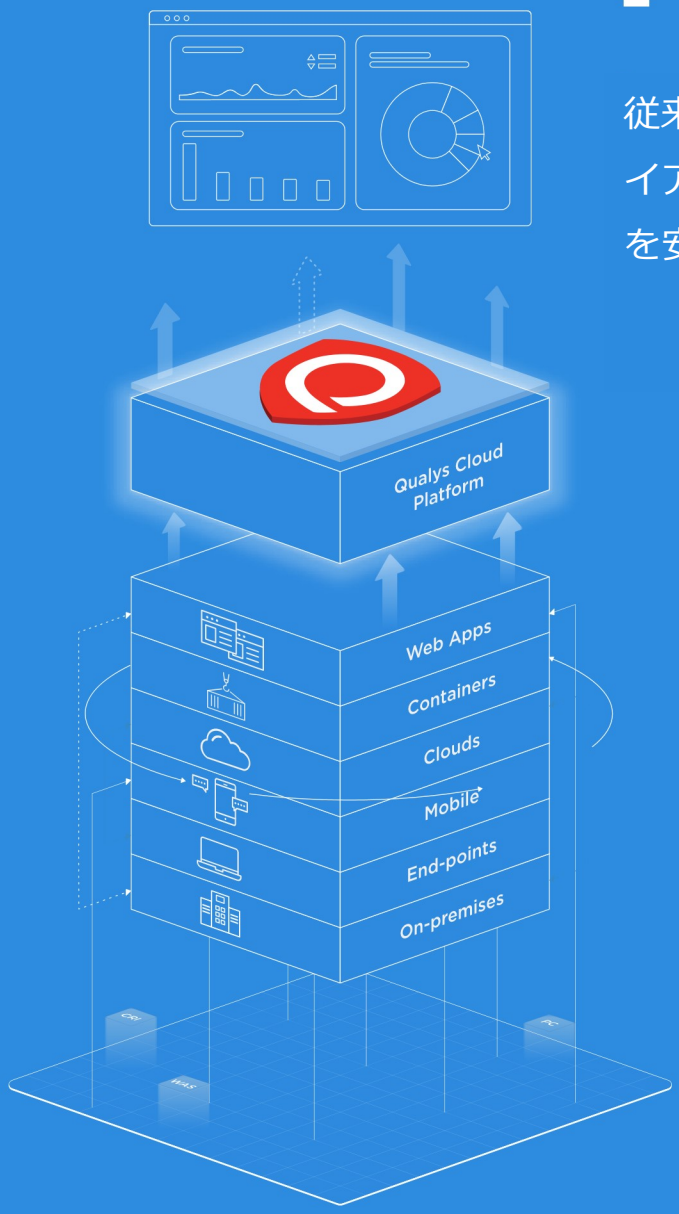
Qualys

Qualys Cloud Platform

従来のエンタープライズセキュリティとコンプライアンスソリューションを統合し、デジタル変革を安全に行う 1 つのスタック



目次

はじめに

組織がビジネスプロセスのデジタル変革を推進し、俊敏性と効率性を高める中で、IT 環境は分散化、柔軟性、ハイブリッド化が進み、セキュリティチームにとって課題となっています。CISO（最高情報セキュリティ責任者）は、従来のセキュリティ製品では対応しきれず、従来の明確に定義された企業境界（ほとんどの資産がオンプレミス）を保護することはもはや困難です。

クラウド、モビリティ、仮想化、その他のイノベーションの導入により、IT インフラストラクチャの境界は押し広げられ、曖昧になり、消滅さえしています。こうした新たな不定形な IT 環境の可視性と制御を取り戻すため、CISO はしばしば異機種混在のポイントツールを積み重ねるという非効率的で逆効果なアプローチに頼ります。

多数の異なるセキュリティ製品を統合、管理、拡張することは困難であるため、この戦略は運用のサイロ化、コストの増加、データの断片化につながります。さらに悪いことに、現代の IT のスピード、オープン性、相互接続性によって生み出される攻撃ベクトルを悪用する、機会を狙ったハッカーの脅威に組織がさらされることになります。

むしろ、セキュリティはデジタルトランスフォーメーションプロジェクトに透過的に組み込む必要があります。そのためには、予防、検知、対応のための統合セキュリティ・コンプライアンスプラットフォームが必要です。

Qualys は、この変化を何年も前から予見していました。先駆的なビジョンに基づき、Qualys はデジタル時代の攻撃対象領域の拡大という課題に対応するための統合クラウドプラットフォームを構築してきました。

ORACLE

「Qualys は、当社のネットワークが安全であり、当社システムだけでなく顧客のシステムも強化されていることを保証するのに役立ちます。」

Qualys を利用することで、組織は従来のようにセキュリティを唐突に追加するのではなく、ハイブリッド IT インフラストラクチャにネイティブかつ有機的にセキュリティを組み込むことができます。

これには、DevOps パイプラインへのセキュリティの組み込みと自動化が含まれます。DevOps パイプラインは、継続的かつ迅速なコード開発とデリバリーによってデジタルトランスフォーメーションプロジェクトを推進します。セキュリティが孤立したまま、ソフトウェアの導入前に詰め込まれると、DevOps の継続的な開発とデリバリーが遅れ、デジタルトランスフォーメーションのメリットが失われてしまいます。つまり、Qualys クラウドプラットフォームは、オンプレミス、クラウド、リモートエンドポイントなど、あらゆる IT 資産を瞬時に可視化し、組織のセキュリティとコンプライアンスの状況を継続的に評価することで、継続的な監視と対応を実現します。

IDC のセキュリティ製品担当リサーチディレクターである Robert Ayoub 氏は最近次のように述べています。「Qualys クラウドプラットフォームは、複数のセキュリティソリューションの管理に伴う複雑さを簡素化すると同時に、セキュリティの自動化、有効性、そしてプロアクティブな性質を高めます。」当社のプラットフォームが、多用途のセンサー、バックエンド分析エンジン、統合されたアプリスイートを通じて、セキュリティとコンプライアンスのタスクを統合および自動化し、ハイブリッド IT 環境を保護する方法について、以下をお読みください。

Part I

今日の IT 環境：ボーダーレス、分散型、弾力性

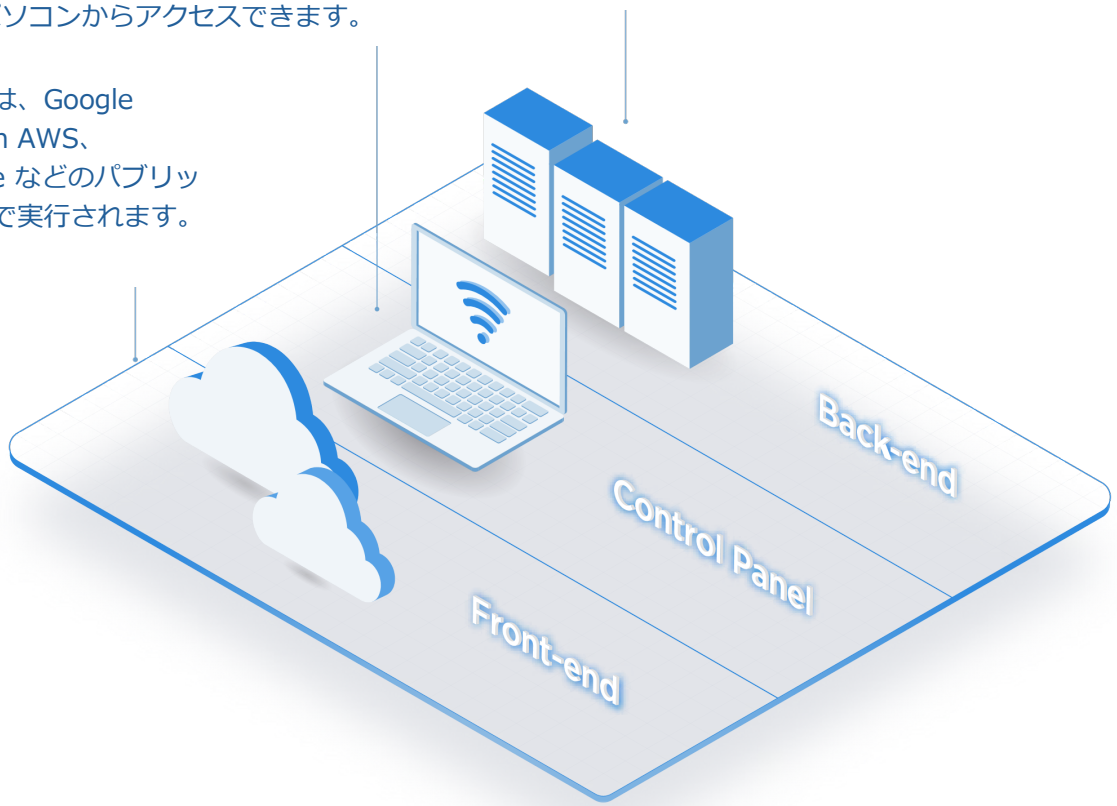
ハイブリッド IT：セキュリティ課題のスナップショット

クラウド コンピューティング、モビリティ、その他の IT イノベーションが IT 部門にもたらした新たな情報セキュリティの課題は、小売業者の決済アプリという架空の、しかし非常に一般的なシナリオによく表れています。

アプリのコントロールパネルには、ホテルのロビーに座っている管理者が、公衆 Wi-Fi ネットワークに接続されたノートパソコンからアクセスできます。

アプリのバックエンド プロセスはオンプレミスのデータ センターで実行されます。

フロントエンドは、Google Cloud、Amazon AWS、Microsoft Azure などのパブリッククラウド環境で実行されます。



このアプリケーションに対するリスクは、これら 3 つの異なる場所に存在します。エンドポイントのみ、クラウドインスタンスのみ、オンプレミスサーバーのみを保護するセキュリティ製品では不十分です。異機種混在の製品を統合してより包括的なソリューションを構築しようとすると、統合の複雑さ、コストの増加、そしておそらくパフォーマンスの低下を招きます。

IT 環境の新たな境界

ペリメーター（境界）は以前は企業の敷地内に限定されていましたが、現在ではクラウド、モバイルデバイス、ウェブアプリ、IoT センサー、さらにはコンピューティング以外の領域にも広がっています。

モバイルデバイス、非コンピューティング機器、IoT システム

境界は、従業員が公共および自宅の Wi-Fi ネットワークに接続するあらゆるデバイス（ノートパソコン、スマートフォン、タブレット、スマートウォッチなど）にまで及びます。これらのデジタルデバイスには、重要な機密データやアプリケーションが含まれており、紛失、盗難、不正アクセスの被害に遭うケースも少なくありません。
もう一つの弱点は、リモートオフィスや小売店など、地理的に分散した組織の拠点です。PC、POS システム、その他のエンドポイントが設置されているこれらの施設は、大規模な企業ビルに比べて物理的セキュリティとサイバーセキュリティが脆弱な場合が多くあります。
一方、コピー機、プリンター、サーモスタット、さらにはオフィスのキッチンにある Wi-Fi 対応コーヒーメーカーなど、コンピューティング以外のデバイスもネットワークに接続しています。
企業は IoT を積極的に導入し、車両、空調システム、医療機器、産業機器、店舗の棚など、以前はオフラインだった無数の「モノ」にセンサーを組み込んでいます。これらの多様で分散したエンドポイントは、膨大な機密データを収集し、組織の IT システムに送信しています。
そのため、多くの組織では、標準的なコンピューティング デバイスよりもサイバー攻撃に対して脆弱である傾向があるため、モバイル エンドポイントや非従来型エンドポイントのセキュリティとコンプライアンスを監視および強化できるツールを備えることが不可欠です。

クラウドコンピューティングサービス

クラウドコンピューティング・プラットフォームとインフラストラクチャ・サービス（PaaS と IaaS）の導入は、世界中の組織で増加し続けています。情報セキュリティチームは、オンプレミス・システムからパブリッククラウドに移行するこれらのワークつまり、プロバイダーはクラウド・プラットフォームを保護し、顧客はデータとソフトウェアのセキュリティ確保に責任を負います。そのため、顧客はオンプレミス・システムと同様に、パブリッククラウド環境でも脆弱性管理、Web アプリケーション・スキャン、ポリシー遵守などを含むセキュリティとコンプライアンスのチェックを実施する必要があります。そのためには、パブリッククラウドのワークロードとインスタンスを可視化できるセキュリティ・ツールが必要です。

Web アプリと Dev(Sec)Ops パイプライン

組織が業務をデジタル変革する中で、これらのイノベーションは主に Web アプリを通じて実現されます。インターネット接続型、社内向け、クラウドホスト型の Web アプリ、そして REST API ベースの Web サービスなどです。これらの Web アプリを活用することで、組織は従業員、顧客、そしてパートナーにとって重要な機能とプロセスを簡素化・自動化できます。しかしながら、多くの Web アプリケーションは潜在的な脆弱性や脆弱な構成のために安全ではありません。当然のことながら、Web アプリケーションはデータ侵害の格好の標的となっています。
ウェブアプリの堅牢化において重要な要素は、ソフトウェアコードが迅速かつ継続的に構築・デプロイされる DevOps パイプライン全体にセキュリティチェックを統合することです。セキュリティが組み込まれると、このプロセスは DevSecOps パイプラインとなり、「ビルド」から「本番」段階まで、あらゆる段階で脆弱性や設定ミスが自動的に検出・修正されます。これにより、セキュリティ対策が最終段階で導入されることがなくなり、デジタルトランスフォーメーションを推進するコードの CI/CD（継続的デリバリー/インテグレーション）が遅延することがなくなります。

この広範囲にわたる環境をどのように監視し、保護できるでしょうか?

現代の IT 環境を守るには、すべての IT 資産とその脆弱性や設定ミスを一元的に把握できる、統合型で一元管理されたクラウドベースのプラットフォームが必要です。データを細分化し、グラフやレポートで視覚化し、分析して複数の関係者と共有できる必要があります。

個々の製品を寄せ集めて、脅威の状況を包括的に把握できるシステムを構築することも可能です。しかし、それは複雑でコストがかかり、効果も低いでしょう。幸いなことに、そのようなソリューションは既に存在します。それが Qualys クラウドプラットフォームです。

Qualys は、セキュリティの状況を可視化し、経営陣に報告する手段として活用されています。このレポートは、eBay のセキュリティリスクを簡潔かつリアルタイムに経営陣に提供し、セキュリティ対策の実施に伴うリスクの変化を測定できます。

Senior Manager,
Information Security

Part II

Qualys Cloud Platform

他社ができないことを、私たちはどうすれば実現できるでしょうか？そのすべては、Qualysのクラウドベースのプラットフォームにあります。クラウド、オンプレミス、モバイル/リモートエンドポイントなど、あらゆる場所にあるあらゆる資産のセキュリティ、IT、コンプライアンスデータを継続的に収集、評価、相関分析します。Qualysクラウドプラットフォームは、包括的なエンドツーエンドのセキュリティソリューションであり、お客様に脅威状況をリアルタイムかつ包括的に把握し、包括的な攻撃防御と迅速なインシデント対応を実現します。

Introduction

Qualys クラウドプラットフォームの概要

Qualys クラウドプラットフォームは、セキュリティの簡素化を目指して設計されています。摩擦をなくし、可能な限り直感的で自動化されたセキュリティを実現することがその目標です。
Qualys はこれを「透過的なオーケストレーション™」と呼んでいます。これはセキュリティの未来を象徴する原則であり、Qualys の重要な指針と目標となっています。
透過的なオーケストレーションは、Qualys クラウドプラットフォームの設計、特にその 3 つの主要な柱である、多用途センサー、非常にスケーラブルなバックエンド、そして統合されたクラウドアプリスイートに反映されています。
Qualys クラウドプラットフォームは、常時稼働センサーを搭載しており、オンプレミス、エンドポイント、クラウドなど、あらゆる IT 資産の継続的なリアルタイム可視化を組織に提供し、包括的な予防、検知、対応を実現します。一元管理され、自己更新機能を備えた Qualys センサーは、物理アプライアンス、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。
一方、Qualys クラウドアプリは、以下の担当者を含む、すべてのセキュリティチームにツールと機能を提供します。

- オンプレミス インフラストラクチャ
- クラウド ワークロード
- エンドポイント デバイス
- DevSecOps 環境
- Web アプリ
- IT 監査とコンプライアンス

一元管理され、自動更新される Qualys クラウドアプリにセキュリティスタックを統合することで、チーム間の連携を維持できます。また、相互運用性が低く、統合が難しく、管理コストもかかる、サイロ化された異機種混在のポイント製品群を大量に抱える必要もありません。

Qualys クラウドプラットフォームの最先端の拡張性に優れたバックエンドは、レポート作成、ストレージ、データ分析、検索インデックス作成、資産タグ付けなど、堅牢で集中化された機能を備えています。一元化された Web ベースの UI により、IT 環境とそのセキュリティおよびコンプライアンス体制を包括的かつ継続的に更新できます。
Qualys は、データセンター内で Qualys クラウドプラットフォームのすべてのメリットを実現するプライベートプラットフォームも提供しています。Qualys プライベートクラウドプラットフォームを利用することで、組織はスキャンデータをローカルに保存し、社内ポリシーや外部規制へのコンプライアンスを確保できます。
このクラウド アーキテクチャにより、Qualys クラウド プラットフォームは、デジタル トランスフォーメーション プロジェクトが構築および展開される DevOps パイプラインを含む、今日のハイブリッド IT 環境を保護するために独自に設計されています。

1+ trillion
セキュリティイベント

3+ billion
1 年間の IP スキャン数・監査数

28+ billion
Elasticsearch クラスター上のデータポイントインデックス

99.999%
シックスシグマのスキャン精度

デジタルトランスフォーメーションの取り組みを安全に守る理想的なアーキテクチャ

1999 年の創業以来、クラウドベースのセキュリティとコンプライアンスのパイオニアである Qualys は、組織の急速なデジタルトランスフォーメーション展開を遅延させることなく保護する独自の立場にあります。

デジタルトランスフォーメーションの取り組みにセキュリティを組み込むには、DevOps ソフトウェア開発およびデリバリーパイプラインに情報セキュリティのプロセスとツールを組み込む必要があります。その理由は、DevOps チームが開発するモバイルアプリ、Web アプリ、そして Web サービスは、新しいデジタルトランスフォーメーション・イニシアチブの媒体となるからです。

Qualys は、開発者と運用スタッフが自動化されたセキュリティツールを利用できるよう支援し、ソフトウェアライフサイクルの早い段階で頻繁にコードをスキャンして、脆弱性、構成ミス、その他のセキュリティ問題を検出できるようにします。

DevOps にセキュリティを組み込む（DevSecOps にする）ことで、コードがよりクリーンになり、結果として得られるシステムのセキュリティが向上します。このアプローチは、IT チームと開発者チームのセキュリティに対する信頼を高め、組織がデジタルトランスフォーメーションを安全に加速するのに役立ちます。

最近のレポートで、451 リサーチのシニアアナリスト、スコット・クロフォードは次のように指摘しました。「Qualys の先見性のあるクラウド戦略は、ハイブリッドエンタープライズへのサービス提供において優位性を築いています。同社は長年にわたり、今日では「レガシー」IT とみなされるものもカバーしてきましたが、そのクラウドのルーツは、未来の IT に取り組むための戦略にも活かされています。」

クロフォード氏によると、「企業がデジタル変革を通じてより機敏で革新的かつ効果的になることを目指す中で、従来のセキュリティアプローチは、こうした新しい技術が依存する自動化、統合、スピードの足かせになる可能性がある」という。「したがって、これらの新しいアプローチに固有の機能は、次世代のセキュリティ技術の特徴となる必要があります。

Qualys の SaaS プラットフォームは、この機会に同社がもたらす唯一の資産ではありません。クラウド向けの開発における同社の経験は、組織が将来を見据えたセキュリティツールに何を求めているかを的確に把握しています。」

デジタルトランスフォーメーションは企業によるパブリッククラウドサービスの利用と密接に結びついているため、Qualys が組織の IaaS および PaaS 展開の保護にどのように役立つかを強調することが重要です。

組織がパブリッククラウドプラットフォームの利用を増やすにつれて、セキュリティとコンプライアンスの脅威、そして次のようなクラウド固有の課題に直面するようになります。

- クラウド資産、使用状況、リソースの可視性の欠如
- クラウドプロバイダーのセキュリティ責任共有モデルに関する誤解

つまり、組織はクラウドワークロードのインベントリを継続的に更新し、それらに対して重要なセキュリティとコンプライアンスのチェックを実行する必要があります。

Qualys は、AWS、Azure、Google Cloud などのパブリッククラウドプラットフォーム向けのネイティブ統合と包括的なセキュリティおよびコンプライアンスソリューションを提供し、以下を支援します。

- すべてのクラウドワークロードとリソースの脆弱性を特定、分類、監視します。
- 社内および社外のポリシーに準拠します。
- 脆弱性の修復を優先します。
- ウェブサイト上のマルウェア感染を自動的に検出し、駆除します。
- DevOps パイプライン全体にセキュリティとコンプライアンスを統合し、自動化します。

Qualys クラウド プラットフォームは、組織にデジタル トランスフォーメーション セキュリティの 5 つの主要な柱を提供します。

Visibility - 完全かつ継続的に更新される IT 資産インベントリをコンパイルし、オンプレミス、クラウド、リモートエンドポイントでの変更を即座に検出します。

Accuracy - すべてのセキュリティおよびコンプライアンスデータを一元的に収集、保存、分析し、サイロ化された断片化されたポイント ソリューションからの不完全な情報を排除します。

Scale - 非常にスケーラブルなクラウド アーキテクチャにより、最大規模のグローバル ハイブリッド IT 環境を保護します。

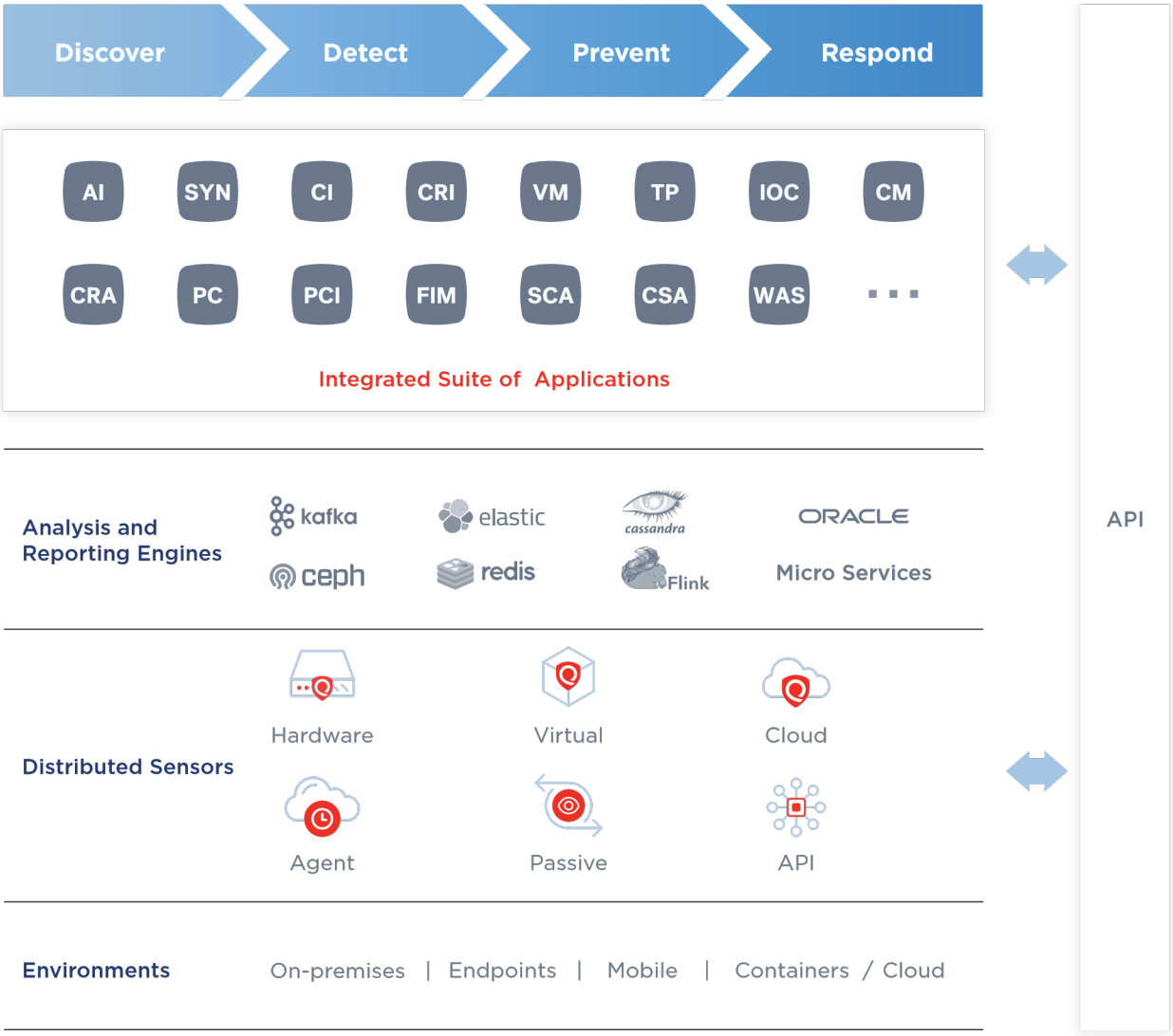
Immediacy - 堅牢なバックエンド エンジンにより、即時の予防機能とインシデント対応が実現します。

Transparent Orchestration (™) - IT 環境全体にシームレスで動的な自動セキュリティをプロビジョニングし、開発者や IT スタッフにとってスムーズで直感的なセキュリティを実現します。

How it operates

Qualys クラウドプラットフォームは、仮想化とクラウドテクノロジーを活用した堅牢でモジュール化された、拡張性と柔軟性に優れたインフラストラクチャ上に構築されており、オンデマンドで容量を割り当てることができます。

Qualys クラウドプラットフォームの実際の動作を詳しく見てみましょう。

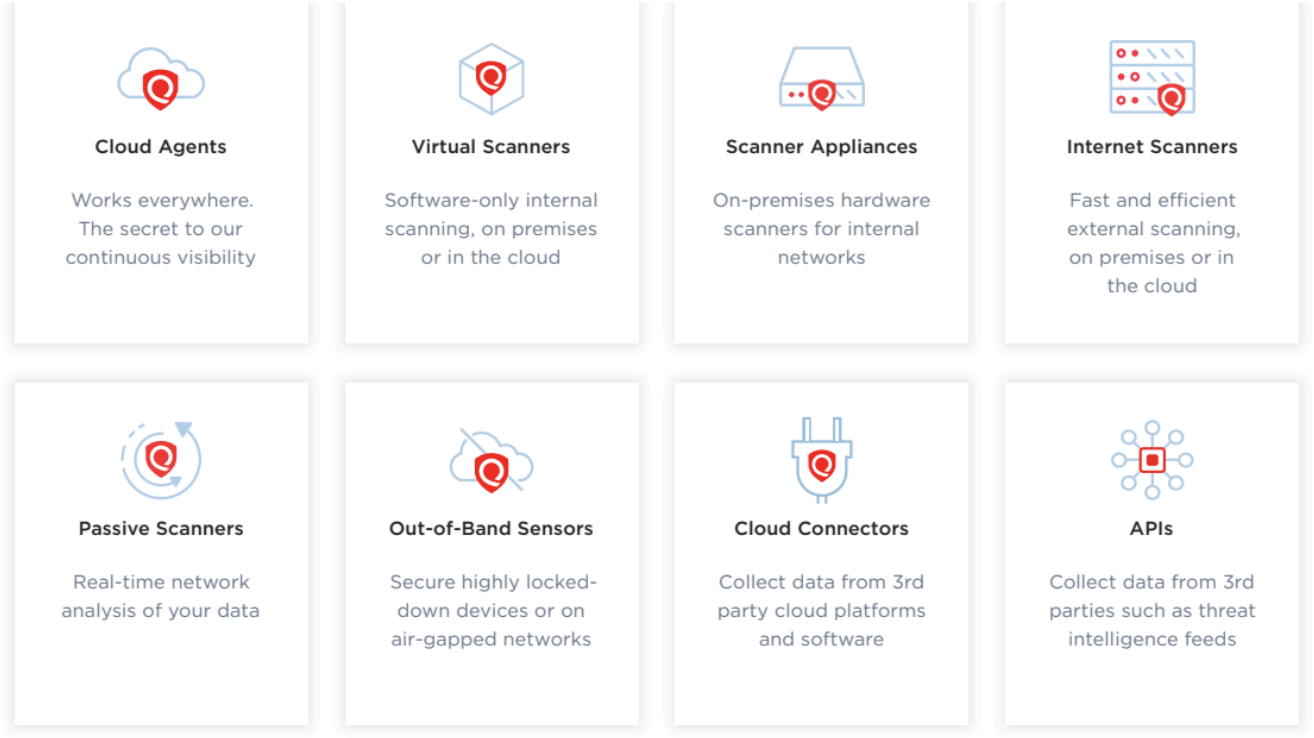


多用途センサーセット

Qualys クラウドプラットフォームのセンサーは、物理アプライアンス、仮想アプライアンス、軽量エージェントとして利用可能で、常時稼働、リモート導入可能、一元管理、自動更新機能を備えています。これにより、今日のハイブリッド IT 環境のあらゆる領域において、真の分散スキャンと監視が可能になります。

- インターネットから
- DMZ 内
- 社内ネットワーク上
- パブリッククラウドプロバイダーがホストするネットワーク上

Qualys センサーは IT 環境からデータを収集し、それを Qualys クラウド プラットフォームに自動的に送信します。Qualys クラウド プラットフォームは継続的に情報を分析して相関関係を関連付け、脅威を迅速かつ正確に特定して排除するのに役立ちます。



Qualys アプライアンス

Qualys は、さまざまなタイプのスキャナー アプライアンスを提供しています。

- オンプレミスの IT 資産をスキャンする物理アプライアンス
- プライベートクラウドおよび仮想化環境をリモートでスキャンする仮想アプライアンス
- 高速かつ効率的な外部スキャンを実現するインターネットアプライアンス
- 商用パブリッククラウドプラットフォーム上のインフラストラクチャ・アズ・ア・サービス（IaaS）およびプラットフォーム・アズ・ア・サービス（PaaS）インスタンスをリモートでスキャンするクラウドアプライアンス

アプライアンスは、使いやすいインターフェースを介して構成され、Qualys Web インターフェースを介してオンラインでアクティブ化されます。

パッシブネットワークセンサー

パッシブネットワークセンサー（PNS）は、ネットワークに接続されたすべてのシステムとそのアクティビティを、継続的かつ目立たずにリアルタイムで検出します。

PNS を利用することで、お客様は以下のことが可能になります。

死角をなくす: Qualys クラウドプラットフォームは、PNS、Qualys スキャナー、Qualys クラウドエージェントから資産テレメトリを集約し、ハイブリッドインフラストラクチャ全体のあらゆる IT 資産の包括的かつ詳細な多次元インベントリを提供します。これには、従業員所有のスマートフォンや不正デバイスなどの管理対象外デバイスも含まれます。PNS はまた、産業機器、IoT システム、医療機器など、クラウドエージェントでは積極的にスキャンや監視ができない資産も検出し、プロファイリングします。

不審なトラフィックを特定する: PNS はディープ・パケット・インスペクションを提供し、不審なトラフィックを継続的に分析・検出します。Qualys クラウドプラットフォームは、これらのネットワーク異常を他の侵害兆候と相関させます。

ネットワークアクセスの保護と制御: PNS は、重要なリソースへのアクセスを制御することで、脅威に自動的に対応します。PNS のリアルタイム検知情報に基づくネットワークアクセス制御は、確立されたポリシーとセキュリティ体制に基づいて、非準拠デバイスを隔離することで、ネットワークを自律的に保護します。

Qualys PNS delivers instant visibility into every asset

Qualys クラウドエージェント

Qualys Cloud Agent は、グローバル企業全体にセキュリティを拡張します。これらの軽量エージェント（2MB）は、リモートから導入可能で、一元管理され、自動更新され、CPU リソースの消費を最小限に抑えます。

Cloud Agent は、ネットワークスキャンが不可能または実用的ではない環境でも動作します。動的 IP クライアントマシン、リモート/ローミングユーザー、静的および一時的なクラウドインスタンス、外部スキャンの影響を受けやすいシステムなどの資産には、Cloud Agent が最適な方法です。

最も汎用性の高い包括的なセンサーセット
エージェントレス、エージェントベース、パッシブなど、あらゆるセンサーオプションを備えているため、組織は特定のインフラストラクチャとニーズに最適な方法、ツール、テクノロジーを自由に組み合わせて使用できます。

最初の導入後、Cloud Agent はホストの完全な構成評価をバックグラウンドで実行し、収集したデータを分析のために Qualys Cloud Platform にアップロードします。その後、変更が発生するとすぐに Cloud Agent は更新をプラットフォームにプッシュし、最新の IT 資産データをすぐに利用できるようにします。
ハイブリッド環境のセキュリティ保護における多くのメリットには、以下が含まれます。

- スキャンウィンドウは不要です。資産がオフラインの場合でも、インストールされている資産のデータを常に収集します。
- 常時監視により、脆弱性の発見とパッチ適用の確認が迅速化されます。
- 複雑な認証情報やファイアウォールの管理は不要です。Qualys プラットフォームへの送信のみを行います。
- 複数の Qualys アプリと連携するため、セキュリティチームは資産からポイントソリューションエージェントを削除し、セキュリティツールを統合できます。

Cloud Agent とそれを活用する複数の Qualys アプリを使用することで、組織は侵害された資産の多次元ビューを取得できます。

最も汎用性の高い、完全なセンサーセット

エージェントレス、エージェントベース、パッシブなど、あらゆるセンサーオプションを備えているため、組織は特定のインフラストラクチャとニーズに最適な方法、ツール、テクノロジーを自由に組み合わせて使用できます。

Qualys クラウドアプリ

Qualys は、セキュリティとコンプライアンスのための包括的なクラウドアプリスイートを構築しており、現在 20 種類以上のアプリが利用可能で、その数は増え続けています。

これらのクラウドアプリは自動更新機能を備え、一元管理され、緊密に統合されており、IT 資産管理、IT セキュリティ、Web アプリのセキュリティ、コンプライアンス監視といった幅広い機能をカバーしています。
すべてのアプリケーションは同じプラットフォームを基盤とし、共通の UI を共有し、同じスキャナーとエージェントからデータを取得し、同じ収集データにアクセスし、同じユーザー権限を活用します。これにより、組織全体で高度なアクセス制御を維持しながら、使用上の複雑さを軽減できます。

集中化された Web ベースの単一画面ダッシュボードは、IT 環境の完全かつ継続的に更新されるビューを提供します。このインタラクティブで動的なダッシュボードでは、IT、セキュリティ、コンプライアンスに関するすべてのデータを一箇所に集約して相関分析し、詳細をドリルダウンして、さまざまなユーザー向けにカスタマイズされたレポートを生成することもできます。

多くの場合、情報セキュリティ チームは、相互運用性が悪く、保守と統合が困難でコストもかかる、さまざまな異機種混合のポイント ツールを使用しています。そのため、CISO が組織のセキュリティとコンプライアンスの体制を単一の統合ビューで把握することが困難になっています。

セキュリティ スタックを Qualys クラウド アプリに統合することで、組織はツールの断片化という悪夢から逃れ、組織のサイロを解体し、保護を担当するセキュリティ チームを含むセキュリティ チームの同期を維持できます。

オンプレミスインフラストラクチャ - Qualys は、脆弱性管理、継続的な監視、構成評価、脅威の優先順位付け、ファイル整合性の監視、侵害の兆候により、組織のネットワークとデータセンターのセキュリティ保護を支援します。

クラウドインフラストラクチャ - Qualys は、パブリッククラウドプラットフォーム上で組織の VM、クラウドインスタンス、コンテナが安全かつコンプライアンスに準拠していることを保証します。Qualys は主要なクラウドプロバイダーと契約・連携を結んでいるため、資産インベントリ、脆弱性管理、Web アプリスキャン、脅威の優先順位付け、ワークロードにおけるポリシーコンプライアンスなど、様々な機能をご利用いただけます。

IT 監査とコンプライアンス- Qualys はコンプライアンスとリスク管理のタスクを自動化し、資産インベントリ、脆弱性管理、構成評価、PCI コンプライアンス、ベンダー リスク管理を通じて、企業が社内ポリシーと外部規制を遵守できるようにします。

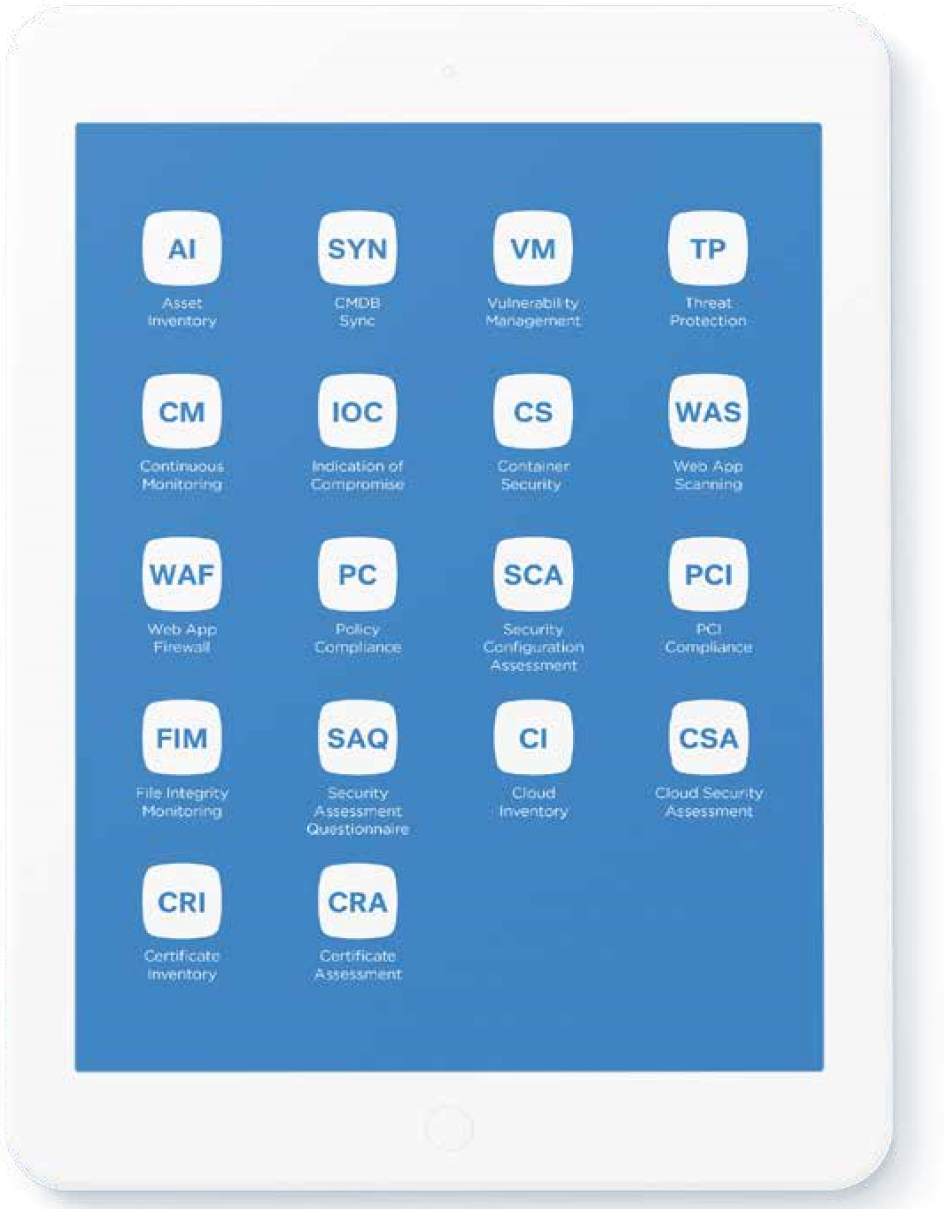
エンドポイント - Qualys は、包括的な資産インベントリ、脆弱性管理、構成評価、脅威の優先順位付け、侵害の兆候を通じて、拡大し複雑化するネットワークエンドポイントの世界を継続的に検出し、監視します。

DevSecOps と Web アプリ - Qualys を使用すると、脆弱性管理、構成評価、脅威の優先順位付け、Web アプリのスキャン、ファイル整合性の監視、侵害の兆候などを通じて、Web アプリの開発と展開のパイプライン全体にわたってコードの脆弱性と構成ミスのテストを自動化できます。

統合クラウドアプリ

組織は、必要なクラウドアプリを必要な時に利用し、1 つまたは複数のクラウドアプリをサブスクライブすることで、徐々に利用範囲を拡大することができます。

多くのお客様は、自社環境のセキュリティとコンプライアンス体制をより包括的に把握するために、複数のクラウドアプリを使用しています。Qualys クラウドプラットフォームは現在、以下のクラウドアプリを提供しています。



Asset Management

Qualys Asset Inventory (AI)

Qualys AI は、オンプレミス、クラウド、モバイルエンドポイントなど、あらゆる IT 資産の包括的なインベントリを継続的に更新します。資産にインストールされているソフトウェア、既存の脆弱性、ハードウェアの詳細をリスト化します。強力な検索エンジンにより、アドホッククエリを実行し、さまざまな基準で絞り込むことができます。

CMDB Sync (SYN)

この認定アプリケーションは、Qualys AI データを ServiceNow の構成管理システムと同期します。デバイスの変更は Qualys クラウドプラットフォームに即座に送信され、その後 ServiceNow と同期されるため、未識別資産や誤分類資産、データ更新の遅延が解消されます。

Cloud Inventory (CI)

Qualys CI は、パブリッククラウドのワークロードとインフラストラクチャの包括的なインベントリを提供します。パブリッククラウド環境内のリソースを継続的に検出し、中央のコントロールパネルからすべてのリソースを一元的に把握できる「単一画面」ビューを提供します。

Certificate Inventory (CRI)

Qualys CRI は、あらゆる認証局から発行されたすべての証明書を継続的に検出・カタログ化することで、お客様の TLS/SSL デジタル証明書のインベントリをグローバル規模で構築し、継続的に更新します。また、期限切れまたは期限切れが迫っている証明書が重要な業務に支障をきたすことを防ぎ、ダッシュボードから直接、期限切れまたは期限切れが迫っている証明書を可視化します。

IT Security

Vulnerability Management (VM)

Qualys VM は、業界をリードする受賞歴のあるソリューションです。組織全体のネットワーク監査と脆弱性管理を自動化し、ネットワークの検出とマッピング、資産管理、脆弱性レポート、修復追跡などを実現します。Qualys VM は、既知の脆弱性に関する包括的なナレッジベースを基盤としており、多大なリソース投入を必要とせずに、コスト効率の高い脆弱性対策を実現します。

Qualys Threat Protection (TP)

Qualys TP を使用すると、最も重要な脅威を特定し、優先的に対策を講じる必要があるものを特定できます。Qualys TP は、外部の脅威情報を脆弱性や IT 資産インベントリと継続的に相関分析するため、どの脅威が組織にとって最も大きなリスクをもたらすかを常に把握できます。

Qualys Continuous Monitoring (CM)

Qualys VM 上に構築された Qualys CM は、ネットワークにおける脅威や予期せぬ変化を監視し、侵害につながる前に検知します。ネットワーク内で異常を検知すると、状況やマシンごとに適切な担当者に、ターゲットを絞ったアラートを即座に送信します。これにより、パブリック境界、内部ネットワーク、クラウド環境全体で何が起こっているかを追跡できます。

Indication of Compromise (IOC)

Qualys IOC は、脅威ハンティングを提供し、ネットワーク内外のデバイスの不審なアクティビティを検知し、既知および未知のマルウェアの存在を確認します。単一のコンソールから、オンプレミスサーバー、ユーザーエンドポイント、クラウドインスタンスの現在のシステムアクティビティと過去のシステムアクティビティを監視できます。

CS

Container Security (CS)

Qualys CS は、クラウド環境とオンプレミス環境の両方において、DevOps パイプラインとデプロイメント内のコンテナを継続的に検出、追跡、保護します。コンテナプロジェクト（イメージ、イメージレジストリ、そしてイメージから生成されたコンテナ）に関する包括的なトポグラフィック情報を収集することで、コンテナホストの完全な可視性を提供します。Qualys CS は、実行中のコンテナのスキャン、保護、セキュリティ確保も可能にします。

CRA

Certificate Assessment (CRA)

Qualys CRA は、継続的な監視、動的なダッシュボード、証明書の問題や脆弱性に関するカスタムレポート機能を提供することで、デジタル証明書と TLS 設定を評価できます。

SCA

Qualys Certificate Assessment(SCA)

は、分かりやすい手法を用いて FIM 証明書インスタンスグレードを生成するため、管理者は SSL の専門家でなくても、見落とされがちなサーバーの SSL/TLS 設定を評価できます。また、署名や鍵長が弱い、ポリシー違反の証明書も特定します。

CSA

Cloud Security Assessment (CSA)

Qualys CSA は、パブリッククラウドインフラストラクチャの継続的な監視を自動化し、設定ミス、悪意のある動作、非標準のデプロイメントを検出し、修復手順を提供します。Qualys CSA は REST API をサポートし、CI/CD ツールチェーンとのシームレスな統合を実現します。これにより、DevSecOps チームは潜在的なリスクとエクスポージャーに関する最新の評価を得ることができます。

Compliance Monitoring

PC

Policy Compliance (PC)

Qualys PC は、ネットワーク全体の IT システムに対してセキュリティ構成の自動評価を実施し、リスクの軽減と社内ポリシーおよび外部規制への継続的なコンプライアンスを支援します。PC では、すぐに使用できるライブラリコンテンツを活用し、業界推奨のベストプラクティスに基づいたコンプライアンス評価を迅速に実施できます。

PCI

PCI Compliance (PCI)

Qualys PCI は、カード会員データの収集、保管、処理、および伝送を保護するための PCI DSS 要件へのコンプライアンスを効率化・自動化します。Qualys PCI は、インターネットに接続されたすべてのネットワークとシステムをシックスシグマ（99.9996%）の精度でスキャンし、レポートを生成して詳細なパッチ適用手順を提供します。自動送信機能により、コンプライアンスプロセスが完了します。

FIM

File Integrity Monitoring (FIM)

Qualys FIM は、一般的なエンタープライズオペレーティングシステム上のファイル変更イベントを記録し、一元的に追跡します。Qualys FIM は、変更を迅速に特定し、ポリシー違反や悪意のある可能性のあるアクティビティを根絶するために必要な重要な詳細情報を収集します。Qualys FIM は、変更管理ポリシーの適用と変更監視の要件への準拠を支援します。

SCA

Security Configuration Assessment (SCA)

Qualys VM アドオンである Qualys SCA は、オペレーティングシステム、データベース、アプリケーション、ネットワークデバイスを対象とした最新の Center for Internet Security（CIS）ベンチマークを用いて IT 資産の構成を自動評価することで、VM プログラムを拡張します。SCA ユーザーは、ダウンロード可能なレポートを自動的に作成し、ダッシュボードを表示できます。

Security Assessment Questionnaire (SAQ)

Qualys SAQ は、サードパーティおよび社内のリスク評価プロセスを自動化・効率化するため、手作業で実施する必要がなくなります。SAQ を使えば、回答者の IT セキュリティポリシーとプラクティスに関する手順管理を評価するためのアンケートを簡単に設計できます。SAQ は、評価キャンペーンの開始と監視を自動化し、データの表示と分析のためのツールも提供します。

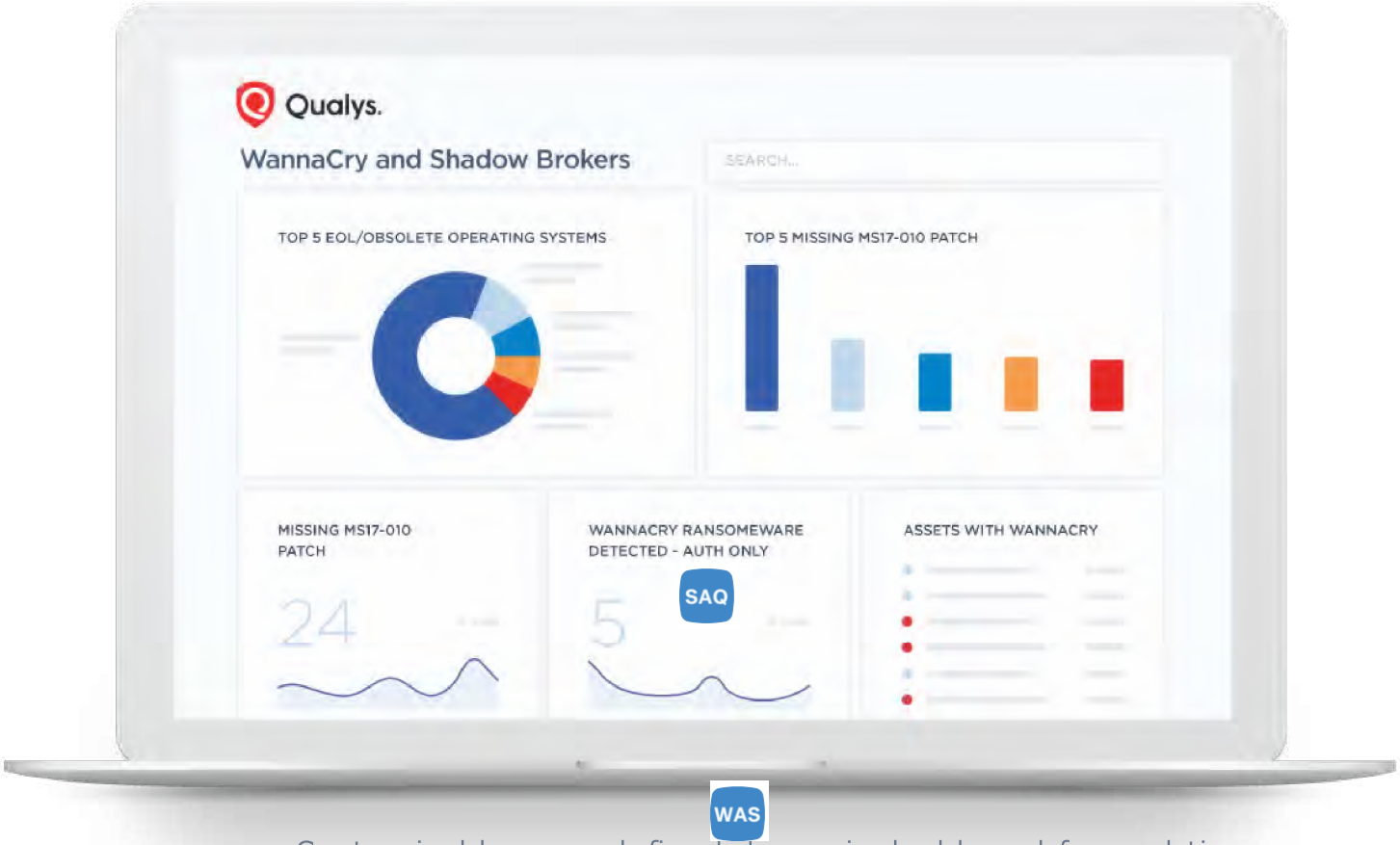
Web Application Security

Web Application Scanning (WAS)

Qualys WAS は、ネットワーク内の Web アプリケーションを継続的に検出・カタログ化し、脆弱性や設定ミスを検出します。Qualys WAF との統合により、Web アプリケーションへのワンクリックパッチ適用が可能になります。WAS を活用することで、DevOps 環境にセキュリティを組み込むことも可能です。Qualys WAS は、動作解析と静的解析を用いて、Web サイトからマルウェアを識別・削除します。

Web Application Firewall (WAF)

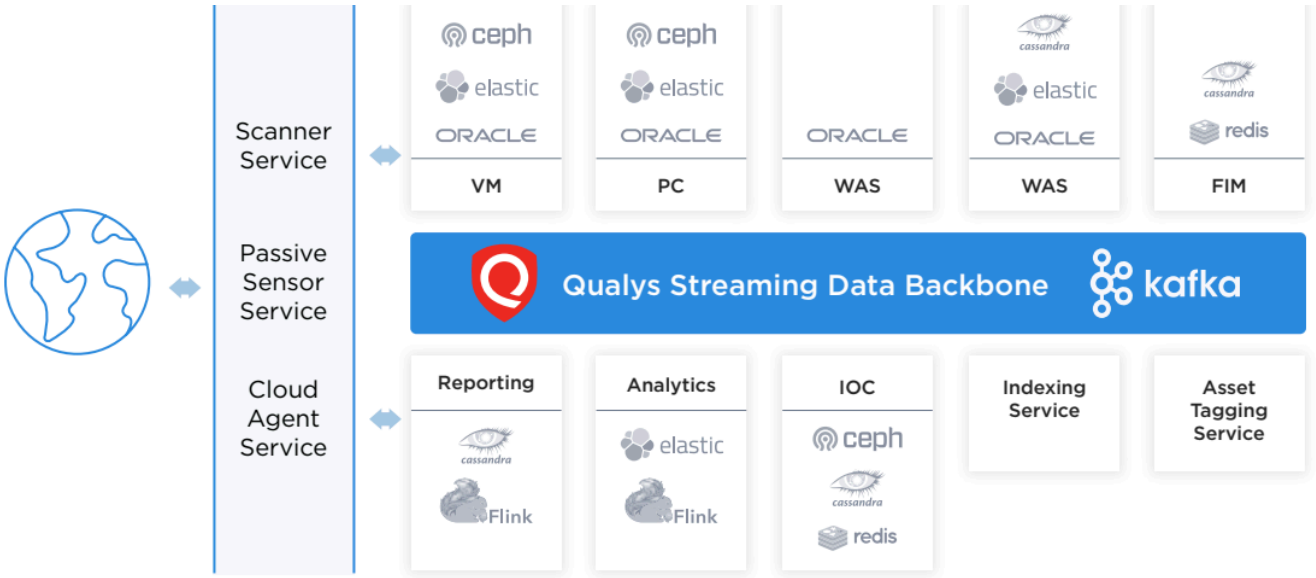
シンプル、スケーラブル、そして適応性に優れた Qualys WAF は、攻撃をブロックし、アプリケーションへのアクセスタイミングと場所を制御できます。Qualys WAF と Qualys WAS はシームレスに連携します。Qualys WAS で Web アプリをスキャンし、WAF で検出された脆弱性に対してワンクリックで仮想パッチを適用し、すべてをクラウドベースの一元ポータルから管理できます。導入はわずか数分で完了します。



Customizable, user-defined dynamic dashboard for real-time WannaCry remediation

BACK-END DATA CATEGORIZATION, VISUALIZATION AND ANALYSIS

このプラットフォームの資産タグ付けおよび管理機能により、お客様は多数の IT 資産を識別、分類、管理し、インベントリ作成と階層的整理のプロセスを自動化できます。また、高度に構成可能なレポートエンジンは、レポート、グラフ、ダッシュボードの作成をサポートし、データの視覚的な表現を生成できます。当社の分析エンジンは、お客様の IT 環境から収集されたペタバイト規模のセキュリティおよびコンプライアンスデータをインデックス化し、検索可能にするとともに、Qualys KnowledgeBase に含まれる外部の脅威データと相関分析を行います。



データ分析は、様々な角度と視点から行われます。例えば、Qualys クラウドプラットフォームが Windows ラップトップでレジストリキーの変更または追加を検出すると、そのデータはバックエンドエンジンに送信され、多次元的に分析されます。この場合、Qualys クラウドプラットフォームはレジストリ変更の考えられる理由を調査し、ポリシーコンプライアンス違反が原因かどうか、あるいはマルウェア感染を示唆しているかどうかを調査します。つまり、Qualys クラウドプラットフォームは、この 1 つのデータポイントを複数回分析します。これは、組織が他のベンダーから複数のポイントソリューションを購入することでしか実行できないタスクです。

当社の統合ワークフローサービスにより、お客様は迅速にリスク評価を行い、修復、インシデント分析、フォレンジック調査のための情報にアクセスできます。お客様は、ヘルプデスクチケットの作成、ポリシーおよびコンプライアンス例外の管理、パッチ適用とリスク軽減の取り組みの追跡とエスカレーションを行うことができます。 Qualys クラウド プラットフォームは、新しい脆弱性やマルウェア感染の検出、スキャンの完了、トラブルチケットのオープン、システム更新など、さまざまなアクションやインシデントについて顧客に事前に警告する通知をトリガーすることもできます。

クラウドベースのアーキテクチャのメリット

単一の包括的なビュー
多種多様なセンサーから得られるデータの一元分析は、クラウドでのみ可能です。導入が容易な当社のアプライアンスと軽量エージェントは、お客様の IT 環境から継続的に収集されるセキュリティおよびコンプライアンスデータを Qualys クラウドプラットフォームに自動的に送信します。

最高品質のアプリケーション
当社のクラウド アーキテクチャにより、統合された最善のアプリケーションの完全なセットを提供し、オンプレミス システム、エンドポイント、クラウド インスタンスからのさまざまなデータを相関させ、新しいサービスを簡単に追加することができます。

簡単で直感的
インストールや管理は不要で、すべてのサービスはクラウド上の Web インターフェースからアクセスできます。Qualys がすべての運用と保守を担当します。プラットフォームは常時稼働し、自動更新されます。

運用コストの削減
すべてがクラウド上にあるため、設備投資や追加の人員は不要で、インフラやソフトウェアの購入・保守も不要です。Qualys は、柔軟なサブスクリプションモデルを通じて、ライセンスコストをより柔軟に管理できます。

簡単なグローバルスキャン
境界、ファイアウォールの背後、動的なクラウド環境、エンドポイントなど、地理的に分散されセグメント化されたネットワークのスキャンを簡単に実行できます。

•

シームレスで柔軟なスケーリング
Qualys クラウドプラットフォームは、IT セキュリティのあらゆる側面に対応する、拡張性の高いエンドツーエンドのソリューションです。導入後は、必要に応じて新しいカバレッジ、ユーザー、サービスを追加できます。サブスクリプションパッケージは、あらゆる規模の組織に合わせてカスタマイズできます。また、アプリのサブスクリプションをアラカルトで購入することも可能です。

最新のリソース
Qualys は業界最大規模の脆弱性シグネチャのナレッジベースを保有し、年間 30 億件以上の IP スキャンを実施しています。セキュリティアップデートはすべてリアルタイムで行われます。

•

安全に保存されたデータ
脆弱性データは、負荷分散された n 層アーキテクチャのサーバー上で安全に保存・処理されます。暗号化されたデータベースは、物理的にも論理的にも安全です。

当社のアプリとサービスは、パブリッククラウドプラットフォームまたはプライベートクラウドプラットフォームを通じて提供されます。

Public Cloud Platform Option

マルチテナント、マルチレイヤー、そして高い拡張性を備えた Qualys のパブリッククラウドプラットフォームは、カリフォルニア州サンタクララ、バージニア州アッシュバーン、スイスのジュネーブ、インドのプネ、そしてオランダのアムステルダムにあるデータセンターから提供されています。
Qualys のパブリッククラウドプラットフォームは、Web ブラウザを介してどこからでも 24 時間 365 日アクセスでき、常に 99%の可用性を維持しています。更新は透過的に行われ、ユーザーへの影響は一切ありません。オフラインになるのは四半期に一度、メンテナンスのためだけです。

保存されたデータは暗号化された状態で保管されます。Qualys は各ユーザーのデータを一意に暗号化するため、データを作成したユーザーのみがアクセスできます。Qualys は顧客データの内容を把握することはできません。また、暗号化キーにアクセスできないため、保存されたデータを復号化することもできません。

Qualys クラウドプラットフォームは、ネットワークベースの冗長化された高可用性ファイアウォールと侵入監視ソリューションによって保護されています。さらに、各ホストは、Qualys 独自のカスタマイズされた堅牢な Linux ディストリビューション上に、ローカライズされたファイアウォールを稼働させています。
プラットフォームは、国際的に認められた会計事務所による SSAE 16 または業界標準の代替監査を少なくとも年に 1 回受けているデータセンターでホストされています。Qualys のすべてのデバイスは、生体認証を含む多要素認証によって保護された、物理的に安全な専用の施錠されたキャビネットに設置されています。

コアサービスには以下が含まれます。

- 資産のタグ付けと管理
- レポートとダッシュボード
- アンケートとコラボレーション
- 修復とワークフロー
- ビッグデータ相関分析エンジン
- アラートと通知

Private Cloud Platform Option

セキュリティとコンプライアンスに関するデータを自社で管理する必要がある組織向けに、Qualys プライベートクラウドプラットフォームを提供しています。このプラットフォームは、マルチテナント型パブリッククラウドプラットフォームのすべての機能を備えています。Qualys プライベートクラウドプラットフォームは、厳格なデータ主権ルールを持つ国に拠点を置く企業、データ保有要件を持つ政府機関、そしてより限定的なサービスを提供したい MSSP に最適です。

大規模組織向けにはフルサーバーまたは仮想ラックとして、小規模企業向けにはスタンドアロンアプライアンスとして利用可能なオールインワンデバイスは、Qualys ソフトウェアがプリロードされ、迅速かつ容易に導入できるよう事前構成されています。アプライアンスが到着する前に、すべての物理的なラックとケーブル配線作業が完了しています。Qualys はリモートでアップデートとメンテナンスを行い、必要なハードウェア拡張も Qualys が対応します。

Qualys Subscriptions

SMB、中規模企業、大企業、コンサルタント、MSP、政府機関

Qualys は、あらゆる業種・規模の組織に、多様なサブスクリプションオプションをご用意しています。お客様のニーズに合わせてサービスをカスタマイズ・拡張することができ、Qualys クラウドプラットフォームの機能、アプリケーション、スキャナー、エージェント、そして監視対象 IT 資産の種類に基づいて価格設定が異なります。

Qualys は、大企業、中規模組織、中小企業、政府機関向けのサブスクリプションを提供しています。また、Qualys を使用して顧客にセキュリティおよびコンプライアンスサービスを提供するコンサルタントや MSP 向けのサブスクリプションもご用意しています。

すべてのサブスクリプションには無料のトレーニングとサポートが含まれています。お客様はデバイスと Web アプリを無制限にスキャンでき、クラウドエージェントも無制限にご利用いただけます。
それぞれのオファーを個別に見てみましょう。

小規模企業向けの Qualys サブスクリプション

中小企業では、社内に IT セキュリティに関するリソースや知識が不足しているため、IT セキュリティが脆弱な点となることがよくあります。Qualys Express Lite のクラウド型セキュリティ・コンプライアンスソリューションスイートを利用すれば、中小企業はブラウザから直接セキュリティとコンプライアンスを監視できます。継続的なネットワーク監視、脆弱性管理、脅威の優先順位付け、PCI コンプライアンス、ベンダーリスク管理、Web アプリケーションスキャンなどの機能を備えています。

256 IPs （スキャン用）
25 web apps （スキャン用）
2 スキャナー
3 ユーザー

中規模サイズ企業向けの Qualys サブスクリプション

Qualys は、中規模企業の IT セキュリティを簡素化し、コンプライアンスコストの削減を支援します。Qualys Express クラウドスイートには、IT 資産インベントリ、脆弱性管理、継続的なネットワーク監視、Web アプリケーションスキャンとファイアウォール、脅威の優先順位付け、PCI を含むポリシーコンプライアンス、ベンダーリスク管理などの機能が含まれています。

5,120 IPs （スキャン用）
200 web apps （スキャン用）
5 スキャナー
ユーザー数　無制限
修復チケットの発行と追跡
パブリッククラウドとの統合

大規模サイズ企業向けの Qualys サブスクリプション

Qualys は、大規模な組織に包括的なセキュリティおよびコンプライアンス ソリューションを提供します。これにより、機能が制限され、サイロ化された状態で運用される従来のスタンドアロン製品を排除し、TCO を大幅に削減できます。

スキャン用 IP アドレス　無制限
スキャン用 Web アプリ　無制限
スキャナー数　無制限
ユーザー数　無制限
修復チケット発行と追跡
パブリッククラウドとの統合

コンサルタントと MSP 向け Qualys サブスクリプション

顧客の IT インフラが複雑化し、ハッカーがより大胆かつ効果的に活動するにつれ、セキュリティコンサルタントが直面する課題、要求、そしてプレッシャーはますます深刻化しています。

コンサルタントが成功するには、ノウハウと経験だけに頼るのではなく、業務を遂行するために利用可能な最高のソフトウェアツールを駆使する必要があります。

クラウドベースで集中管理されたコンサルティングエディションを提供することで、Qualys は機能が制限された手動ツールが溢れる市場において、際立った存在となっています。

コンサルティング エディションは、コンサルタントや MSP が顧客に幅広い第一級のセキュリティおよびコンプライアンス評価サービスを提供できるように支援します。

• マルチテナント：複数のクライアントからのデータを、中央のダッシュボードから簡単に整理・管理できます。スキャンを実行すると、結果は適切なクライアントレコードに直接関連付けられます。クライアント固有のネットワーク環境をセグメント化できます。

• 柔軟性と包括性：オンプレミス、クラウド、エンドポイントにおいて、脆弱性管理、ポリシーコンプライアンス、Web アプリケーションスキャンなど、幅広いサービスを提供します。これは、Qualys の多彩なセンサー（ローカル、仮想、クラウドスキャナー、クラウドエージェント、パッシブネットワークスニファーなど）によって実現されています。すべてのプロセスは、Qualys の API を使用して自動化できます。

•実用的なレポート：脆弱性の傾向を示す、クライアント重視のレポートを作成し、さまざまな形式（HTML、DocX、MHT、XML、PDF、CSV）でエクスポートできます。

政府向け Qualys サブスクリプション

政府がデジタル変革を推進する中で、クラウド導入は最前線にあります。サイバー脅威を特定、検知、対応し、規制およびコンプライアンス要件を満たすことでデジタル化の取り組みを保護することは、この変革において不可欠です。成功するためには、地方、州、連邦政府機関、そして国防総省は、進化する IT 環境を完全かつ継続的に管理できる、統合セキュリティおよびコンプライアンス・プラットフォームを必要としています。

FedRAMP 認定の Qualys Gov プラットフォームは、政府機関が容易に大規模に導入できる統合ソリューションを提供し、IT 資産のセキュリティとコンプライアンス状況を可視化します。Qualys Gov プラットフォームは、均質でカプセル化された環境向けに設計された従来のエンタープライズセキュリティ製品の限界を克服します。Qualys Gov プラットフォームは、今日のハイブリッドでボーダーレス、そして急速に変化する IT 環境を保護しなければならない高度なサイバー防御担当者が求める、拡張性、俊敏性、そして汎用性を提供します。

- FedRAMP 認定および CDM 承認：Qualys Gov プラットフォームは、2016 年に FedRAMP 運用認可（ATO）を取得し、米国一般調達局（GSA）の CDM プログラムの承認製品リストに掲載されています。

- 導入の柔軟性：厳格なデータストレージ要件を持つ機関向けに、Qualys のプライベートクラウドプラットフォーム（PCP）オプションは、Qualys Gov プラットフォームのすべてのメリットをお客様のデータセンター内で提供し、データを管理下で保存できるようにします。

- 連邦政府機関向けカスタムテンプレート：Qualys Cloud Apps は、連邦政府が義務付ける規制やポリシーへのコンプライアンスを効率化するために設計された、すぐに使用できる複数のテンプレート、機能、および構築済みコンテンツを提供します。

- エンドツーエンドのセキュリティプラットフォーム：NIST サイバーセキュリティフレームワークに完全にマッピングされた Qualys Gov プラットフォームは、識別と検出から保護と対応まで、組織を支援します。

Qualys コミュニティエディション

Qualys は、小規模組織が今日のセキュリティとコンプライアンスの課題に取り組むのを支援するため、プラットフォームの無料版である Qualys Community Edition を提供しています。Qualys Community Edition を利用することで、小規模企業は Qualys Cloud Platform の精度と信頼性を活用し、IT 資産と脆弱性の検出、コンプライアンスギャップの特定、詳細なレポートの取得が可能になります。

Qualys エージェントとスキャナーを使用することで、このコミュニティエディションは、資産の検出、脆弱性評価、構成評価、Web アプリケーションのスキャン、パブリッククラウドワークロードのインベントリ作成などの機能を提供します。

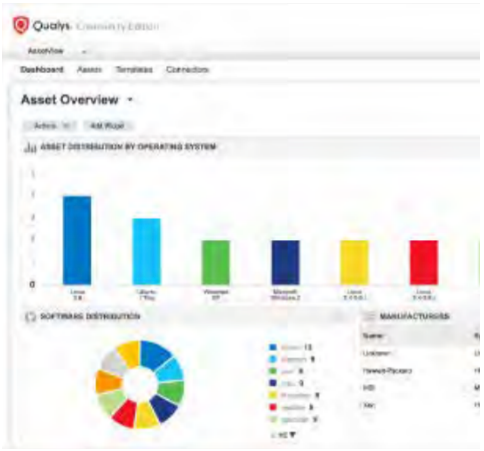
Qualys Community Edition は、プラットフォームのインタラクティブでカスタマイズ可能な動的なダッシュボードを通じて、小規模組織に監視対象の資産と Web アプリケーションの統合された合理的なビューを提供します。

インストール、保守、管理は一切不要です。すべてのサービスはクラウド上にあり、Web インターフェースからアクセスできます。Qualys Community Edition は、IT インフラストラクチャと Web アプリケーションを、Qualys の包括的な脆弱性ナレッジベースに照らし合わせてスキャンします。

Qualys Community Edition には、Qualys CloudView と Qualys CertView が付属しています。

CloudView を使用すると、組織はパブリッククラウドのすべての資産とリソースを一元化された「単一のビュー」インターフェースから確認できます。インスタンスや仮想マシン、ストレージバケット、データベース、セキュリティグループ、ACL、ELB、ユーザーなどの資産とリソースを、すべてのリージョン、複数のアカウント、複数のクラウドプラットフォームにわたって継続的に検出し、追跡します。

CertView を使用すると、組織はインターネットに接続する証明書をインベントリ化して評価することで、証明書の管理を取り戻すことができます。インターネットに接続するすべての証明書と SSL/TLS 構成を可視化し、証明書と構成の修正の優先順位を一元的に管理および視覚化できます。カスタマイズ可能なダッシュボードと高度に設定可能なウィジェットにより、証明書のステータス、グレード情報、脆弱性データを確認できます。CloudView と CertView は、Community Edition 以外でも、スタンドアロンの無料アプリとしてご利用いただけます。



包括的なトレーニングとサポート

Qualys は、お客様とのパートナーシップと、あらゆる段階でのサポートの重要性を深く認識しています。

Qualys は、無料の製品トレーニングと 24 時間 365 日対応の電話サポートを提供しています。電話は 1 分以内に応答し、サポート、運用、エンジニアリングのスタッフが連携して対応します。サポートメールへの返信は平均 24 時間以内に行われます。カリフォルニア州フォスターシティ本社、ノースカロライナ州ローリー、英国レディング、インドプネーにカスタマーサポートセンターを設置しています。

さらに、Qualys のウェブサイトには、2 万人を超えるメンバーが参加するサポートコミュニティ、トレーニングビデオ、ナレッジベースが用意されています。Qualys の従業員とお客様が集まり、ベストプラクティスを共有したり、互いの質問に答えたりしています。

Part Ⅲ

カスタマー

カスタマーベース

当社の製品の品質を最もよく証明しているのは、顧客基盤です。Qualys は、130 カ国以上、あらゆる主要垂直産業にわたる 10,300 社以上の顧客を擁しています。Forbes Global 100 および Fortune 100 企業の大半が当社の顧客です。

9 of the top 10 in **Software**

8 of the top 10 in **Consumer Discretionary**

8 of the top 10 in **Consumer Staples**

8 of the top 10 in **Major Banks**

8 of the top 10 in **Technology**

8 of the top 10 in **Telecommunications**

7 of the top 10 in **Healthcare**

6 of the top 10 in **Industrial & Materials**

5 of the top 10 in **Insurance**

Qualys は、Accenture、AT&T、HPE、BT、Deutsche Telekom、HCL Technologies、IBM、Infosys、NTT、Verizon、Wipro などの主要なマネージド サービス プロバイダーやコンサルティング組織とも戦略的パートナーシップを確立しています。

継続的なセキュリティ監視で解決策を発見

Geisinger

Geisinger Health System は、オンプレミスとクラウドシステムが混在する IT 環境を保護するため、Qualys Cloud Platform の脆弱性管理、PCI、Web アプリケーションスキャン、そして Cloud Agent を使用しています。ペンシルベニア州ダンビルに拠点を置くこの医療サービスプロバイダーは、複数のデータセンター、2 万台を超えるエンドポイント、そして数千台のサーバーを保有しています。

Geisinger は約 8 年間 Qualys の顧客であり、その間 Qualys 製品の活用を深めてきました。「当初は従来の脆弱性管理から始めましたが、組織の成長に伴い、デバイス、アプリケーション、インフラストラクチャ、特に患者ケアに直接影響を与える機器の複雑化に伴い、Qualys 製品の活用範囲を拡大してきました」と、Geisinger のサイバーオペレーション担当情報セキュリティアナリスト、Nathan Cooper 氏は述べています。

3 万人の従業員を擁する Geisinger は、セキュリティチーム部門のサーバーで Cloud Agent を試験的に導入しました。「結果は合格でした。エージェントと Qualys Cloud Platform の VM 脆弱性スキャンの間に矛盾はありませんでした」と Cooper 氏は述べています。 「これで、ベースサーバーイメージにエージェントを追加できるようになりました。これにより、仮想テンプレートから構築された新しいサーバーには、エージェントが即座にインストールされます。つまり、新しいサーバーはすぐに Qualys クラウドプラットフォームに自己報告することになります。」

「新しいシステムがプロビジョニングされ、脆弱性管理ライフサイクルに組み込まれていることを、すぐに把握できます」と Cooper 氏は述べています。「Qualys クラウドプラットフォームを搭載した Qualys クラウドエージェントは、まさにこのようにして、Geisinger の脆弱性管理の取り組みを改善し、セキュリティチームと Geisinger の両方が必要とするリアルタイムで継続的なセキュリティを実現しています。」

クラウドエージェントが Synovus の脆弱性検出を強化

SYNOVUS®

Qualys Cloud Agent は、ジョージア州コロンバスに本社を置き、資産規模約 280 億ドルの金融サービス企業である Synovus Bank で大きな成果を上げています。
Synovus Bank は、Qualys VM を導入することで、社内外のすべての資産に対して頻繁な脆弱性スキャンを実施し、ゼロデイ攻撃や重大な脅威に関する通知と対策を迅速に受け取り、パッチ配布の優先順位付けに役立つデータを提供することで、脆弱性分析とセキュリティパッチ適用プログラムを改善しています。
その後、同社は Cloud Agent を導入し、ノートパソコンからの脆弱性情報の収集精度を高めました。デスクトップワークステーション、サーバー、ネットワークアプライアンスとは異なり、ノートパソコンはモバイルであるため、ネットワークへの接続が断続的になります。そのため、Synovus Bank では、事前にスケジュールされた脆弱性スキャンの実施時間を逃すことがよくありました。
Cloud Agent の導入により、Synovus Bank はノートパソコンの脆弱性をほぼリアルタイムかつより正確に検出できるようになりました。
そしてすぐに、以前の推定とは異なり、平均的なノートパソコンには 30 件ではなく、約 200 件の脆弱性が存在することが判明しました。Synovus 社はノートパソコンのパッチ適用スケジュールを変更し、毎日実施するように頻度を増やしました。その結果、平均的なノートパソコンの脆弱性は約 10 件となり、劇的に減少しました。
「Cloud Agent の導入はすぐに効果を発揮しました」と、Synovus 社のシニアセキュリティアナリストである Corey Reed 氏は述べています。

Synovus 社は、Cloud Agent が自動更新されるためメンテナンスが最小限で済むこと、そしてグループポリシーと SCCM（System Center Configuration Manager）を通じて簡単に導入できることを高く評価しています。また、Cloud Agent はコンピューティングリソースをほとんど消費しないため、ネットワークや IT 資産への影響がごくわずかであることも高く評価しています。

Capital One、DevOps にセキュリティを組み込む

Capital One は Qualys の支援を受けて、DevOps パイプラインに自動セキュリティチェックを組み込み、仮想マシンイメージとコンテナの脆弱性や構成ミスの評価を大幅に加速しました。
その結果、DevOps パイプラインで作成されたコードは安全であると認証され、不要な遅延なく本番環境にリリースされます。これにより、Capital One は Web プロパティ、モバイルアプリ、オンラインサービス、デジタルサービスを迅速かつ継続的に改善することで、事業全体を着実に成長させることができました。

「これは会社全体に大きなメリットをもたらしました」と、Capital One の脆弱性/構成管理担当シニアマネージャー、Emmanuel Enaohwo 氏は述べています。

安全な AMI ベーカリーの構築

当初、Capital One の Amazon Machine Images (AMI) のセキュリティ認証プロセスは手作業で行われており、DevOps チームとセキュリティチームが「修正 / 発見 / 検証」のループを繰り返していたため、最大 2 週間もかかっていました。

このプロセスを短縮するために、DevOps チームにセキュリティチームの Qualys 脆弱性管理およびポリシーコンプライアンスツールへの API アクセスが付与されました。これにより、開発者はセキュリティチームの介入なしに、自らスキャンを実行し、レポートを取得し、必要に応じて修正と再スキャンを実行できるようになりました。これにより、プロセスは 24 時間未満に短縮されました。

Capital One はまた、本番環境にデプロイされたすべての AMI に Qualys Cloud Agent をシードすることで、ライブインスタンスで新たに発見されたセキュリティおよびコンプライアンスの問題について即座にアラートを受信できるようにしています。

Capital One は、DevOps の「ベーカリー」を通過するほぼすべての AMI に Cloud Agent を導入することで、IP アドレスの 95%の評価範囲を達成しました。

このエージェントにより、脆弱性や設定ミスの検出精度が向上し、誤検知が削減され、スキャンデータの可用性が迅速化されました。「これらの KPI はすべて、Qualys Cloud Agent と API を使用した DevOps との統合によって達成されました」と彼は述べています。

コンテナの確保

Capital One は、アプリケーション開発とデリバリーのスピードと柔軟性を高めるために Docker コンテナを使用しています。

これらの環境を保護するために、Capital One は Qualys Container Security（CS）を選択しました。これは、DevOps パイプラインにおけるコンテナの継続的な検出と追跡を提供します。

Capital One は Qualys CS の Jenkins CI/CD ツール用プラグインを使用することで、DevOps チームがコンテナイメージを自らスキャンして修正できるようにしています。

Part IV

The future

今後の展望

Qualys クラウドプラットフォームは、競合他社をリードする中で、その範囲を拡大し続けます。現在開発中の新製品には、パッチとデジタル証明書を管理するためのクラウドアプリが含まれます。

また、iOS、Android、Windows Mobile 向けのクラウドエージェント、EMM（エンタープライズモビリティ管理）機能、資産インベントリ、脆弱性管理、脅威検出、ポリシーのコンプライアンスと適用を含むモバイルセキュリティ製品も開発中です。

当社は革新を続け、業界をリードする製品を提供し続けることで、お客様はクラウド指向でモジュール型の包括的かつ統合されたアーキテクチャを備えた Qualys クラウドプラットフォームの独自のメリットを継続的に享受できるようになります。

- 最善のソリューションを統合したスイート
- グローバル配信
- より迅速、シンプル、低コストな導入
- より高い品質
- 継続的な改善

Qualys: ハイブリッド IT 環境にシームレスにセキュリティを組み込み、デジタル変革を実現します。

Qualys について

Qualys, Inc.（NASDAQ: QLYS）は、クラウドベースのセキュリティおよびコンプライアンスソリューションのパイオニアであり、リーディングプロバイダーです。130 カ国以上で 10,300 社以上の顧客を抱え、Forbes Global 100 および Fortune 100 企業の過半数を占めています。Qualys は、組織がセキュリティおよびコンプライアンスソリューションを単一のプラットフォームに統合・合理化し、デジタルトランスフォーメーションの取り組みにセキュリティを組み込むことで、俊敏性の向上、ビジネス成果の向上、そして大幅なコスト削減を実現できるよう支援します。Qualys クラウドプラットフォームと統合されたクラウドアプリは、企業に重要なセキュリティインテリジェンスを継続的に提供し、オンプレミス、エンドポイント、そして柔軟なクラウド上の IT システムと Web アプリケーションの監査、コンプライアンス、保護の全範囲を自動化することを可能にします。1999 年に最初の SaaS セキュリティ企業の 1 つとして設立された Qualys は、主要なマネージドサービスプロバイダーやコンサルティング組織と戦略的パートナーシップを築いてきました。

Qualys, Inc. - Headquarters
Qualys is a global company with offices around the world. To find an office near you, visit
http://www.qualys.com
919 E Hillsdale Blvd, 4th Floor Foster City, CA 94404 USA
T: 1 (800) 745 4355,
info@qualys.com