



Global Asset View (GAV) から CyberSecurity Asset Management (CSAM) へのアップグレード

Global Asset View は VMDR をサポートし、既にスキャンしている社内資産を検出・管理します。

CyberSecurity Asset Management (CSAM) にアップグレードすると、以下のことが可能になります。

- ✓ 社内外の攻撃対象領域における盲点をすべて排除
- ✓ 脆弱性にとどまらず、あらゆるリスク要因を考慮
- ✓ IT/セキュリティツールとの統合により、サイバーセキュリティプログラムを運用可能に

資産の可視性

Global Asset View は、社内の攻撃対象領域のベースライン・ビューを提供します。CSAM にアップグレードすると、外部攻撃対象領域管理 (EASM)、クラウド・エージェント・パッシブ・センシング (CAPS)、サードパーティ製コネクタなど、市場で最も汎用性の高い検出ツールセットを活用できます。

特徴	VMDR/ GAV	CSAM
 内部攻撃対象領域を完全に可視化 複数の Qualys センサーを使用して、資産を継続的に検出し、インベントリを作成します。オンプレミスおよびクラウド環境のサーバー、デスクトップ、ネットワーク、モバイル、IoT に関する情報を表示します。	✓	✓
 EASM で外部資産を 38%多く発見 合併、買収、子会社化によってこれまで知られていなかった資産を特定し、VM プログラムに追加します。		✓
 ネットワーク上の管理されていないデバイスや信頼できないデバイスをリアルタイムで特定 クラウドエージェントを、IoT デバイスや不正デバイスなど、ネットワークに接続された資産を検出するパッシブセンサーに変換します。		✓
 サードパーティ製コネクタで死角を削減 ServiceNow、BMC Helix、Active Directory、Webhook などの資産を検出することで、セキュリティプログラムのカバー範囲とビジネスコンテキストを強化します。		✓

CMDB との同期

多くの組織は、IT 資産と依存関係に関する真実の記録として CMDB を活用しています。CSAM は、CMDB の盲点を減らし、リスクのコンテキストを追加することで、IT チームとセキュリティチームの優先順位を一致させ、MTTR を短縮します。

特徴	VMDR/ GAV	CSAM
 包括的な資産インベントリで CMDB を最新の状態に維持 社内外の資産を継続的に検出し、正確な CMDB を維持します。IT チームとセキュリティチームの連携を、信頼できる唯一の情報源で実現します。		✓
 EoL/EoS などのサイバーリスクのコンテキストを CMDB に追加 CMDB で EoL/EoS、不足しているセキュリティエージェント、期限切れの SSL 証明書を追跡し、IT チームとセキュリティチームのリスクの優先順位を一致させます。		✓
 96% の精度で改善チケットをマッピング Qualys タグを使用してルールを作成し、チケットの割り当てを自動化することで、改善にかかる時間を 60% 短縮します。		✓
 CMDB のビジネスコンテキストを活用して TruRisk スコアリングを強化 資産の重要度、スコープ (PCI など)、所有者、サポートグループなどのビジネスデータを追加することで、リスクの優先順位付けを強化できます。		✓

脆弱性を超えて、あらゆるリスク要因を特定

資産リストだけでは役に立ちません。CSAM と VMDR を組み合わせることで、資産のあらゆるリスク要因を把握し、数十万もの資産に対して正確な TruRisk スコアリングと優先順位付けを実現します。

特徴	VMDR/ GAV	CSAM
 技術負債 (EoL/EoS) を積極的に管理 EoL/EoS を迎えるソフトウェアおよびハードウェアを最大 12 ヶ月前までに特定します。 関連するリスクを IT リーダーに伝え、積極的にリスクを軽減します。		✓
 不足しているセキュリティ対策を自動的に特定 柔軟なポリシーに基づき、資産グループにおける IT/セキュリティエージェント (EDR やデータ損失防止など) の不足を監視します。		✓
 許可されていない危険なポートとサービスを特定 許可されていないソフトウェアを識別して削除し、外部に公開されている資産上の危険なポートを検出するためのルールを作成し、適用します。		✓

外部攻撃面のリスクを軽減

合併、買収、子会社化によって生じたすべての資産を特定し、それらを特定の事業領域に紐付け、脆弱性、設定ミス、その他多くのリスク要因を即座に検知します。業界をリードする脆弱性スキャンを検知後すぐに活用することで、外部リスクを正確かつ継続的に評価します。

特徴	VMDR/ GAV	CSAM
 インターネットに接続された資産を組織に確実に帰属させる ドメイン、WHOIS、その他さまざまなデータポイントに基づいて資産を検出し、帰属させます。 信頼性スコアリングを使用して、組織に本当に属するものを判別します。		✓
 軽量スキャンで脆弱性検出を向上 25以上の脅威情報源とシックスシグマの精度を活用した業界最先端のスキャンにより、外部資産の脆弱性と構成ミスを検出します。		✓
 外部資産の TruRisk を確認 資産の重要度、脅威インテリジェンスに基づく脆弱性スコア、リスクの高いポート、期限切れの証明書などを含む単一のスコアで、リスクを即座に優先順位付けできます。 多くの EASM ツールが生成する誤検知や無関係な脆弱性といったノイズを排除します。		✓

SecOps と ITOps 全体のワークフローを合理化

資産インベントリは、実用的な情報に基づいて初めて威力を発揮します。ワンクリックで、これまで不明だった資産を VM、Web アプリスキャン、パッチ適用ジョブに追加できます。IT および SecOps ツールとのすぐに利用可能な連携機能を活用し、経営幹部レベル向けのリスクレポートを作成できます。

特徴	VMDR/ GAV	CSAM
 CMDB および SIEM ソリューションとの統合 Splunk や IBM QRadar などの SIEM ソリューションとサイバーリスクデータを同期し、プロアクティブなアラートとイベント管理を実現します。組み込みのコネクタアプリで、ServiceNow または BMC Helix ソリューションを最新の状態に保ちます。		✓
 VMDR、WAS、Patch、その他 Enterprise TruRisk プラットフォームをワンクリックでワークフロー化 VMDR または WAS に追加し、Enterprise TruRisk プラットフォーム内でパッチジョブを展開することで、重要な資産や資産グループに対して即座に対応できます。		✓
 多様なステークホルダーに柔軟なレポート機能を提供し、リスクコミュニケーションを実現 CISO KPI とコンプライアンス要件に関するレポートをすぐに作成できます。 EoL/EoS や外部資産へのリスクといったリスク要因について、IT 部門に常に情報を提供します。		✓

Qualys について

Qualys, Inc. (NASDAQ: QLYS) は、Forbes Global 100 および Fortune 100 の大部分を含む、世界中に 10,000 社以上のサブスクリプション顧客を持つ、革新的なクラウドベースのセキュリティ、コンプライアンス、および IT ソリューションのパイオニアおよび大手プロバイダーです。 Qualys、Qualys VMDR®、および Qualys のロゴは Qualys, Inc. の商標または登録商標です。 その他すべての製品や名前は、それぞれの会社や組織の商標や登録商標である場合があります。

詳細については、[qualys.com](https://www.qualys.com) をご覧ください。