Data Protection and It's Role in Modern Security and Cyber Response Strategies

OCT 2023

Vidya Shankaran (vshankaran@commvault.com)

Field CTO, Commvault

Business Data Is Everywhere

Organizations are rapidly modernizing but still have workloads from prior generations across mixed environments that increase the attack surface. This makes managing, protecting, and using data increasingly difficult.

ON-PREMISE

PUBLIC/PRIVATE CLOUD

SAAS APPLICATIONS

END-USER DEVICES

The Balancing Act

Innovation

89%

Organizations report having a **muti-cloud** strategy.

60%

Of all **IT spending** on application software will be **Cloud** related.

Readiness

$1.4M

is the average cost for rectifying a ransomware attack.

1 in 3

Organizations report having successfully been **hit more than once** by a ransomware attack.

Efficiency

35%

Annual **volume of data** growth reported by organizations. Up from 27%

54%

Decision makers rate **IT Cost Optimization** as their biggest challenge.

COMMVAULT

Sources; VDBR 2022, ESG, Gartner, Sophos: The State of Ransomware 2022

Attacks are faster and broader than ever.

What once took months, now takes minutes...and backup and recovery environments are under attack.

Access

Breach and gain foothold

Damage

Execute attacks below the radar, exfiltrating and encrypting data

Disable

Break operational continuity to prevent recovery

ACROSS HYBRID MULTI-CLOUD ENVIRONMENTS





Average breakout times have accelerated to

84 MINUTES

Percentage of attacks targeting backup repositories

93%

Sources: CrowdStrike 2023 Global Threat Report, 2023 Global Report Ransomware Trends

The Data Protection Disconnect

Conventional Approaches Are No Longer Enough

Ward Off Threats

Security Tooling

Fortify and defend perimeter and environments

Perimeter Defenses

Post Event Recovery

Data Protection

Routine backup and post-event recoverability

Last Line of Defense

The Data Protection Disconnect

Conventional Approaches Are No Longer Enough

Cyber threats demand a proactive response plan = Readiness

NIST Cyber Defense Framework:

Security Team

- Access controls (MFA)
- Monitoring (SEIM)
- Patching currency
- Network segmentation
- Prioritized response
- Exercised playbooks

Data Recovery Team

- Recovery automation and metering
- Rogue prevention
- Early warning anomaly detection
- Control zones / air-gap segmentation
- Data store hardening (Immutable Copies)

Incident Response Team

Cyber Insurance Partner

Transforming with Intelligent Data Services

1998 - 2010

Backup & Recovery

Patented no-limits architecture for data protection

2010 - 2019

Data Management Platform

AI/ML intelligence and scale to enable use case and workload expansion

Now & Forward

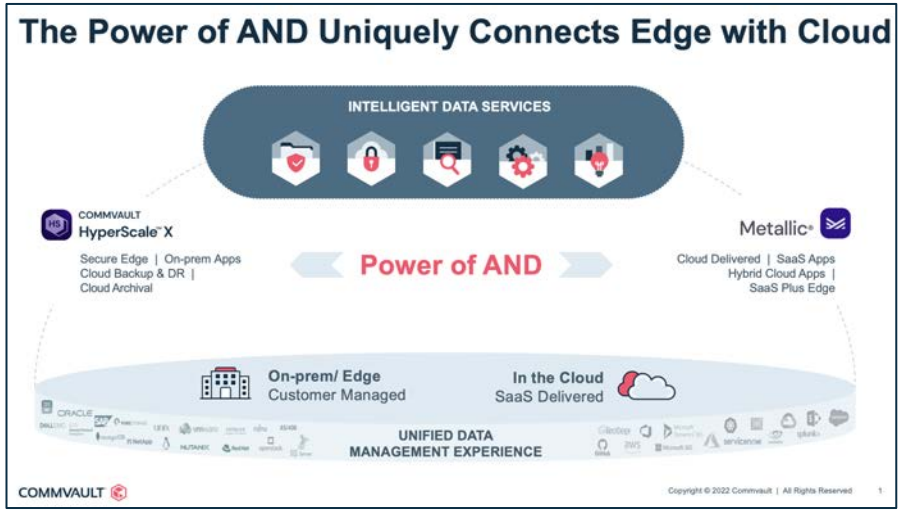
Unified Data Management Services

Intelligent Data Services (Data Protection, Security, Transformation, GRC)

Multi-Cloud, On-Prem and Edge

SaaS, cloud and legacy application workloads

Delivered as Software **and** SaaS



27 years
as a pioneer in data management

12
consecutive years
as Gartner Magic Quadrant leader

>1,000
issued patents

98%
customer support satisfaction

100,000+
organizations rely on Commvault

>3.5+ exabytes
moved to the cloud

>11+ exabyte
data under management

Next-Generation Data Protection From Commvault

Layered protection that actively defends data and its recoverability across production and backup environments

Stay resilient.

Secure

Hardened, zero-trust architecture, with best-in-class protocols.

- Secure data
- Prevent unwanted access
- Maintain integrity

Anticipate threats.

Defend

Early warning, in-depth monitoring, and advanced forensics.

- Limit exposure windows
- Flag attacks
- Increase visibility

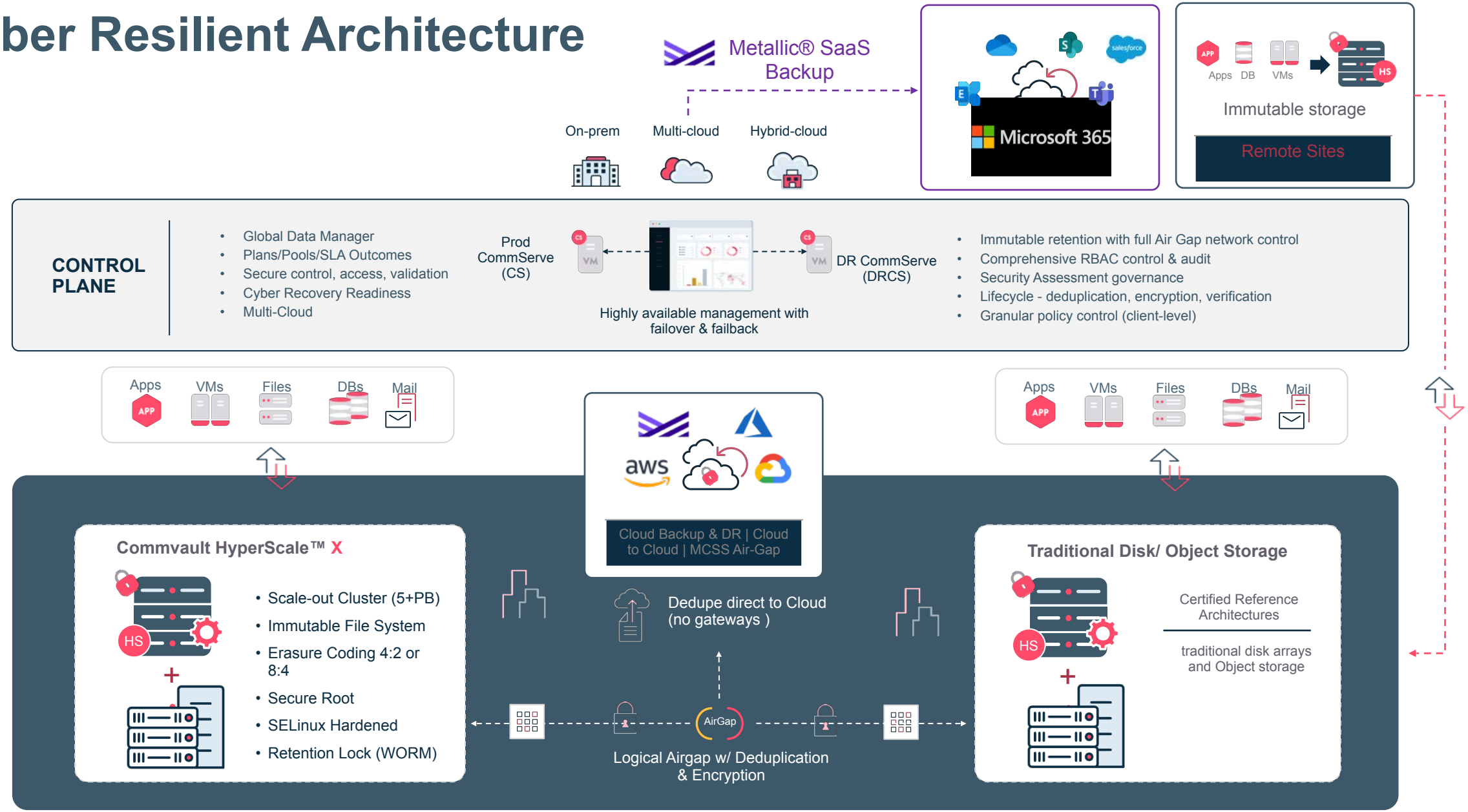
Respond with confidence.

Recover

Rapid recoverability and trusted compliance across data estates.

- Reduce downtime
- Thwart data loss
- Exceed SLAs

Cyber Resilient Architecture

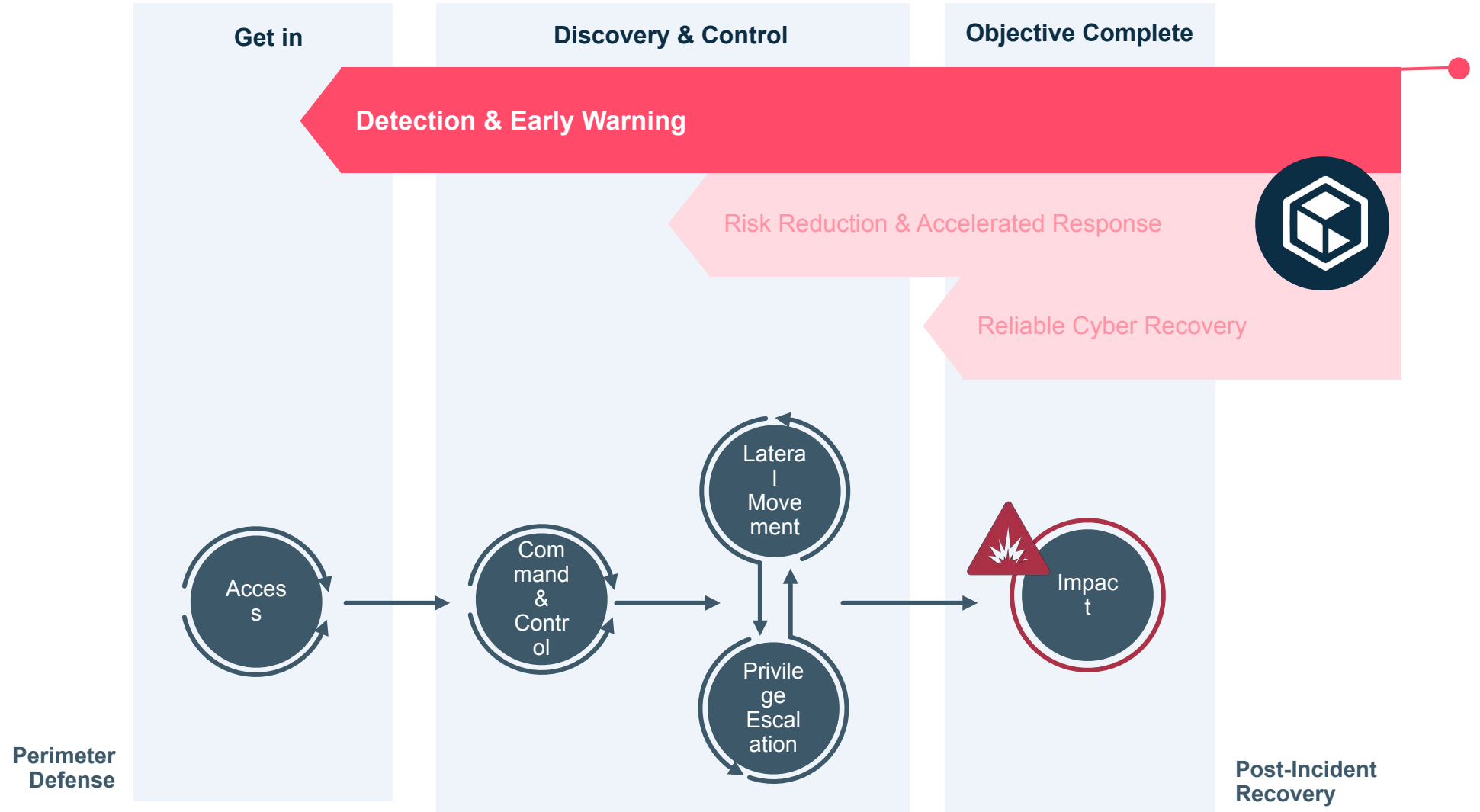


COMMVAULT

Active Defense:

Defending Data from Sophisticated Threats

Shifting Data Protection Left



Only **12% of businesses** have ransomware detection tools that are adequate and equally secure on-prem and cloud environments[1]

Source 1: ESG Research, ThreatWise InstaPoll, Sept 2022

What is “shifting left”?

Commvault!

Everyone else…

Hackers move throughout the environment, seeking weak points, looking for critical systems/data

Regular backups performed to pull in the data for immutable protection

Secondary copies of the data are sent to air-gap cloud / object storage targets for additional resilience

Deception

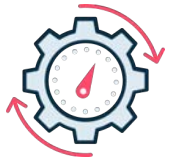
Honeypots

6+ months earlier | Lateral Movement | ATTACK! | Daily Backups | Anomaly Detection | Air-Gap/Vault

Bad actors gain access to the environment, start planting seeds for later intrusion.

After sitting in the background for months, they finally execute the attack and put forth the ransom notices.

Anomaly detection performed against data after protection. Alerts and warnings generated – **incident response begins**



Recovery efforts…

Defending Data Sooner

Alerting threats in production

Uncovering stealth and zero-day attacks

Providing clear and precise signals

Masking backup infrastructure

Metallic ThreatWise

Early Warning Cyber Deception

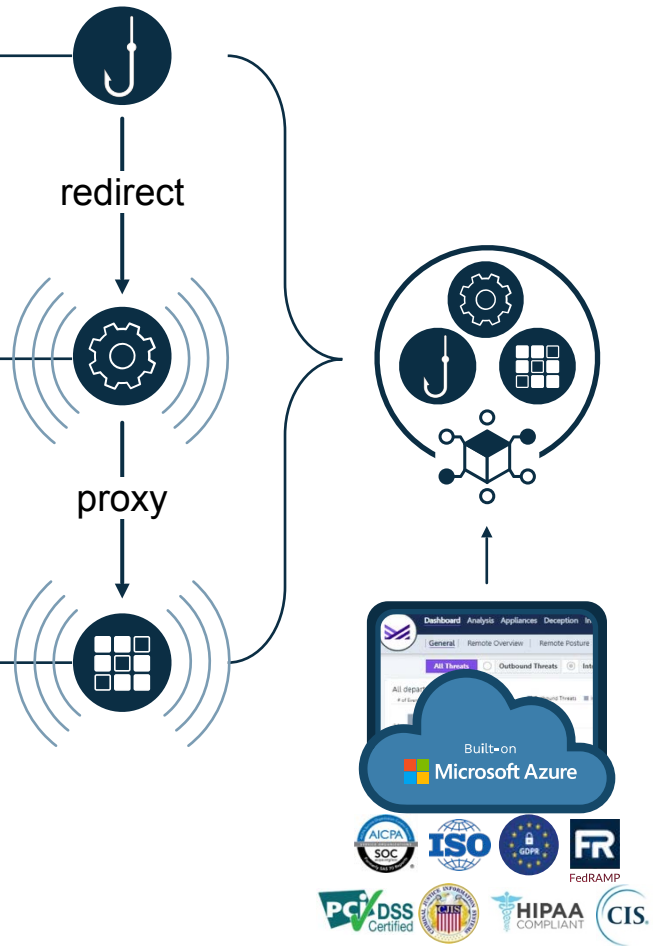
see NIST SP 800-53, Revision 5

Surface zero-day, unknown, and internal threats in production – before they reach your data.

Lures
artifacts that redirect attack toward sensors
- Files, Cached credentials, Bookmarks, etc.
- Unlimited use – no agents

Sensors
microservices of native interactions
- Clone production assets
- Highest scalability and agility

Full System
full interaction decoy
- Unlimited interaction
- Fit for specific use cases



Virtual Appliance / Container
- On-premise, Cloud, IoT and OT
- 100's of Deceptive Assets configured and deployed

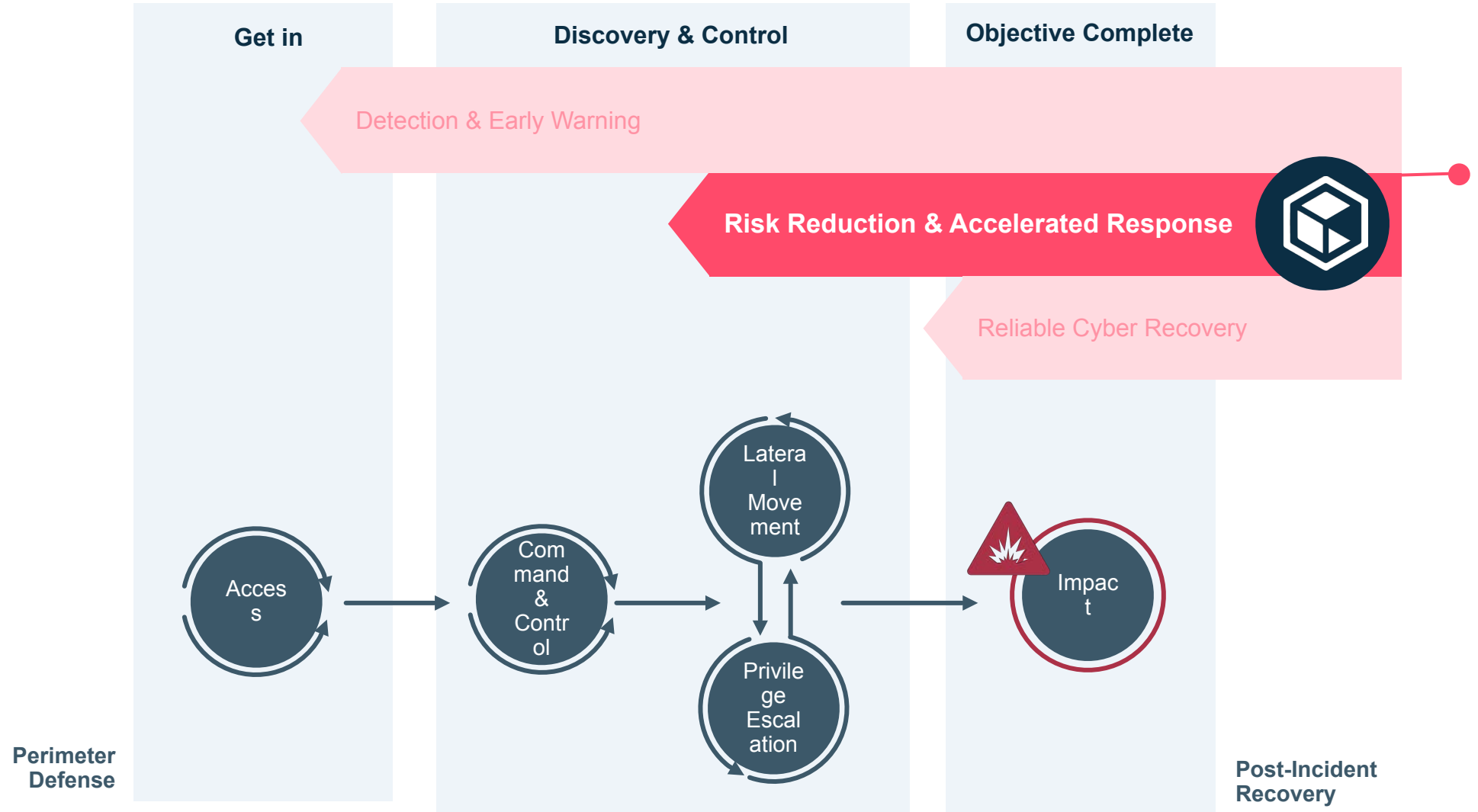
TSOC
ThreatWise Security Operations Console
- Managed and monitored from a secure SaaS environment
- Alerts integrated with SIEM, SMS or Email

1) IBM and Palo Alto 2) Microsoft 3) Splunk

COMMVAULT

Securing Data:
Bridging the Gap Between IT & Security Teams

Shifting Data Protection Left



9 in 10 cyberattacks attempt to disable or compromise backup repositories[1]

Source 1: ESG Research, ThreatWise InstaPoll, Sept 2022

Proactive, Multi-layered Security

Actively defend data and its recoverability

COMMVAULT

Secure-by-Design Architecture

Immutable – Air-Gapped – Zero-Trust

+

Security IQ

Monitor threats & improve security postures

Risk Analysis

Identify anomalies, secure sensitive files, & assign stringent security

Security Integrations

Increase visibility, coordination, & countermeasures

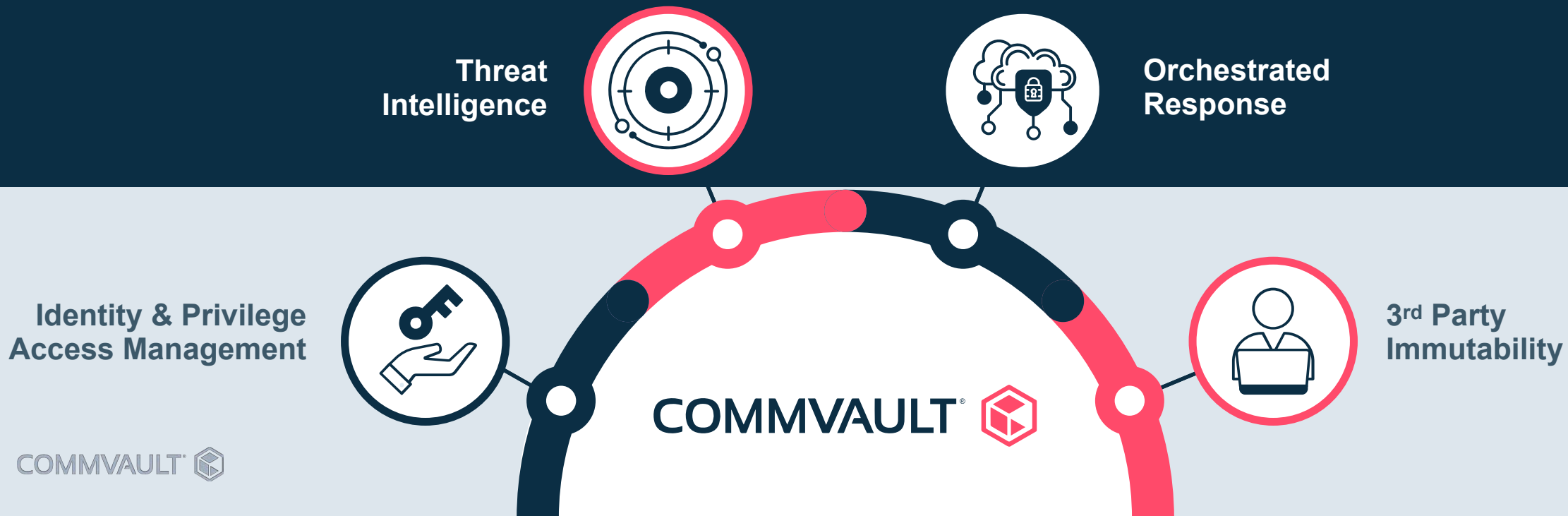
Ecosystem Integrations

Uniquely connecting Data Protection and Security

Improved Security
Hardened security through enhanced platform resiliency

Better Collaboration
Increased visibility through correlated and shared insights

Faster Incident Response
Improved event handling through automated countermeasures

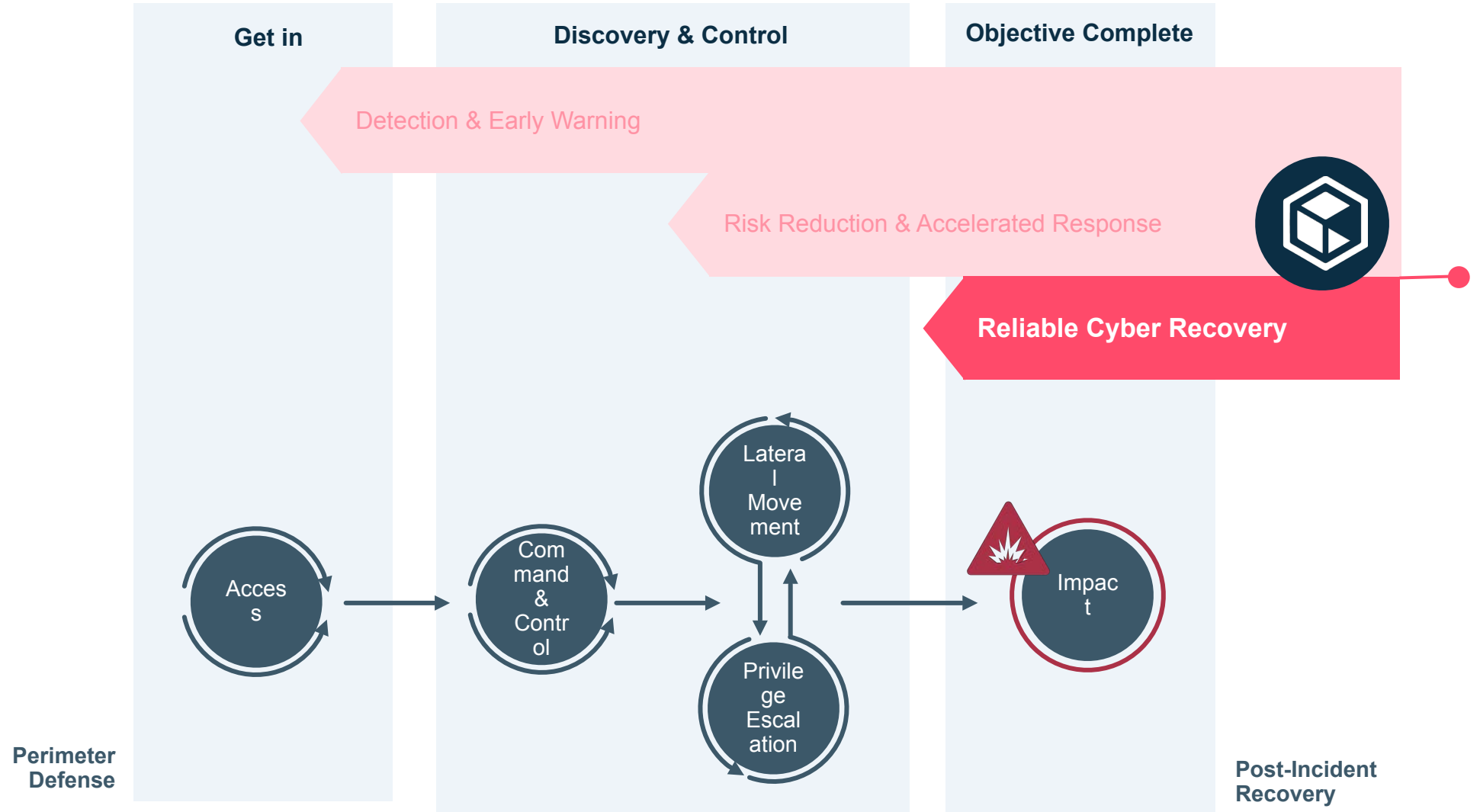


COMMVAULT

Cyber Recovery:

Eliminating Downtime while Keeping Data Clean

Shifting Data Protection Left



As cybercrime rises, **less than 23% of businesses** are confident in their ability to recover data[1]

Source 1: ESG Research, ThreatWise InstaPoll, Sept 2022

Threat Behavior Overview

Business Issue: As threats remain dormant for days at a time, backups are continuous. Files may contain infection prior to backup, causing a false sense of safety and impact to recoveries.

Cyber threats challenge **data integrity, compliance,** and **cost.**

Is my data clean?

Can I recover fast?

Preventing Reinfection ⟷ **Driving Business Continuity**

COMMVAULT

Commvault Threat Scan

Commvault Threat Scan optimizes and simplifies ransomware recovery objectives, by helping organizations recover uninfected versions of backup data, and eliminating the risk of reinfecting recovery targets with malware

1

Identify

Identify threats within backups so only clean data is recovered

2

Deliver Insights

Provides insights that can help drive informative actions

3

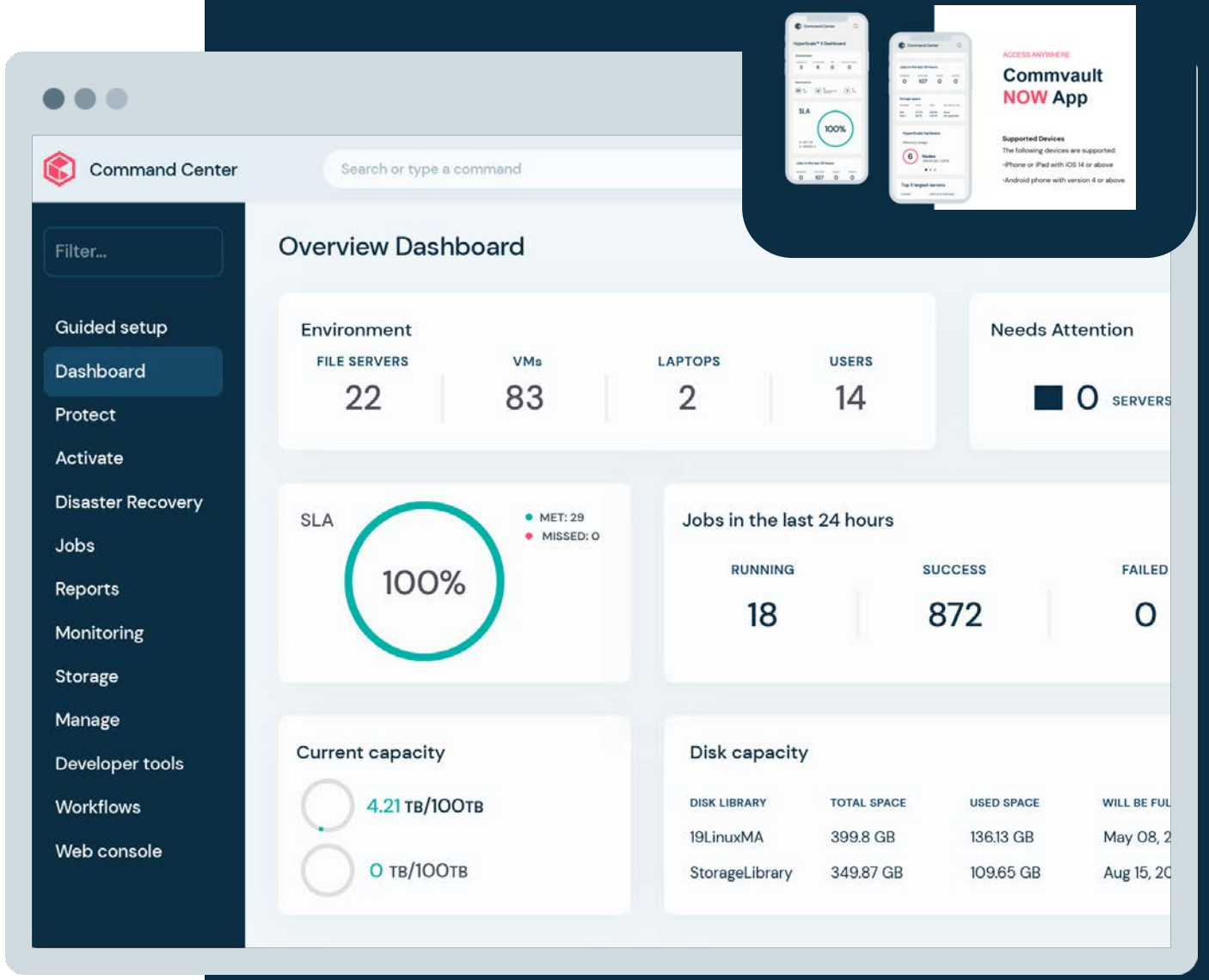
Clean Recovery

Improves recovery scenarios by reducing post recovery processes and guess work

- Monitoring risk
- Keeping data clean
- Validating recovery
- Restoring data fast

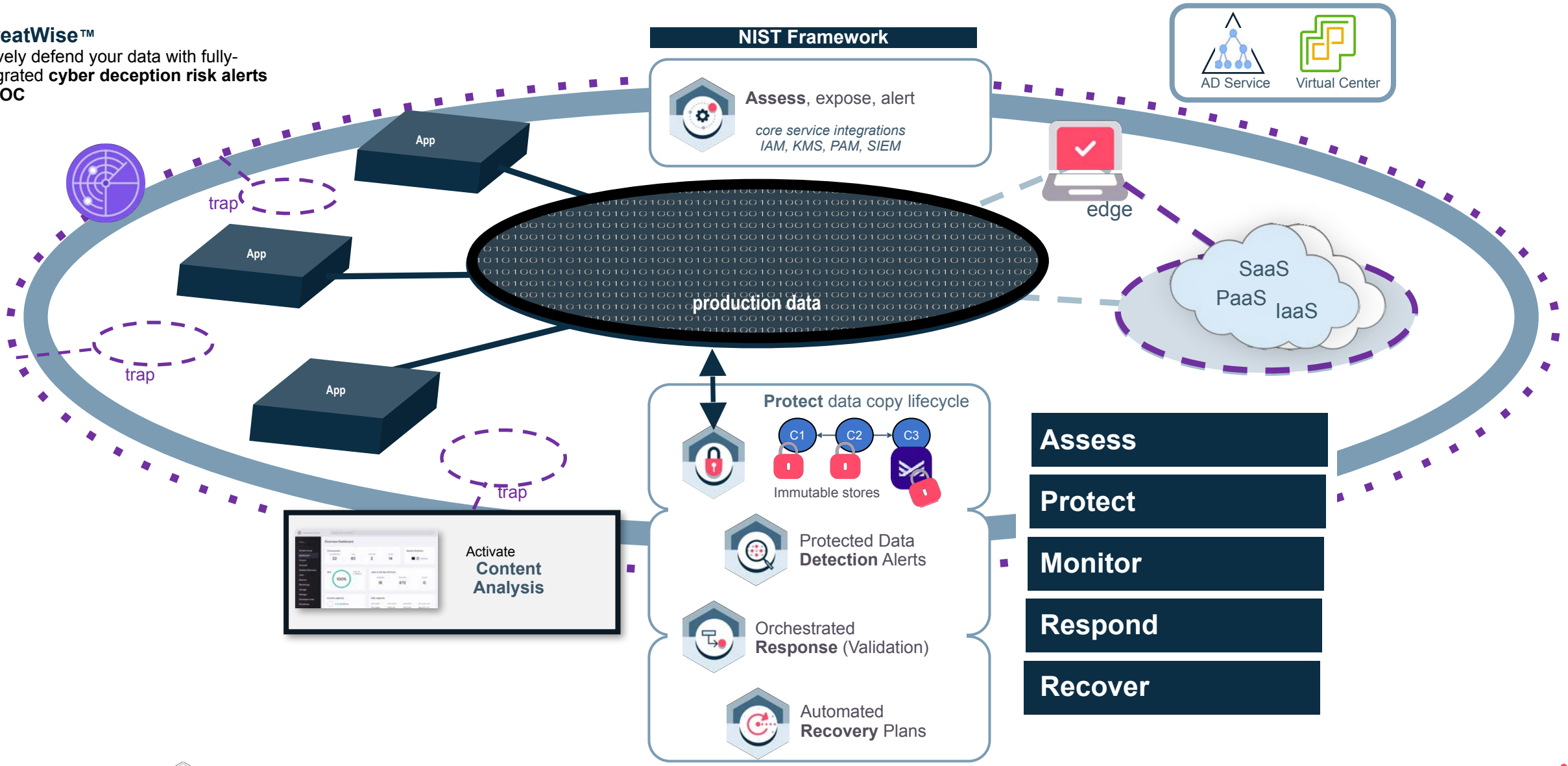
One Experience for Your Entire Data Security Strategy

- **Comprehensive Data Insights:** Commvault reporting provides detailed and comprehensive insights into the organization's data environment, including backup and recovery status, storage utilization, data growth trends, and resource consumption.
- **Customizable Dashboards:** Commvault offers customizable dashboards that allow users to tailor the reporting interface to their specific requirements, providing a clear and concise overview of critical data protection metrics.
- **SLA Compliance Tracking:** Commvault reporting enables users to monitor Service Level Agreement (SLA) compliance, ensuring that backup and recovery operations meet the defined performance and availability targets for critical data.



Commvault Cyber Resiliency Framework

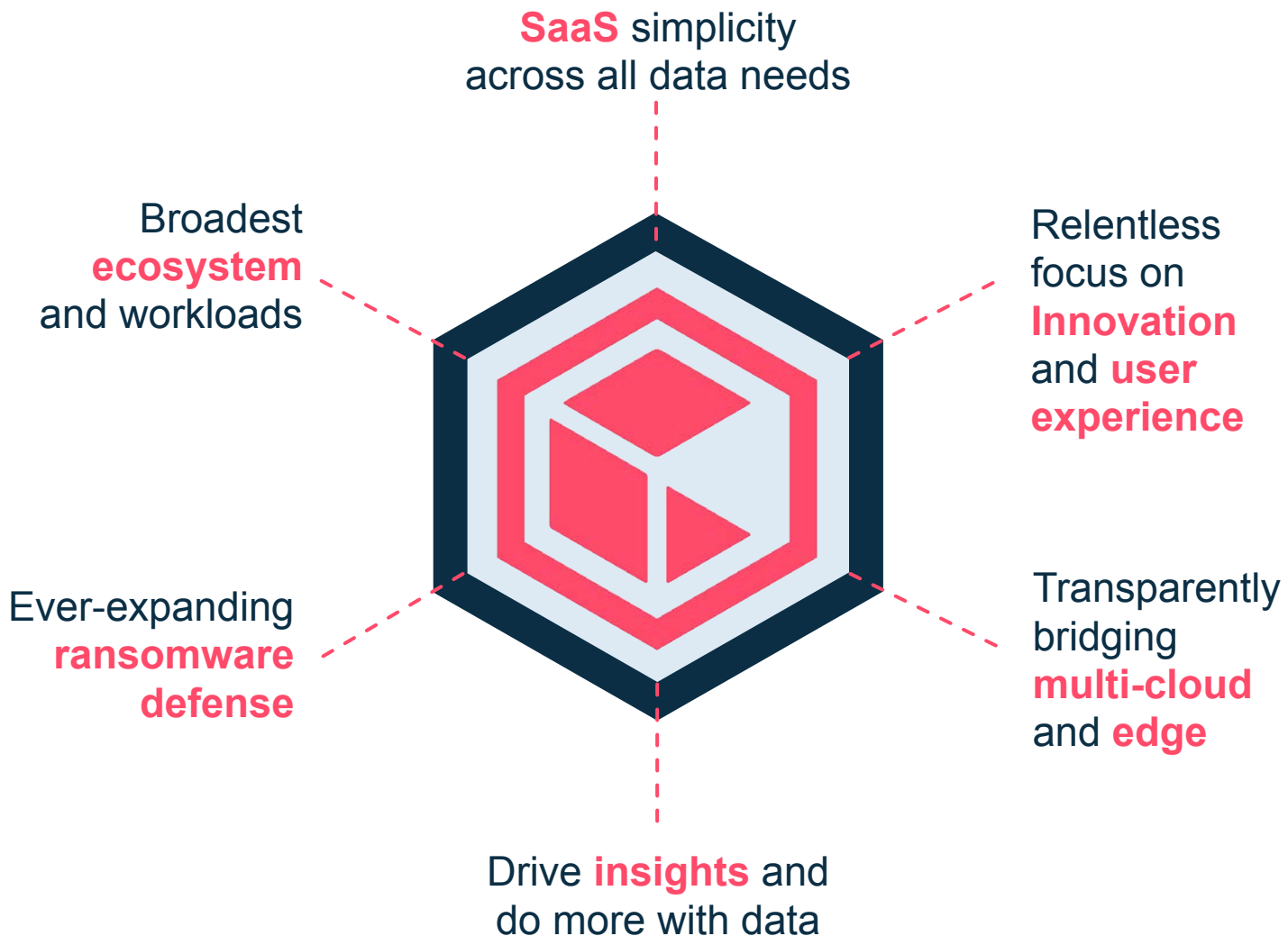
ThreatWise™
Actively defend your data with fully-integrated **cyber deception risk alerts to SOC**



COMMVAULT

Continuous Innovation Roadmap Strategy

SIMPLE AND ELEGANT SOLUTIONS FOR YOUR EXPANDING DATA MANAGEMENT CHALLENGES



Video Demos on YouTube!

COMMVAULT

1. **Commvault: Threat Scan**
   - A demonstration of Commvault® Threat Scan, technology that scans backups for malware and other nefarious changes. The session simulates a ransomware attack, shows how to analyze the backup content, and demonstrates a clean recovery of data.

2. **Commvault: Risk Analysis**
   - This session covers Commvault® Risk Analysis and how it helps in minimizing risk in the environment. The session focuses on locating sensitive data, identifying overexposed data, and controlling data sprawl.

3. **Commvault: ThreatWise**
   - Ransomware is evolving, targeting critical business data in new ways. As adversaries go beyond encryption, aiming to leak, exfiltrate, and steal your data, early threat detection has never been more important for today's organizations. In this demo, we'll show you how Metallic ThreatWise, integrated cyber deception from Commvault, surfaces potential ransomware threats before they reach your data.

COMMVAULT

Thank You