AWS Well-Architected フレームワークに沿ってCloud Oneがお手伝い出来る事

トレンドマイクロ株式会社
セールスエンジニアリング部
姜 貴日

姜 貴日 - Kwiil Kang

トレンドマイクロ株式会社
セールスエンジニアリング部
AWS Alliance Tech Lead

「Security Automation」、「DevSecOps」、 「Container」など
よりクラウドと親和性が高い領域に特化したソリューション提案を行う。

AWS Summit Tokyo 2019

JAWS DAYS 2020

トレンドマイクロ Webinar 2020

トレンドマイクロ
& New Relic共催セミナー

本日のゴール

AWS Well-Architected フレームワークを考えるにあたり

トレンドマイクロがどういったご支援が出来るのか弊社の

製品やサービス面含めご理解頂く。

トレンドマイクロについて

会社概要

Company Profile

Our Vision

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

A world safe for exchanging digital information

Our Mission

お客様のデジタルライフやITインフラを脅威から守る

Defend against threats that would impact user's digital life or IT infrastructure.

日本発の世界企業へ

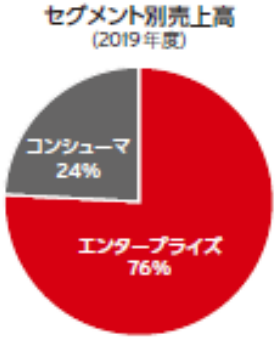
日本発のトレンドマイクロは、サイバーセキュリティのグローバルリーダとしてデジタル情報を安全に交換できる世界の実現に貢献します。私たちの革新的なソリューションはデータセンター、クラウド、ネットワーク、エンドポイントにおける多層的なセキュリティをお客さまに提供します。

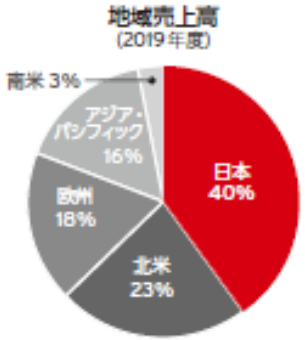
代表取締役社長
(CEO)
エバ・チェン

取締役副社長

大三川 彰彦

本社	東京（日経225に選出）
設立	1989年10月24日
資本金	188億2,200万円 (2019年12月31日付)
事業内容	コンピュータ及びインターネット用セキュリティ関連製品・サービスの開発・販売
社員数	6,854名 (2019年12月31日付)
売上高	1,651億9,500万円 (2019年12月31日付)

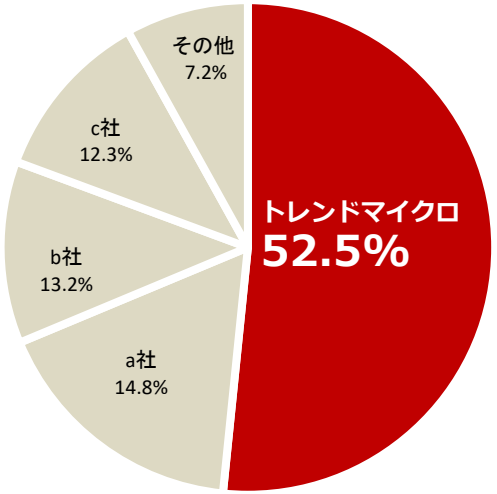




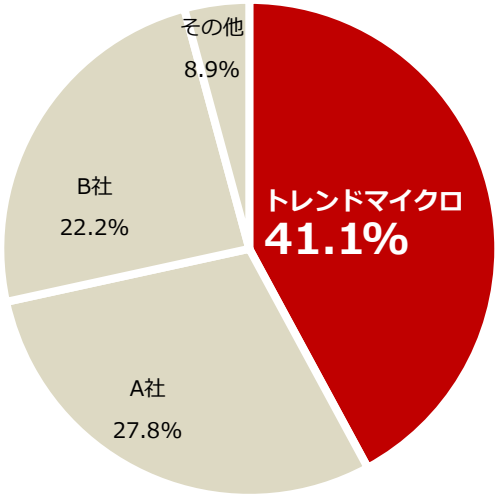
トレンドマイクロは
お客さまのセキュリティのベストパートナーです

企業向け製品
国内市場シェア 16年連続No.1※1

トレンドマイクロ製品は、(株)富士キメラ総研の調査で企業のサーバ/クライアント向けウイルス対策ツール、ゲートウェイにおけるウイルス対策ツールで16年連続※最も高いシェアを占めています。



サーバ/クライアント

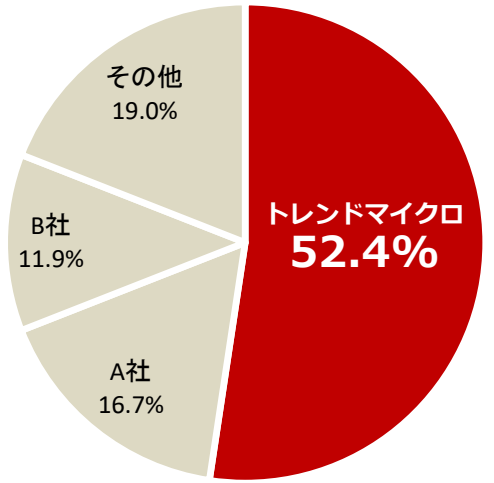


ゲートウェイ

※1 出典：（株）富士キメラ総研「ネットワークセキュリティビジネス調査総覧」2003～2018年度金額ベース（グラフは2018年度金額ベース）

企業向けサーバセキュリティ製品
国内クラウド向け市場シェア No.1※2

トレンドマイクロ製品は、(株)富士キメラ総研の調査で企業のクラウド向け市場のセキュリティツールにおけるサーバーセキュリティツールで最も高いシェアを占めています。



クラウド向け市場

※ 出典：（株）富士キメラ総研「2018 クラウドコンピューティングの現状と将来展望」2017年度見込金額ベース

トレンドマイクロのクラウド向けブランド – Trend Micro Cloud One

Trend Micro
Cloud One™

Trend Micro Cloud Oneとは

- 従来のクラウド向け製品および新規リリース予定製品の名称を揃え、統一されたブランド。
- IaaS環境 / コンテナ・サーバレスを用いたクラウドネイティブ環境 両方を保護。

～スローガン～

Cloud Security Simplified.
Automated. Flexible. All in One.

Cloud One AWS対応製品群

Trend Micro
Cloud One™

Trend Micro Cloud One

- **Workload Security**
  クラウドワークロードおよびコンテナの保護
  Amazon EC2 / Amazon Elastic Container Service / Amazon Elastic Kubernetes Service / AWS Elastic Beanstalk
- **Network Security**
  クラウド向けネットワークIPS
  Amazon VPC
- **Container Security**
  ビルドパイプラインでのコンテナイメージスキャン
  Amazon Elastic Container Registry
- **Application Security**
  サーバレスおよびアプリケーションの保護
  AWS Fargate / Amazon Elastic Container Service / Amazon Elastic Kubernetes Service / AWS Lambda
- **File Storage Security**
  クラウドストレージの不正プログラムスキャン
  Amazon Simple Storage Service
- **Conformity**
  クラウドの設定不備を可視化、コンプライアンス対応支援
  AWS Cloud

トレンドマイクロがご支援できること

トレンドマイクロがご支援可能な項目

(AWS Well-Architected Framework セキュリティのベストプラクティスより要約)

※以降、AWS Well-Architected FrameworkをAWS W-Aと記載

SEC1：
ワークロードを安全に運用するには

SEC2：
ユーザIDとマシンIDの管理

SEC3：
人とマシンのアクセス許可とその管理

SEC4：
セキュリティイベントの検出/調査

SEC5：
ネットワークリソースの保護

SEC6：
コンピューティングリソースの保護

SEC７：
データの分類

SEC8：
保管時のデータ保護

SEC9：
転送時のデータ保護

SEC10：
インシデントの予測、対応、復旧

＝トレンドマイクロがご支援可能な項目

AWS Well-Architected フレームワークへの対応技術

項目名	トレンドマイクロ特有の技術	お客様のメリット
SEC1： ワークロードを安全に運用するには	①Smart Protection Network ②Zero Day Initiative	①世界中のトレンドマイクロのラボの脅威データを活かした防御を実現できます。 ②業界No.1の脆弱性発見組織のデータを活かした防御を実現できます。
SEC4： セキュリティイベントの検出/調査	①各製品のダッシュボード/レポート機能 ②3rd Party連携でのログ分析	①脅威を可視化/分析を行うことで脅威に対して、より早い対応ができます。 ②他社サービスとの連携を簡素化し、多角的な視点/分析を行う事が可能となります。
SEC5： ネットワークリソースの保護	Trend Micro Cloud One	・業界No.1の脆弱性発見組織のデータを活かしたクラウドネットワークの保護が可能です。
SEC6： コンピューティングリソースの保護		①コンピューティングリソースを各レイヤーから保護することができます。 ②上記製品を単一管理し、運用負荷の軽減を実現できます。
SEC10： インシデントの予測、対応、復旧	①Cloud One - Workload Security/Deep SecurityのAWSサービスとの自動連携 ②スタンダードサポート	①有事の際も製品連携により自動的な対処を行う事ができます。 ②満足度90%以上の無償サポートで、有事の際も安心したサポートを受ける事ができます。

SEC1：ワークロードを安全に運用するには

◇**AWS Well-Architected フレームワークの文言**

○ワークロードを安全に運用するには、どうすればよいですか?

ワークロードを安全に運用するには、セキュリティのすべての領域に包括的なベストプラクティスを適用する必要があります。組織レベルおよびワークロードレベルにおいて、運用上の優秀性で定義した要件とプロセスを抽出し、それらをすべての領域に適用します。**AWSや業界のレコメンデーション及び脅威インテリジェンスを最新に保つことで、脅威モデルと管理の目標を進化させることができます。**

セキュリティプロセス、テスト、検証を自動化することで、セキュリティオペレーションをスケールできます。

◇**TM対応製品：**Cloud One - Workload Security、Cloud One – Container Security、Cloud One - Network Security
Cloud One - Application Security、Deep Security、Cloud One - File Storage Security

トレンドマイクロではSmart Protection network（SPN）や、Zero Day Initiative（ZDI）の機関を運営することにより、迅速に最新の脅威/脆弱性を特定し、リアルタイムに最適なソリューションを提供することが可能です。

□最新パターン情報の提供

※2018年トレンドマイクロ調べ

□最新の脆弱性情報の提供

ZERO DAY INITIATIVE

①3,000名以上の研究者の参加
②2億円以上の報奨金(2016年)
③全世界の66.7%の脆弱性を発見

Microsoft
- 公開されている脆弱性の**1/4が**ZDIのもの
- 社外として一番バグ情報を提供しています

Adobe
- 公開されている脆弱性の**1/3**がZDIのもの
- 社外として一番バグ情報を提供しています

SEC4：セキュリティイベントの検出/調査①

◇**AWS Well-Architected フレームワークの文言**

○セキュリティイベントをどのように検出し、調査していますか？

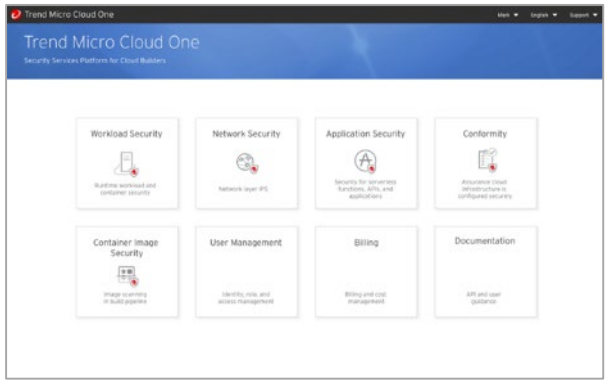
ログやメトリクスからイベントを可視化して把握し分析します。

セキュリティイベントや潜在的な脅威に対して措置をとることで、ワークロードを保護します。

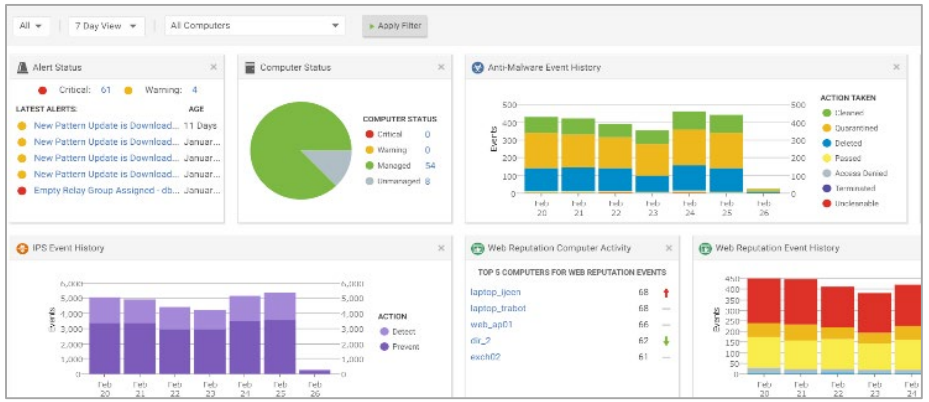
◇**TM対応製品：**Cloud One - Workload Security、Cloud One – Container Security、Cloud One - Network Security
Cloud One - Application Security、Deep Security、Cloud One - File Storage Security

トレンドマイクロの各製品では脅威のログを保管し、各製品のダッシュボード/レポート機能によりセキュリティイベントや潜在的な脅威を可視化/分析することが可能です。

Cloud Oneコンソール トップページ



ダッシュボード（Cloud One - Workload Security）



レポート（Cloud One - Workload Security）

SEC4：セキュリティイベントの検出/調査②

◇**AWS Well-Architected フレームワークの文言**

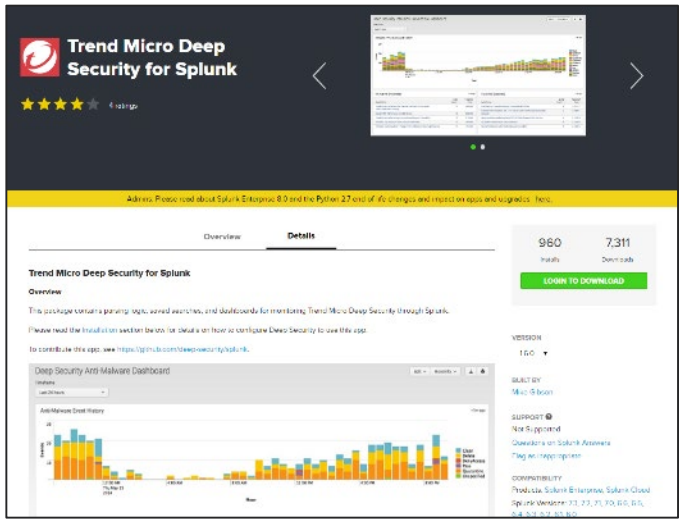
○セキュリティイベントをどのように検出し、調査していますか？

ログやメトリクスからイベントを可視化して把握し分析します。

セキュリティイベントや潜在的な脅威に対して措置をとることで、ワークロードを保護します。

3rdパーティー連携

Splunk連携

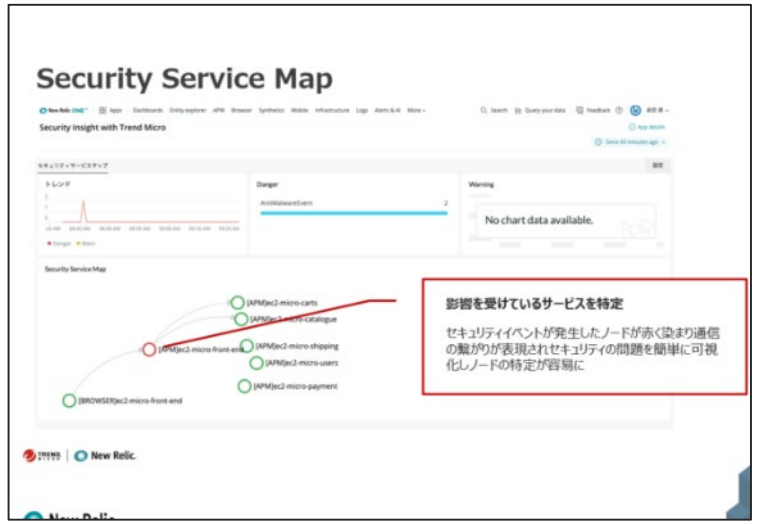


https://splunkbase.splunk.com/app/1936/#/details

Sumo Logic連携

https://help.sumologic.jp/07Sumo-Logic-Apps/22Security_and_Threat_Detection/Trend_Micro_Deep_Security/Trend-Micro-Deep-Security-App-Dashboards

New Relic連携



https://resources.trendmicro.com/jp-webinar-form-0267-ds0819.html

SEC5：ネットワークリソースの保護

◇**AWS Well-Architected フレームワークの文言**

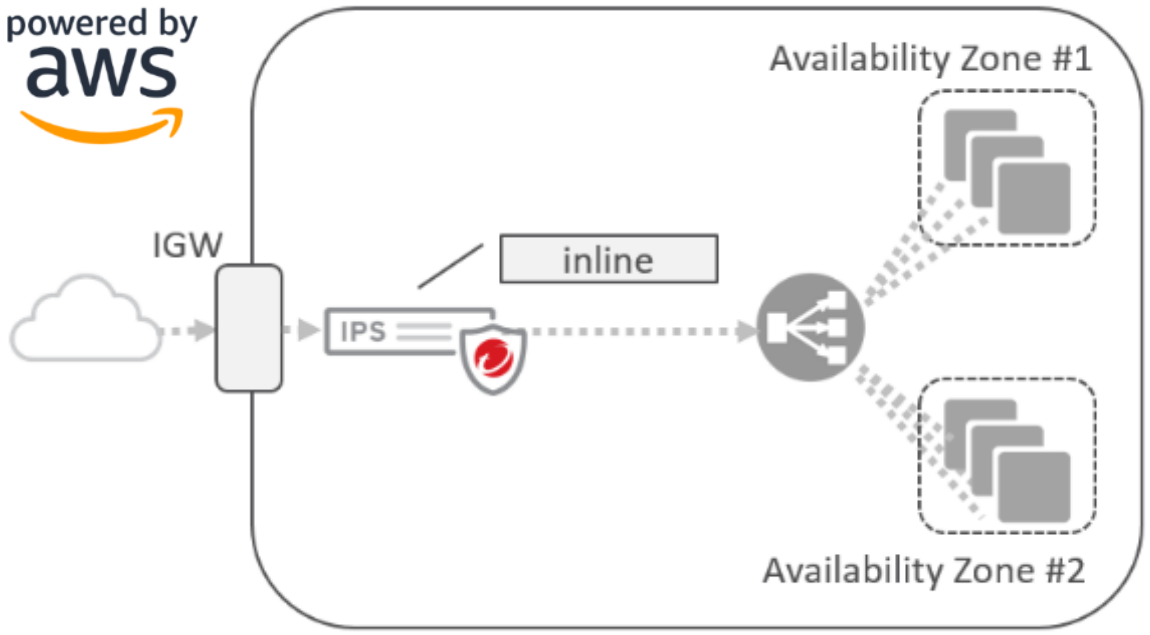
○ネットワークリソースをどのように保護しますか？

何らかの形式のネットワーク接続があるワークロードは、**インターネットでもプライベートネットワークでも、外部および内部ネットワークベースの脅威から保護するために、複数の防御レイヤーが必要**です。

◇**TM対応製品：**Cloud One - Network Security

ハードウェアIPS製品TippingPointのテクノロジーを実装した、クラウド環境上のネットワーク型IPS製品です。
AWSの環境ではVPCへの脆弱性を利用する悪意のある通信を検知・ブロックをすることができます。

構成イメージ



提供機能

- 仮想パッチを提供して、脆弱性を利用するVPCへの通信をブロック
- VPC内部からの不正な通信やC&Cサーバへの通信をブロック

特徴

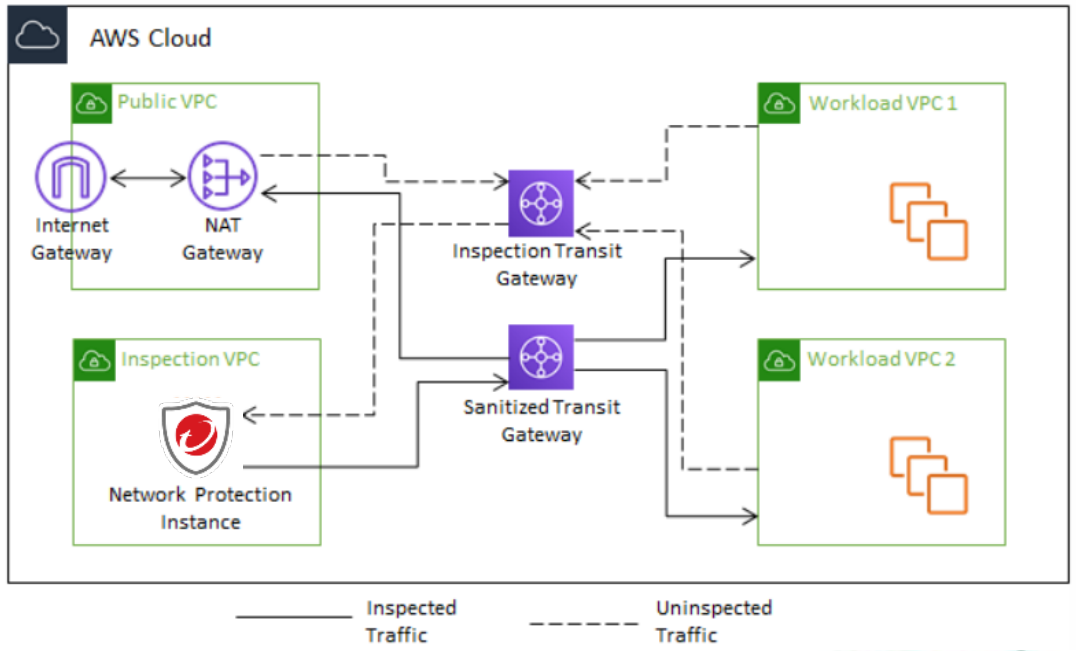
- インバウンド / アウトバウンド通信ともに対応可能
- プロダクトの方針は
  ① デプロイを簡単に速く
  ② SSLインスペクション可能に
  優先事項として開発中。

TREND MICRO

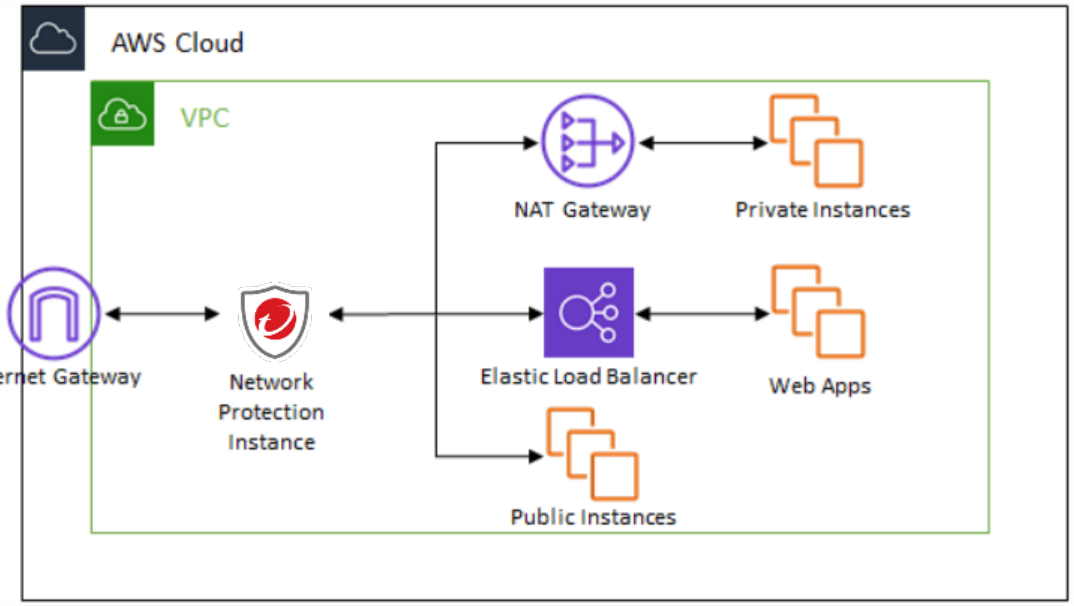
Cloud One - Network Security ユースケース

2つのデプロイユースケースでAWS環境を脅威から守る

1．システム内の脅威拡散を遮断
Transit Gatewayを使用したモデル



2．公開サーバへの脆弱性攻撃を遮断
VPC Ingress Routingを使用したモデル



SEC6：コンピューティングリソースの保護①

◇**AWS Well-Architected フレームワークの文言**

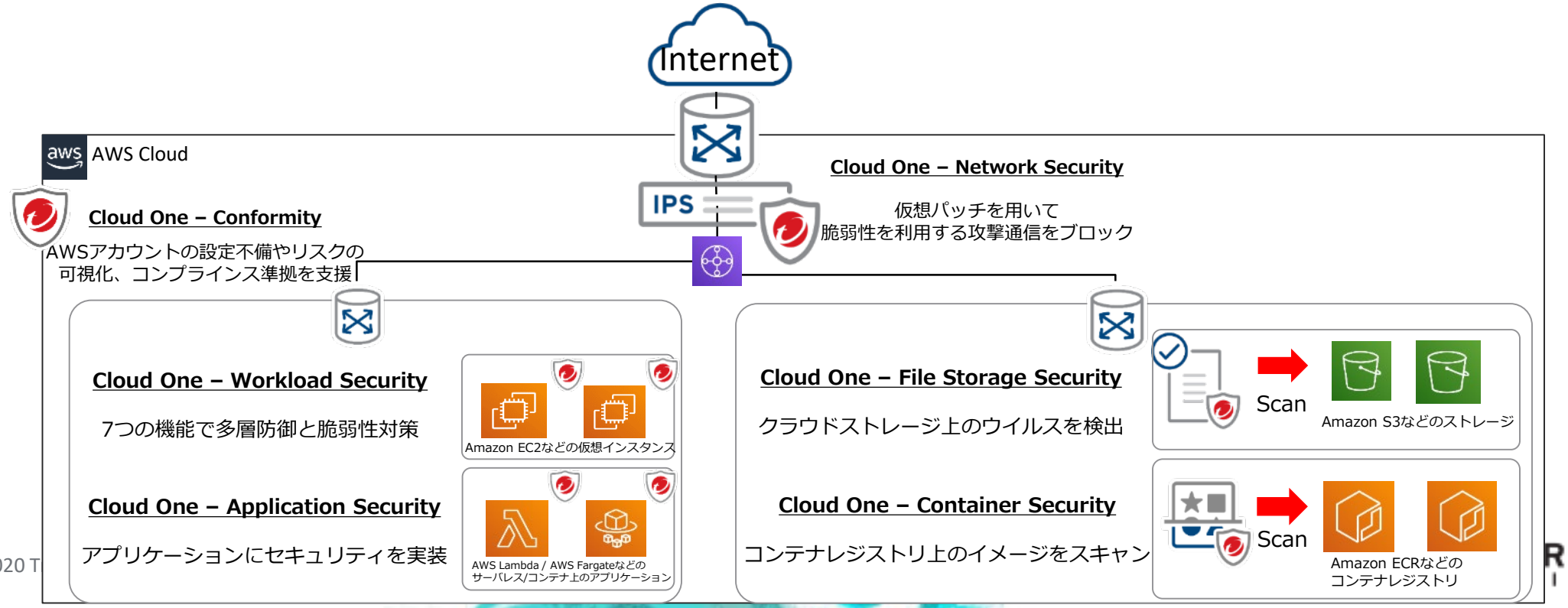
○コンピューティングリソースをどのように保護していますか？

ワークロード内のコンピューティングリソースを内外の脅威から守るには、複数の防御レイヤーを設ける必要があります。

コンピューティングリソースには**EC2インスタンス、コンテナ、AWS Lambda 関数、データベースサービス**、IoT デバイス等があります。

◇**TM対応製品：**Cloud One - Workload Security、Cloud One – Container Security、Cloud One - Network Security
Cloud One - Application Security、Deep Security、Cloud One - File Storage Security

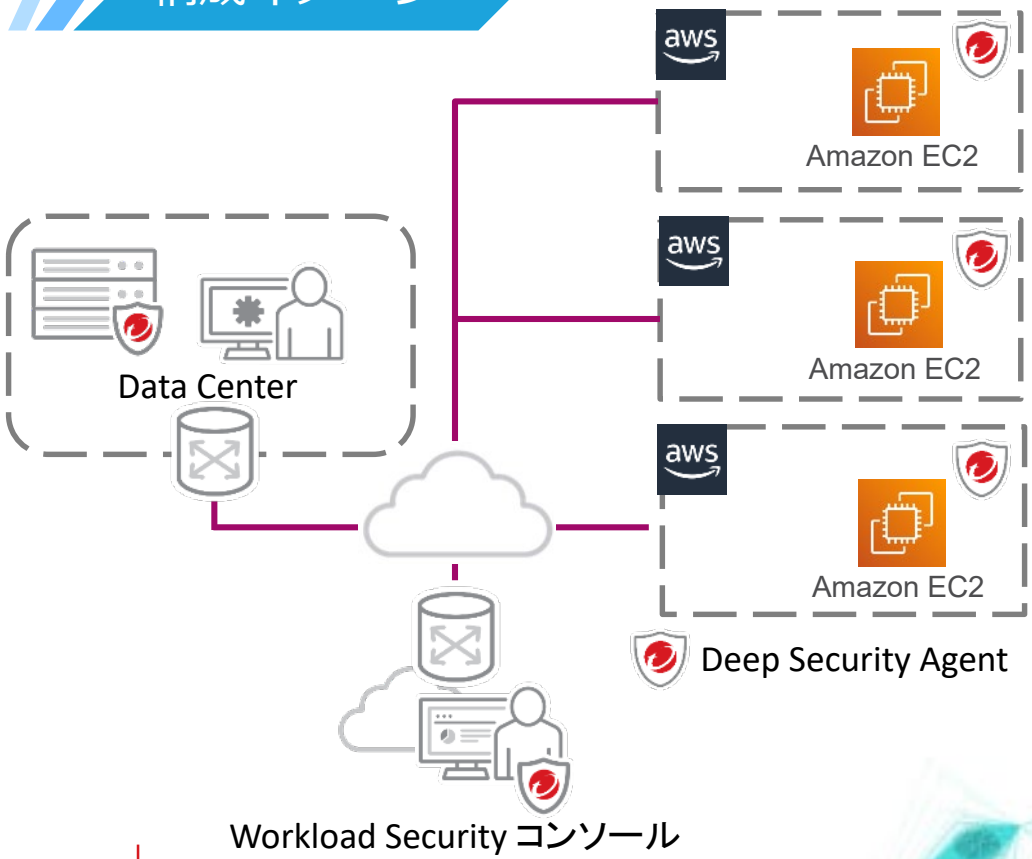
Cloud Oneシリーズの活用によって、コンピューティングリソースを複数のレイヤーから防御する事が可能です。
下記AWSのネットワーク図とCloud Oneとの相関図を記載致します。（各製品の対象については次頁）



Cloud One - Workload Security (旧名称:Deep Security as a Service)

クラウド上のサーバにインストールすることで、脆弱性対策や多層防御を提供。トレンドマイクロが管理サーバをクラウド上で提供するため、導入にあたり管理サーバを構築する必要がありません。

構成イメージ



提供機能

- Agentをインストールしたサーバに対して下記の機能を提供。サーバの多層防御･脆弱性対策を実現。
  - 不正プログラム対策
  - IPS/IDS（侵入防御）
  - Webレピュテーション
  - ファイアウォール
  - アプリケーションコントロール
  - 変更監視
  - セキュリティログ監視

特徴

- 管理サーバの構築・運用が不要
- サーバ保護に必要な複数の機能を単一Agentに搭載

Cloud One - Workload Security ユースケース

侵入防御機能（仮想パッチ）

仮想パッチとは

脆弱性を修正するセキュリティパッチをインストールする代わりに、脆弱性を突く攻撃をブロックし、仮想的にパッチの役目を提供します。

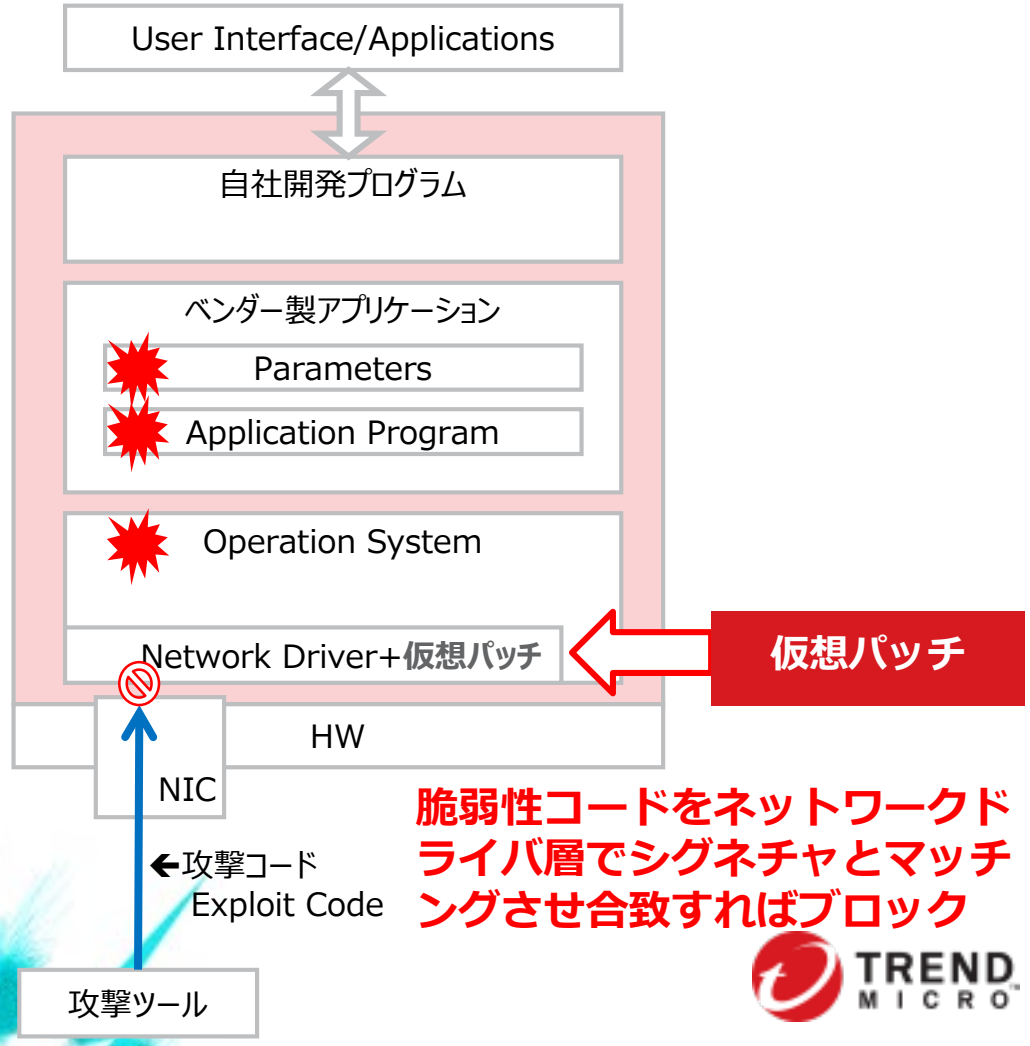
脆弱性を突いた攻撃をブロックする機能

OSやアプリケーションの脆弱性を突いた攻撃をネットワークレベルでブロック

ポイント１：
ソフトウェアのコードレベルでの修正を行わないので、動作中のシステムへ影響が少ない

ポイント２：
WindowsやLinuxのようなOSだけでなく、様々なアプリケーションの仮想パッチがトレンドマイクロから提供される

※トレンドマイクロから提供される侵入防御ルールの他にも、独自のルールを作成することも可能です。



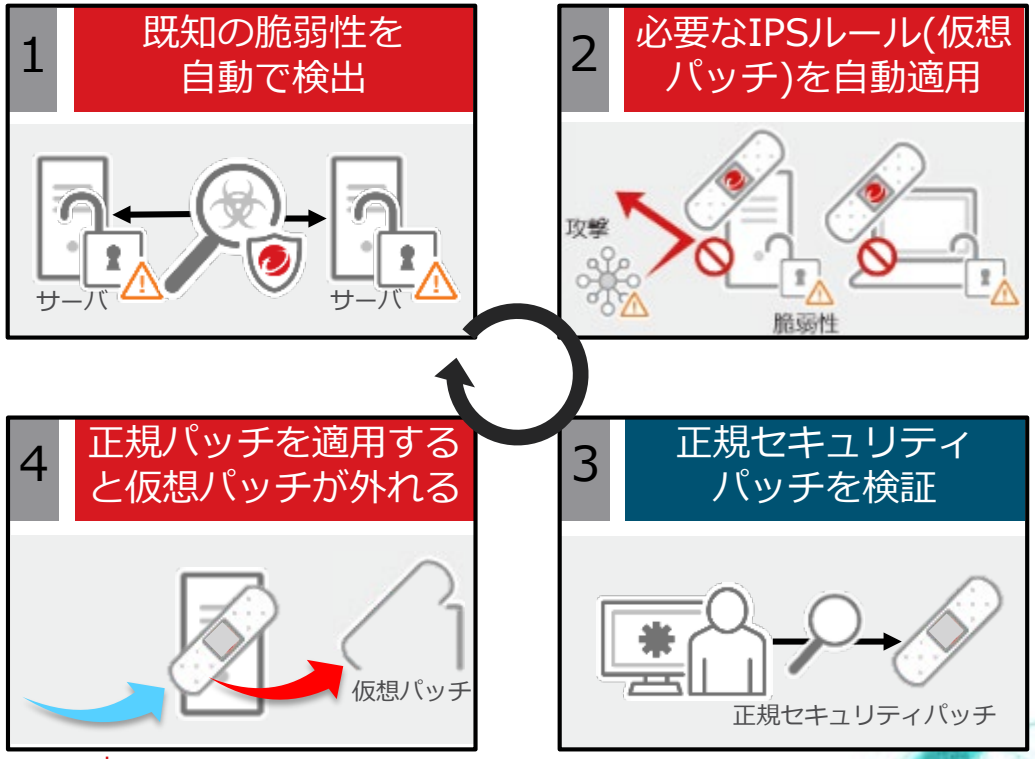
脆弱性コードをネットワークドライバ層でシグネチャとマッチングさせ合致すればブロック

TREND MICRO

Cloud One - Workload Security ユースケース

システム運用者の運用負荷を軽減 ～推奨設定～

「推奨設定」とはDeep Security Agentが自動でサーバ内のシステム情報をスキャンし、
サーバ上にある脆弱性を見つけて、そこに対する必要なIPS/IDSルール”仮想パッチ”を自動で適用する機能です。結果的にサーバは、必要な保護だけを適切に自動で受けることが可能となります。



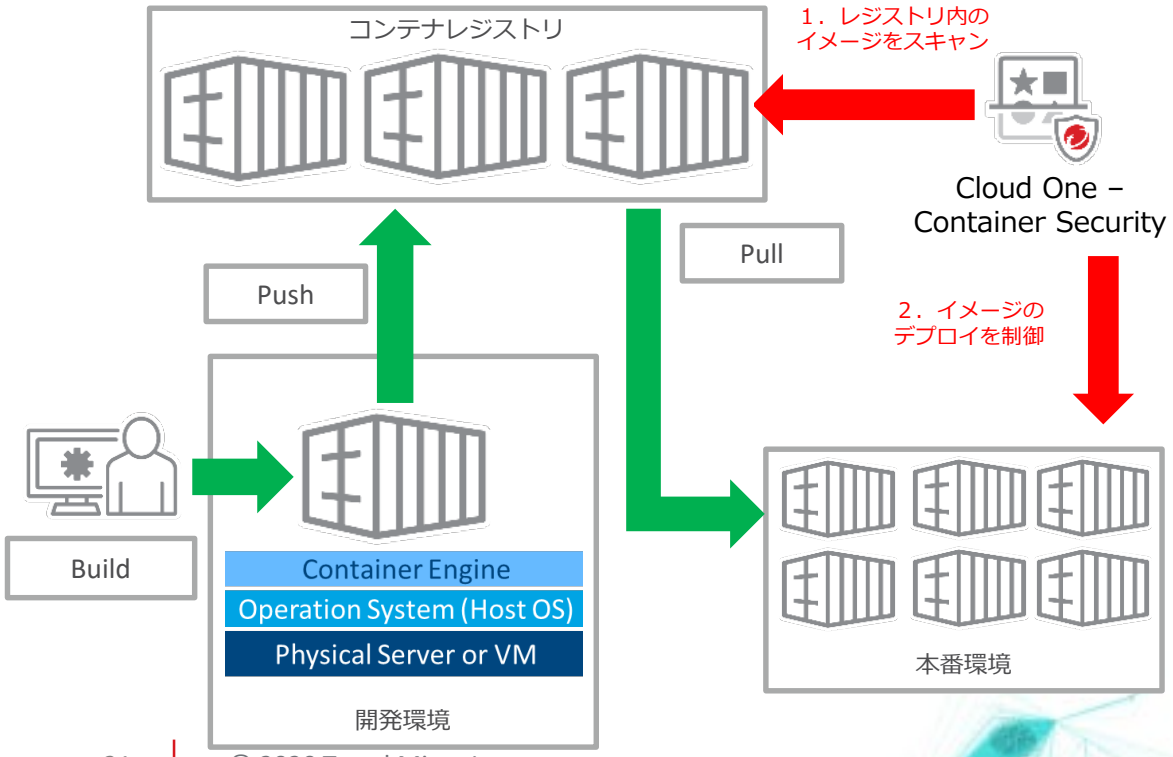
解決可能なペインポイント

- サーバ管理者の脆弱性管理や、脆弱性を狙った攻撃への対処負荷を低減。
- 管理者自身でIPSルールの適用を行う必要がない。

Cloud One - Container Security

コンテナ環境開発プロセスの中で、レジストリに保存されているコンテナイメージに対して、脆弱性や不正プログラムなどを検知してリスクを可視化。
決められたポリシーベースでデプロイを制御する製品です。

構成イメージ



提供機能

1. コンテナイメージのスキャナー
   - コンテナイメージ内の不正プログラム検索
   - コンテナイメージ内に存在する脆弱性の検出
   - AWSのシークレットキーやSSHに利用する秘密鍵の検出
2. コンテナイメージのデプロイを制御
   - イメージに紐づく情報を基にデプロイを制御
   - スキャン結果の情報に基づきデプロイを制御

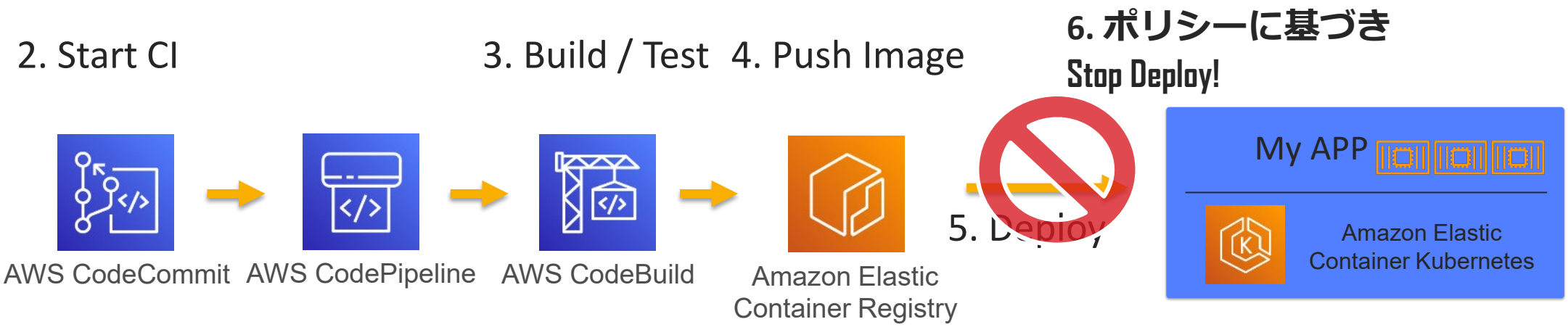
特徴

- イメージのデプロイ前にセキュリティチェック。
  - セキュリティを本番環境から実装する「後乗せ」ではなく、コンテナを用いたDevOpsのサイクルに組み込むことが可能。

Cloud One - Container Security ユースケース

SEC6：
コンピューティングリソースの保護

脅威が潜むコンテナイメージを早期検出し、開発手戻りを最小化



Cloud One - Application Security

RASP(Runtime Application Self Protection)方式を採用、アプリケーション自身にセキュリティを実装することで、アプリケーションを保護。コンテナマネージドサービスやサーバレス環境も保護することできます。

対応言語

ユースケース

AWS Lambda　AWS Fargate　Amazon ECS　Amazon Elastic Container Kubernetes

提供機能

- アプリケーションに対する下記攻撃の検知・防御
  - 悪意のあるペイロード（IPS/IDS機能相当）
  - SQLインジェクション
  - リモートコマンド実行
  - オープンリダイレクト
  - 不正なファイルアクセス
  - 不正なファイルアップロード

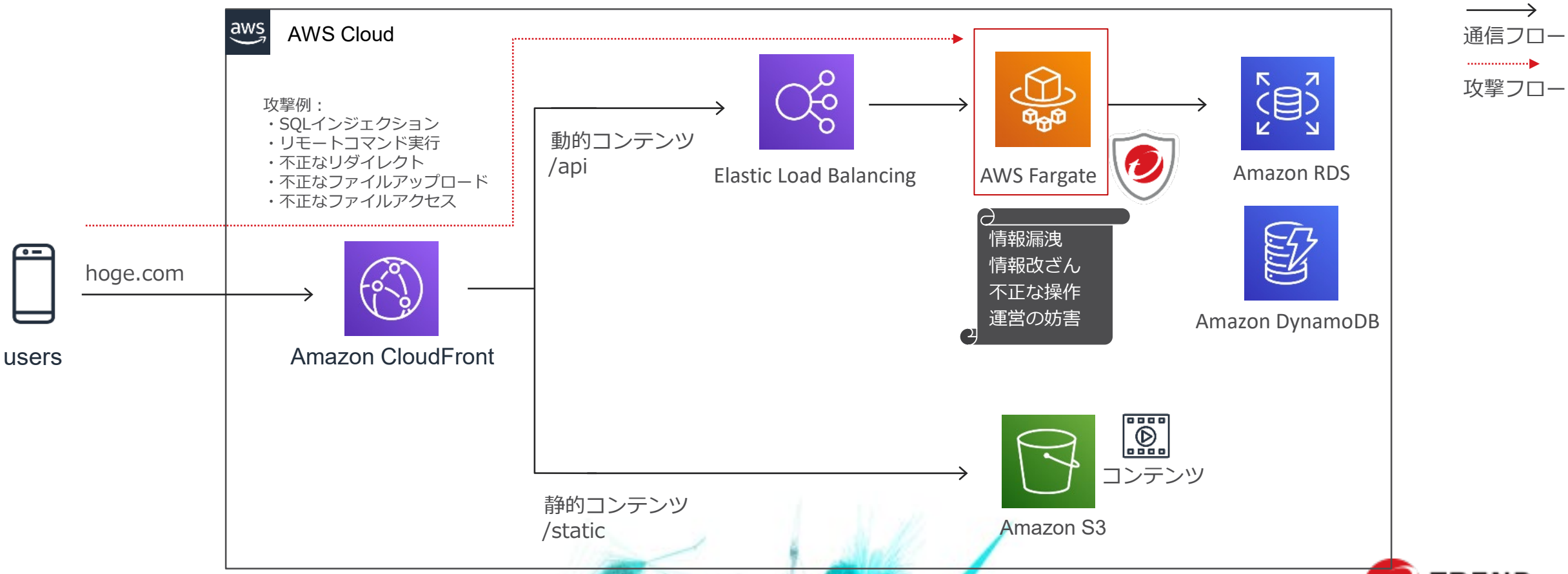
特徴

- 様々な環境・言語をサポート
  各言語にパッケージとして提供
- 数行のコードを書き込むだけで完了
  - ソースコードの大きな変更は不要
  - パフォーマンス低下と展開負荷を最小限に

Cloud One – Application Security ユースケース

Webアプリケーションへの攻撃からシステムを守る

例）ECサイトのシステム



Cloud One – File Storage Security

パブリッククラウドベンダーが提供するクラウドストレージを保護するセキュリティ機能を提供します。
これらに対してアップロード、保管されるファイルをスキャンします。

構成イメージ

提供機能

- Amazon S3内のファイルをスキャン

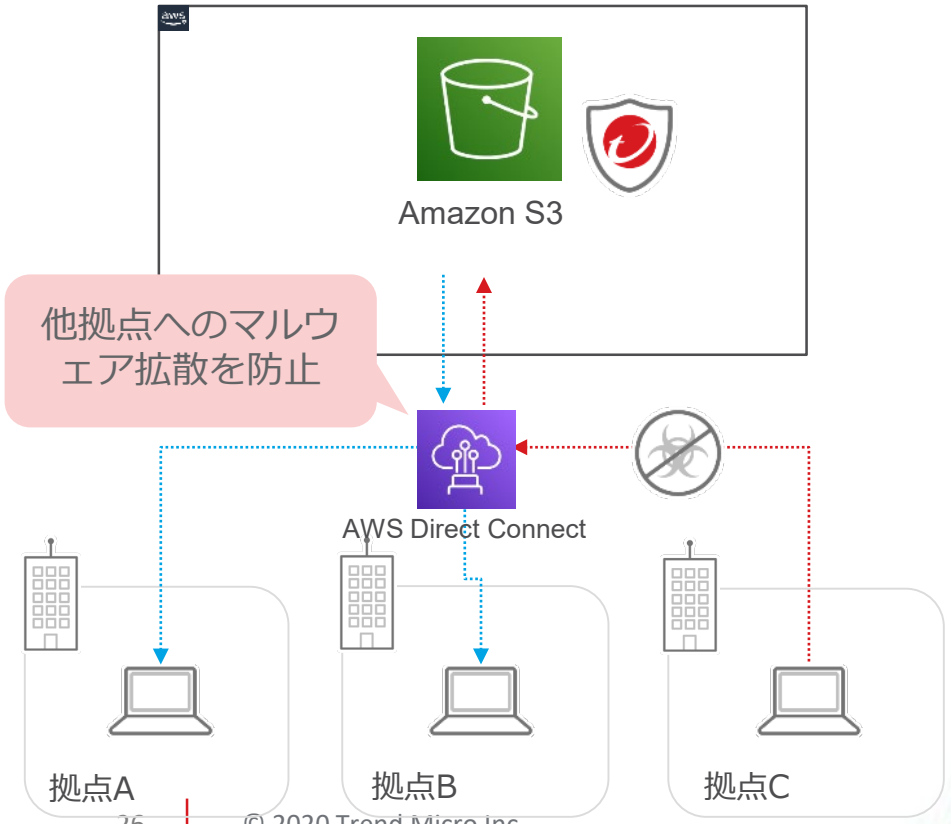
特徴

- ユーザごとの異なるスキャンタイミングにあわせるため、APIを提供
- ファイルの新規アップロードの際には自動的にスキャン可能
- AWS CloudFormation Templateとして提供
サーバレスで機能実装
(初期リリースはAmazon S3向けのみ)

Cloud One – File Storage Security ユースケース

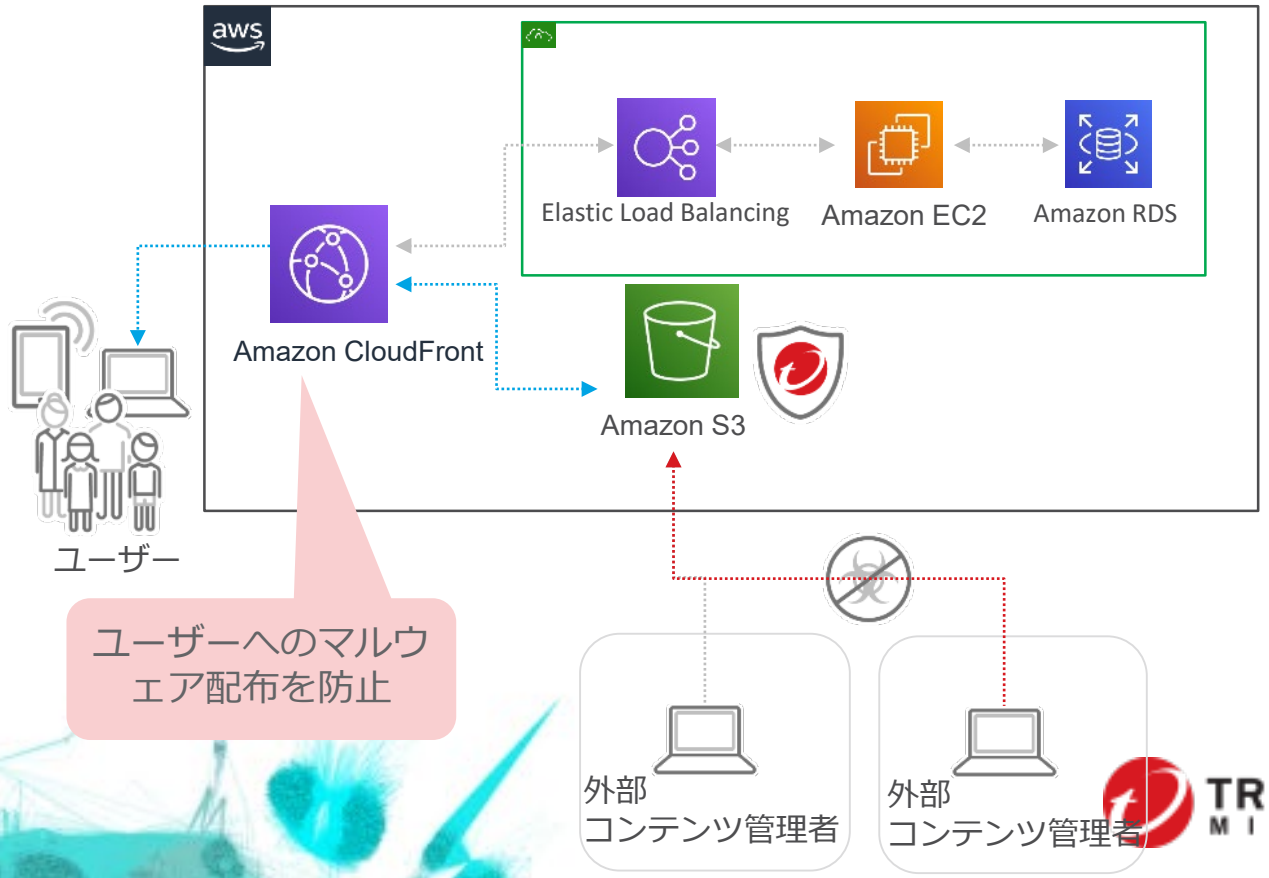
Amazon S3起点のマルウェア混入・拡散防止

1、社内における複数拠点間のファイル共有先として Amazon S3を利用している場合、 マルウェアの混入および拡散を防止



2、外部からデータを取り込んでAmazon S3へ保存する公開系システムの場合、マルウェアが混入および配信されることを防止

(例)　ECサイト、投稿サイト、データクローリング　etc.



Cloud One - Conformity

AWSなどのクラウドアカウントと連携させることで、情報漏えいなどのインシデントにつながる設定不備･設定ミスを検知して、リスクを可視化します。ユーザのコンプライアンス対応を支援します。

スキャン結果イメージ

実際のコンソールは英語表記のみです。

特徴

- AWSが提供する60以上のサービスに対応
- 500を超えるルール
- AWS Well Architected Framework, PCI, HIPAA, NIST, GDPR, CISなどに対応

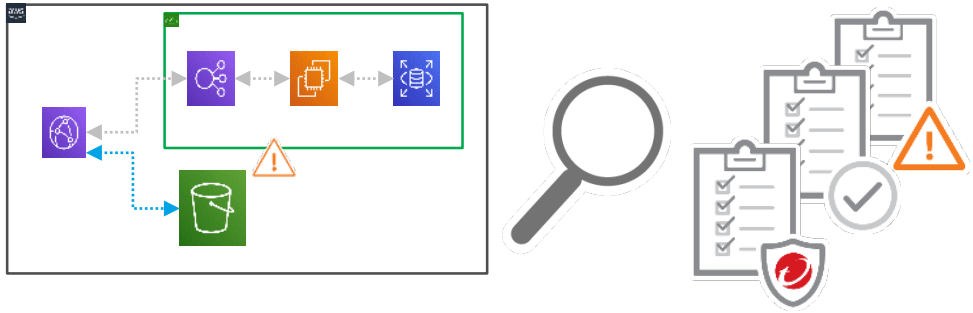
提供機能

- Security and Compliance
  - AWS Well-Architected Frameworkをベースとして、500個以上のルールで設定不備やコンプライアンス状況を可視化。
- CloudFormation Template Scanner
  - CloudFormation Templatesをアップロードする事でテンプレート上のリスクを可視化・修復を支援。
- Real-Time Threat Monitoring
  - AWSアカウント上のリソースにルール違反がないかをリアルタイムに検出。
- Auto-Remediation
  - 修正方法を提示、AWS Lambdaと連携することで、簡易的なセキュリティやガバナンスの自動化を実現。
- Cost Management
  - AWSアカウント上のコスト状況を可視化、コストの最適案を提案、アラートや月次のAWS使用料を予測。

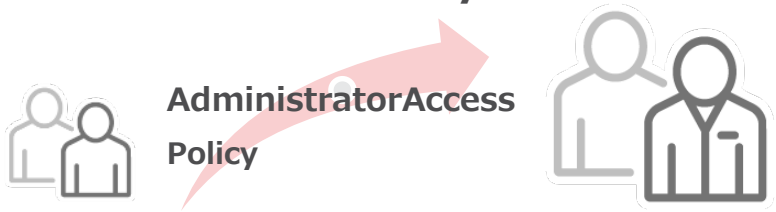
Cloud One – Conformity ユースケース

1、Amazon S3の閲覧権限のPublic設定を検出し情報漏えいを抑止

2、コンプライアンスに違反する設定不備を検出



3、意図しない権限昇格がされていないか AdministratorAccess Policyの付与の監視



4、許可していないリージョンでのリソース利用を検出

5、CloudFormation Templateをスキャンすることによるセキュリティ課題の早期発見

下記項目の一部分においてもConformityで支援する事が可能です

SEC1：ワークロードを安全に運用するには
・パイプラインのセキュリティコントロールのテストと検証を自動化

SEC8：保管時のデータ保護

SEC6：コンピューティングリソースの保護②

前ページでご紹介したCloud Oneシリーズにおいて、
各製品のコンピューティングリソースへの対応について以下に記載致します。

Cloud One	Cloud One – Workload Security	Cloud One – Container Security	Cloud One – File Storage Security	Cloud One – Application Security	Cloud One – Network Security	Cloud One – Conformity
デプロイ先	サーバホストOS	Kubernetes	AWS Lambda	アプリケーション	AWS, ネットワーク上	N/A
スキャン対象	サーバホスト	コンテナ レジストリ	Amazon S3内の ファイル	アプリケーション	AWS ネットワーク	AWS等あわせて60以上のサービスの設定状況
目的 ・ ユースケース	サーバを 多層防御・ 脆弱性対策	コンテナイメージをデプロイ前にスキャン、デプロイの制御 DevOpsにセキュリティ組み込む	クラウド環境のファイルストレージの保護	アプリケーション自身でスキャン サーバレス環境にセキュリティ実装	クラウド環境をネットワークで保護 サーバレス環境にセキュリティ実装	ポリシー違反（セキュリティ設定ミス）があった際にアラート発報・修復支援

SEC10：インシデントの予測、対応、復旧①

◇**AWS Well-Architected フレームワークの文言**

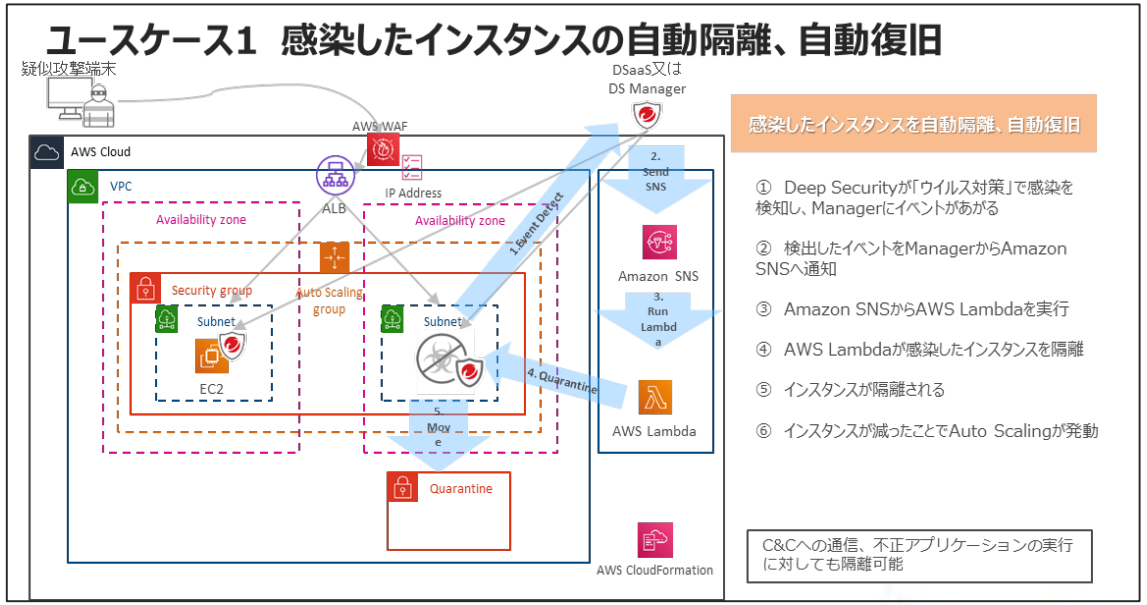
○インシデントの予測、対応、復旧はどのように行いますか?

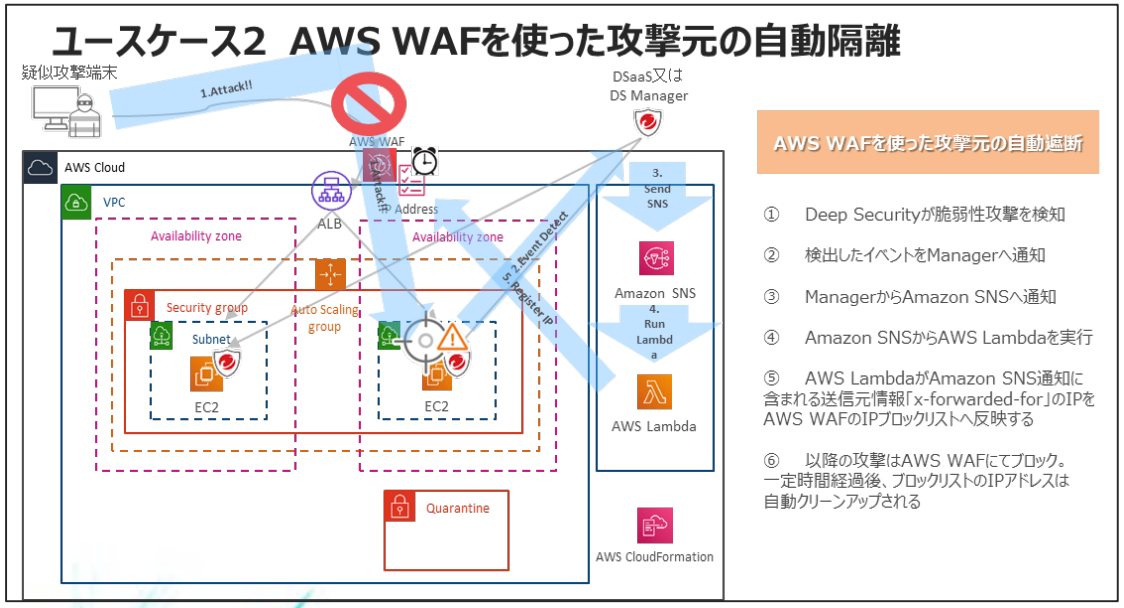
組織に支障をきたすことを最小限に抑えるために、セキュリティインシデントのタイムリーで効果的な調査、対応、復旧に備えることが重要です。

改善計画：封じ込め機能を自動化する

◇**TM対応製品：** Cloud One - Workload Security、Deep Security

AWSサービスとの自動連携によって、 Cloud One - Workload Security、Deep Securityが検知した攻撃を自動的にブロック/隔離/復旧を行うことが可能です。





■今すぐ試せる クイックスタートガイド
https://www.trendmicro.com/ja_jp/business/campaigns/aws/security-automation-deepsecurity-aws.html

SEC10：インシデントの予測、対応、復旧②

◇AWS Well-Architected フレームワークの文言

○インシデントの予測、対応、復旧はどのように行いますか?

組織に支障をきたすことを最小限に抑えるために、セキュリティインシデントのタイムリーで効果的な調査、対応、復旧に備えることが重要です。

改善計画：外部パートナーを特定する: 必要に応じて、インシデント対応と復旧を支援できる外部パートナーと連携します。

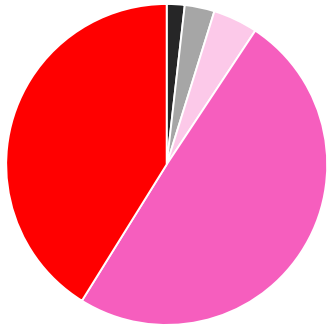
◇TM対応製品：トレンドマイクロテクニカルサポート

トレンドマイクロでは、弊社製品をご購入いただいたお客さまに「スタンダードサポート」を標準提供しております。

サポート体制に満足しています。
メーカーのサポート/技術力があるため、
安心して顧客に提供できる。

サポートに安心感がある

スタンダードサポートの満足度(5点満点)



満足度:90.8%

平均:4.30

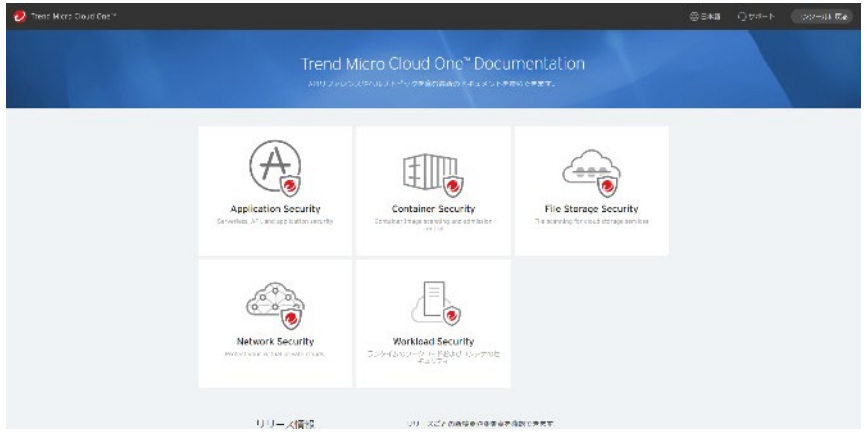
■1 ■2 ■3 ■4 ■5

数回利用しているが、対応が丁寧で迅速である。

Cloud Oneのオンライン資料

【Cloud Oneの各種ドキュメント】

- APIリファレンスやヘルプトピックを含む最新のドキュメントを用意。
- 新機能や互換性、ユーザガイド等も掲載。



https://cloudone.trendmicro.com/docs/jp/

https://success.trendmicro.com/jp/product-support/deep-security-20-0
http://esupport.trendmicro.com/ja-jp/enterprise/ds/top

【サポートページ】

- 日本のテクニカルサポートチームが作成しているサポート情報ページ。
- 日本のお客さまからのよくある質問などをFAQ化。
- アップグレードガイドなどの各種手順書も公開。

Trend Micro Cloud One リリーススケジュール(予定)

※2020/11月時点の情報です

製品名称	グローバル提供開始時期（予定）	日本販売開始時期（予定）	備考
Cloud One – Workload Security	2020年 3月末～	2020年 6月1日	リリース済
Cloud One – Application Security	2020年 12月	2021年 2月～	PoC受付中
Cloud One – Network Security	2020年 12月	2021年 2月～	PoC受付中
Cloud One – Container Security	2020年 12月	2021年 2月～	Private Preivew中
Cloud One – File Storage Security	2020年 12月	2021年 2月～	PoC受付中
Cloud One – Conformity	2020年 12月	2021年 4月～	体験版利用可能

※ リリーススケジュールは確約出来るものではない事を、あらかじめご了承ください。

まとめ

- Trend Micro Cloud One とは何か？
  - Trend Micro Cloud Oneのコンセプトとその製品群

- トレンドマイクロがご支援可能なAWS W-Aの項目とは？

✓ SEC1：ワークロードを安全に運用するには
✓ SEC4：セキュリティイベントの検出/調査
✓ SEC5：ネットワークリソースの保護
✓ SEC6：コンピューティングリソースの保護
✓ SEC10：インシデントの予測、対応、復旧
※ご支援可能な項目は今後拡充していく可能性がございます。

Q & A

ご質問ある方は GoToWebinar を利用して質問を
お願い致します。

AWS 大場様、トレンドマイクロ 姜にて回答をさせて
頂きます。

また、この場でご質問出来なかったAWSや
トレンドマイクロに関する質問は

aws@trendmicro.co.jp

に頂ければ別途個別で回答をさせて頂きます。

TREND MICRO™

THE ART OF CYBERSECURITY

数千のハイブリッドクラウドワークロードを7日間トレンドマイクロのAPIを通じて自動保護をした結果。**実際のデータを使用し、 Trend Micro threat researcherまたアーティストの Jindrich Karasek によって作成されました。**