



컨테이너 환경의 데이터와 서비스 관리

Veeam Software Korea

Sales.Korea@veeam.com, 2022.9

컨테이너 환경의 데이터/서비스 관리

Stateful vs. Stateless

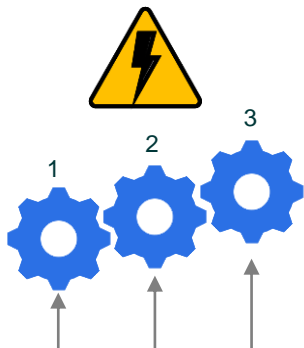
쿠버네티스의 Stateful 어플리케이션 구성은 백업이 필요합니다.



Stateful	Stateless
<ul style="list-style-type: none">▪ 데이터, 거래내역 또는 로그가 저장 또는 참조되어야 하는 어플리케이션▪ Persistent Volume (데이터가 저장되는 공간을 말하는 쿠버네티스 용어) 사용▪ 예를 들면 데이터베이스▪ 상대적으로 쿠버네티스 구현이 더 복잡함	<ul style="list-style-type: none">▪ 데이터 저장이 필요없는 어플리케이션▪ Persistent Volume 사용안함▪ 예를 들면 핸드폰 통신 중계기 또는 접속만 전달해주는 웹서버▪ 상대적으로 쿠버네티스 구현이 더 단순함

Why Backup Kubernetes – Real Life Cases, 1/2

쿠버네티스는 원래 장애가 없는 시스템이나 현실적으로 운영과정에서 다양한 요인으로 전문 백업이 필요한 경우가 발생합니다.



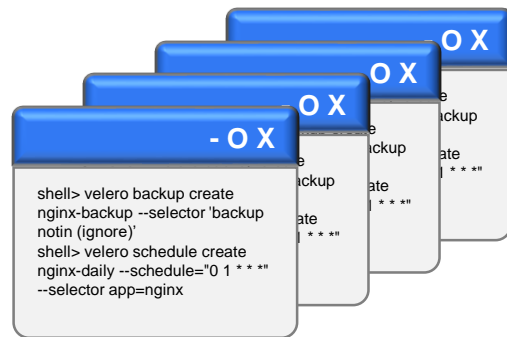
- 국내 모 대기업, 데이터센터에 일시적인 정전 발생
- K8s 가 재시작 되면서 서비스들이 뒤박인 순서로 시작되어 데이터 정합성이 깨지는 사고 발생
- 2주간 서비스 다운. 수작업으로 정합성 작업함
- 고객은 K8s는 백업이 필요할지 몰랐는데 이번 계기를 통해 백업이 필요하다는 것을 인식하여 솔루션 도입 검토



- 국내 모 대기업, 백업 고려없이 라이브 서비스 운영
- 쿠버네티스는 정책상 3개월 주기로 버전 업데이트를 요함
- 업데이트 작업전 라이브시스템임을 감안했을때 데이터의 안정성에 대해서 보장할수 없었음
- 업데이트를 미루고 백업 솔루션을 도입하기로 결정함

Why Backup Kubernetes – Real Life Cases, 2/2

쿠버네티스는 원래 장애가 없는 시스템이나 현실적으로 운영과정에서 다양한 요인으로 전문 백업이 필요한 경우가 발생합니다.



- 국내 모 대기업, 온프레미스에서 K8s 라이브 서비스 운영
- 전사적인 IT 비전의 일환으로 퍼블릭 클라우드로의 마이그레이션 계획하게 됨
- 막상 마이그레이션을 실행에 옮기려니 모든 작업을 수작업으로 해야했고 위험요소가 높다는 것을 실감함
- 자동화된 K8s 전문 마이그레이션 솔루션인 빔 카스텐을 검토중에 있음

- 오픈소스 벨레로는 100% CLI (커맨드라인) 방식
- 국내 모 대기업에서 벨레로를 이용해 백업을 구현하려 했으나 K8s에 대한 깊은 전문성이 필요함을 인지
- 대형 플랫폼인 관계로 CLI 작업량과 구성변경, 자동화 스크립트 등 작업의 범위가 매우 방대하여 현실적으로 구현과 유지보수가 불가능할것으로 판단내림
- 100% GUI 그리고 CLI 까지 가능한 전문 솔루션인 빔 카스텐 검토중에 있음

Why Backup Kubernetes



1. 클러스터 데이터/서비스 정합성
2. DB/어플리케이션 정합성
3. 장애 시 복구 **SLA** 준수
4. 랜섬웨어 대응
5. 재해대응 DR 환경 구축
6. 클러스터 업그레이드 / 마이그레이션

Kasten K10

kubernetes 백업과 이동을 쉽게 제공

K10 PLATFORM



어플리케이션
검색



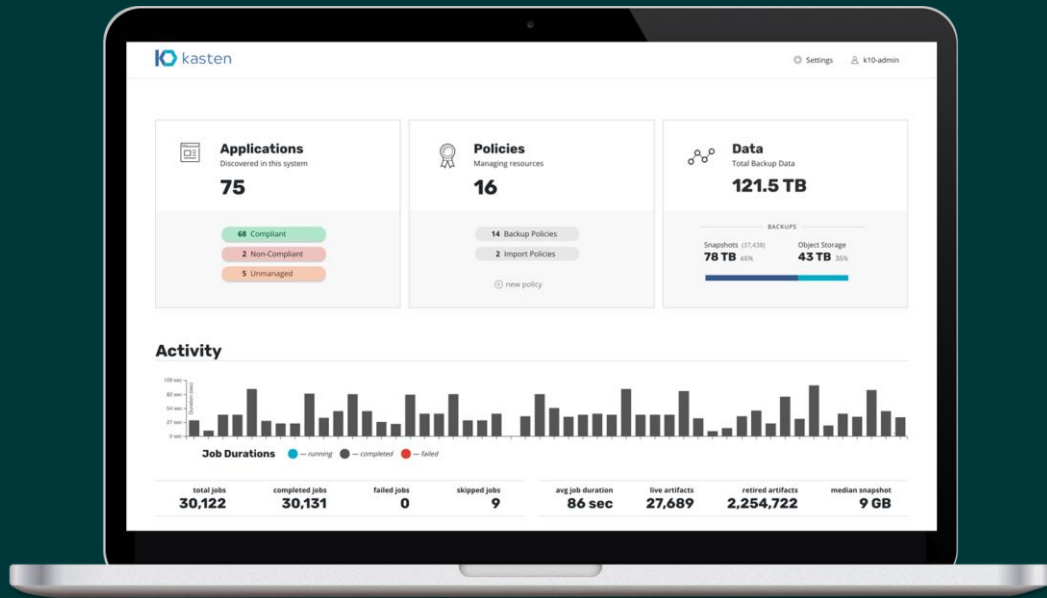
정책 중심
자동화



손쉬운 사용,
간편한 UX

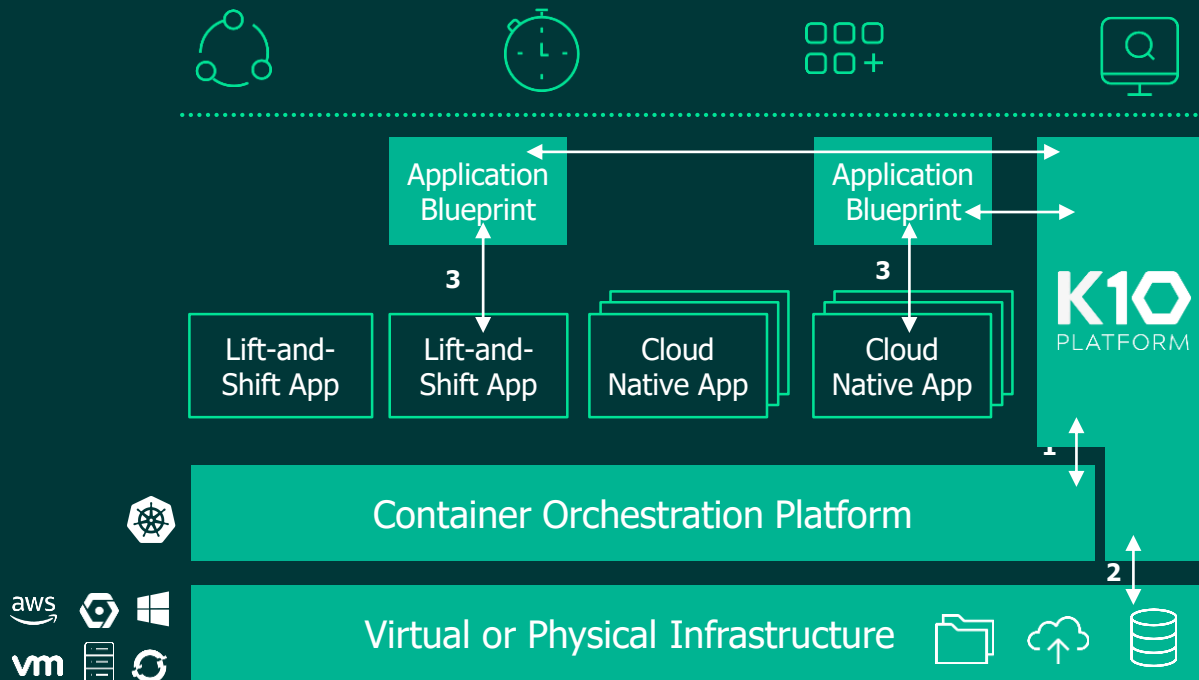


보안
강화



Veeam 컨테이너 백업 아키텍처

Veeam Kasten 작동방식에 대한 개념도



1 Orchestrator APIs

Kubernetes API를 사용하여 애플리케이션 및 기본 구성 요소를 검색하고 수명주기 작업을 수행.

2 Infrastructure APIs

스토리지 계층에 대한 제약이 없음.
- 특정 제품에 대한 Lock-in이 없음
스냅샷 기반의 데이터 관리.
- CSI 기반의 스토리지 스냅샷 수행
다양한 스토리지를 백업 저장소로 확장.
- Object Storage, S3 compatible store, NFS storage

3 Application Framework

별도의 스크립트 작업이 없는
어플리케이션 백업 수행
Optional 어플리케이션 Blueprint 기능을
통해 논리 데이터 캡처 제공

어플리케이션/데이터의 일관성

다양한 방식의 어플리케이션/데이터 정합성 보장



Crash
consistent

Storage snapshots



“App”
consistent

Freeze data service
Storage snapshot
Unfreeze data service



DB
consistent

Logical dumps via dat
a service-specific tool
(e.g., pg_dump)

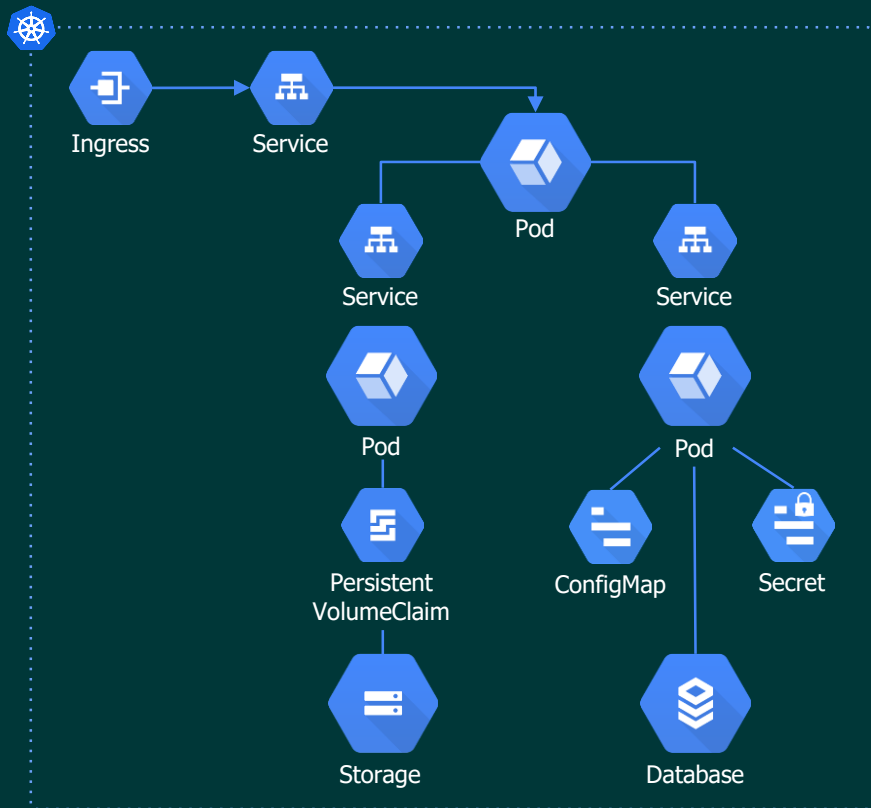


System
consistent

Full app capture
Combination of tools across d
ata and storage layers

어플리케이션 중심 데이터 보호

쿠버네티스 환경의 통합된 어플리케이션 보호

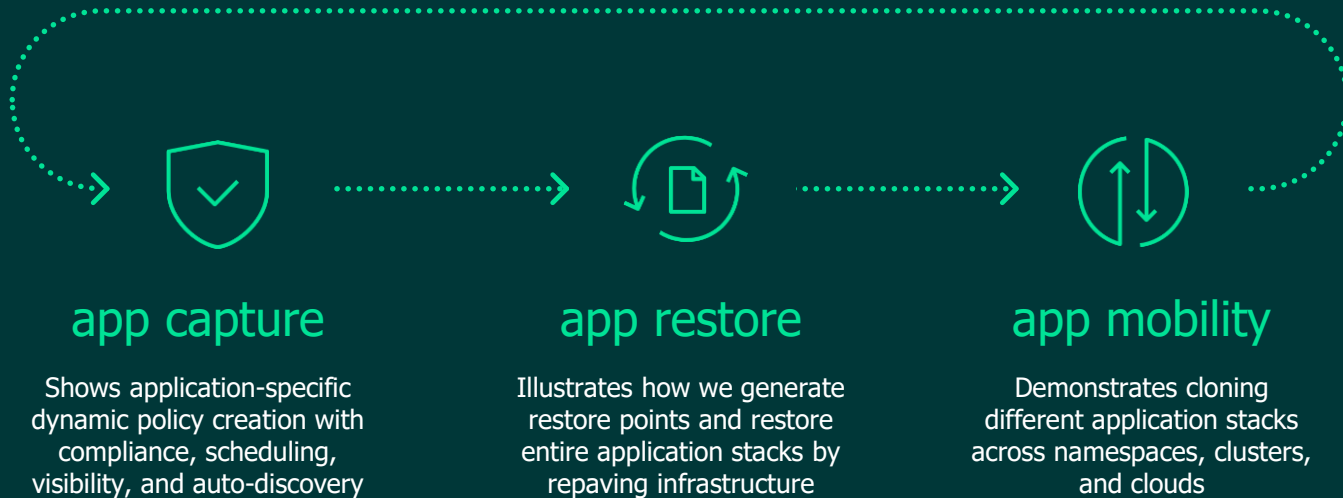


운영단위로의 어플리케이션 보호

- 자동화된 데이터 및 어플리케이션 자원 인식
- 클러스터 및 클라우드 간의 스토리지와 데이터에 대한 보호
- 효율적인 리소스 사용과 안전한 데이터 처리

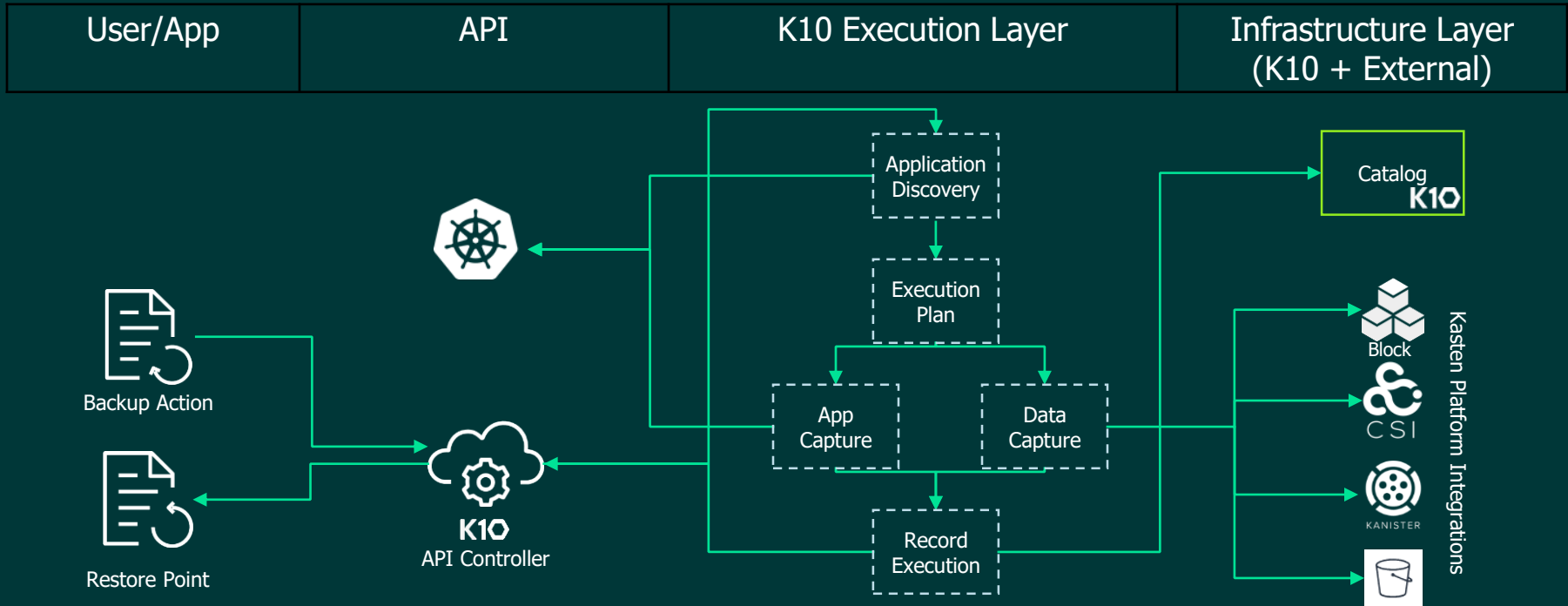
K8s 환경의 데이터 관리

walkthroughs



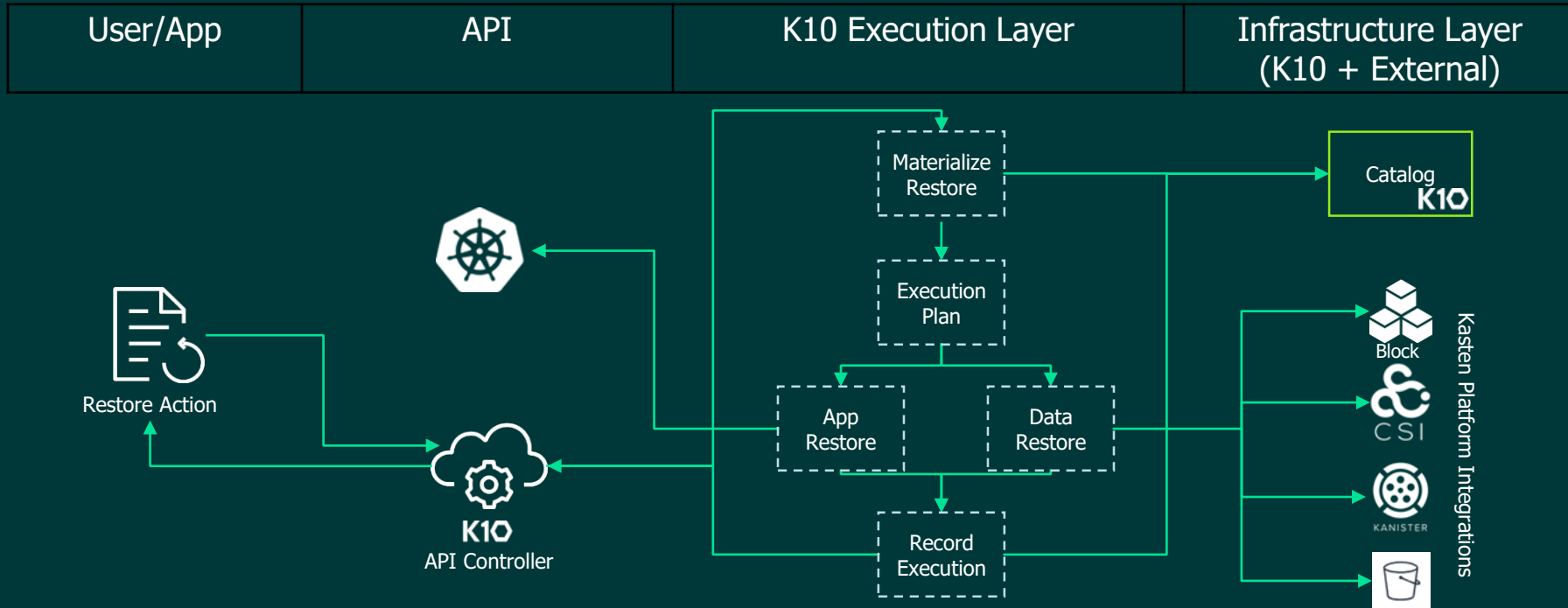
K8s 환경의 데이터 관리

application capture



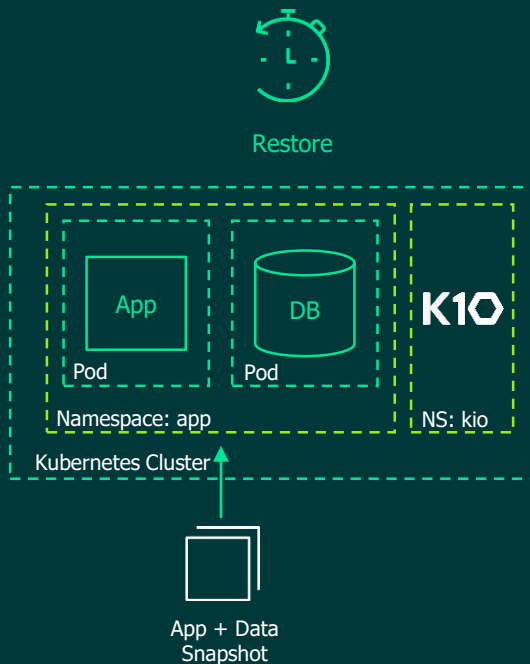
K8s 환경의 데이터 관리

application restore



Seamless application transformation

application portability requirements



Across:

Storage Systems

Kubernetes Versions

Seamless application transformation

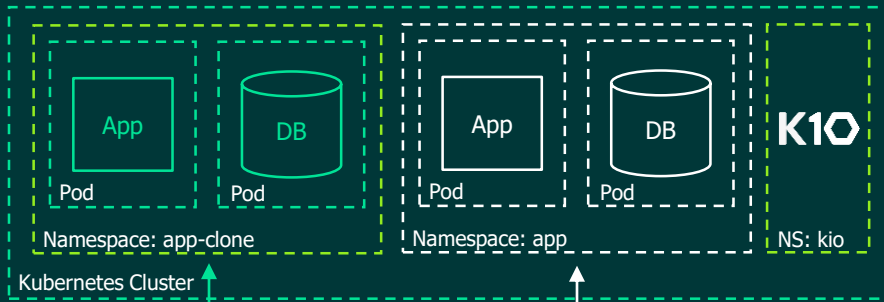
application portability requirements



Restore



Clone



Across:

Storage Systems

Namespaces

Kubernetes Versions

Availability Zones

Seamless application transformation

application portability requirements



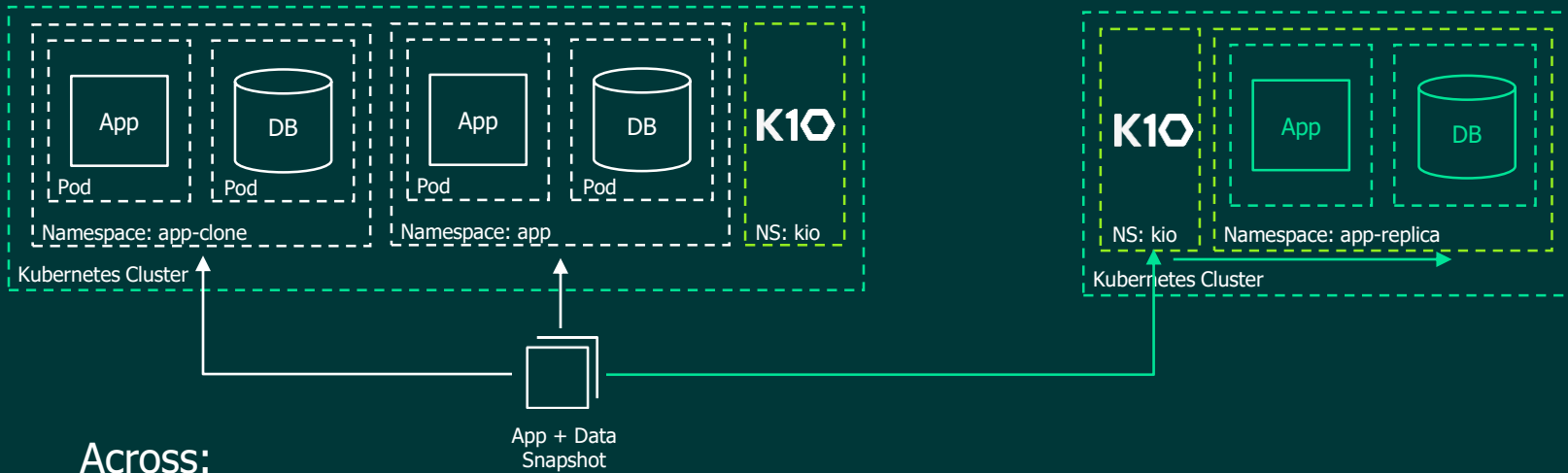
Restore



Clone



Migrate



Storage Systems

Namespaces

Clusters and Regions

Kubernetes Distributions

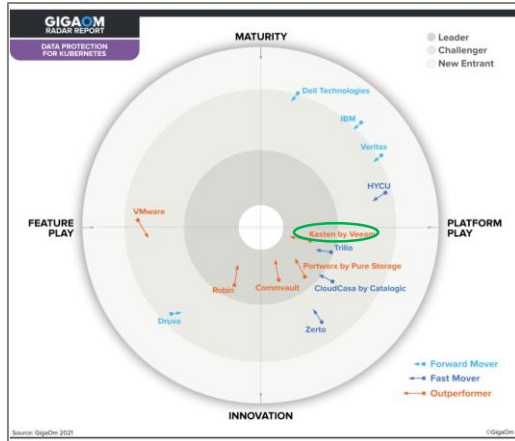
Kubernetes Versions

Availability Zones

Cloud Providers

Prod to Dev Clone

Kasten K10 by Veeam #1 백업/마이그레이션 솔루션

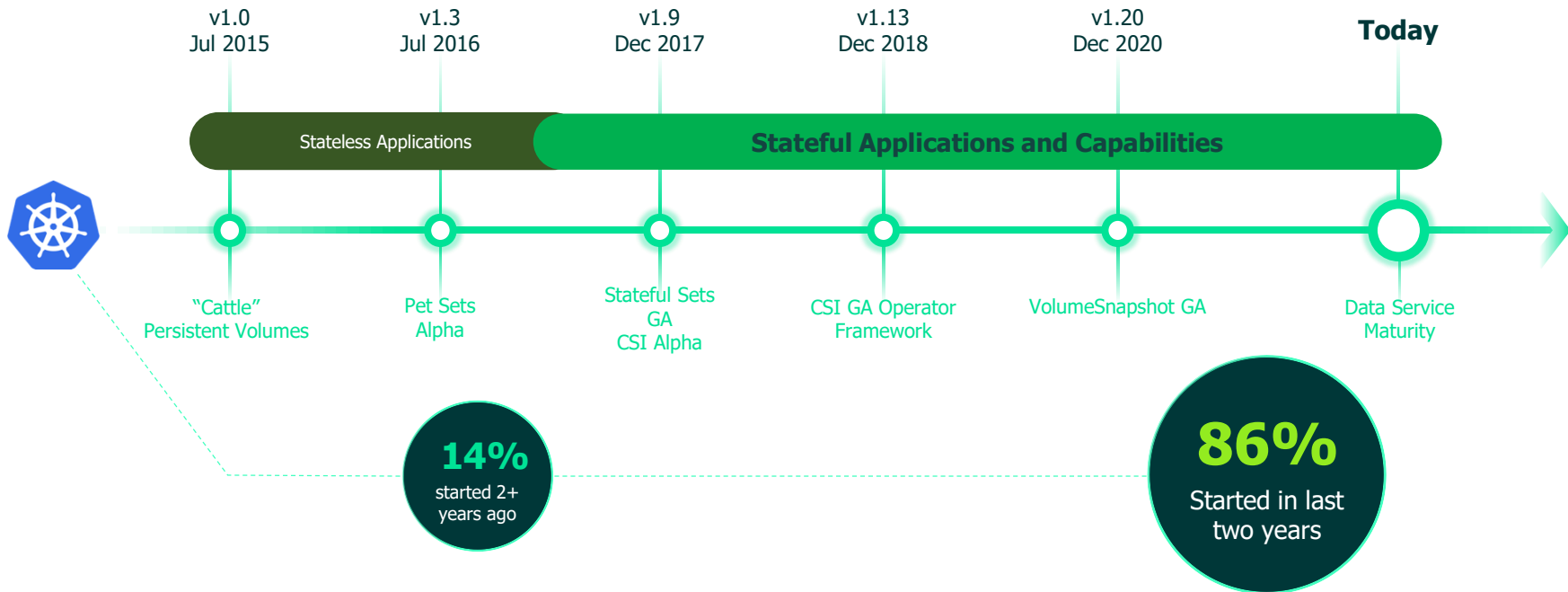


#1 Kubernetes Backup

Free Kubernetes Platform



쿠버네티스의 진화 Stateful 어플리케이션의 성장



[2021 Data on Kubernetes Report \(N=502\)](#)

백업 및 복원

- 중단된 상태의 애플리케이션으로 복원
- 잘못 구성된 애플리케이션 복구
- 데이터베이스를 보호하기 위해 강력한 백업 제공
- 감사 규정 준수를 위한 환경 상태 재현



멀티-테넌시



RBAC



다중 언어



확장과 성능

재해 복구

- 세분화된 복원 기능을 통해 모든 애플리케이션 구성 요소 복원
- 정책 중심의 자동화를 사용하여 백업이 오프사이트 스토리지에 안전하게 복제되는 방법 관리
- Kubernetes 워크로드에 대해 0에 가까운 RTO 사용



**Cross A Z and
Region**



**Multi and Hybrid
Cloud**



**Storage
Transforms**

어플리케이션의 이동성

- 클라우드 간 이식성 및 K8s 클라우드 간 어플리케이션 마이그레이션 실현
- 일부 어플리케이션 및 환경은 온-프레미스로 유지하면서 다른 어플리케이션 및 환경은 클라우드 공급자에서 실행
- 퍼블릭 및 프라이빗 K8s 배포 간에 효율적으로 마이그레이션
- 어플리케이션을 업그레이드된 클러스터로 예측 가능하게 마이그레이션하여, K8s 업그레이드에 대한 계획 및 이해 제공



클러스터
업그레이드

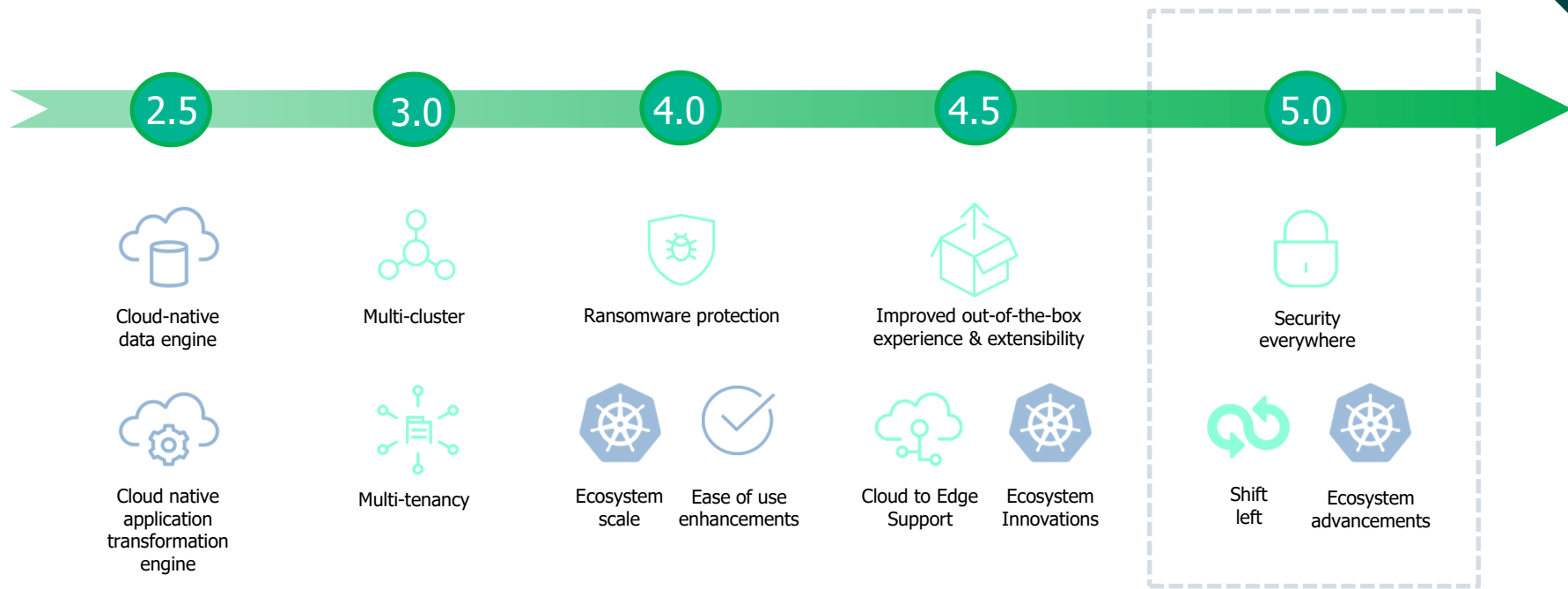


어플리케이션
전환



테스트/개발
클러스터

DevOps 가속화 Veeam Kasten의 진화



보안성 강화

• 개발에서 배포까지



플랫폼 강화 & 사용 편의성



- AWS KMS 및 Vault와의 통합
- 대시보드 UI와 쿠버네티스 네이티브 RBAC 통합



데이터 보호정책 가드레일

- 잘못된 구성을 식별(및 수정)하여 취약점 연결
- 시행 가능한 정책 표준(예: RPO, 보존, 불변성)



랜섬웨어 공격 탐지

- 잠재적 또는 임박한 공격의 조기 탐지
- S3 Object-Lock을 지원하는 AWS S3 또는 S3 호환 스토리지



불변성을 제공하는 Veeam 리눅스 저장소

- 성능 계층에서 클라우드 계층까지 포괄적인 종단 간 랜섬웨어 보호
- VBR 데이터 경로 통합의 다음 단계

Kubernetes-Native RBAC with Kasten K10

Add Role

Role Name
The display name for this RBAC Role.
app-owner

Role Level
Select whether this role applies to an entire Cluster, or only to specific Applications.
 Entire Cluster Specific Applications

Access Privileges
Select which Read, Write and Delete operations are available to this Role on different Resources.

API GROUPS/RESOURCES	READ	WRITE	DELETE
All	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Actions	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Backup	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Backup Cluster	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Cancel	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Export	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Import	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Report	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Restore	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Restore Cluster	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Retire	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Run	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Apps	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Applications	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Cluster Restore Points	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Restore Points	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Restore Point Contents	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Config	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Policies	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Save Role **Cancel**

app-owner

```
1 kind: ClusterRole
2 apiVersion: rbac.authorization.k8s.io/v1
3 metadata:
4   name: app-owner
5   uid: 1840c0a3-183d-4317-9a0f-1ae3f9f12a4c
6   resourceVersion: "17351983"
7   creationTimestamp: 2022-04-01T17:49:41Z
8   managedFields:
9     - manager: Go-http-client
10     operation: Update
11     apiVersion: rbac.authorization.k8s.io/v1
12     time: 2022-04-01T17:49:41Z
13     fieldsType: FieldsV1
14     fieldsV1:
15       f:rules: {}
16 rules:
17   - verbs:
18     - get
19     - list
20     - watch
21     - create
22     - update
23     - patch
24   apiGroups:
25     - actions.kio.kasten.io
26   resources:
27     - backupactions
28     - backupactions/details
29   - verbs:
30     - get
31     - list
32     - watch
33     - create
```

User Roles
Roles are a set of access | can apply across an entire | or user groups.

Roles (18)

K10 specific RBAC roles for

The list below is based on your

CLUSTER ROLE
app-owner

ACTIONS **APPS**
R W D R W

REPORTING **VAULT**
R W D R W

Add Assignment

Assignment Name
Only lowercase letters, numbers, dash, and dot.
app-53-owners-permissions

Assignment Level
Select whether this assignment applies to an entire Cluster, or only to specific Applications.
 Entire Cluster Specific Applications

Applications
Choose the application namespaces to which this role should be applied.
app-53

K10 Roles
Select the RBAC Role you would like to assign.
app-owner

Subjects
Add Users and Groups to which this Role should be assigned.

KIND	NAME
Group	app-53-dev@kasten.io

User **Group**
Name

Add Subject

Save Assignment **Cancel**

1 역할 정의

2 옵션 확인 또는 수정

3 역할 할당

데이터보호정책 가드레일 - Kyverno

```
! prod-backup-enforce-policy.yaml
1  apiVersion: kyverno.io/v1
2  kind: ClusterPolicy
3  metadata:
4    name: prod-backup-enforce-policy
5  spec:
6    validationFailureAction: enforce
7    rules:
8    - name: cd-prod-backup-policy
9      match:
10     resources:
11       kinds:
12         - Deployment
13         - StatefulSet
14     validate:
15       message: "Production Deployments
16       pattern:
17         metadata:
18           labels:
19             =(purpose): production
20             dataprotection: k10-?*
21             immutable: enabled
```

프로덕션일 경우 K10 백업정책을 적용하고 변경불가 저장소에 저장

```
11  apiVersion: apps/v1
12  kind: Deployment
13  metadata:
14    name: nginx-deployment
15    namespace: nginx
16    labels:
17      app: nginx
18      purpose: production
19      dataprotection: k10-goldpolicy
20      immutable: enabled
21  spec:
22    replicas: 3
23    selector:
24      matchLabels:
25        app: nginx
26    template:
27      metadata:
28        labels:
29          app: nginx
30      spec:
31        containers:
32          - name: nginx
33            image: nginx:1.14.2
34            ports:
35              - containerPort: 80
```

어플리케이션을 정의된 데이터 보호 정책으로 보호

> namespace/nginx created

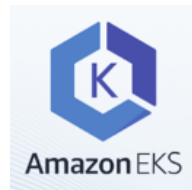
> Error from server: error when creating "nginx-deployment.yaml": admission webhook

> "validate.kyverno.svc-fail" denied the request

데이터 보호 정책이 적용되지 않은 상태로 배포되는 상황을 방지

Shift Left

- Shift Left를 데이터 보호정책에 적용



Amazon EKS Blueprints

- EKS 클러스터에서 완벽한 데이터 보호를 위해 EKS Blueprint를 통합기능을 추가



향상된 Red Hat OpenShift 환경지원

- 전체 수명 주기 기능(백업, 장애 복구/DR)으로 레벨 III 인증



데이터 서비스 Blueprint

- Microsoft SQL Server를 위한 새로운 기본 제공Blueprint
- PostgreSQL Operator(PGO)를 위한 새로이 내장된 Blueprint

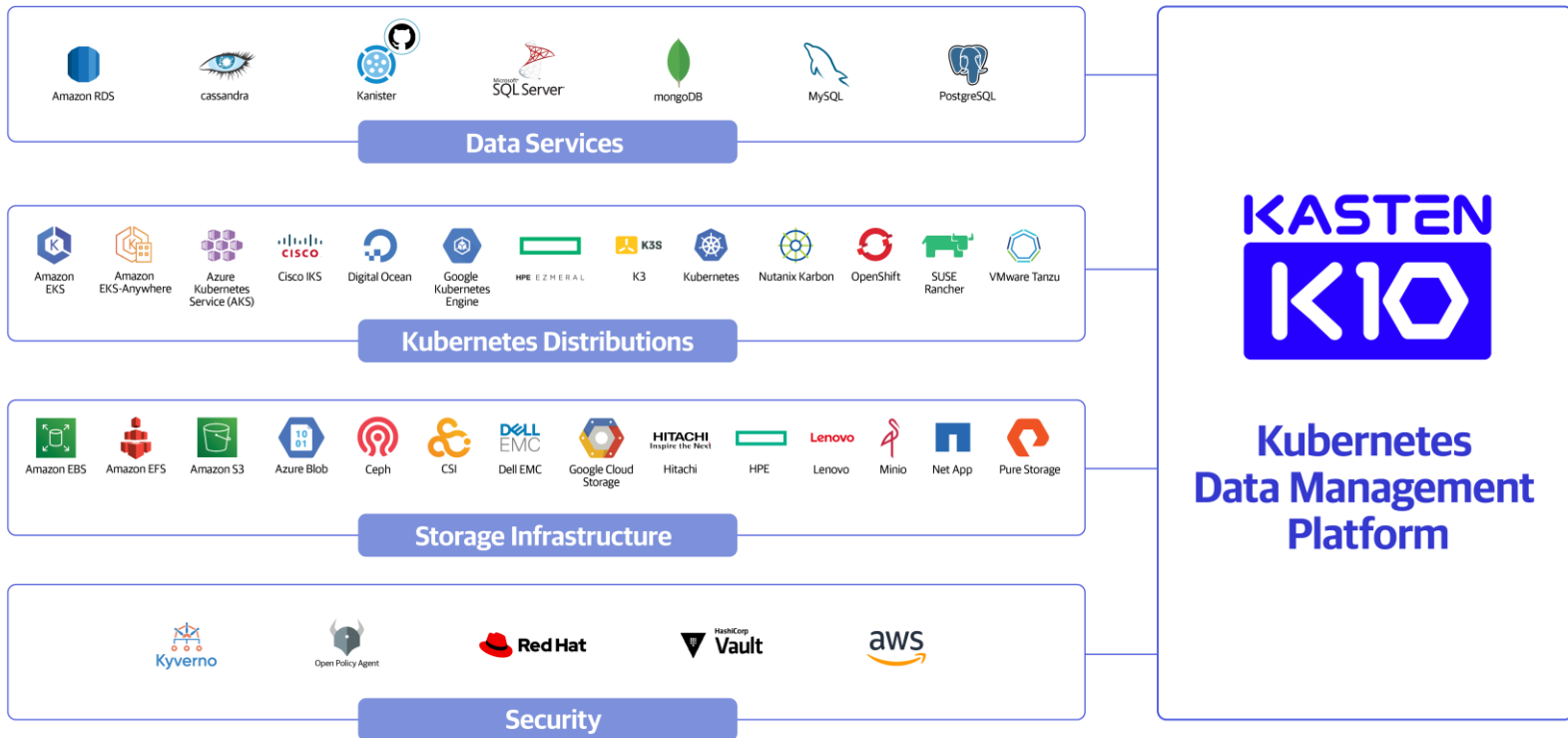


단순화된 GUI 기반의 운영환경

- Blueprint 구현을 위한 직관적이고 간소화된 워크플로를 위한 Blueprint Editor
- 중요한 측정항목에 대한 보고서 생성기능

에코시스템 통합

• Kasten K10 에코시스템



감사합니다.

veeam