"Fortifying the Future: AI-Powered Data Security, Recovery, and Compliance in the Age of Cyber Threats"

Ian Malish – Senior Sales Engineer

March 2025

The World Has Changed. And it'll keep changing

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

Design Principles

One solution. Complete resilience.

Hybrid enterprises need a single, unified view for absolute resilience.

Across everything.

Built-in. Not bolted on.

Data security and cyber recovery must be integrated. A single policy engine. Consistent control.

AI is pervasive and persistent.

AI integration should be deep and hardwired throughout to drive automation, speed, scale, and reliability.

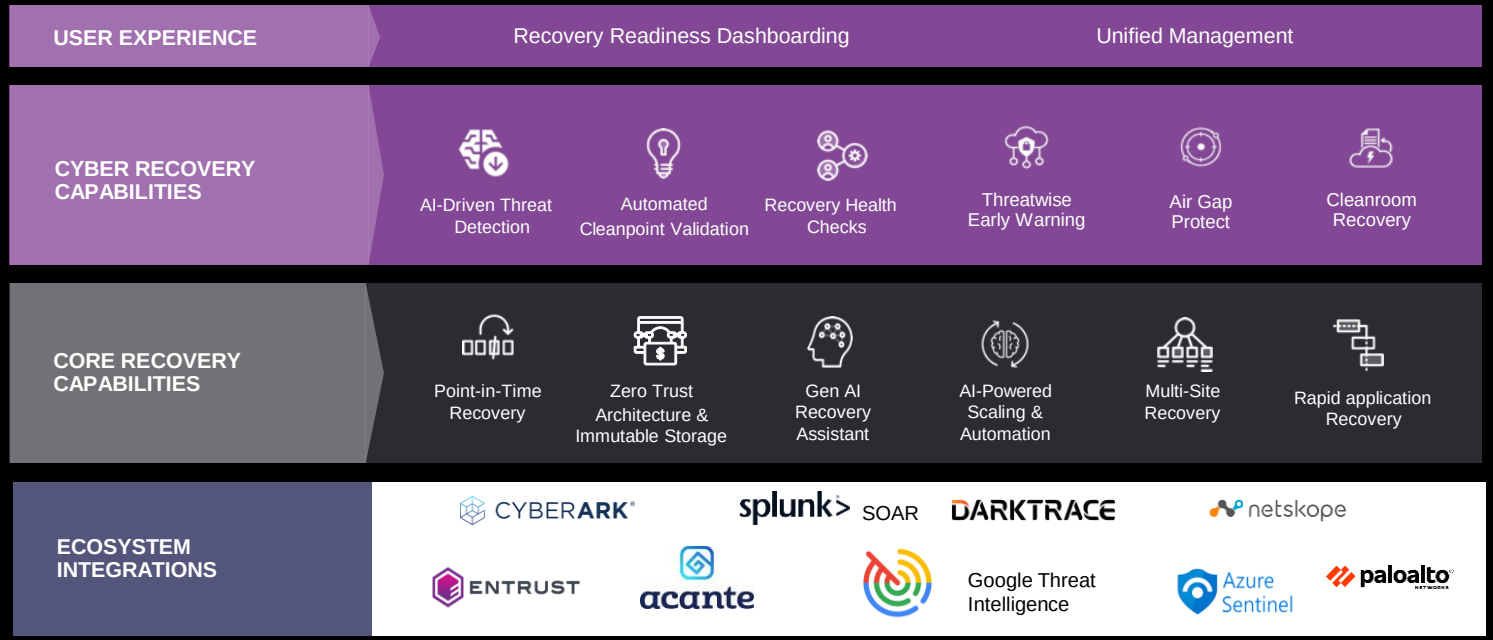
Immutability

Immutable storage

One if not two copies for On-prem and Cloud.

Cyber Resilence Platform

Deliver total cyber resilience from a central, cloud-based control plane—no matter where your data lives.



AI Scenarios

- ✓ Generative AI
- ✓ Emergent AI
- ✓ Machine Learning (ML)
- ✓ Natural Language Processing (NLP)
- ✓ Heuristics
- ✓ Intelligent Automation

Custom Walk-throughs & Documentation Search

Predictive forecasting

File anomaly detection

File entropy

Backup anomaly detection

Real-time insights into operational failures

Generate code with APIs in seconds

Contextual learning for sensitive data classification

Email classification for eDiscovery

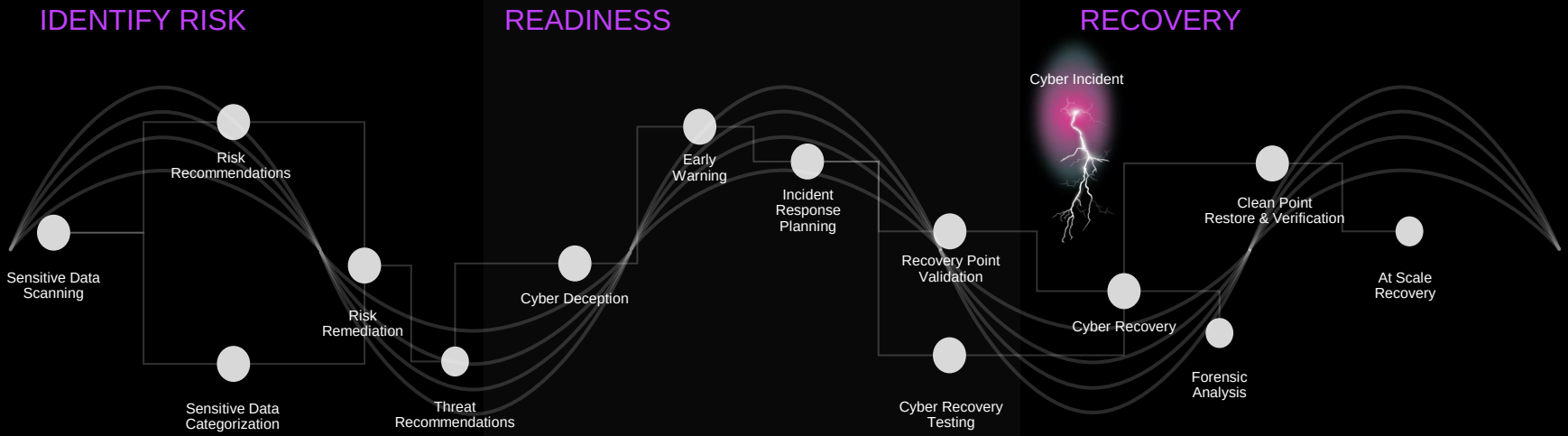
Entity search bar

Cognitive search

Proactive notification

Generative AI-powered Troubleshooting

Getting Resilient



Zero Trust Access

MFA | Multi Person Auth | SAML | PAM | RBAC | KMIP | YubiKey | MS Auth | Google Auth

Palo Alto | MS Sentinel | Dark Trace | Netskope | CyberArk | Entrust | ServiceNow

Risk Analysis

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

Early Warning

- ✓ Cyber deception lures
- ✓ Threat Sensors

Indicators of Compromise

- ✓ Canary Files
- ✓ File hashing
- ✓ Agentless VM CMDR
- ✓ Extension changes
- ✓ MIME Type Mismatch
- ✓ File Entropy Detection

Immutable Storage

- ✓ Object
- ✓ Appliance
- ✓ Cloud
- ✓ Secure NAS

ThreatScan AI

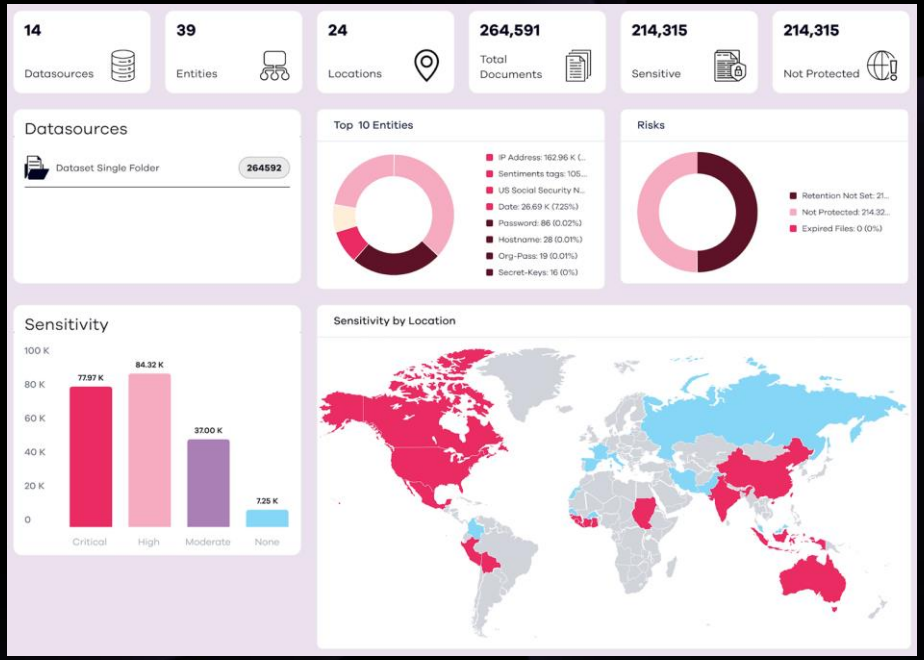
- ✓ Quarantine suspicious files
- ✓ Pre-view Corrupt file versions SIM Hash
- ✓ Signature Based scan
- ✓ AI Zero Day Scan

Isolated Recovery

- ✓ On-premise IRE
- ✓ Cloud IRE
- ✓ Forensics
- ✓ Validate Recovery Points

Risk Analysis

DISCOVER, CLASSIFY, AND PROTECT SENSITIVE M365 DATA

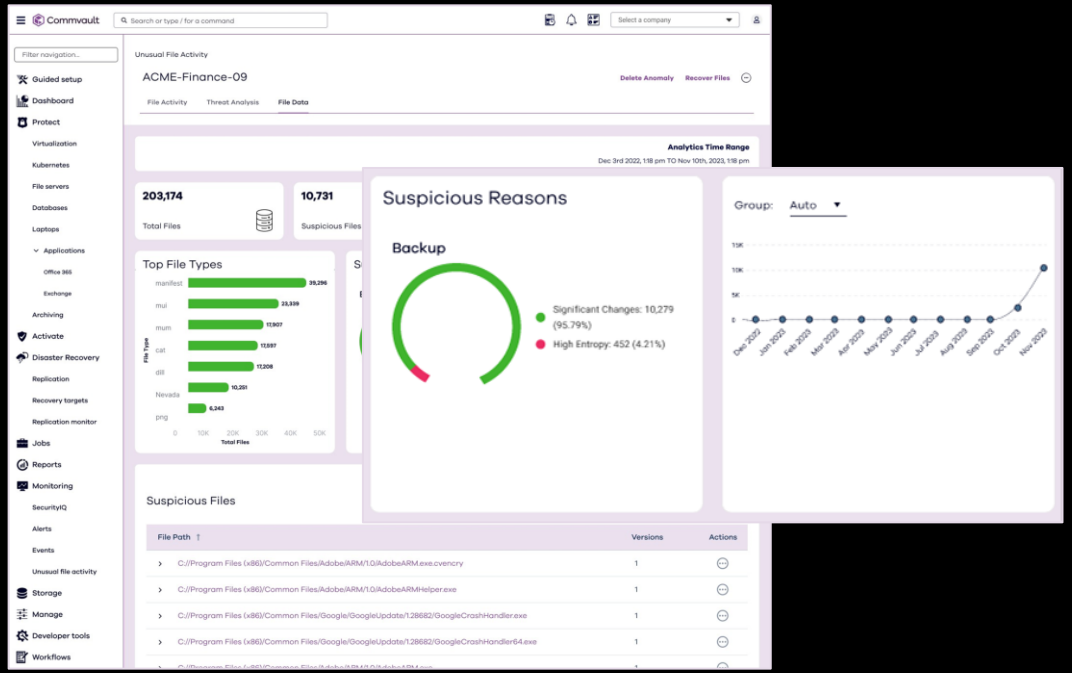


Proactive defense against data breaches and help ensure compliance

Get a complete picture of data risks to respond to security events faster

Reduce costs by removing ROT 365 data

Detect threats and unusual activity

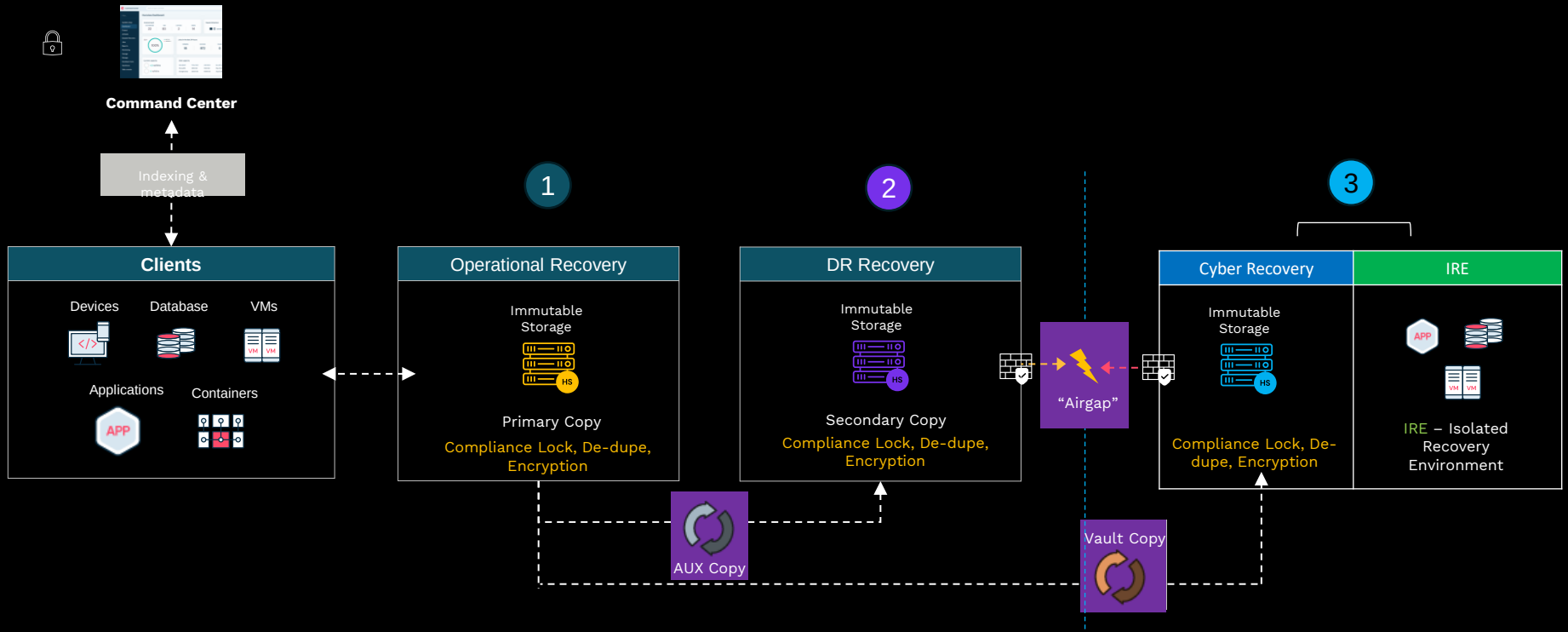


Identify threats within backups so only clean data is recovered

Gain insights that can help drive informative actions

Improve recovery scenarios by reducing post-recovery processes and guesswork

Data Isolation Flow



Compliancy

Cybersecurity

NIS

NIS2

Cybersecurity Act

Digital Operational Resilience Act (DORA)

Critical Entities Resilience Directive (CER)

Cyber Resilience Act (CRA)

Data & Privacy

GDPR

Regulation on free flow of non-personal data

European Data Act

Data Governance Act

Interoperable Europe Act

AI & Other

AI Act

AI Liability Directive

Digital Services Act

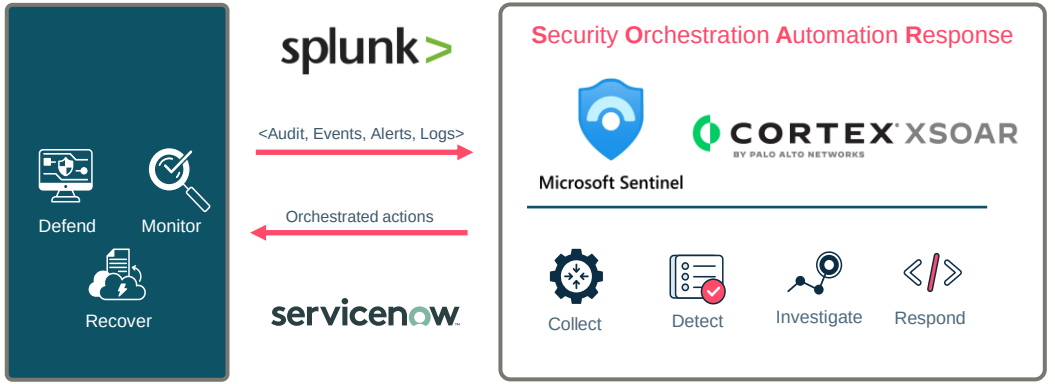
Digital Markets Act

NYCRR500

Security Integrations

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

- 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> SOAR · DARKTRACE · netskope · paloalto NETWORKS · DASERA DATA SECURITY ERA · acante · Google Threat Intelligence

Thank you!