

Aqua Security × OKE

AWSでも実績多数のDocker環境セキュリティ・ソリューションを
デモで分かりやすく解説

日本オラクル株式会社
クラウド事業戦略統括
ビジネス推進本部
田中隆三郎

Modern Cloud Day Tokyo

次世代クラウドが変える日本のビジネス



以下の事項は、弊社の一般的な製品の方向性に関する概要を説明するものです。また、情報提供を唯一の目的とするものであり、いかなる契約にも組み込むことはできません。以下の事項は、マテリアルやコード、機能を提供することをコミットメント（確約）するものではないため、購買決定を行う際の判断材料になさらないで下さい。オラクル製品に関して記載されている機能の開発、リリースおよび時期については、弊社の裁量により決定されます。

OracleとJavaは、Oracle Corporation 及びその子会社、関連会社の米国及びその他の国における登録商標です。文中の社名、商品名等は各社の商標または登録商標である場合があります。

本セッションの流れ

ORACLE®

Cloud Infrastructure

1. コンテナ技術が必要とされる背景
2. Oracle Cloudのコンテナ・サービスとその特徴

※スピーカ交代



CREATIONLINE, INC.

3. コンテナ・セキュリティが必要とされる背景
4. Aqua Securityとその特徴
5. Aqua Securityのデモ
6. まとめ



コンテナ技術が必要とされる背景： ペースレイヤリング

新しいビジネスに対応するにはアプリケーションを高頻度で更新する必要がある



Systems of
Innovation

新しいビジネス
の発見

- 新たなビジネス要件や機会に対処するために構築される新規アプリケーション。
- ライフサイクルは12カ月未満と短い。



Systems of
Differentiate

既存ビジネスの
遂行

- 企業固有のプロセスや業界固有の機能を実現。
- ライフサイクルは1～3年程度だが、頻繁に変更・強化して変化に対応する必要がある。



Systems of
Record

バックオフィス
業務

- 中核的なトランザクション処理を担い、企業の重要なマスターデータを管理。
- 変更のペースは遅い。

更新頻度
高



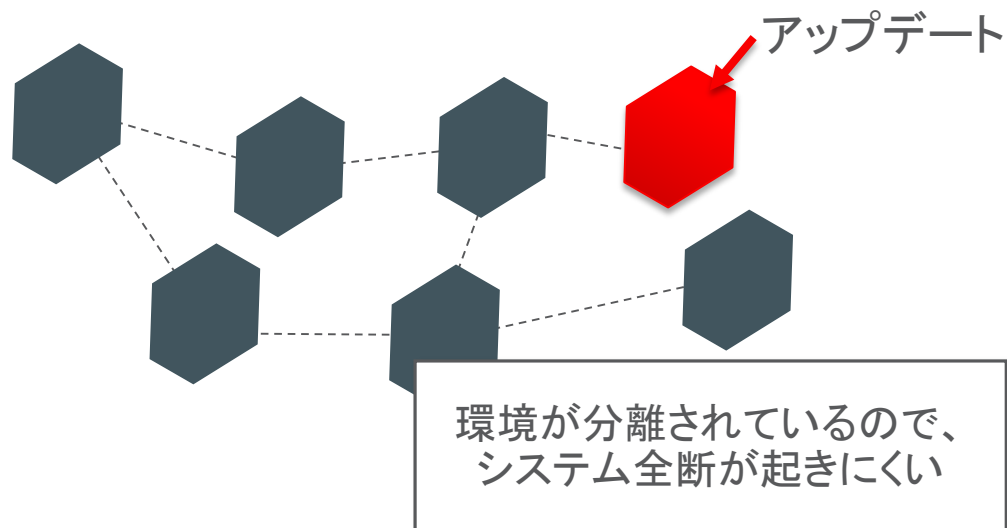
更新頻度
低

参考:「ペースレイヤリング」が変えるIT戦略 <http://itpro.nikkeibp.co.jp/article/COLUMN/20120306/384850>

コンテナ技術が必要とされる背景： 高頻度リリースを実現するための開発トレンド

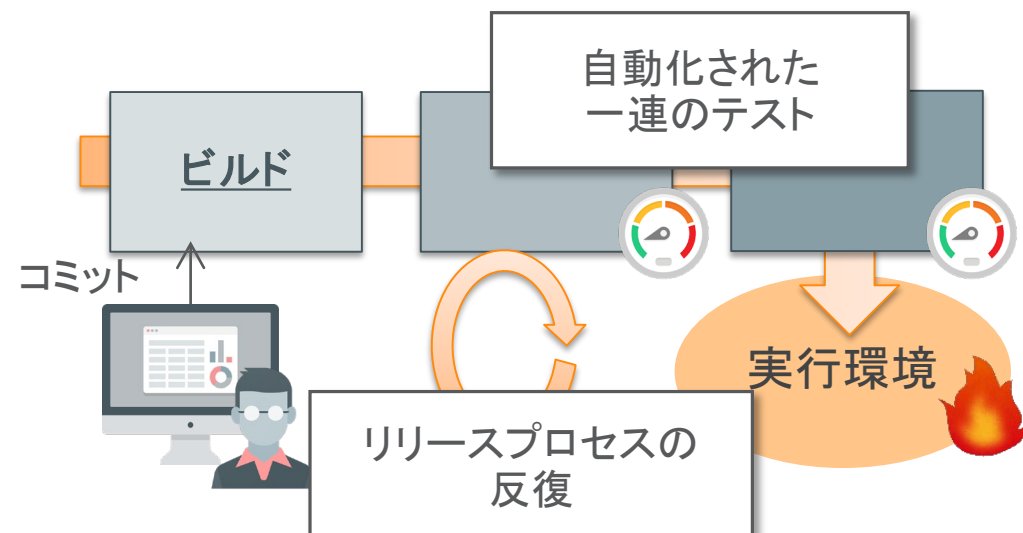
・マイクロサービス・アーキテクチャ

- 大規模なシステムを疎結合な複数のサービスの組み合わせで実現する設計方式
- 変更の影響範囲をサービス単位に留められるため、高頻度のリリースに適する



・継続的インテグレーション/デリバリー

- ソースコードの変更から、本番環境へのリリースまでのプロセスを極力自動化
- 人手を極力排したテスト・リリースにより、アプリの品質の安定と高頻度リリースを実現する



コンテナ技術が必要とされる背景：

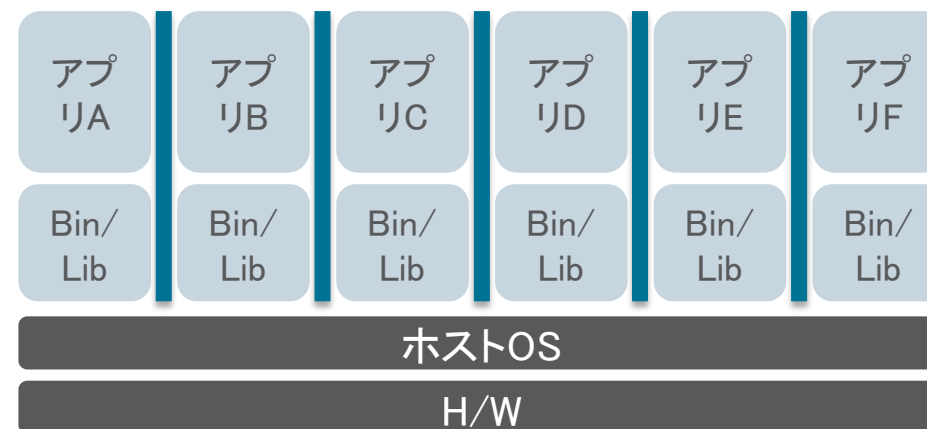
なぜコンテナが注目を浴びているのか…？

マイクロサービスの構築に、コンテナの独立性と高集約性が寄与

- コンテナにより、少容量、低オーバーヘッドの仮想的環境を実現
- 多数のサービスを可動させるマイクロサービスにコンテナが適する



従来型の仮想化



コンテナ型仮想化

コンテナ技術が必要とされる背景： コンテナ・オーケストレータ

- コンテナのデプロイ・スケーリング等を管理するプラットフォーム
 - 自動分散配置（HWを意識しない）
 - 手動／自動でスケーリング
 - 複数コンテナをまとめて制御
 - 障害時のコンテナ再立ち上げ
 - クラスタ内／外のネットワークアクセスの管理
- Kubernetesがデファクト・スタンダードになりつつある状況



kubernetes

Oracle Cloudのコンテナ・サービスとその特徴：

Oracle Container Engine for Kubernetes (OKE)

エンタープライズ品質と開発生産性を両立するKubernetesプラットフォーム

エンタープライズ品質を維持する確実な性能と可用性

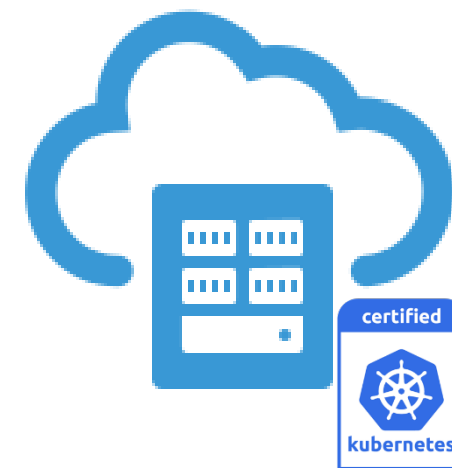
- 次世代インフラストラクチャによるばらつきのない高性能な分散アプリケーション環境
- アプリケーション環境と管理ノードの冗長化を自動的に構成し高可用性システムを実現

マネージド環境による開発への注力の実現と費用対効果

- 複雑なKubernetes環境の構築を不要としアプリケーション開発を即座に開始
- 追加費用を一切不要とする標準機能としてのマネージドKubernetes環境

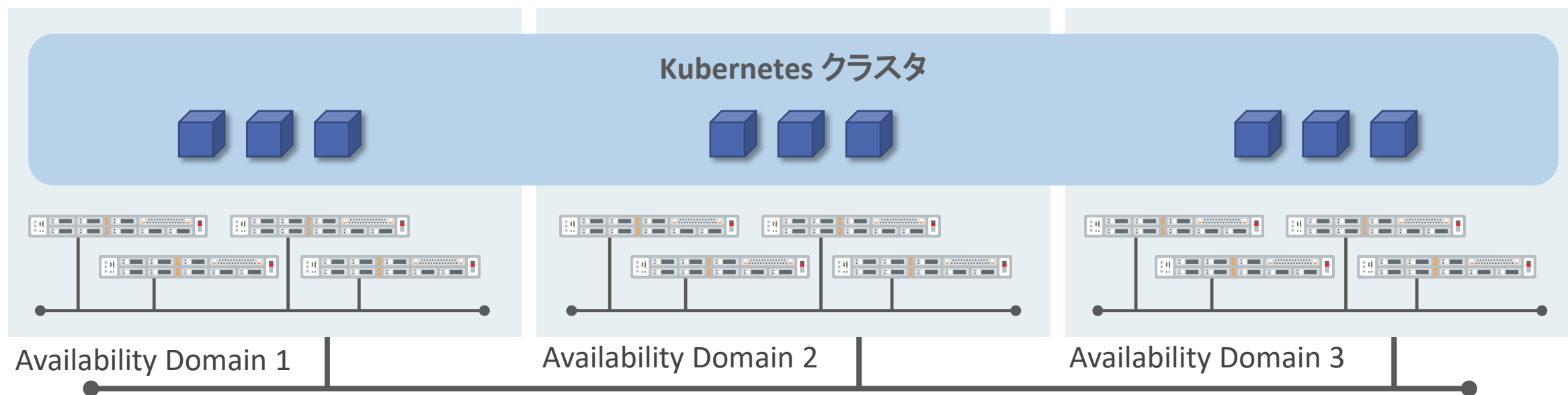
ニーズにいち早く対応する豊富なクラウドサービスとの親和性

- 迅速なアプリケーション開発を支えるCloud Native Frameworkとの連携
- 様々なビジネスニーズの迅速な実現にフォーカスするOracle PaaSサービス群との連携



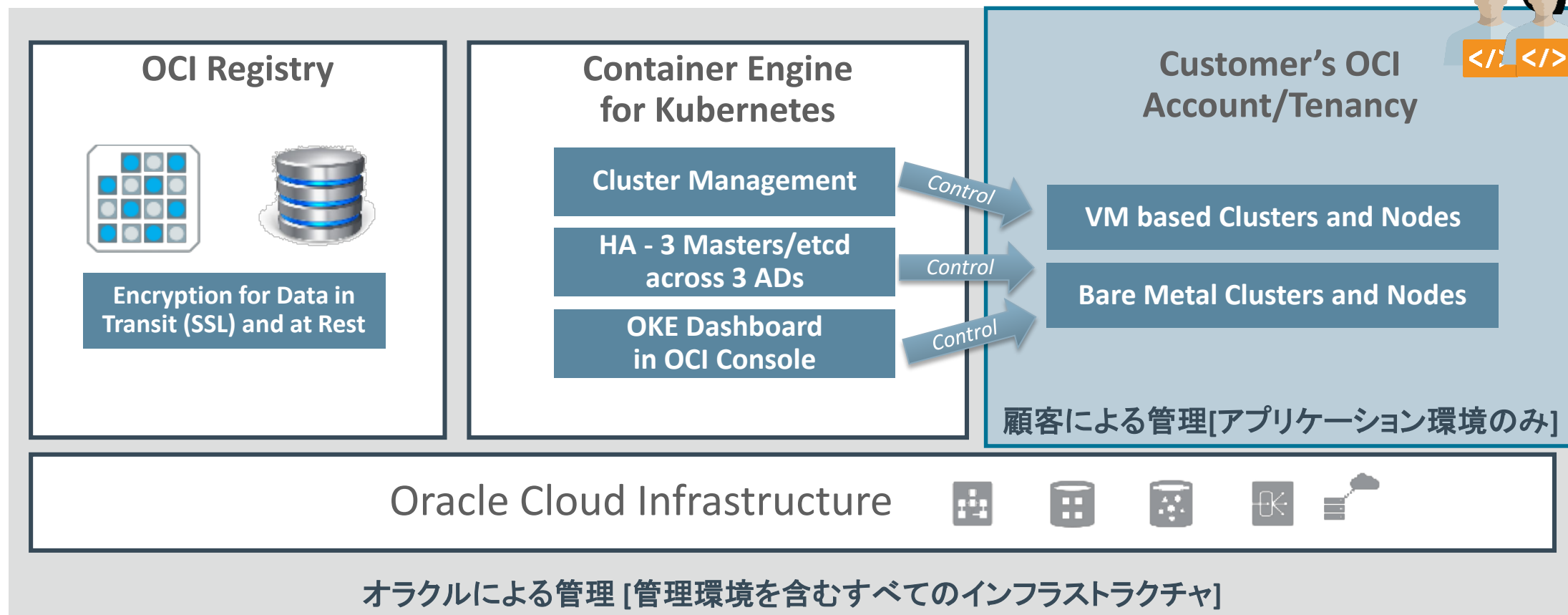
Oracle Cloudのコンテナ・サービスとその特徴：
エンタープライズ品質のコンテナ・オーケストレータ
エンタープライズに最適なパフォーマンス・可用性を実装したKubernetes基盤

- 次世代IaaS上にKubernetesクラスタを構築し、**安定したパフォーマンス**
- ドメインを横断してクラスタを構成を標準とする、**高可用性アーキテクチャ**



Oracle Cloudのコンテナ・サービスとその特徴： アプリケーション開発への注力を実現するマネージド環境

容易な環境構築と運用負担の極小化を実現するOKEの責任分掌モデル

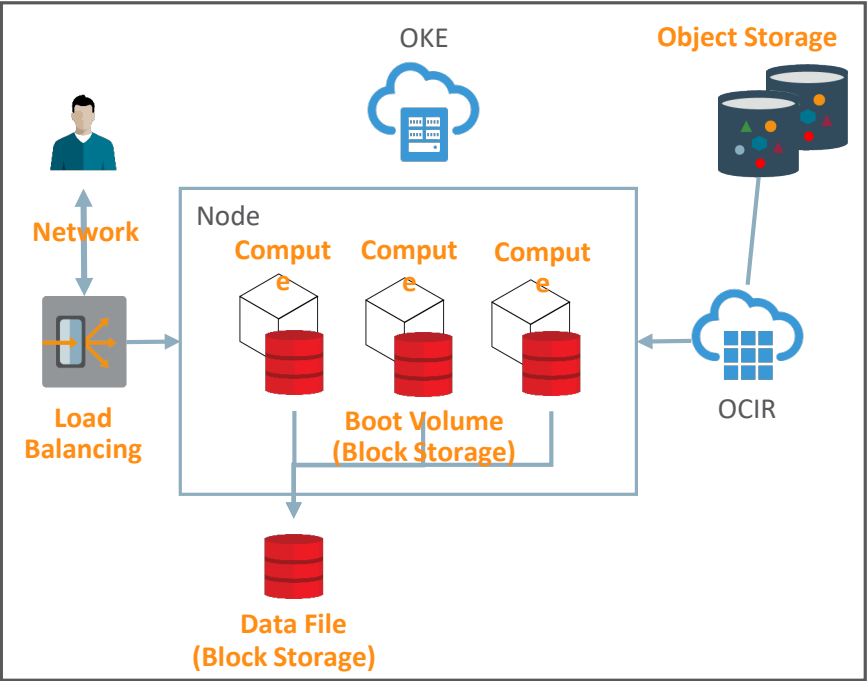


Oracle Cloudのコンテナ・サービスとその特徴：
OCI標準機能として提供されるKubernetesプラットフォーム

追加費用を不要とする費用対効果の高いKubernetes環境

- Kubernetesクラスタとレジストリに必要なIaaSリソースに対する費用のみ
- Master Nodeを含むKubernetesの管理ノードの費用は一切不要

展開イメージ



	必要となるOCIリソース
OKE (Kubernetesクラスタ)	Compute
	Block Storage
	Load Balancing
	Network(Data Transfer)
OCIR (コンテナレジストリ)	Object Storage

ここまでのまとめ

1. コンテナ・テクノロジーが必要とされる背景

- 新しいビジネスに対応するには**アプリケーションを高頻度で更新**する必要がある
 - 高頻度リリースを実現するための開発トレンドの**マイクロサービス**・アーキテクチャ
 - マイクロサービスの構築に、**コンテナ**の独立性と高集約性が寄与
 - コンテナ・オーケストレータの**Kubernetes**

2. Oracle Cloudのコンテナ・サービスとその特徴

- **Oracle Container Engine for Kubernetes (OKE)**
 - エンタープライズ品質の**パフォーマンス・可用性**
 - 容易な環境構築と**運用負担の極小化**（マネージド・サービス）
 - 追加費用を不要とする**費用対効果の高いKubernetes環境**



こんな時、かけこむ会社が増えています。



ビジネスプロセスを
改善したい!



今のシステムは
使いにくい!



システムコストを
下げたい!



パフォーマンスを
良くしたい!



経営分析を
したいのだが...



どんなソリューションが
あるの?



見積りはどれくらい
なんだろう?



楽に管理を
したい!

Oracle Digitalは、オラクル製品の導入をご検討いただく際の総合窓口。
電話とインターネットによるダイレクトなコミュニケーションで、どんなお問い合わせにもすばやく対応します。
もちろん、無償。どんなことでも、ご相談ください。



お問い合わせは電話またはWebフォーム

☎ 0120-155-096

受付時間 月～金 9:00-12:00 / 13:00-17:00
(祝日および年末年始休業日を除きます)

<http://www.oracle.com/jp/contact-us>

ORACLE®



Aqua Security概要

2019年8月7日（水）
クリエーションライン株式会社
マグルダー 健人

アジェンダ

1. 会社紹介
2. Aqua Security 概要
3. Aqua Security 機能紹介 (デモ)
4. まとめ (Aqua Securityとコンテナのライフサイクル)

アジェンダ

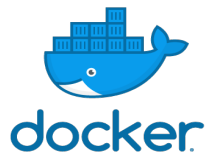
1. 会社紹介
2. Aqua Security 概要
3. Aqua Security 機能紹介 (デモ)
4. まとめ (Aqua Securityとコンテナのライフサイクル)

クリエーションライン株式会社



CREATIONLINE, INC.

サブスクリプション製品販売・導入コンサル



クリエーションライン株式会社

先日行われましたCNDT2019(Cloud Native Days Tokyo)にてLinux Foundationよりご紹介いただきました。

- ・ KCSP
- ・ KTP
- ・ Member

※弊社はLinux Foundation認定Kubernetesトレーニングを提供しています。(日本で唯一)

弊社URL : <https://www.creationline.com>

Kubernetes.io : <https://kubernetes.io/partners/>



アジェンダ

1. 会社紹介
- 2. Aqua Security 概要**
3. Aqua Security 機能紹介 (デモ)
4. まとめ (Aqua Securityとコンテナのライフサイクル)

Aqua Security Software Ltd.のご紹介について(1)

- 設立 : 2015年
- 本社 : イスラエル
- 事業 : コンテナ向けセキュリティ製品を提供



Dror Davidoff
Co-Founder and CEO
元Mcafee



Amir Jerbi
Co-Founder and CTO
元CA Technologies



Michael Cherny
Chief Architect
元Imperva



Liz Rice
Technology Evangelist
2018年Kube-Con議長

Aqua Security Software Ltd.のご紹介について(2)

- セキュリティプロバイダー出身のスペシャリスト集団で構成。
- AWS、Azure、GCP、OracleCloud等主要クラウドプロバイダーともパートナー関係。
- M12(Microsoft Ventures Found)はじめとするベンチャーキャピタルも出資。
- 米国Fortune500に選ばれている60社以上の企業で採用実績あり。

TEAM

80 passionate, experienced innovators coming from:

McAfee

ca
technologies

SAP

Microsoft

IBM

Check Point
SOFTWARE TECHNOLOGIES LTD.

IMPERVA CYBERARK

STRATEGIC PARTNERSHIPS

amazon
web services

Microsoft
Azure

RED HAT
OPENSIFT

IBM

Google Cloud Platform

docker

CLOUD NATIVE
COMPUTING FOUNDATION

Pivotal
Cloud Foundry

vmware

splunk

BACKED BY

Microsoft Ventures | Lightspeed | Shlomo Kramer | TLV Partners

◎ Boston

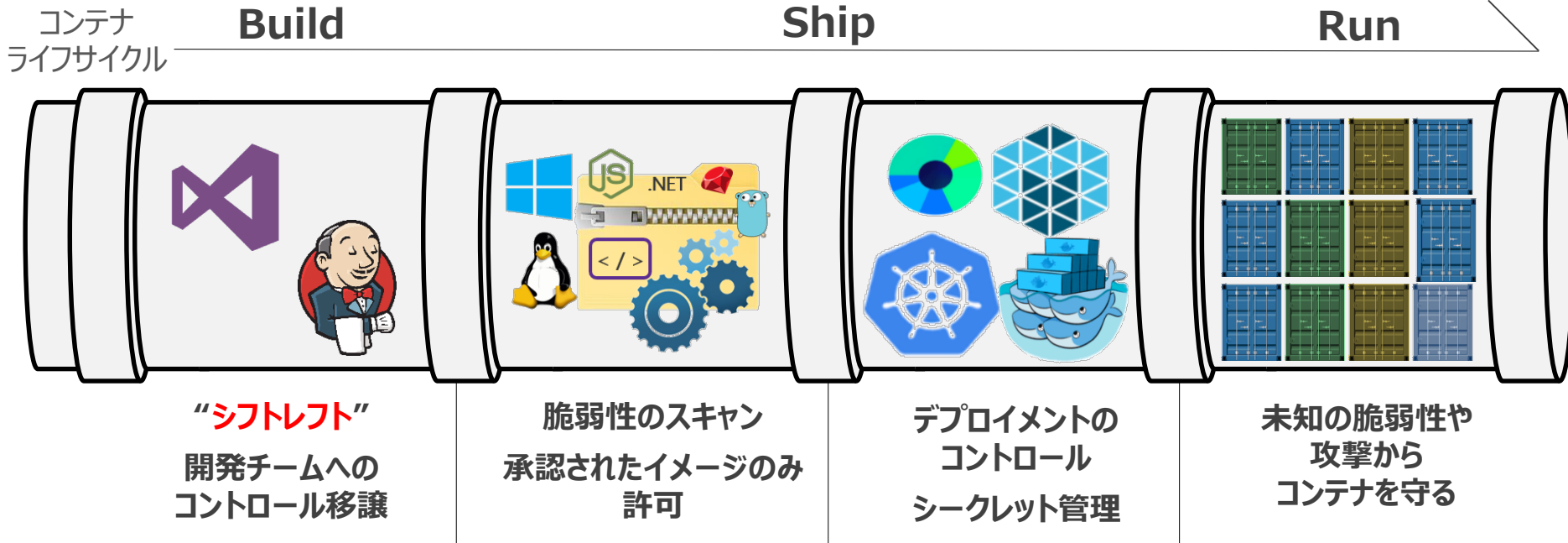
◎ San Francisco

◎ Sydney

◎ Tel Aviv

コンテナのライフサイクルとAqua Securityのセキュリティイメージ

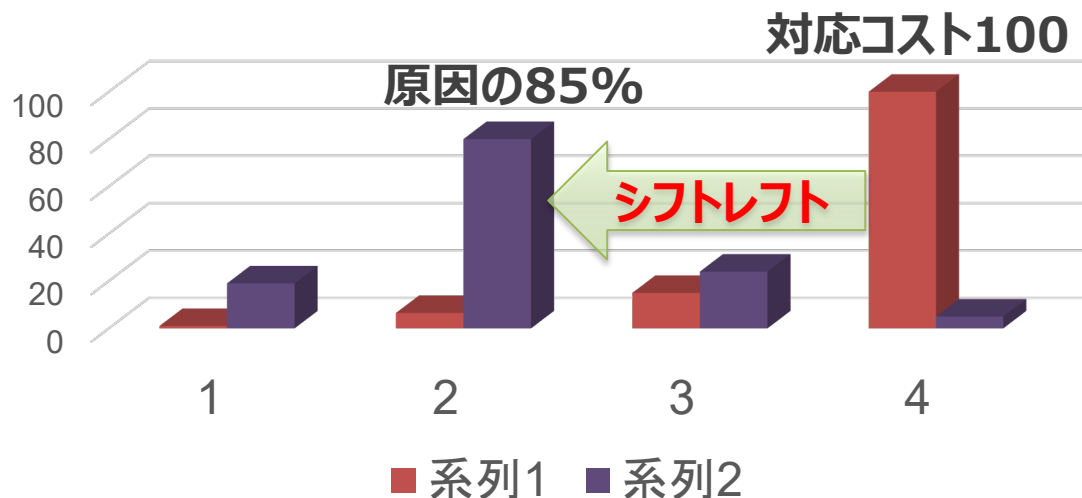
コントロールの移譲 → インシデントの削減 → コンプライアンスの実現



シフトレフトとは？

セキュリティに問題があるシステムの原因の大部分は設計と構築時の問題であり、
また後期段階での対応はコストが非常に高くなる

⇒開発のより早い段階でセキュリティ対策を施すこと(**シフトレフト**の実践)が大切



Aqua Security の3つのアプローチ

DevSecOps の自動化



- CI/CD パイプライン全体を守る
- セキュリティの“シフトレフト”、問題は早い段階で発見、対処
- セキュリティの自動化でアプリのデリバリーを早める

コンテナ全般への 次世代のセキュリティ



- イミュータブル(不変)の徹底
=変更や追加は不可
- ホワイトリストによる制御、異常な挙動を検知
- マイクロサービスレベルのファイアウォールによるアクセス制御
- 状況の可視化とコンプライアンス対応

一度の導入で、あらゆる プラットフォームに対応

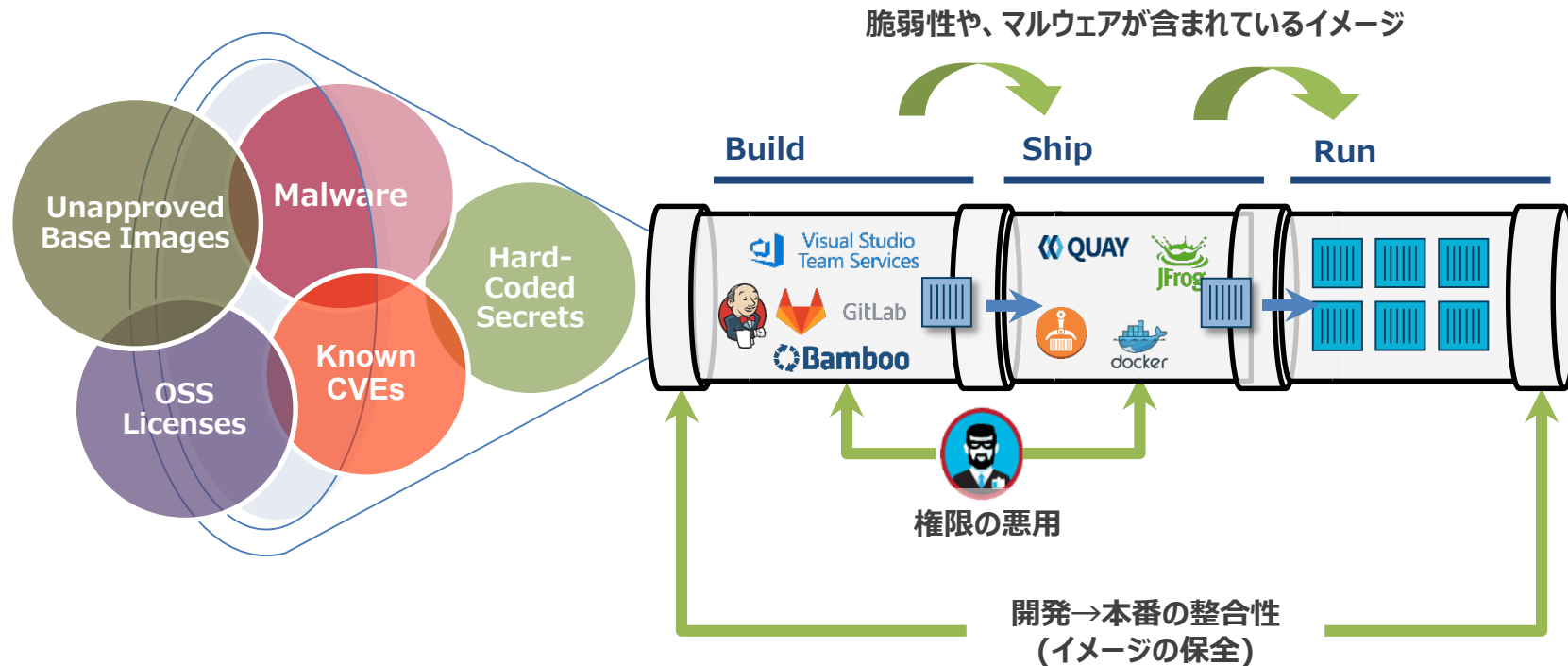


- プラットホーム、クラウド、OSに関わらずアプリを守る
- ハイブリッドクラウドやクラウド移行が可能

DevSecOpsの自動化：パイプラインのセキュリティ(課題)

課題

DevOpsの速度を損なうことなく、安全なソフトウェア供給チェーンを実現

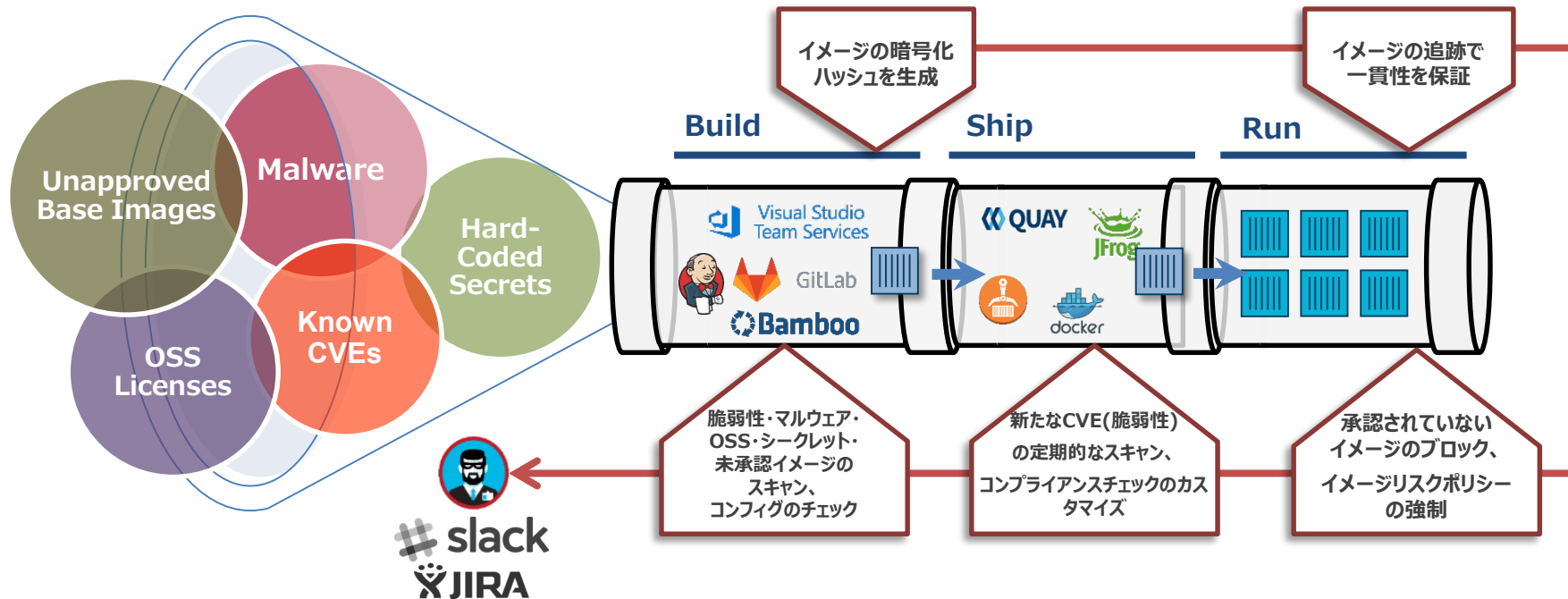


DevSecOpsの自動化：パイプラインのセキュリティ(ソリューション)

Aquaのソリューション

“シフトレフト”

⇒ セキュリティチェックの自動化とイメージの検知を開発初期段階で実施

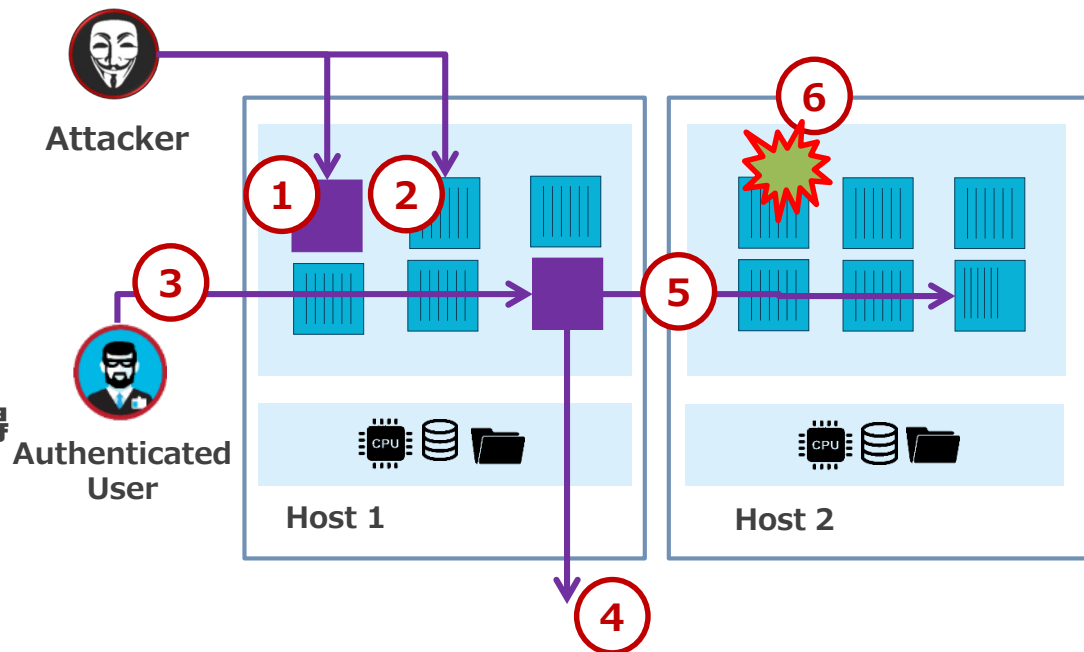


コンテナ全般への次世代のセキュリティ(課題)

課題

大規模なデプロイ環境への侵入、攻撃を未然に防止

1. 不正なコンテナ(例:クリプトマイニング)
2. 不正コード注入
3. 不適切な権限による内部の不正操作
4. 不法なデータ漏洩
5. 外部の攻撃者によるネットワーク資源取得
6. 未知の攻撃(ゼロデイ攻撃)



コンテナ全般への次世代のセキュリティ(ソリューション)

Aquaのソリューション

手動または機械学習によるデータを用いて、
必要最小限の権限利用とイミュータブル(不変)を徹底

課題

1. 不正なコンテナ(例:クリプトマイニング)
2. 不正コード注入
3. 不適切な権限による内部の不正操作
4. 不法なデータ漏洩
5. 外部の攻撃者によるネットワーク資源取得
6. 未知の攻撃(ゼロデイ攻撃)

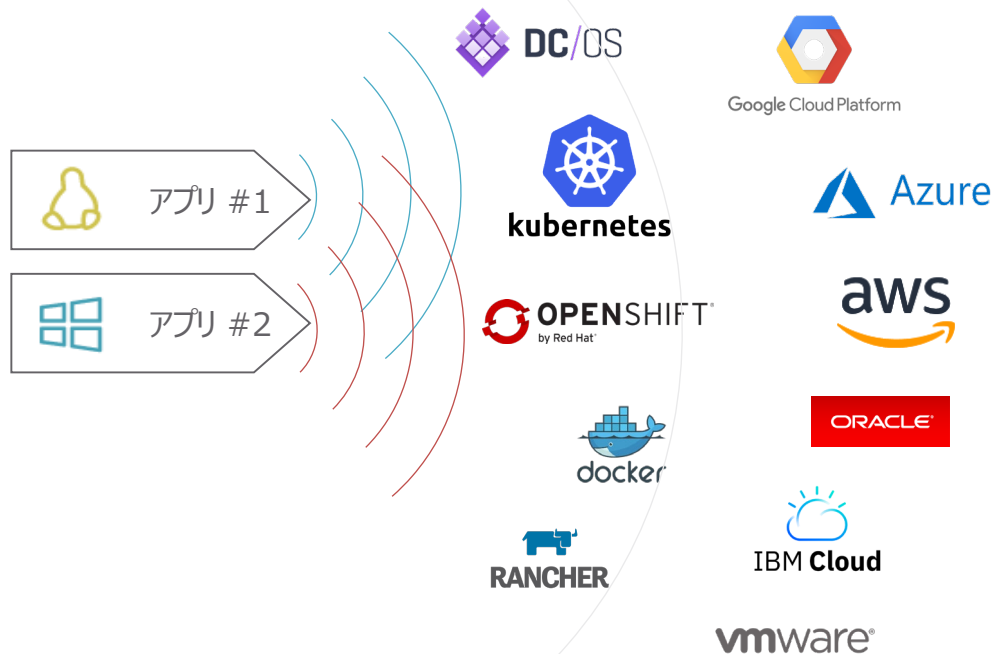
Aquaのソリューション

- 1. 承認されていないイメージをブロック
- 2. イメージの変更を防止(=イミュータブル)
- 3. 必要最小限の権限利用のみ許可
- 4. 安全なシークレット管理 + 未承認の外部向け接続をブロック
- 5. コンテナファイアウォールで許可されない接続を阻止
- 6. 機械学習とホワイトリスト化により、コンテナのアクション
(実行環境、処理内容、ファイル、ボリューム、リソース等)を限定

あらゆる環境でアプリを守る

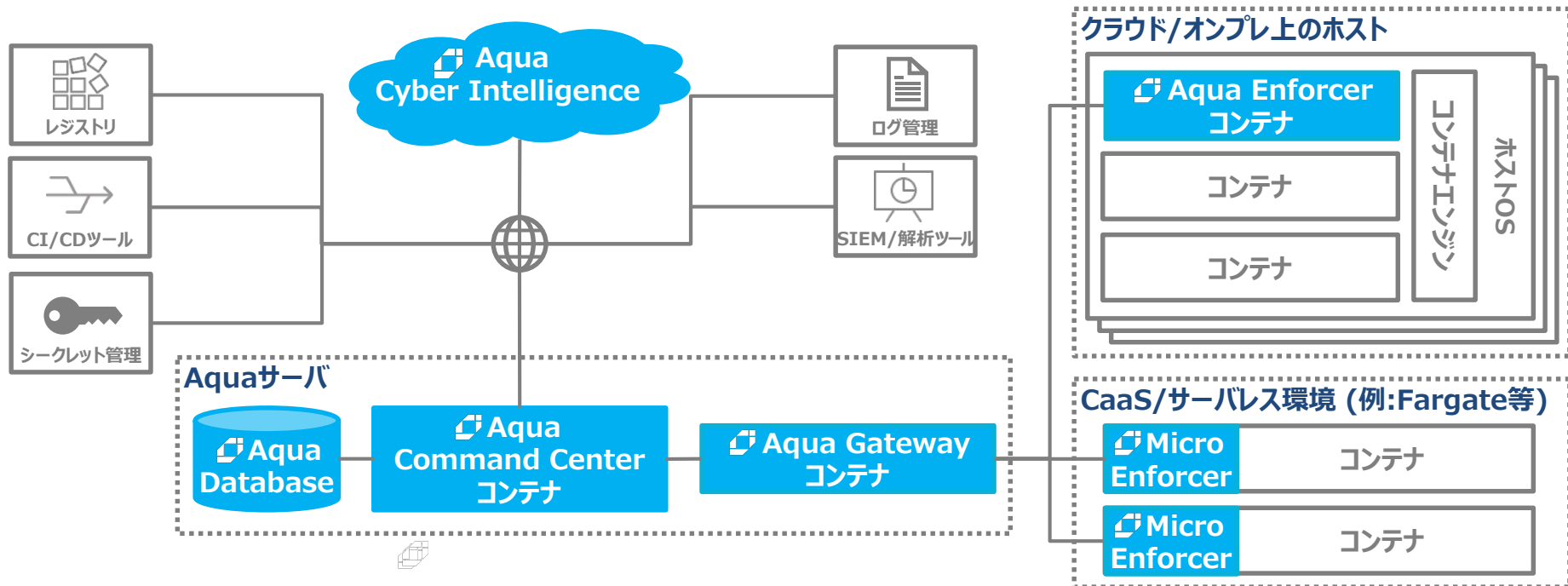
Aquaのソリューション

一度の導入であらゆるプラットフォームに対応、
セキュリティはアプリと共にインフラを移動



- LinuxとWindowsコンテナ
- あらゆるオーケストレータ :
Kubernetes、OpenShift、DC/OS、
Docker Swarm、etc
- クラウドでもオンプレでも :
Oracle Cloud Infrastructure、AWS、
Azure、GCP、Pivotal Cloud、etc
- CaaS :
AWS Fargate、Azure ACI
- マルチテナント管理

Aqua Security コンポーネント構成イメージ



アジェンダ

1. 会社紹介
2. Aqua Security 概要
- 3. Aqua Security 機能紹介 (デモ)**
4. まとめ (Aqua Securityとコンテナのライフサイクル)

Aqua Security 機能紹介

ここからはデモをお見せ致します。

Aqua Security 機能紹介

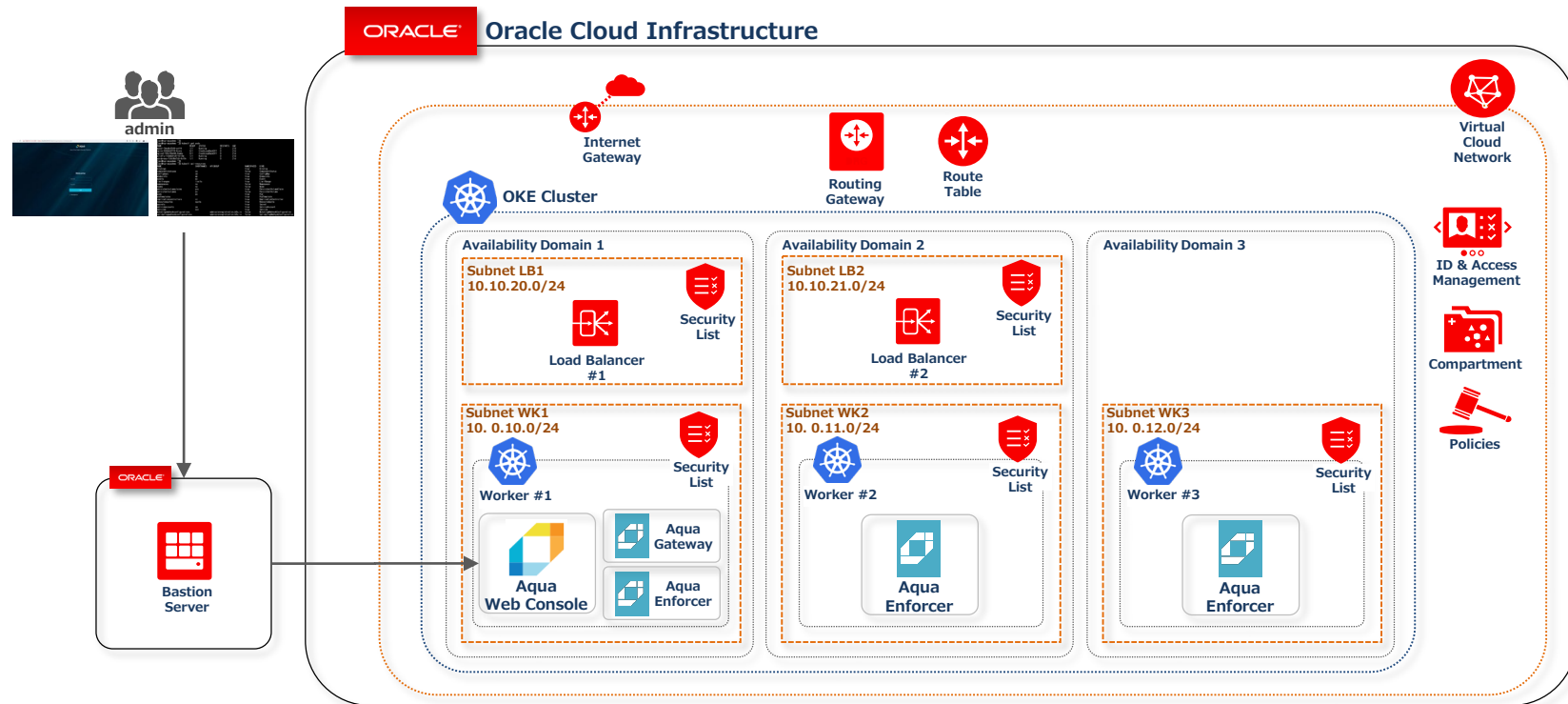
No.	機能	説明
1	Image Scan (イメージスキャン)	イメージ内に含まれる、既知の脆弱性(CVE)やマルウェア、ハードコーディングされたシークレットなど、セキュリティ上のリスクを検知します。
2	Assurance Policy (イメージスキャン設定)	イメージスキャンに関する細かな設定を組むことが可能です。
3	Runtime Policy (ランタイムポリシー)	実行中のコンテナを監視し、ポリシーにしたがってコンテナの動作を制御/制限します。また機械学習によりポリシーを生成することも可能です。
4	Container Firewall (コンテナファイアウォール)	コンテナのネットワーク接続を視覚化、また、コンテナ単位で接続の許可/拒否をルール設定できます。
5	Secrets (シークレット管理)	コンテナに対して、セキュアな方法でパスワードやSSHキーなどのシークレットをデリバリできます。
6	Compliance (コンプライアンス対応)	リスクを一覧化し、対応方法などを含む詳細レポートを生成します。また、イメージやコンテナで発生した各種セキュリティイベントも収集されます。
7	Integration (外部ツール/サービス統合)	Docker Hubなどのレジストリ、JenkinsなどのCI/CDツール、SplunkなどのSIEMサービスなど、さまざまな外部ツールやサービスとの統合/連携が可能です。
8	vShield ← New! (仮想パッチ機能)	Runtime Policyの一環として、既知の脆弱性を持つ実行中コンテナに対しての脆弱性を狙った攻撃を検知/ブロックすることが可能です。

Aqua Security 機能紹介

No.	機能	説明
1	Image Scan (イメージスキャン)	イメージ内に含まれる、既知の脆弱性(CVE)やマルウェア、ハードコーディングされたシークレットなど、セキュリティ上のリスクを検知します。
2	Assurance Policy (イメージスキャン設定)	イメージスキャンに関する細かな設定を組むことが可能です。
3	Runtime Policy (ランタイムポリシー)	実行中のコンテナを監視し、ポリシーにしたがってコンテナの動作を制御/制限します。また機械学習によりポリシーを生成することも可能です。
4	Container Firewall (コンテナファイアウォール)	コンテナのネットワーク接続を視覚化、また、コンテナ単位で接続の許可/拒否をルール設定できます。
5	Secrets (シークレット管理)	コンテナに対して、セキュアな方法でパスワードやSSHキーなどのシークレットをデリバリできます。
6	Compliance (コンプライアンス対応)	リスクを一覧化し、対応方法などを含む詳細レポートを生成します。また、イメージやコンテナで発生した各種セキュリティイベントも収集されます。
7	Integration (外部ツール/サービス統合)	Docker Hubなどのレジストリ、JenkinsなどのCI/CDツール、SplunkなどのSIEMサービスなど、さまざまな外部ツールやサービスとの統合/連携が可能です。
8	vShield ← New! (仮想パッチ機能)	Runtime Policyの一環として、既知の脆弱性を持つ実行中コンテナに対しての脆弱性を狙った攻撃を検知/ブロックすることが可能です。

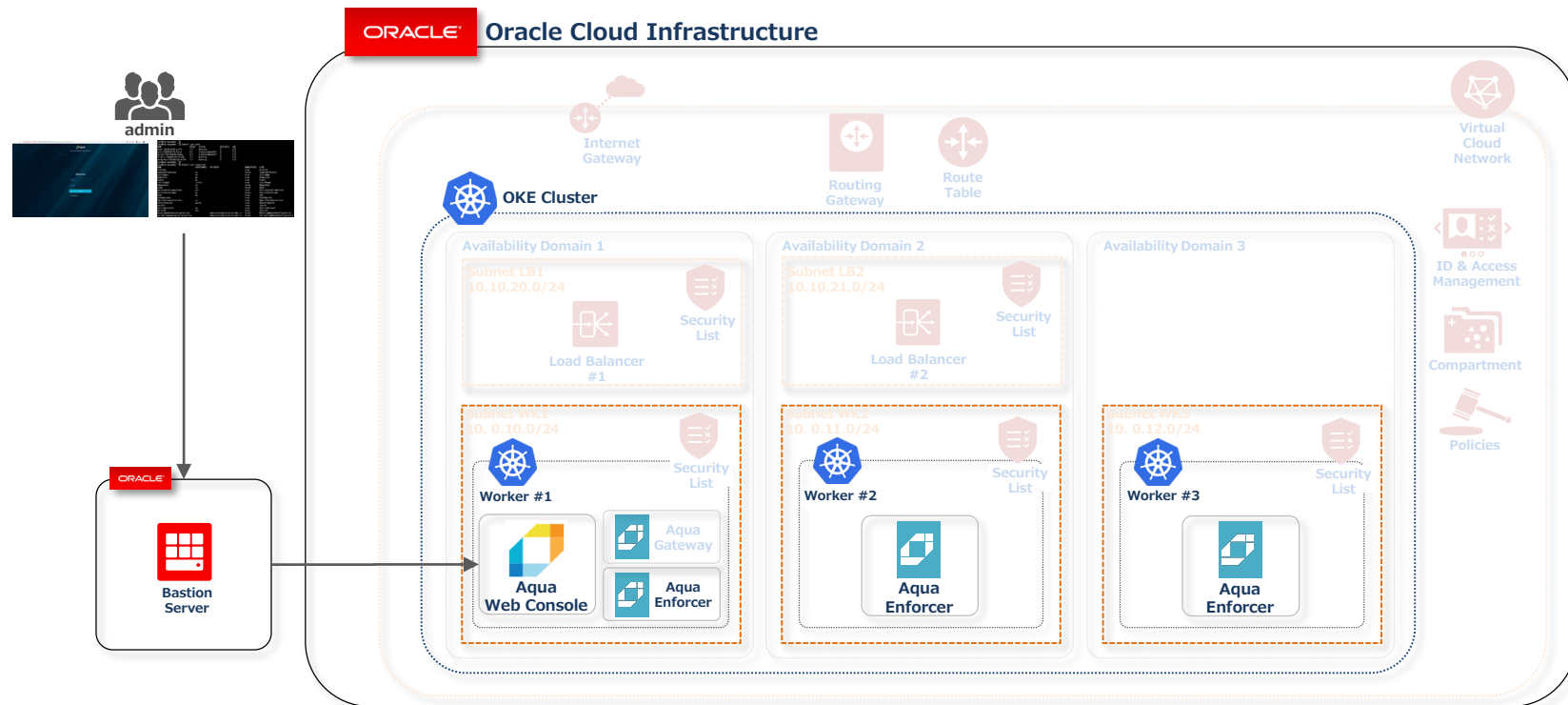
デモ環境イメージ

- OKE(Oracle Container Engine for Kubernetes)を利用
- AquaSecurity 関連コンポーネントはPod(コンテナ)上で稼働



デモ環境イメージ (本日の登場箇所)

- OKE(Oracle Container Engine for Kubernetes)を利用
- AquaSecurity 関連コンポーネントはPod(コンテナ)上で稼働



Aqua Security 機能紹介

No.	機能	説明
1	Image Scan (イメージスキャン)	イメージ内に含まれる、既知の脆弱性(CVE)やマルウェア、ハードコーディングされたシークレットなど、セキュリティ上のリスクを検知します。
2	Assurance Policy (イメージスキャン設定)	イメージスキャンに関する細かな設定を組むことが可能です。
3	Runtime Policy (ランタイムポリシー)	実行中のコンテナを監視し、ポリシーにしたがってコンテナの動作を制御/制限します。また機械学習によりポリシーを生成することも可能です。
4	Container Firewall (コンテナファイアウォール)	コンテナのネットワーク接続を視覚化、また、コンテナ単位で接続の許可/拒否をルール設定できます。
5	Secrets (シークレット管理)	コンテナに対して、セキュアな方法でパスワードやSSHキーなどのシークレットをデリバリできます。
6	Compliance (コンプライアンス対応)	リスクを一覧化し、対応方法などを含む詳細レポートを生成します。また、イメージやコンテナで発生した各種セキュリティイベントも収集されます。
7	Integration (外部ツール/サービス統合)	Docker Hubなどのレジストリ、JenkinsなどのCI/CDツール、SplunkなどのSIEMサービスなど、さまざまな外部ツールやサービスとの統合/連携が可能です。
8	vShield ←New! (仮想パッチ機能)	Runtime Policyの一環として、既知の脆弱性を持つ実行中コンテナに対しての脆弱性を狙った攻撃を検知/ブロックすることが可能です。

Aqua Security 機能紹介

No.	機能	説明
1	Image Scan (イメージスキャン)	イメージ内に含まれる、既知の脆弱性(CVE)やマルウェア、ハードコーディングされたシークレットなど、セキュリティ上のリスクを検知します。
2	Assurance Policy (イメージスキャン設定)	イメージスキャンに関する細かな設定を組むことが可能です。
3	Runtime Policy (ランタイムポリシー)	実行中のコンテナを監視し、ポリシーにしたがってコンテナの動作を制御/制限します。また機械学習によりポリシーを生成することも可能です。
4	Container Firewall (コンテナファイアウォール)	コンテナのネットワーク接続を視覚化、また、コンテナ単位で接続の許可/拒否をルール設定できます。
5	Secrets (シークレット管理)	コンテナに対して、セキュアな方法でパスワードやSSHキーなどのシークレットをデリバリできます。
6	Compliance (コンプライアンス対応)	リスクを一覧化し、対応方法などを含む詳細レポートを生成します。また、イメージやコンテナで発生した各種セキュリティイベントも収集されます。
7	Integration (外部ツール/サービス統合)	Docker Hubなどのレジストリ、JenkinsなどのCI/CDツール、SplunkなどのSIEMサービスなど、さまざまな外部ツールやサービスとの統合/連携が可能です。
8	vShield ←New! (仮想パッチ機能)	Runtime Policyの一環として、既知の脆弱性を持つ実行中コンテナに対しての脆弱性を狙った攻撃を検知/ブロックすることが可能です。

Aqua Security 機能紹介

No.	機能	説明
1	Image Scan (イメージスキャン)	イメージ内に含まれる、既知の脆弱性(CVE)やマルウェア、ハードコーディングされたシークレットなど、セキュリティ上のリスクを検知します。
2	Assurance Policy (イメージスキャン設定)	イメージスキャンに関する細かな設定を組むことが可能です。
3	Runtime Policy (ランタイムポリシー)	実行中のコンテナを監視し、ポリシーにしたがってコンテナの動作を制御/制限します。また機械学習によりポリシーを生成することも可能です。
4	Container Firewall (コンテナファイアウォール)	コンテナのネットワーク接続を視覚化、また、コンテナ単位で接続の許可/拒否をルール設定できます。
5	Secrets (シークレット管理)	コンテナに対して、セキュアな方法でパスワードやSSHキーなどのシークレットをデリバリできます。
6	Compliance (コンプライアンス対応)	リスクを一覧化し、対応方法などを含む詳細レポートを生成します。また、イメージやコンテナで発生した各種セキュリティイベントも収集されます。
7	Integration (外部ツール/サービス統合)	Docker Hubなどのレジストリ、JenkinsなどのCI/CDツール、SplunkなどのSIEMサービスなど、さまざまな外部ツールやサービスとの統合/連携が可能です。
8	vShield ←New! (仮想パッチ機能)	Runtime Policyの一環として、既知の脆弱性を持つ実行中コンテナに対しての脆弱性を狙った攻撃を検知/ブロックすることが可能です。

Aqua Security 機能紹介

No.	機能	説明
1	Image Scan (イメージスキャン)	イメージ内に含まれる、既知の脆弱性(CVE)やマルウェア、ハードコーディングされたシークレットなど、セキュリティ上のリスクを検知します。
2	Assurance Policy (イメージスキャン設定)	イメージスキャンに関する細かな設定を組むことが可能です。
3	Runtime Policy (ランタイムポリシー)	実行中のコンテナを監視し、ポリシーにしたがってコンテナの動作を制御/制限します。また機械学習によりポリシーを生成することも可能です。
4	Container Firewall (コンテナファイアウォール)	コンテナのネットワーク接続を視覚化、また、コンテナ単位で接続の許可/拒否をルール設定できます。
5	Secrets (シークレット管理)	コンテナに対して、セキュアな方法でパスワードやSSHキーなどのシークレットをデリバリできます。
6	Compliance (コンプライアンス対応)	リスクを一覧化し、対応方法などを含む詳細レポートを生成します。また、イメージやコンテナで発生した各種セキュリティイベントも収集されます。
7	Integration (外部ツール/サービス統合)	Docker Hubなどのレジストリ、JenkinsなどのCI/CDツール、SplunkなどのSIEMサービスなど、さまざまな外部ツールやサービスとの統合/連携が可能です。
8	vShield ←New! (仮想パッチ機能)	Runtime Policyの一環として、既知の脆弱性を持つ実行中コンテナに対しての脆弱性を狙った攻撃を検知/ブロックすることが可能です。

Aqua Security 機能紹介

No.	機能	説明
1	Image Scan (イメージスキャン)	イメージ内に含まれる、既知の脆弱性(CVE)やマルウェア、ハードコーディングされたシークレットなど、セキュリティ上のリスクを検知します。
2	Assurance Policy (イメージスキャン設定)	イメージスキャンに関する細かな設定を組むことが可能です。
3	Runtime Policy (ランタイムポリシー)	実行中のコンテナを監視し、ポリシーにしたがってコンテナの動作を制御/制限します。また機械学習によりポリシーを生成することも可能です。
4	Container Firewall (コンテナファイアウォール)	コンテナのネットワーク接続を視覚化、また、コンテナ単位で接続の許可/拒否をルール設定できます。
5	Secrets (シークレット管理)	コンテナに対して、セキュアな方法でパスワードやSSHキーなどのシークレットをデリバリできます。
6	Compliance (コンプライアンス対応)	リスクを一覧化し、対応方法などを含む詳細レポートを生成します。また、イメージやコンテナで発生した各種セキュリティイベントも収集されます。
7	Integration (外部ツール/サービス統合)	Docker Hubなどのレジストリ、JenkinsなどのCI/CDツール、SplunkなどのSIEMサービスなど、さまざまな外部ツールやサービスとの統合/連携が可能です。
8	vShield ←New! (仮想パッチ機能)	Runtime Policyの一環として、既知の脆弱性を持つ実行中コンテナに対しての脆弱性を狙った攻撃を検知/ブロックすることが可能です。

Aqua Vulnerability Shield (vShield) とは

vShield は以下の方法により実行される「仮想的なパッチ」です。



- 既知の脆弱性を狙った攻撃を検知/ブロック
- コンテナイメージの内容を変更することなく、開発者の介入が不要
- ランタイム(コンテナ)に対して補完的に制御

コンテナイメージの脆弱性に対応するのは大変です。

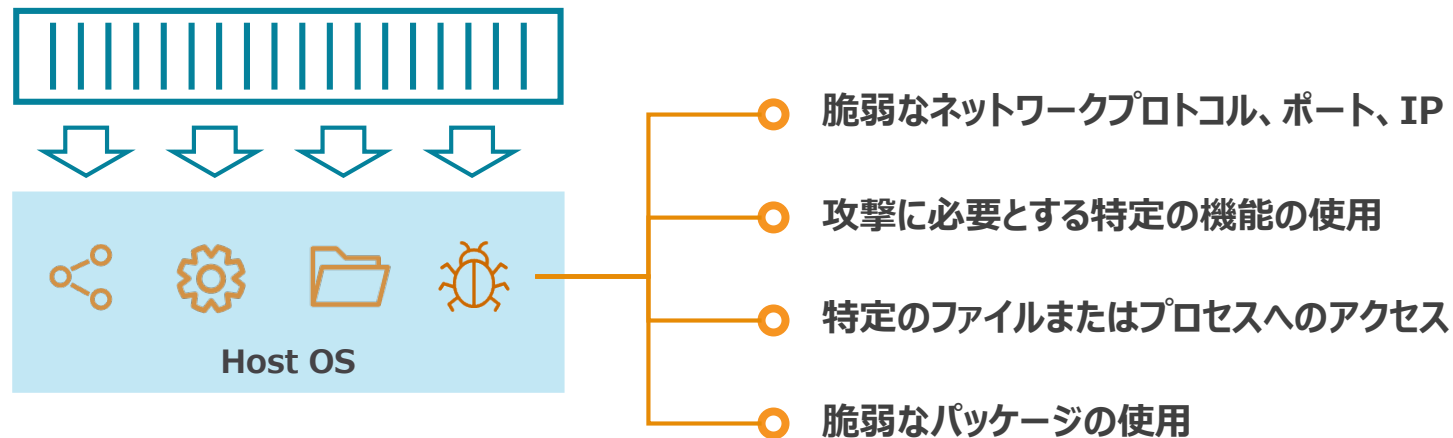
組織の大半が既知の脆弱性が内包されたアプリ(コンテナ)を利用しています。



- イメージのアップデートは時間を要する。
- 運用上の制約や依存関係の理由で対応していないことが大半。
- 脆弱なアプリを落とすのは選択肢にない。

Aqua Vulnerability Shield (vShield) とは

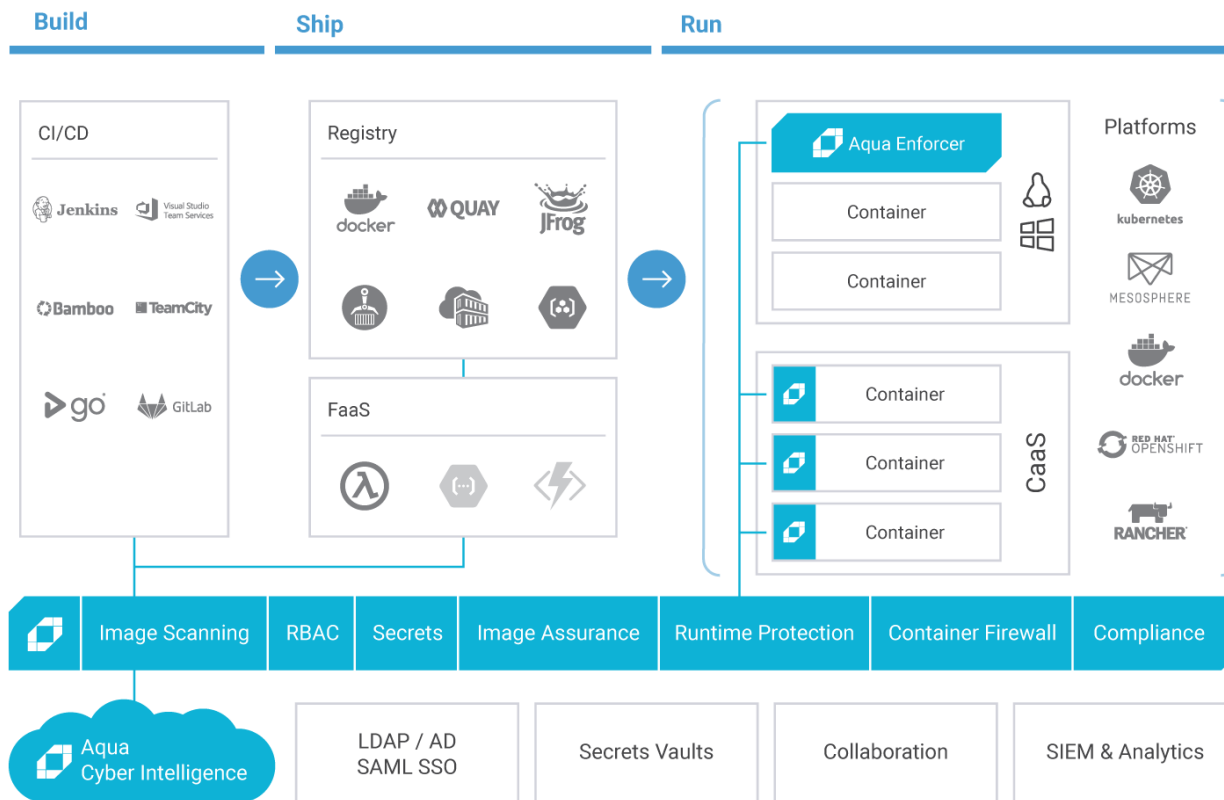
脆弱性が及ぼす根本的な問題に対して、vShield は検知/ブロック



アジェンダ

1. 会社紹介
2. Aqua Security 概要
3. Aqua Security 機能紹介 (デモ)
4. まとめ (Aqua Securityとコンテナのライフサイクル)

Aqua アーキテクチャ



Aqua Life Cycle

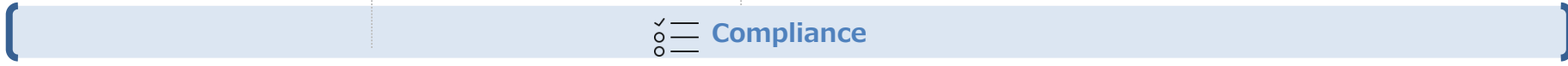
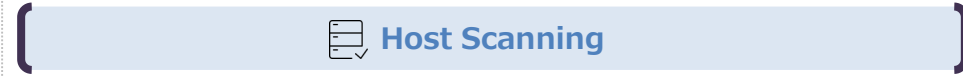
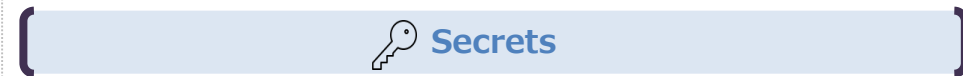
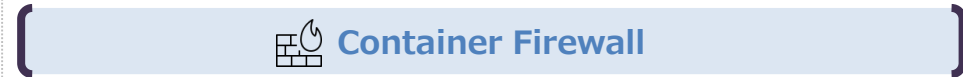
Build



Ship



Run



Aqua Securityに関するお問い合わせおよび本製品デモのご要望は
sales@creationline.com へご連絡ください。

他の製品/サービスについても興味ございましたら弊社サイトをご参照ください。
<https://www.creationline.com>



以上です。
ご清聴ありがとうございました。



CREATIONLINE, INC.