

From Threat to Recovery: Securing the Complete Client Environment

Goran Slijepčević
Sales Manager - Adriatic

Primož Golob
Senior Sales Engineer - Adriatic

September, 2026

“

Cyber Resilience is the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems."

National Institute of Standards and Technology (NIST)

WHY COMMVAULT?

The trusted leader in cyber resilience

#1

In cyber resilience
for more than 25
years and counting

G

Only Gartner MQ Leader
for 15 consecutive years

>6_{EB}

Safeguard more than
6 exabytes of cloud data

FR

Only FedRAMP High
cyber resilience platform

1.6K

We have over 1.4K
patents for
groundbreaking
innovation



The first to unify data protection
for on-prem, cloud and hybrid



The first to integrate ransomware
protection into our platform



The only to offer unique
architecture with any-to-any
portability and defense in depth



The only vendor to offer
Cleanroom Recovery

THE CHALLENGE

Resilience has always been a big job.

Delivering on your mission depends on overcoming adopted, inherited, and ongoing risks.

10 years ago

- Distributed on-prem backups
- Slow, tape-based recovery
- Begin transition to VMs

5 years ago

- Lift-and-shift programs begin en masse
- Digital transformation propagates machine identities
- SaaS adoption for mission critical data
- Cloud-native backup infrastructure

2 years ago

- From cloud and then back to on-prem
- Ransomware goes mainstream
- Structured and unstructured data at scale

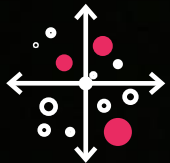
Yesterday

- Passive security models begin to *fail* en masse
- IDC projects 100% growth in data volumes every 4 yrs
- Data center storage to grow from 10.1 ZB (zettabytes) in 2023 to 21.0 ZB in 2027: an 18.5% CAGR

THE CHALLENGE

Resilience has always been a big job.

Delivering on your mission depends on overcoming adopted, inherited, and ongoing risks.



Data is
**Scattered
Everywhere**



Identities
are **Exploding**



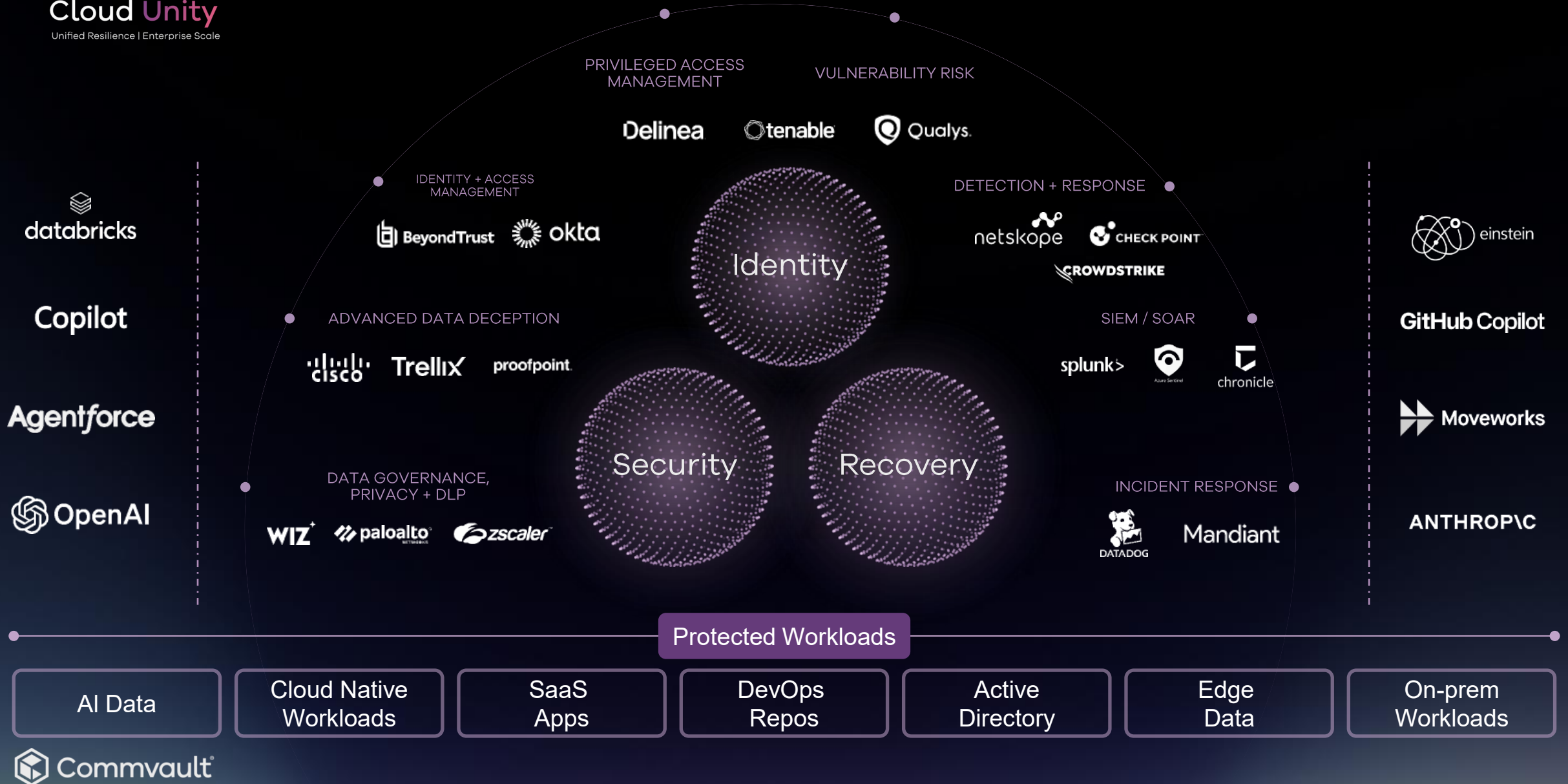
Compliance
Challenges
Keep **Expanding**



Ransomware
Accelerates,
Security Lags



AI **Unlocks
Innovation,**
Unprecedented
Risk





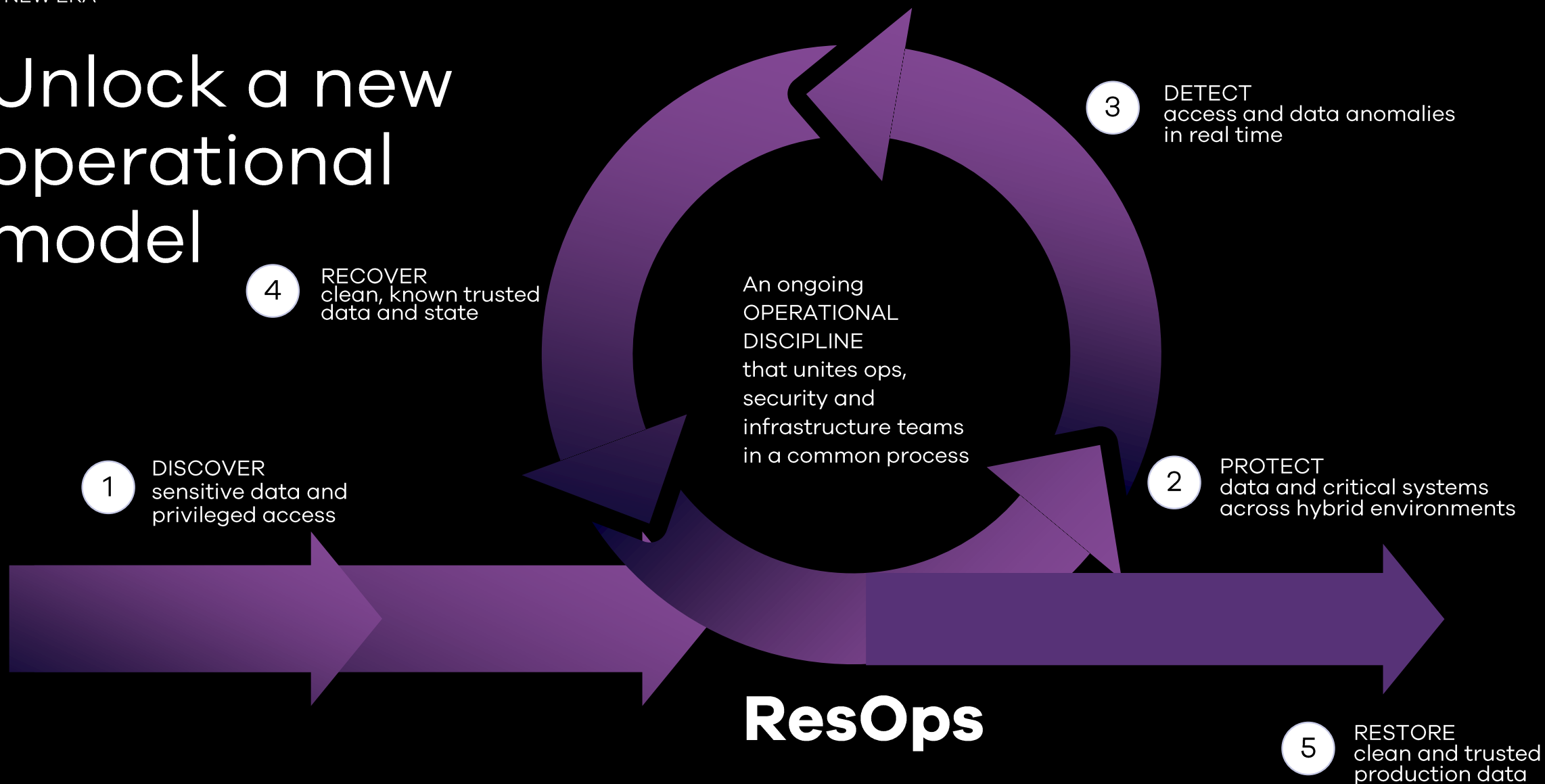
Identity

Security

Recovery

A NEW ERA

Unlock a new operational model



CONTROL PLANE – ZERO TRUST ARCHITECTURE

Secure ANY workload

DATA PLANE – STORAGE AGNOSTIC PROTECTION

In ANY location

► CLOUD ► SAAS
► ON PREM ► EDGE



3. Self-protected & Re-generating Index and Metadata

2. Storage Agnostic & Immutability

1. Encrypt at Source

STORAGE (DISK, CLOUD, HSX)

Recover to ANYwhere

0. Data



AND NEARLY 200 MORE

Commvault cloud unity for protecting your entire data estate



Cloud			Hybrid			SaaS
VM & K8s	Database	File & Object	VM & K8s	Database	File & Object	SaaS
Azure VM	AWS DocumentDB	AWS S3	VMware vCenter	Oracle	Windows Server	Azure EntraID
AWS EC2	AWS DynamoDB	Azure Blob	Microsoft Hyper-V	Oracle RAC	Linux Server	M365
OCI VM	AWS RDS	Azure Data Lake Storage Gen2	Nutanix AHV	SAP HANA	Clustered File Server	Dynamics 365
Alibaba Cloud	AWS Redshift	Google Cloud Storage	Kubernetes	SQL Server	Endpoint	Salesforce
Google Cloud Compute	Azure Cosmos	Oracle Object Storage	Morpheus	Active Directory	S3 Compatible	Google Workspace
Azure Stack Local	Azure SQL	Azure Files	OpenStack	VM & K8s	NetApp	Azure DevOPS
Azure Stack Hub	Azure Table Storage	AWS FSx Lustre	Proxmox VE	DB2	Dell EMC Isilon	GitHub
	Google Cloud SQL	AWS FSx NetApp ONTAP	Red Hat Virtualization	DB2 Multinode	Dell EMC Unity	GitLab
	Oracle Auto. Database	Azure NetApp Files	VMware Cloud Director	DB2 HADR	Dell EMC VNX/Celerra	
	Google BigQuery	Alibaba Cloud Storage	XenServer	Sybase	Hitachi NAS	
	Databricks	IBM Cloud Storage	Oracle VM	Sybase Cluster	Nutanix	
	MongoDB Atlas		Red Hat OpenShift	Informix	Qumulo	
	Yugabyte			SAP for MaxDB	Google Cloud SQL	
	CouchDB			Postgresql Cluster	VAST	
				Oracle Data guard	Hadoop	
				SAP for Oracle	Cassandra	
				Postgresql		
				Mysql		
				MongoDB		
				CockroachDB		

Future proof readiness for Kubernetes



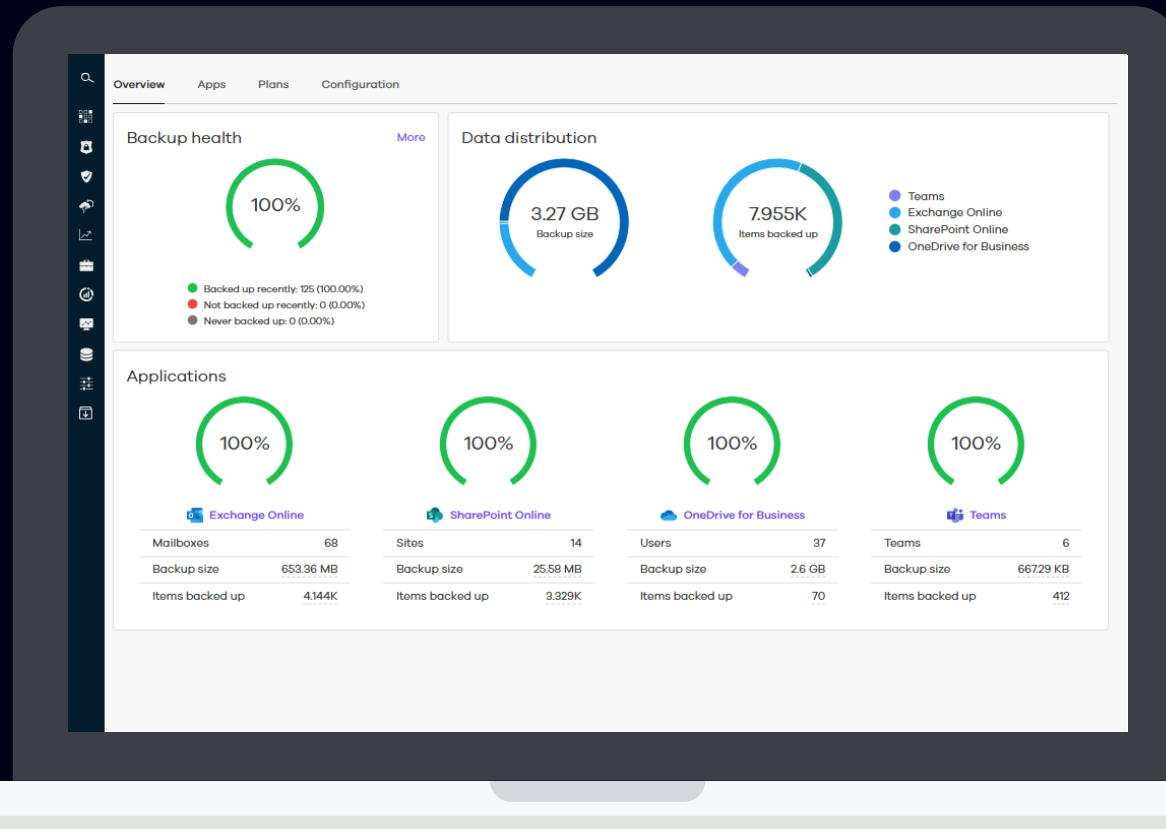
protection, application mobility, and disaster recovery for containerized applications

- ✓ Native Kubernetes® protection (on-prem, cloud)
- ✓ Container Storage Interface (CSI) integration
- ✓ Application consistent protection
- ✓ Granular protection and recovery
- ✓ Migration of containerized apps
- ✓ Validated with Red Hat® OpenShift™, GKE, EKS, AKS
- ✓ Validated with NetApp® Trident™ and VMware® Tanzu™
- ✓ Open approach to Kubernetes support, leveraging CNCF certified distributions



Commvault Cloud: Backup & Recovery for Microsoft 365

Now With Premium M365 Backup Storage



Comprehensive coverage of Exchange, OneDrive, SharePoint, Teams, and more



Proven recovery with granular point-in-time, out-of-plate, and self-service restore options



All-inclusive solution with cloud storage and extended data retention built-in



Robust controls, hardened security, and intuitive eDiscovery to meet SLA regulatory requirements



Premium, high-speed in-place restores for mission-critical users where you demand accelerated recovery times

Automated Forest Recovery for AD

Get Back To Business In Hours Rather Than Days or Weeks



Automate the entire forest recovery process



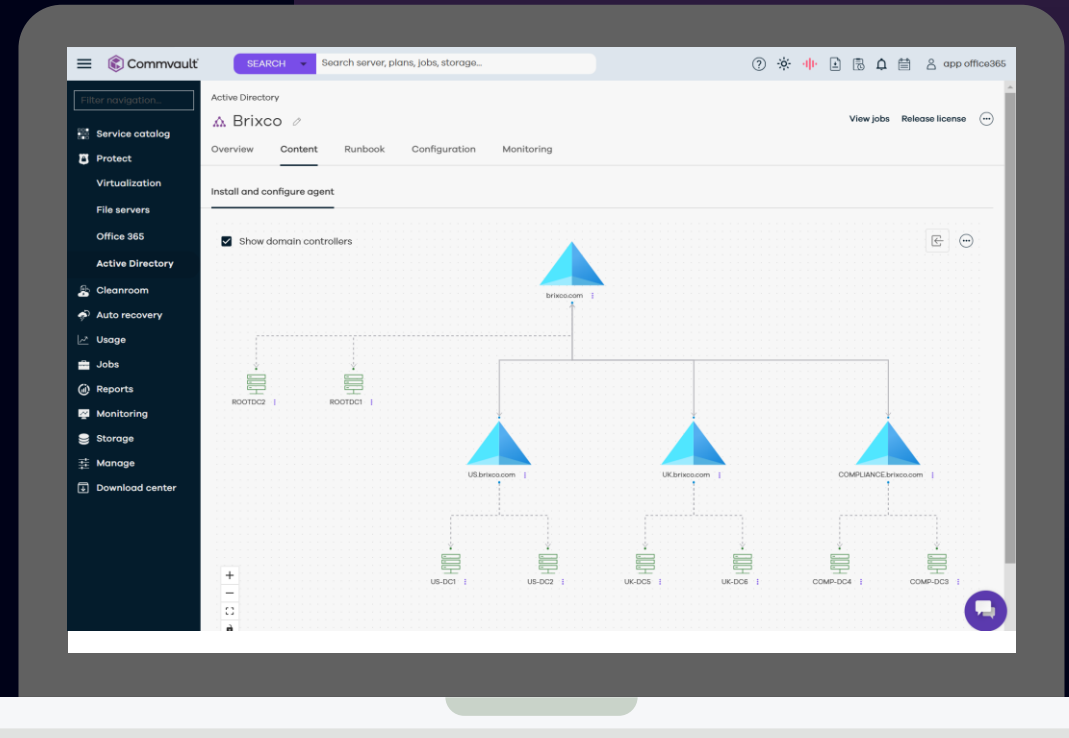
Simplify recovery planning and testing



Accelerate recovery times and advance resilience

Commvault Cloud Backup & Recovery For Ad Enterprise Edition

- **Rapid recovery of the AD forest** to a point in time before an attack
- **Automated orchestration** of multi-step AD forest recovery process
- **Simplified recovery planning** with visual AD topology and prescriptive runbook views
- Supports frequent **disaster and cyber recovery testing**



Identity Resilience

Active Directory | Entra ID | Okta

IAM Resilience

- Real-Time Auditing & Detection = Early Warning
- Automated Rollback & Recovery = Fast, Precise Response
- Forensic Timeline & Cleanroom Validation = Trusted Recovery



Active Directory
ENTRA ID



Okta Protection

brixco.local

● Last updated November 16, 2025 at 10:29 pm EST

Overview Resources Audit Forest recovery Indicators

Recommended actions

Granular recovery for Active Directory

● brixco.local
Granular AD recovery: domain backup failed

Restore

● corp.brixco.local
Granular AD recovery: domain backup failed

Restore

Forest recovery

● lon-dc06.brixco.local
Forest recovery: domain controllers backup failed

Restore

● FR_AzureDRPilot
Step 2.1.16 - Runbook in progress [Waiting for user input](#)

Needs configuration

Granular recovery for Active Directory

2 / 11
Domains not configured

Real-time auditing

Audit Events

Last updated 2 minutes ago

[View all events](#)

5
● Critical

921
● Unclassified

Forest recovery backup

50
Domain controllers

2
● Failed

48
● Success

Granular AD recovery backup

9
Domains

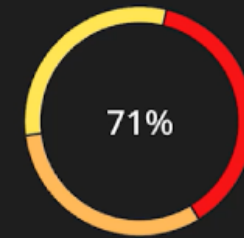
1
● Failed

1
● Pending

7
● Success

Assessment result ⓘ

[View all indicators](#)



5
● Critical
4
◆ High
4
▲ Medium

Recent activity

November 16, 2025

- Critical audit event 10:29 PM
2 critical events occurred
- mfg.brixco.local 10:29 PM
Granular AD recovery: domain backup completed successfully

Enhancing Backup and Extending Beyond With Data Insights and Access



Commvault Data Posture 360

GA Aug'26

Continuous discovery, classification, and risk assessment of sensitive data across production and protected copies to reduce risk and strengthen cyber resilience.



Security Team

Monitors data activity in real time to detect anomalies and enforce zero-trust controls.



Analytics Team

Uses classified, policy-filtered data to drive insights and AI initiatives securely.



Commvault Data Access Manager

GA

Real-time data activity monitoring and fine-grained, policy-based access controls to enforce least-privilege access to production data and AI.



DevOps Team

Delivers governed data access to production data stores for developers or support.



Compliance Team

Audits data access and validates policy enforcement to meet regulatory requirements.

Commvault's Enhanced Threat Analysis

Integrated intelligence to detect threats and recover cleanly with minimal rollback



AI-Enabled Threat Detection

Integrated threat intelligence, SecOps tools, and partner solutions to analyze backup data and identify threats



Flexible protection modes

Flexible scan and hunting modes, with enhanced user experience prepares organizations before recovery is needed

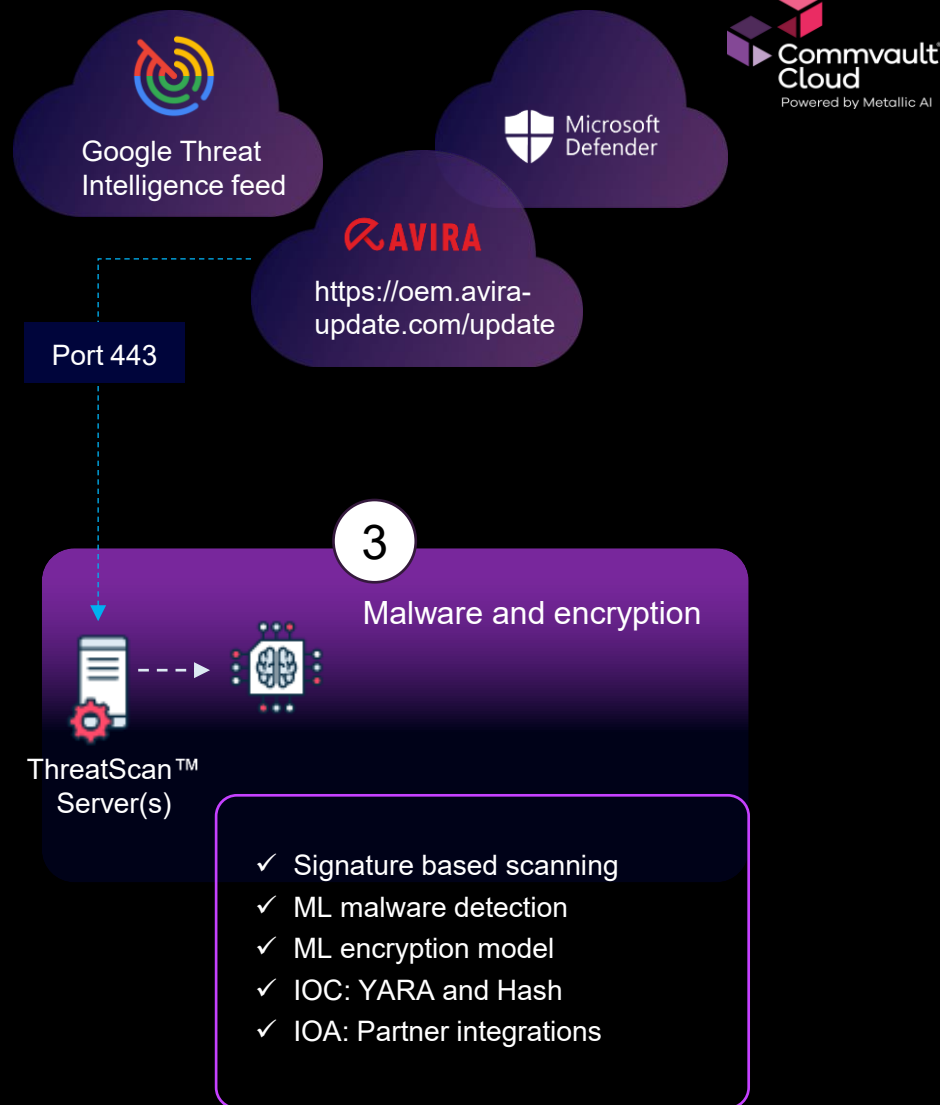
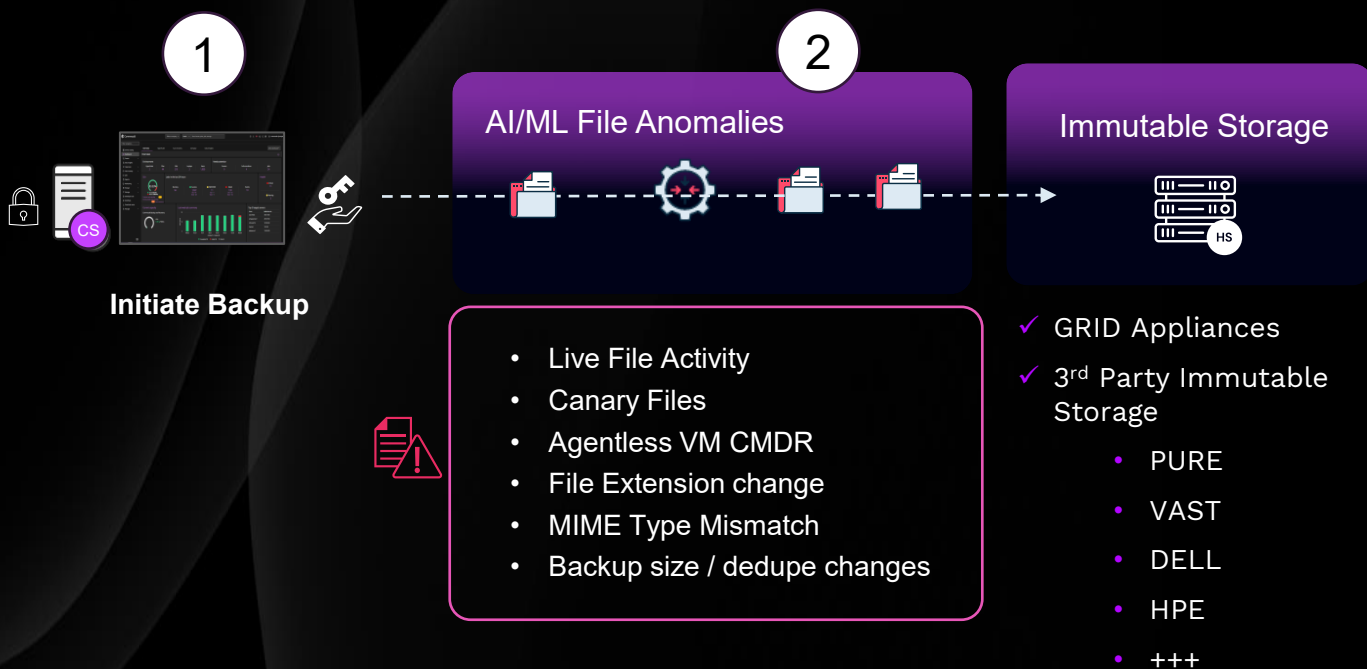


Confident, Clean Recovery

Enables recovery to a trusted state with minimal rollback, reducing the risk of reinfection and business impact

ThreatScan™ for Files | VMs | Objects

scheduled | on-demand | at restore



Clean Recovery point in-time restore

Commvault

Search

Search server, plans, jobs, storage...

⌕

🌙

🔦

🔄

📄

📄

Select a company

@ pschleper

Try new navigation

Filter navigation...

Service catalog

Dashboard

Companies

Protect

Discover

Data Insights

Security services

Cleanroom

Threat scan

Auto recovery

Jobs

Reports

Metrics

Monitoring

Storage

Manage

Developer tools

Workflows

Download center

Store

My apps

Threat scan

FileServerSite1

Restore

Restore

Start your recovery process

Recovery Type

Manual

Select a specific point in time to recover from

Recovery points

Clean Recovery points.

Encryption / Malware

<

May 2026

>

Sun	Mon	Tue	Wed	Thu	Fri	Sat
3	4	5	6	7	1	2
10	11	12	13	14	8	9
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31						

● Clean recovery point

▲ Threats detected

Recovery points Wednesday 06, May 2026

4:51 PM

5:24 PM

Threat findings summary

Malware detected	13
Encryption detected	4

○ Synthetic

Cancel

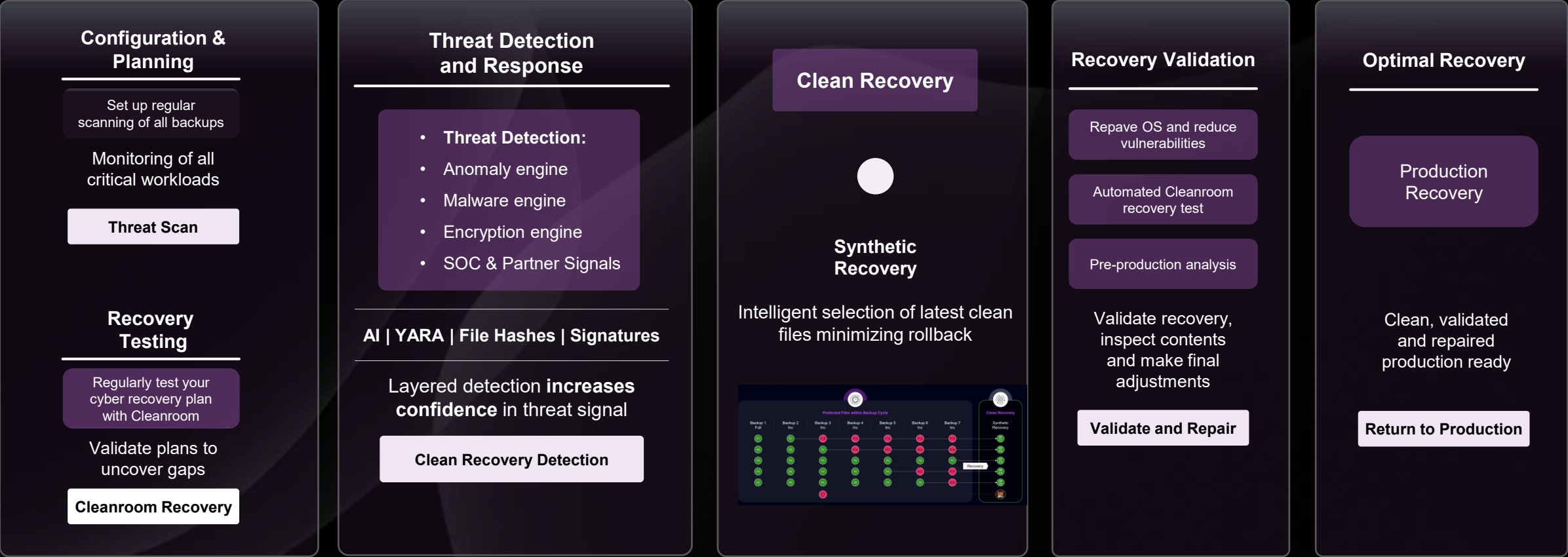
Next →

Commvault

© Commvault 2026

18

Cyber Recovery Process



Patent Pending “Synthetic Recovery”

WHAT IT DOES

Synthetic Recovery uses AI-powered intelligence to restore data to a trusted, clean state – minimizing rollback and reducing reinfection risk and downtime

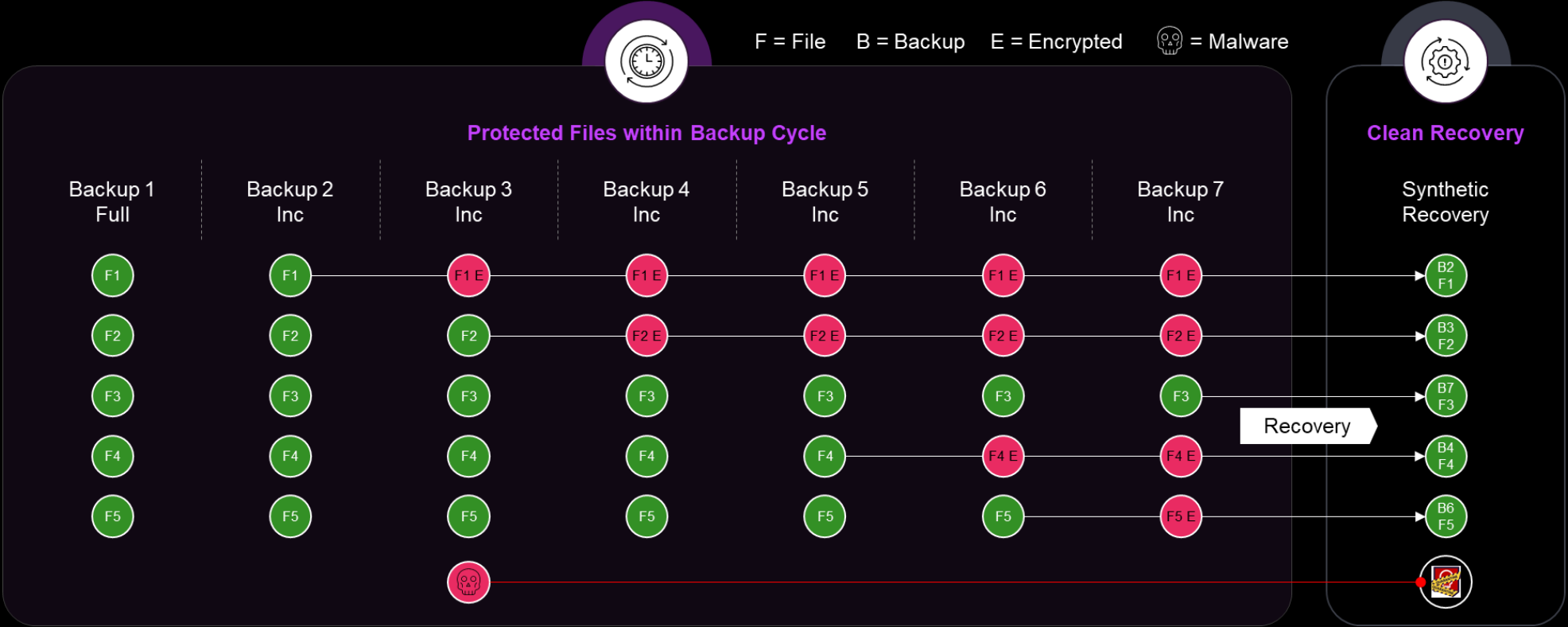
THE CHALLENGE

Traditional recovery forces a painful trade-off

- Roll back far enough to be safe — and lose days of data
- Or recover recent data — and risk bringing the infection back

THE BREAKTHROUGH

Synthetic Recovery helps eliminate that compromise. It automatically reconstructs the latest verified dataset by



Commvault cloud's Cleanroom Recovery:

A COMPREHENSIVE SOLUTION

Commvault Cloud's Cleanroom Recovery is a comprehensive testing and failover solution enabling organizations to mitigate cyber risk effectively. It provides a safe and isolated environment for testing cyber recovery plans, conducting forensic analysis, and supporting business continuity in case of a breach.

Key Features of Commvault Cloud's Cleanroom Recovery

- **Comprehensive testing environment:** Cleanroom Recovery provides a safe and isolated environment where organizations can test their cyber recovery plans without the risk of disrupting production systems.
- **Secure forensic analysis:** Cleanroom Recovery can be used to conduct forensic analysis of known infected systems and identify the root cause of an attack.
- **Faster recovery times:** Cleanroom Recovery can help organizations recover from cyberattacks more quickly by providing a streamlined recovery process.
- **Reduced downtime:** Cleanroom Recovery can help organizations minimize downtime by providing a production failover solution.

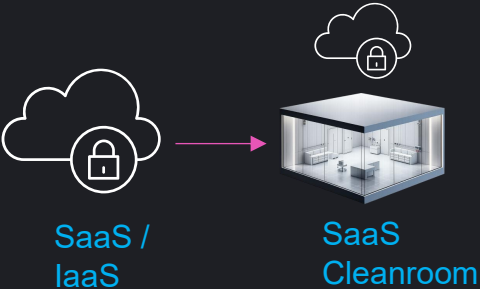


Commvault Cleanroom Recovery Options



1

Commvault Cloud SaaS with Cloud Cleanroom & AGP



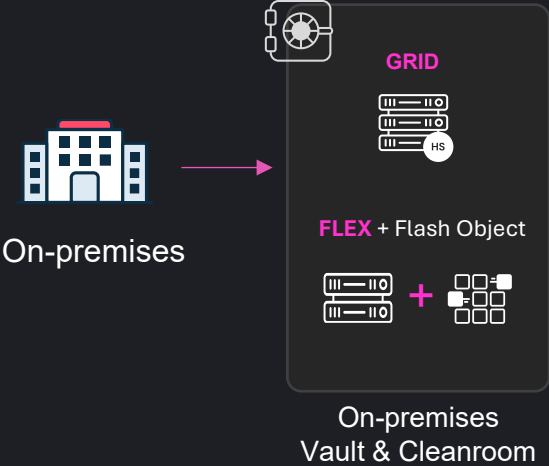
2

On-Premises to Cloud Cleanroom



3

On-Premises Cleanroom with HSX GRID & FLEX Immutable Storage





01

Immutable & Secure Backups

Ensures data protection with immutable backups & air-gapped storage to prevent unauthorized access or ransomware encryption

02

Rapid Recovery from Cyber Threats

AI-driven anomaly detection identifies suspicious activities & potential ransomware attacks early

03

Zero Trust Security Approach

Zero Trust principles enforced by role-based access control (RBAC), encryption, and data segmentation to prevent unauthorized access.

04

Automated Threat Detection & Response

Automated disaster recovery ensures business continuity across cloud platforms

AI-powered threat intelligence in Commvault proactively scans for anomalies

Identification and mitigation of threats on primary storage as well as secondary storage before they spread

Readiness assessment services

05

Hybrid & Multi-Cloud Protection

Seamless data protection across on-premises, hybrid, and cloud environments with integration to Commvault Cloud SaaS solutions

Thank You