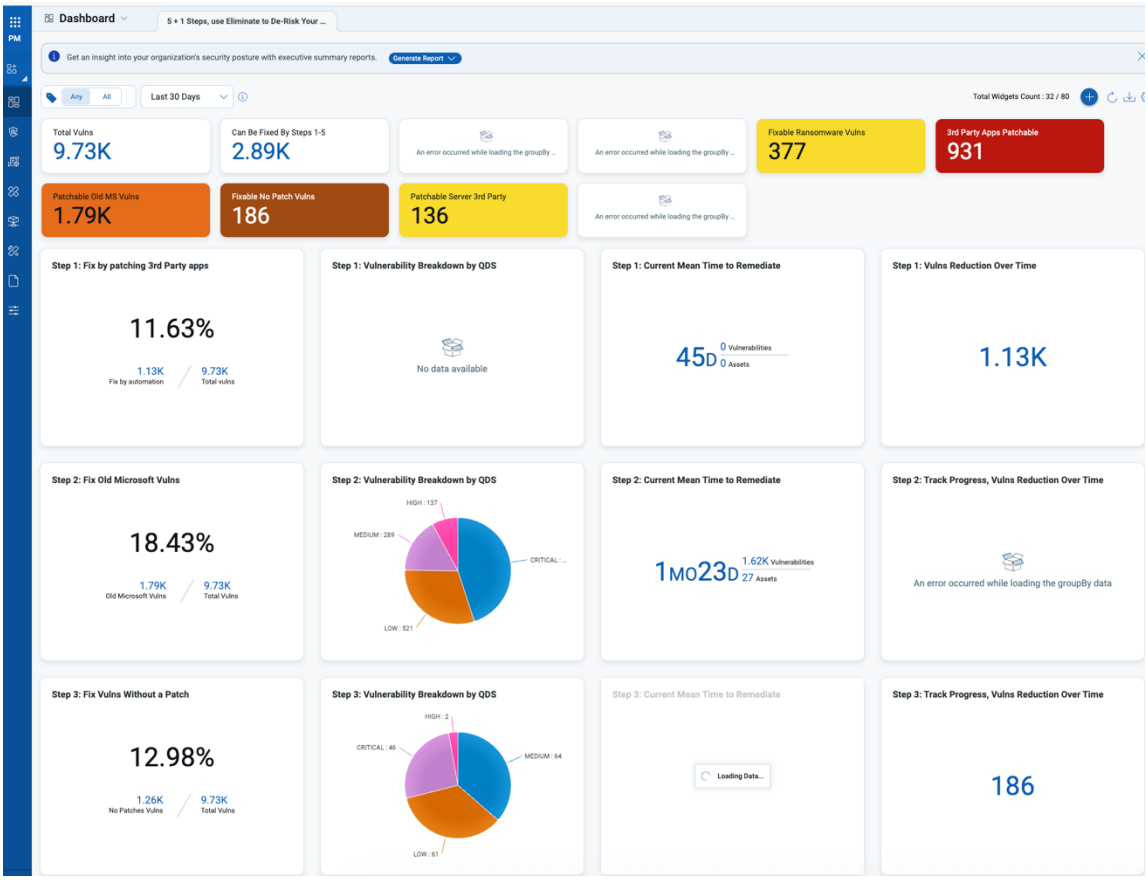
ダッシュボードは、情報管理やビジネスインテリジェンスの活用において非常に重要なツールです。メトリクスや主要業績評価指標（KPI）などのデータを、複数のデータソースから収集し、整理し、簡単にアクセスできる場所に表示します。データビジュアライゼーションを用いることで、ダッシュボードはメトリクスを視覚的に伝え、ユーザーがデータ内の複雑な関係を理解しやすくします。

データダッシュボードでは、異なるが関連するメトリクス間の比較を容易に行え、トレンドを特定し、組織のデータに潜む潜在的な課題を事前に把握できます。ダッシュボードは資産を視覚化するのに役立ちます。各ダッシュボードは、関心のあるリソースデータを表示するウィジェットの集合体です。検索クエリを使ってウィジェットを追加し、データビジュアライゼーションを強化できます。複数のダッシュボードを作成し、切り替えることも可能です。また、ダッシュボードやウィジェットの構成をエクスポート・インポートして、アカウント間や Qualys コミュニティ内で共有できます。デフォルトのダッシュボードを個別にカスタマイズし、ウィジェットの追加、サイズ変更、レイアウト変更ができます。メニューを使ってダッシュボードを管理してください。

パッチ構成変更ダッシュボードは、全体的なパッチ適用状況と進捗を表示します。最新の未適用パッチの数をカテゴリ別（セキュリティパッチ、セキュリティツール、非セキュリティパッチ）に示します。また、再起動が必要なパッチや再起動待ちのホストの概要も確認できます。デフォルトのダッシュボードページには多くのウィジェットがあり、編集・削除・追加が可能です。ダッシュボードやウィジェットの使い方、共有方法については、下部に記載されたトレーニング動画をご覧ください。
リスク削減ダッシュボードは、脆弱性を修正するための主要な手順を提示します。5 つのステップには、サードパーティアプリケーションのパッチ適用が含まれます。脆弱性の QDS ランクの内訳や MTR 概要も表示されます。古い Microsoft 脆弱性の修正についても同様のビューがあります。パッチ不要で修正できる脆弱性や、Java、Web サーバー、SQL などの非 OS 脆弱性の修正方法も確認できます。5 番目のステップは Mac の脆弱性修正です。さらに、潜在的なリスク削減の全体像やメーカー別の脆弱性ビューも提供されます。
ランサムウェア防止のための 3 つのヒントダッシュボードでは、ランサムウェアの脅威を複数の側面に分けて分析します。最初のセクションは、ランサムウェア脆弱性の全体像を理解することです。Qualys は

25 以上の脅威インテリジェンスパートナーを活用して、この洞察を構築しています。2 番目は、OS で修正可能なランサムウェア脆弱性です。3 番目は、ブラウザや拡張機能などのアプリケーションで修正可能な脆弱性です。これらの情報により、ランサムウェア脆弱性の重大性や現在の平均修復時間を深く理解でき、修復プロセスを改善してリスクを減らせます。

Qualys の平均修復時間ダッシュボードは、脆弱性管理、検出、対応の重要な要素です。



TruRisk Mitigate

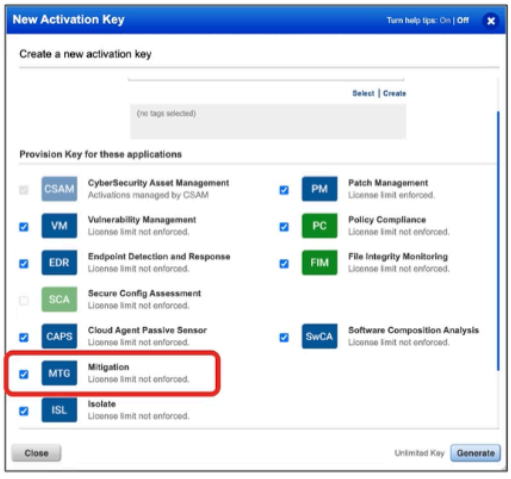
このセクションでは、**TruRisk Mitigate** の重要性とその機能、軽減のための資産のアクティブ化から脆弱性の軽減までのワークフロー、軽減モジュールに関連するさまざまな QQL トークンについて学習します。

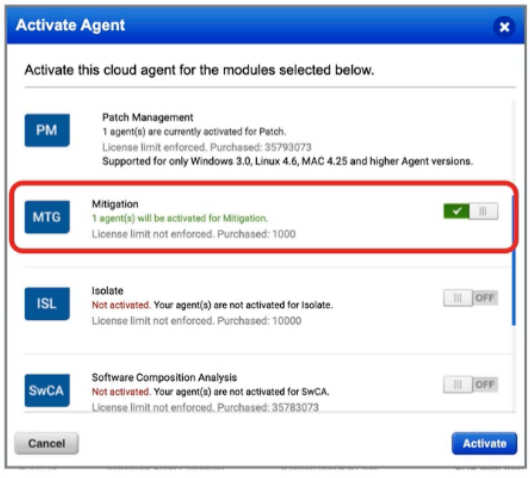
脆弱性のすべてにパッチが提供されるわけではありません。パッチの適用が高リスクと判断される場合や、組織がパッチ適用のサイクルで運用している場合もあります。そのため、パッチ適用までの間に脆弱性のリスクを軽減する必要があります。こうしたシナリオでは、**リスク軽減（Mitigation）によって脆弱性に対応し、リスクを下げることができます**。

True Risk Mitigate は、CISA や Qualys のベンダーから提供される高度な制御やスクリプトを使用して脅威に対応します。**True Recommendations** では、パッチ適用ができない脆弱性に対して QID を修正アクションにマッピングし、代替の緩和策を提供します。これにより、パッチ適用による障害リスクを回避できます。統合されたパッチ適用、構成変更、ミティゲーションのワークフローにより、シームレスな体験を実現します。また、ゼロデイ脆弱性に対する防御も提供し、すべての結果は VMD レポートに反映され、完全な可視性を確保します。

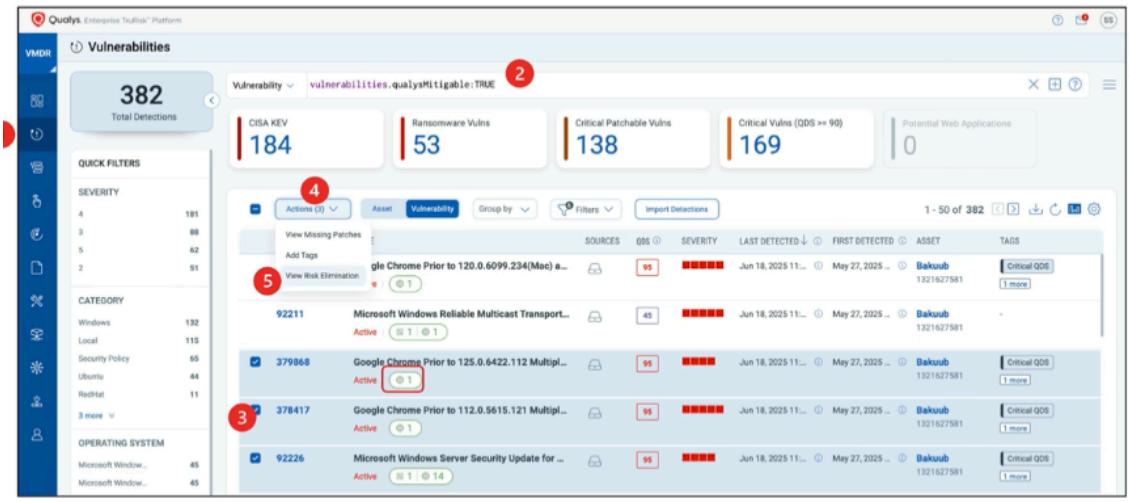
例として、**QID 378985** の場合、リモート攻撃者が長時間の暗号化セッションに対してバースデー攻撃を行い、平文データを取得できる脆弱性があります。この解決策は、DES、Triple DES、IDEA、RC2 暗号の使用を停止することです。これはミティゲーションによって実現できます。

ホストでミティゲーションを有効化する方法は 2 つあります。1 つ目は、クラウドエージェントのアクティベーションキーを使用し、そのキーを使ってすべてのホストを更新する方法です。2 つ目は、エージェントメニューから個別または複数のアクティブホストを選択し、ミティゲーションを有効化する方法です。
ライセンス消費状況を確認するには、ミティゲートメニューの構成画面からライセンス画面をクリックします。ここで、保有ライセンス数、消費状況、アクティブ化された OS を確認できます。





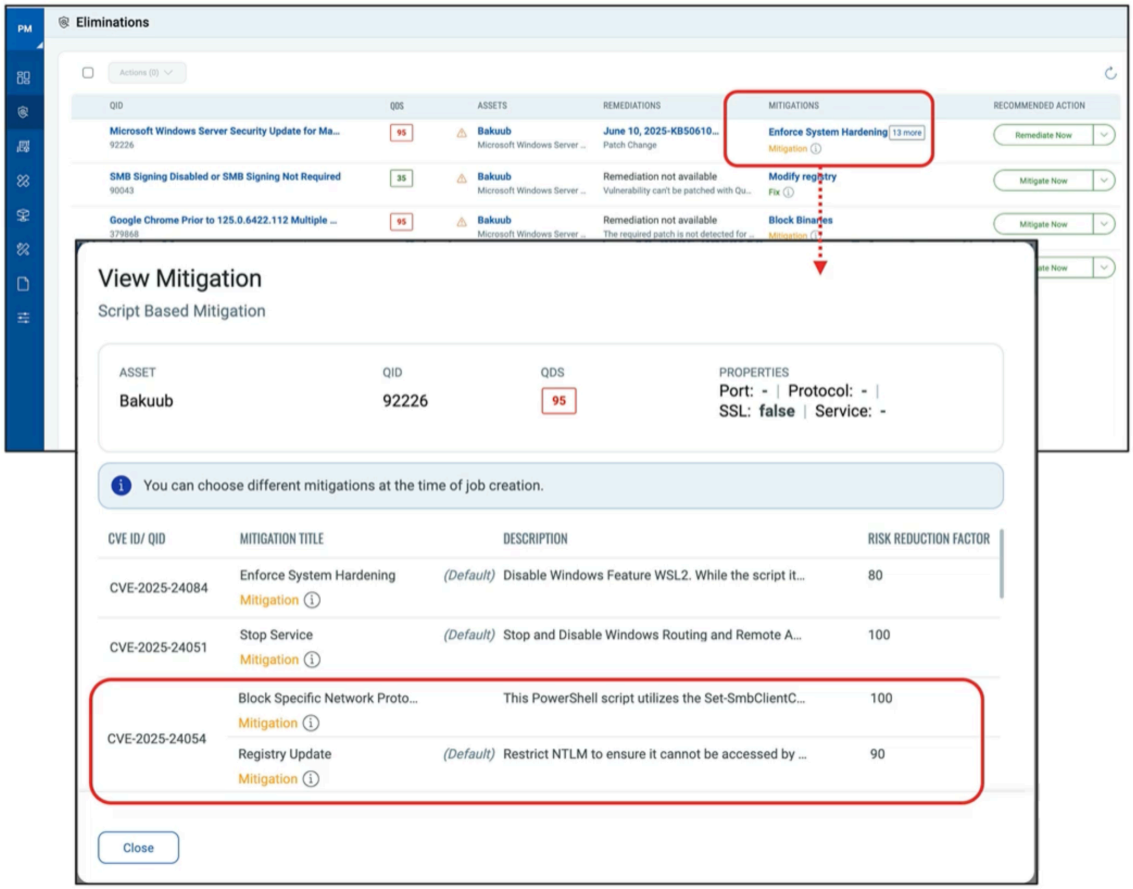
VMDR では、True Mitigate でミティゲート可能な脆弱性を確認できます。簡単な QQL トークン「**vulnerabilities.qualysMitigable:true**」を使用すると、ミティゲート可能な脆弱性を一覧表示できます。また、ミティゲーションアイコンで識別することも可能です。



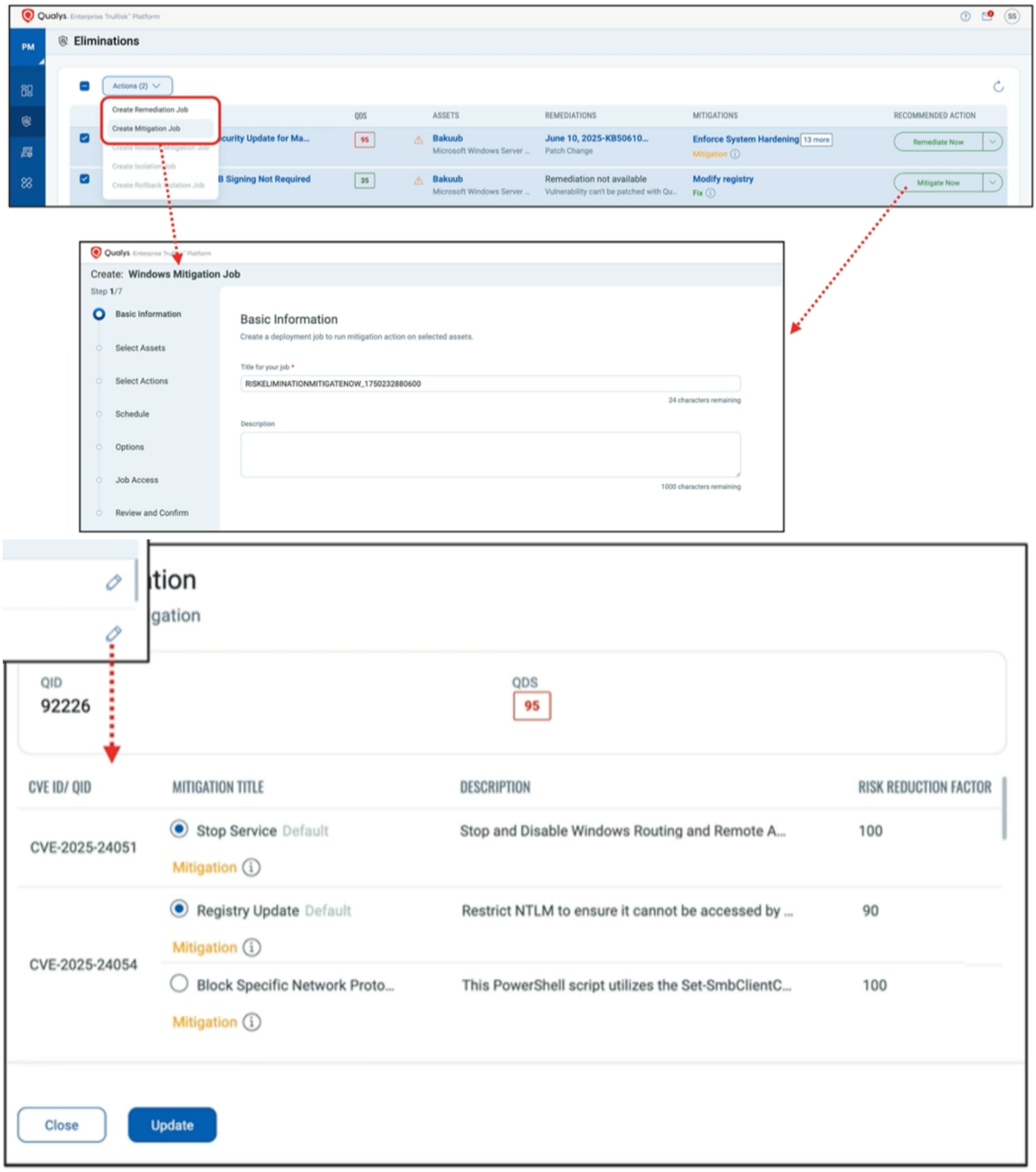
選択した脆弱性に対しては、アクションボタン（画面上の番号 4）をクリックすることで、欠落しているパッチの確認、タグ付け、リスク除去手順の表示ができます。修正やパッチがある場合は、脆弱性を修正できます。パッチがすぐに適用できない場合は、ミティゲートするオプションもあります。

ミティゲーションには、レジストリキーの更新やバイナリのブロックなどがあります。バイナリのブロックは一時的な解決策であり、将来的には完全な修正が必要です。ミティゲートされた資産や脆弱性はタグ付けされ、後で確認できます。ミティゲーションや修正が適用されると、該当資産や脆弱性のリスクは適切に低減されます。

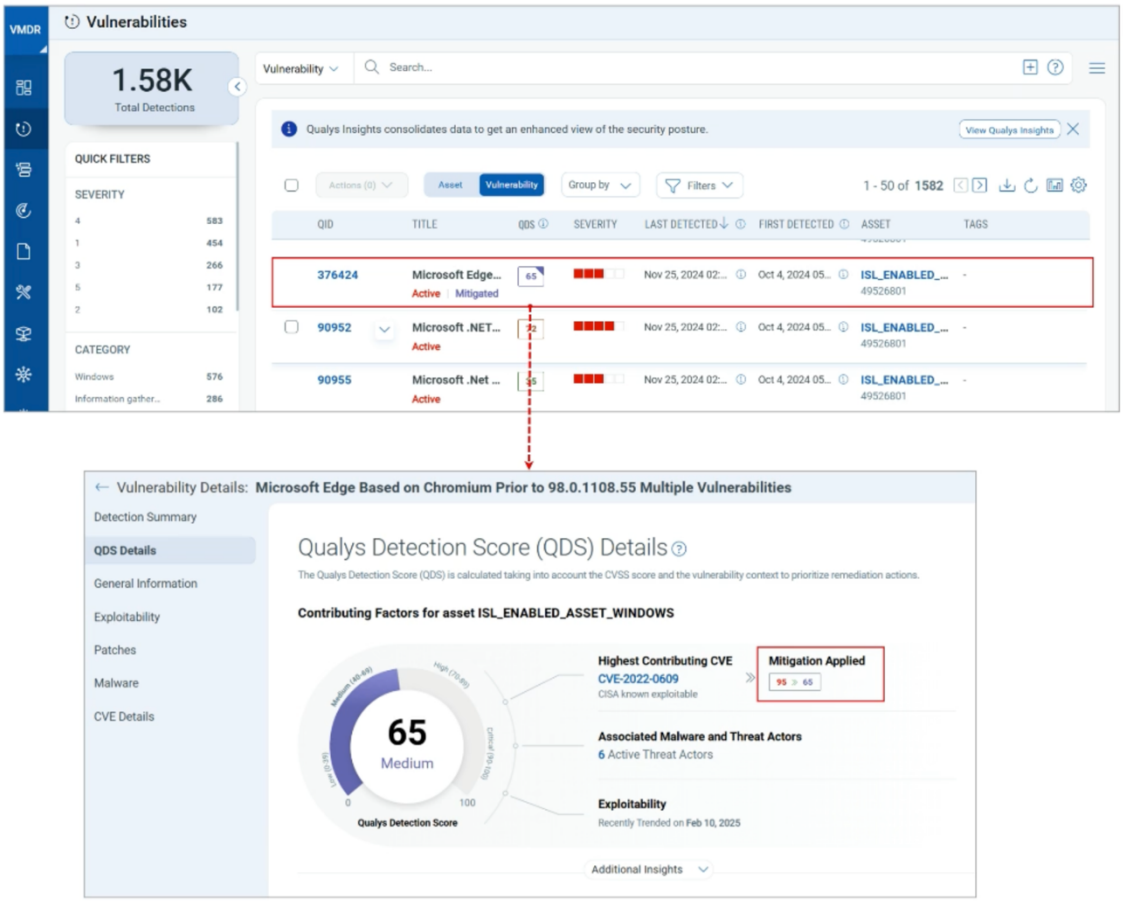
例えば、QID 92226 はパッチで修正するか、システムハードニングでミティゲートできます。システムハードニングオプションを選択すると、関連する CVE が表示されます。ここでは、レジストリ更新（デフォルト）または特定のネットワークプロトコルのブロックを選択できます。ネットワークプロトコルのブロックはリスクを 100%低減しますが、レジストリ更新は 90%低減します。選択したミティゲーションによって QDS スコアは異なる割合で調整されます。

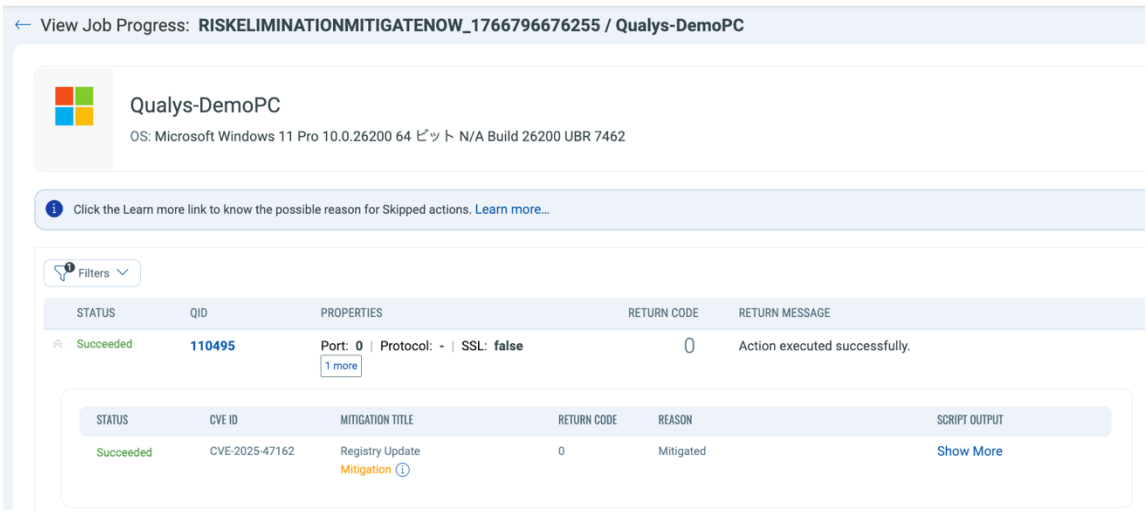


ミティゲーションジョブの設定では、ジョブタイトルや説明を入力し、資産やアクションを選択します。スケジュールはオンデマンド（次回クラウドエージェントのチェックイン時に実行）または指定日時で設定できます。通知設定や共同編集者の追加も可能です。設定を確認後、ジョブを保存して後で実行するか、すぐに有効化できます。



ジョブ実行後、QDS 値は適切に低減されます。例えば、QID 376424 はスコアが 95 から 65 に下がり、資産全体のリスクスコアも低減します。SQL トークン「**vulnerabilities.mitigated:true**」を使用すると、ミティゲート済みの脆弱性を一覧表示できます。





QID は、関連するすべての CVE がミティゲートされた場合にのみ「ミティゲート済み」となります。

QQL トークンを使えば、ミティゲート可能な脆弱性や状態（部分的・完全）、修正済みかどうか、ミティゲート方法（True Risk Mitigate、PC コントロール、資産隔離）を確認できます。

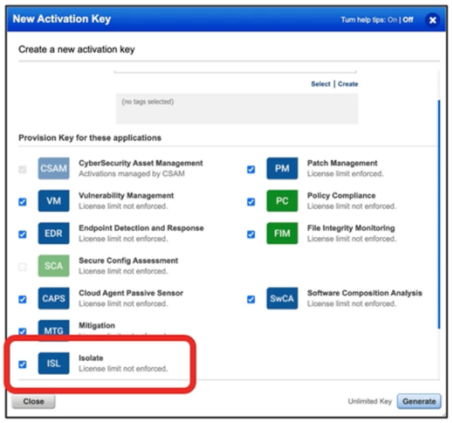
最後に、ミティゲーションのロールバックも可能です。ミティゲート済みの脆弱性を選択し、ロールバックジョブを作成すると、資産や脆弱性を元の設定に戻せます。これは、パッチ適用や代替コントロールが利用可能になった場合に有効です。

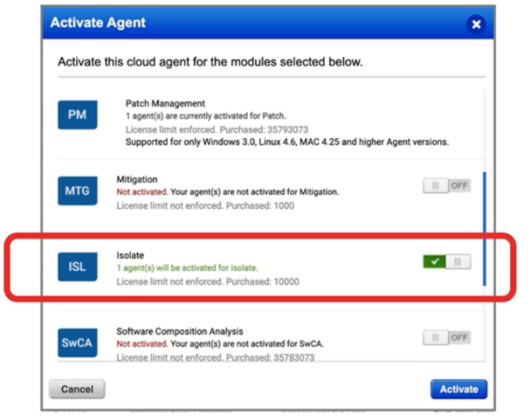
TruRisk Isolate

資産の隔離(isolation)は、脆弱性に対してパッチや緩和策を適用できない場合の**最後の手段**として実施します。隔離とは、資産をネットワークから切り離し、通信を遮断することです。クラウドエージェントによって適用されるため、クラウドエージェントを介した管理や通信は可能ですが、オペレーティングシステムからの通信は許可されません。パッチや緩和策が利用できない場合、隔離を有効化することで TrueRisk を活用できます。

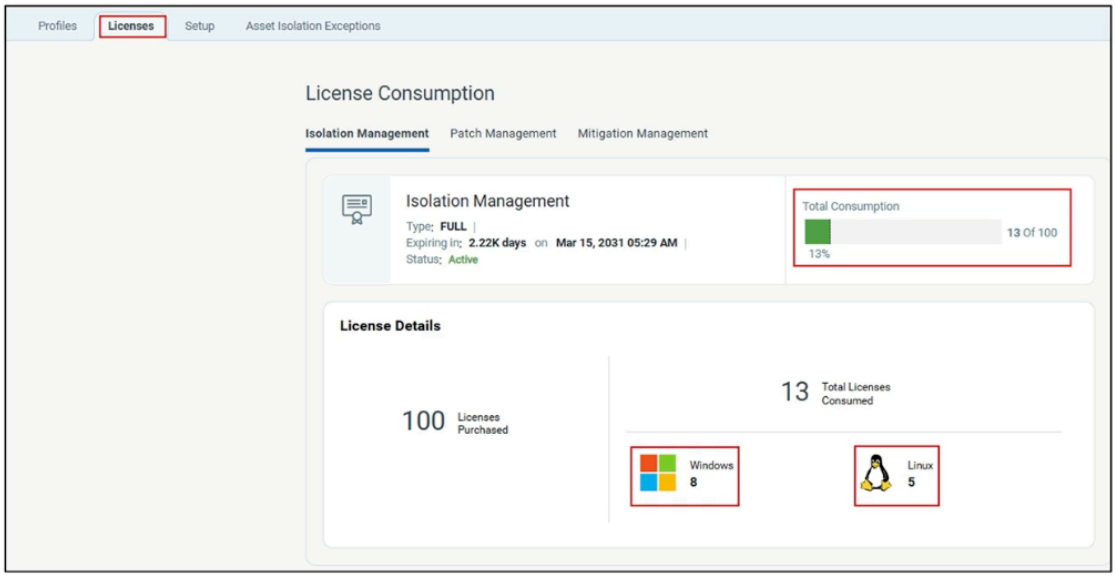
隔離の方法は主に 2 種類あります。1 つ目は、アクティベーションキーを使用する方法です。このキーを使えば、同じキーを持つすべてのホスト、または後から追加されるホストに隔離を適用できます。2 つ目は、個別のエージェントホストを選択し、モジュールの有効化オプションから隔離をオンにする方法で

す。隔離を利用するには、Windows では Qualys Cloud Agent バージョン 6.1.1 以降、Linux では 7.1.1 以降が必要です。



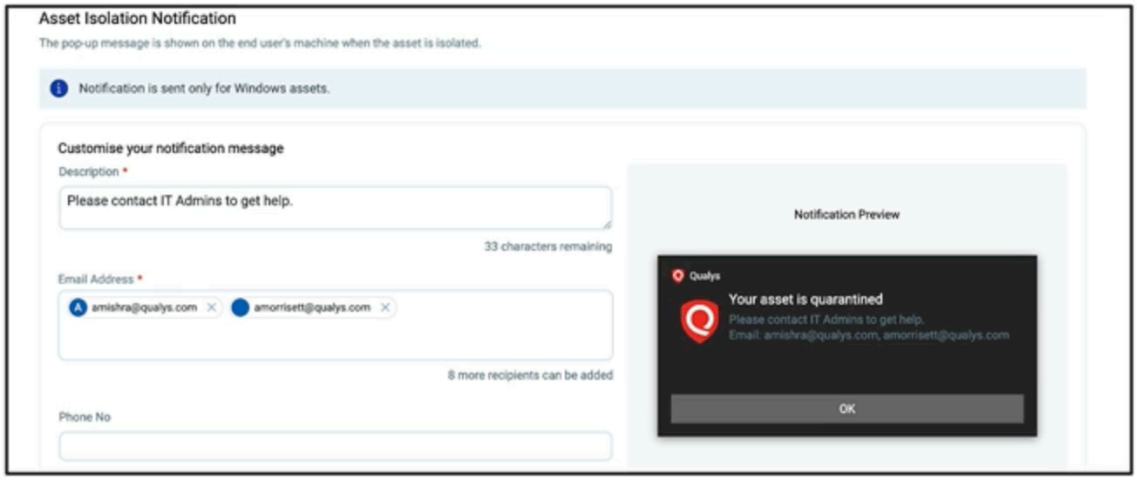


ライセンスの消費状況はライセンスタブで確認できます。購入済みライセンス数、隔離を使用している資産数、全体の消費レベルを確認でき、OS 別の内訳も表示されます。例えば、Windows で 8 件、Linux で 5 件というように確認できます。

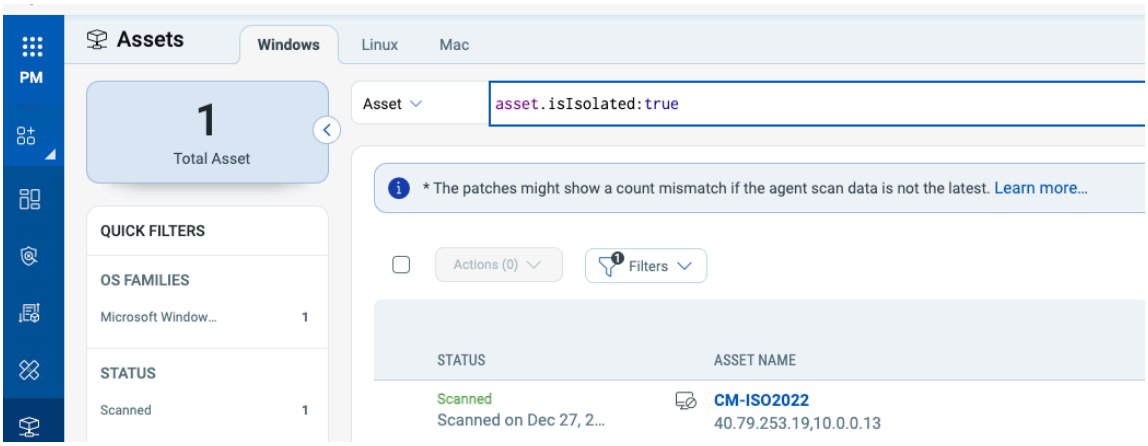


隔離を設定した後、例外を作成できます。例外は、隔離されたホストが特定のネットワークサービスやデバイスと通信できるようにするために重要です。例えば、ホスト内の特定アプリケーションを許可したり、特定のドメイン（例：updates.microsoft.com）への接続を許可したりできます。また、特

定の IP アドレスへの接続も許可できます。これにより、隔離された資産が必要なサービスにアクセスし、再統合の準備を進められます。
隔離通知ポップアップの外観やテキストも設定できます。隔離された端末のユーザーが情報を要求できるよう、メールアドレスを入力することも可能です。

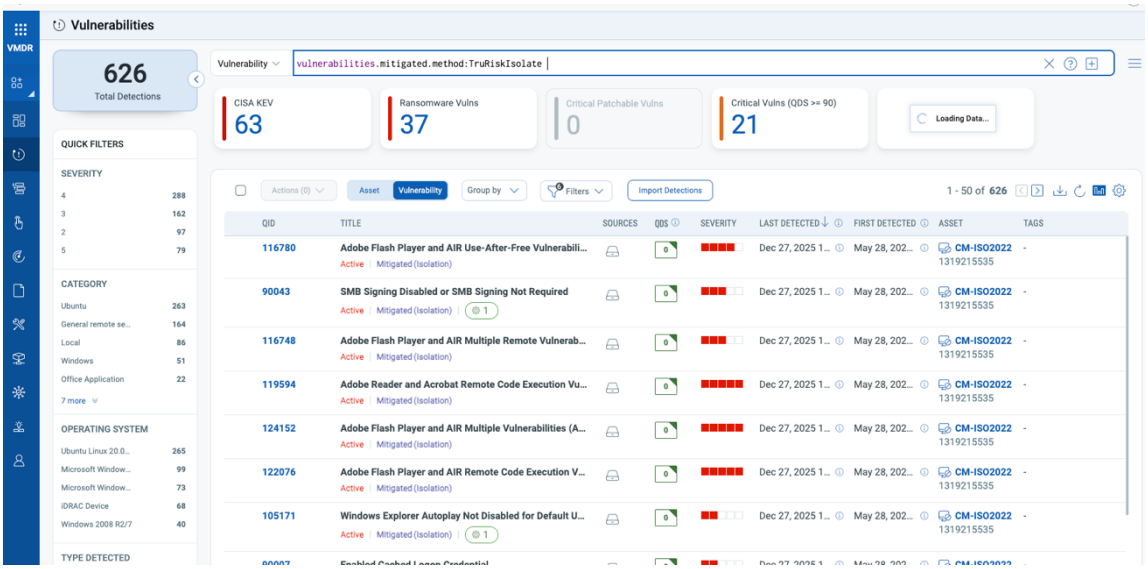


隔離ジョブの作成は、パッチ管理画面で脆弱性を選択し、アクションのドロップダウンから隔離を選択することで行います。脆弱性ごとに「今すぐ修正」から隔離を選択することもできます。
隔離後は、安全に脆弱性の修正作業を行い、ネットワークに再統合できます。再統合には隔離のロールバックジョブを使用します。**隔離された資産を検索するには**、QQL トークン「**isolated: true**」を使います。対象資産を選択し、アクションから「リスク排除の表示」を選択すると、隔離解除のオプションが表示されます。



隔離された脆弱性は、QQL トークン「**vulnerabilities.mitigated.method:TruRiskisolate**」で確認できます。この場合、

QDS スコアは 0 に減少し、脆弱性がネットワークに接続されていないため、実質的に存在しないと見なされます。再統合後、必要な修正が行われていなければ、スコアは再び上昇します。修正後に再スキャンを行うことで、スコアが適切に評価されます。



以上