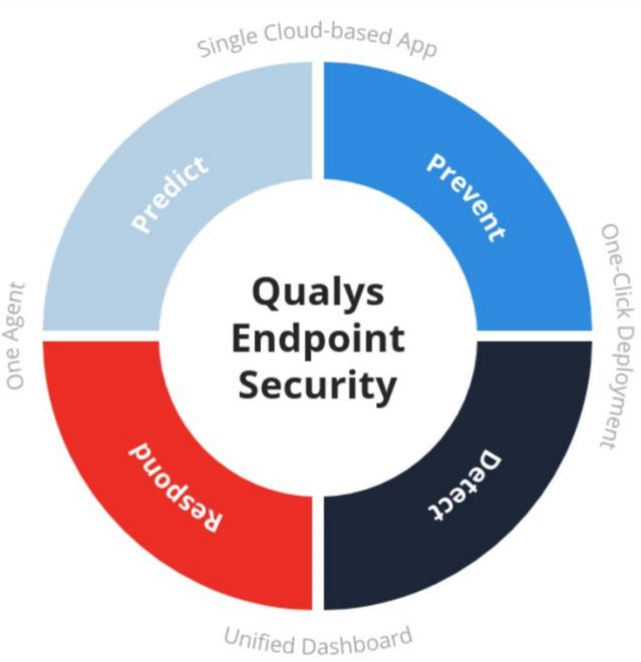
Qualys Endpoint Security

脆弱性管理とエンドポイントの脅威の検出と対応(Endpoint Detection&Response)を統合することで、侵害のリスクを軽減します。

Qualys Endpoint Security は、業界で最も包括的な振る舞い検出、脅威インテリジェンス、機械学習モデルを利用して、既知および未知の脅威から企業を保護します。

Qualys プラットフォームにより、Qualys Endpoint Security は、アセットの重要度、脆弱性、脅威に関連するシステムの設定ミスなど、複数のコンテキストベクトルを統合する業界唯一のソリューションです。



また、平均修復時間 (MTTR) を短縮する重要な部分として、公開されているすべてのアセットにパッチを適用することを推奨する唯一のソリューションでもあります。MITRE ATT&CK Tactics and Techniques とリアルタイムのエンドポイントテレメトリを組み合わせてサイバー脅威を評価することで、比類のない脅威分析と自動化された脅威対応を提供します。

さらに良いことに、単一の軽量エージェント、クラウド配信、統合ダッシュボードなど、導入が容易で、使いやすく、管理が簡単です。Qualys Cloud Platform とともに Qualys Endpoint Security に投資することで、サイバーセキュリティ ツール スタックを統合しながら、エンドポイントで高度な脅威保護を実現することができます。

主な機能

クローズドループの脅威への対応

攻撃の症状に対処するだけでなく、発生源で阻止します。 Qualys Endpoint Security は、Qualys の脆弱性との緊密な統合と、TruRisk プラットフォームによるパッチ管理を提供し、防御者がアクティブな脅威を阻止するだけでなく、マルウェア インシデント、CVE、パッチを自動的に関連付けて将来の攻撃を防止できるようにします。

マルチベクトル保護

Qualys Endpoint Security は、次のような独自のマルチベクトル アプローチにより、マルウェアやその他の形式の攻撃からシステムを保護します。

- 成熟し十分にトレーニングされた機械学習モデル により、悪意のあるバイナリをブロックします。
- 2000+以上の振る舞いルールがユーザーとエンドポイントのアクティビティを監視し、悪意のある振る舞いからリアルタイムで保護します。
- メモリや脆弱なアプリケーション(ブラウザ、ドキュメントリーダー、メディアファイル、ランタイムなど)を利用する攻撃をブロックするエクスプロイト対策。
- フィッシングサイトやマルウェアホスティングサイトへのアクセスをブロックするフィッシング対策技術。
    - ネットワークの振る舞いをリアルタイムで分析し、マルウェアの活動を正確に発見するネットワーク型攻撃防御。
    - デバイスとアプリケーションの制御により、詳細なコンテキスト環境をきめ細かく制御

Qualys TruRisk プラットフォームは、アセットの重要度、攻撃の戦術や手法への露出、悪用可能性に関する情報など、防御者が重要な意思決定を行うために必要な重要な情報を提供します。このコンテキストを、リアルタイムのエンドポイント、ネットワーク、Web テレメトリなどの幅広いセットと組み合わせることで、セキュリティチームは脅威を理解して優先順位を付け、断固とした行動をとるために必要なデータを得ることができます。

Endpoint Detection and Response

Qualys Endpoint Security は、エンドポイントをリアルタイムで監視し、不審なアクティビティの検出、脅威ハンティング、自動応答のワークフローを実現します。

- **インシデント管理** - 自動インシデントの優先順位付け、可視化、根本原因分析により、セキュリティ管理者は最も重要な脅威に集中できます。
- **脅威ハンティング** - セキュリティ管理者は、ネットワーク内のイベントをプロアクティブに検査して、疑わしいアクティビティを見つけることができます。
- リスクのしきい値と対応を定義するためのすぐに使用できる**自動化オプション**により、手動調査から自動修復に移行できます。
- 高度で徹底的な調査のための **脅威フォレンジックとリモートシェル**

メリット

侵害リスクの軽減

より多くの脅威を最も早い段階で防止し、インシデント対応者が迅速に行動できるようにします。

- 脆弱性の修復を優先することで、セキュリティチームはより多くの攻撃をより早く予測し、防止することができます。
- エンドポイント、メール、Web などにわたるマルチベクトルの保護と可視性により、防御者は攻撃を迅速に理解し、より迅速で完全な対応を促進することができます。

アラート疲れの解消

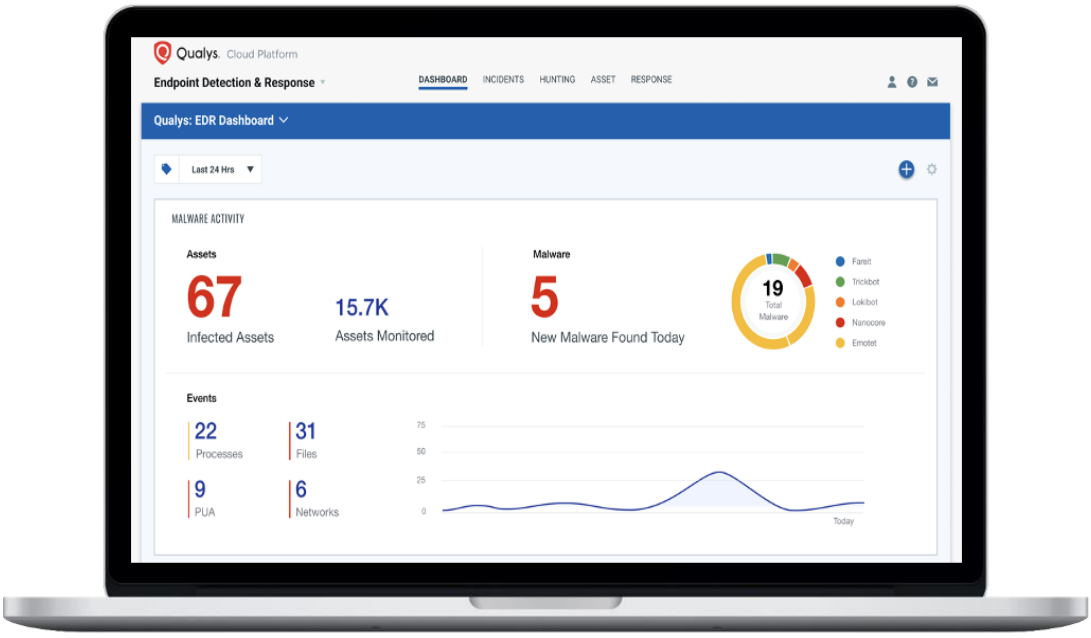
攻撃サイクルの早い段階でより多くの脅威を阻止することは、アラートの量を減らし、より迅速で強力な調査を可能にすることで、セキュリティチームが追跡するアラートを減らすことを意味します。

- 優先順位付けの自動化により、防御側は常に最も重要な脅威に最初に対応できます。
- 詳細なコンテキストは、セキュリティチームが企業全体の攻撃ストーリー全体をすばやく理解するのに役立ちます。

時間とコストの節約

Qualys のシンプルで安価なプラットフォームは、数分で組織の境界を打ち破ります。

- 防御側は、コンソールホッピングや異種ソリューションの管理/保守に費やす時間を短縮できます。
- Qualys の革新的な TruRisk クラウドプラットフォームにより、制限や摩擦のない成長が可能になります。
- 手間のかからないトライアル – Qualys Endpoint Security は、追加のエージェントやインフラストラクチャを導入することなく、ワンクリックで有効にできます。



Qualys Cloud Platform を搭載

– 動力源となる革新的なアーキテクチャ

Qualys の IT セキュリティおよびコンプライアンスクラウドアプリ

継続的な可視性を提供するセンサー

オンプレミス、エンドポイント、クラウドのいずれでも、Qualys Cloud Platform センサーは常にオンになっているため、すべての IT アセットを 2 秒間継続的に可視化できます。リモートで展開でき、一元管理され、自己更新可能なセンサーは、物理アプライアンスまたは仮想アプライアンス、または軽量エージェントとして提供されます。

すべてのデータをリアルタイムで分析

Qualys Cloud Platform はエンドツーエンドのソリューションを提供し、複数のセキュリティベンダーの管理に伴うコストと複雑さを回避できます。Qualys Cloud Platform は、スケーラブルで最先端のバックエンドでセキュリティとコンプライアンスのデータを自動的に収集して分析し、追加のクラウド アプリのプロビジョニングはチェックボックスをオンにするのと同じくらい簡単です。

脅威に即座に対応

Qualys Cloud Agent テクノロジーを使用すると、スキャン ウィンドウをスケジュールしたり、スキャン用の資格情報を管理したりする必要はありません。また、Qualys Continuous Monitoring サービスでは、新しい脆弱性が発生するたびに潜在的な脅威にプロアクティブに対処し、リアルタイムのアラートで即座に通知できます。

結果を 1 か所で、いつでも、どこでも確認

Qualys Cloud Platform はブラウザから直接アクセスでき、プラグインは必要ありません。すべてのアプリで直感的に操作できる 1 つの画面のユーザー インターフェイスにより、ダッシュボードのカスタマイズ、詳細のドリルダウン、チームメイトや監査人向けのレポートの生成を行うことができます。