DELIVERING OPERATIONAL RESILIENCE IN AN AGE OF RANSOMWARE & DIGITAL TRANSFORMATION

Chris Beckett
Security Sales Engineer, Rubrik X

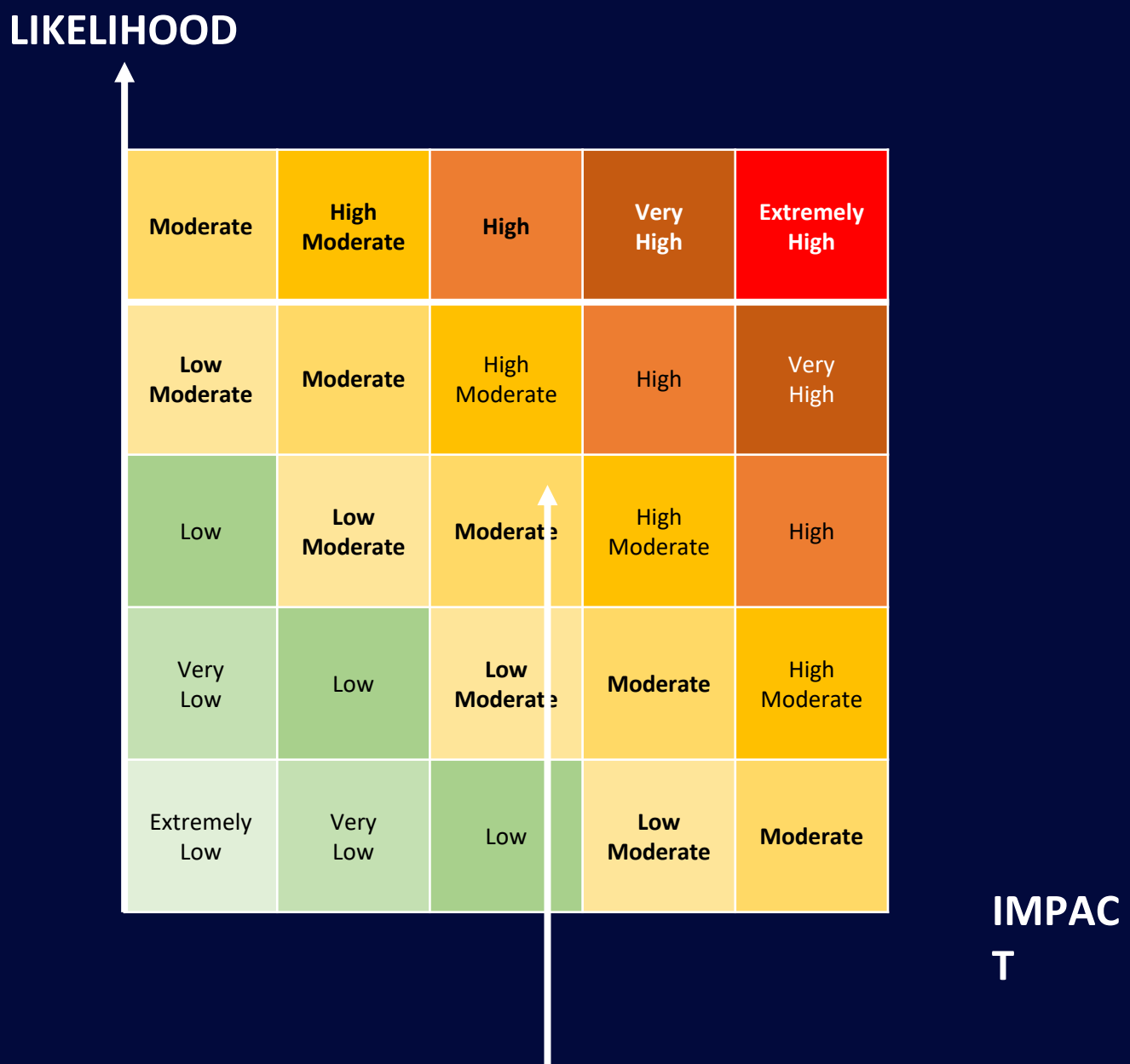
chris.beckett@rubrik.com
www.rubrik.com
Come and see us! Booth F25

rubrik


ADVERSARIES
HAVE FIRST MOVER
ADVANTAGE

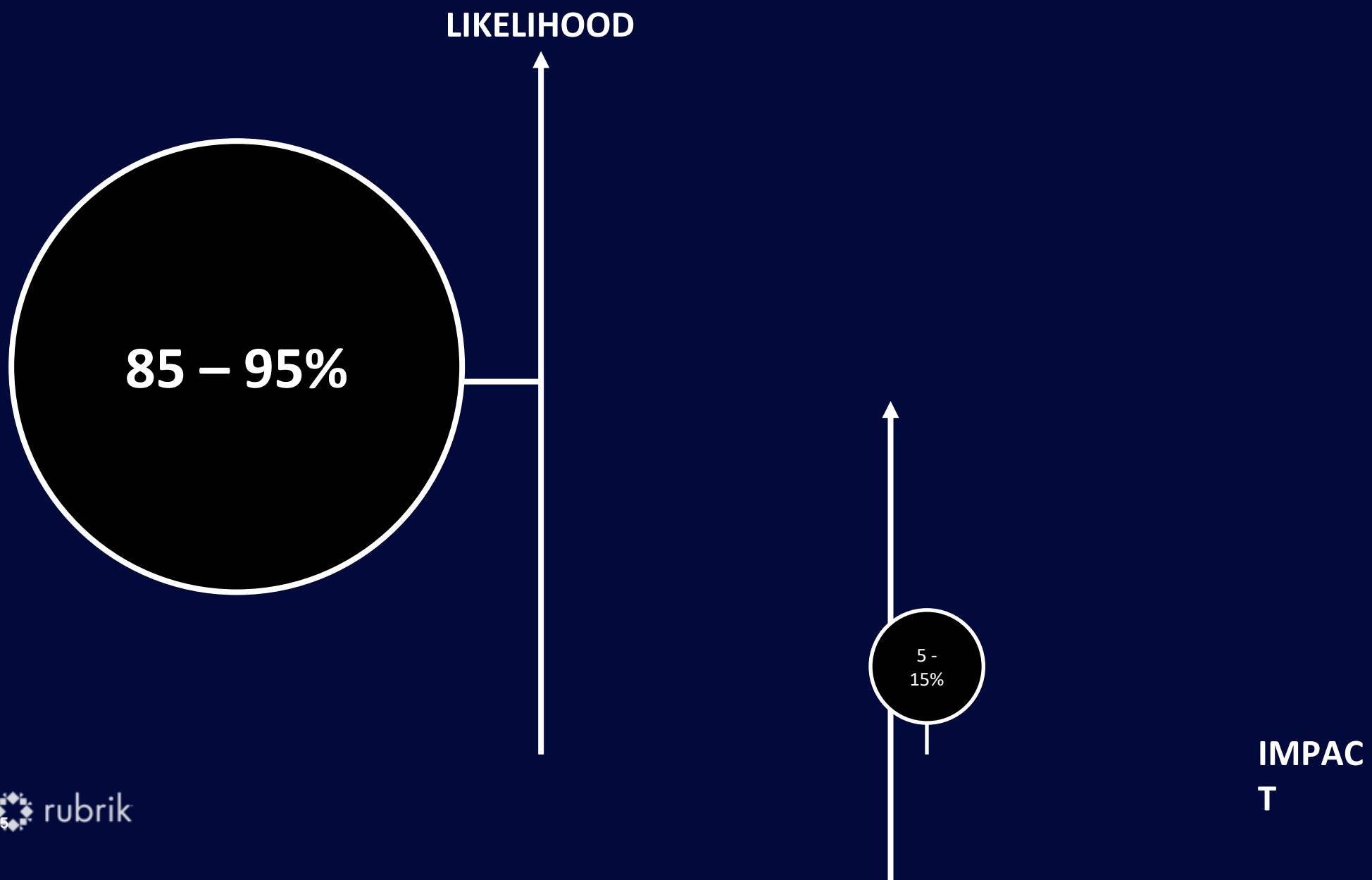
ADVERSARIES ADAPT

RISK EQUATION



rubrik

AVERAGE CYBER SECURITY BUDGET ALLOCATION



rubrik

CISO IN THE AGE OF TOOL SPRAWL

+ Budget
+ Headcount
+ Complexity
+ Licensing Costs
+ Attack Surface
+ Alerts
+ User Friction
+ Reduced Agility

Average enterprise has over 130 different cyber security tools deployed

Deloitte.

75% of organisations that pay ransoms have up-to-date network & endpoint security tools deployed

SOPHOS

rubrik

PRE-RANSOMWARE LOSS EVENTS

REPUTATION
LITIGATION
REGULATOR
Y

SECONDARY

LIKELIHOOD

Moderate	**High Moderate**	**High**	**Very High**	**Extremely High**
Low Moderate	**Moderate**	High Moderate	High	Very High
Low	**Low Moderate**	**Moderate**	High Moderate	High
Very Low	Low	**Low Moderate**	**Moderate**	High Moderate
Extremely Low	Very Low	Low	**Low Moderate**	**Moderate**

IMPACT

rubrik

POST-RANSOMWARE LOSS EVENTS

INABILITY TO EXECUTE ORGANISATION'S MISSION

LIKELIHOOD

Moderate	High Moderate	High	Very High	Very Very High	Extremely High	Ultra High	Unsustainable
Low Moderate	Moderate	High Moderate	High	Very High	Very Very High	Extremely High	Ultra High
Low	Low Moderate	Moderate	High Moderate	High	Very High	Very Very High	Extremely High
Very Low	Low	Low Moderate	Moderate	High Moderate	High	Very High	Very Very High
Extremely Low	Very Low	Low	Low Moderate	Moderate	High Moderate	High	Very High

IMPACT

PRIMARY

rubrik

WITH ALL THIS INVESTMENT IN PREVENTION & DETECTION THE BOARD OFTEN HAVE AN EXPECTATION THAT INCIDENTS WON'T HAPPEN

35% OF ORGANISATIONS THAT HAVE HAD A RANSOMWARE ATTACK SUFFERED C-LEVEL RESIGNATIONS OR FIRINGS AFTER THE INCIDENT

cybereason

SHARED INCIDENT RESPONSIBILITY


INCIDENT
SECURITY
IT


RECOVERY
REBUILD
ANTICIPATE
PREVENT
ADAPT
RESILIENCE

IT EVENT RESILIENCE

rubrik

CYBER EVENT RESILIENCE

rubrik Security Cloud

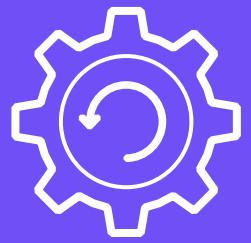
IT

USE CASES

DATA RESILIENCE

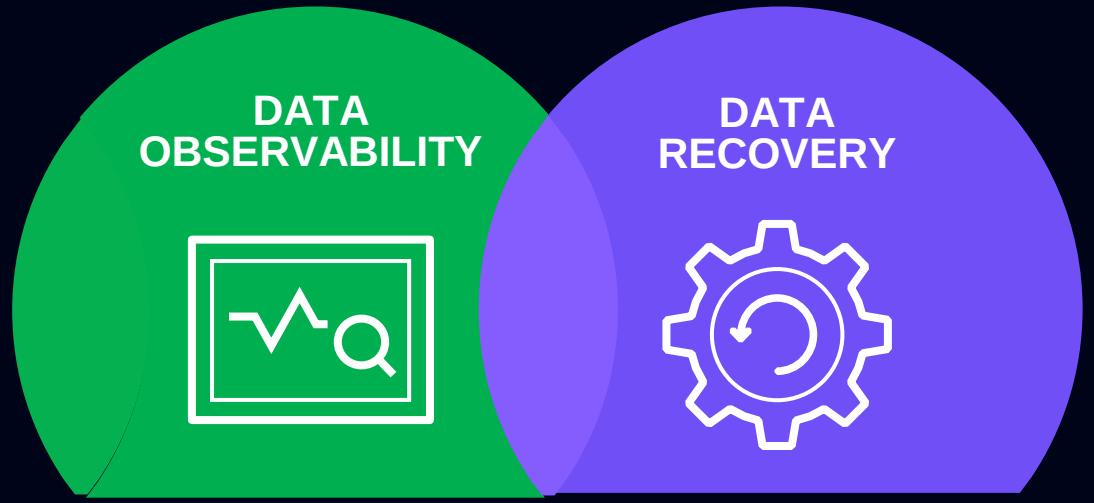
- Enterprise Data Protection
- Cloud Data Protection
- M365 Protection
- Invulnerable to Ransomware & Wiper Attacks

DATA RECOVERY



- Mass Recovery
- Orchestrated App Recovery

rubrik Security Cloud



CYBER

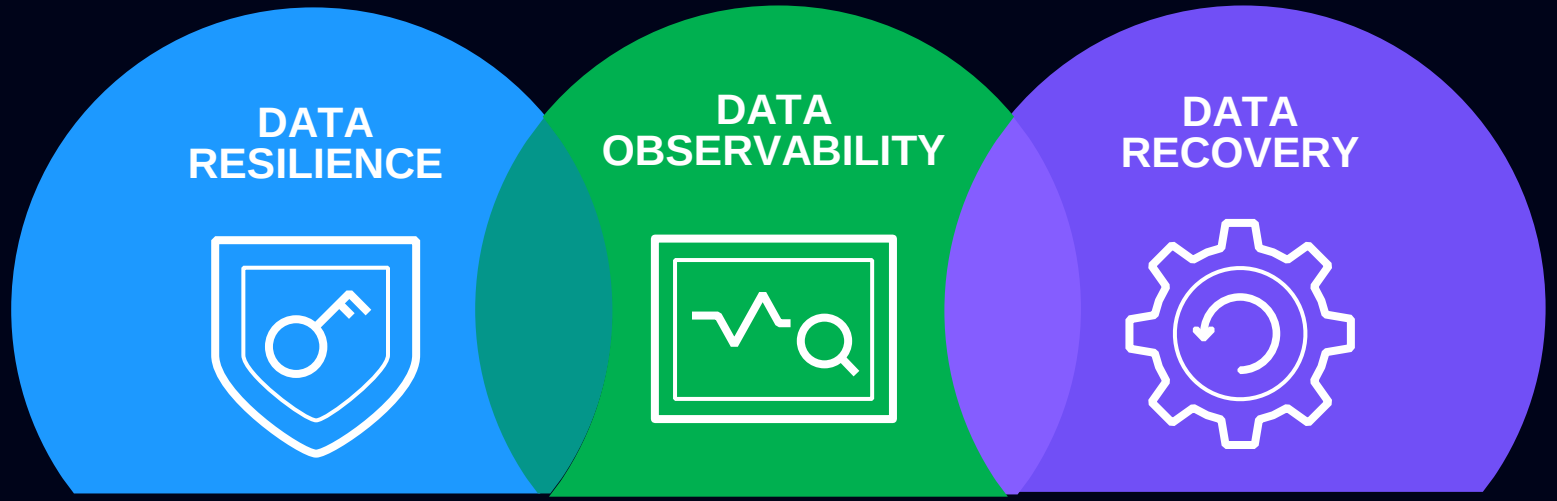
USE CASES

- Ransomware Monitoring & Investigation
- Wiper & Malicious Insider Monitoring & Investigation
- Sensitive Data Discovery
- Permission Auditing
- Threat Hunting
- Filesystem Forensics
- Threat Containment
- Vulnerability Containment
- Artefact Extraction
- Digital Twins for Cloud Migration, Pen Testing, Vulnerability Management & Deception

rubrik Security Cloud

IT

USE CASES



CYBER

USE CASES

- Enterprise Data Protection
- Cloud Data Protection
- M365 Protection
- Invulnerable to Ransomware & Wiper Attacks

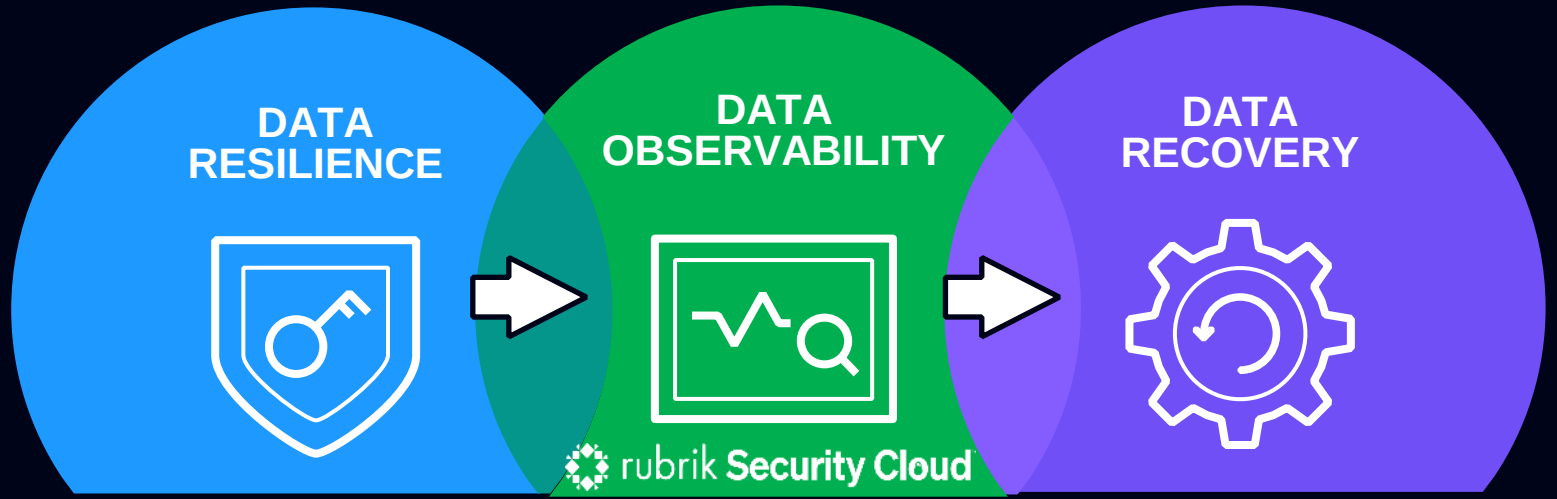
- Ransomware Monitoring & Investigation
- Wiper & Malicious Insider Monitoring & Investigation
- Sensitive Data Discovery
- Permission Auditing
- Threat Hunting
- Filesystem Forensics

- Mass Recovery
- Orchestrated App Recovery
- Threat Containment
- Vulnerability Containment
- Artefact Extraction
- Digital Twins for Cloud Migration, Pen Testing, Vulnerability Management & Deception

RUBRIK SECURITY CLOUD: THE PLATFORM FOR OPERATIONAL RESILIENCE

IT

USE CASES



CYBER

USE CASES

- Enterprise Data Protection
- Cloud Data Protection
- M365 Protection
- Invulnerable to Ransomware & Wiper Attacks

- Ransomware Monitoring & Investigation
- Wiper & Malicious Insider Monitoring & Investigation
- Sensitive Data Discovery
- Permission Auditing
- Threat Hunting
- Filesystem Forensics

- Mass Recovery
- Orchestrated App Recovery
- Threat Containment
- Vulnerability Containment
- Artefact Extraction
- Digital Twins for Cloud Migration, Pen Testing, Vulnerability Management & Deception

DELIVERING VALUE ACROSS DAY-TO-DAY CYBER OPERATIONS

rubrik Security Cloud

IDENTIFY	PREVENT	DETECT	RESPOND	RECOVER
Sensitive Data Discovery	Permission Auditing	Ransomware Detection	Artefact Extraction	Mass Recovery
	Penetration Testing	Wiper & Malicious Insider Detection	Filesystem Forensics	Orchestrated App Recovery
	Breach & Attack Simulation	Threat Hunting		Threat Containment
	Invulnerable to Ransomware & Wiper Attacks	Deception		Vulnerability Containment

WHAT THIS MEANS FOR THE CISO

Don’t Backup. Go Forward.