SHIFT

Commvault

CHRISTIAN KUBIK

From Security to Resilience

Manager Field Advisory Services Team, EMEA&I Regions

TODAY’S 3 OBJECTIVES

1. DISCUSS THE PROBLEM OF EXPANDING ATTACK SURFACES

2. EXPLORE THE RELATIONSHIP BETWEEN THESE RISKS AND STATE-OF-THE-ART CYBER RESILIENCE

3. DEMONSTRATE WHY A FOCUS ON CYBER RESILIENCE APPROACH MAKES SENSE

TRADITIONAL VIEW

ATTACK SURFACE

NETWORK INSECURITIES		SOFTWARE BUGS		PHYSICAL SECURITY LOOPHOLES		SOCIAL ENGINEERING-PRONE PEOPLE	
OPEN PORTS	WEAK PROTOCOLS	INSUFFICIENTLY SECURED IN-HOUSE DEVELOPED APPLICATIONS	VULNERABLE COMMERCIAL PROGRAMS (E.G. WORDPRESS)	ROGUE OR DISSATISFIED CURRENT AND FORMER EMPLOYEES	OPENLY DISPLAYED LOGIN CREDENTIALS (E.G., USERNAME-PASSWORD COMBINATION ON STICKY NOTES)	REUSED OR RECYCLED PASSWORDS	UNMONITORED USE OF SOCIAL MEDIA AND UNPROTECTED PERSONAL DEVICES

RIGHT NOW,
IN THE REAL
WORLD…

ATTACK TYPES AND ATTACK SURFACES

RANSOMWARE	PHISHING	DATA EXFILTRATION	SOCIAL ENGINEERING	DDOS
1. CLOUD	2. REMOTE	3. IOT	4. SSC	5. SOCIAL	6. AI

THE STATUS QUO FALLS SHORT

TOOLS

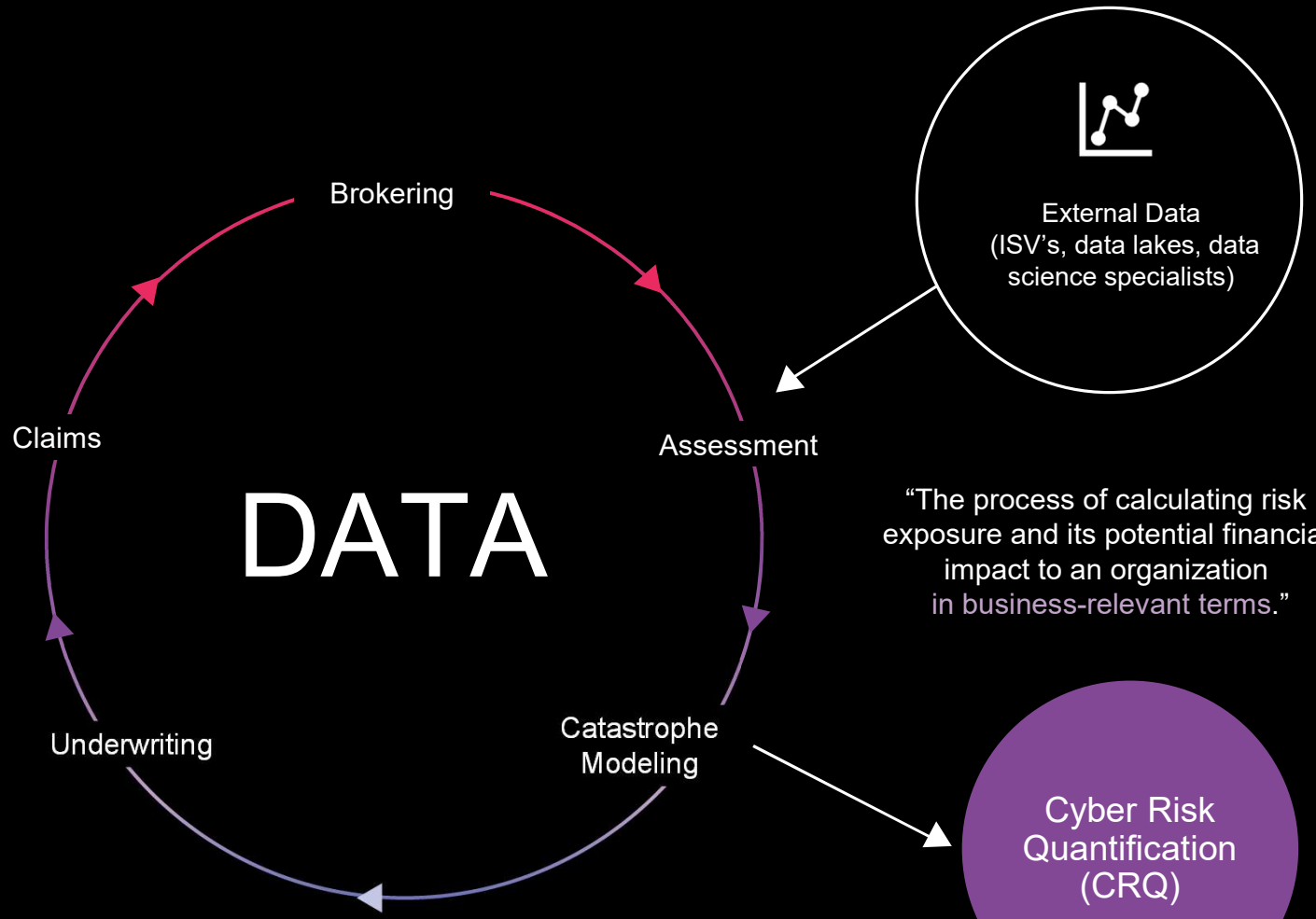
HYBRID CLOUD TOO OFTEN
MEANS TOO MANY TOOLS

SKYROCKETING

COSTS


BUILDING A RESILIENT
BUSINESS REQUIRES
A RE-THINK

THE HIDDEN VALUE OF CYBER INSURANCE



RECOVERY READINESS: A SECURITY IMPERATIVE

Recovery Readiness Is a Critical Step in Cyber Resilience

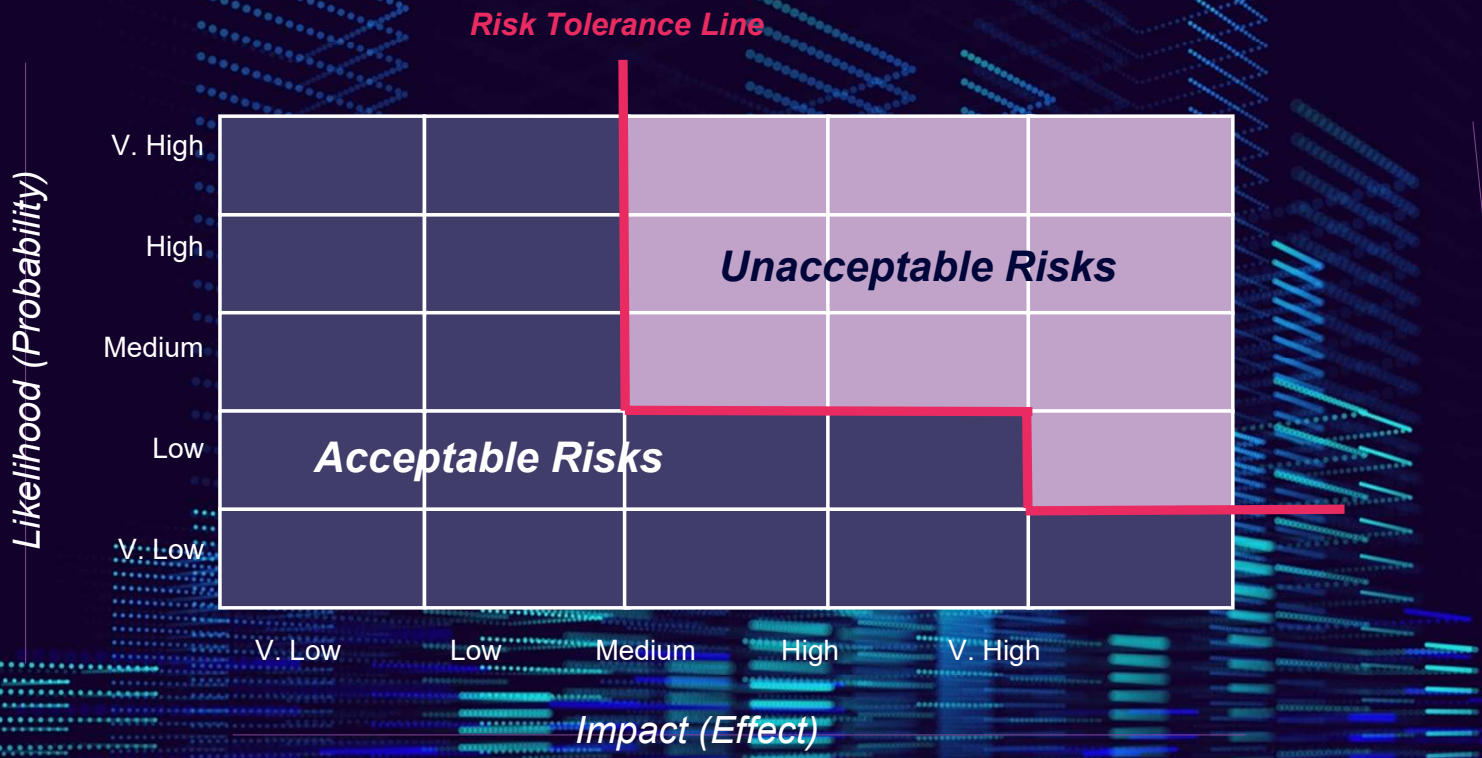
Security is blind to unknowns.
They must embrace the breach.

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


SOME CULTURAL
BEST PRACTICES…


MIND THE GAP
Infrastructure Team (CIO)
Security Team (CISO)

Preferred Risk Profiling




Cyber Recovery ≠ Disaster Recovery


M.T.C.R.
Mean Time to Clean Recovery

Cyber Recovery Maturity Model

	Level 1 | **Initial**	Level 2 | **Developed**	Level 3 | **Defined**	Level 4 | **Managed**	Level 5 | **Optimized**
IDENTIFY	Awareness of need for asset and risk management.	Asset and risk management procedures are developed.	Asset and risk management processes are fully documented and standardized.	KPIs for asset and risk management are tracked and analyzed.	Continuous refinement of asset and risk identification using predictive analytics.
PROTECT	Basic cybersecurity measures in place.	Comprehensive cybersecurity policies developed.	Cybersecurity measures are fully integrated and standardized.	Cybersecurity effectiveness is measured, tested, and analyzed.	Continuous improvement and adaptation of cybersecurity measures and processes, which are routinely tested.
DETECT	Initial detection methods are used.	Systematic approach to threat detection.	Threat detection processes are fully integrated and standardized.	Quantitative measures of detection effectiveness.	Predictive analytics inform detection strategies.
RESPOND	Incident response is reactive.	Incident response plans are developed.	Incident response is standardized and documented.	Incident response effectiveness is quantitatively managed and occasionally tested.	Adaptive incident response strategies based on continuous testing and learning.
RECOVER	Recovery efforts are ad hoc.	Formal recovery processes are developed.	Recovery processes are standardized and integrated.	Recovery processes are quantitatively managed, tested, and measured.	Recovery processes are continuously simulated, tested, improved and adapted to threats.

Developing A Cyber Recovery Plan

- Scope & Objectives
- Risk Assessment
- The Recovery Team
- Technical Architectures
- Processes
- Threat Modelling
- Testing & Validation
- Communications
- Continuous Improvement


SOME ARCHITECTURAL
BEST PRACTICES…

RECOVERY READINESS: A SECURITY IMPERATIVE

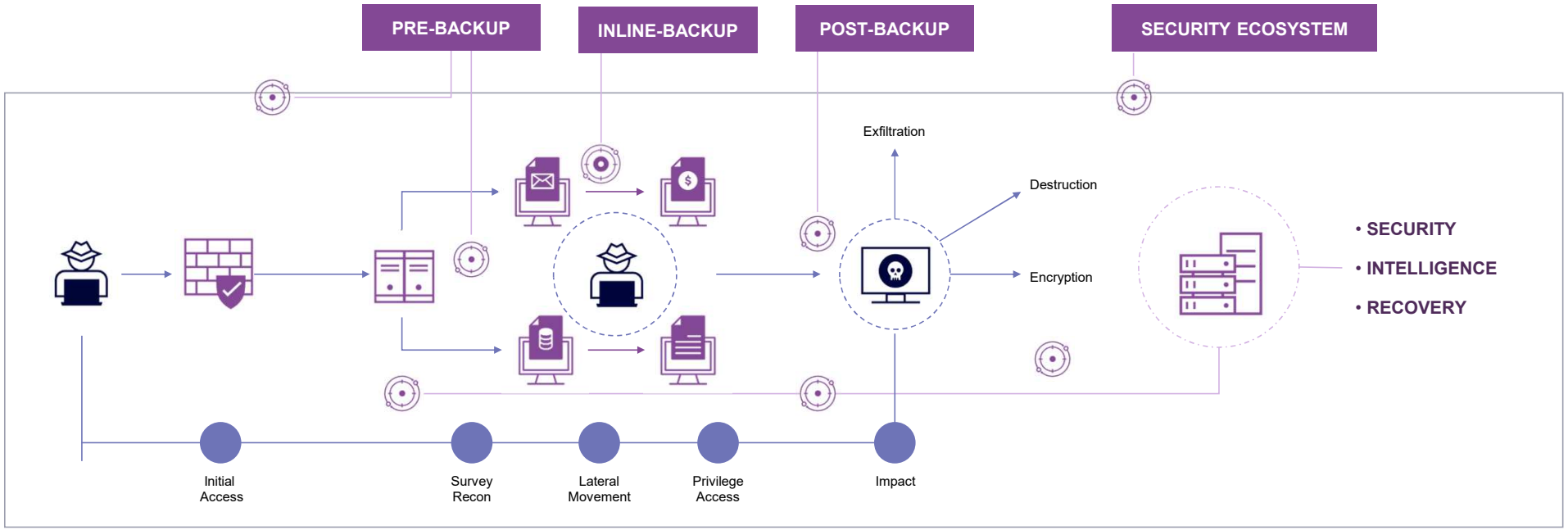
Recovery Readiness Is a Critical Step in Cyber Resilience

Security is blind to unknowns.
They must embrace the breach.

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

HOW IT WORKS

EARLY WARNING



PRE-BACKUP

- ThreatWise
- Risk Analysis
- Canary Files
- Live Anomaly

DURING-BACKUP

- File Activity
- File Type
- Backup Size
- Extensions
- Operational

POST-BACKUP

- Threat Scan
- Risk Analysis
- Data Verification
- Auto Recovery

SECURITY ECOSYSTEM

- SIEM/SOAR
- Threat Intelligence
- EDR/XDR/NDR
- Vulnerability

RECOVERY READINESS: A SECURITY IMPERATIVE

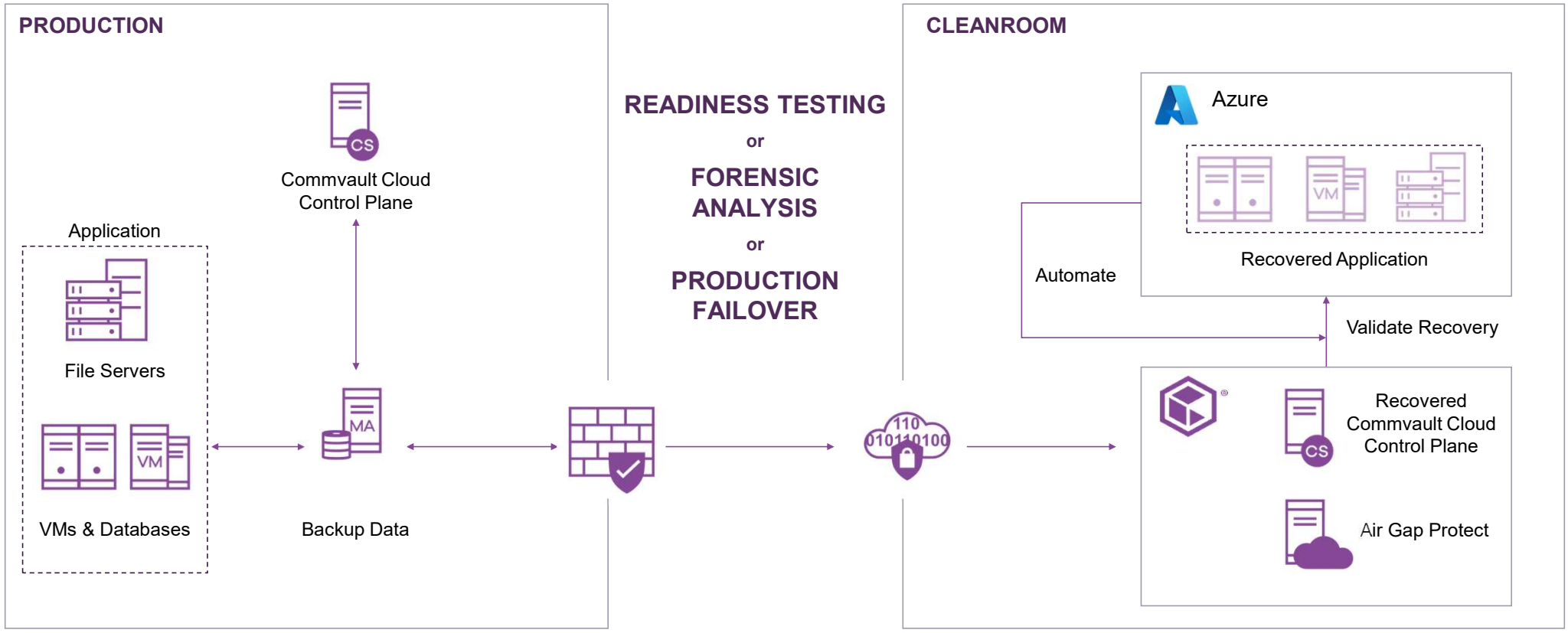
Recovery Readiness Is a Critical Step in Cyber Resilience

Security is blind to unknowns.
They must embrace the breach.

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

HOW IT WORKS – CLEANROOM RECOVERY

CLEANROOM RECOVERY – DELIVERING END-TO-END AUTOMATION



SUMMARY

- The threat landscape has **fundamentally changed**
- An over-reliance on “Protect-Detect-Respond” is **unwise**
- Actuarial science is teaching us lessons about **what matters**
- Need to focus on Risk, Readiness & Recovery…. **RESILIENCE**

Commvault®
Cloud
Powered by Metallic AI

Thank you!