TrendAI™

TrendAI Vision One™ Cloud Security

～ 開発、配備（デプロイ）、ランタイムのライフサイクル全体を保護 ～

お客さまの課題

- クラウドを急速かつ広範囲で利用したい
- 設定ミス、脆弱性、権限過剰など、攻撃対象領域が守れない
- 結果として、侵害が発生してからの事後対応に忙殺されそう

クラウドアプリケーションの開発からデプロイ（配備）ランタイムまでの、ライフサイクル全体での予防、保護、対応する、CNAPP※への期待が高まっています。

※Cloud Native Application Protection Platforms

CNAPPの主な機能

CSPM (Cloud Security Posture Management)
クラウドインフラの設定ミス、AWS-Well-Architectedフレームワークなどのポリシー準拠の確認。

CIEM (Cloud Infrastructure Entitlement Management)
クラウド環境の権限過剰など、侵害につながる不適切なアクセス権限と特権を特定、管理。

CWPP (Cloud Workload Protection Platform)
仮想マシン、コンテナなどのランタイム監視、異常検出、迅速な対応を支援。

ASPM (Application Security Posture Management)
IaC※の設定ミスの検出、セキュリティテスト、ソフトウェア構成の解析と脆弱性の検知 ※Infrastructure as Code

KSPM (Kubernetes Security Posture Management)
コンテナイメージの脆弱性やセキュリティリスクを検出。

TrendAI Vision One™でまとめて管理、まとめて対策

保護できるAWS環境

AWS Colud

TrendAI Vision One™ Cloud Risk Management

AWS環境全体にわたるセキュリティポスチャから攻撃対象領域まで、包括的・継続的に可視化し、
脅威の予測・リスクの軽減策を管理

課題 ①

クラウドの設定が正しく設定されているのか、コンプライアンス要件に順守しているのか自信がない。

課題 ②

すべての資産を把握できないため、リスクの原因となる脆弱性や設定ミスなどを特定できない。

課題 ③

権限の種類が多いため、ユーザやアカウントに設定した権限がポリシーに準拠しているのか管理できない。また、突然、管理者権限が付与されたユーザによる不審な挙動があっても検知できない。

課題 ④

社員がAIサービスや新機能をAPIで利用しているが、リスクを把握できていない。AIサービスの悪用について知見がないため不正アクターによる侵入後の対応が取れない。

保護できるAWS環境

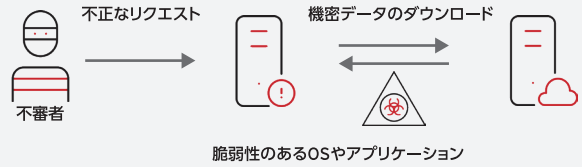
Amazon EC2　Amazon Work Spaces

TrendAI Vision One™ Endpoint Security

エンドポイントの防御力を高めるセキュリティ機能を単一エージェントに搭載し、多層防御/脆弱性対策を実現。
サーバ、クラウドワークロード、ランタイムコンテナにおけるセキュリティに対応

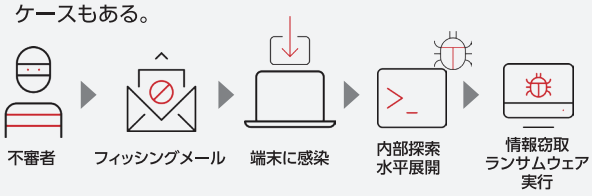
課題 ①

修正パッチを速やかに適用できず脆弱性が放置されている。



課題 ②

正規経路、正規なツールを利用した攻撃は検知・防御できないケースもある。



EPPやNGAV、脆弱性対策、EDR/XDRなどの機能でサイバー攻撃に対応

ネットワークセキュリティ

マルウェア対策

検出と対応（アクティビティ監視）

システムセキュリティ

TrendAI Vision One™ Container Security

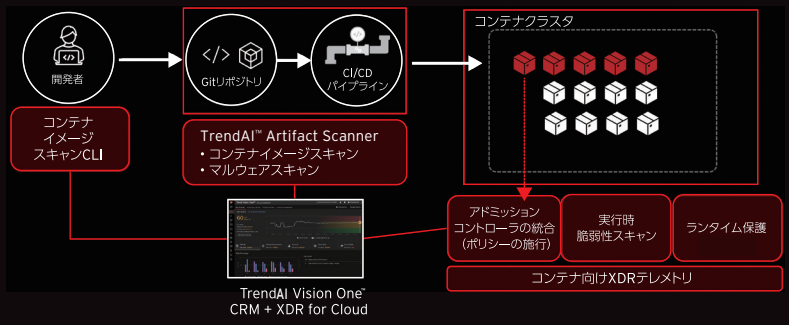
保護できるAWS環境

レジストリ内のコンテナイメージをスキャンして脆弱性や不正プログラムのリスクを可視化。
決められたポリシーベースでデプロイを制御、さらにランタイム環境の監視も一つの製品で実現

課題

コンテナ環境でセキュリティ対策を実施したいが、複数の製品を使わずシンプルに運用したい。

コンテナを用いたアジャイル開発環境に対してシフトレフトの組み込みが可能



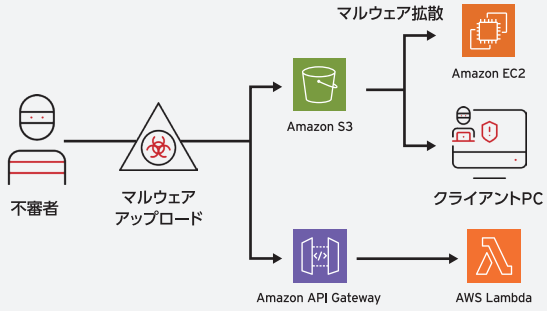
TrendAI Vision One™ File Security

保護できるAWS環境

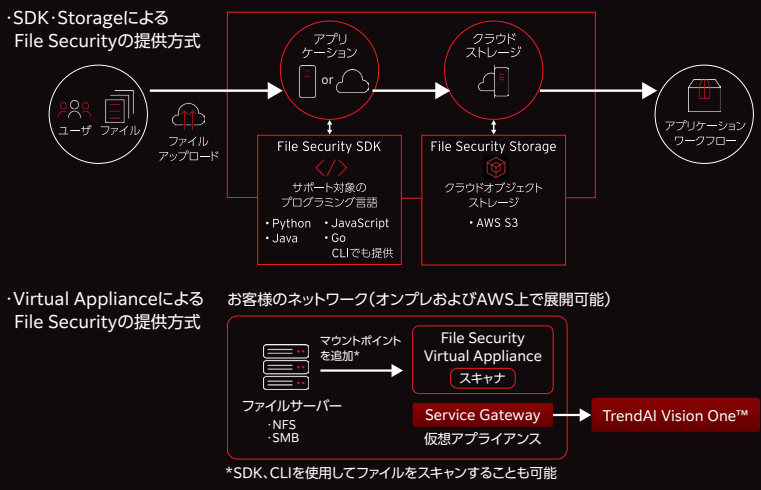
AWS環境上のファイル、オブジェクトサービスを自動でスキャンしアプリケーションやデータを保護。
サーバレスアーキテクチャやSDKなどご利用豊富な提供方法

課題

AWS環境にマルウェアが混入し、アプリケーションやファイルサーバーを通じて他サーバやユーザへ拡散するリスクをなくしたい。



ご利用環境に合わせてスキャン機能を組み込むことが可能



TrendAI Vision One™ XDR for Cloud
TrendAI Vision One™ Endpoint Security

保護できるAWS環境

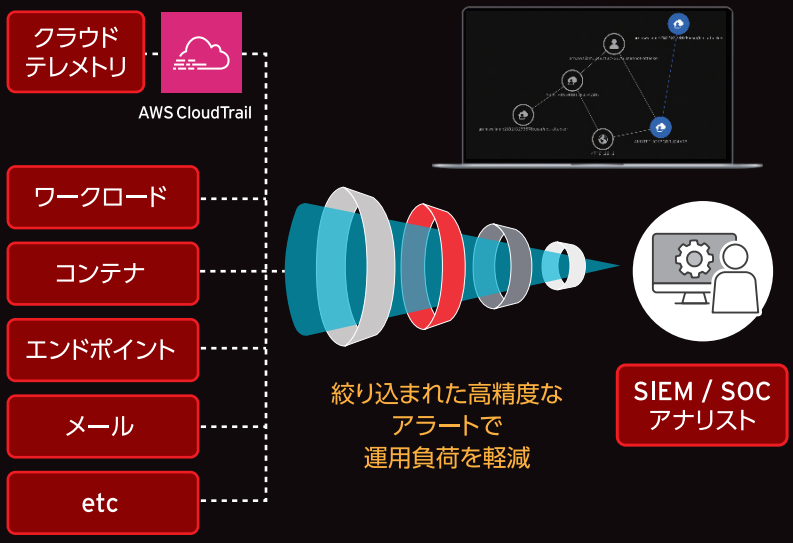
センサーから集約されたログを、MITRE ATT&CKやTrendAI™の脅威情報とマッピングし、
優先順位付けされた高精度なアラートにより、クラウド環境における迅速なインシデント対応を実現

課題 ①

有事の際、オンプレ、クラウド、メールなど影響範囲が分からない。

課題 ②

複数システムからの大量のアラートログにより、運用負荷が高くなり調査～対応まで難航してしまう。



TrendAI Vision One™のクラウドセキュリティ

TrendAI Vision One™ Cloud Risk Management

- ASM
- CSPM
- EASM
- CIEM
- AI-SPM
- DSPM
- IaC/ テンプレートの検索
- 攻撃経路の予測
- エージェントレス脆弱性検索
- エージェントレスマルウェア検索
- API のリスク可視化

TrendAI Vision One™ Server & Workload Protection

- CWPP
- 侵入防止
- ログの検査
- 変更監視
- 脅威ハンティング
- 挙動監視
- EDR
- マルウェア対策
- 予測型の機械学習
- アプリケーションコントロール
- デバイスコントロール

TrendAI Vision One™ Container Security

- コンテナイメージの検索
- 脆弱性の検索
- マルウェア検索
- シークレットの検索
- KSPM
- ランタイムセキュリティマルウェア検索
- 脆弱性の検索
- ポリシー強制
- コンテナの DR

TrendAI Vision One™ Code Security

- シークレットの検索
- マルウェア検索
- IaC/ テンプレートの検索
- ストレージ
- オープンソースの脆弱性の検知
- 脆弱性の検索

TrendAI Vision One™ File Security

- SDK
- 仮想アプライアンス
- クラウドストレージ
- ストレージ
- コンテナ化されたスキャナ
- 予測型の機械学習

TrendAI Vision One™ XDR for Cloud

- XDR
- CDR
- AI-DR

※記載内容は2026年2月時点での情報です。変更が入る可能性があります。

TrendAI™ トレンドマイクロ株式会社

本資料に関するご質問/お問い合わせは貴社の担当営業、
もしくは下記の法人お問い合わせ窓口までお問い合せください。
www.trendmicro.com/ja_jp/contact/contact-us.html?modal=1845cb

東京本社
〒160-0022
東京都新宿区新宿4-1-6
JR新宿ミライナタワー

名古屋営業所
〒460-0002
愛知県名古屋市中区丸の内3-22-24
名古屋桜通ビル7階

大阪営業所
〒532-0003
大阪府大阪市淀川区宮原3-4-30
ニッセイ新大阪ビル13階

福岡営業所
〒812-0011
福岡県福岡市博多区博多駅前2-4-2
H1O博多駅前 305号室