Service Mesh [後編]

Introducing Calisti & Panoptica

28 October 2022

Kazuki Tsutsumi – CCIE#25343, Cisco Systems (ktsutsum@cisco.com)

Self Introduction

シスコシステムズ合同会社　クラウド＆サービスプロバイダアーキテクチャ
テクニカルソリューションズスペシャリスト

2007年に新卒でシスコに入社。

サービスプロバイダー担当のアカウントSEとして9年間、NGNや3G/4G/5Gのモバイルネットワーク、データセンター、国際ネットワークなど様々なお客様や部署へのプリセールス活動に従事。その後、モバイルパケットコアの仮想化を3年間担当しお客様であるMVNOの完全仮想化を推進。

DXを担当するエンタープライズ・ソリューションアーキテクトチームを経て2019年より現職。データドリブンなビジネスに欠かせないデーターセンターソリューションを担当。

学生時代は理論物理学、数理物理学、脳科学を専攻し脳神経回路網のダイナミクスをモデルにより研究。

2018年 IIJの皆様と@SanJose

Agenda

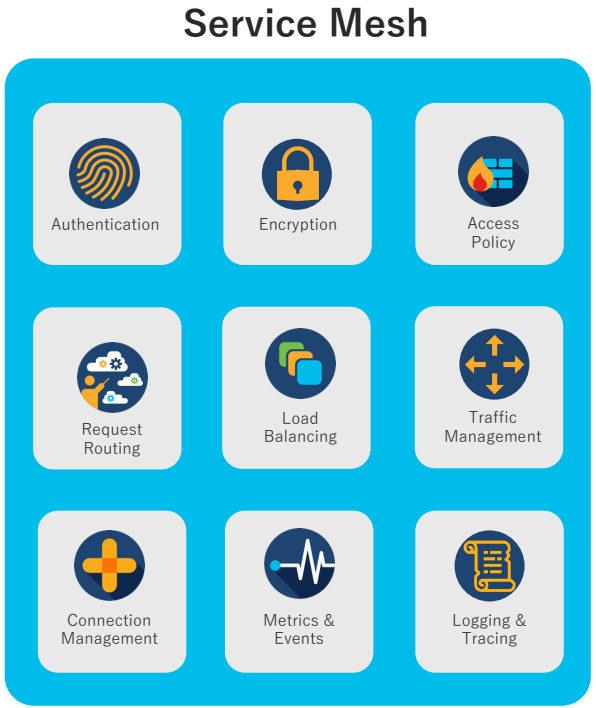
- Service Meshの課題
- Ciscoのアプローチ
- Cloud Native Securityの課題
- Ciscoのアプローチ
- まとめ

今回お話する項目

Service Mesh ざっくりおさらい – 課題

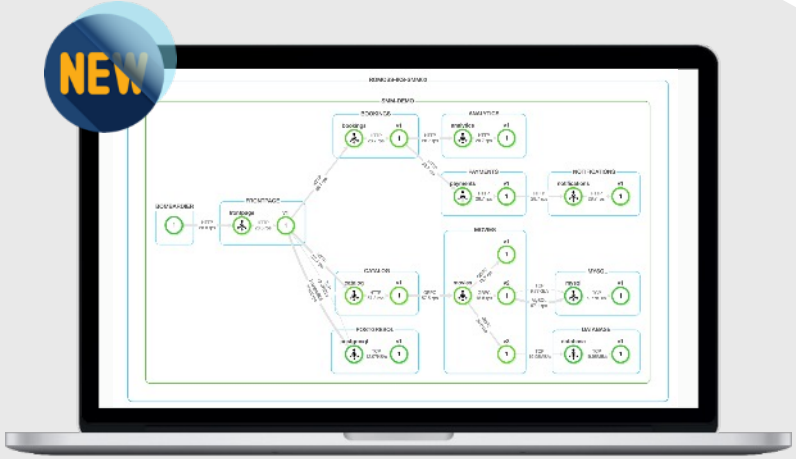
Service Mesh運用上の課題

- ライフサイクルマネジメント
- 観測性のばらつきと断片化
- マルチクラスターの課題
  - Availability（可用性）
  - クラスタ横断的なサービス発見
  - クラスタ間トラフィック管理ポリシー
  - マルチテナンシー
- 非同期メッセージングの処理



Cisco Calisti – The Cisco Service Mesh Manager

https://calisti.app/



サービスメッシュの運用

マルチクラウド、マルチクラスタの接続性と観測性
Connect any on-prem and public cloud together

サービスメッシュの管理を簡素化
Single pane of glass, in depth metrics

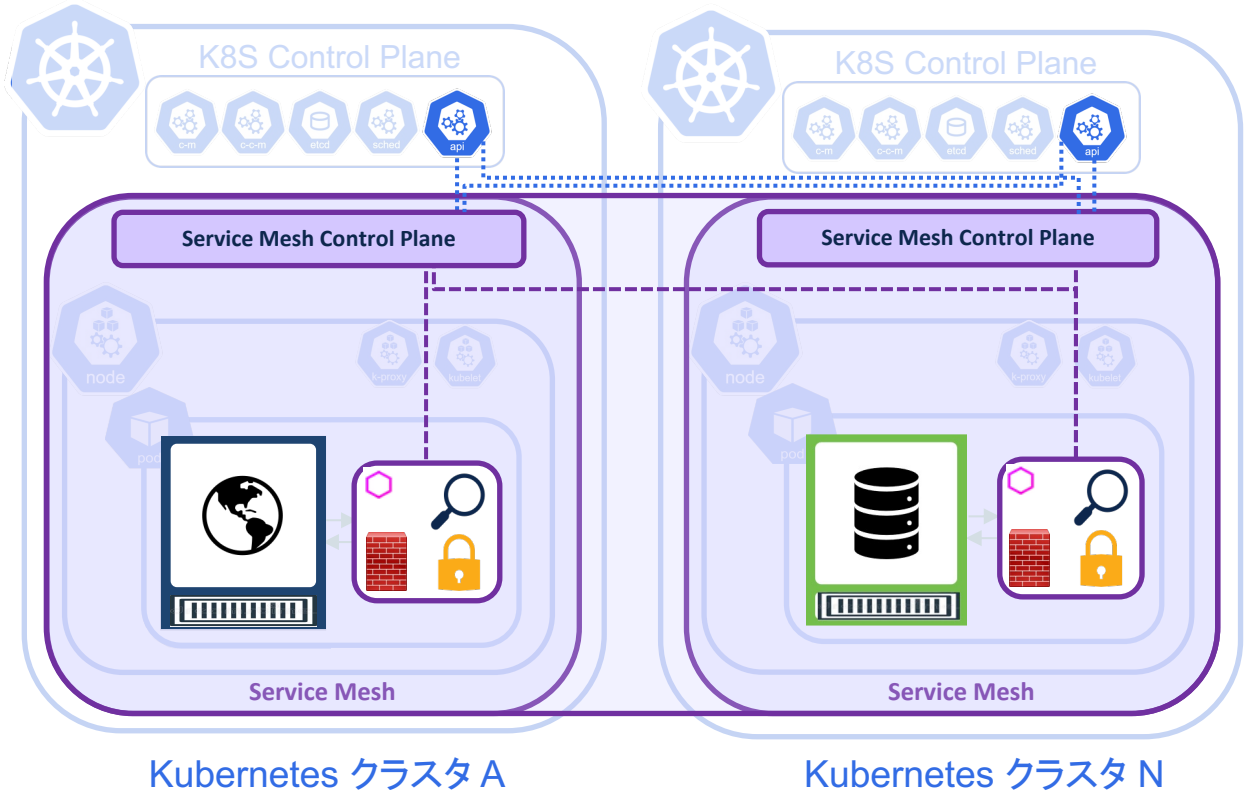
ポリシーベースのアプリ・ネットワーキング＆セキュリティ
Policy management for DevOps teams

トラフィック管理による
スムーズなアプリ更新を実現

統一された可観測性

クラスターとクラウド間のあらゆる
レイヤーでセキュリティを確保

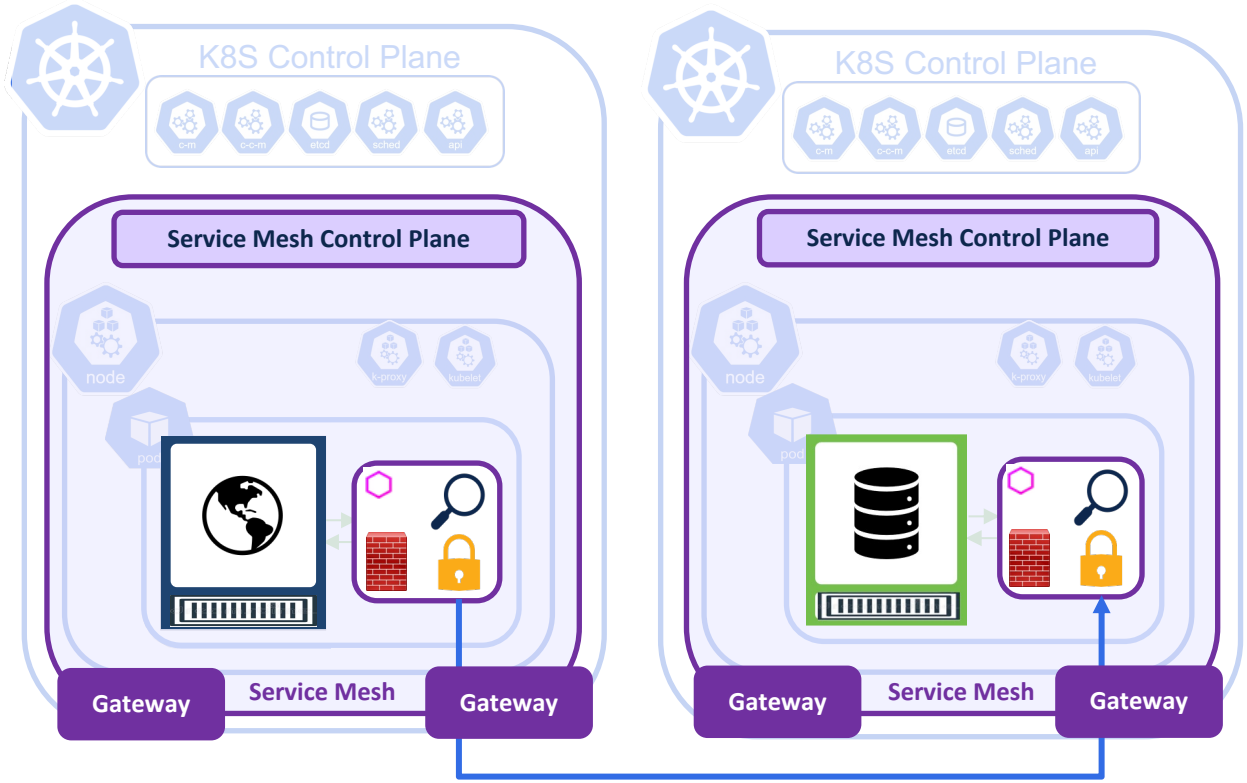
Availability（可用性） Multi-primary Control Plane



- デフォルトでは、Service Meshはクラスタごとにデプロイされます
- Service Meshは、Control Planeをプライマリ クラスタからリモート クラスタに拡張するなどして、クラスタ全体に拡張できます
- Multi-Primary Control Planeと呼ばれる、クラスタ全体に複数のControl Planeをデプロイすることで、より高い可用性を実現できます。
- Calisti は、クロス クラスタ サービス ディスカバリによるMulti-Primary Control Planeのサポートを提供するService Mesh管理ソリューションです

https://smm-docs.eticloud.io/docs/mesh-management/multi-cluster/attach-peer-cluster/

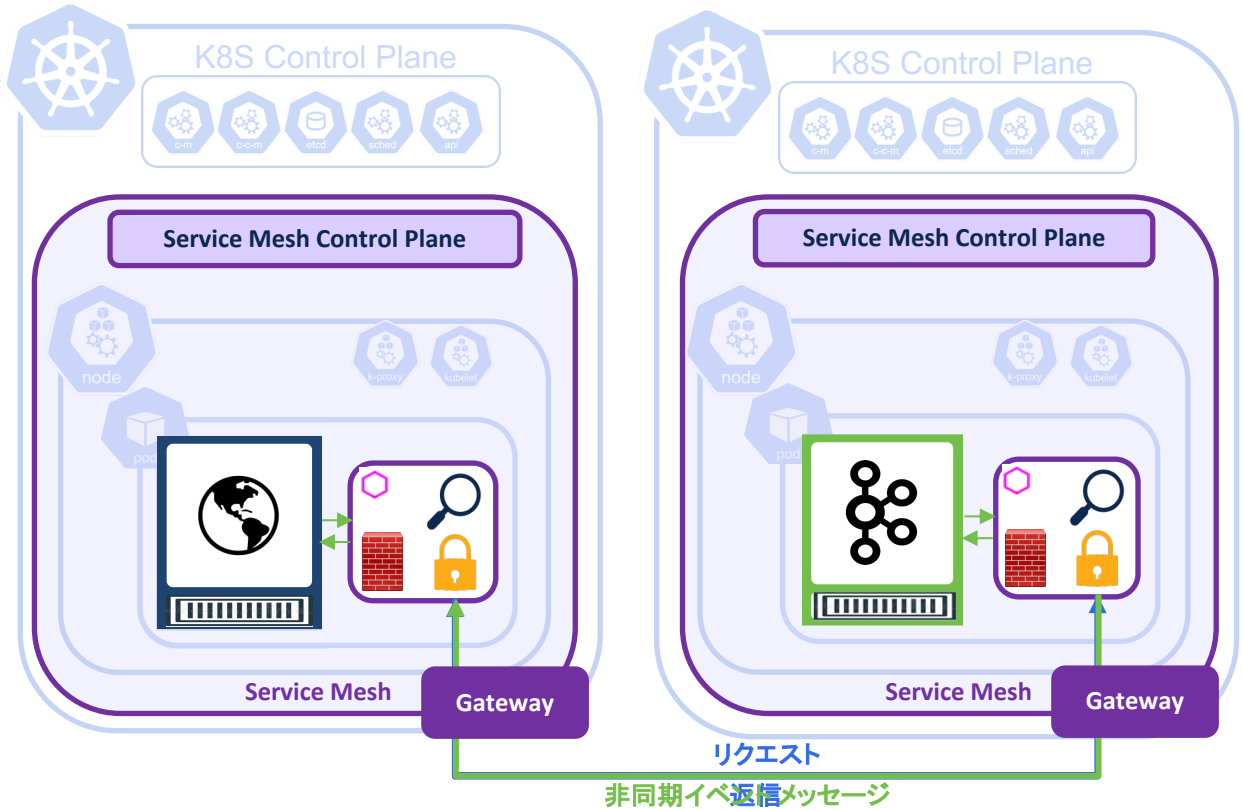
マルチテナンシーとマルチゲートウェイ



- 通常、Service Meshはメッシュごとに 1 つのGatewayのみをサポートします
- Cisco の Istio ディストリビューションには、マルチGateway サポートを可能にするカスタム リソース定義(CRD)が含まれており、MSP のマルチテナント サポートなど、入力/出力の柔軟性と拡張ポリシー オプションを提供します
- これらの追加機能は、ポリシーの柔軟性を提供するだけでなく、インテリジェントなリソースの再利用により、より持続可能なソリューションを提供します
- Calisti は、マルチテナント、マルチGatewayを提供するService Mesh管理ソリューションです

https://smm-docs.eticloud.io/docs/dashboard/gateways/create-ingress-gateway/

非同期メッセージング処理への対応



- Service Meshは、同期要求/応答メッセージング パターンに最適化されています
- ただし、Apache Kafka などのイベントドリブン アーキテクチャ (EDA) は、通信を分離することによってより高いレベルのスケーリングを可能にするため、非同期データ ストリームを生成します
- Cisco の Istio ディストリビューションと Calisti は、同期メッセージングと非同期メッセージングの両方を最適化して保護し、Apache Kafka などの EDA にセキュリティと可観測性の利点をもたらします
- Calisti は、同期と非同期の両方のマイクロサービス通信をサポートするハイブリッド Service Mesh管理ソリューション*です

*Kafka Brokerの管理
Kafka on Istio Deploy Apache Kafka on the same K8S Cluster
Kafka on Istio Provide encryption between Kafka microservices
Kafka on Istio Provide single pane of glass for Kafka Broker Mgmt
Kafka on Istio Provide frictionless Kafka Upgradeability

その他のCisco Calistiの特徴

1

Multi-Cluster Observability

- ✓ SLO[1]によるプロアクティブな問題解決、エラーバジェッティング、SLOが危険にさらされている場合の実行可能なアラート通知
- ✓ タイムラインビュー、異常値検出、トラフィックタッピング/トレースによる根本原因解決の迅速化
- ✓ Traffic Analyticsによるサービス間パフォーマンスの可視化

2

Simplified mesh & traffic management

- ✓ Istioのライフサイクルマネジメント
- ✓ 自動化されたツール、メトリクスによる高可用性の確保
- ✓ オペレーションに特化した豊富で包括的なダッシュボード
- ✓ エンタープライズクラスのセキュリティ強化およびライフサイクル
- ✓ Canary Upgradeによるデプロイメント2日目のリスク軽減
- ✓ コンフィグ検証によるヒューマンエラーの低減
- ✓ VM-extensions for brownfield and external service linkage

3

Policy based & Security

- ✓ セキュリティ、観測性、プラットフォームトラフィック管理によるアプリケーション展開の簡素化
- ✓ セキュリティ脆弱性に対し、ポリシーの適用による迅速な対応
- ✓ Avoid issues via canary deployments, circuit breakers
- ✓ DevOps friendly traffic debugging

[1]**S**ervice **L**evel **O**bjectives

Major API Attacks

Sep 2018 **T-Mobile (BOLA attack)** - 2M subscribers sensitive data theft by an internal user

Sep 2019 **Facebook (Authentication)** - 130 millions US phone numbers linked to Facebook

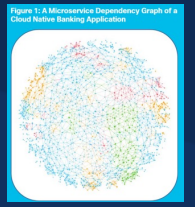
Jan 2021 **Facebook (video trimming DOS)** - block video owner from controlling content

April 2021 **John Deere, Springfox** - BOLA, Extensive data exposure

April 2021 **Experian (Authentication)** - API exposed Credit Scores of Most Americans

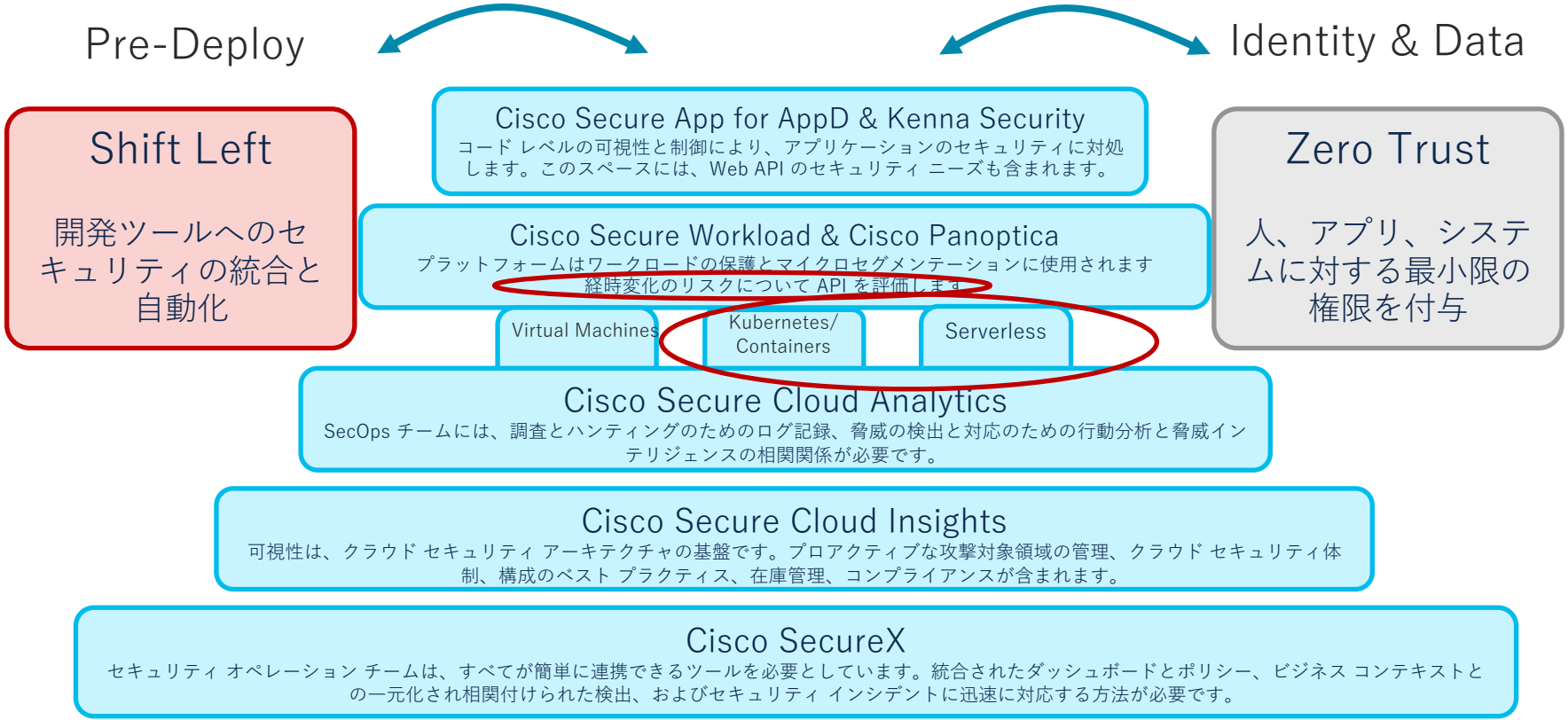
May 2021 **Peloton's Fitness (Data Exposure)** - leaky API let anyone grab riders' private account data 3M subscribers

June 2021 **LinkedIn (Data Exposure)** - Huge, 92% of users, including inferred salaries



今回お話する範囲

Ciscoが考えるセキュリティの全体像

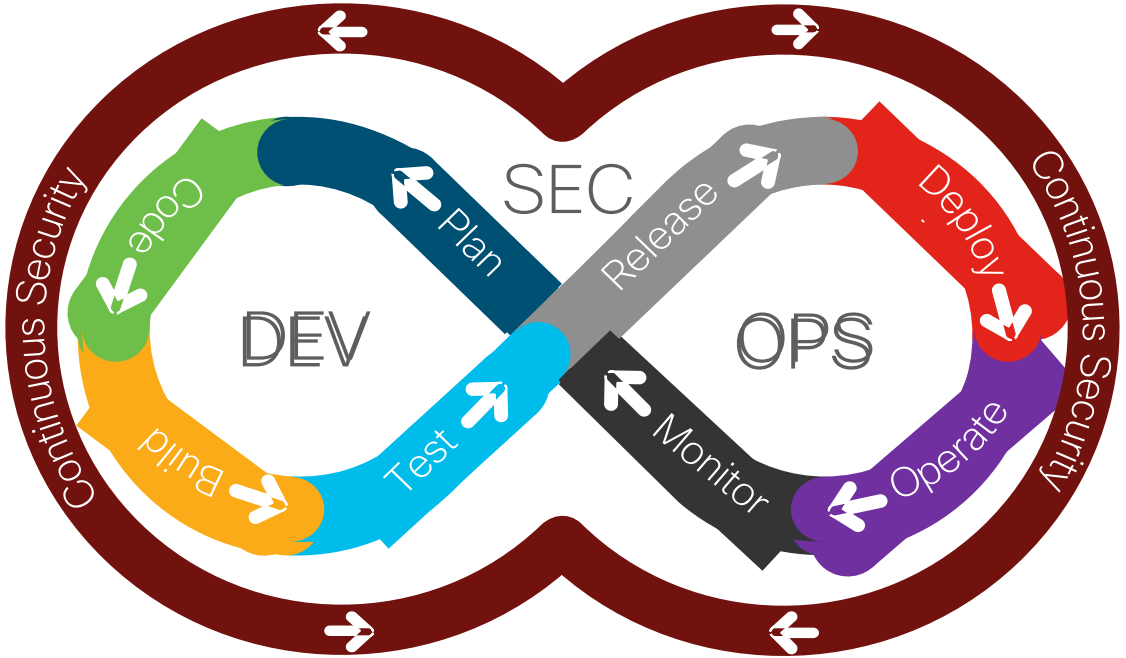


TALOS

“Shift Left” とは？

Cisco Secure Application - Panoptica は、クラウド ネイティブ アプリケーションのすべての段階、およびマイクロサービス、function、API、構成などのすべてのコンポーネントに対してセキュリティを確保します。

Panopticaは継続的なセキュリティも可能にします



1

クラウドネイティブアプリを守るには？ そもそも何を何から守らなければならないのでしょうか？- Present

2

アプリケーションの構成は健全ですか？防御すべきものに対しての制御はどうすればよいでしょうか？ - Control

3

クラウドアプリの中にバリアーを作ればよいでしょうか？ 脆弱性には何から対処すればよいのでしょうか？ - Prioritize

4

脆弱性があるアプリケーションを管理するためのポリシーとは？ コンプライアンスを定義することは可能でしょうか？ - Define

Cisco Panoptica - The Cisco Secure Application Cloud
https://panoptica.app/

Present

アプリケーションのすべてのアーティファクトとその脆弱性を可視化

Control

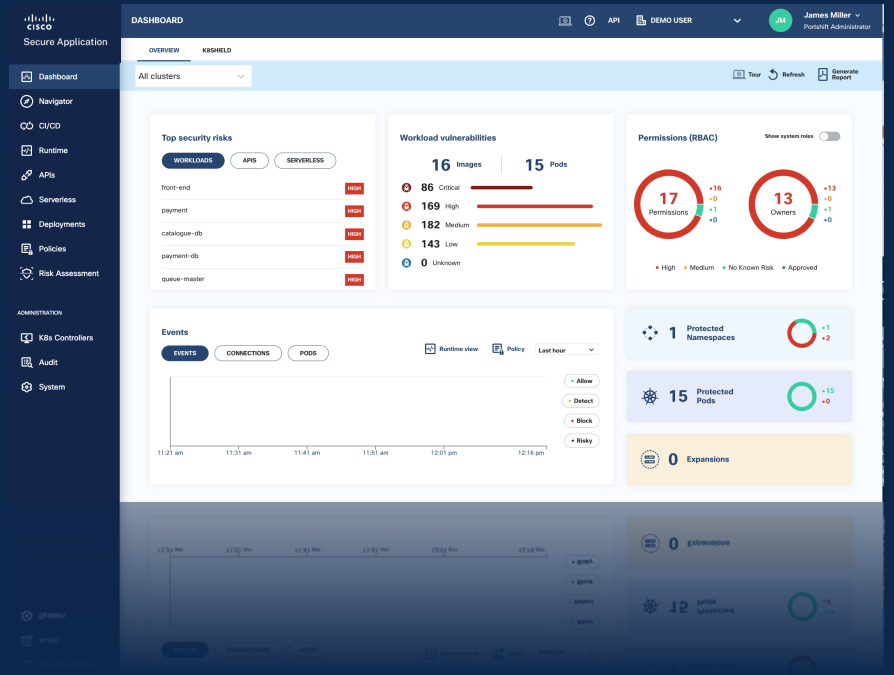
コンテナ、イメージ、SBOM*、サプライチェーン、サーバーレス、APIを制御

Prioritize

統合されたService Meshで接続を管理しながら、悪用可能性**によってワークロードの修復に優先順位をつける

Define

企業におけるセキュリティポリシー・コンプライアンスの定義と実施



*Software Bill Of Materials
**MITRE ATT&CK frameworkが利用可能

Panoptica: Open-Sourced Architectural Components

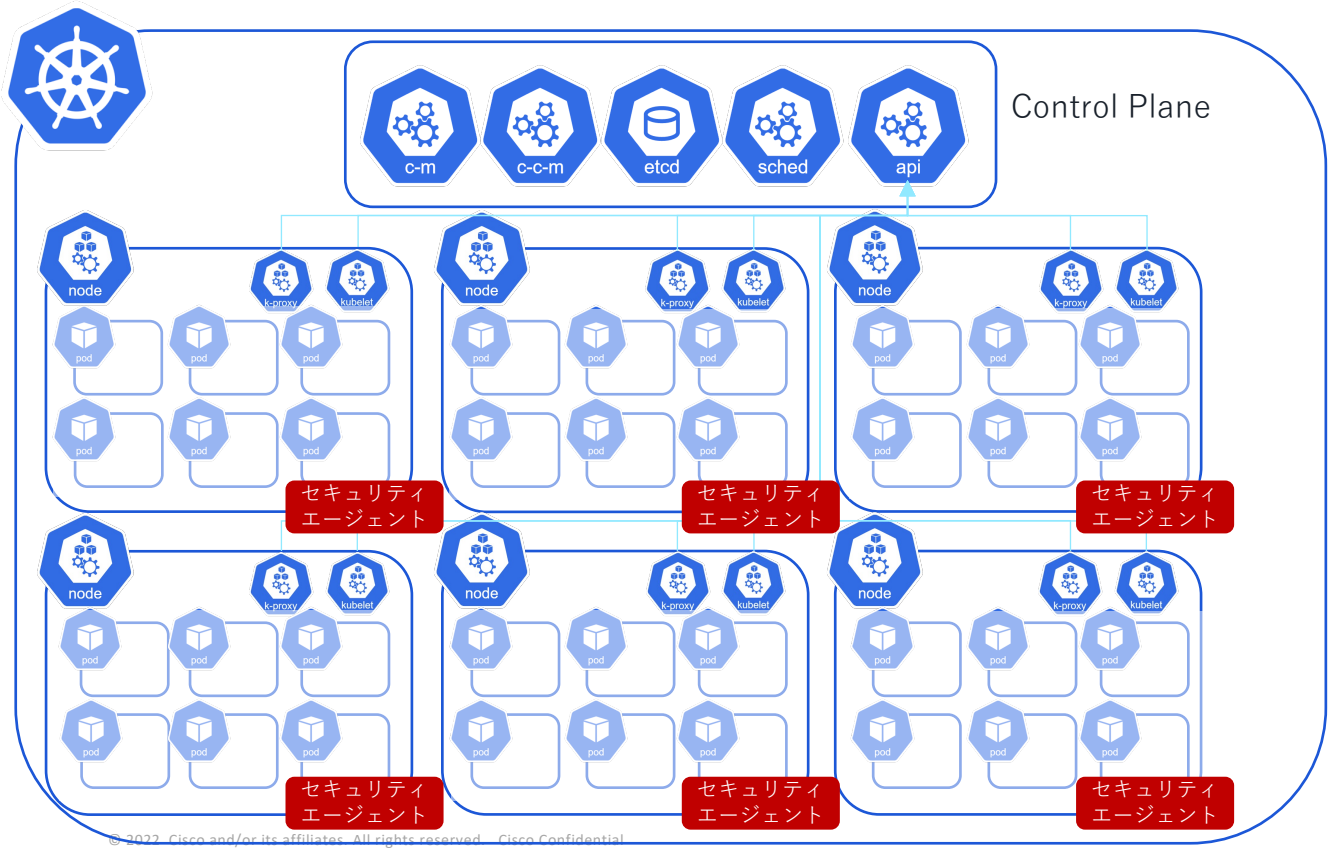
- Kube Clarityは、コンテナイメージやファイルシステムのSBOM（Software Bill Of Materials）や脆弱性を検出・管理するための、シスコが開発したオープンソースツール
- ランタイムのK8sクラスタとCI/CDパイプラインの両方をスキャンし、ソフトウェアサプライチェーンセキュリティを強化

https://github.com/openclarity/kubeclarity/

- API Clarityは、APIの脆弱性や脅威を検出するための、シスコが開発したオープンソースツール
- 非推奨のAPI、文書化されていないAPI、文書化されているものと異なる挙動を示すAPIを使用しているマイクロサービスを特定することが可能

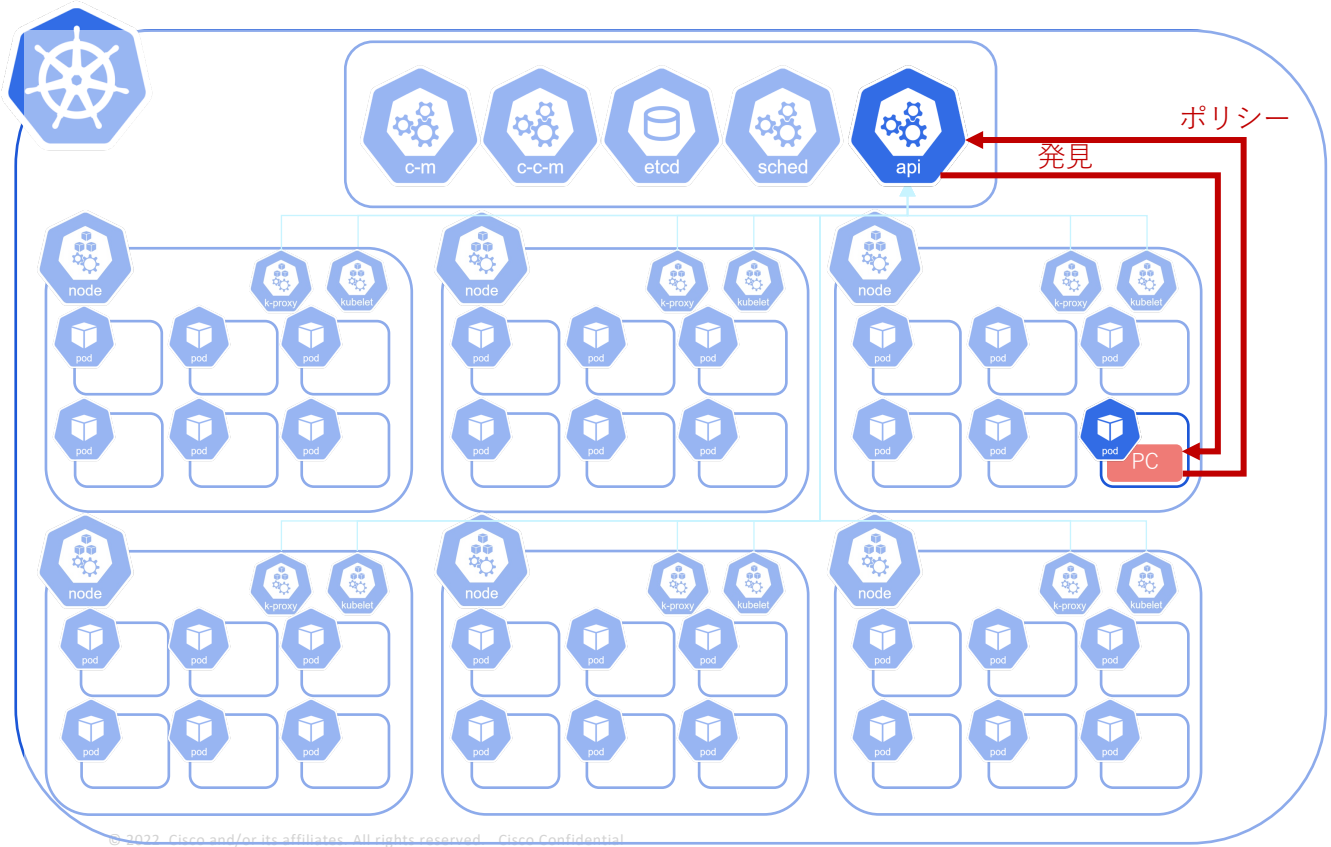
https://www.apiclarity.io/

エージェントベースのアーキテクチャ



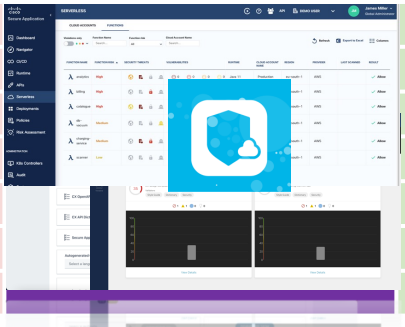
- 多くの場合、コンテナのセキュリティにエージェントベースのアプローチを使用しています
- このアプローチでは、個別のエージェントをインストールし、各ワーカー ノードに合わせて調整する必要があります。
- このようなアプローチは、スケーラビリティとパフォーマンスを制限します

エージェントレスアーキテクチャ - Panoptica



- Panopticaは、コンテナのセキュリティにエージェントレスのアプローチを利用しています
- Panopticaが必要とする唯一の専用リソースは、Panoptica Controller (PC) として機能するClusterごとに 1 つのポッドです
- Panopticaは、Kubernetes API サーバー内のネイティブ Kubernetes アドミッション コントローラー機能を利用してポリシーを適用します

その他のCisco Panopticaの特徴

特徴	説明	Powered By	備考
Universal scan	ソースコードとコンテナイメージの脆弱性スキャン	KUBE Clarity	
Runtime scan	K8sをスキャンし、そのリスクの正確なスナップショットを提供		
S-BoM creation	リスクとその関連性を迅速に検出するためのS-BOMの作成		
Flexible	アプリ全体のスキャン、複数のスキャナの使用、特定の脆弱性と深刻度の警告		
Accurate	複数の脆弱性フィードを使用し、効果的かつ正確な発見を実現		
Frictionless	アプリのコード変更は不要		
Automated	APIトラフィックを観測し、OpenAPI仕様を構築する		
Reconcile and Drift	OpenAPI仕様のアップロードとレビュー、時間経過による差分のトラッキング		
Zombies & Shadows	非推奨のAPIや文書化されていないAPIの使用状況の可視化	API Clarity	
Test	APIをファズしてテストし、脆弱性、認証ミスなどを発見する		
Visual	UIダッシュボードによるAPI所見の監査・監視		
Serverless scan	クラウドシステムにおけるサーバーレス機能のソフトウェアや設定の問題をスキャンする		
Policies	サーバーレス関数の実行を許可する際のルールを定義し、そのルールのEnforcement		
Integrate	一つのクラウドアカウントによりサーバーレス機能にアクセス		
Analyze	デプロイ前にアプリのAPIを分析し、APIを経時的に追跡		
Deploy	APIゲートウェイの背後にアプリを自動的にデプロイし、アプリをインターネットに接続		
Periodic Test	APIを毎日テストし、ファジングを行い、機能クリープを検出		
Manage	APIのセキュリティ脆弱性を管理し、アプリの停止、報告、ブロックを行う		

まとめ – Ciscoの取り組み

- Calisti - Service Meshの課題に対して
  - Multi-Primary Control Plane & Gatewayのサポート
  - マルチテナントのサポート
  - 非同期メッセージングへの対応

- Panoptica - Cloud Native Securityの課題に対して
  - Present – イメージ・ファイルシステム・API・SBOM等すべてを可視化
  - Control – 可視化した対象を制御
  - Prioritize – 脆弱性・脅威の順位付け
  - Define – 様々なポリシーをカスタマイズして定義・実施

無料で使用できます！

- Calistic は calisti.app から
  - 機能制限も時間制限もありません
  - 10 ノードのスケーラビリティ制限のみ
  - 追加のノードサポートのライセンスを取得できます
- Panopticaはpanoptica.app から
  - 無料利用枠で利用できます (単一Cluster内の最大 5 ノード)
  - 追加のノードサポートのライセンスを取得できます
  - Demo用ページもあります！
    - https://demo.panoptica.app/


cisco
The bridge to possible
Thank you