Next-Gen Protection Platform for Next-Gen Applications

DEEPAK VERMA

Director, Product Strategy, Zerto

deepak.verma@zerto.com

Webinar Abstract

As many enterprises start to bring applications designed for containerized platforms into production, they are faced with the challenge of meeting traditional resilience requirements for these new apps. Regardless of the platform choices, many organizations still require production applications and their data to meet specific service levels for data protection and recovery, disaster recovery, and long-term retention. While these requirements stem from external industry regulations, often the business imposes more stringent requirements upon itself. This is indeed the same driving force behind the rapid adoption of containers, Kubernetes and DevOps by businesses.

Zerto has been a leader in the VM protection space for over 10 years and when we ventured into building our next generation protection platform for next-gen app that utilize containers and Kubernetes, we quickly learned several new lessons. Zerto also engaged Enterprise Strategy Group to conduct a survey across enterprises to gather industry direction and validate requirements.

In this session, we will share some of the key survey results and the design considerations that have shaped the architecture pattern for a next-gen protection platform. We will bust the myth that next-gen applications relying on Kubernetes and container platforms do not need protection, and in turn illustrate what next-gen apps require.

About the Speaker

- 20 years experience in data protection and disaster recovery
- Certified on GCP, AWS, and Azure
- Climbed 132,674 ft during quarantine

About Zerto

Zerto

Survey Objectives with Enterprise Strategy Group (ESG)

- Market Adoption
- Understand challenges
- Buyer Persona
- Gauge feature preferences

ESG Survey Details

Quantitative Web-Based Survey

- 334 Respondents
- North America (US & Canada)
- Survey Dates: 6/12/2020 – 6/24/2020

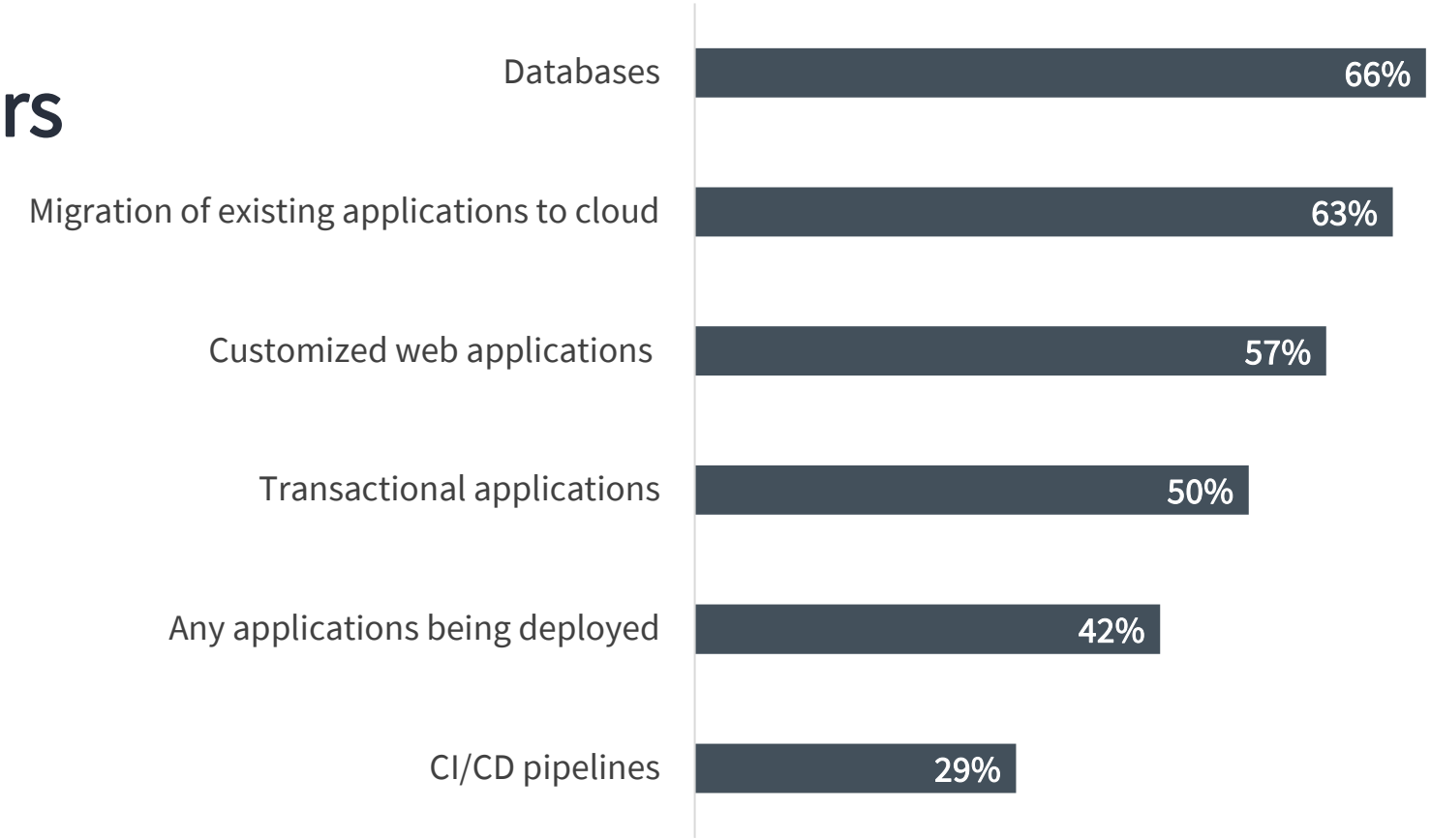
Survey Respondents

- IT operations professionals responsible for application environment and strategy
- Multiple Sizes
  - 32% midmarket
  - 68% enterprise
- All industry verticals

Source: ESG Research Publication, *Container Data Protection*, June 2020

Survey:
Workloads in containers

Question text:
What business applications/workloads are supported by your organization's container runtime environment? (Percent of respondents, N=334, multiple responses accepted)



Zerto

Source: ESG Research Publication, *Container Data Protection*, June 2020

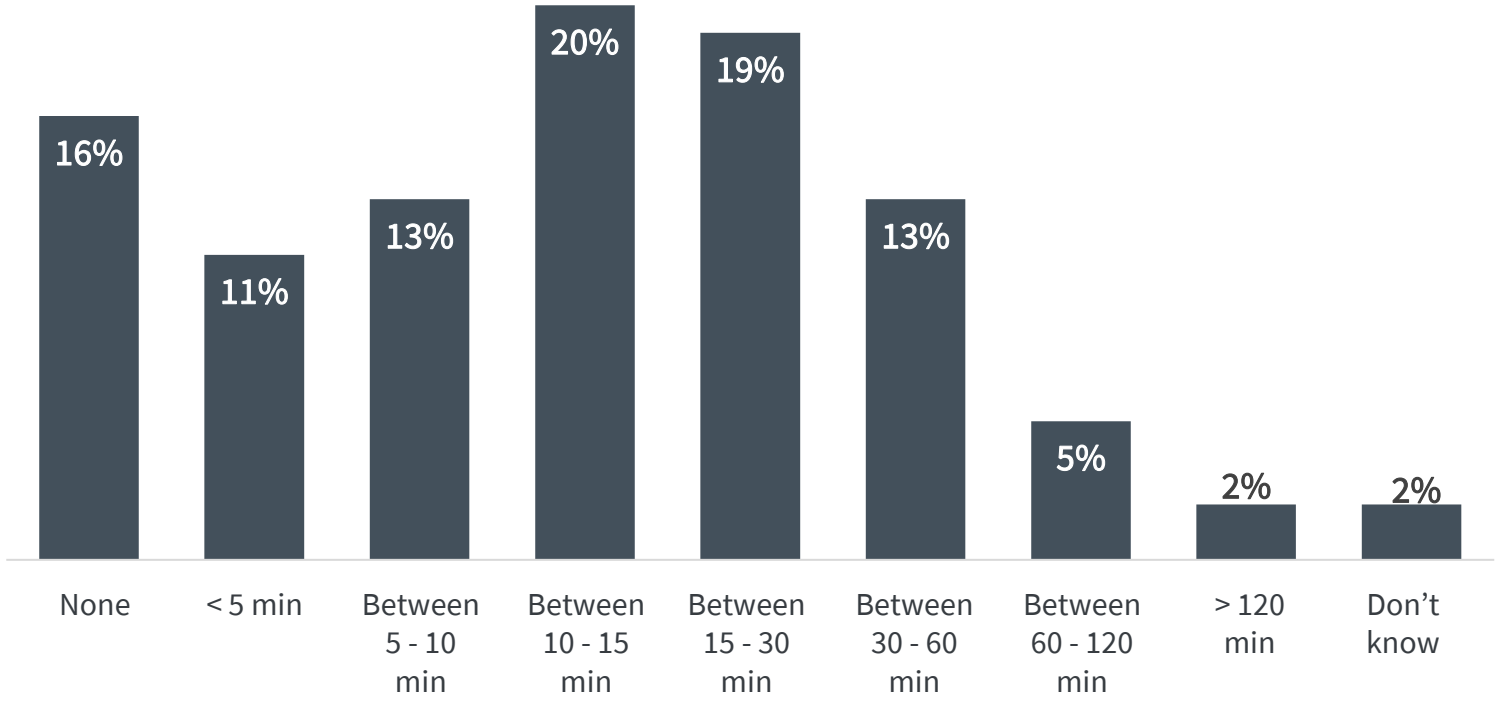
Key Design Element: **Stateful with Stateless**

- Evolving persistence inside containers
- Avoid lock-in with VMs, PaaS, and SaaS
- Orchestrate both stateful and stateless components

Survey:
RPO Tolerance

Question text:
Considering "lost data" (or RPO) as data that must be re-created, how much data associated with container-based applications can be lost without significant impact to the business? (Percent of respondents, N=334)

Estimated mean = 22 minutes



X = Data Loss

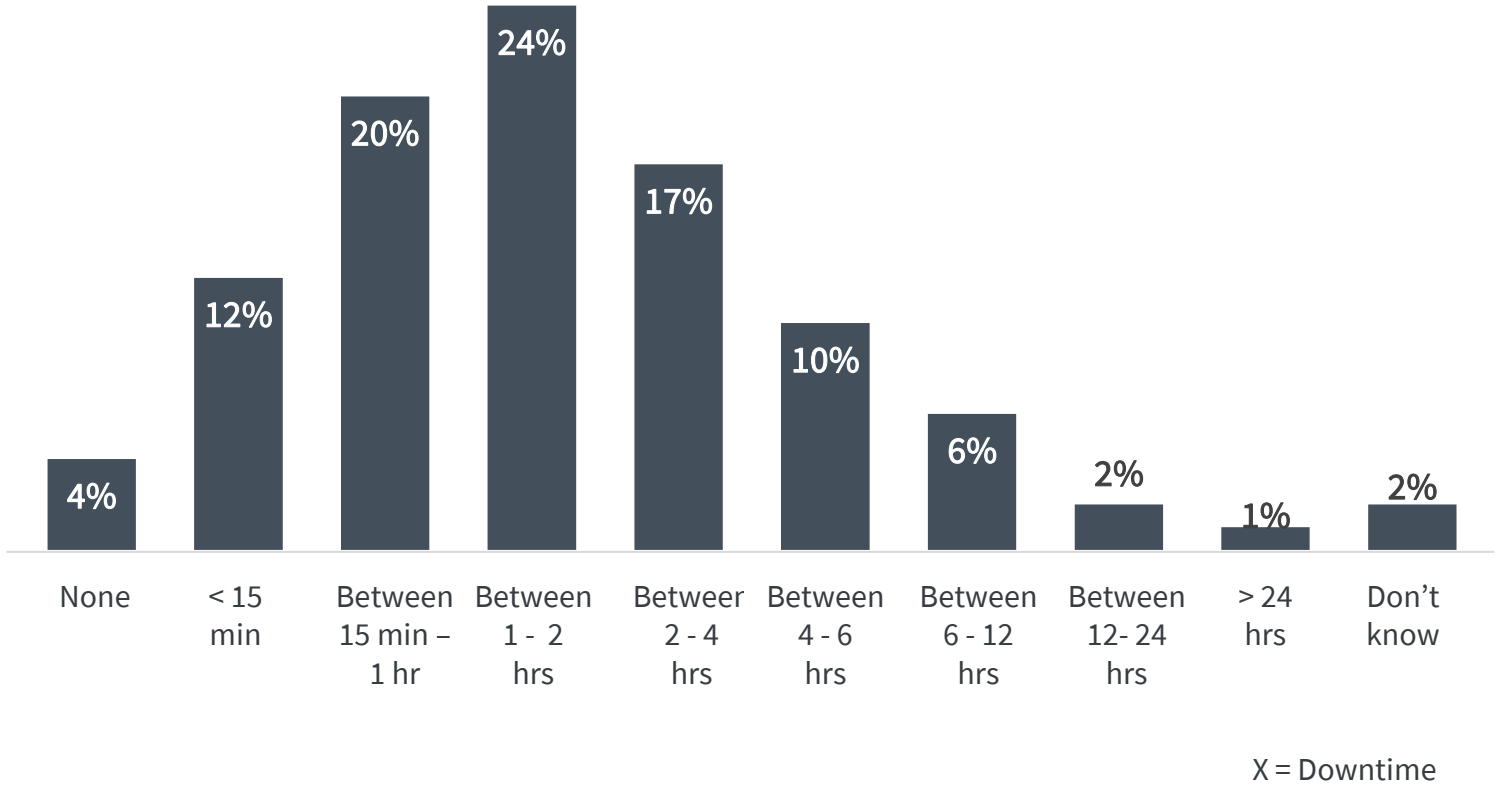
Zerto

Source: ESG Research Publication, *Container Data Protection*, June 2020

Survey:
RTO Tolerance

Question text:
What is the amount of downtime your organization can tolerate from servers running container-based applications/workloads before making the decision to "failover/recover" to a BC/DR secondary site or service provider? (Percent of respondents, N=334)

Estimated mean = 2.87 hours



Zerto

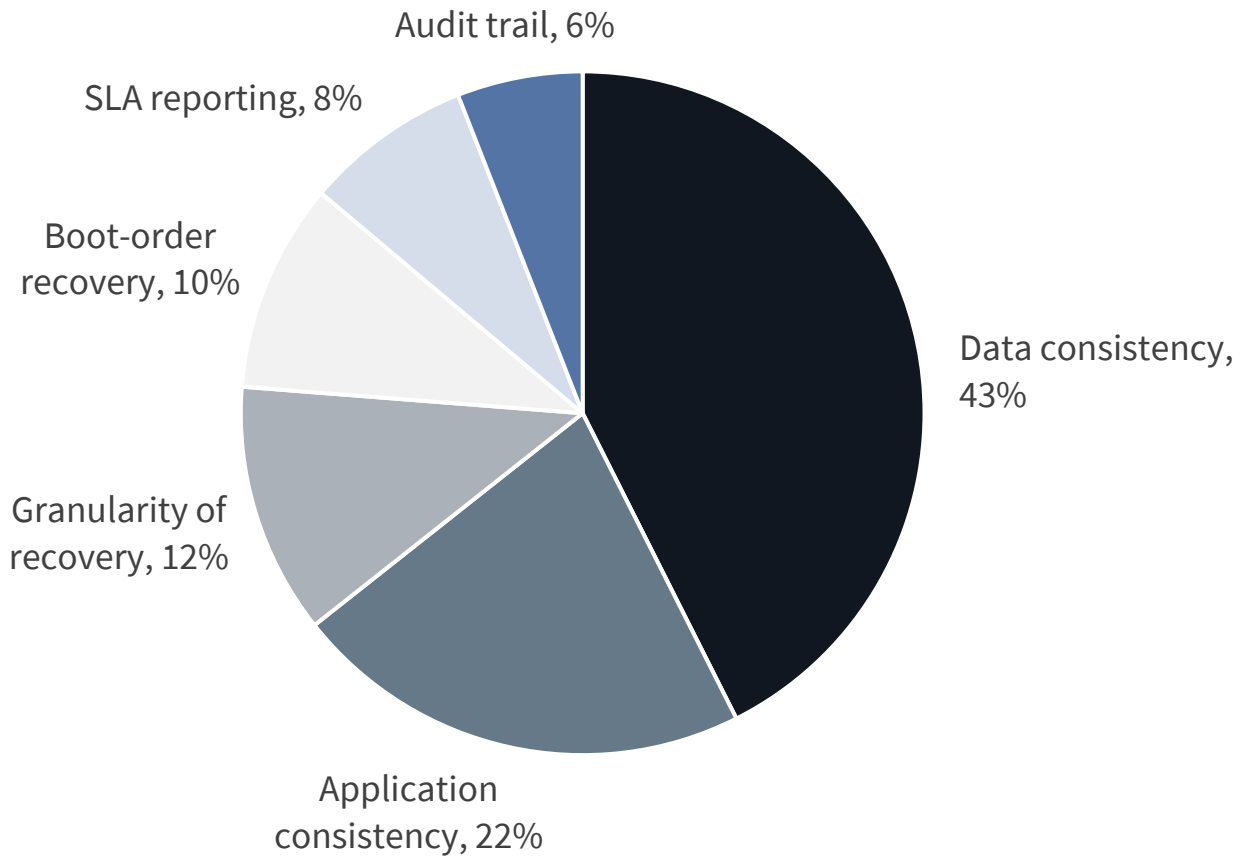
Source: ESG Research Publication, *Container Data Protection*, June 2020

Key Design Element: **Continuous Protection**

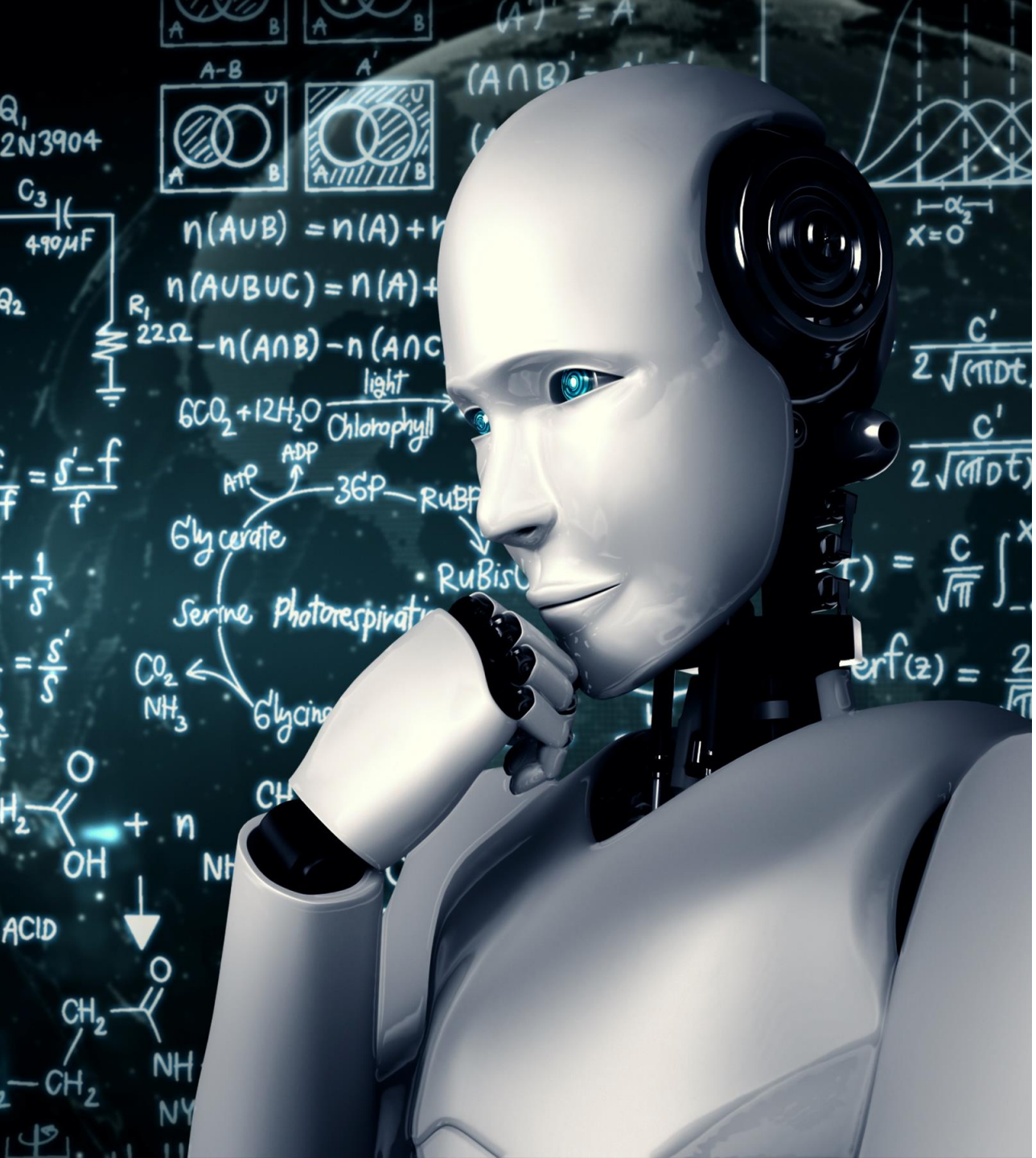
- Continuous Replication for PVs
- Low RPO Checkpoints & Tagging
- Ordered Recovery of Applications

Survey: **Multi-Container App Recovery**

Question text:
When it comes to the recovery of multi-container business applications, what capability is most critical to your organization? (Percent of respondents, N=334)



Source: ESG Research Publication, *Container Data Protection*, June 2020

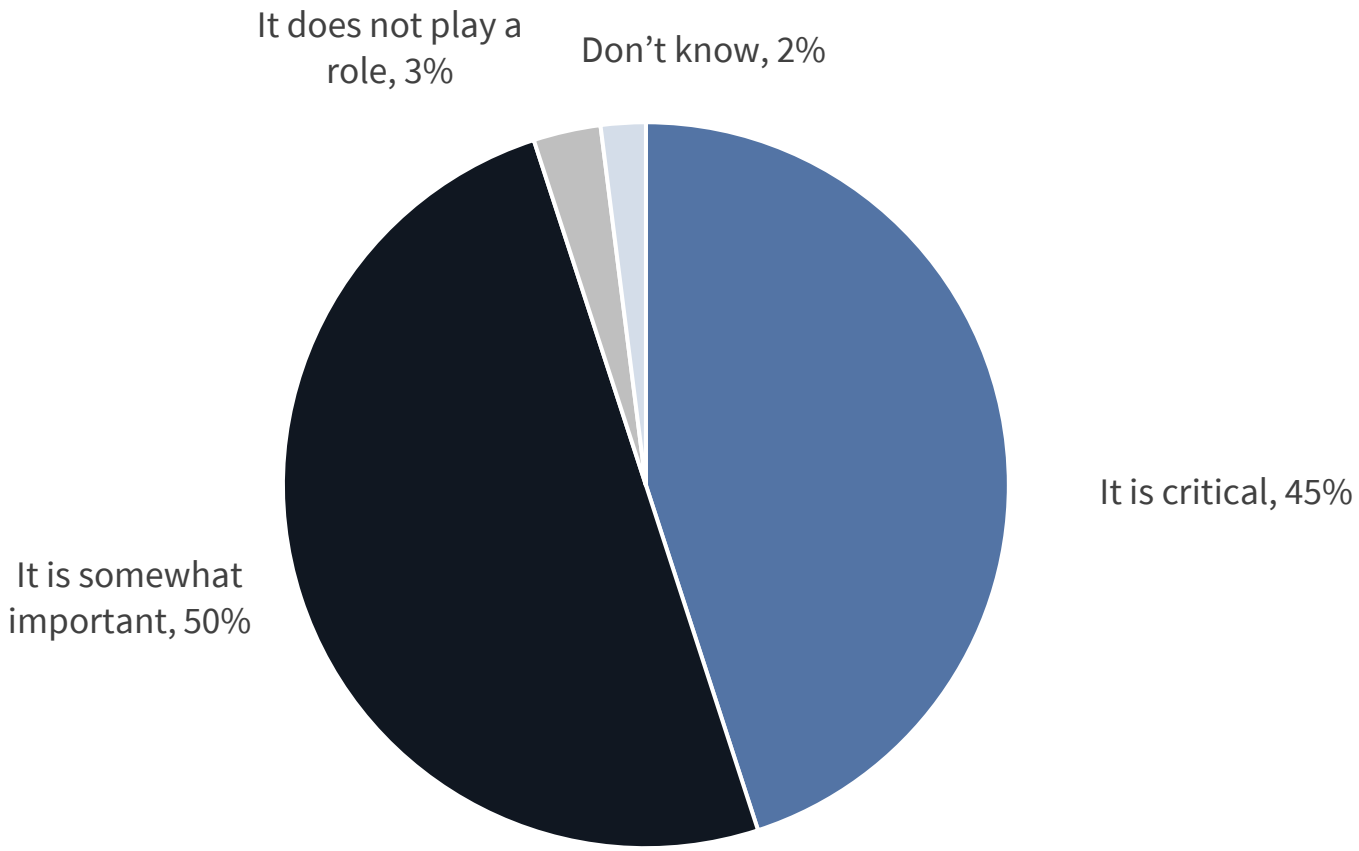


Key Design Element: **Environment Awareness**

- Storage-agnostic Volume Consistency
- Entire K8s App
- Virtual Protection Groups

Survey: Orchestration of Backup and Recovery

Question text:
What is the role of orchestration in container backup and recovery? (Percent of respondents, N=334)



Source: ESG Research Publication, *Container Data Protection*, June 2020

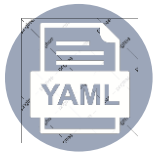
Terminal

```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: debian-dep
  labels:
    app: my-debian
  annotations:
    vpg: test_group
spec:
  replicas: 1
  selector:
    matchLabels:
      app: my-debian
  template:
    metadata:
      labels:
        app: my-debian
    spec:
      containers:
        - name: debian
          image: debian:stable
          command: ["/usr/bin/tail","-f","/dev/null"]
          volumeMounts:
          - mountPath: "/var/pvpath"
            name: external
      volumes:
        - name: external
          persistentVolumeClaim:
            claimName: my-vol-claim
```

Key Design Element: **APIs and Automation**

Data Protection as Code

K8s API Extension for data protection

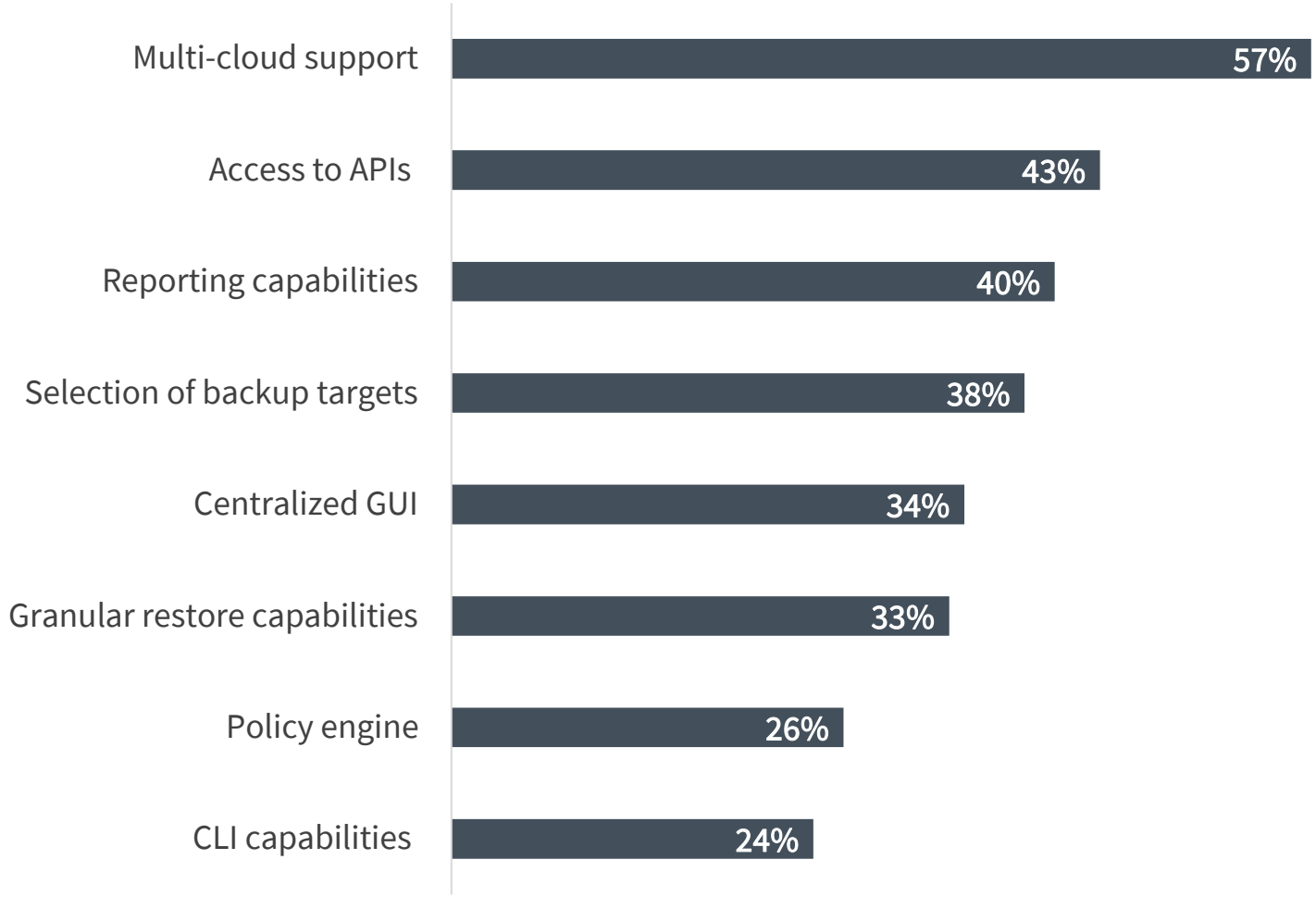


Declarative Configuration

Zerto

Survey: **Features Importance**

Question text:
What features are most important when it comes to backing up your organization's container environments? (Percent of respondents, N=334, multiple responses accepted)

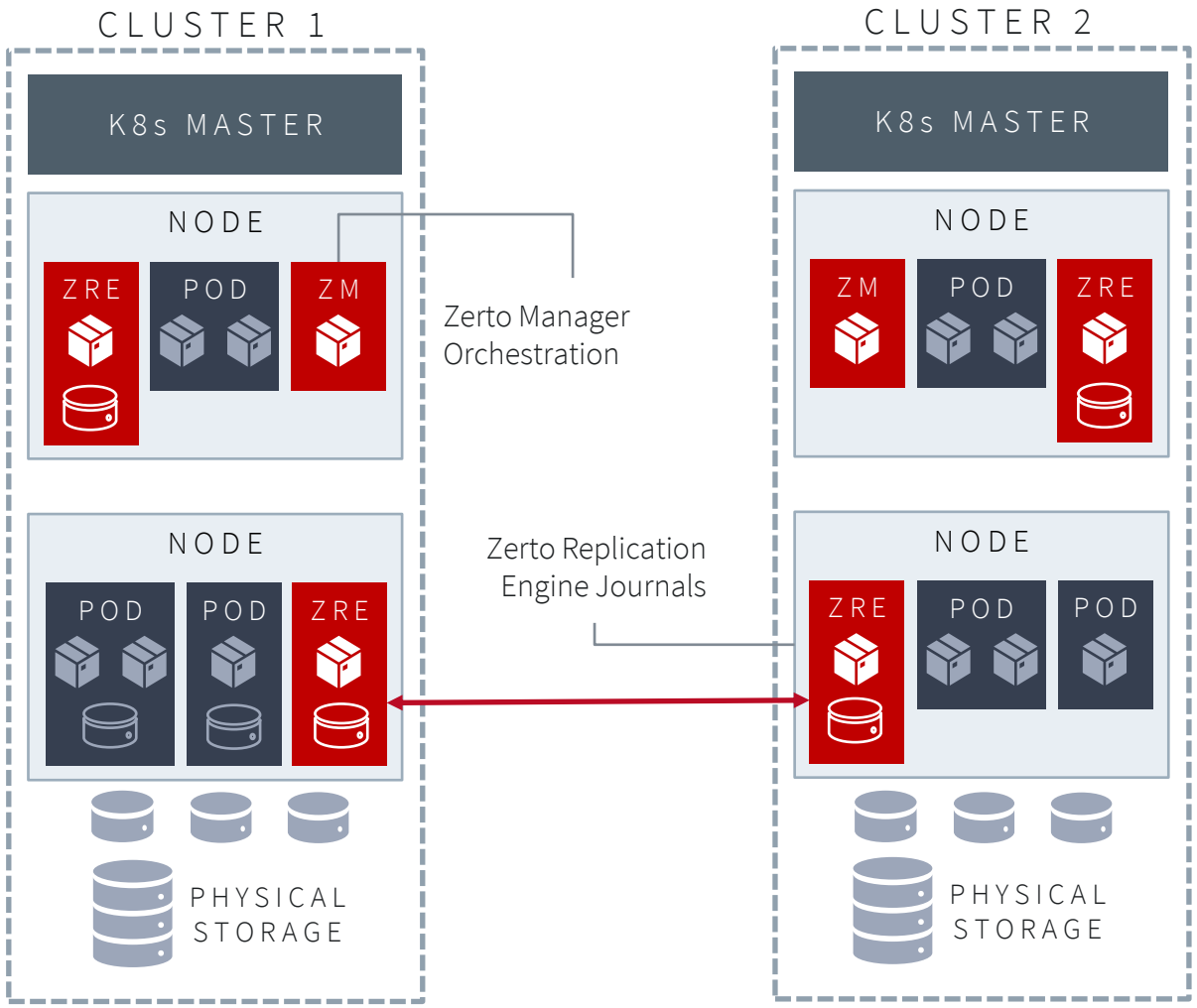


Source: ESG Research Publication, *Container Data Protection*, June 2020

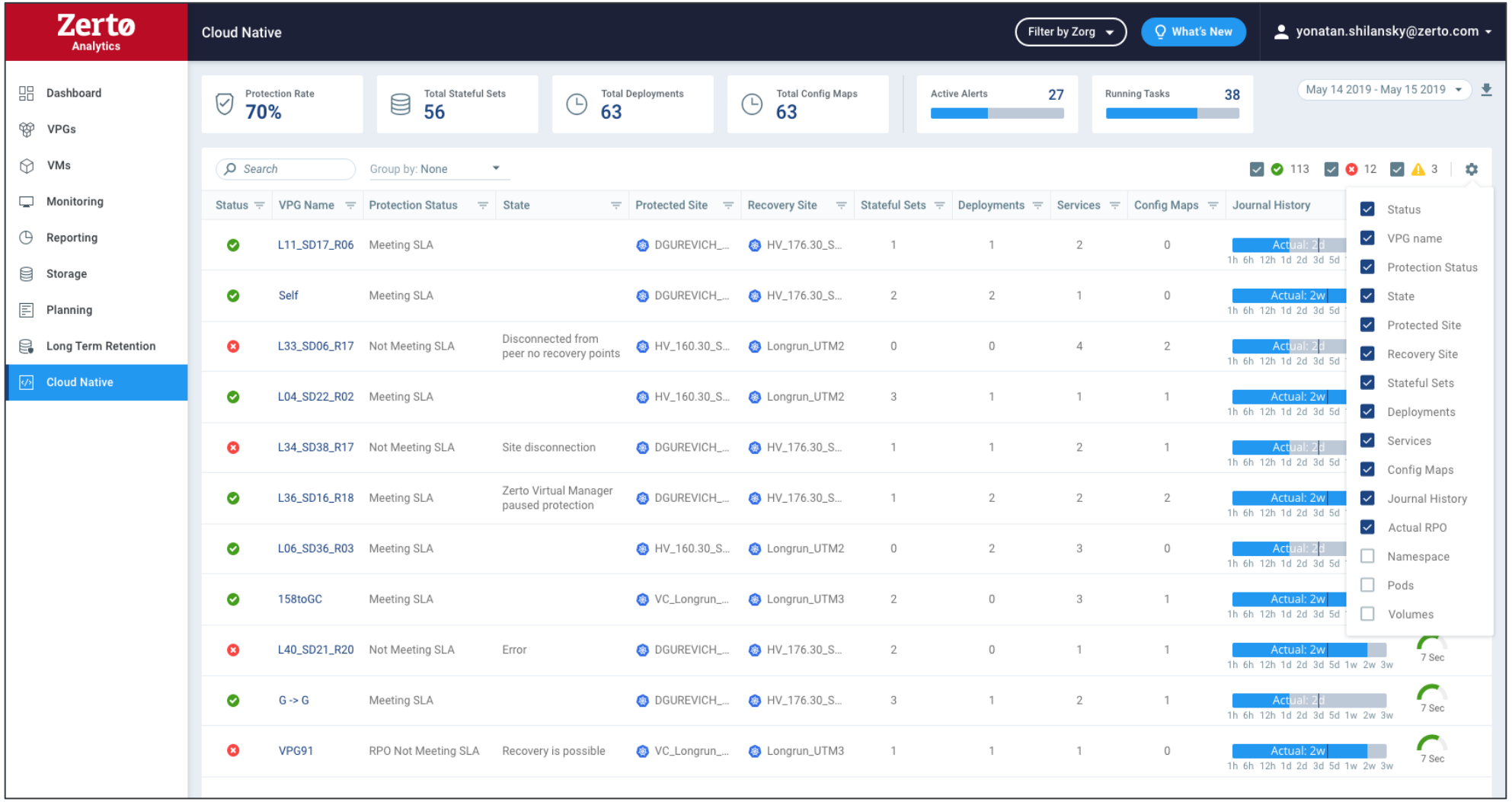
Key Design Element: **Going Native**

- Design as a K8s application
- Platform Independence
- Scale with the environment

Key Design Element: **Hybrid and Multi-Cloud Architecture**

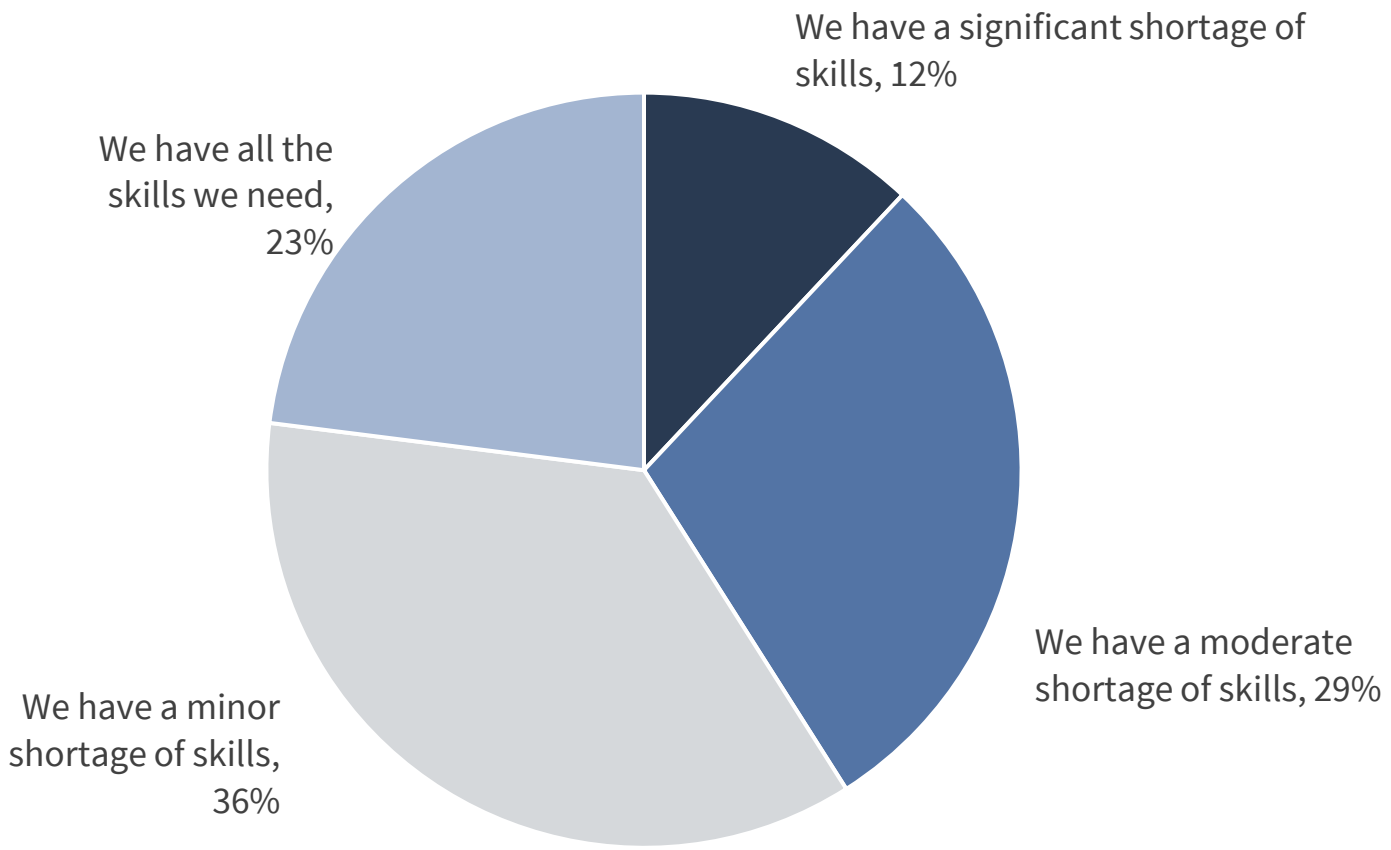


Key Design Element: Deep Analytics



Survey: **Skillset**

Question text:
How would you characterize your organization's available level of skills when it comes to container backup and recovery requirements? (Percent of respondents, N=334)



Source: ESG Research Publication, *Container Data Protection*, June 2020

Key Design Element: **Resources & Education**

- Online materials and POV
- myZerto Hands-on Lab
- Technical Preview Download

Thank you