Red Hat Summit

Connect

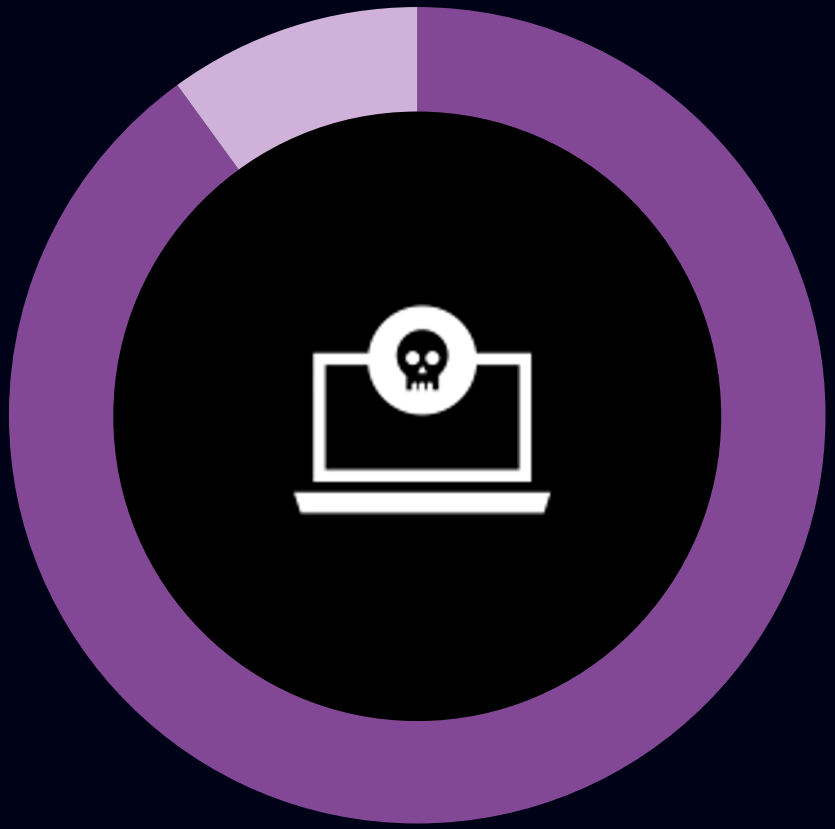
The Business Value of Unified Resilience

Alessandro Palagiano | Sales Engineer, Commvault

Commvault | Red Hat

90%

of organizations report cyber resiliency is impacted by fractured tools*



Commvault

* Futurm Group Insights

Modern Cyber Resilience Landscape

The perimeter is gone

- Increased Cloud Utilization
- Remote Work
- The Internet of Things
- Software Supply Chain
- AI and Machine Learning
- Social Networking

Companies have focused here. But…
Security is blind to unknowns.
Administrators must embrace the breach.

The next fight is here…Recovery readiness and testing enables businesses to be cyber resilient.

The breaches keep coming.
83% of organizations studied have reported a material breach, with 50% happening in the last year.

Commvault

Source: 2024 Commvault Cyber Readiness Report

You can’t trust complex, siloed data ecosystems

Commvault Cloud delivers the cleanest, fastest, most complete cyber recovery. Unified resilience that spans across Kubernetes, OpenShift VMs, cloud-native applications, and AI data pipelines. Simplify your resilience and gain confidence you’ll be able to recover when disaster strikes.

Commvault®

Commvault Kubernetes Protection

Full cluster protection

Commvault allows creation of a **Full cluster Application group**.

Dynamic discovery and protection of all namespaces (including system namespaces) at backup runtime.

Full-cluster protection is the **default** protection method for the default application group, including existing default app groups

Namespace protection

Commvault protects **entire namespaces** (vs. only detected apps)

Namespace protection protects all^ API resources or objects contained within a namespace.

Namespace-level protection is the **default** protection method when selecting a namespace

ETCD & SSL cert protection

Commvault protects the **ETCD key-value backing store** and **SSL certs** for Kubernetes.

Commvault utilizes **etcdctl** to create an ETCD snapshot file, then copies this file to the Commvault content store.

Commvault also protects some of the SSL certificates for the control plane node the etcd backup runs on

Commvault

Broader ecosystem support

docker

VMware Tanzu

RED HAT® OPENSHIFT

aws

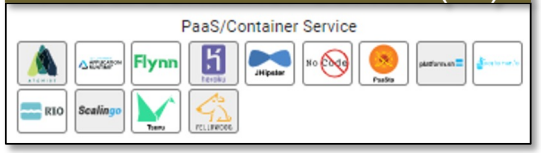
Microsoft Azure

ORACLE Cloud

Azure Kubernetes Service (AKS)

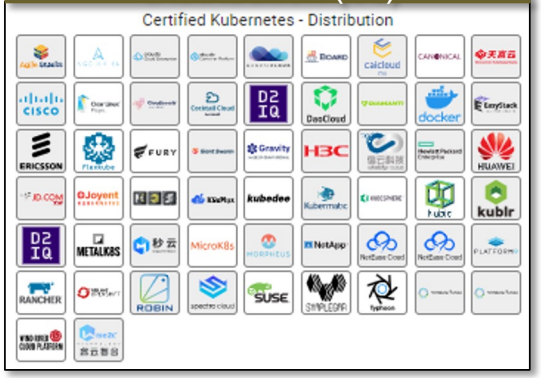
Google Kubernetes Engine

PaaS/Container Service (13)



Hosted (143)

Distribution (56)



CNCF Cloud Native Interactive Landscape

Native OpenShift Protection

UNIFIED PROTECTION FOR CONTAINERS AND VMS

- Manage OpenShift Virtualization VMs and Kubernetes workloads through one policy model (application group)
- Auto-discover workloads (containers, PVCs, VMs) in OpenShift clusters
- Protect mixed environments without juggling multiple backup tools

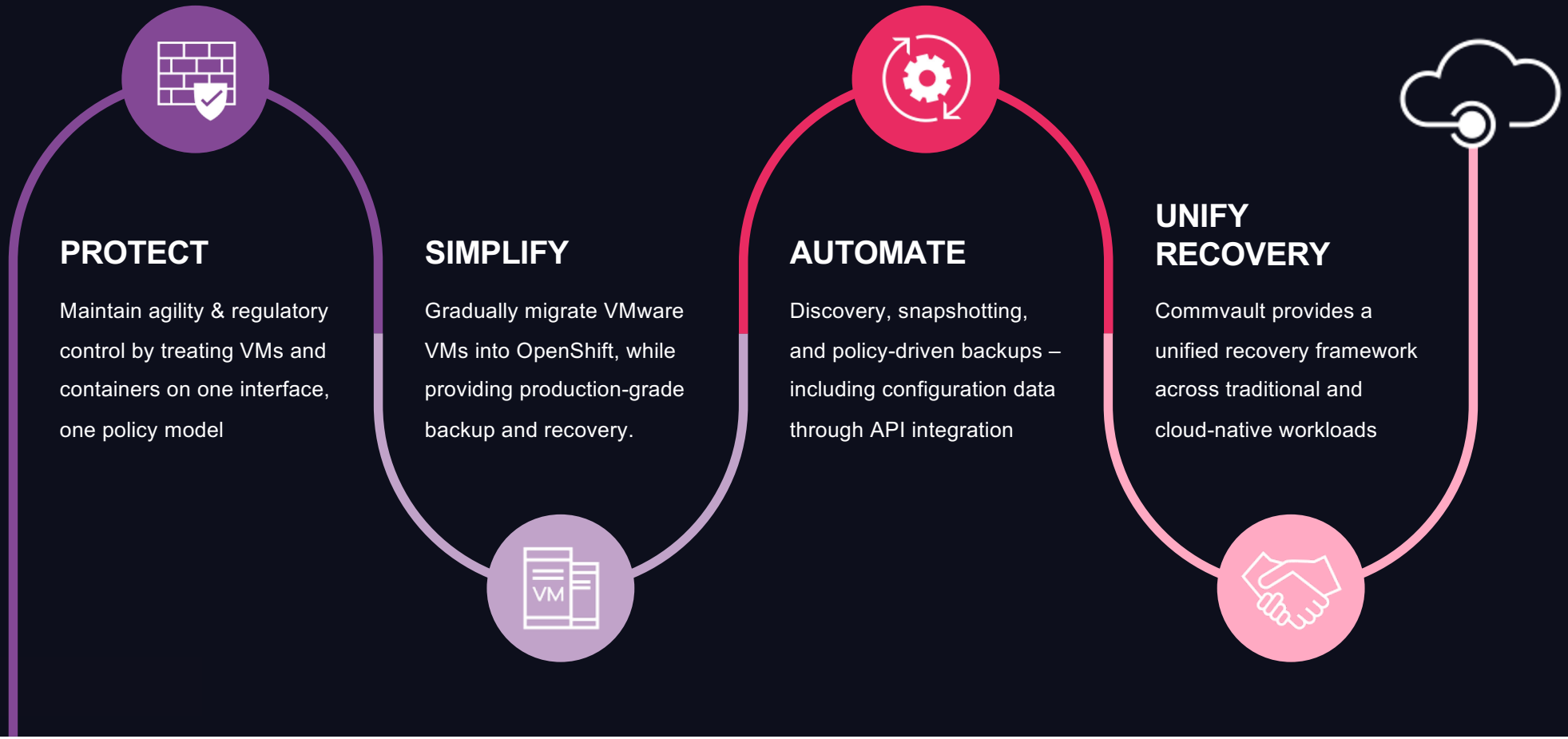
FLEXIBLE BACKUP AND RESTORE OPTIONS

- Incremental backups by default (automatic full backups if no incremental backups exist)
- In-place restores (same cluster, same namespace)
- Out-of-place restores (different cluster/namespace, with StorageClass mapping)
- VM configuration preserved (CPU, Memory, hostname, power-on option)

ADVANCED RESTORE CONTROLS

- Apply restore modifiers during restore (change namespace, labels, StorageClass)
- Cross-cluster recovery for DR, migration, or testing/development scenarios
- Granular exclusion rules applicable to specific workloads, VMs, PVCs, or resource types

Streamline VM Protection in OpenShift Virtualization



PROTECT

Maintain agility & regulatory control by treating VMs and containers on one interface, one policy model

SIMPLIFY

Gradually migrate VMware VMs into OpenShift, while providing production-grade backup and recovery.

AUTOMATE

Discovery, snapshotting, and policy-driven backups – including configuration data through API integration

UNIFY RECOVERY

Commvault provides a unified recovery framework across traditional and cloud-native workloads

Unified Interface for Multi-Cloud & Hybrid Deployments

SINGLE POINT OF CONTROL

For all protection across cloud, on-prem, and hybrid

CENTRALIZED POLICY ADMINISTRATION

One central repository for policies to span workload types, providing protection levels to meet varying SLAs

SCALE ACROSS CLOUDS

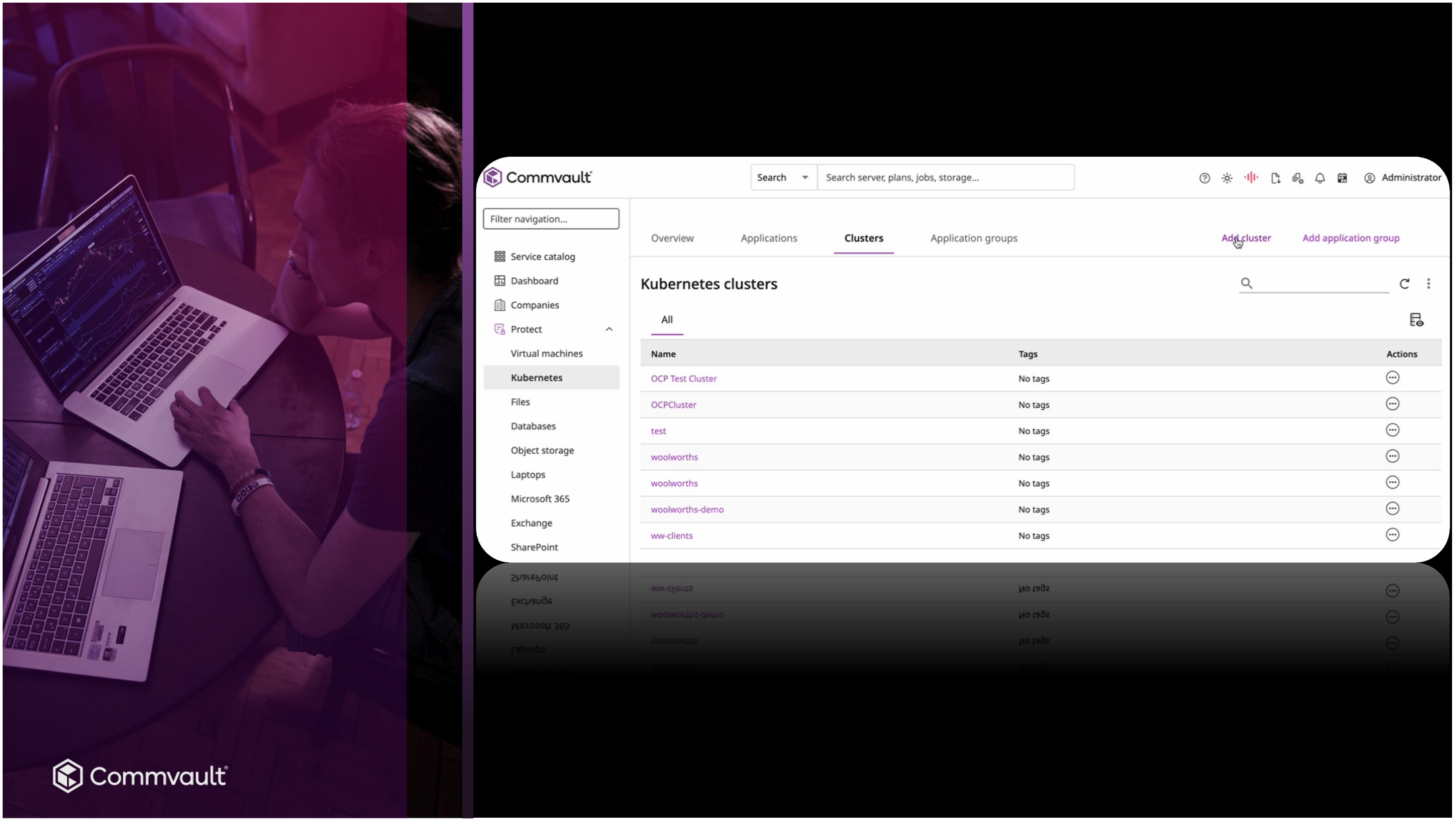
Supports multi-region, multi-cloud, and hybrid deployments

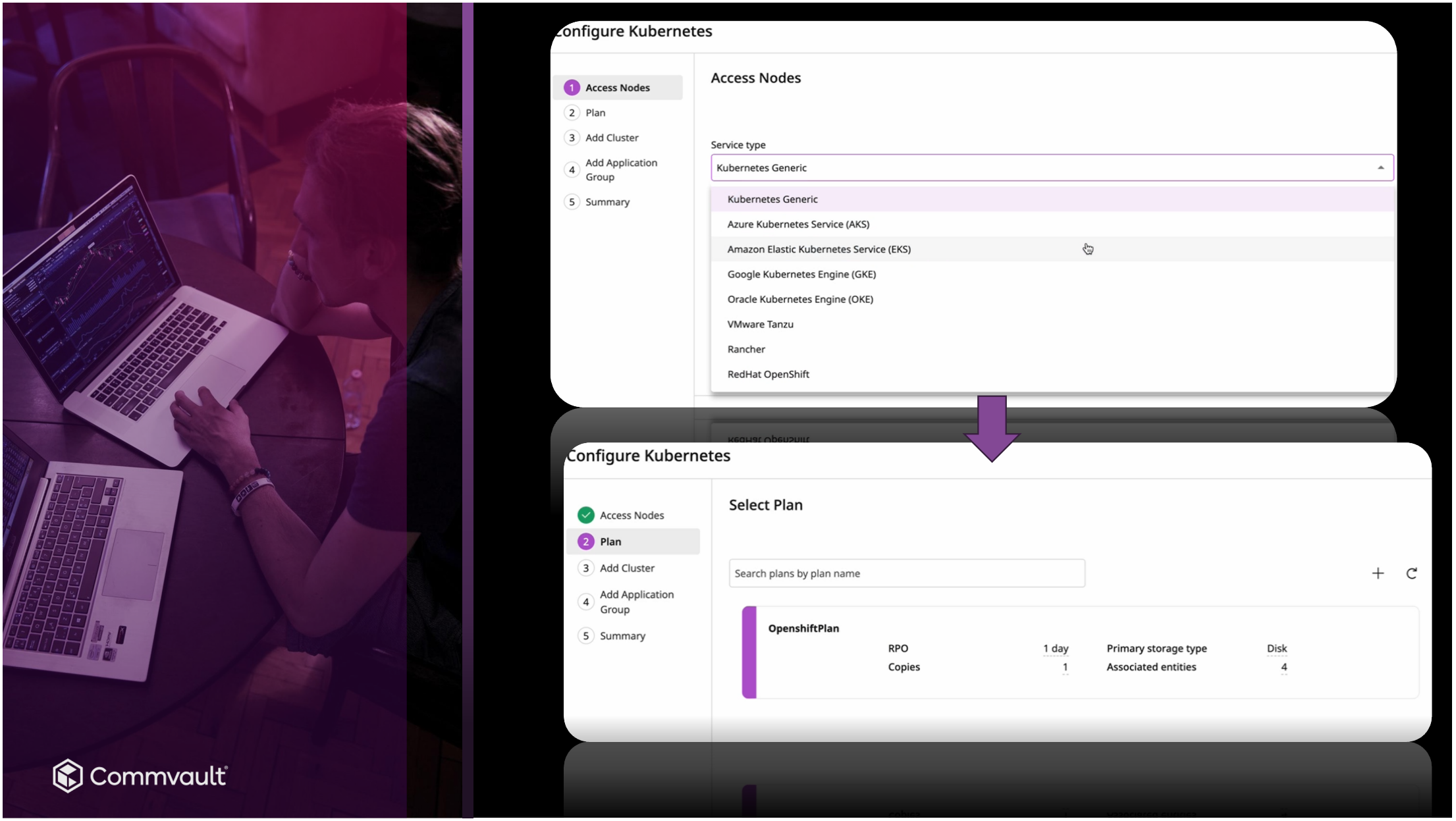
UNIFIED REPORTING

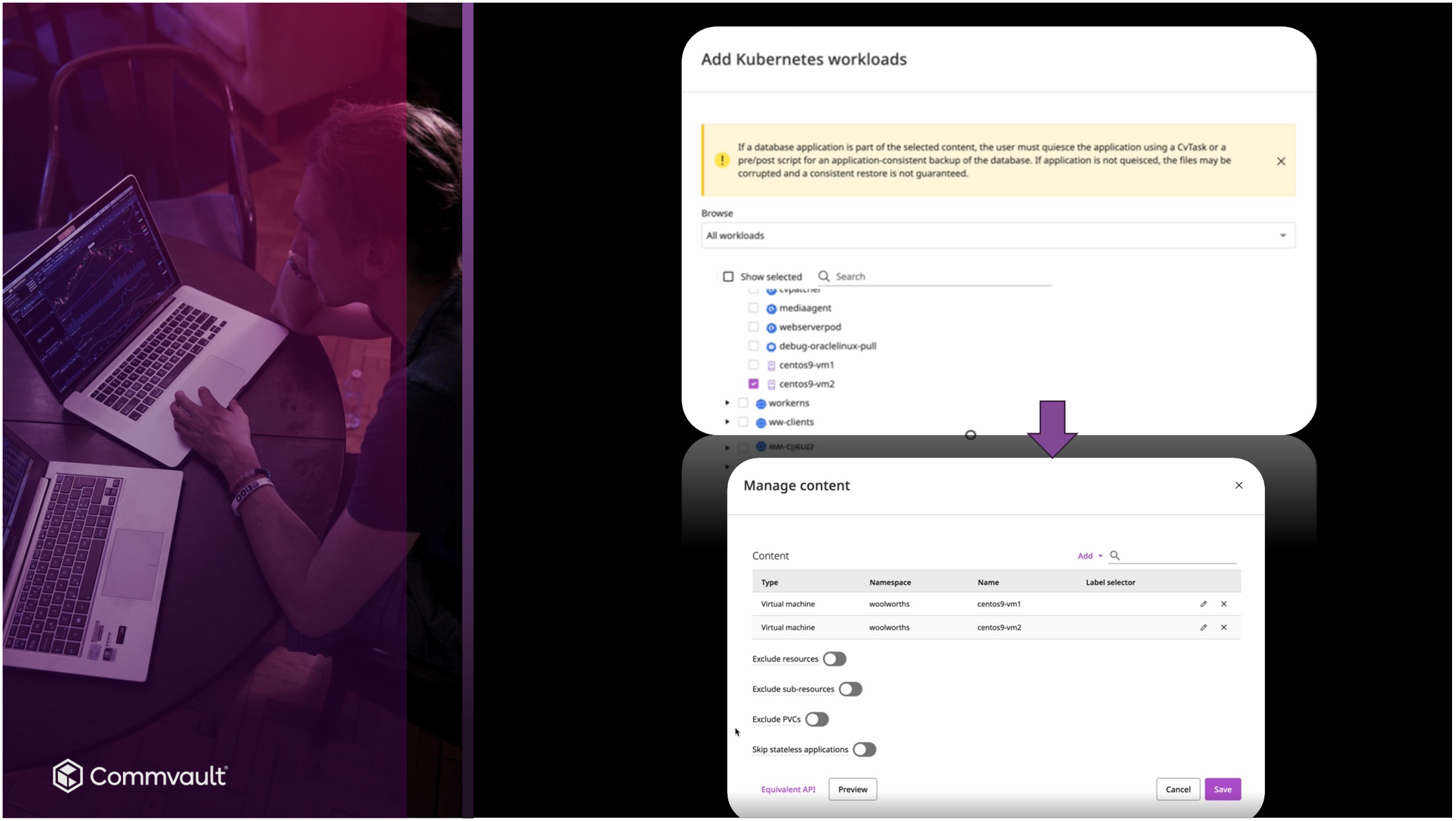
Customizable dashboards for performance, cost, usage, and health metrics

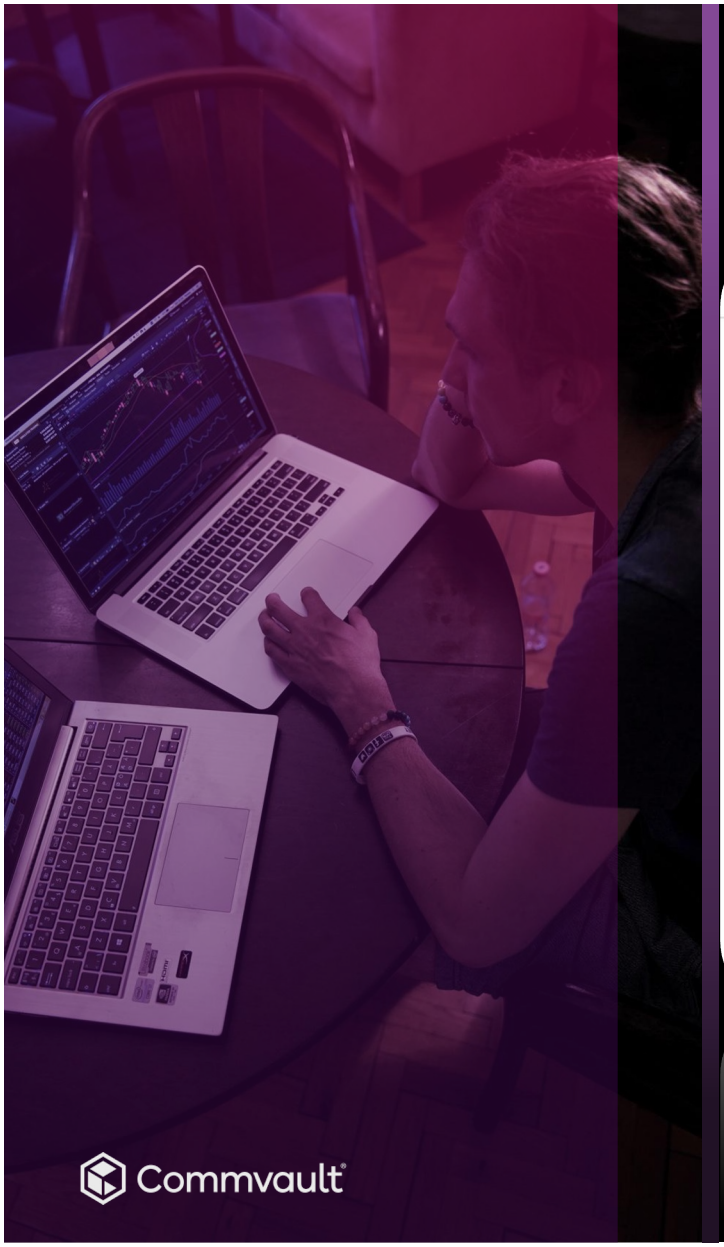
Commvault

Walkthrough Sample Screenshots


Commvault
Search
Search server, plans, jobs, storage...
Administrator
Filter navigation...
Service catalog
Dashboard
Companies
Protect
Virtual machines
Kubernetes
Files
Databases
Object storage
Laptops
Microsoft 365
Exchange
SharePoint
Overview
Applications
Clusters
Application groups
Add cluster
Add application group
Kubernetes clusters
All
Name
Tags
Actions
OCP Test Cluster
No tags
OCPCluster
No tags
test
No tags
woolworths
No tags
woolworths
No tags
woolworths-demo
No tags
ww-clients
No tags
Commvault


Configure Kubernetes
1 Access Nodes
2 Plan
3 Add Cluster
4 Add Application Group
5 Summary
Access Nodes
Service type
Kubernetes Generic
Kubernetes Generic
Azure Kubernetes Service (AKS)
Amazon Elastic Kubernetes Service (EKS)
Google Kubernetes Engine (GKE)
Oracle Kubernetes Engine (OKE)
VMware Tanzu
Rancher
RedHat OpenShift
Configure Kubernetes
Access Nodes
2 Plan
3 Add Cluster
4 Add Application Group
5 Summary
Select Plan
Search plans by plan name
OpenshiftPlan
RPO 1 day
Copies 1
Primary storage type Disk
Associated entities 4
Commvault


Commvault
Add Kubernetes workloads
If a database application is part of the selected content, the user must quiesce the application using a CvTask or a pre/post script for an application-consistent backup of the database. If application is not queisced, the files may be corrupted and a consistent restore is not guaranteed.
Browse
All workloads
Show selected
Search
mediaagent
webserverpod
debug-oraclelinux-pull
centos9-vm1
centos9-vm2
workerns
ww-clients
Manage content
Content
Add
Type
Namespace
Name
Label selector
Virtual machine
woolworths
centos9-vm1
Virtual machine
woolworths
centos9-vm2
Exclude resources
Exclude sub-resources
Exclude PVCs
Skip stateless applications
Equivalent API
Preview
Cancel
Save



Configure Kubernetes

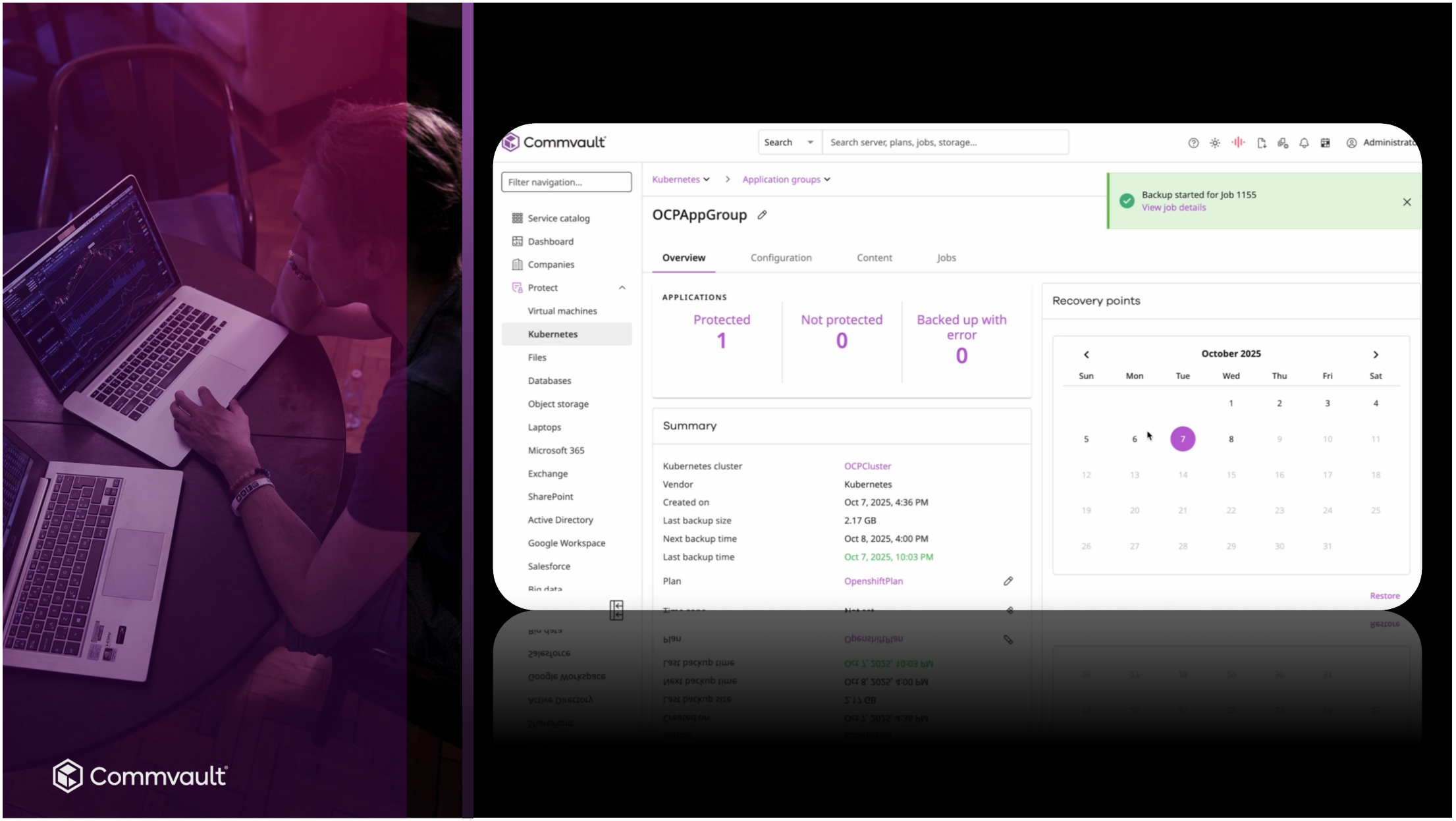
- Access Nodes
- Plan
- Add Cluster
- Add Application Group
- 5 Summary

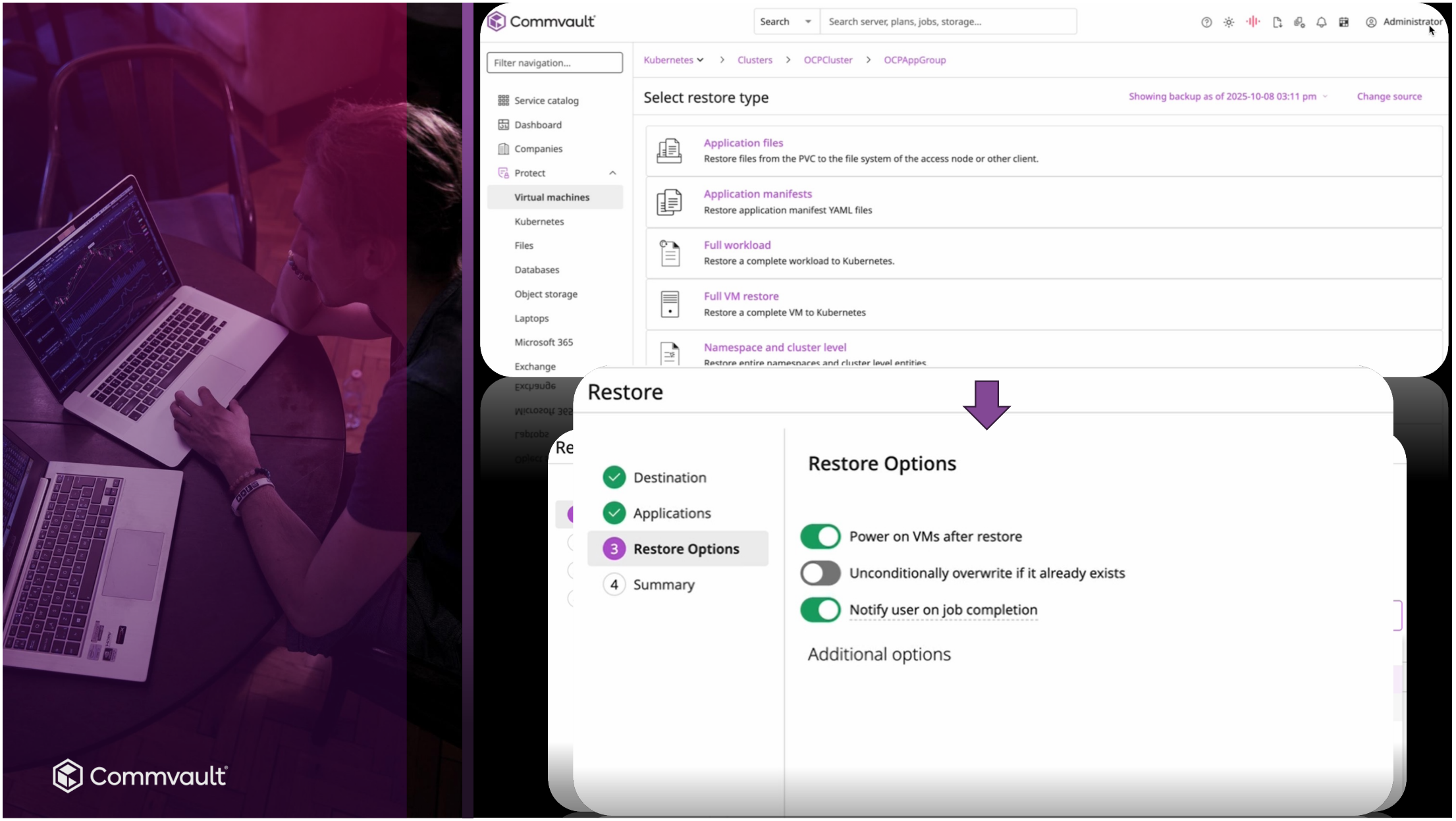
Summary

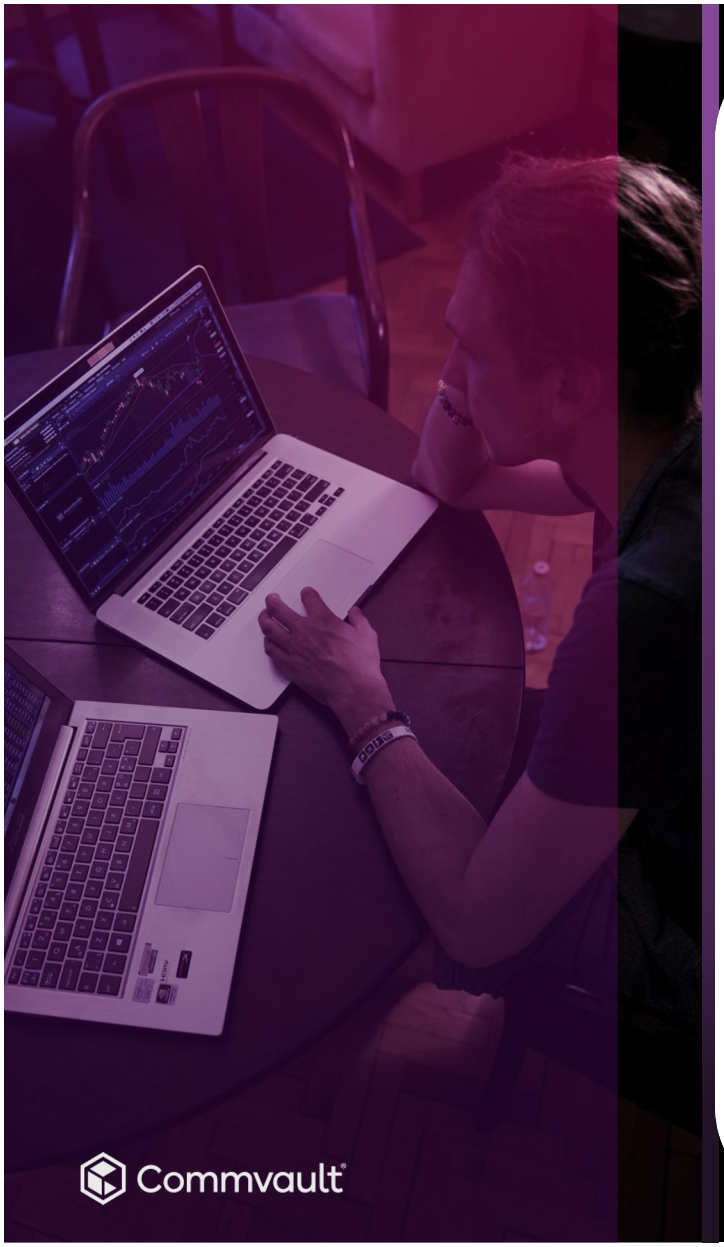
Congratulations! You have successfully configured a new Kubernetes cluster and selected your applications for protection. A backup job will be started in accordance with your selected backup plan.

Kubernetes cluster	woolworths-demotest
Application group name	woolworths_appgroup_demotest
Plan name	OpenshiftPlan
Schedule	1 day
Copies	1
Primary storage type	Disk
Entities	4
Next backup time	Dec 31, 6:00 PM

Finish


Commvault
Search
Search server, plans, jobs, storage...
Administrator
Filter navigation...
Service catalog
Dashboard
Companies
Protect
Virtual machines
Kubernetes
Files
Databases
Object storage
Laptops
Microsoft 365
Exchange
SharePoint
Active Directory
Google Workspace
Salesforce
Big data
Kubernetes
Application groups
OCPAppGroup
Backup started for Job 1155
View job details
Overview
Configuration
Content
Jobs
APPLICATIONS
Protected
1
Not protected
0
Backed up with error
0
Summary
Kubernetes cluster
OCPCluster
Vendor
Kubernetes
Created on
Oct 7, 2025, 4:36 PM
Last backup size
2.17 GB
Next backup time
Oct 8, 2025, 4:00 PM
Last backup time
Oct 7, 2025, 10:03 PM
Plan
OpenshiftPlan
Recovery points
October 2025
Sun
Mon
Tue
Wed
Thu
Fri
Sat
Restore
Commvault


Commvault
Search
Search server, plans, jobs, storage...
Administrator
Filter navigation...
Service catalog
Dashboard
Companies
Protect
Virtual machines
Kubernetes
Files
Databases
Object storage
Laptops
Microsoft 365
Exchange
Kubernetes
Clusters
OCPCluster
OCPAppGroup
Select restore type
Showing backup as of 2025-10-08 03:11 pm
Change source
Application files
Restore files from the PVC to the file system of the access node or other client.
Application manifests
Restore application manifest YAML files
Full workload
Restore a complete workload to Kubernetes.
Full VM restore
Restore a complete VM to Kubernetes
Namespace and cluster level
Restore
Destination
Applications
3
Restore Options
4
Summary
Restore Options
Power on VMs after restore
Unconditionally overwrite if it already exists
Notify user on job completion
Additional options
Commvault



Example: Change the host for the resources of kind "Route" with the name "ocp-route" after restore

Selectors and Actions

- **Selector**: Kind | **Value**: Route
- **Selector**: Name | **Value**: ocp-route
- **Action**: Modify | **Path**: /spec/host | **Value**: ilocpbkp401.source | **New value**: ilocpde487.destination | **Parameters**: Exact

YAMLs

Test modifiers

Selected modifiers

modify-h...

Paste source YAML here

```yaml
apiVersion: route.openshift.io/v1
kind: Route
metadata:
  name: ocp-route
spec:
  host: ilocpbkp401.source
  port:
    targetPort: 8080
  to:
    kind: Service
    name: route-svc
```

TEST

Modified YAML

```yaml
apiVersion: route.openshift.io/v1
kind: Route
metadata:
  name: ocp-route
spec:
  host: ilocpde487.destination
  port:
    targetPort: 8080
  to:
    kind: Service
    name: route-svc
---
```

EQUIVALENT API CLEAR COPY

Simplify Resilience

Align cyber resilience with business efficiency. Organizations leveraging Commvault's unified platform have seen measurable reductions in operational overhead and recovery time

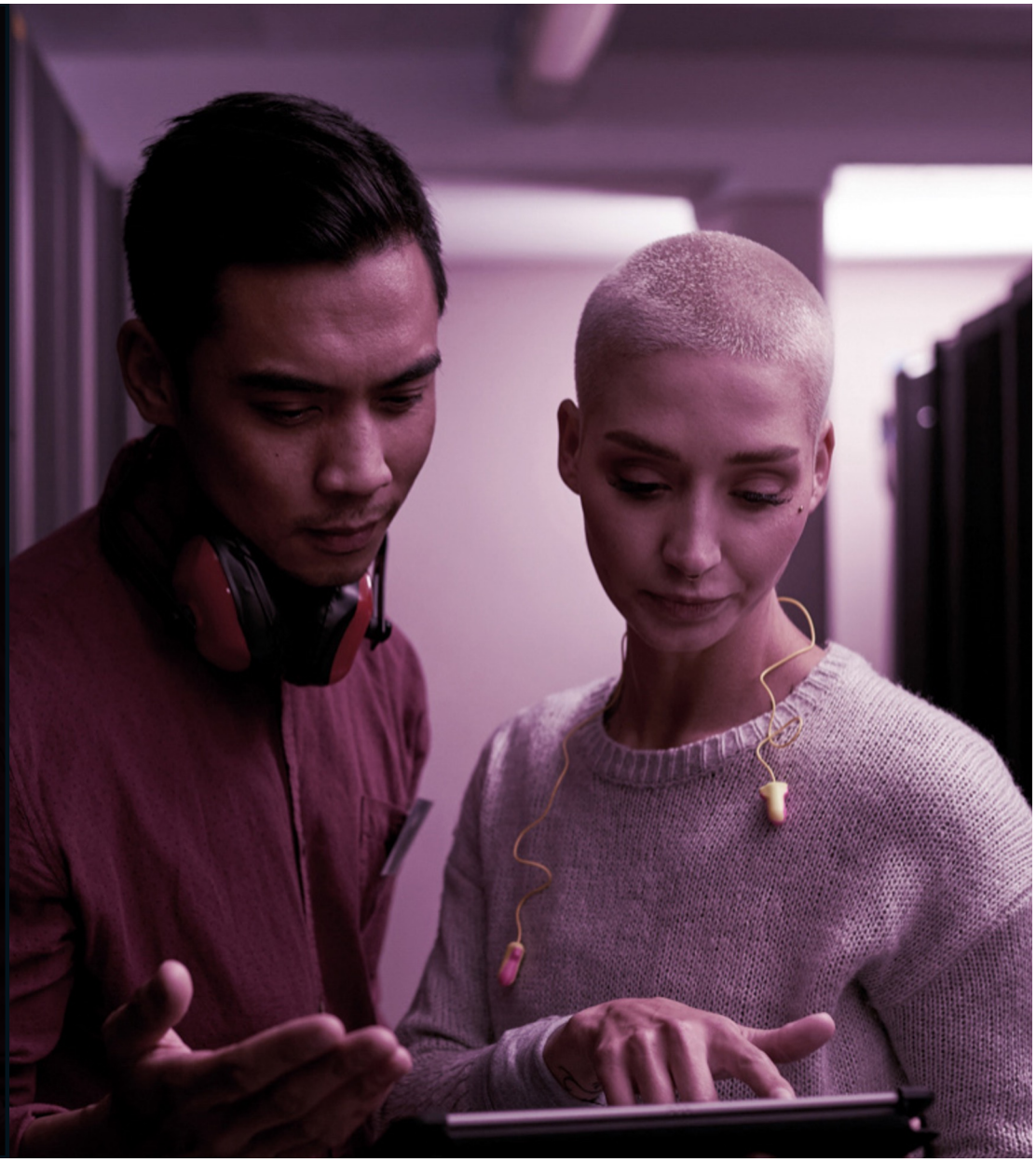
Reduce Risk

Minimize downtime and data loss during an attack. Unified governance reduces the surface area of risks of compromised data as it sprawls across clouds, regions, data centers and edge locations.

Control Cost

Reduce administrative burden and accelerate modernization. Consolidated tools and automation reduce TCO while improving governance across hybrid environments

Commvault®



Commvault

Thank You

Red Hat Summit

Connect

linkedin.com/company/red-hat

facebook.com/redhatinc

youtube.com/user/RedHatVideos

twitter.com/RedHat

Commvault