



クラウド&コンテナセキュリティ: バイヤーズ・ガイド

包括的なクラウドセキュリティに不可欠な機能とツール



目次

- 1 [はじめに](#)
 - 2 [クラウドの現状](#)
 - 5 [クラウドおよびコンテナセキュリティに不可欠な10の機能](#)
 - 10 [CNAPPが現代のクラウドセキュリティの基盤である理由](#)
 - 13 [Qualysが選ばれる理由](#)
 - 14 [リソース](#)
-

はじめに

競合他社を凌ぐスピードでイノベーションを起こし、成長を遂げることでデジタル領域での優位性を確立しようと、多くの組織がクラウドへの移行を進めています。しかし、成功を収めている企業は、クラウドへの移行にはリスクが伴うことも理解しており、そうしたリスクを適切に管理・対応するためのツールや技術を導入しています。本ガイドでは、リスクを低減し、組織がクラウドの価値を最大限に享受できるよう、適切な技術を選定するための指針を提示します。



クラウドの現状

ビジネスがクラウド上の魅力的なサービスやアプリケーションと連携するにつれ、かつてないレベルの生産性を実現し得る、強力かつ新たな機能が利用可能になります。しかし、こうしたメリットには代償も伴います。接続が増えるたびに攻撃対象領域は拡大し、リスクも増大していくからです。

多くの組織が、自社のセキュリティ対策とクラウド環境で直面しているリスクとの間に乖離があることに気づき始めています。リソースが不足するセキュリティチームは、死角や断片化されたツール、そして完全には監視しきれないほど拡大する攻撃対象領域への対応に追われています。こうしたセキュリティ上の「隙間」の深刻さをチームが十分に認識していない場合でも、サイバー犯罪者はその実態を確実に把握しています。そのため企業には、生産性を損なうことなく、かつ脆弱な隙間を放置することなく、業務と資産を保護できるソリューションが求められています。



4社に1社以上（28%）が、過去1年間に自社がクラウドやSaaSに関連するデータ侵害の被害に遭ったことを認めました。

— [QUALYS | THE STATE OF CLOUD AND SAAS SECURITY REPORT](#)

マルチクラウドやハイブリッド環境に伴う多くの課題は、主に3つの重要な障壁に集約されます。

1. クラウドにおける攻撃対象領域の拡大

現在、クラウド環境は、コンテナ、サーバーレス、仮想マシン（VM）、データベース、その他外部に公開された資産など、多岐にわたるワークロードが混在する複雑なマルチクラウドやハイブリッド構成となっています。さらに、複数のクラウドサービスプロバイダーにまたがる膨大な数のサービスが利用されていますが、その多くは監視が不十分な状態にあり、何が真のリスクにさらされているのかを把握しにくくなっています。実際、自社の攻撃対象領域を完全に可視化できていると考えている組織は、[わずか9%](#)にとどまります。

2. 可視性の危機

セキュリティインシデントの[80%近くは](#)、未知の資産や管理されていない資産に起因しています。リスクを統合的に把握できなければ、セキュリティチームは個々の事象の関連性を結びつけることが困難になります。その結果、戦略的な対応ではなく場当たり的な対応に追われることになり、優先度の低い「ノイズ」に紛れて、真の脅威や脆弱性が見過ごされてしまう恐れがあります。

3. コスト上昇とコンプライアンスの断片化

クラウドの複雑化は、セキュリティリスクと運用コストの両方を押し上げています。PCI DSS 4.0、HIPAA、ISOなどのコンプライアンスフレームワークが急速に進化する中、マルチクラウド環境やコンテナ環境全体で継続的なコンプライアンスを維持することは、特に連携していない個別ツールを使用している場合、多大なリソースを必要とします。多くの組織は、脆弱性スキャナー、CSPM ツール、IDガバナンスプラットフォーム、サードパーティ製自動化ツールなどを寄せ集めざるを得ず、結果としてギャップや非効率性が生じ、TCOが急激に上昇しています。その結果、支出の増加、リスクの増大、そしてコントロールの低下という事態を招いています。



クラウド利用におけるチームの課題

- クラウドおよびホスティング環境の可視性の欠如
- 攻撃対象領域の拡大
- 絶え間なく続く高度な脅威
- 最適なリソースや自動化されたワークフローの不足
- 過剰なアラート
- クラウド環境の複雑さ
- クラウド制御の設定ミス
- 未修正の脆弱性
- クラウドの一時的な性質
- 責任共有モデル
- コンプライアンスの維持
- 熟練したセキュリティ人材の不足
- クラウドおよびSaaSのコスト非効率性
- システムの信頼性



それらの課題を解決するために必要なもの



すべてのワークロード、サービス、環境にわたる可視性を統合する単一のプラットフォーム



最も重要なものに優先順位を付ける、リスクベースの脆弱性管理



ゼロトラストの原則に準拠した、組み込み型のコンテナおよびKubernetesセキュリティ



修復のための自動化されたワークフローとプレイブック



振る舞い分析と攻撃パスの追跡による、多層的な脅威保護



ビルドからランタイムまで可視性を確保し、開発者がすぐに利用できるセキュリティ



リアルタイムの監査対応力を備えた、継続的なコンプライアンスの徹底



従来のIAMの枠組みを超えた、IDを認識する制御機能



DevOpsライフサイクル全体にわたるリスクを関連付ける、コードからクラウドに至るトレーサビリティ



統合されたリスクスコアリングによる、APIおよびAI/LLMワークロードへの包括的な保護



クラウドおよびコンテナセキュリティに不可欠な10の機能

サイロ化されたレガシーなツールでは、今日のクラウドネイティブ環境やハイブリッド環境の要求に対応できません。相互に関連し合うワークロード、API、アプリケーション、IDが複雑に絡み合う環境においては、単なる可視化にとどまらず、設定ミス、脆弱性、権限、接続されたエンドポイント、ランタイムの挙動などを相関的に分析する、より統合的なアプローチが求められます。断片的な情報だけでは真のリスクが見えにくくなるうえ、迅速な対応ができなければ（特に本番環境で発生する脅威に対して）、重要な資産が危険にさらされる恐れがあります。

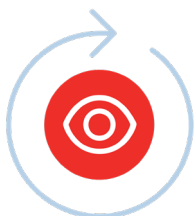
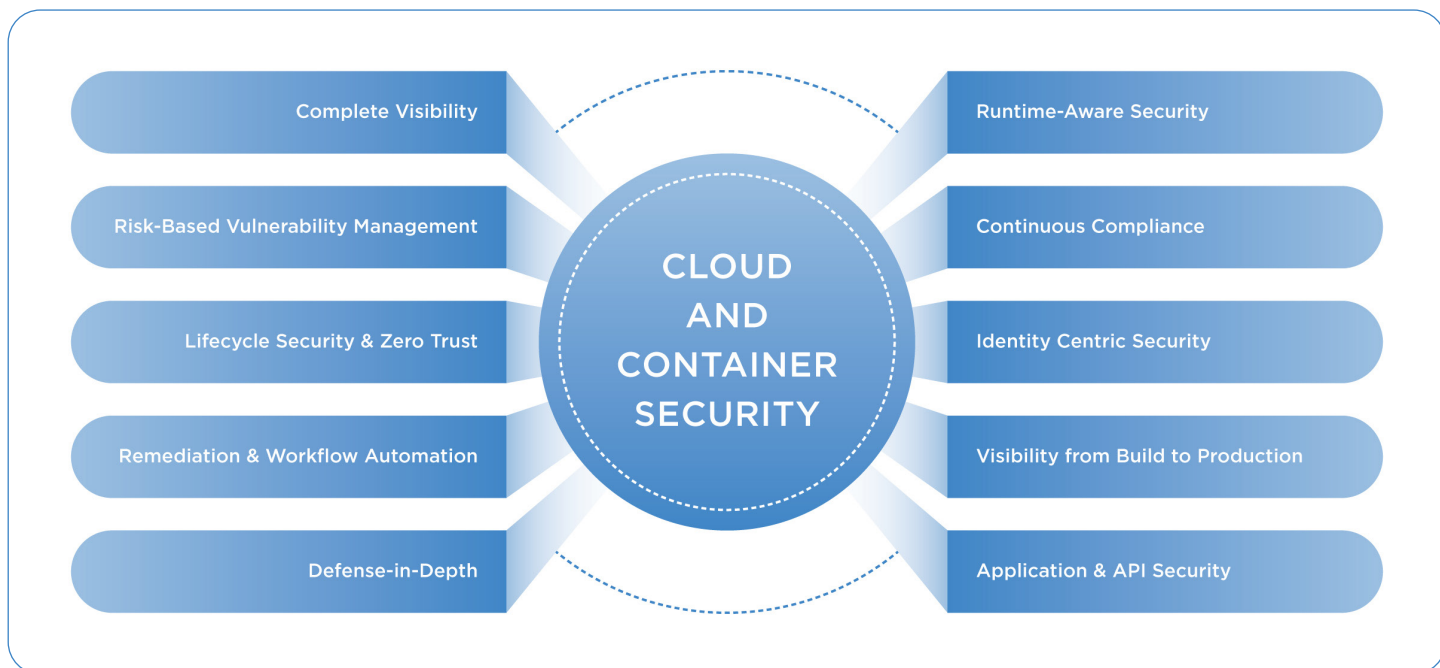
シームレスな修復が可能な、統合型かつコンテキストを認識するセキュリティプラットフォームへの進化は、現代の環境を保護する上で不可欠な転換を反映しています。

組織が導入を検討する際、効果的なクラウドおよびコンテナセキュリティソリューションには、これら9つの基本機能が包括的なアーキテクチャに統合されている必要があります。それにより、セキュリティチームは進化し続けるクラウドの脅威に対して先手を打つことが可能になります。



昨年、28%の組織がクラウドやSaaSにおけるデータ侵害を経験しました。そのうち3分の1以上が、複数回にわたって被害を受けています。

— [DARK READING STATE OF CLOUD & SAAS SECURITY REPORT](#)



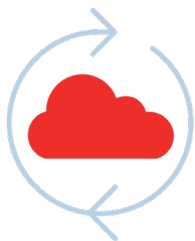
クラウドワークロードとサービスを完全に可視化

A包括的なCNAPPソリューションは、AWS、Azure、GCP、OCI、Red Hat OpenShift など、あらゆるクラウド環境にわたる統合的な可視化を実現します。VM、コンテナ、サーバーレス関数、データベース、マネージドサービスといったあらゆるリソースタイプを網羅し、それらを正規化することで、クラウドプロバイダーを問わず一貫したインサイトを提供します。死角を排除するため、CSP API経由でのエージェントレスなリソース検出を行うと同時に、脆弱性、ネットワークの露出状況、ID、マルウェア、シークレット、機密データに関するリアルタイム情報を活用して可視化を強化します。その結果、セキュリティチームはリスクの全体像を把握し、即座に対策を講じることが可能になります。



多角的な優先順位付けに基づくリスクベースの脆弱性管理

すべてのリスクが同等に重要であるわけではなく、それらを一律に扱うことは、貴重な時間とリソースの浪費につながります。多角的なリスクの優先順位付けでは、脆弱性の深刻度に加え、実際の悪用可能性、資産の重要性、実行時のコンテキスト、脅威インテリジェンスを組み合わせることで、真に対処すべき問題を浮き彫りにします。これらの情報を統合してリスクスコアや攻撃パスとして可視化することで、セキュリティチームは「ノイズ」に振り回されることなく、ビジネスに実質的なリスクをもたらすごく一部の脆弱性に注力できるようになります。このアプローチにより、修復までの平均時間（MTTR）が短縮され、最も大きな効果をもたらす領域に確実にリソースを集中させることが可能になります。



コンテナおよびKubernetesにおけるフルライフサイクル・セキュリティとゼロトラスト

コンテナとKubernetesは優れた俊敏性をもたらす一方で、攻撃対象領域が急速に変化する環境でもあります。こうした環境でゼロトラストを実践するには、CI/CDでのイメージスキャン、デプロイ前の構成や依存関係の検証、さらにはアドミッションコントローラーやドリフト検知によるランタイムポリシーの適用に至るまで、ライフサイクル全体にわたる可視性と制御が不可欠です。成熟したCNAPPは、脆弱性や設定不備を早期に特定するだけでなく、信頼できるワークロードのみを本番環境で稼働させ、デプロイ後の予期せぬ挙動を検知し、悪意ある動作をリアルタイムで阻止する機能を備えている必要があります。EKS、AKS、GKE、OpenShiftのいずれを利用する場合でも、組織には、ワークロードID、ロールベースのアクセス制御（RBAC）ポリシー、クラスターレベルのセキュリティポスチャーと整合性の取れた、一貫性のあるコンテナセキュリティが求められます。これにより、現代のKubernetes環境において、ラテラルムーブメント、権限の悪用、サプライチェーンリスクを防ぐために必要なガードレールと可視性が確保されます。



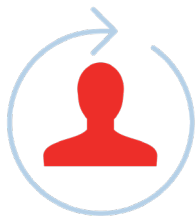
コンテキストに応じた修復とワークフローの自動化

リスクの特定は、あくまで出発点に過ぎません。真の価値は、迅速かつ正確で、拡張性のある修復を行うことで生まれます。包括的なCNAPPは、自動化されたワークフローによって「ラストワンマイル」の課題を解消し、手作業を削減しつつ、一貫した対応を確保する必要があります。これには、クラウドネイティブAPIとの連携による設定ミスや脆弱性の修復、CISA KEVなどのフレームワークに基づいたパッチ適用の優先順位付け、そしてランタイムのインサイトを含むコンテキストに即したガイダンスを開発者向けツールやチケット管理システムへ提供することなどが含まれます。あらゆる組織にシームレスに適合するためには、サードパーティ製システムとも連携可能な、柔軟かつカスタマイズ性の高い自動化機能が不可欠です。これにより、セキュリティチームは、自組織の運用ペースやコンプライアンス要件に合わせた対応策を構築できるようになります。



多層防御と未知の脅威への対策

パッケージに潜むクリプトマイナー（暗号資産マイニングツール）、ストレージを標的とするランサムウェア、公開されたコンテナやIAMロールを悪用したデータ流出といったクラウドネイティブな脅威に対抗するには、多層防御戦略が不可欠です。堅牢なCNAPPには、スタック全体にわたるシグナルを相関分析する能力が求められます。具体的には、CloudTrailやVPCフローログといったクラウド上のアクティビティと、eBPFやエージェントによる詳細なランタイム可視化情報を結びつけ、脅威がクラウドからクラスター、そしてコンテナへと移動する動きを検知する必要があります。従来のツールでは見逃されがちなゼロデイ攻撃、長期にわたる潜伏（ロング・ドウェル・タイム）、サプライチェーンにおける異常などを特定するには、ディープラーニングや行動分析が鍵となります。さらに重要なのは、単なる検知にとどまらず、悪意あるプロセスの停止、ホストの隔離、ファイルアクセスの制限、公開されたセキュリティグループの閉鎖といった自動応答アクションを実行できることです。これにより、チームは迅速に行動し、脅威が深刻化する前に封じ込めることが可能になります。



ランタイム情報を活用したセキュリティによる 開発者との協調体制の構築

修復作業を真に加速させるには、セキュリティは開発者の「敵」ではなく「味方」として機能する必要があります。つまり、単に何百ものCVE（共通脆弱性識別子）を開発者に押し付けるのではなく、ランタイム（実行環境）での知見を活かして「本当に重要な問題」だけを提示するような「シフトレフト」が求められます。優れたCNAPPIは、AWS CodeBuild、Azure DevOps、Google Artifact Registryといった各クラウドプロバイダー（CSP）のツールや、GitHub、GitLab、Jenkins、JFrog Artifactoryなどのサードパーティ製ツールと連携し、開発者のワークフローに直接組み込まれます。そして、実際のランタイムリスクに基づいた、具体的かつ実行可能なガイダンス（何を修正すべきか、なぜ重要なのか、どのパッチを適用すべきか）を提供します。セキュリティのガードレールは柔軟である必要があり、イノベーションを阻害することなくポリシーを適用しなければなりません。これには、新たに公表された脆弱性やパッチ適用が不可能なリスクに対する、ランタイム情報を考慮した例外処理や、環境に応じた適用範囲の調整（本番環境では厳格な制御、開発環境ではより緩やかなルールなど）が含まれます。その結果、ノイズではなく、コンテキストと協調に基づいた開発者体験が実現します。これにより、摩擦を生むことなく、より迅速かつ効率的な修復作業が可能になるのです。



常時稼働するコンプライアンス監視と監査への備え

クラウド環境における継続的なコンプライアンスの維持には、単なる「ある時点でのスキャン」以上の対応が求められます。環境のあらゆるレイヤーにわたり、リアルタイムでの可視化、ポリシーの強制適用、そして監視を行う必要があるのです。従来の監視エージェントでは、クラウドのコントロールプレーンやKubernetes APIレイヤーといった領域の死角を見落としがちであり、こうした場所で設定ミスや構成の乖離（ドリフト）が生じ、密かにリスクを招く恐れがあります。PCI DSS 4.0のように、ホストとコンテナ双方の継続的な監視を義務付ける規制要件が進化する中、ファイル整合性監視（FIM）やKubernetesセキュリティポスチャ管理（KSPM）といった機能は不可欠となっています。包括的なCNAPP（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）は、AWS、Azure、GCPにまたがる設定の監査を行うだけでなく、環境（開発環境と本番環境など）に応じたカスタムポリシーの適用や例外処理への対応、さらには大規模環境での一貫したガバナンスの確保を実現します。これにより、チームはリスクを積極的に低減しつつ、コンプライアンスの遵守を確実に証明できるようになります。



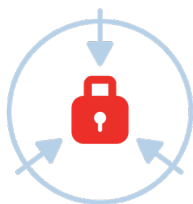
IAMの枠を超えた、アイデンティティ中心のセキュリティ

クラウド環境においては、インフラストラクチャではなく「アイデンティティ」こそが新たな境界（ペリメーター）となります。人間やマシンによるアイデンティティが数千規模に及ぶ中、過剰な権限やラテラルムーブメントのリスクが見過ごされてしまうケースが少なくありません。包括的なCNAPPには、CIEMの機能が不可欠です。CIEMは、権限を継続的に分析して「パブリックアクセスと管理者権限の組み合わせ」といった危険な構成を検出し、過剰な権限を持つアイデンティティを特定します。さらに、AWS、Azure、GCPにまたがるIAMポリシーと連携して「最小権限の原則」の適用を支援するとともに、リスク・役割・環境に応じてアクセス範囲を適切に制御するための明確な是正策を提示します。



「コードからクラウドへ」にわたる リスクの相関性とトレーサビリティ

クラウド侵害の主な原因は依然として人的ミスにあり、その多くは、安全でない設定や脆弱性のあるコードといった形で、開発ライフサイクルの初期段階で混入します。CNAPPは、ランタイムにおけるリスクやコンプライアンス上の問題を、IaC (Infrastructure as Code) 、アプリケーションコード、あるいはCI/CDの設定ミスといった根本的な原因と結びつける必要があります。IaCスキャンとSAST/SCAツールを組み合わせ、検出された問題をランタイムでのリスク（脅威への露出）と関連付けることで、セキュリティチームは、どのコード変更が実際にリスクをもたらしたのかを特定できます。ビルド時の設定ミスから本番環境への影響に至るまで、このようなエンドツーエンドの可視性を確保することで、より効果的な「シフトレフト」の実践が可能になります。これにより、開発者は問題の潜在的な影響範囲を明確に把握しつつ、早期に問題を修正できるようになります。



APIおよびAI活用型ワークロードのための統合セキュリティ

クラウドワークロードの保護は、単にインフラストラクチャを守るだけにとどまりません。攻撃者が実際に標的とするアプリケーションやAPIの保護も不可欠です。包括的なCNAPPは、ランタイム保護の対象をAPIやWebアプリケーションにまで拡大し、従来のWAFやインフラストラクチャ向けツールでは検知・阻止できないWebマルウェア、APIの悪用、ロジック攻撃といった脅威を特定・遮断する必要があります。これを実現するには、スタック全体にわたるシグナルを統合し、インフラストラクチャの脆弱性や設定ミスと、アプリケーション層でのエクスプロイト（悪用攻撃）、さらにはオンプレミスやクラウドのワークロード上で稼働するLLM（大規模言語モデル）との関連性をリアルタイムで把握しなければなりません。APIの挙動、ファイルアクセスパターン、インバウンドトラフィックを既知のリスクや脆弱性と相関分析することで、セキュリティチームは攻撃による被害が発生する前にそれを阻止するために必要なコンテキストを得ることができます。仮想マシンからコンテナ、API、そしてLLMに至るまでを網羅するこのフルスタック・アプローチにより、ビジネスを支えるサービスは、デプロイ時だけでなく、最も重要な局面であるランタイムにおいても継続的に保護されます。



CNAPPが現代のクラウドセキュリティの基盤である理由

今日の動的なクラウド環境を保護するには、手作業でつぎはぎした個別のツールだけでは不十分です。組織には、セキュリティポスチャ管理やコンプライアンスから、脅威の検知、そして迅速かつ自動化された修復に至るまで、エンドツーエンドのセキュリティを提供する**統合プラットフォーム**が必要です。この戦略の中核を担うのが**CNAPP (Cloud Native Application Protection Platform)**です。これは、クラウドセキュリティに不可欠なすべての機能を一つの包括的なソリューションに集約する、現代的なアプローチです。

CNAPPは、個別に導入された断片的なツールに頼るのではなく、ポスチャ（構成状態）やコンプライアンスの監視、ID保護、コンテナおよびKubernetesのセキュリティ、シフトレフト分析、API保護、そして資産の完全な可視化といった機能を**単一の管理画面**に統合します。これにより、チームはクラウドワークロード、SaaSアプリケーション、ハイブリッド環境のすべてにわたり、一貫した制御と可視性を確保できるようになります。

ガートナーが指摘するように、CNAPP製品は、単一の統合されたソリューションを通じて、クラウドネイティブ・アプリケーションのライフサイクル全体および多岐にわたる構成要素にわたるリスクを特定することを可能にします。これにより、運用が効率化され、精度が向上し、複雑さが軽減されます。

チームがCNAPPに基づいて連携しない場合、その影響は明らかです。

- 可視性の断片化と一貫性のない管理による**コンプライアンスリスクの増大**
- 重複するツールやワークフローによる**コスト増と非効率性**
- コンテキストのないアラートや断片的な検出結果による**セキュリティ担当者の疲弊**
- 修復における最終段階のギャップによる**対応時間の遅延とSLAの未履行**

最新のCNAPPは、自動化されたコンテキストを考慮した修復ワークフローをリスク管理プロセスに直接組み込むことで、こうした課題に対処します。開発者のパイプラインへの修正ガイダンスの提示、クラウドAPI経由での設定ミスの修正、あるいは本番環境におけるポリシーベースの制御の適用など、CNAPPはチームが重要な問題に対して迅速に対処できるよう支援します。

CNAPPは、CSPM、CWPP、KSPM、CIEMといった機能を統合することで、コードからクラウドに至るアプリケーションのライフサイクル全体にわたり、多様なワークロードを柔軟に保護します。

最新のCNAPPに求められる機能:

Cloud Security Posture Management (CSPM)

CNAPPの構成要素

CNAPPの主要な構成要素であるCSPMツールは、クラウド資産を継続的に検出・監視・分析し、設定ミスやベストプラクティスからの逸脱を特定します。リアルタイムのリスクに関する知見を提供することで、CSPMはクラウド環境における設定ミスやコンプライアンス違反を最小限に抑え、チームが迅速かつ確かな対応をとれるよう支援する、迅速かつ効果的な修復機能を実現します。

Cloud Infrastructure Entitlement Management (CIEM)

CNAPPの構成要素

CIEMは、主にクラウド環境におけるIDと権限の管理に重点を置いています。組織がクラウド上のIDを可視化できるようにするとともに、「最小権限の原則」（ユーザーに対し、業務遂行に必要な最小限のアクセス権限のみを付与すること）の遵守を徹底します。

Cloud Workload Protection (CWP)

CNAPPの構成要素

CWPP（Cloud Workload Protection Platforms）とも呼ばれるCWPは、クラウド環境全体にわたり、仮想マシン、コンテナ、サーバーレスアプリケーションといったワークロードを保護します。その主な目的は、脆弱性管理、ランタイム保護、および監視を通じて、クラウド上の資産であるランタイムインフラストラクチャやアプリケーションを保護することにあります。

Kubernetes and Container Security (KCS)

CNAPPの構成要素

KCSが提供するKubernetesクラスターおよびコンテナ化アプリケーション向けの高度な可視化機能とセキュリティ制御により、死角に潜む脆弱性のリスクを大幅に低減できます。セキュリティチームは、リスクが深刻化する前にそれを特定・対処することで、脆弱性や設定不備を早期に発見できるようになります。

また、コンテナランタイムセキュリティ機能では、eBPFの技術を活用し、悪意ある脅威、マルウェア、異常な挙動を検知して対応します。

Infrastructure as Code (IaC)

CNAPPの構成要素

IaCセキュリティツールは、開発の重要な段階においてセキュリティ上の欠陥が混入するのを防ぐのに役立ちます。これらのツールは、インフラストラクチャのコードをスキャンして設定ミスを特定し、IaCテンプレート内のセキュリティ上の不備の修正を支援するとともに、デプロイ前に潜在的なセキュリティ脅威を検出します。これにより、コードからクラウドに至るまで、リスクを適切に管理した運用が実現します。

Cloud Detection And Response (CDR)

CNAPPの構成要素

CDRは、あらゆるクラウド環境にわたり、リアルタイムの監視と脅威検知を提供します。チームは、アクティブなエクスプロイト（脆弱性悪用）やマルウェアといった悪意ある活動を迅速に特定・対処できるため、既知および未知の攻撃による潜在的な影響を低減できます。

Cloud Workflow Automation (CWA)

CNAPPの構成要素

プロセスを合理化し効率性を高めるために、CWAはクラウド環境をまたぐ一連のタスクやプロセスを連携させ、自動化を推進するとともに、不要な手作業を排除することを可能にします。

アプリケーションセキュリティ (ASPM)

ASPMは、コードからランタイムに至るまで、ソフトウェア開発ライフサイクル全体にわたり、アプリケーションセキュリティのリスクに対する継続的な可視化、相関分析、および制御機能を提供します。

SAST、SCA、DAST、クラウドランタイム環境などのツールから得られるデータを統合・分析することで、セキュリティチームは、悪用可能性やビジネスへの影響度に基づいて脆弱性の優先順位を付け、セキュリティポリシーを適用し、安全なコードのみを本番環境へリリースできるようになります。

Webアプリケーションスキャンおよびマルウェア検出 ASPMの構成要素

WebやAPIベースのアプリケーションは、攻撃者に最も狙われやすい標的の一つです。チームが感染を迅速に特定・修復できるよう、「Webマルウェア検出」機能ではディープラーニングを活用し、外部公開されているサイトをスキャンして、隠れたマルウェア、埋め込まれたスクリプト、悪意のあるコンテンツを検出します。

APIセキュリティ ASPMの構成要素

デジタルトランスフォーメーション (DX) の進展に伴い、イノベーションを推進する手段として、マイクロサービスやAPIの利用が拡大しています。現代的なアプリケーション開発を行う組織には、設定ミスや悪意のあるペイロードをリアルタイムで検知し、機密データやアプリケーションの整合性を保護する「APIセキュリティ」のようなソリューションが不可欠です。

AIセキュリティ

ASPMおよびCNAPPの構成要素

AIセキュリティおよびワークロード保護は、クラウドやオンプレミス環境全体にわたり、AI/LLMモデルとその基盤となるインフラストラクチャを保護することに重点を置いています。これには、脆弱性、設定ミス、コンプライアンス上の不備を特定するための、デプロイ済みモデルの可視化、リスク分析、およびポリシーの適用が含まれます。Amazon Bedrock、Azure AI、Hugging Faceといったプラットフォームの導入が進む中、こうしたAIワークロードのセキュリティ確保は、リスクポスチャーの管理、責任あるAI利用の保証、そしてソフトウェアサプライチェーンの完全性保護において極めて重要となっています。

アタックサーフェス管理 (ASM)

ASMは、組織が既知・未知を問わず、自社のデジタルフットプリント全体にわたる潜在的なリスクを特定、分析、および軽減できるよう支援します。組織内のあらゆるサイバー資産のインベントリ管理とリスク評価に重点を置き、絶えず変化する脅威の状況を継続的に監視・評価します。真のアタックサーフェス管理とは、より強固な脆弱性管理と修復を推進するための「リスクのコンテキスト」を組み込んだものです。

サイバーセキュリティ資産管理 (CSAM)

CSAMは、組織のハードウェア、ソフトウェア、クラウド資産を継続的に発見・監視・追跡・保護することで、セキュリティチームによるリスクのある資産の迅速な特定や複雑なIT環境の評価を支援します。また、ハイブリッド環境全体にわたるリスクを低減するためのタイムリーな対応を可能にします。強固な攻撃対象領域管理（アタックサーフェス管理）を実現するには、CSAMを「外部攻撃対象領域管理（EASM）」と組み合わせて運用することが推奨されます。

外部攻撃対象領域管理 (EASM)

サイバーセキュリティ資産管理 (CSAM) を補完する「外部攻撃対象領域管理 (EASM)」は、組織がその存在を認識していなかった可能性のあるインターネット公開資産を特定し、それらに関連するリスクを低減するのに役立ちます。こうした資産は外部の攻撃者から可視状態にあり、悪用される恐れがあるものです。



Qualysが選ばれる理由: あらゆる攻撃対象領域に対応する、リスクを重視したクラウドセキュリティ

クラウドセキュリティは複雑な領域であり、高度な機能が必要としますが、それらは効率的かつ円滑に提供される必要があります。Qualysは、現代のクラウド環境特有の複雑さに対処するために専用設計された、包括的かつ拡張性の高いセキュリティ機能を、効率的かつ大規模に実現します。

Qualysライセンスユニットを1つ購入するだけで、すべての機能をすぐに利用できます。すべての機能が有効な状態で、異なるユースケースや攻撃対象領域間でユニットを柔軟に再割り当てできるため、クラウドへの移行を加速させ、レジリエンスを強化することが可能になります。

Qualysのソリューションについて詳しくはこちら

[TotalCloud™](#)

TruRisk™と攻撃パスのコンテキストを活用し、コード、設定、ランタイムにわたる**クラウドのリスクを統合的に可視化**します。

自動化されたプレイブック、制御機能、ランタイムでの脅威緩和策を**組み込み、修復を支援**します。

[TotalAppSec™](#)

800万件以上: 統合・自動化されたワークフローにより、API、LLM、アプリケーションにわたる重大な問題を修正。

[CyberSecurity Asset Management](#)

比類なき可視性: 組み込みのEASM機能により、既知・未知を問わず、インターネットに公開されているすべての資産を特定します。

よりスマートなカバレッジ: ハイブリッド環境全体にわたり、リスクに基づくタグ付けと優先順位付けを行うことで、スキャン範囲を拡大します。

リソース

ケーススタディおよびレポート

[2025 Gartner® Voice of the Customer for Cloud- Native Application Protection Platforms](#)

[2023 Qualys TruRisk Threat Research Report](#)

[2024 Gartner® Market Guide for CNAPP](#)

[The State of Cloud and SaaS Security Report](#)

[Securing Dental Patient Data in the Cloud Customer Success Story](#)

ソリューション・ブリーフ

[VMDR and CyberSecurity Asset Management with External Attack Surface Management \(EASM\)](#)

[TotalCloud™ - The Risk-Minded CNAPP](#)

[The Good, the Bad, and the Ugly of Cloud-Native Application Protection Platforms \(CNAPPs\)](#)

eBooks

[The 6 Essential Must-Haves: Cloud-native Application Protection Platform \(CNAPP\)](#)

[5 Questions To Ask Your Cloud Security Provider Before It's Too Late](#)

ブログ

[Our Takeaways From 2024 Gartner Market Guide for Cloud-Native Application Protection Platforms \(CNAPP\): Insights and Market Evolution](#)

[Best Practices for Cloud Compliance](#)

[From Vulnerability Scanning to Risk Management: The Complete VMDR Advantage](#)

About Qualys

Qualys, Inc. (NASDAQ: QLYS) is a pioneer and leading provider of disruptive cloud-based Security, Compliance and IT solutions with more than 10,000 subscription customers worldwide, including a majority of the Forbes Global 100 and Fortune 100. Qualys helps organizations streamline and automate their security and compliance solutions onto a single platform for greater agility, better business outcomes, and substantial cost savings. Qualys, Qualys VMDR® and the Qualys logo are proprietary trademarks of Qualys, Inc. All other products or names may be trademarks of their respective companies.

For more information, please visit [qualys.com](https://www.qualys.com)