Commvault Cloud
Powered by Metallic AI

Cyberodporna i wiarygodna kopia backupowa z **Commvault**

Przemysław Fafara
Principal Sales Enginner
Sep 2025

Assume your compromised at all times

490%

increase in data breach victims in the first half of 2024 over the same period the year before

200

avera[illegible] time

ASSUME BREACH

78%

of businesses that paid ransom were compromised again

81%

of breaches caused by weak, reused stolen credentials

96%

of businesses that pay the ransom don't get all their data back

24

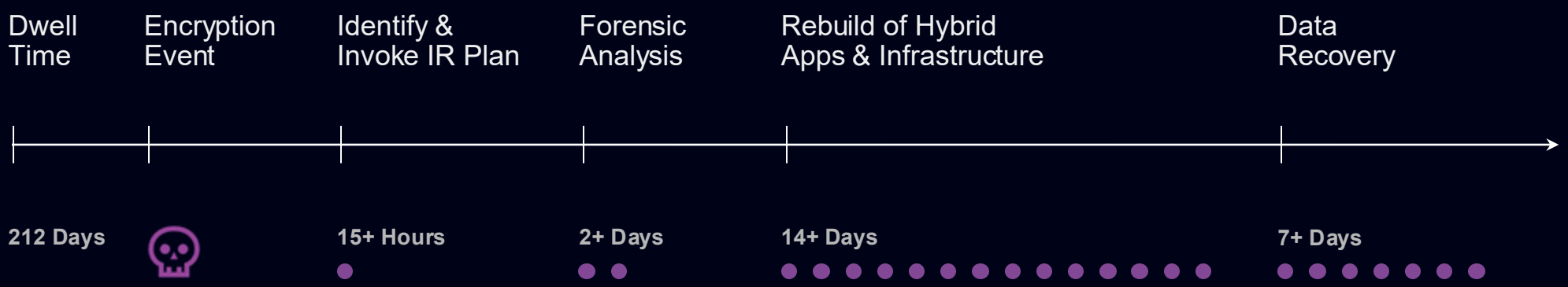
average days lost to downtime

Commvault

Why is Cyber Recovery different?

	Operational Recovery	Disaster Recovery	Cyber Recovery
Use Case			
Value To Improve Resilience	Foundational, Hybrid Enterprise Recovery	+ Speed and Scale	+ Clean Recovery
Platform Capabilities	Self-Service Recovery Granular Point-in-Time Recovery Wide Platform Support	AI-Driven Automation Rapid Recovery (RTO / RPO) Bare Metal Recovery	Clean Restores Any-to-Any Data Portability Forensic Analysis
Work Focus	Security hardening Enterprise-grade recovery “Cyber Safe” Data protection (3-2-1, Immutable + Indelible copies)	Hybrid cloud, mass recovery Recovery validation Continuous data protection	Cleanroom recovery Cleanpoint validation Cyber Posture Assessment + threat detection

Data recovery is only half the battle.



24 days

average time to recover

Security of backup solution

Zero Trust

- Continually validate trust
- Separate access to data access both logically and physically
- Block unauthorized changes to backups
- Reinforce security at application runtime

IDENTITY

- Privileged Access Management
- MPA - Multi-person Authorization
- MFA | 2FA Authentication
- RBAC | SAML | Data Privacy

PRIVACY CONTROLS

- Privacy passkey and lock
- Passkeys for Restore & Install
- Encryption: Data, key management & Network

SEGMENTATION

- Network Topologies | Airgap Controls | Object Locks & Tiering
- Multi-tenancy

DATA IMMUTABLITY

- Compliance & Storage Locks
- Storage WORM Locks

APPLICATION

- CIS Hardened Images
- Binary tamper protection
- Full Audit trail
- NTP Poisoning Protection

RANSOMWARE PROTECTION

- AI & Machine learning events and incident detection
- Antivirus scan of backuped data
- Ransomware protection of backup data

What is *minimum viability?*

Minimum viability is the combination of critical applications, assets, processes, and people required for an organization to deliver on their mission after an attack or disaster.

Commvault

Developing a *plan* for *minimum viability*

What do you need?

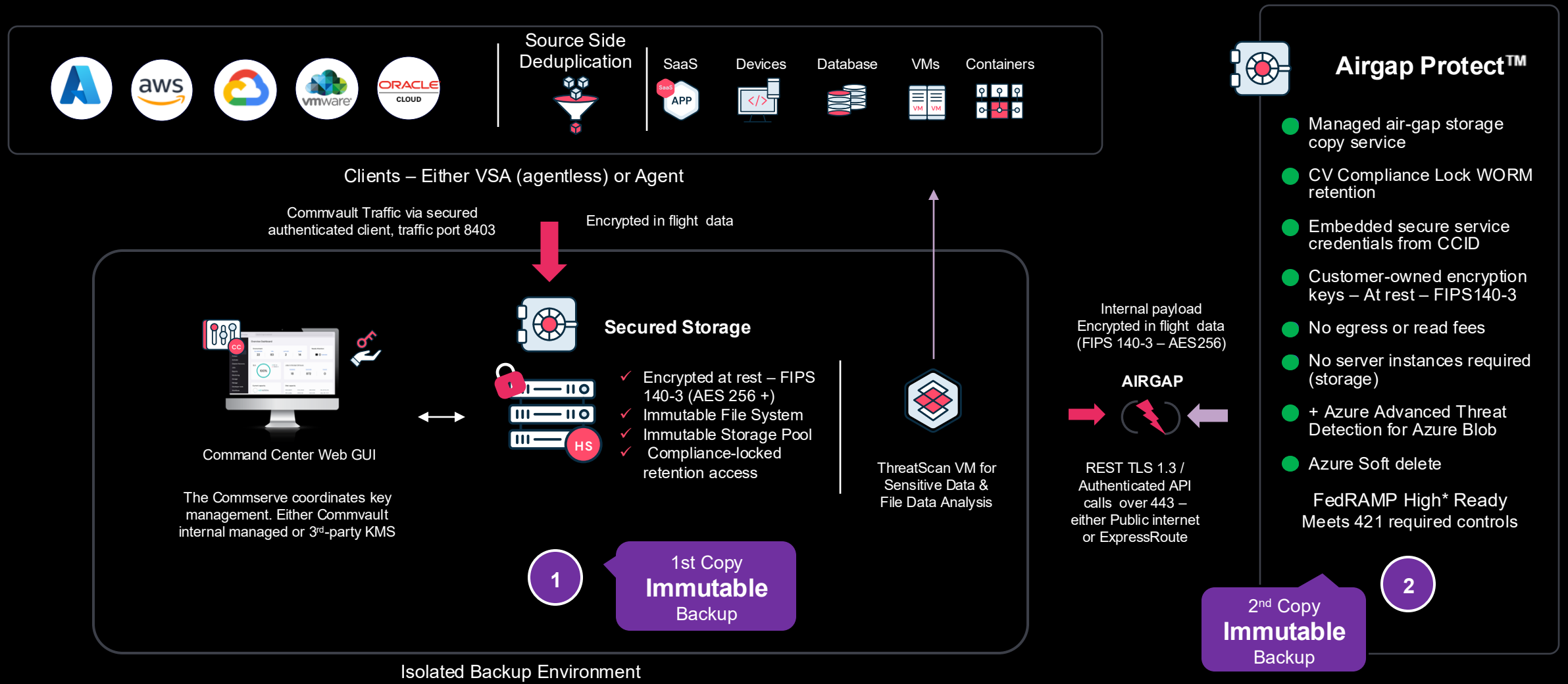
Accurate and aligned view of the core processes and dependent systems.

Understanding the cost of downtime for those core resources.

Clear and actionable plan to restore critical systems, data, and processes.

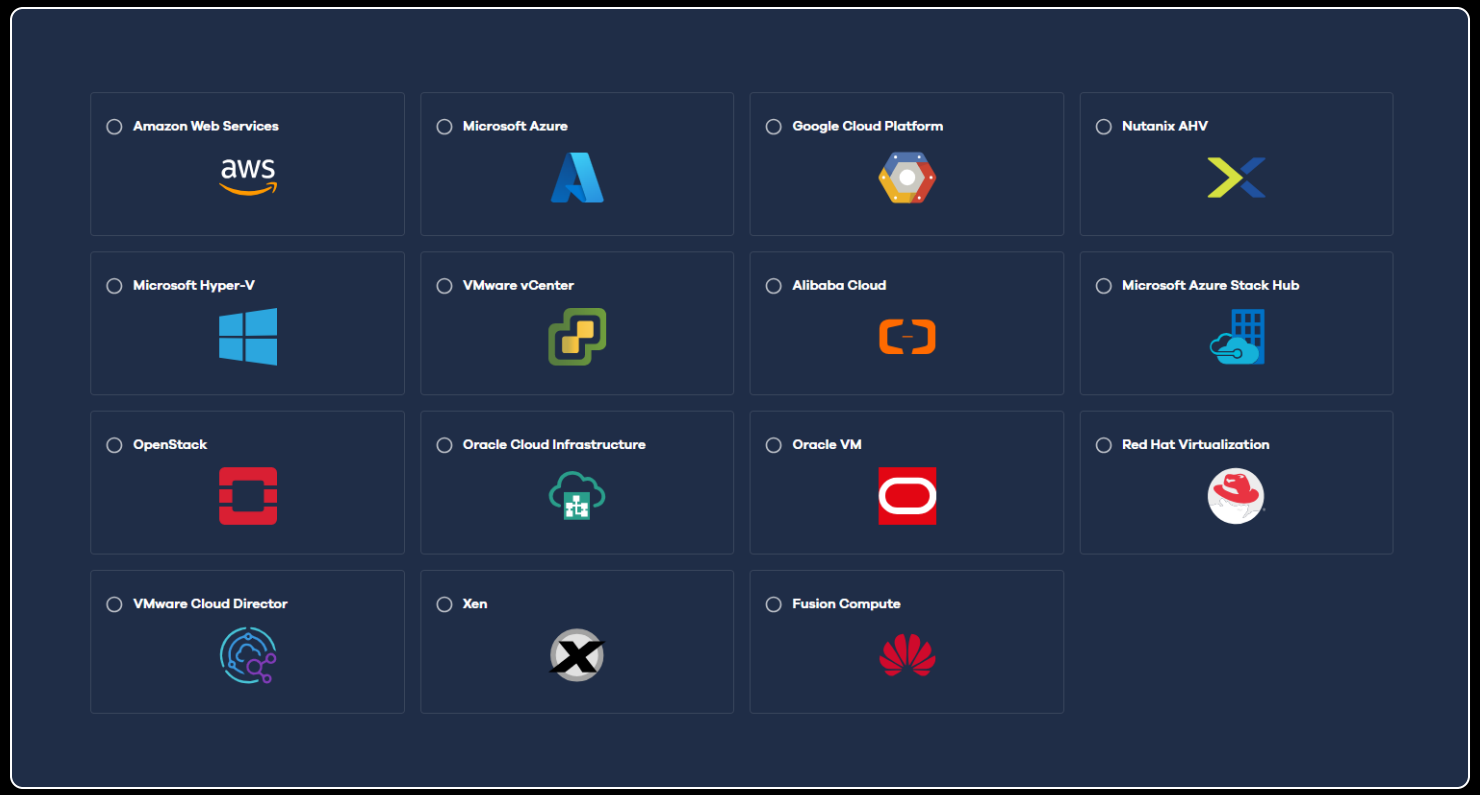
Commvault®

Commvault Immutable Architecture

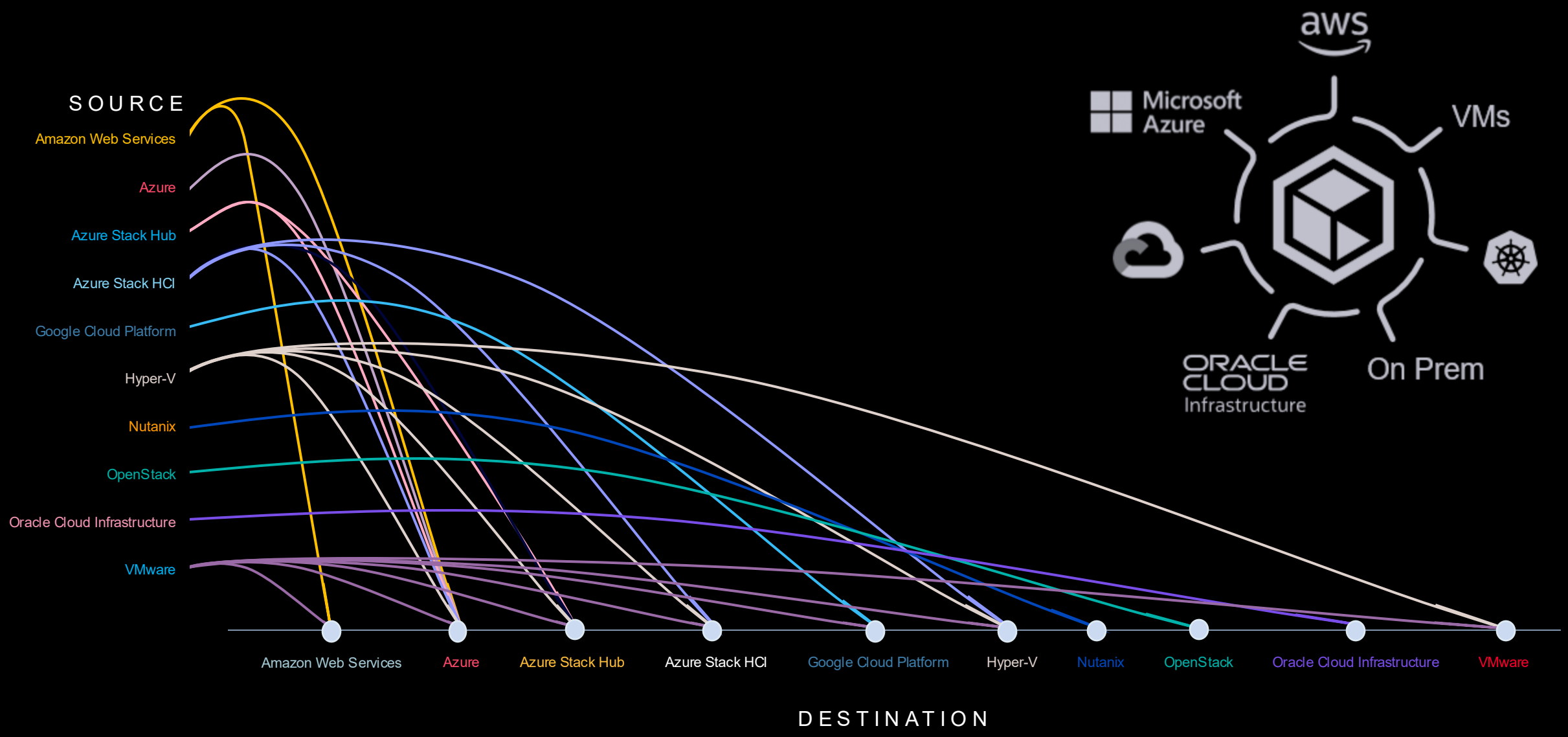


Broadest Hypervisor Support using an Agentless Approach

- Reduced Compute costs
- Reduced Store + Egress
- Breadth of protection
- Unified Management
- Flexibility

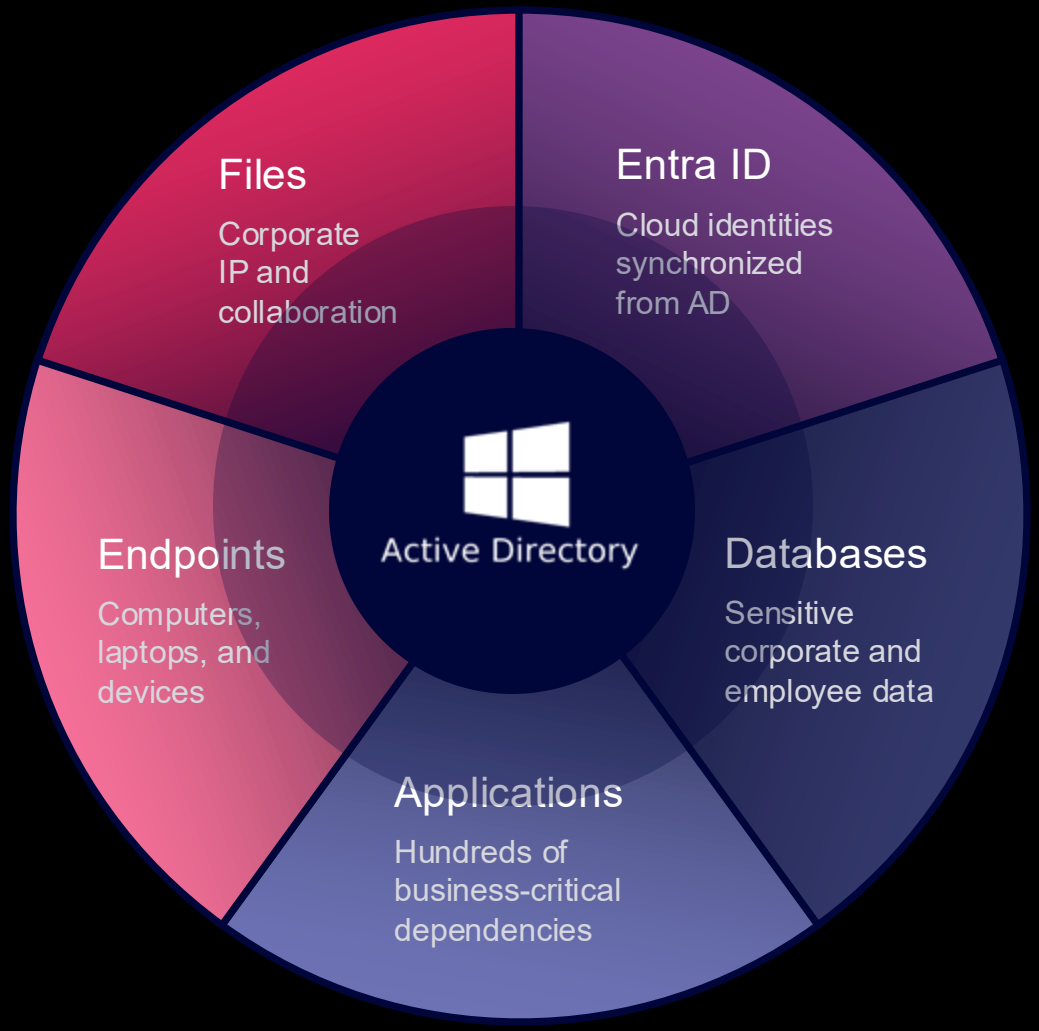


Workload portability



Commvault

Protect the Heart of Your Business



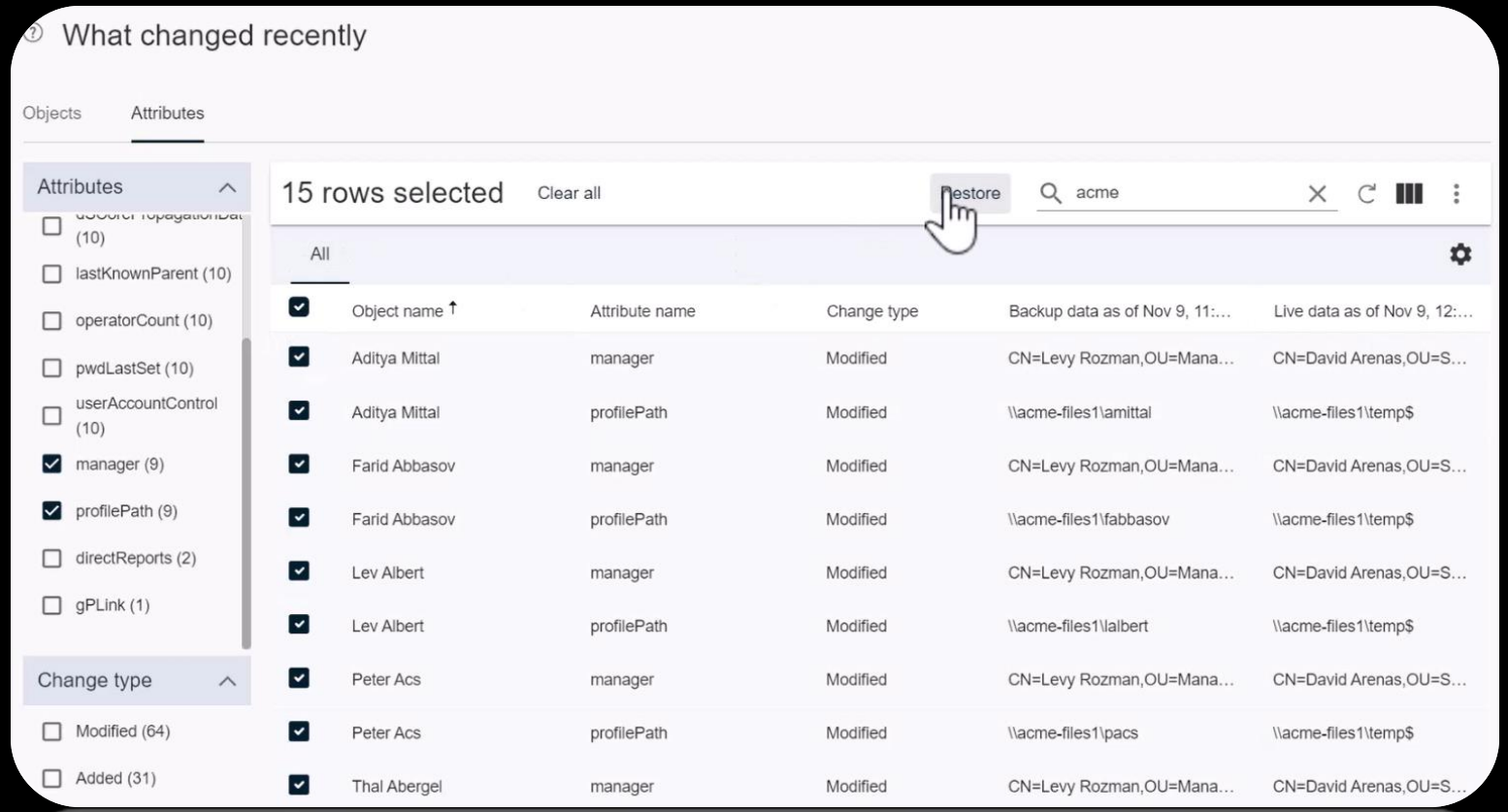
Active Directory holds the keys to the kingdom.

- AD provides identity and access control for mission-critical systems and apps which makes it a **critical first step in cyber recovery**
- Active Directory controls access to critical applications and data, with an estimated **90% of attacks involving AD**.
- In an ethical hacking survey, 56% of respondents report being able to gain access to their targets by **escalating privileges or via lateral movement in 5 hours or less after initial intrusion**.

Interactive, domain-wide comparisons

Poorly written PowerShell scripts and application upgrades gone wrong could unexpectedly overwrite attribute data across hundreds of objects throughout your directory

Quickly locate mass attribute overwrites, establish scope and rollback data to its last good state directly from the report



Commvault

Automated forest recovery for AD

Get back to business in hours rather than days or weeks.

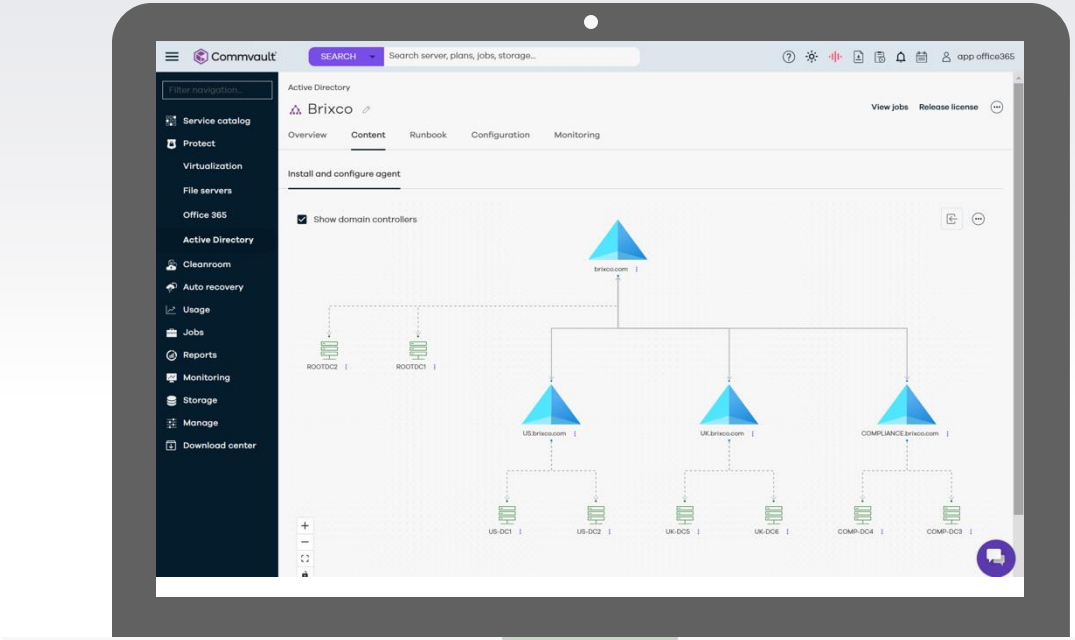
Automate the entire forest recovery process

Simplify recovery planning and testing

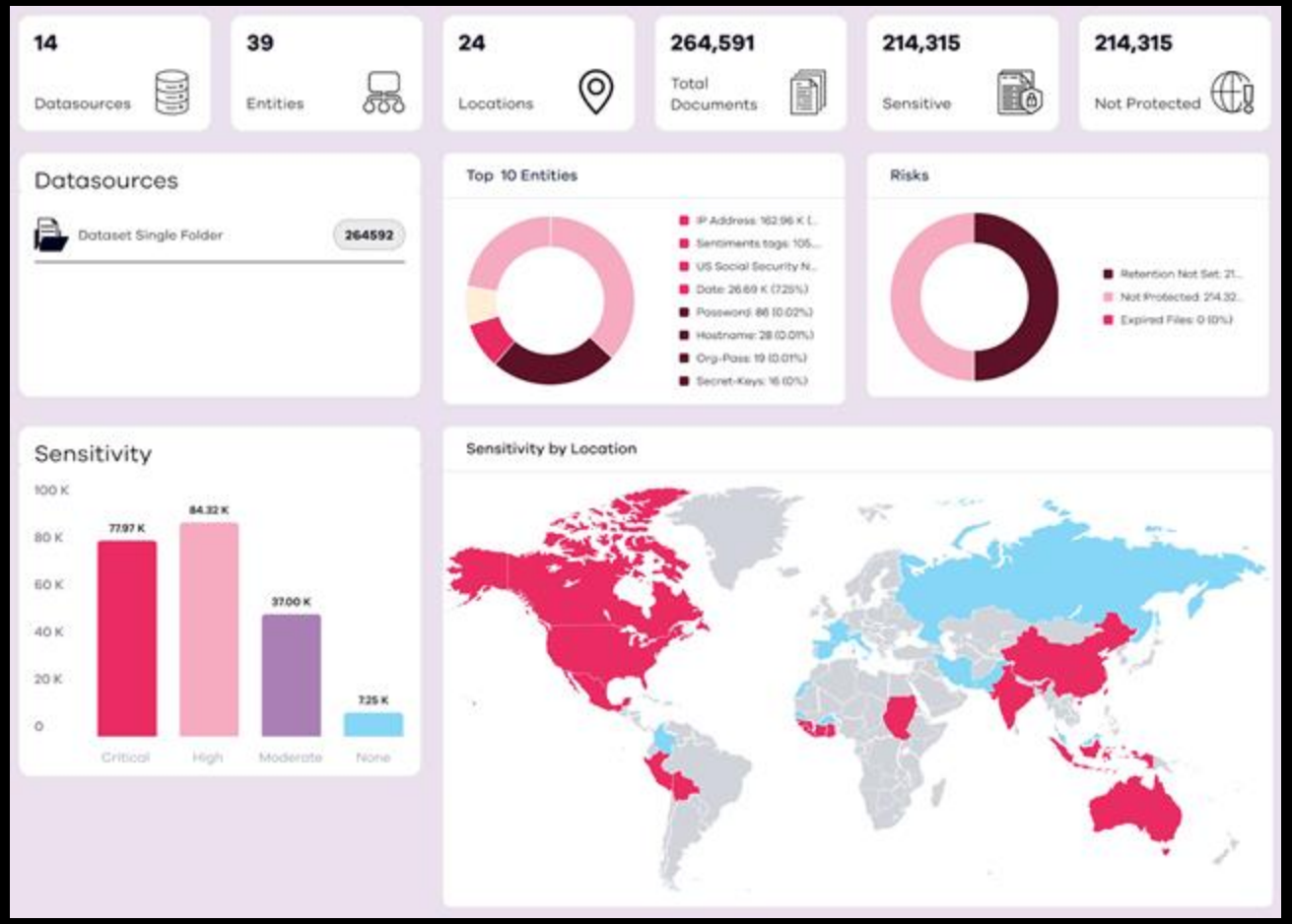
Accelerate recovery times and advance resilience

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**



Discover, classify, and protect sensitive data

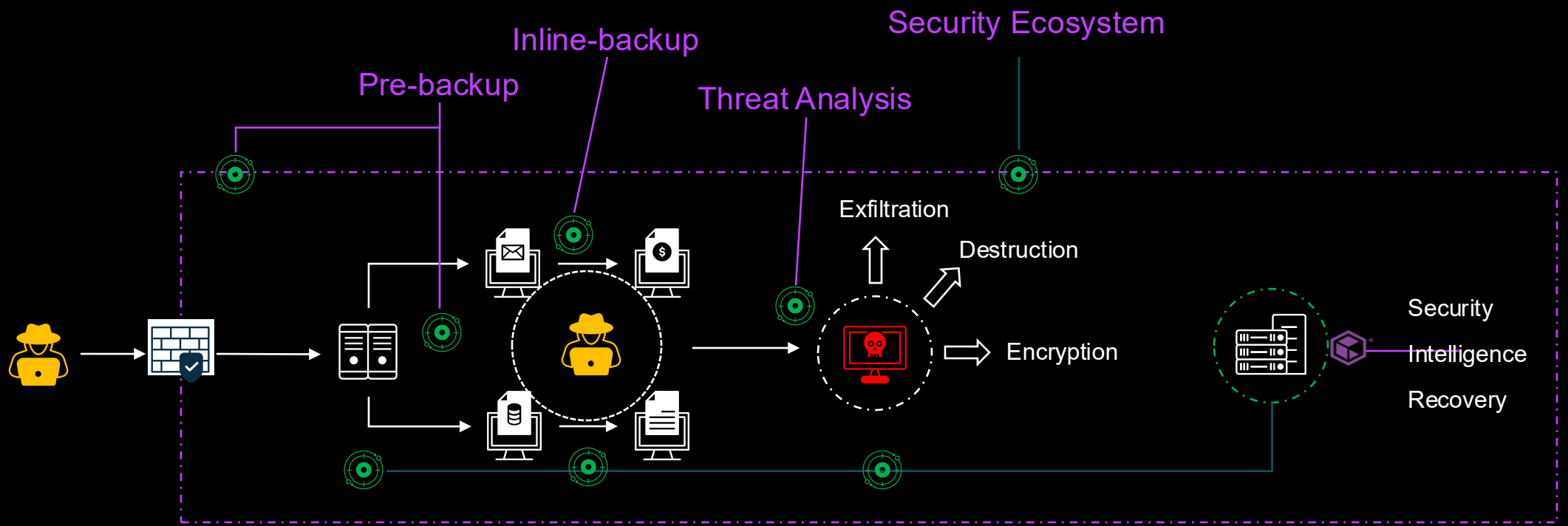


identify and categorize sensitive data

deep understanding of data access

Identify and remove ROT data to reduce costs

Protecting the backup environment for clean recovery



Proactive Monitoring	Inline Monitoring	Threat Analysis	Security Ecosystem
✓ ThreatWise	✓ File Activity	✓ Threat Scan	✓ SIEM/SOAR
✓ Risk Analysis	✓ File Type	✓ Risk Analysis	✓ Threat intelligence
✓ Canary Files*	✓ Backup Size*	✓ Data Verification	✓ EDR/XDR/NDR
✓ Live Anomaly	✓ Extensions*	✓ Auto/Clean Recovery	✓ DSPM/CSPM
	✓ Operational		

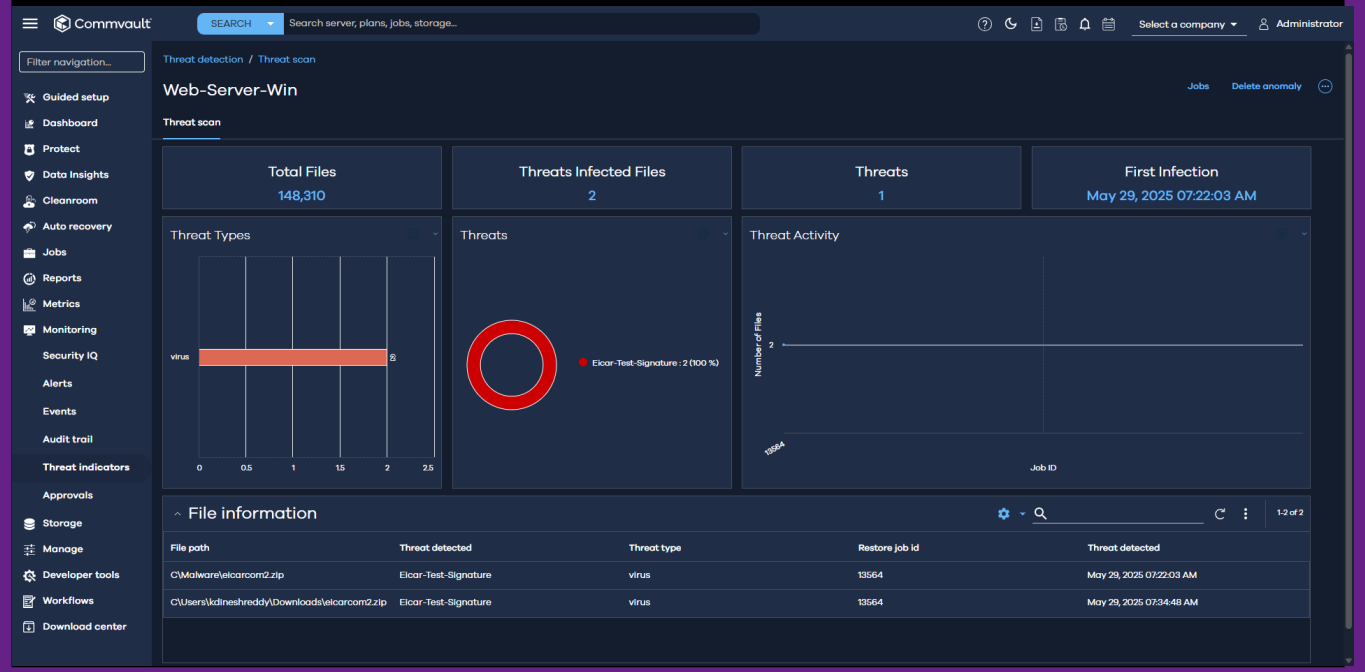
Commvault

Threat Intelligence Dashboard

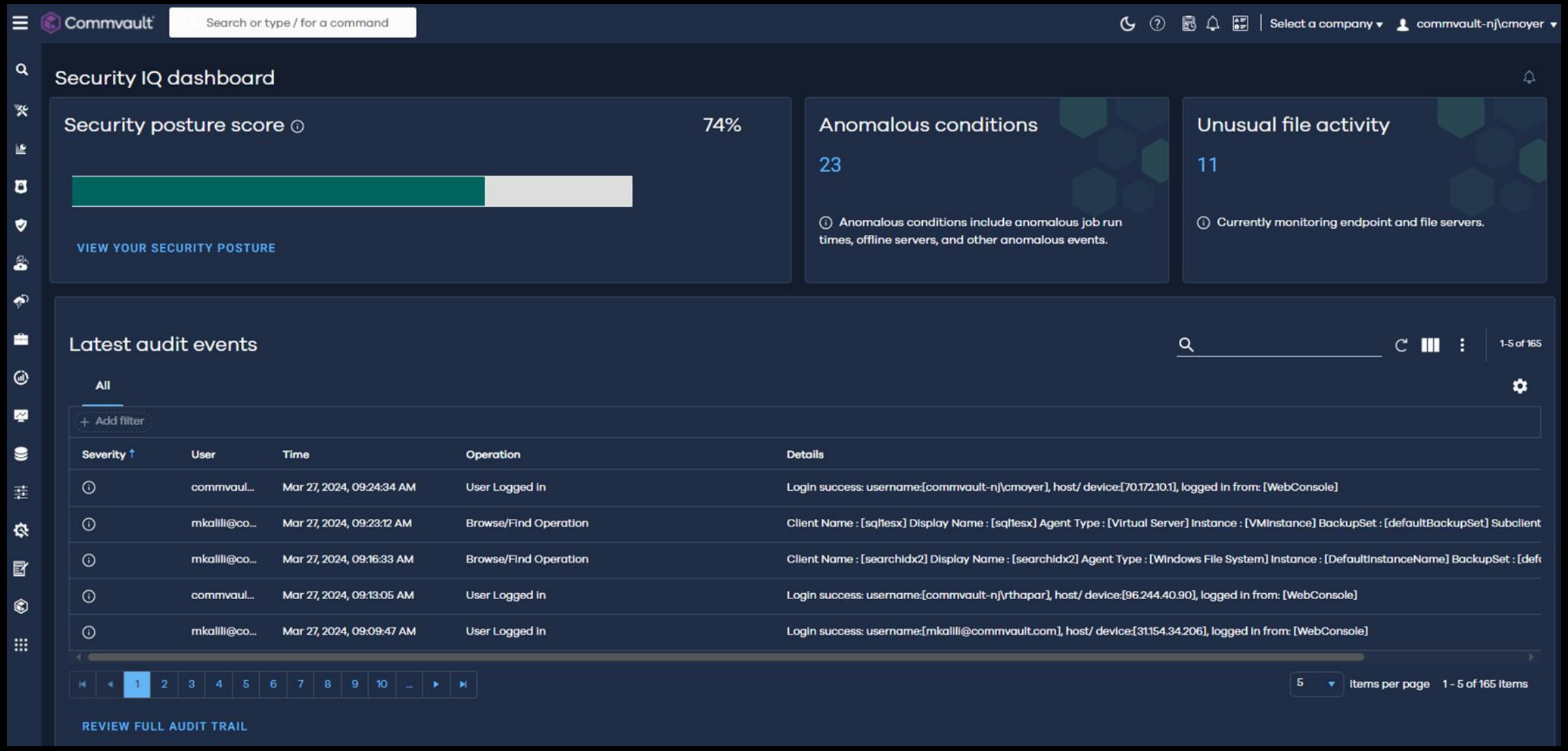
- Automated discovery
- Automated remediation policies
- Smart actions enabled by AI
- Seamless scalability

Suspicious Files

Detected Malware



Security IQ Dashboard

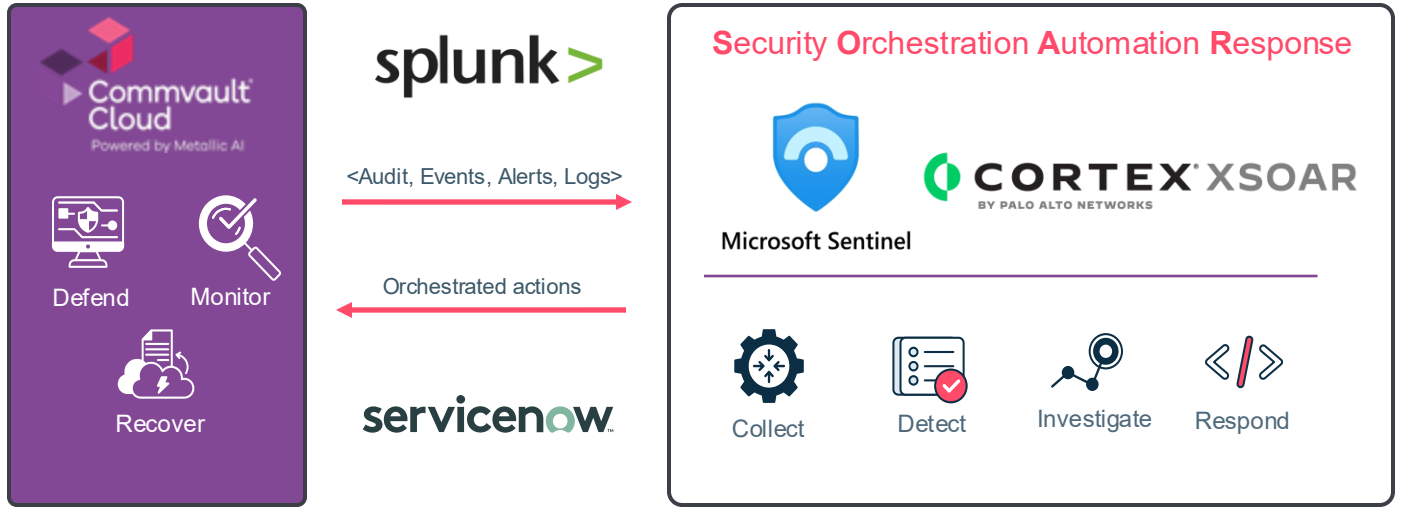


Commvault SIEM / SOAR Integrations

Send Audit trail, events, alerts, and logs into your favorite SIEM using Syslog, Integrated plugins or API's

Security Integrations

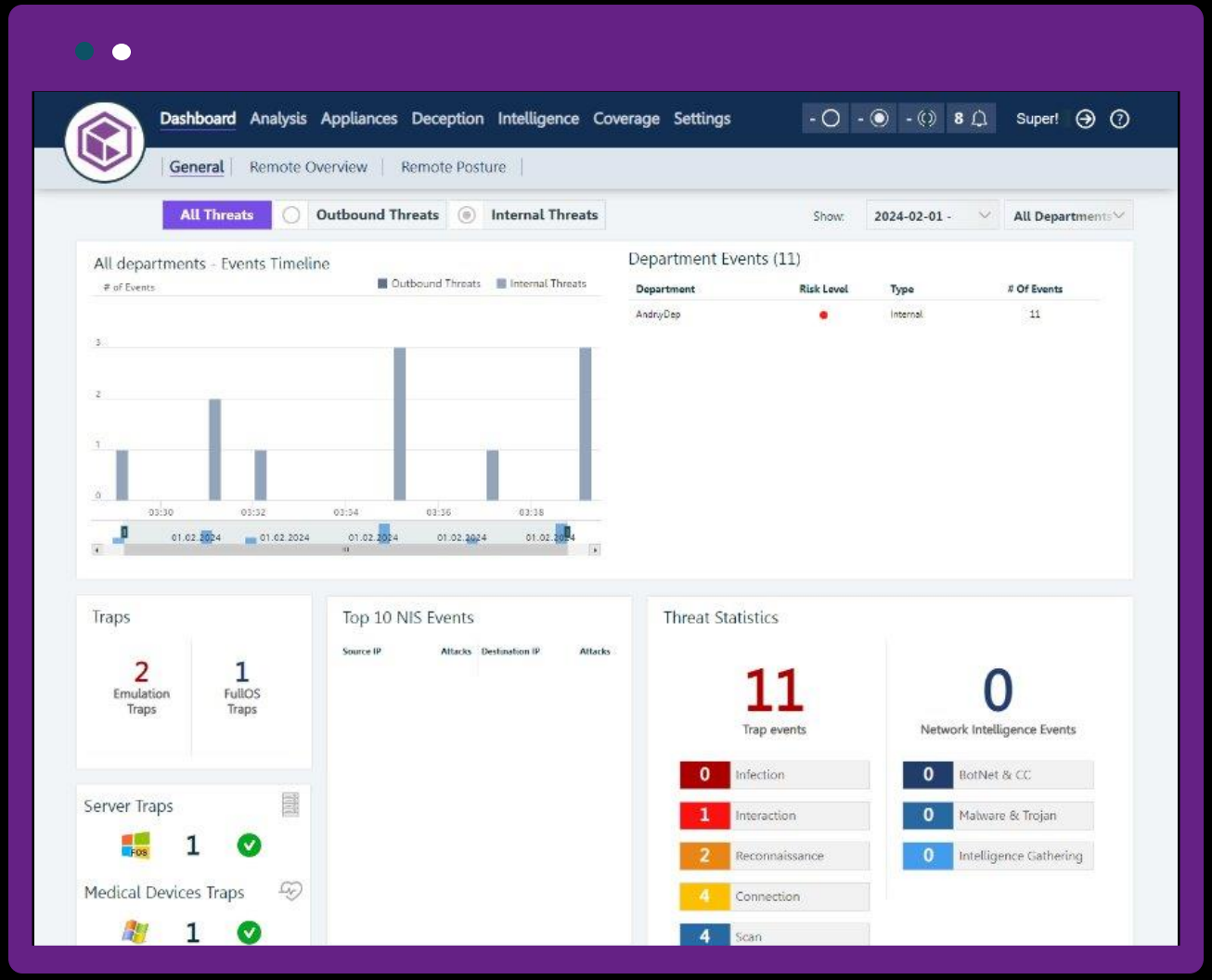
- Out-of-the-box SIEM and SOAR integration
- ServiceNow integration for automated ticket management.
- Automated change control with multi-person authorization flows
- Bi-directional orchestration and audit



ENTRUST · Azure Sentinel · CYBERARK · splunk> · DARKTRACE · netskope · paloalto

ThreatWise Early Warning

- Intelligent decoys
- Precise alerts to pinpoint threats
- Security tooling integrations
- Seamless scalability

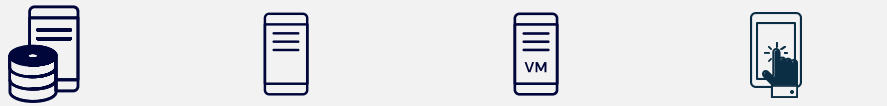


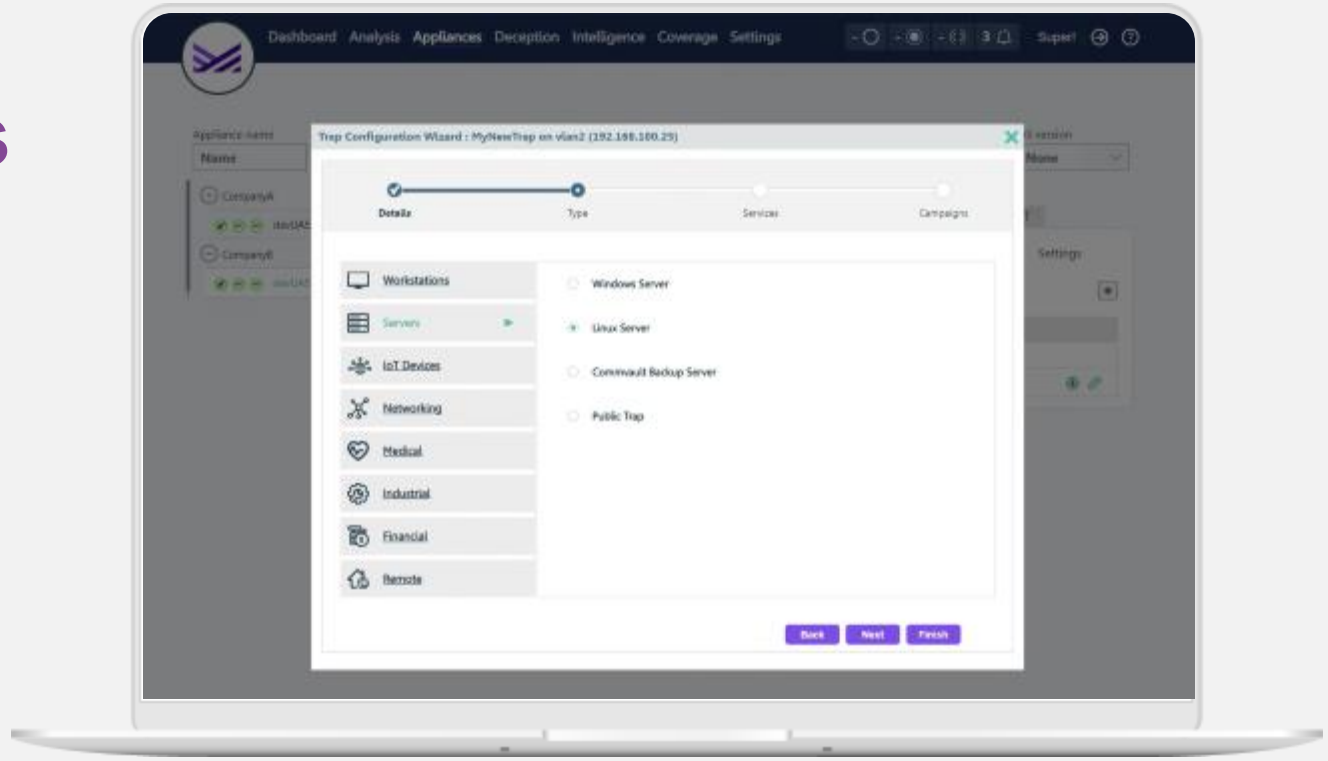
Threatwise: Threat Sensors

Lightweight, Authentic Decoys

Medium interaction decoys that replicate network assets

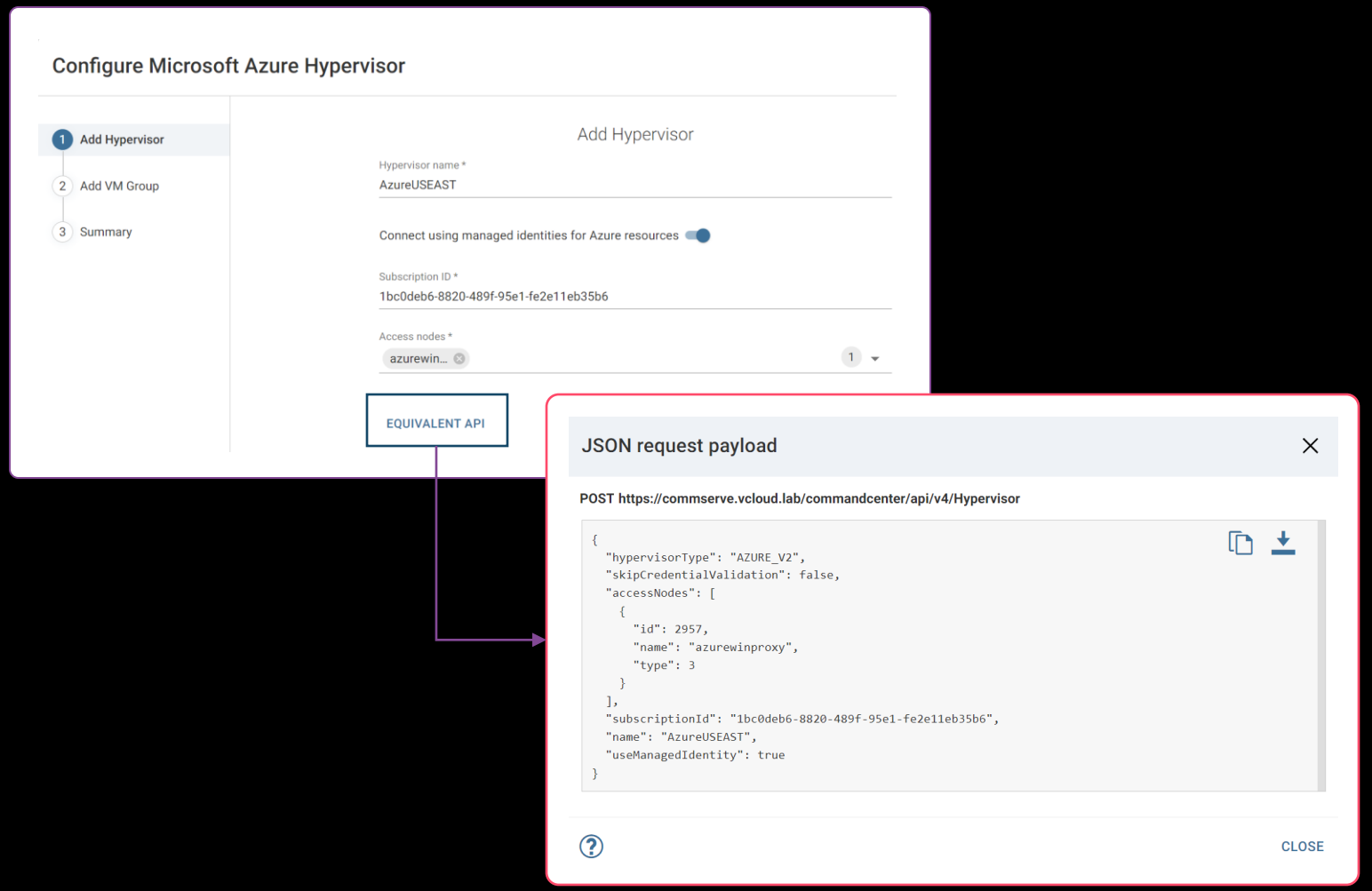
- Recommended decoy placement
- Rapid, wizard-based deployment
- Easy scalable via Mass Deployment
- Seamlessly customizable and blend-in
- Up to 512 sensors per appliance





Simplifying Automation With API

- Equivalent API button accelerates adoption of APIs by providing the exact “Verb” “Endpoint” and JSON body
- Quickly onboard workloads across the platform leveraging the Metallic API gateway
- Industry standard “Bearer token” authorization
- No compromises when it comes to securing the API

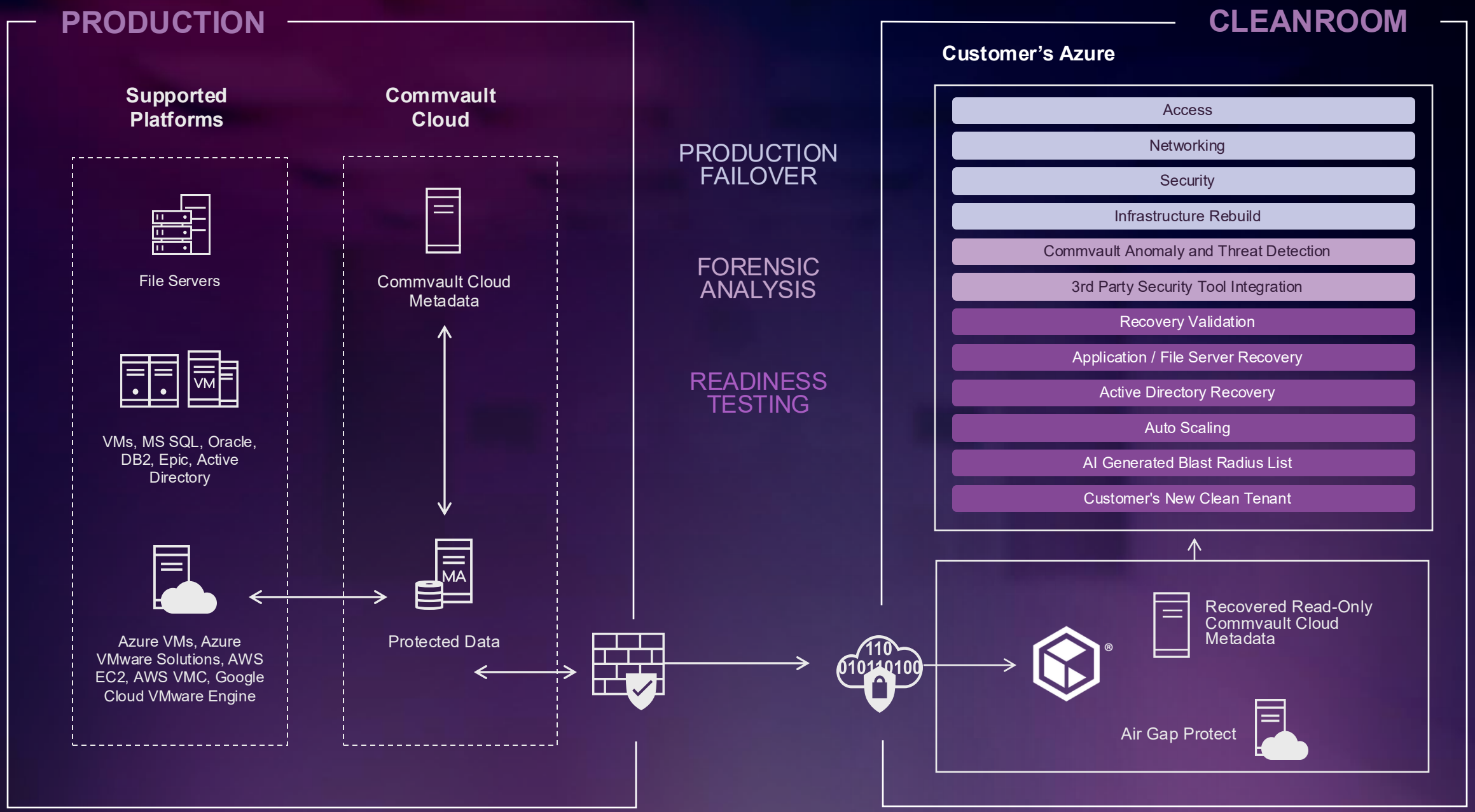


CYBER RESILIENCE

Commvault Cloud
Powered by Metallic AI

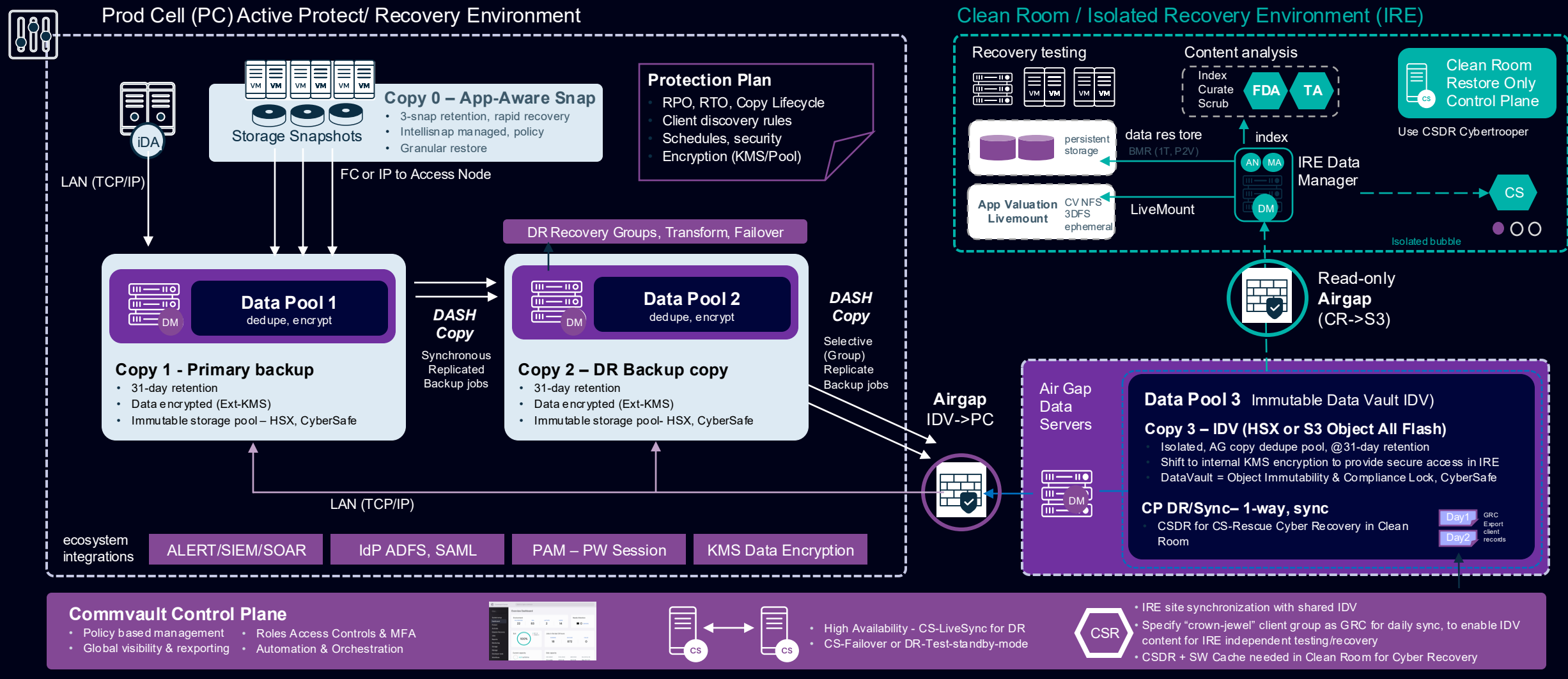
CLOUD CLEANROOM RECOVERY

Commvault


PRODUCTION
Supported Platforms
Commvault Cloud
File Servers
VMs, MS SQL, Oracle, DB2, Epic, Active Directory
Azure VMs, Azure VMware Solutions, AWS EC2, AWS VMC, Google Cloud VMware Engine
Commvault Cloud Metadata
MA
Protected Data
PRODUCTION FAILOVER
FORENSIC ANALYSIS
READINESS TESTING
CLEANROOM
Customer's Azure
Access
Networking
Security
Infrastructure Rebuild
Commvault Anomaly and Threat Detection
3rd Party Security Tool Integration
Recovery Validation
Application / File Server Recovery
Active Directory Recovery
Auto Scaling
AI Generated Blast Radius List
Customer's New Clean Tenant
Recovered Read-Only Commvault Cloud Metadata
Air Gap Protect

On-premises (IRE)–High-level Whiteboard

Design Pattern: Gartner-Configuration **A**, Isolated Recovery Environment with Immutable Data Vault



DM = Data Manger (MA/DedupeStore/roles)

Thank You

Commvault