

TREND VISION ONE™

Cloud Security

ハイブリッドおよびマルチクラウド環境向けの包括的かつプロアクティブなクラウドセキュリティ

クラウドの安全を確保し、業務を簡素化

デジタル環境が急速に進化しつつある中で、クラウド環境は高度化した脅威に絶えずさらされています。組織は、重要な資産を保護し、コンプライアンスを維持し、ビジネスを加速するために、ハイブリッドおよびマルチクラウド環境の強力なセキュリティを確保する必要があります。

Trend Vision One™ Cloud Securityは、脅威を迅速に予測、防御し、対策を実施するために設計されたさまざまな機能を総合的に提供します。Cloud Securityは、AIや機械学習などの高度な技術と、リスクの可視化や管理、運用効率を向上させる Trend Vision One™ のCyber Risk Exposure Managementを活用し、セキュリティ担当部門による潜在的な脅威に対するプロアクティブな対策をサポートします。

Trend Vision One™で始めるプロアクティブなクラウドセキュリティ

AIを活用したエンタープライズサイバーセキュリティプラットフォームである Trend Vision Oneは、集中型のダッシュボードとして利用できます。Trend Vision Oneを利用することで、潜在的な脅威と攻撃経路に対するリアルタイムのリスク評価、エクスポージャー管理、監視、詳細な可視化が可能になります。予測型のモデル、プロアクティブなセキュリティ対策、機械学習、AIを活用して、潜在的な脅威を予測し、自動的に対処することができます。これにより、クラウドの脅威とエクスポージャーの包括的な管理が可能になり、脅威の検出および対応のための機能が統合されるため、セキュリティ担当部門の負担が軽減されます。

クラウドの脅威に対抗できる、さまざまな機能を搭載：

- Trend Vision One™ Cloud Risk Management
- Trend Vision One™ XDR for Cloud
- Trend Vision One™ Server and Workload Security (SWP)
- Trend Vision One™ Container Security
- Trend Vision One™ File Security
- Trend Vision One™ Code Security

主な効能：

- クラウドリスクを一元的に可視化
- クラウドリスクをプロアクティブに管理
- 業務効率を向上
- 既存のインフラストラクチャと円滑に連携
- コンプライアンス管理とコスト管理を簡素化

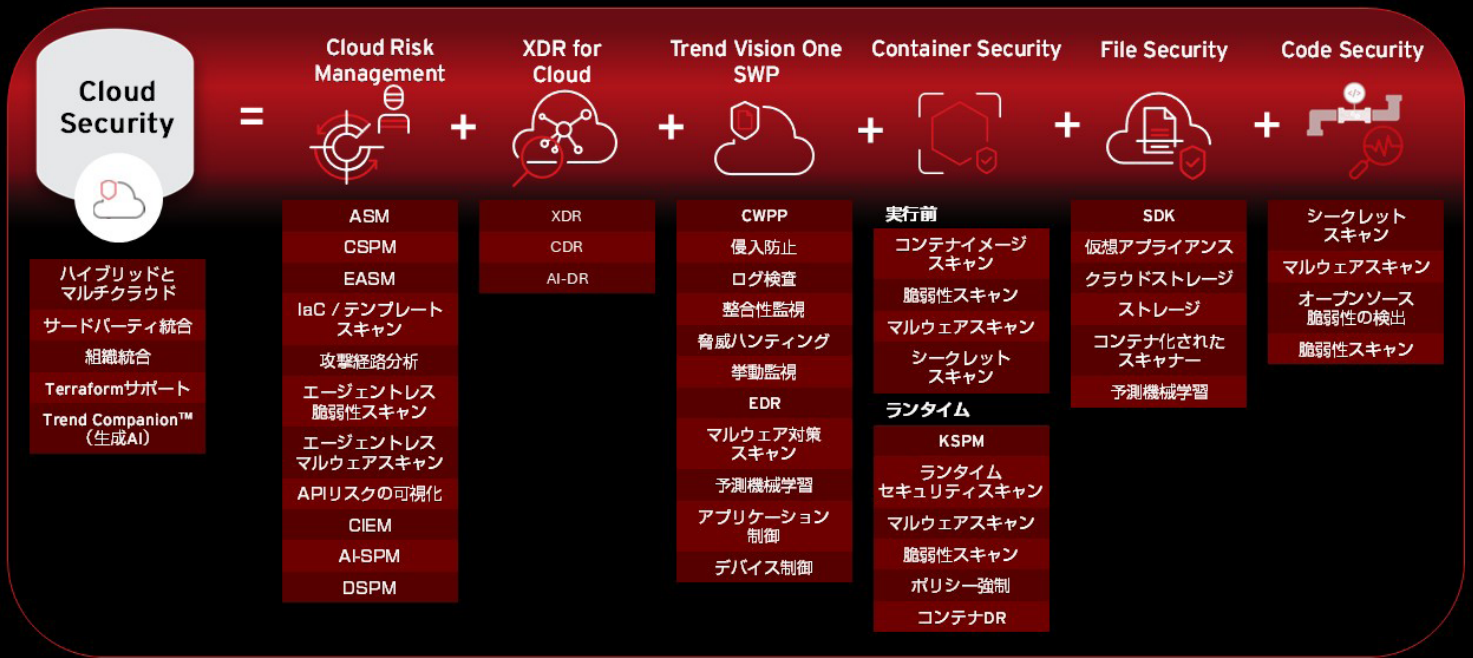


図1：Cloud Securityの概要

Cloud Risk Management

多くの組織が、拡大するクラウド環境を継続的に可視化しリスクを管理することに困難を抱えている結果、脆弱性への対応が遅れ、潜在的な攻撃手段となってしまう状況が散見されます。お客様のクラウドリスク状況全体のビューを提供するCloud Risk Management機能は、アタックサーフェス（攻撃対象領域）の検出、リスクの評価および軽減のための機能を提供し、リスクを効果的に優先順位付けして、対策を講じることができます。既存のセキュリティインフラストラクチャと円滑に連携することで、潜在的な脅威と攻撃経路をリアルタイムで監視し、詳細に可視化することができます。



図2：クラウドセキュリティに関する一般的な懸念

Cloud Risk Managementの機能：

- ・ 攻撃経路の予測
- ・ 全クラウドアカウントのリスクを一元的に表示
- ・ 継続的なリスク評価と優先順位付け
- ・ 脅威をプロアクティブに検出、軽減
- ・ コンプライアンスと報告
- ・ 幅広いエージェントレス機能

継続的なリスク評価と優先順位付け

- ・ EASM（External Attack Surface Management）：外部デジタル資産の脆弱性を監視
- ・ CSPM（Cloud Security Posture Management）：ベストプラクティスに準拠したクラウド構成を維持
- ・ CIEM（Cloud Infrastructure Entitlement Management）：クラウドのアクセス制御と権限を管理
- ・ DSPM（データセキュリティパスチャ管理）：機密性の高いクラウドデータを保護しコンプライアンスを確保
- ・ AI-SPM（AIセキュリティパスチャ管理）：強力なAIを活用して高度な脅威の検出とその軽減を実現

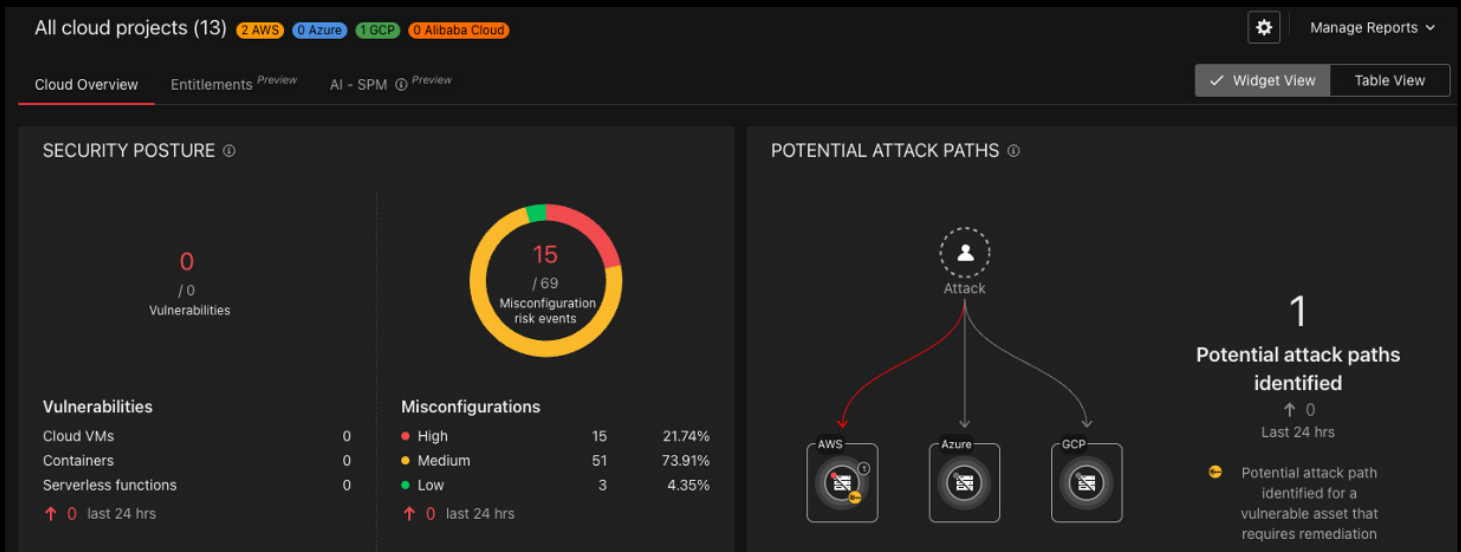


図3：Trend Vision Oneのクラウド概要の画面

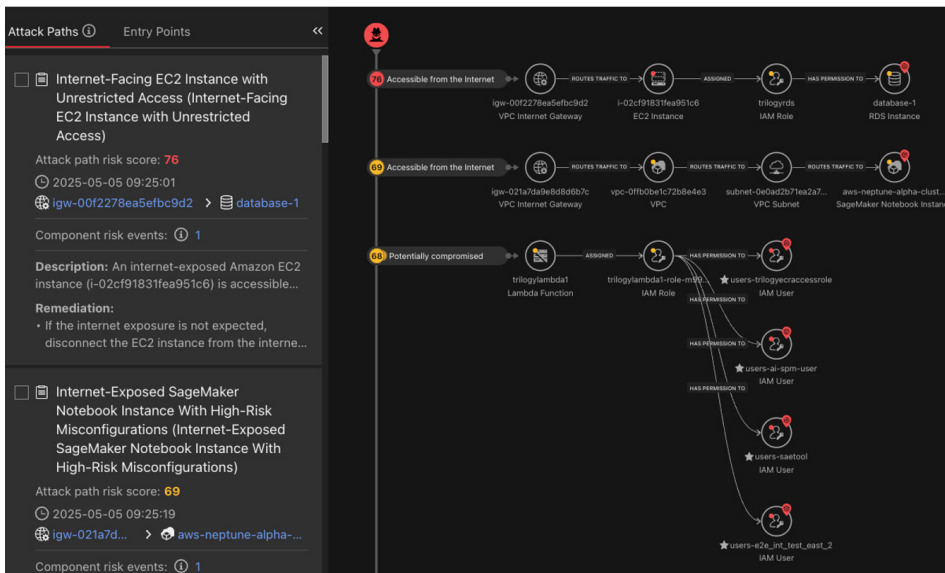


図4：Trend Vision Oneの攻撃経路概要の画面

お客様のクラウドのリスクを正確に把握

- すべてのクラウドアカウントに対する可視化を強化
- リスクをプロアクティブに特定して軽減
- 侵害される前に攻撃経路を予測
- 全体的なセキュリティの状態（ポスチャ）を改善

Container Security

コンテナ化された環境を開発から実装に渡るライフサイクル全体で保護することは難しく、特に開発と展開のペースが速い場合、本番環境に脆弱性が残る可能性があります。Container Securityの機能を使用することで、ビルドから展開、本番のランタイムまで、コンテナをライフサイクル全体にわたって保護できます。包括的な保護が可能になり、コンプライアンスが確保されるため、可視化を改善するとともに、プロアクティブなリスク管理が実現します。

Container Securityの機能：

- コンテナイメージの高度なスキャン機能で脅威を検知、対応
- ポリシーベースのアドミッション制御
- 実行前およびランタイムのコンテナ保護
- CI/CDパイプラインと円滑に連携

ビルドからランタイムまでのコンテナ保護

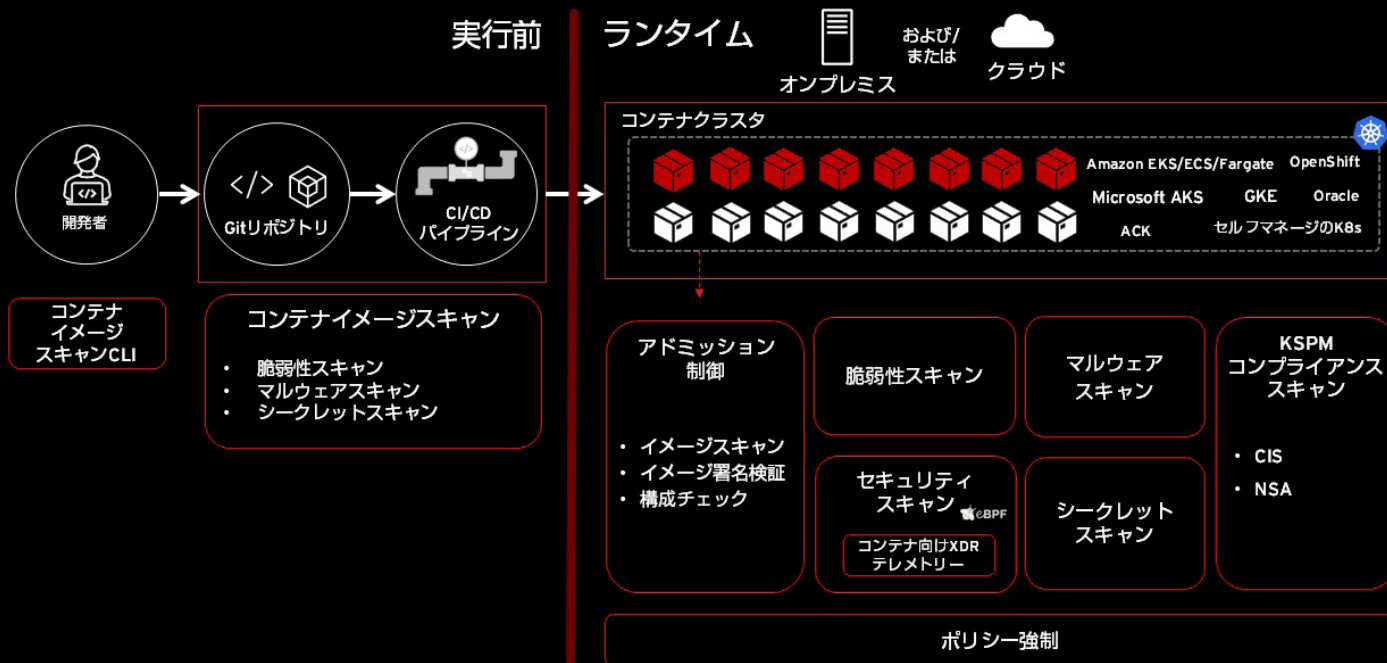


図5：Container Securityによる実行前からランタイムまでの保護の概要

実行前の保護

Container Securityは実行前の段階でコンテナイメージ内の脆弱性、マルウェア、シークレットをスキャンするため、本番環境まで到達する前に問題点を特定し、修正することができます。イメージスキャンの結果をアドミッション制御ルールとして使用することで、コンプライアンスに違反しているイメージの展開を防ぐポリシーを適用できます。

ランタイム保護

ランタイム環境では、脆弱性、マルウェア、シークレットを継続的に監視するとともに、プロセス、ファイル、ネットワークアクティビティを追跡してドリフトやアノマリーなどの悪意のある挙動を検出し、ルール違反を修正します。コンプライアンススキャンを定期的に行い、標準ベンチマークの順守を確認します。XDRとCloud Risk Managementによって強化されたTrend Vision Oneは、コンテナ環境の可視化と関係性の把握により、攻撃、リスク、脆弱性を優先順位付けし、迅速な対応を可能にします。

開発時からデプロイ時まで コンテナを保護

- コンテナのライフサイクル全体で継続的な保護を実現
- 本番環境展開前に脆弱性を排除
- セキュリティを開発プロセスに取り込み



図6 : File Securityの概要

File Security

クラウドファイルサービスやオブジェクトストレージサービスをマルウェアなどの脅威から保護することは非常に重要ですが、絶えず変化しデータがアップデートされるクラウド環境では対応が困難な場合が多く見られます。File Securityでは、クラウドのファイルおよびオブジェクトストレージサービスに対し、堅牢な保護を実装します。また仮想アプライアンス、SDK、コンテナ化されたスキャナーにより、オンプレミスのファイルストレージもサポートします。

File Securityはクラウドネイティブアプリケーションアーキテクチャを活かし、包括的なマルウェア対策を提供。加えてアップロードのたびに実行される自動ファイルスキャンによって、脅威を効果的に検出して軽減します。これにより、クラウド上のファイルをスキャンする場合でもオンプレミスのファイルをスキャンする場合でも、ファイルの安全性とコンプライアンスを確保することができます。

File Securityの機能:

- クラウドまたはオンプレミスでのマルウェア対策スキャン
- アップロードが実行されるたびにファイルを自動的にスキャン
- クラウドネイティブアーキテクチャとの統合
- 脅威をリアルタイムで検出して軽減

クラウドベースのファイルの円滑な保護

- マルウェアや脅威に対するリアルタイム保護を実現
- 自動スキャンを活用した円滑なセキュリティ対策
- 業界標準のコンプライアンス対応をサポート

Trend Vision One™ Server and Workload Security (SWP)

高度な脅威からサーバ、クラウドワークロード、コンテナを総合的に保護することは不可欠ですが、多様化し変化の激しいこのような環境では、作業の負担が大きくなります。高度な脅威に対するサーバ、クラウドワークロード、コンテナの対策を強化しましょう。Cyber Risk Exposure ManagementとXDR機能に支えられたTrend Vision One SWPは、重要な資産に対する総合的な保護機能を提供します。カスタマイズ可能なダッシュボードとリアルタイム監視を活用して、堅牢でプロアクティブなセキュリティ状態を維持しましょう。

サーバとワークロードの総合的な保護を実現

- 可視化とリスク管理の強化
- 高度な脅威検出と対応を実現
- 監視と制御を簡素化

Code Security

ランタイム環境展開前に脆弱性や脅威を排除するためには、開発プロセスの早い段階にセキュリティ機能を導入することが重要です。アプリケーションのライフサイクル全体で脅威を効率的に追跡しながら、開発、セキュリティ、運用の活動を統合することで分断された開発プロセスを統合し、部門間のコラボレーションを促進する手段が必要です。

Code Securityの利用により、CI/CDパイプラインに合わせて、開発プロセスの早い段階から、セキュリティ機能を導入できます。マルウェア、脆弱性、シークレットなどの脅威を可視化し、ランタイム環境への展開前に排除します。コードの作成時からクラウド展開まで、ライフサイクル全体でコードの安全性が確保されます。Trend Vision Oneを利用して可視化を継続し、開発中およびランタイム環境で得られる気づきを関係付けさせることで、ごく初期の段階からアプリケーションにセキュリティを組み込むことができます。

コードからクラウドまでのセキュリティ

- 脆弱性を早期に検出して修正
- 開発ワークフローと円滑に連携
- コード作成からクラウド展開まで、可視化を実現

Trend Vision One SWPの機能：

- ログ検査
- 変更監視
- 侵入防止
- 仮想パッチと推奨スキャン



クラウドポスチャツールは、設定ミス特定し、HIPAA、HITRUST、NIST Cyber Security Frameworkへの準拠を確実にするうえで欠かせない存在です。

Andrew Adams 博士
Xsolis社 情報セキュリティ
アソシエイトマネージャ



Code Securityの機能：

- CI/CDパイプラインとの連携
- 脅威の可視化と軽減
- コード内のマルウェア、脆弱性、シークレットを排除
- コード開発からクラウド環境まで、継続的な可視化

XDR for Cloud

クラウドの管理業務は複雑で負担が大きく、複数のセキュリティツールが分散し、誤検知の多さから、本当に重要な問題への集中が妨げられ、新たな脅威を見落としてしまうこともあります。XDR for Cloudは、クラウドネイティブインフラストラクチャのテレメトリから脅威を検出し、ノイズから明確な情報を引き出します。さまざまなクラウド環境と組織内のシステムといった複数のログを統合し、レイヤ全体の可視化とセキュリティを実現。セキュリティ担当部門は迅速かつ安全に拡張を進めることができます。

XDR for Cloudの機能：

- Amazon Security Lake、Microsoft Azure Monitorのアクティビティログ、AWS CloudTrail、仮想プライベートクラウド、コンテナ、エンドポイント、ネットワーク、コンピューティング、ストレージなどを含む、複数のログソースの統合
- IAM（IDおよびアクセス管理）における権限昇格、ポリシーロールバック、マスターパスワード変更の検出
- Amazon Simple Storage Service（Amazon S3）からのデータ流出、多要素認証の無効化などの検出
- 250以上の高度な検出モデルによる保護および対応処理の自動化

クラウドセキュリティの明確化を実現

- クラウドの保護と可視化を一元化
- ログ情報を対策につながる脅威データとして活用可能に変換
- 疑わしいクラウドアクティビティを簡単に検出して対応
- AIを利用して得た気づき（インサイト）で脅威ハンティングを強化

トレンドマイクロ製品

- IDとデータ
- クラウドワークスペース
- サーバ
- ワークロード
- コンテナ
- ファイルとオブジェクト
- ネットワーク

サードパーティ

- 脆弱性管理 (aws)
- 脅威インテリジェンス (A)
- ファイアウォール
- クラウド
- ゼロトラスト

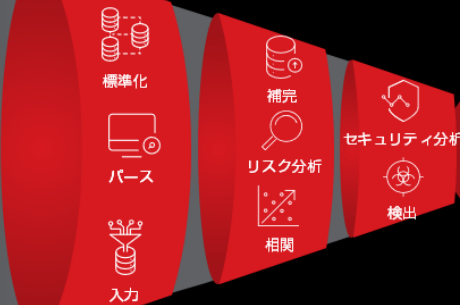


図7：XDR for Cloudの可視化と統合の概要



トレンドマイクロは、Cloud-Native Application Protection Platforms (CNAPP) の分野において **2024年の Gartner Peer Insights™ Customers' Choice** の1社と評価

The Forrester Wave™ : Cloud Workload Security, Q1 2024 にて強力なパフォーマーとして評価

IDC MarketScapeにて CNAPPにおけるリーダーとして評価



AI-Poweredエンタープライズ
サイバーセキュリティ
プラットフォーム



プロアクティブセキュリティ、始動。

Trend Vision Oneは、サイバーリスクの管理 (Cyber Risk Exposure Management)、セキュリティ運用 (Security Operations)、多層防御を一元化し、脅威の予測と防止をサポートする唯一のAI-Powered エンタープライズ サイバーセキュリティプラットフォームです。

トレンドマイクロについて

サイバーセキュリティの世界的なリーダーであるトレンドマイクロは、デジタルインフォメーションを安全に交換できる世界の実現に向けて取り組んでいます。Trend Vision One エンタープライズサイバーセキュリティプラットフォームは、数十年におよぶセキュリティ分野の知見、国際的な脅威研究、そして終わりのないイノベーションに基づき、AIを活用して50万以上の組織と、2億5,000万人以上の個人ユーザを、クラウド、ネットワーク、デバイス、エンドポイントなどのさまざまな環境で保護しています。

[TrendMicro.com](https://www.trendmicro.com)

**30日間の無料体験版を
お試しください**

[TrendMicro.com/trial](https://www.trendmicro.com/trial)

Copyright ©2025 Trend Micro Incorporated. All rights reserved. Trend Micro, Trend Microロゴ, t ボールロゴ, および Trend Vision Oneは、Trend Micro Incorporatedの商標または登録商標です。その他の会社名および製品名は、各社の商標または登録商標です。本書に含まれる内容は予告なしに変更される場合があります。Trend Micro, Trend Microロゴ, およびt ボールロゴは、米国特許商標庁に登録済みです。[SB06_Cloud_Security_Solution_Brief_250515US]
当社が収集する個人情報とその目的の詳細については、トレンドマイクロのWebサイトでプライバシーポリシーをご覧ください。 [trendmicro.com/privacy](https://www.trendmicro.com/privacy)