Qualys

ホワイトペーパー

クラウドセキュリティに関する 10 の誤解

Qualys のソートリーダーシップ

目次

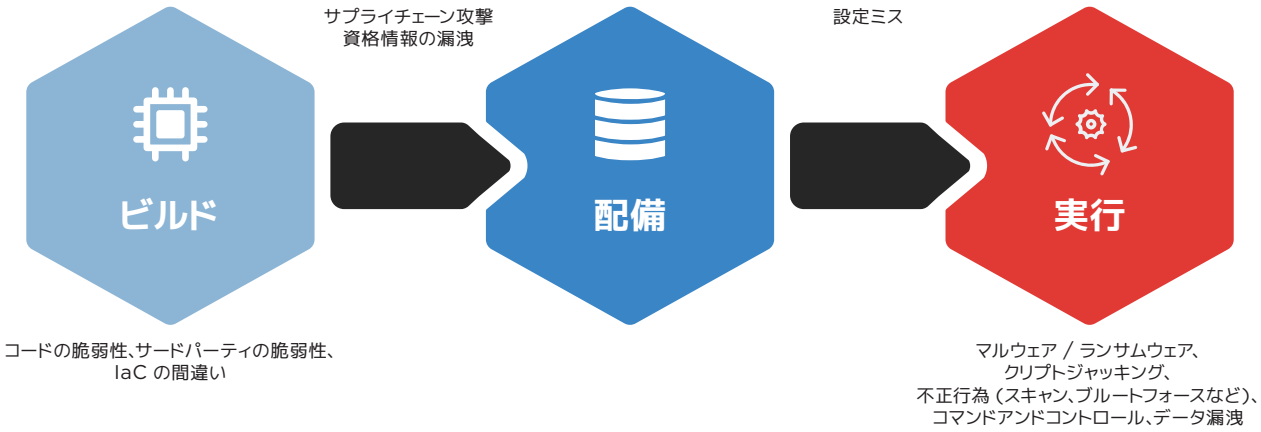
はじめに

クラウドセキュリティは複雑な状況であり、クラウドサービスのライフサイクルのあらゆる段階で包括的なツール、ポリシー、取り組みが必要です。クラウドセキュリティ プログラムを最も効果的にするには、クラウドリスクを効果的に測定、伝達、排除できなければなりません。
クラウド サービスへの移行は、DevOps チームとセキュリティ チームに一連の新たなセキュリティ課題をもたらします。まず、クラウド サービス プロバイダーを使用してもセキュリティの責任が免除されるわけではないことを理解する必要があります。

すべてではないにしても、ほとんどのクラウドプロバイダーは、セキュリティに対して責任共有モデルを適用しています。最近のクラウド移行は、単純なSaaS(Software-as-a-Service)プラットフォームだけでなく、より機能の充実したIaaS(Infrastructure-as-a-Service)やPaaS(Platform-as-a-Service)へとますます拡大しており、それに伴い社内チームの責任も大きくなっています。
残念ながら、多くのチームは、最新のクラウド環境でどのツール、ポリシー、実践が最も効果的であるかをまだ完全には理解していません。セキュリティフレームワークとポリシーをオンプレミスからクラウドに単純に適用する試みは、成功するアプローチではありません。CISO から SecOps チーム、DevSecOps チームに至るまで、社内のセキュリティ専門家にとって、堅牢で効果的なクラウド固有のセキュリティ プログラムを構築する方法を学ぶことは不可欠です。

このホワイトペーパーでは、クラウドセキュリティに関する10のよくある誤解を特定し、それらがセキュリティへの取り組みに及ぼす影響について説明します。次に、IT 部門とセキュリティ部門がこれらの誤りを克服してクラウドセキュリティ体制を改善する方法について説明します。

クラウドでの一日



クラウドのライフサイクルにおけるセキュリティリスク

IaC と設定ミスのチェックで クラウド セキュリティのすべてのニーズをカバー

01

信念

- Infrastructure as Code (IaC) の ベスト プラクティスに従うことで攻撃を防止できます。
- 構成ミスチェックを定期的に実行することで 攻撃を防止します。

現実

- 関係者全員がベスト プラクティスに従うという 保証はありません。
- 攻撃はチェック間または構成修正作業中に 頻繁に発生します。

クラウドの構成ミスは、クラウド環境のセキュリティ保護に関連する最も重大な問題であることは間違いありません。構成に誤りがあると、データ侵害のリスクが増幅されます。**2023 Qualys TotalCloud Security Insights** の調査結果によると、3 つの主要プロバイダー全体で平均して CIS ベンチマークの 50% が失敗しています。Center for Internet Security (CIS) コントロールは、CSP 環境の構成を強化し、監査人にコンプライアンスを実証するためのゴールドスタンダードです。CIS コントロールは、クラウドの基本的なセキュリティ衛生を確保するために必要な最低限のものです。

さらに、コードとしてのインフラストラクチャ(IaC)の構成チェックを含む頻繁な構成チェックも、組織のセキュリティのベスト プラクティスの一部である必要があります。ただし、設定ミスが一般的な脆弱性であるからといって、セキュリティへの取り組みがそのベクトルのみに対処するだけで済むわけではありません。構成チェックのみに依存することは、たとえ家の窓の多くがまだ大きく開いているにもかかわらず、家の玄関ドアを閉めて侵入者を完全に阻止できると信じるようなものです。

例えば、Infrastructure as Code(IaC)のスキャンを考えてみましょう。一般的な組織では、開発者の数がサイバーセキュリティ担当者の数をはるかに上回っています。そのため、IaCのセキュリティ・ツールチェーンに関係者全員が準拠していることを確認することは、特に開発者が組織自体ではなくクラウド・プロバイダーのために働いている場合(つまり、シャドウ・クラウドITグループ)には、困難な作業になります。

脆弱性管理だけで十分

02

信念

- クラウド CI/CD パイプラインにより、アジャイルな脆弱性管理の実践が可能。
- ワークロードをオンプレミスよりも迅速に再デプロイできる。

現実

- 内部サーバーは外部に面したワークロードほどパッチが適用されていないことが多いため、攻撃者は依然としてクラウド サービスにアクセスする手段を多く持っています。

もう 1 つのよくある誤解は、継続的インテグレーションおよびデリバリー（CI/CD）パイプラインのおかげで、クラウド セキュリティ ツールと手法はオンプレミスのセキュリティへの取り組みよりもはるかに速く進化し、その結果、攻撃に対する耐性が強化されるというものです。クラウドでの脆弱性管理がオンプレミスよりも機敏であることは一般に真実ですが、これはクラウド システムが無敵であることを意味するものではありません。アジャイルなセキュリティ慣行が導入されている場合でも、ハッカーには常にチャンスが存在します。たとえば、企業の内部サーバーには、外部に面したワークロードやサーバーに比べてパッチがあまり適用されていないことがよくあります。これにより、攻撃者は、資格情報の侵害、水平攻撃、設定ミスの悪用、またはサプライ チェーン攻撃を通じて組織のクラウド サービスへのアクセス経路を作成し、内部サーバーの脆弱性を悪用することができます。

もう 1 つの例は、一般的な脆弱性とエクスプロイト（CVE）のみに焦点を当てた機敏なセキュリティの取り組みの失敗です。最近のいくつかの侵害は、標準のセキュリティ　パッチでは対処されていない未確認の CVE を攻撃者が悪用していることを証明しています。効果的なクラウド防御には、この種の攻撃に対する正確なスキャン機能と制御を組み込む必要があります。

クラウドではサプライ チェーン攻撃は問題になりません

03

信念

- サプライチェーン攻撃はオンプレミスシステムに限定される。

現実

- 攻撃者にとって、コンテナを介してクラウド サプライチェーンにバックドアを挿入するのは簡単です。

一部のセキュリティ専門家は、サプライ　チェーン攻撃という言葉を聞くと、すぐにオンプレミス システムを思い浮かべます。この関連性は、SolarWinds ハッキングやモルガン・スタンレー・アクセリオンのファイル転送アプリケーションの侵害など、いくつかの著名なサプライ チェーン攻撃が従来のオンプレミス　システムを標的としたものであるためです。しかし、これらのイベントがクラウド システムの免責を妨げるものではありません。

アジャイル クラウド ソフトウェア開発には、サードパーティや大規模なコード リポジトリから取得したオープンソース コードなどのコードの再利用が含まれます。コード リポジトリは急速に拡大し、毎日何千もの新しいコンテナが追加されています。コードの柔軟な供給により、攻撃者はコード リポジトリを介して攻撃を注入することで、サプライ チェーンにバックドアを追加することが簡単になります。

コードに挿入されたバックドアは、個々のファイルではなくパッケージのみを分析する標準の CVE チェックでは認識できません。

クラウド サプライチェーン攻撃を阻止するには、包括的なセキュリティへの取り組みの一環として、毎日数百万のファイルを迅速に分析できるツールを適用する必要があります。

強力な IAM ポリシーが すべてを解決します

04

信念

- クラウド内のきめ細かい IAM により、攻撃対象領域のサイズが制限されます。

現実

- IAM は基礎となるポリシーと同等の性能しかありません。

ID およびアクセス管理 (IAM) ツールは、効果的なクラウド セキュリティ プログラムの重要な部分です。クラウド サービスでは通常、非常にきめ細かい IAM を使用して、その露出を制限し、攻撃対象領域を最小限に抑えることができます。リソースのマイクロセグメント化、クラウド リソースへの時間制限付きアクセスとともに最小アクセス ポリシーの適用、効果的なプロビジョニングおよびプロビジョニング解除プロトコルの構築により、クラウド サービス管理者は、攻撃者がシステムやデータにアクセスする方法を制限できます。

ただし、IAM システムの優れた点は、その基礎となるポリシーによって決まります。製品やアップデートを迅速に市場に投入するというビジネス上のプレッシャーや、効率性に関する従業員の苦情などの問題により、寛容なポリシーが許可または「容認」されると、脆弱性が発生します。

厳格な IAM ポリシーが導入されている場合でも、攻撃者は依然としてクラウドの脆弱性を悪用する可能性があります。たとえば、EC2 ポリシーとストレージ バケット ポリシーの間など、複雑なポリシーの相互作用によりカバレッジ ギャップが発生する可能性があります。IAM ツールも、クラウド サービスのサプライ チェーンのあらゆる時点で漏洩の危険にさらされたままです。CI/CD の一部としてシークレット検出ツールを使用しても、攻撃を回避するには不十分です。

代わりに、ハッカーはフィッシング、ユーザー感染、インスタンス感染などの実績のあるツールに単純に戻ったり、以前の侵害で取得した認証情報を使用して IAM セキュリティをバイパスしたりすることができます。攻撃者が資格情報にアクセスすると、それを使用するのにそれほど時間はかかりません (通常は数時間以内)。

IAM ポリシーとツールはクラウド セキュリティへの取り組みの重要なコンポーネントですが、他のツールや分析と組み合わせて使用する必要があります。

マルウェアはクラウドをターゲットにしないため、AI ベースのクラウド セキュリティ ソリューションは必要ありません

05

信念

- マルウェアは主に Windows を実行しているユーザー マシンに影響を与えます。
- マルウェアを引き起こすクラウド内のフィッシング リンクをクリックする人は誰もいません。

現実

- マルウェアはますますクラウドの問題となり、クリプトジャッキングが好まれる攻撃となっています。マルウェアをリアルタイムで検出するには、AI ベースのソリューションが必要です。

近年、クラウドを中心としたマルウェアやフィッシング攻撃が急増しています。2023 Qualys TotalCloud Security Insights データによると、クラウド資産に対する 2 つの最大の脅威はクリプトマイニングとマルウェアです。どちらも環境への足がかりを提供したり、横方向の移動を容易にしたりするように設計されています。特に、サイバー犯罪者がクラウド システムで利用可能な膨大なコンピューティング リソースを悪用しようとするにつれて、クラウド サービスに対する非常に儲かる暗号ハッキング攻撃がより一般的になりました。

マルウェアはクラウドに影響を与えないという考えは、マルウェア感染の従来のベクトル (最も一般的なものはフィッシングメール) に注目しているために生まれました。

ただし、クリエイティブなハッカーは、他の多くの経路を使用してクラウド システムにマルウェアを注入し、クラウド サービス、設定ミス、脆弱性、安全でない管理コンソールを悪用する可能性があります。エンドポイント保護プラットフォーム（EPP）やエンドポイント検出と対応（EDR）などの従来の脅威検出ソリューションはクラウドネイティブではなく、動的なクラウド環境で拡張できないソフトウェア エージェントを必要とします。したがって、セキュリティ チームが開発から実行時まで既知と未知の両方のマルウェアを検出し、ステルス攻撃を防止し、クラウド侵害のリスクを軽減できるように、AI ベースのクラウド セキュリティ ソリューションが必要です。組織のユーザーがクラウドにマルウェアを仕込む犯人である可能性もあります。
イネーブラーは、ユーザーが感染したファイルをクラウド環境にアップロードできるようにする任意のクラウド サービスです。クラウド サービス プロバイダーは通常、特定の構成設定で指示されない限り、ストレージ バケット データをスキャンしてマルウェアを検出しません。セキュリティ チームにとって、マルウェアがクラウドに侵入する前に阻止することが不可欠です。
クラウドベースのマルウェア感染のその他の原因には、変異する Linux マルウェア（ほとんどのクラウド サービスは Linux ベースです）や仮想マシン内の Windows コンテナの感染などがあります。

スナップショットスキャンで十分です

06

信念

- スナップショット スキャンは、特に一時停止したワークロードをスキャンする機能とその効率性が宣伝されているため、クラウドの脆弱性をスキャンするための「十分な」方法であると認識されています。

現実

- スナップショット スキャンには利点もありますが、万能のソリューションではありません。エージェントベース、ネットワークベース、API ベースの評価など、さまざまなスキャン技術により、さまざまなユースケースやワークロードをより包括的かつ継続的にカバーします。

進化し続けるクラウド セキュリティの状況では、スナップショット スキャンなどの 1 つのスキャン方法だけに依存するのは限界のあるアプローチです。スナップショット スキャンは、一時停止したワークロードの調査など、特定のシナリオに大きな利点をもたらしますが、セキュリティ スキャンのすべての側面において単一のテクノロジーが最高の地位を占めるわけではないことを認識することが重要です。堅牢なクラウド セキュリティの鍵は、スキャン テクノロジーを組み合わせて活用することにあります。
たとえば、エージェントベースの評価は、長時間実行されるワークロードに最適であり、詳細かつ高精度の脆弱性検出を提供します。
一方、ネットワークベースのスキャンは、外部にさらされるワークロードや、厳しいコンプライアンス要件の下にあるワークロードには不可欠です。
さらに、API ベースの評価は、特に一時的なインスタンスがある環境では、初期スキャンに非常に効果的です。
この多面的なアプローチにより、システムの脆弱性をより包括的に把握でき、内部と外部の両方の脅威がカバーされます。また、さまざまなワークロードや環境の固有の特性に対応して、セキュリティポスチャーをより細やかに理解することも可能になります。さまざまなスキャン方法を統合することで、組織は幅広い脅威や脆弱性に対処できる、より回復力が高く適応力のあるセキュリティ フレームワークを実現できます。

SaaS ベンダーは、SaaS アプリケーションのセキュリティとコンプライアンスのあらゆる側面を管理します

07

信念

- セキュリティとコンプライアンスのあらゆる側面は、SaaS ベンダーによって完全に管理されます。

現実

- SaaS ベンダーは基盤となるインフラストラクチャとアプリケーション コードを保護する責任がありますが、組織は依然としてデータ、ユーザー アクセス、および SaaS 環境全体を保護する責任を負っています。

SaaS ベンダーがアプリケーションのセキュリティのあらゆる側面を担当してくれるという一般的な考えは危険な誤りです。ベンダーはインフラストラクチャとプラットフォームのセキュリティ保護において重要な役割を果たしますが、SaaS アプリケーション スタック全体のセキュリティポスチャーとリスクを管理する責任は企業自体に大きくあります。
SaaS ベンダーは基本的なセキュリティ対策を実装していますが、包括的な保護には十分ではないことがよくあります。堅牢な SaaS セキュリティポスチャーを構築および維持する責任は組織にあり、それは現代のビジネス運営にとって不可欠な側面となっています。組織は、機密データを保護し、業界規制へのコンプライアンスを維持するために、SaaS アプリケーションの保護に積極的に参加する必要があります。これには、ユーザー アクティビティの定期的な監視、データ アクセス権の管理、サイバー脅威に対する警戒が含まれます。組織は、設定ミスを特定して修正し、SaaS スタックのリスク プロファイルを理解し、セキュリティ慣行がベスト プラクティスおよびコンプライアンス ベンチマークと一致していることを確認することに積極的に取り組む必要があります。

クラウドのセキュリティを確保するには、左または右にシフトすることが最善の方法です

08

信念

- 開発中または納品後のセキュリティにさらに重点を置くことで、セキュリティ専門家は攻撃を阻止する最大のチャンスを得ることができます。

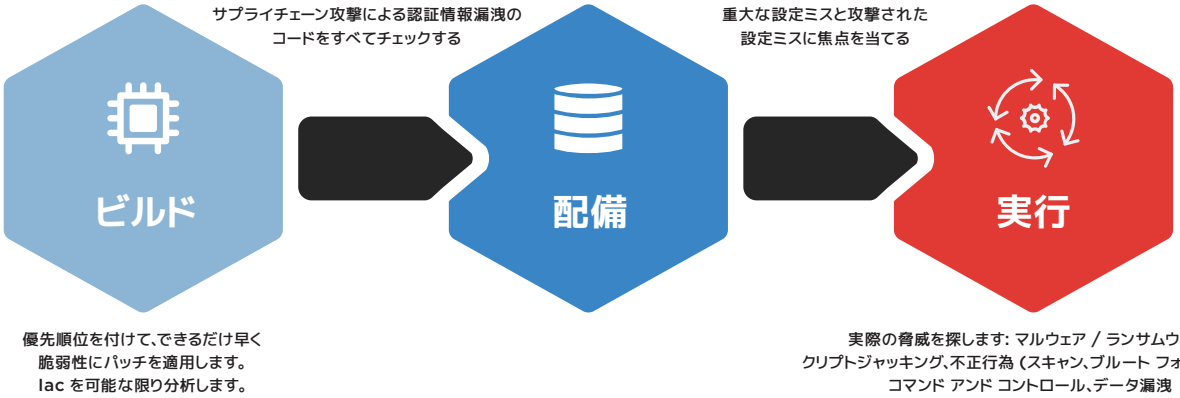
現実

- 攻撃はクラウド サービスのライフサイクルのあらゆる時点で発生します。

一般的なテクノロジーの信条は、企業はセキュリティへの取り組みをより効果的にするために「左にシフト」(ベンダーが提供するものによっては「右にシフト」)する必要があるというものです。これは、チームが開発またはリリース後のセキュリティ ツールを使用して、クラウド サービス サプライ チェーンのエンドポイントにもっと重点を置くべきであると言う派手な言い方です。しかし、これは見当違いで近視眼的なアプローチです。
攻撃者はクラウド サービスのサプライ チェーンのあらゆる部分を悪用しようとしますが、一端のみに焦点を当てると、企業は他の場所で脆弱なままになります。クラウド セキュリティへのフルスペクトラム アプローチは、上で説明した誤った問題のそれぞれに対処し、最善の徹底した防御を提供します。

Shift-leftやShift-rightは使用しないでください

ミドルパスはzenの徹底した守備につながる



リスクの優先順位付けは、単に一般的なCVE に対処することだけです

09

信念

- 蔓延している CVE の発見と修復に重点を置いているため、当社の脆弱性管理は良好な状態にあります。

現実

- リスクの優先順位付けは、脆弱性の悪用、資産の重要性、場所 (内部または外部) などの複数の要素に基づいて行う必要があります。

多くのセキュリティ専門家は、企業の IT 環境で検出された脆弱性のリストに悩まされています。マネージャーの典型的な反応は、「すぐに修正して、リストから消してください」です。脅威のリストが短いと関係者はより安心できるかもしれませんが、企業の危険にさらされる可能性はこれまで以上に高くなる可能性があります。最も無害な脆弱性が、有名な共通脆弱性と危険にさらされている(CVE)ほど重要ではないと思われたために残されたものであってもです。

真実は、すべての脆弱性が同じようにリスクがあるわけではなく、クラウド内のリスクは単なる加算的なものではなく、乗算的なものであるということです。脆弱性は、設定ミスと組み合わされ、インターネットへの露出によってさらに悪化すると、非常に大きな脅威にエスカレートします。この有害な組み合わせには、即時かつ優先順位の高い修復が必要です。最も深刻な脆弱性が世に出回っていても、価値の高い資産を脅かさない場合、または資産がインターネットに公開されていない場合は、クラウド環境にはまったく無関係である可能性があります。

それどころか、いわゆる軽微な脆弱性は、組織のクラウドネイティブインフラストラクチャ、アプリケーション、重要なデータを直接脅かす場合、核爆弾のような威力を持つ可能性があります。

こうした理由から、修復作業の順序と緊急性を適切に判断するには、環境に対するリスクに基づいて優先順位を付けることが不可欠です。

クラウドはランサムウェアからの安全な避難所です

10

信念

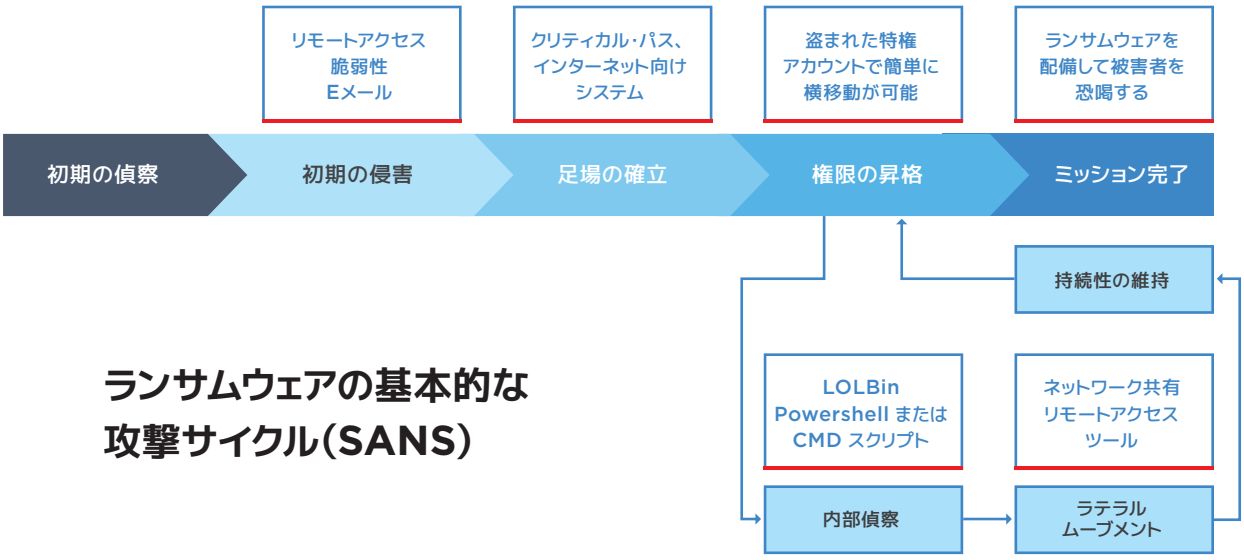
- 当社の IT 環境は、すべてをより安全なクラウドに移行したため、ランサムウェアの影響を受けません。

現実

- クラウド環境もオンプレミス IT と同様にランサムウェア攻撃に対して脆弱です。

ランサムウェアは被害者のデータを暗号化して使用できなくします。被害者の資産が凍結されると、攻撃者は、影響を受けたファイルを復号して回復するために必要なキーと引き換えに、通常はビットコインまたはその他の暗号通貨の形で支払いを要求する可能性があります。生産性の低下、ビジネスの損失、クリーンアップなどのコストが、実際の身代金を大幅に上回る可能性があります。

クラウド環境は攻撃サイクルが加速されることが多いため、特に脆弱です。サンドボックス分析やその他の分析などの従来の制御では、被害が発生してからずっと後になってから攻撃を特定することがよくあります。



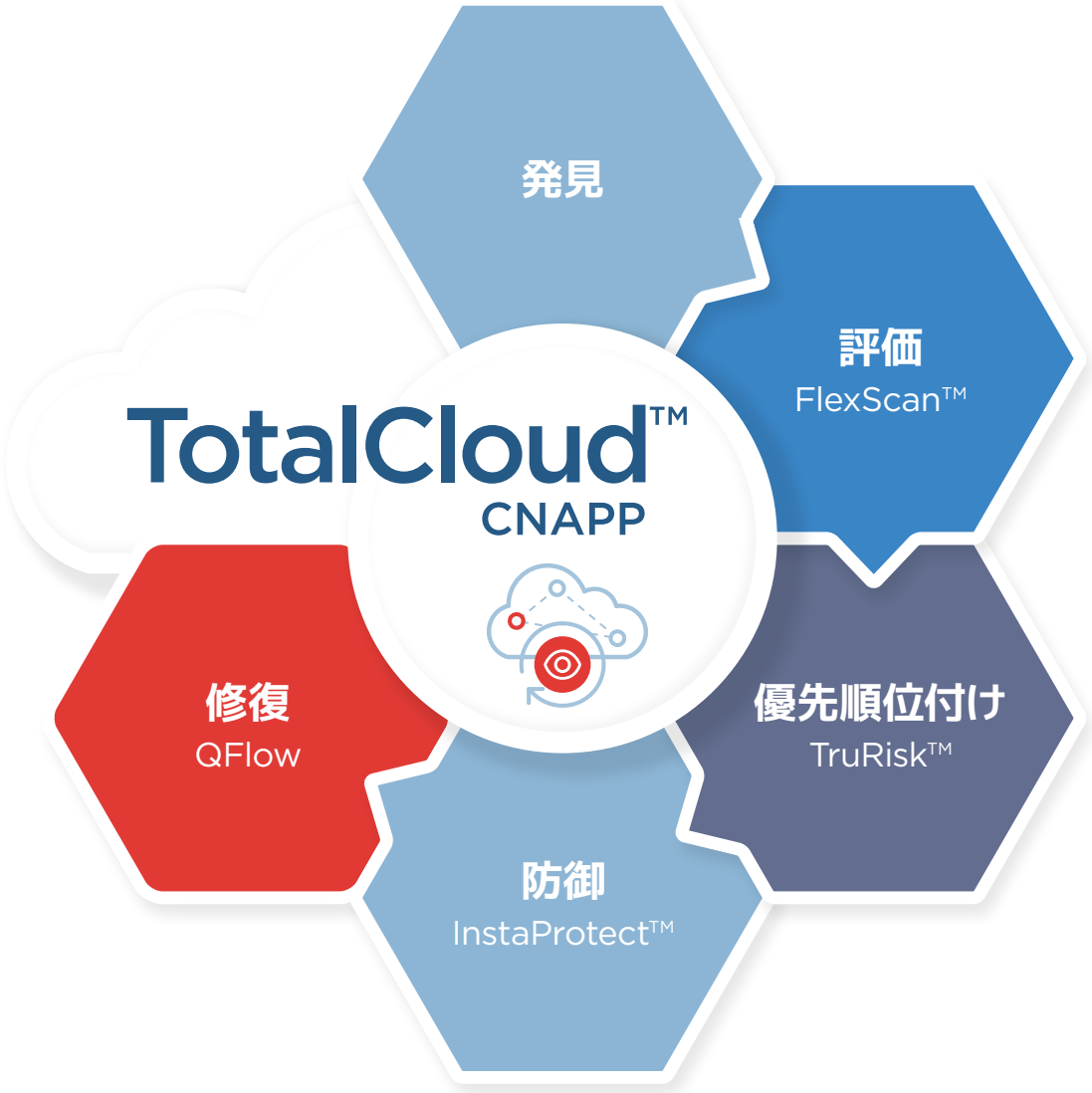
ランサムウェアの基本的な攻撃サイクル(SANS)

クラウド ランサムウェアの悪用を防ぐには、セキュリティにおける 2 つの重要な改善が必要です。
1 つは、マルウェアが進化してシグネチャを回避する場合でも検出する機能、もう 1 つはほぼリアルタイムの速度でマルウェアを検出する機能です。

結論

クラウド セキュリティは複雑な状況であり、クラウド サービスのライフサイクルのあらゆる段階で包括的なツール、ポリシー、取り組みが必要です。クラウド セキュリティ プログラムを最も効果的にするには、クラウド リスクを効果的に測定、伝達、排除できなければなりません。

TotalCloud は、AI を活用したクラウドネイティブ アプリケーション保護プラットフォーム (CNAPP) ソリューションであり、開発から実行時まで統合された脆弱性、脅威、ポスチャー管理を提供します。ハイブリッド環境全体のリスクを効果的に測定、伝達、排除し、クラウドネイティブおよび SaaS アプリケーションに包括的な保護を提供します。



Qualys TotalCloud は、コンピューティング資産、PaaS/IaaS リソース、Kubernetes、および SaaS アプリケーションのクラウド構成の誤りや非標準的な展開を継続的に監視および特定します。

Qualys TotalCloud は、クラウド フットプリントの 360 度ビューを実現するために、マルチクラウド環境全体にわたるサイバー リスクのエクスポージャに対する完全な可視性と洞察を提供します。API、スナップショット、エージェント、ネットワークベースのスキャン技術など、エージェントレス技術とエージェントの両方を利用した柔軟なスキャン機能を提供し、マルチクラウド環境における脆弱性を継続的かつ迅速かつ徹底的に可視化します。このアプローチは、脆弱性を迅速に特定するだけでなく、シックス シグマ (99.99966%) の精度を維持し、アラート疲労と侵害のリスクを大幅に軽減します。

Qualys TotalCloud は、設定ミス、ワークロードの重要度、脆弱性など、さまざまなソースからの重要な指標を集約し、それらをランサムウェア、マルウェア、およびエクスプロイトの脅威インテリジェンスと関連付けて、統合された実用的なデータを作成します。この単一のリスクの優先順位付けビューにより、組織はクラウド環境内の最も重大な脅威を迅速に特定して対処できます。

Qualys TotalCloud は、ディープ ラーニング AI を活用して、クラウド キル チェーン全体で既知と未知の両方のマルウェアをリアルタイムで検出し、開発から実行時までクラウド セキュリティを強化します。Qualys TotalCloud は新しいデータから継続的に自己学習するため、誤検知を特定する能力が強化され、セキュリティ チームの負担が軽減されます。さらに、Qualys は、効率的なチケット割り当てとオーケストレーションのための ITSM ツールの統合に加え、自動化されたワンクリックのカスタマイズ可能なソリューションを含む、さまざまな修復オプションを提供します。これらの機能により、運用タスクが簡素化され、脆弱性の管理が容易になり、コンプライアンス スコアが向上し、最終的にはクラウド侵害のリスクが軽減され、平均修復時間 (MTTR) が最小限に抑えられます。

これらの誤解についてさらに詳しく話し合いたい場合、またはクラウド セキュリティ体制を強化するための支援が必要な場合は、**セキュリティ専門家によるプライベート 1 対 1 のコンサルティングとセキュリティ評価をリクエストできます。**