Commvault

CITE™

CALIFORNIA IT IN EDUCATION

Cyber Resilience

CITE

Agenda

01 CITE + Commvault Discount Program Plus

02 Commvault + Microsoft

03 Rewind / Cleanroom / Packages

04 Call to Action

CITE + Commvault: Discount Program Plus

DISCOUNT PROGRAM PLUS

Provides cyber resilience, advanced data security and ransomware recovery solutions to California Local Education Agencies at pre-negotiated volume discounts.

KEY PROGRAM FEATURES

- Continuous security, readiness, recovery, and rebalance of data in the event of a cyber attack
- End-to-end risk monitoring
- Isolated cloud recovery testing in a Cleanroom
- Automation for rapid recovery
- Protection for SaaS applications such as Google Workspace & Microsoft 365

PROCUREMENT

- Value Added Reseller Community
- Azure Marketplace

K-12 Cybersecurity Challenges

- Protect systems, networks, programs, and data from digital attacks and misuse.
- Increased risk with more devices in educational settings, making them prime targets for cyber attacks.
- Threats such as ransomware, DDoS attacks, malware, phishing, and social engineering.
- Importance of multi-factor authentication and the legal liabilities for LEAs without strong cybersecurity.
- Reporting breaches and improving cybersecurity practices.
- Financial and operational impacts of cyber attacks, including **recovery costs** and **potential service interruptions.**

Source: Cybersecurity Realities Risks Responsibilities A guide prepared for local education agency board members and staff. - CITE

https://drive.google.com/file/d/1PDM_pWKRT8pl0eJanNTF7WkhY4SmRk-I/view

Enterprise Level Security Challenges

Commvault + Microsoft

Partnership Overview

True Cloud Cyber Resilience for Today's Hybrid World.

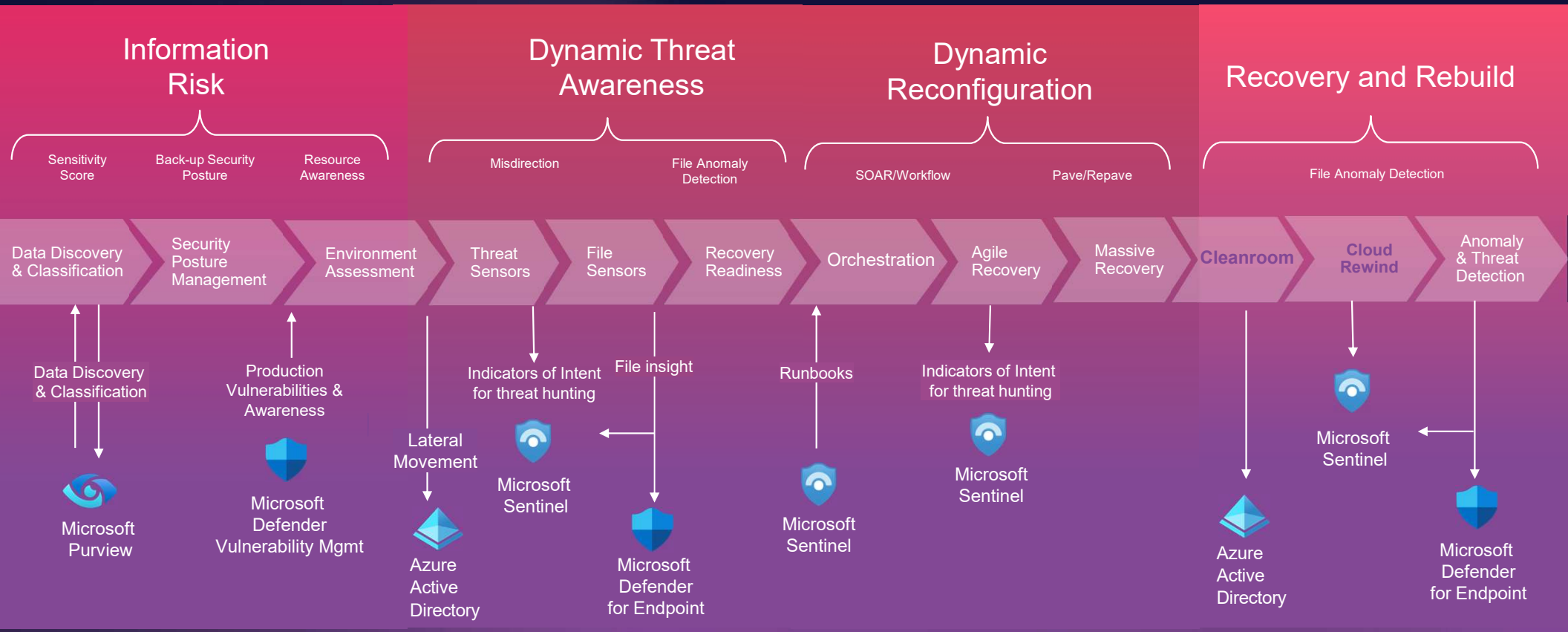
Microsoft

Commvault

2EB+ of customer data protected on Azure

- 25+ years of co-engineered, industry-firsts
- Integrated with Microsoft solutions for lockstep innovation
- Built on Azure / Available in Marketplace

Enable end to end resilience for modern data environments with a zero-trust architecture and deep security integrations.



Commvault Overview

Commvault® Cloud, powered by Metallic® AI

INTRODUCTION

The trusted leader in cyber resilience.

#1

in cyber resilience for more than 25 years and counting.

- Gartner MQ Leader 13 years running
- >3EB Safeguard more than 3 exabytes of cloud data
- FR Only FedRAMP High cyber resilience platform

1.4K

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.

Commvault

We help over 100K organizations around the world secure their data.

NIST Cyber Security Framework

Security is blind to unknowns. **Administrators must embrace the breach.**

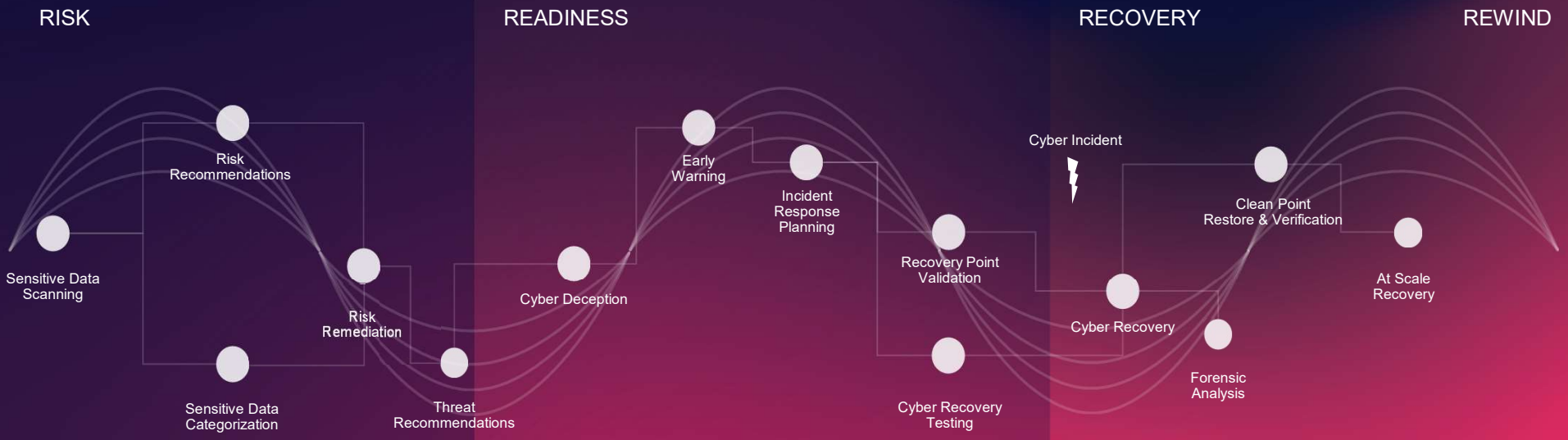
Recovery readiness and testing enables business to be **cyber resilient.**

79% of organizations studied have reported a material data breach over the past 18 months

WHAT'S REQUIRED

True cyber resilience starts before the attack — and never ends.

Based on MITRE CREF and NIST frameworks



Commvault

Cyber Resilience Whiteboard

Legend

Unique Differentiator

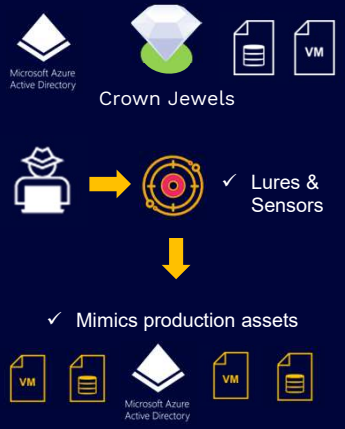
Backup Independent

Commvault Cloud
Powered by Metallic AI

Risk Analysis

- ✓ Identify Data Owners | Access | Permissions
- ✓ PII or other critical contents for leakage or exposure risks

ThreatWise™ Cyber Deception



Commvault Zero-Trust Architecture

CYBERARK MFA | MPA | SAML | PAM | RBAC ENTRUST

Security Ecosystem

✓ Automation | ✓ Webhook's | ✓ Syslog | ✓ API

Microsoft Sentinel | Azure Sentinel

Threat Indicator Detection (IoC's)

Pre-backup Detection	In-line Backup	Post "Threat Scan"
✓ Live File Activity ✓ Canary Files ✓ Deception lures* ✓ Threat Sensors*	✓ Agentless VM CMDR ✓ Extension change ✓ MIME Type Mismatch ✓ File Entropy	✓ View Corrupt versions ✓ Quarantine Versions ✓ Signature Based Scan ✓ AI Zero Day Scan

Quarantine & Clean

Secure Immutable Storage

1 — Immutable Storage (HS) — DC to DC Replication WORM, De-dupe, Encryption — Immutable Storage (HS) — 2

"Airgap"

Cyber Vault Storage

Vault (HS) — 3 — AirGap Protect™ STaaS

SaaS Apps Protection

Cloud Rewind™ Formerly Appranix
Cloud Rebuild as Code

Microsoft Azure Active Directory
Cleanroom Recovery

Commvault

Commvault Cloud Rewind

REWIND • RECOVER • REBUILD

Application resilience is shared responsibility between Customers, CSPs and Partners

CUSTOMER

Responsibility for resilience **'in'** the cloud

Workload Architecture

Change and Data Management and App Resilience | Observation and Failure Management

Observation and Failure Management

CLOUD PROVIDER

Responsibility for resilience **'of'** the cloud

Hardware and Services

Compute | Storage | Database | Networking

Global Cloud Infrastructure

Compute | Availability Zones | Edge Locations

Before

Cloud Rewind™
Formerly Appranix

After

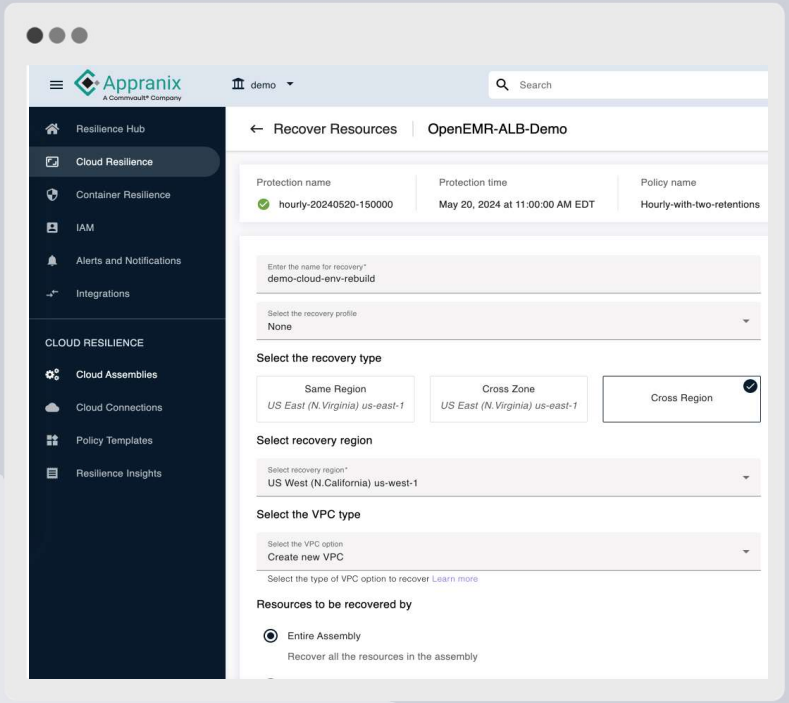
Scale across environments and clouds

REBUILD FROM RANSOMWARE???

- Cloud Recovery Assurance (SLA)
- Dashboard and Reports
- Policy and SLA Management
- Scripting and Infrastructure-as-Code
- Cloud Management Tooling
- CMDB Backup for Recovery
- DR-as-a-Service
- Replication and DR
- Backup-as-a-Service
- Backup Products

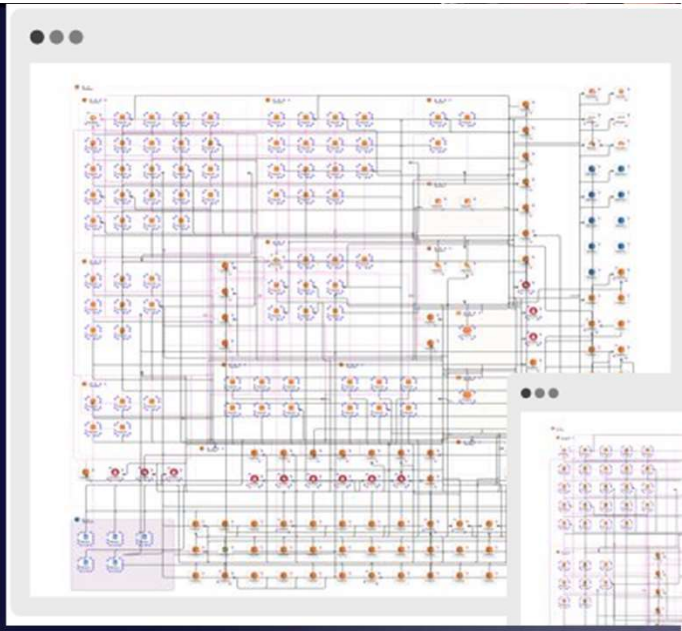
HYPERSCALER CHANGES

Step 1 Log in → **Step 2** Rebuild



Average rebuild time for cloud environments is 24 days!

Do you know your rebuild time?



Do you have the complete picture of what's running your cloud applications?

Most senior leaders do not know what they are running in their environments!

Are you protecting everything you are supposed to?

You are putting organization at an enormous risk!

Do you know what to rebuild?

Financial impact and reputation impact will be enormous!

Commvault

CASE STUDY

Cloud Rewind Solution for **e-Discovery Firm**

Protects all Azure subscription resources, all the cross-border legal documents and data, infrastructure configurations, and dependencies with Cloud Rewind. With an application resilience model, this e-discovery firm has the capability to go back in time along with the application data to be able to get the business back up and running in minutes when a disaster strikes.

With a recent encryption attack across the entire subscription happened, Cloud Rewind was able to recover all the resources in an isolated vNet environment in 36 minutes away from the production network.

> **I can't thank you enough for getting our business back up and running. I will give you reference anytime**
>
> CIO, e-Discovery and AI Analytics

Cloud Rewind Manages

1480 Azure resources across **18 Azure subscriptions** with **329 virtual machines**, **400+ managed data disks**, several scale sets, network security groups, vNets, gateways, resources groups.

\+

Cloud **Infrastructure** Cloud **Application Resiliency**

Commvault

Cleanroom Recovery Overview

HELPS ENSURE RESILIENCE WITH CLEANROOM RECOVERY

The world has changed

Ransomware everywhere — including the backup

99% of ransomware tampers with security and backup infrastructure

Breaches are becoming the norm

66% of organizations surveyed were breached in 2023[1]

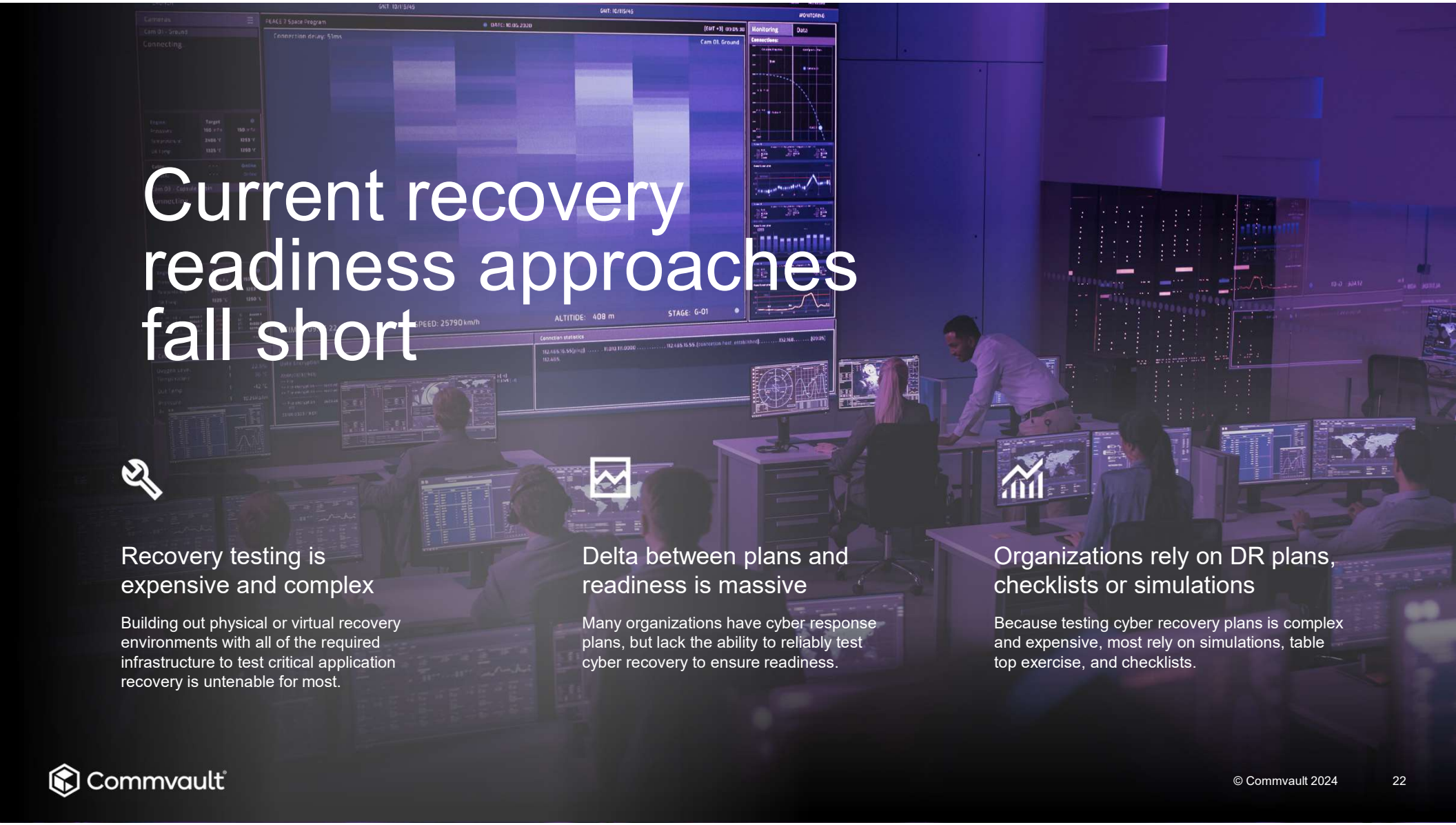
Average time to recover is devastating

24 days is the average reported time to recover from a cyberattack

Commvault

Sources: Microsoft. Sophos. Coveware.

Current recovery readiness approaches fall short



Recovery testing is expensive and complex

Building out physical or virtual recovery environments with all of the required infrastructure to test critical application recovery is untenable for most.

Delta between plans and readiness is massive

Many organizations have cyber response plans, but lack the ability to reliably test cyber recovery to ensure readiness.

Organizations rely on DR plans, checklists or simulations

Because testing cyber recovery plans is complex and expensive, most rely on simulations, table top exercise, and checklists.

BUT … WHAT IF?

There was a way to make certain **clean applications are reliably recovered into a cleanroom**, especially for:

- Recovery testing
- Conducting forensic analysis
- Production failover

Commvault

Commvault® Cloud Packages

PACKAGES TO MEET YOUR PARTICULAR NEEDS

Outcome-oriented, solution packaging

WHAT'S INCLUDED	OPERATIONAL RECOVERY	AUTONOMOUS RECOVERY	CYBER RECOVERY
Foundational Backup & Recovery	●	●	●
Unified management	●	●	●
Security insights	●	●	●
Automated disaster & cyber recovery		●	●
Validated application recovery		●	●
Threat scanning			●
Data discovery & compliance			●
Data security posture remediation			●
AI-driven threat detection			●
Cyber deception & early warning			●

What's Included by Capabilities

OPERATIONAL RECOVERY Foundational data security, recovery, and AI-driven automation	AUTONOMOUS RECOVERY Automated validation, live data replication, and rapid recovery	CYBER RECOVERY Cyber recovery, data security and governance, and early warning
• Backup & Recovery	• Backup & Recovery • Auto Recovery	• Backup & Recovery • Auto Recovery • Threat Scan • Risk Analysis • Threatwise (SaaS Add On): Not Included

Add-ons	M-365	Dynamics	Cleanroom Recovery	Rewind	Air Gap Protect

Call to Action

Call to Action

Engagement at local CITE Chapter Events & Upcoming Microsoft Events

&

Cyber Resilience Whiteboard Sessions

&

Commvault Cloud Rewind, Cleanroom, SaaS Demos

&

Free Cyber Resilience Assessment for CITE Partners

~$20K Value

Braden Connolly
Account Executive – NorCal/Nevada
SLED
M: 408.838.0233
bconnolly@commvault.com

Jeremy Vidales
Account Executive – SoCal/Hawaii
SLED
M: 714.904.7417
jvidales@commvault.com

Thank You!