Amazon GuardDutyの守備範囲と補完をおすすめしたい2つのポイント

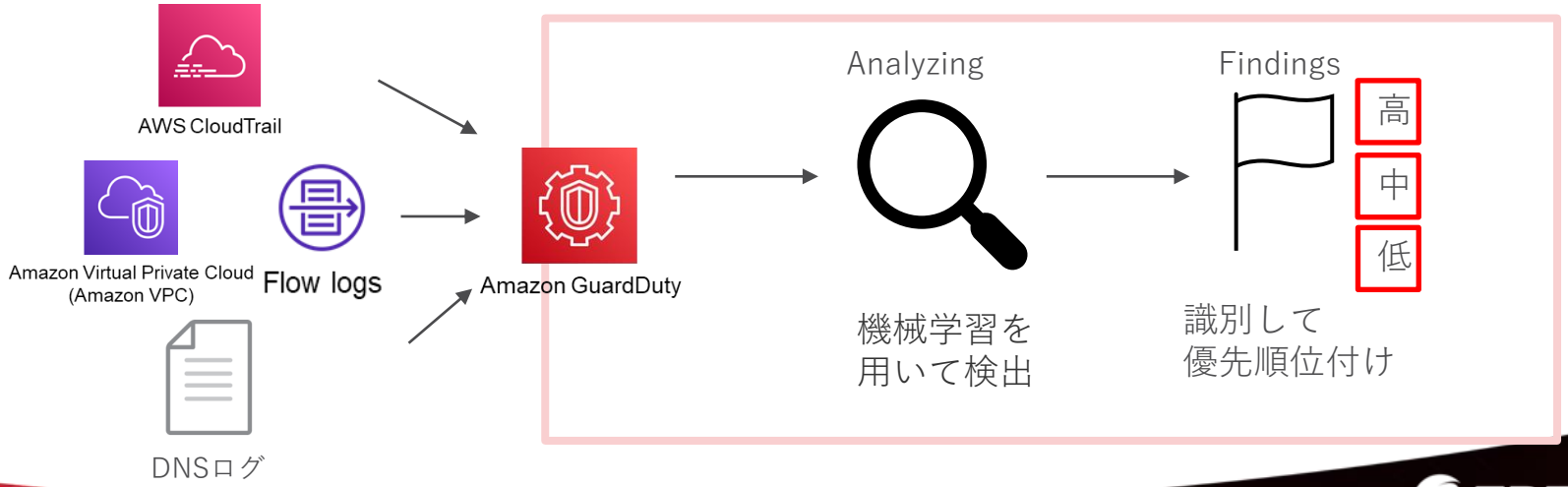
2024年1月
トレンドマイクロ株式会社

＊弊社製品、および他社製品に関する記載は、
2024年1月時点の情報をもとに作成しています。
＊一部弊社環境での検証に基づく内容も記載していますが、
お客様環境で同様の動作を保証するものではありません。

Amazon GuardDutyとは

Amazon GuardDutyは、AWSのアカウント、ワークロード、およびAmazon S3 に保存されたデータを保護するために、**悪意のあるアクティビティや不正な動作を**継続的にモニタリングする**脅威検出サービス**です。（中略）
GuardDutyは、**AWS CloudTrailイベントログ、Amazon VPCフローログ、およびDNSログ**などの複数のAWSデータソース全体で何百億件ものイベントを分析します。

参照：https://aws.amazon.com/jp/guardduty/



 Copyright © 2024 Trend Micro Incorporated. All rights reserved.

Amazon GuardDutyは非常に便利なサービスですが…

- 検出ソースに含まれないもの
- 検出した脅威への対応

には注意が必要です。

 Copyright © 2024 Trend Micro Incorporated. All rights reserved.

➢ 検出ソースに含まれないもの

AWS CloudTrail

AWS インフラストラクチャ全体でアカウントアクティビティをログに記録し、継続的に監視し、保持（AWS HPより）

いつ、だれ
（又はどのAWSリソースが）
が何をしたか

Amazon Virtual Private Cloud
(Amazon VPC)

Flow logs

VPCフローログは、VPCのネットワークインターフェイスとの間で行き来する IP トラフィックに関する情報をキャプチャできるようにする機能（AWS HPより）

VPC内に発生した
通信結果の記録

DNSログ
DNSサーバの動作ログ

DNSに関する
記録

Amazon GuardDutyは
通信のデータ部分（**ペイロード**）**を検出ソースに含まないので**
脆弱性を突く攻撃コード等は検知できない

参照：https://docs.aws.amazon.com/ja_jp/vpc/latest/userguide/flow-logs.html
https://aws.amazon.com/jp/cloudtrail/

 Copyright © 2024 Trend Micro Incorporated. All rights reserved.

➢ 検出した脅威への対応

例：Amazon GuardDutyの場合

↑どのようなログに対して、何を実行させるのか、
予め設定しておくことで実現可能となる。

Amazon GuardDutyは脅威**検出**サービスであり、
防御にはユーザ自身での実装が必要

 Copyright © 2024 Trend Micro Incorporated. All rights reserved.

Amazon GuardDutyを補完するTrend Cloud One™

Amazon GuardDutyは		Trend Cloud Oneなら
検出ソースに ペイロードを含まない	→	ペイロードまでを含み監視 ネットワーク/サーバ/ Webアプリケーションのセキュリティを強化
脅威検出サービスで 防御にはユーザ自身での 実装が必要	→	脅威検出から防御までを一気通貫に実施

 Copyright © 2024 Trend Micro Incorporated. All rights reserved.

～クラウドセキュリティはまとめてシンプルに～

Trend Cloud One™

Trend
Cloud One™

単一コンソールから各製品にシングルサインオン
クラウドセキュリティを管理運用しやすく――

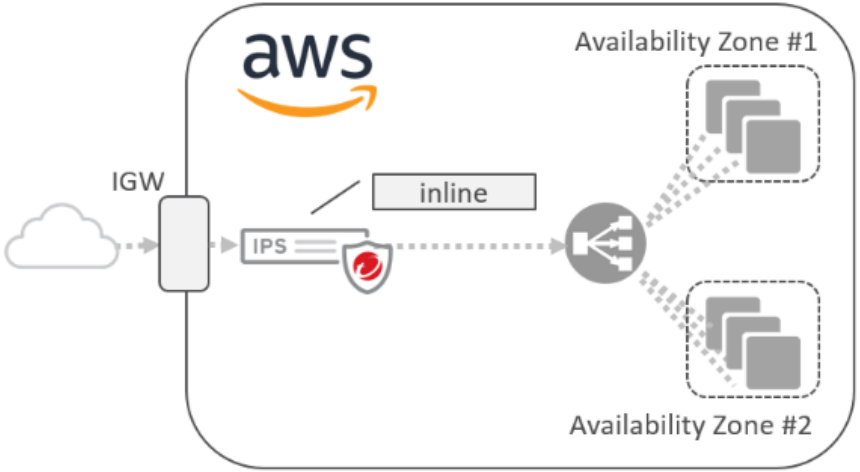
- **Workload Security**
  クラウドワークロードおよびコンテナの保護
- **Network Security**
  クラウド向けネットワークIPS
- **Container Security**
  コンテナイメージのスキャンとランタイム保護
- **File Storage Security**
  クラウドストレージの不正プログラムスキャン
- **Conformity**
  クラウドの設定不備を可視化、コンプライアンス対応支援
- **Open Source Security by Snyk**
  オープンソースに存在する脆弱性やライセンス問題などをスキャン

 Copyright © 2024 Trend Micro Incorporated. All rights reserved.

Trend Micro 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



※ 図版はAWSで記載していますが、Azure版もあります。

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

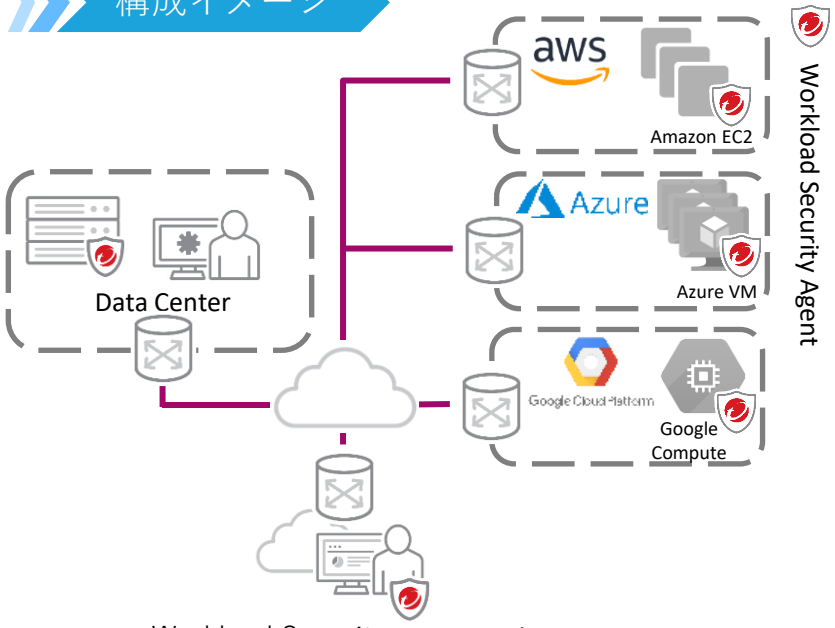
- インバウンド / アウトバウンド通信ともに対応可能
- デプロイを簡単に速く/CloudFormation 展開可能
- TLSインスペクション

 Copyright © 2024 Trend Micro Incorporated. All rights reserved.

Trend Micro Cloud One – Workload Security™

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

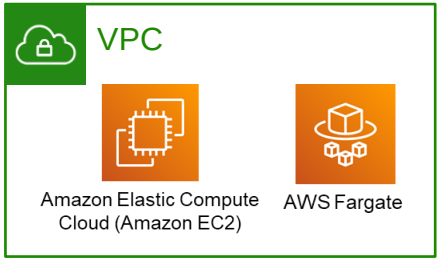
- 下記の機能でサーバの多層防御･脆弱性対策を実現
  - 不正プログラム対策
  - IPS/IDS（侵入防御）
  - Webレピュテーション
  - ファイアウォール
  - アプリケーションコントロール
  - 変更監視
  - セキュリティログ監視
  - XDR/Vision One連携機能

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

 Copyright © 2024 Trend Micro Incorporated. All rights reserved.

Cloud One各製品の対応領域の整理

製品名	Network Security	Workload Security
概要	ネットワーク型IPS	ホスト型IPSとサーバの多層防御
構築方法	ネットワーク経路上に インラインで設置	Amazon EC2にインストール
保護の対象	Amazon VPCへの通信を検知・ブロック（Amazon EC2だけではなく、コンテナサービスやサーバレスも保護対象）  	Amazon EC2の保護（Amazon EC2ベースのコンテナサービスも含む）

 Copyright © 2024 Trend Micro Incorporated. All rights reserved.

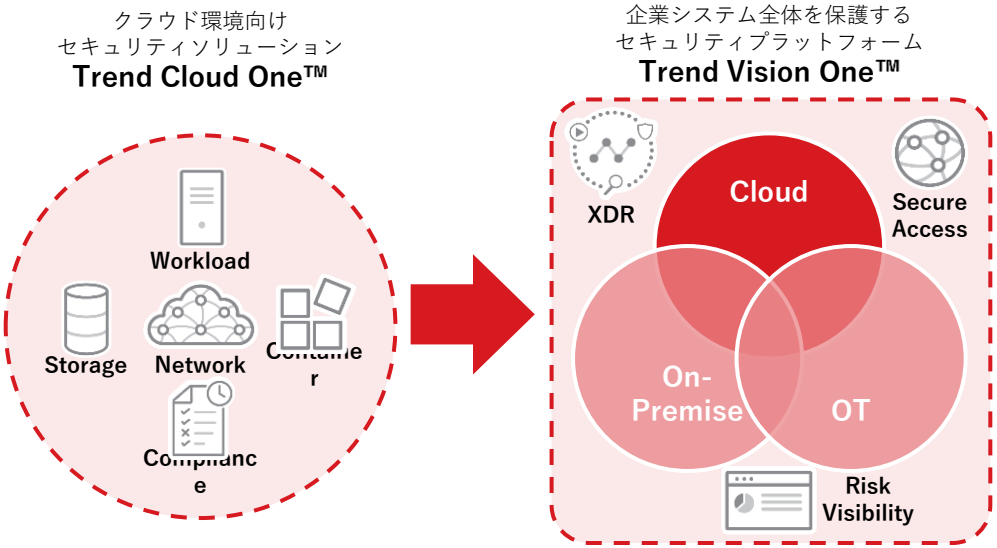
参考：Amazon GuardDuty と Workload Securityの違い

	GuardDuty	Cloud One – Workload Security
対象リソース	AWSアカウント内の全てのEC2とIAM	Workload SecurityがインストールされたEC2インスタンス
サービス概要	フルマネージドの継続的な脅威**検出**サービス (Lambdaと連携させる事で遮断も可能)	脅威の検知、**遮断**を行う製品
検出ソース	CloudTrail、VPC Flow Logs(**ペイロードは含まれない**)、DNSクエリログ	**ファイルデータ、パケットインスペクション**
既知の脅威検出のテクノロジ	AWSのセキュリティ、商用やオープンソースのフィード、感染ホスト情報、匿名化プロキシ、暗号化マイニングプール、ハッカーのツール等々	トレンドマイクロ提供の -アンチウイルスパターン -脆弱性のシグネチャ -トレンドマイクロのSmart Protection Network
未知の脅威検出のテクノロジ	アノマリ検出 -通常と違った挙動の検出アルゴリズム(正常値との差異やML等利用) -大規模な研究開発体制	挙動監視、サンドボックス分析 変更監視、ログ監視 アプリケーションコントロール
対応する脅威の代表的なもの	下記の実行を**検出** ■偵察行為 ***ポートスキャン***、脆弱性探索 ■外部通信 ***C&C通信***、*不正なDNSクエリ*、DGA通信 ビットコインマイニングやビットコイン関連のDNS通信 ■CloudTrailのアクティビティ CloudTrailの無効化、Password Policyの変更 ■不正なログイン試行 ***ブルートフォース***等 ※参考：http://docs.aws.amazon.com/ja_jp/guardduty/latest/ug/guardduty_finding-types.html	下記の実行を**遮断** ■許可されていない通信(*ポートスキャン含む*) ■*C&Cや不正サイトへの通信* ■**不正プログラムの実行** ■**OSやミドルウェアへの脆弱性攻撃** ■登録されていないプログラムの実行 下記の実行を検知 ■**サーバの改ざん** ■*大量の認証試行(ブルートフォースなど)*

 Copyright © 2024 Trend Micro Incorporated. All rights reserved.

Trend Cloud OneからTrend Vision Oneへ

- Cloud Oneは2023年秋より徐々に、後継製品Trend Vision Oneへ統合致します。
- Cloud Oneはクラウド環境向けのソリューション群でしたが、 後継製品Vision Oneは企業システム全体を保護するセキュリティプラットフォームです。Vision Oneに進化することで、クラウド以外の環境のセキュリティ管理と統合することができ、セキュリティ強化と運用効率化を支援します。



 Copyright © 2024 Trend Micro Incorporated. All rights reserved.

Cloud One各製品のVision Oneへの統合

防御力の強化

インシデント発生リスクの低減

Runtime Protection

オンプレミスとクラウド上のワークロードにランタイム保護を提供
サーバ・コンテナ・ストレージなどのワークロードに対する攻撃をブロック

Endpoint Security
Cloud One – Workload Security
Container Security
Cloud One – Container Security
File Security
Cloud One – File Storage Security

検知・対応能力の強化

不正侵入による被害の最小化

Cloud Detection and Response

オンプレミスとクラウドを横断した
インシデント分析やインシデントに対する
迅速な対応を支援

XDR for Cloud

リスクマネジメント能力の強化

サイバー攻撃への事前対策

Attack Surface Risk Management for Cloud

クラウドの内部、および外部から
攻撃を受ける可能性のある領域を
可視化し、リスクを順位付けして、
その修復を支援

Attack Surface Risk Management for Cloud (ASRM for Cloud)
Cloud One – Conformity

 Copyright © 2024 Trend Micro Incorporated. All rights reserved.

法人組織のエンドポイントを保護

Trend Vision One - Endpoint Security™

Trend Micro Apex One SaaS,
Trend Micro Cloud One - Workload Security の後継製品

PC、サーバ、クラウドワークロードのセキュリティを統合し、ひとつのコンソールで管理することで、
効率的なエンドポイントセキュリティの運用を実現。EPP機能に加えて EDR/XDR も提供

Trend Vision One - Endpoint Security

PC、サーバ、クラウドワークロードのセキュリティを統合

ラップトップ　デスクトップ　サーバ　仮想サーバ　パブリック/プライベートクラウド

EPP: エンドポイントの保護
(Trend Micro Apex One SaaS 相当)

EPP: サーバ/ワークロードの保護
(Cloud One - Workload Security 相当
)

EDR/XDR

**EPP, EDR/XDRを
1コンソールで管理**

V1ESライセンス(3種類)

- **Core**: PC/基本サーバ用途 (EPP)
- **Essentials**: PC/基本サーバ用途 (EPP+EDR/XDR)
- **Pro**: クリティカル サーバ/ワークロード用途 (EPP+EDR/XDR)

多層防御とEDR/XDR

- 仮想パッチ (IPS)
- 次世代アンチウイルス (挙動監視, 機械学習型検索)
- アプリケーション制御
- Webレピュテーション
- EDR / XDR、等

セキュリティ運用の複雑さを低減

- 1つの管理コンソール (Trend Vision One) に統合された管理、可視化、対処
- プラットフォーム全体で一貫したRBAC(役割に応じたアクセス管理)、ライセンス管理を実現

拡張性

- Trend Vision One プラットフォームの構成要素であり、XDR や ASRM* などへの拡張が容易

*ASRM: Attack Surface Risk Management

 Copyright © 2024 Trend Micro Incorporated. All rights reserved.

参考情報

■Cloud One各製品の紹介資料

各製品の概要、特長などを確認したい場合は以下の資料をご確認ください。

- Network Security
- Workload Security
- Conformity
- Container Security
- File Storage Security

■体験版について

30日間の無償のトライアルが可能です。
登録方法紹介動画はこちら、登録画面はこちらから、ご確認ください。

■価格について

- 年額版ライセンス
  Workload Securityはこちら、Workload Security以外はこちらをご確認ください。
- 従量課金制（AWS Marketplace）
  こちらをご確認ください。

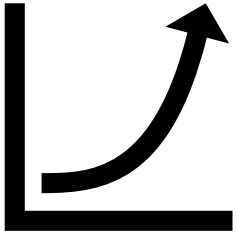
 Copyright © 2024 Trend Micro Incorporated. All rights reserved.

AWS Marketplaceについて

- AWS MarketplaceとはAWSが展開するソフトウェア販売プラットフォームです。
トレンドマイクロは出店者としてAWS Marketplace上で、Trend Cloud Oneを　販売/サポートしています。

日本語サポート

管理画面から日本語での
質問受付が可能。
より安心してご利用できます。



従量課金
AWS利用料と一括で請求

一時的にしか利用しない環境や、
オートスケールする環境でも、
使った分だけご請求。
コストパフォーマンスに優れます。

有効化が簡単

管理画面からSubscribeボタンを
押せば簡単に利用開始可能。
今すぐにでも使いはじめられます。

参考：Trend Cloud One利用料金試算ツール(https://www.trendmicro.com/ja_jp/business/products/hybrid-cloud/aws/pricing.html)

 Copyright © 2024 Trend Micro Incorporated. All rights reserved.

新機能：
Amazon GuardDuty Malware Protectionに関して

 Copyright © 2023 Trend Micro Incorporated. All rights reserved.

Amazon GuardDuty Malware Protection サービス概要

【検出の仕組み】

1. Amazon EC2がマルウェアに感染。
2. マルウェアが外部との通信を開始。Amazon GuardDutyがAmazon EC2（Amazon EC2ベースのコンテナサービスも含む）のマルウェアに関する通信を前述した検出ソース　（Amazon VPCフローログ、DNSログが主なソース）から検知。（トリガーとされる検知はAWSのHPでこちらに紹介されています）
3. 検知のあったAmazon EC2にアタッチされているAmazon EBSを特定、Snapshotを取得。取得したSnapshotに対してAmazon GuardDutyがマルウェアスキャンを行い、マルウェアを特定する。

 Copyright © 2024 Trend Micro Incorporated. All rights reserved.

一般的なマルウェア対策機能と本サービスの違い

一般的なマルウェア感染の流れ

検知のタイミングの違い

一般的なマルウェア対策機能
ディスクのI・Oをフックし、
パターンマッチングや機能学習型検索を実施。
マルウェアと判定された場合、
特定したマルウェアの隔離/削除/駆除を行い、
マルウェアの実行を止めることができる。

Amazon GuardDuty Malware Protection
マルウェア実行後のアクティビティを
VPCフローログ/DNSログを主なソースとして監視。
マルウェアの実行後の挙動から検知し、
対象のAmazon EBSスナップショットをスキャン、
マルウェアの特定をする。

➢ **検知のタイミング/マルウェアに対して行う対処に差がある。**

 Copyright © 2024 Trend Micro Incorporated. All rights reserved.

～クラウドセキュリティはまとめてシンプルに～

Trend Cloud One™

Cloud Oneで
マルウェアに対策機能のある製品

Trend
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 Elastic Compute Cloud (Amazon EC2)
  Amazon Elastic Container Service (Amazon ECS)
  Amazon Elastic Kubernetes Service (Amazon EKS)
  AWS Elastic Beanstalk
- **Network Security**
  クラウド向けネットワークIPS
  Amazon Virtual Private Cloud (Amazon VPC)
- **Container Security**
  コンテナイメージのスキャンとランタイム保護
  Amazon Elastic Container Registry (Amazon ECR)
  Amazon Elastic Kubernetes Service (Amazon EKS)
  Amazon Elastic Container Service (Amazon ECS)
  ※ECSのRuntime保護は今後対応予定
- **File Storage Security**
  クラウドストレージのマルウェアスキャン
  Amazon Simple Storage Service (Amazon S3)
- **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

 Copyright © 2024 Trend Micro Incorporated. All rights reserved.

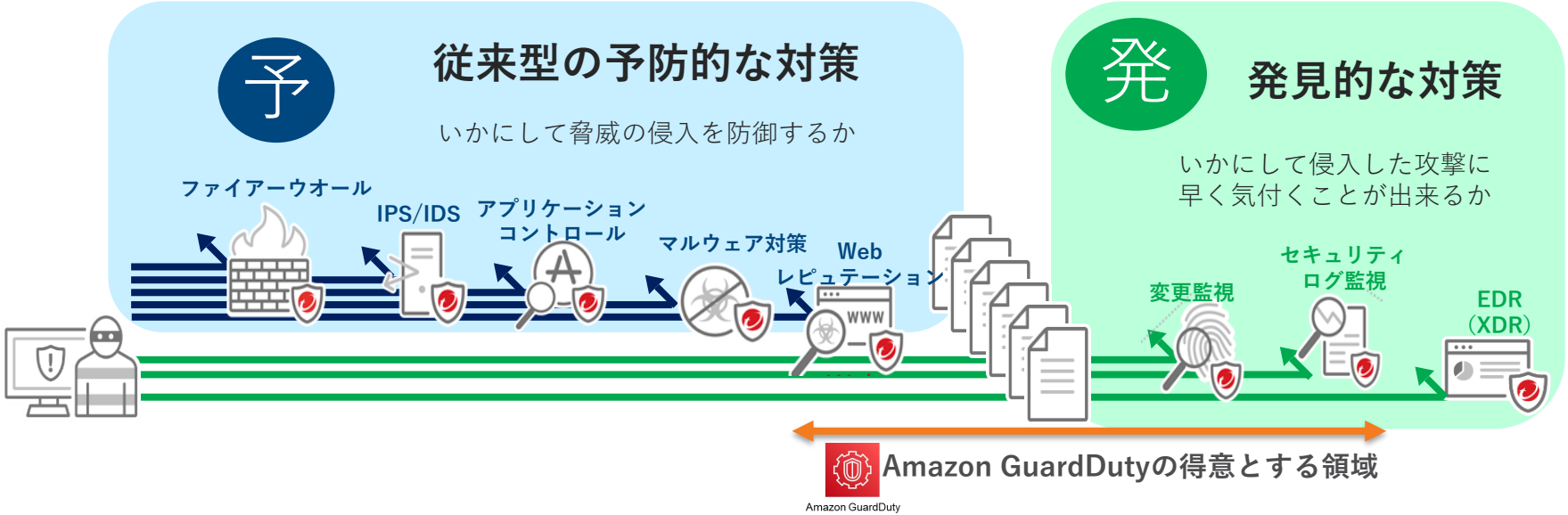
Cloud Oneのマルウェア対策機能とAmazon GuardDutyの違い

	Amazon GuardDuty Malware Protection	Cloud One Workload Security	Cloud One Container Security	Cloud One File Storage Security
スキャン対象	Amazon EBSのスナップショット	Amazon EC2	Amazon ECR上の コンテナイメージ	Amazon S3のオブジェクト
スキャントリガ	VPCフローログ、DNSログを ベースに不審な通信を発見	・ディスクI/O ・不審な挙動(連続した暗号化処理やレジストリへの書き込み) ・任意のスケジュール	・1回/日　(カスタマイズ可) ・APIでキック(カスタマイズ)	・バケットへのファイル アップロード ・任意のタイミング (カスタマイズ)
マルウェア検出時のアクション	検知 ※Amazon EBSスナップショットの保存可	検知/隔離/削除/駆除	検知	検知 ※カスタマイズで隔離や削除が可

 Copyright © 2024 Trend Micro Incorporated. All rights reserved.

Workload SecurityとAmazon GuardDutyの違い

Workload Securityの持つ多層防御を実現するセキュリティ機能



Workload Securityは**マルウェアの実行を止める**ことが可能。
複数のセキュリティ対策機能で**多層防御を実現**することが可能。
Amazon GuardDutyとはマルウェアに対して行う挙動と守備範囲が異なる。

 Copyright © 2024 Trend Micro Incorporated. All rights reserved.

Container SecurityとAmazon GuardDutyの違い

Container Securityの持つセキュリティ機能

Container Image Scanning

- **コンテナイメージ内のマルウェア検索**
- コンテナイメージ内に存在する脆弱性検出

Code → Build → Store

Buildフェーズ

Container Admission Control

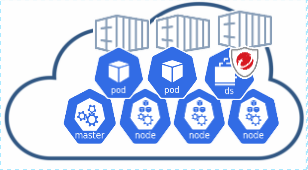
イメージ/スキャン結果に
紐づく情報を基に
デプロイを制御

deploy

Deployフェーズ

Container Runtime Security

- 不正なファイル操作を検知
- 不正なコマンド実行を検知
- MITRE ATT&CK® frameworkに沿った対策が可能



Amazon GuardDuty

- Amazon EC2ベースのコンテナサービス環境において、Amazon EC2からの通信を元に挙動を監視し、Amazon GuardDutyが検知。
- 該当するAmazon EBSのスナップショットを取得。マルウェアスキャンを実行。

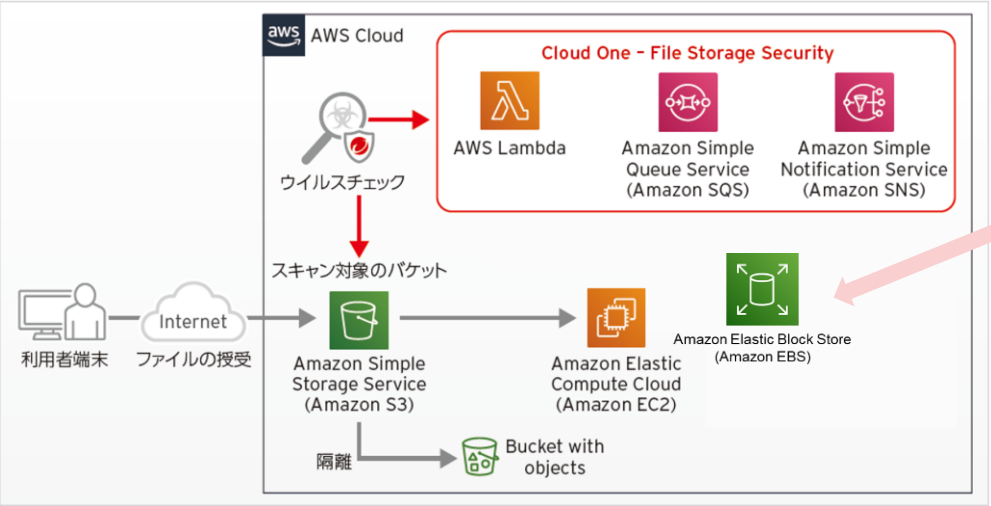
Runフェーズ

Container Securityは**コンテナイメージ内のマルウェア検索**が可能。
コンテナライフサイクルのセキュリティを一気通貫で実現。
Amazon GuardDutyとは、スキャン対象とフェーズが異なる。

 Copyright © 2024 Trend Micro Incorporated. All rights reserved.

File Storage SecurityとAmazon GuardDutyの違い

File Storage Securityのマルウェア対策機能のスキャンフローイメージ



Amazon GuardDuty Malware ProtectionはAmazon EC2からの通信を元に挙動を監視し、Amazon EBSのスナップショットをスキャンする。

File Storage Securityは**Amazon S3のマルウェア対策製品**で、
Amazon S3へのファイルアップロードをトリガーにマルウェアスキャン。
検知したファイルは隔離用バケットに移動させるカスタマイズが可能。
Amazon GuardDutyとは、スキャン対象/トリガー/マルウェア特定後の動作が異なる。

 Copyright © 2024 Trend Micro Incorporated. All rights reserved.

TRENDMICRO、TREND MICRO、ウイルスバスター、InterScan、INTERSCAN VIRUSWALL、InterScanWebManager、InterScan Web Security Suite、PortalProtect、Trend Micro Control Manager、Trend Micro MobileSecurity、VSAPI、Trend Park、Trend Labs、Network VirusWall Enforcer、Trend Micro USB Security、InterScan Web Security Virtual Appliance、InterScan Messaging Security Virtual Appliance、Trend Micro Reliable Security License、TRSL、Trend Micro Smart Protection Network、SPN、SMARTSCAN、Trend Micro Kids Safety、Trend Micro Web Security、Trend Micro Portable Security、Trend Micro Standard Web Security、Trend Micro Hosted Email Security、Trend Micro Deep Security、ウイルスバスタークラウド、スマートスキャン、Trend Micro Enterprise Security for Gateways、Enterprise Security for Gateways、Smart Protection Server、Deep Security、ウイルスバスター ビジネスセキュリティサービス、SafeSync、Trend Micro NAS Security、Trend Micro Data Loss Prevention、Trend Micro オンラインスキャン、Trend Micro Deep Security Anti Virus for VDI、Trend Micro Deep Security Virtual Patch、SECURE CLOUD、Trend Micro VDIオプション、おまかせ不正請求クリーンナップサービス、Deep Discovery、TCSE、おまかせインストール・バージョンアップ、Trend Micro Safe Lock、Deep Discovery Inspector、Trend Micro Mobile App Reputation、Jewelry Box、InterScan Messaging Security Suite Plus、おもいでバックアップサービス、おまかせ！スマホお探しサポート、保険&デジタルライフサポート、おまかせ！迷惑ソフトクリーンナップサービス、InterScan Web Security as a Service、Client/Server Suite Premium、Cloud Edge、Trend Micro Remote Manager、Threat Defense Expert、Next Generation Threat Defense、Trend Micro Smart Home Network、Retro Scan、is702、デジタルライフサポート プレミアム、Airサポート、Connected Threat Defense、ライトクリーナー、Trend Micro Policy Manager、フォルダシールド、トレンドマイクロ認定プロフェッショナルトレーニング、Trend Micro Certified Professional、TMCP、XGen、InterScan Messaging Security、InterScan Web Security、Trend Micro Policy-based Security Orchestration、Writing Style DNA、Securing Your Connected World、Apex One、Apex Central、MSPL、TMOL、TSSL、ZERO DAY INITIATIVE、Edge Fire、Smart Check、Trend Micro XDR、Trend Micro Managed XDR、OT Defense Console、Edge IPS、スマスキャ、Cloud One、Cloud One - Workload Security、Cloud One - Conformity、ウイルスバスター チェック！、Trend Micro Security Master、Worry-Free XDR、Worry-Free Managed XDR、Network One、Trend Micro Network One、らくらくサポート、Service One、超早得、先得、Trend Micro One、Workforce One、Security Go、Dock 365、TrendConnect、TREND MICRO FORUM、トレンドマイクロ知恵袋、Trend Cloud One、Trend Service One、およびAccelerating Youは、トレンドマイクロ株式会社の登録商標です。

© 2024 Trend Micro Incorporated. All rights reserved.