COHESITY

#PWCHackaday2022
Hong Kong

COHESITY

DEFEND YOUR DATA REFUSE the RANSOM

Victor Keong

Field CISO, APJ

Nov 24, 2022

Customer Case Study: Origin Property (Bangkok)

- Thailand’s premier real estate company
- One fine day …
- All Storage data cleaned up
- All existing backup repository cleaned up

Disaster Scenarios

Scenario	Scope of VMs	Business Impact	Likelihood	Time to Recover Today	Time to Recover Goal	Cohesity POC Results
Deleted or Corrupted File	1	Low	High	Variable based on file-count	Variable based on file-count	Global Search with flexible restore options. **< 1 minute**
Single VM Corruption	1	Low	Medium	1-2 hours	<10 minutes	Instant VM Restore **< 1 minute**
Storage Volume Corruption	30-50	Medium	Low	3 hours+	<10 minutes	Instant VM Restore of 50 VMs **< 3 minutes**
Storage Array Corruption	300-1,200	High	Low	8 hours	8 hours	Instant Recovery of 1,000 VMs **39 minutes**
Application Upgrade Rollback	1-50	Medium	High	30 minutes	<10 minutes	Instant VM Restore of 50 VMs **< 3 minutes**
OS Patching Goes Wrong	300-1,000	High	Low	5 Days	28 hours < 1 hour	Instant VM Restore of 250 Randomly selected VMs **<7 minutes**
Large-Scale Malware Attack	1,000-16,000	High	Low	4 Weeks	< 24 hours	2,200 VMs Powered on and available **47 Minutes** Back on primary storage = 4 hours

Cyber Resilience Day
Next-Gen Data Management
with eat Defense
from ge to Cloud

Ransomware Accelerates need for Data Management and Data Security

Imperatives to Defend your Data

Resilience is **Strategic** and **Foundational** to cybersecurity

Data-Centric security is **Intelligent** and **Dynamic**

Recovery must be **Scalable** and **Predictable**

Are Enterprises Ready?

21% HAVE CONTINGENCY PLANS TO RECOVER FROM RANSOMWARE ATTACKS

11% COULD RECOVER DATA AND APPS WITHIN THREE DAYS AFTER AN ATTACK

92%

DO NOT MAINTAIN AN **ISOLATED** VAULT FOR THEIR DATA

Source: Forrester Research Ransomware Recoverability Must Be a Critical Component Of Your Business Continuity Plans, Cybersecurity Venture Customer Advisory Board Oct 2021

The IT and Security Gap

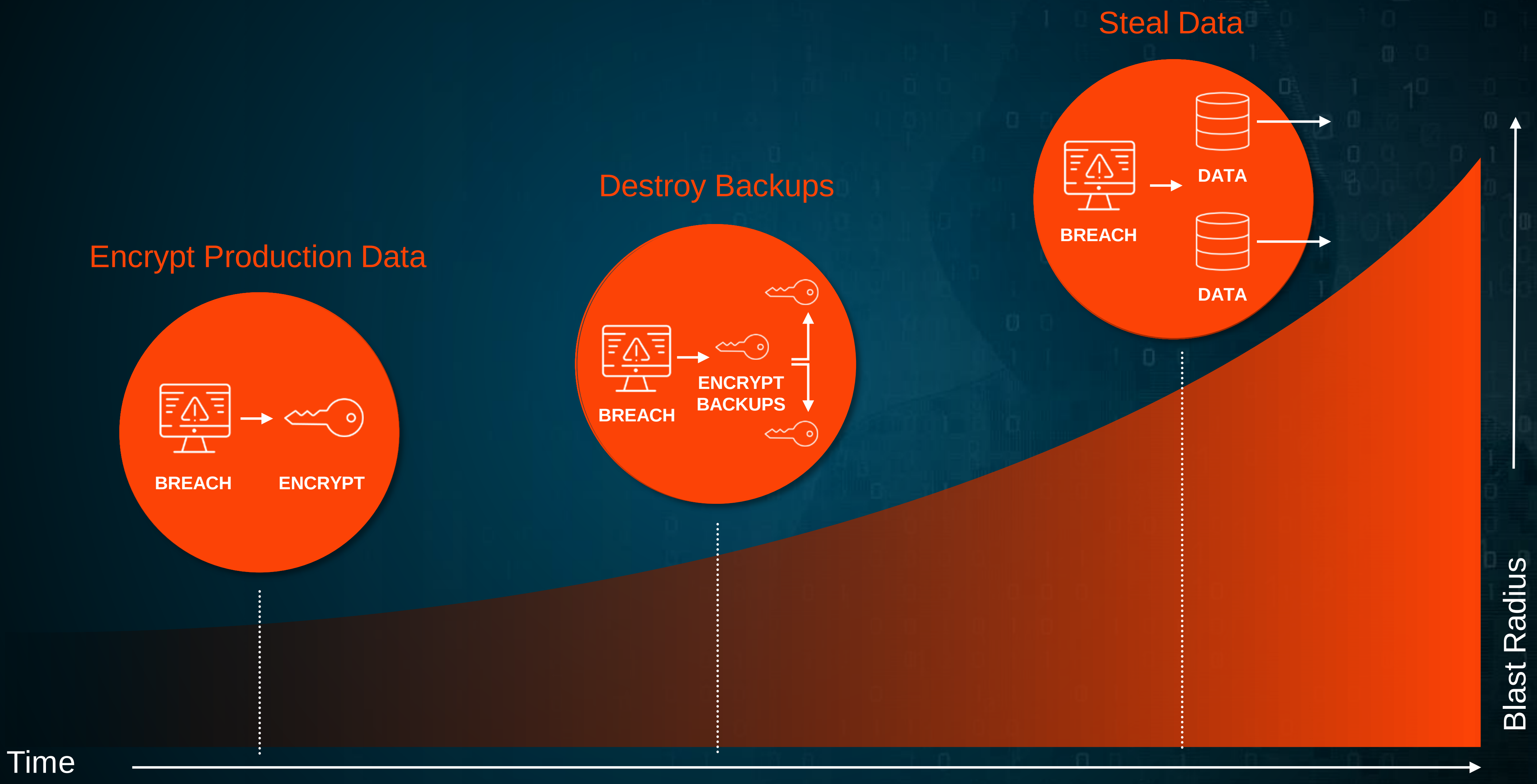
Security

- ☑ Backups in place
- ☑ Tape copy offsite
- ☑ Encryption, MFA, etc.

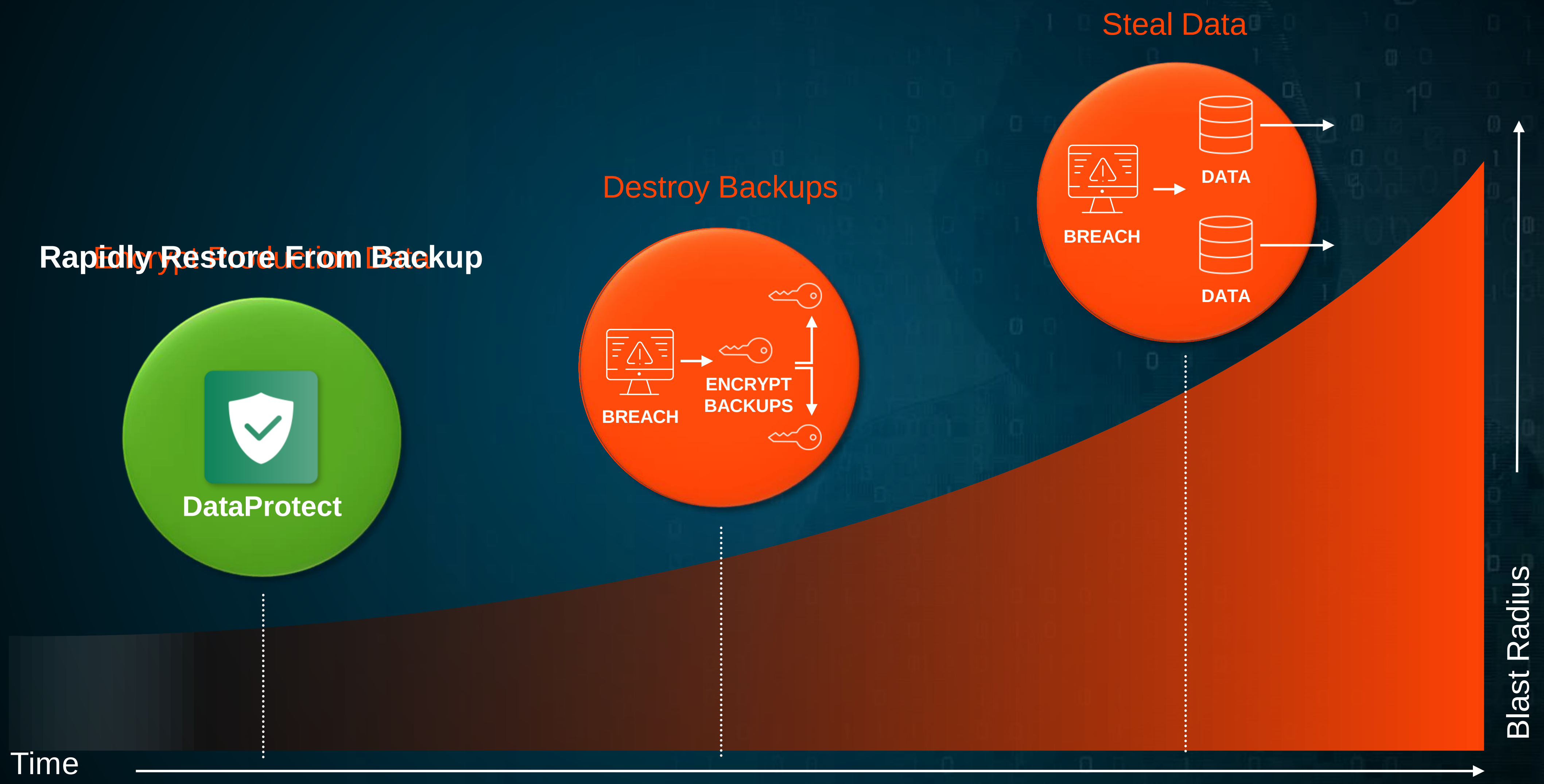
IT

- ✗ Days/Weeks to Recover
- ✗ Missing/Unreliable Tapes
- ✗ Data Loss

The Growing Blast Radius of Ransomware



Minimizing the Blast Radius of Ransomware



Steal Data

BREACH

DATA

DATA

Destroy Backups

BREACH

ENCRYPT BACKUPS

Rapidly Restore From Backup

Encrypt Production Data

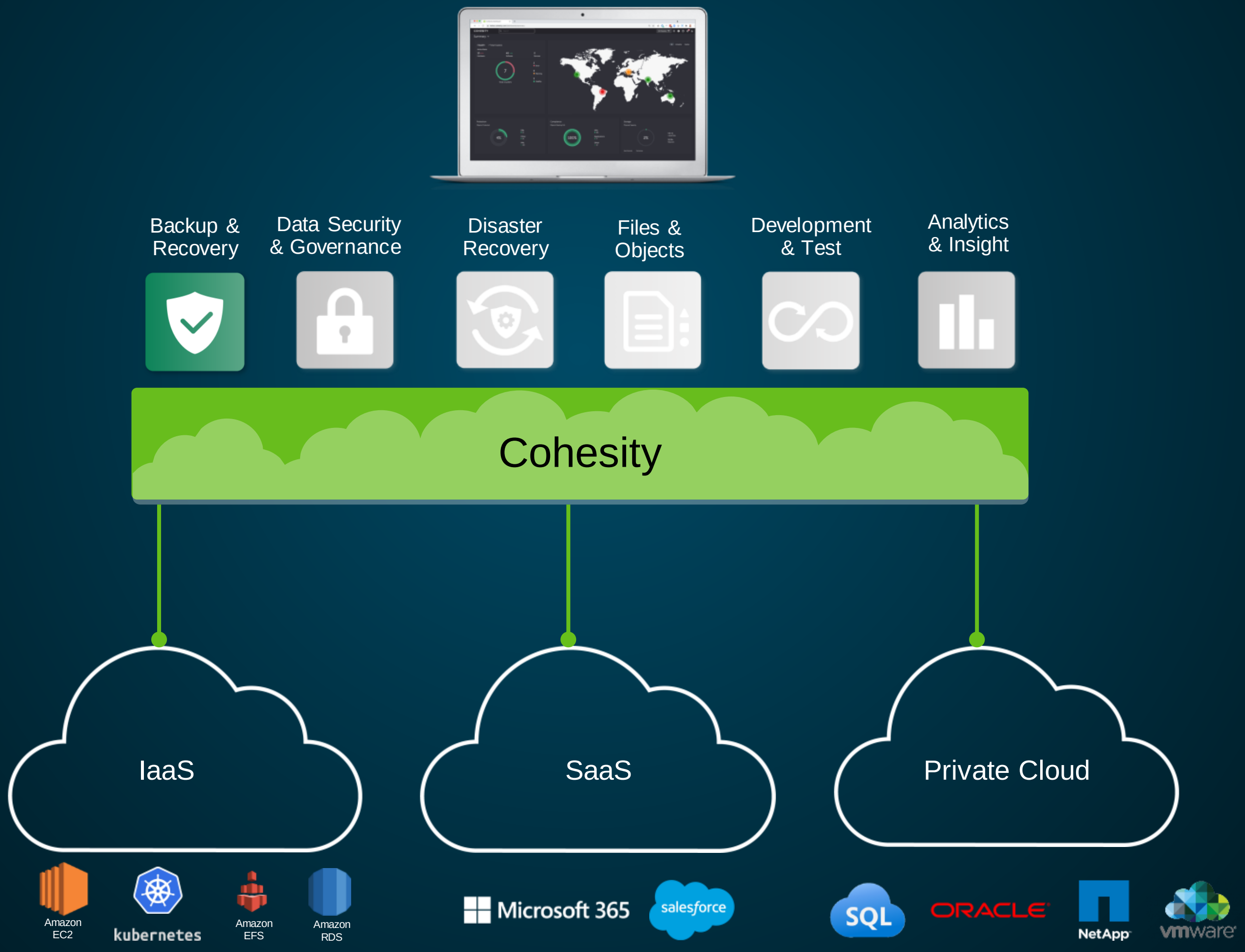
DataProtect

Time

Blast Radius

Protect Any Data Anywhere

One simple solution



Backup & Recovery

Data Security & Governance

Disaster Recovery

Files & Objects

Development & Test

Analytics & Insight

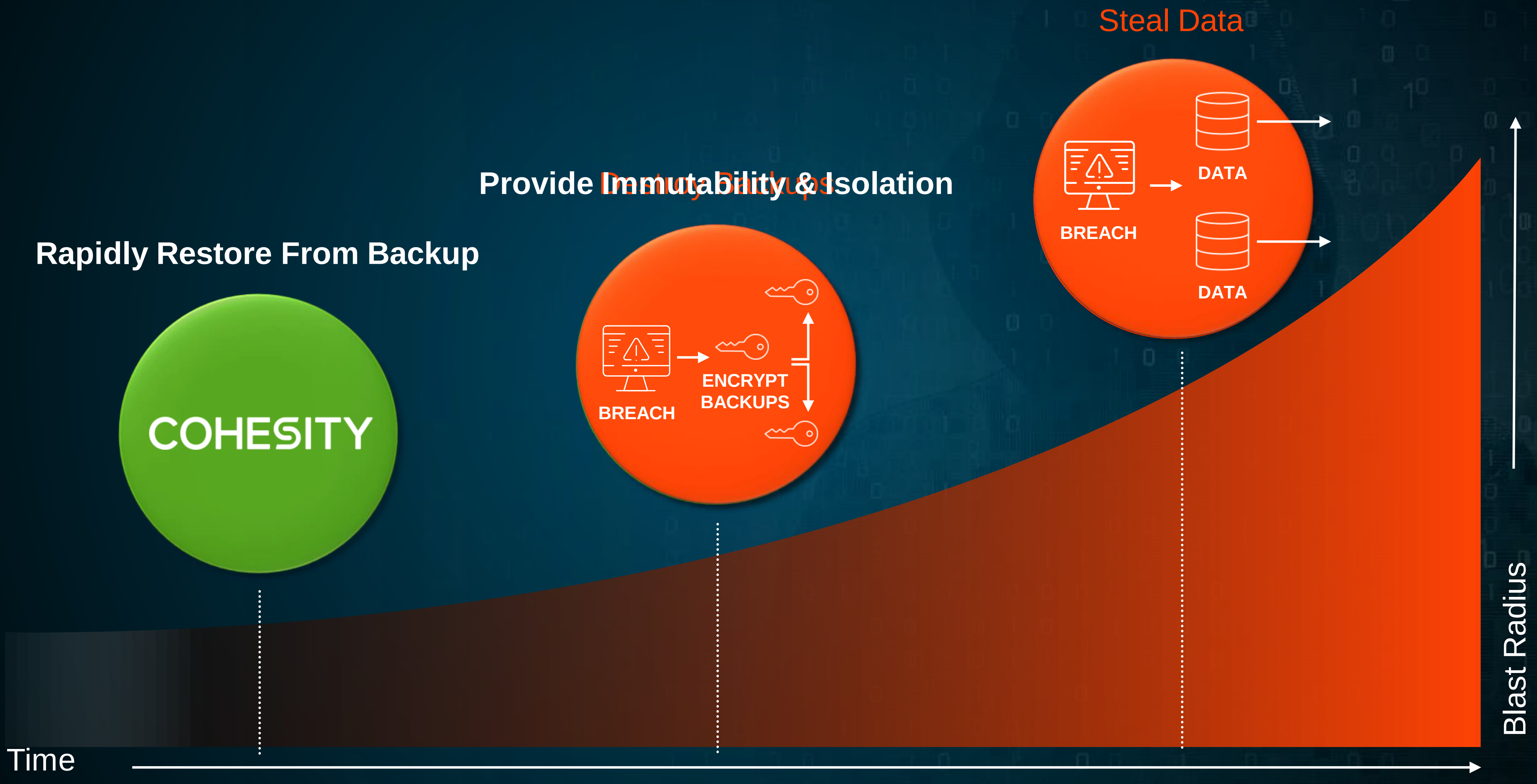
Cohesity

IaaS

SaaS

Private Cloud

Minimizing the Blast Radius of Ransomware



Steal Data

Provide Immutability & Isolation

Destroy Backups

Rapidly Restore From Backup

How Confident Are You That You Can Recover From an Attack?

Do you have an offsite vault?

Do you have advanced detection capabilities?

Do you run drills to simulate an attack?

The 3-2-1 Rule

3

Copies of your data

Snapshots

2

Copies in different locations

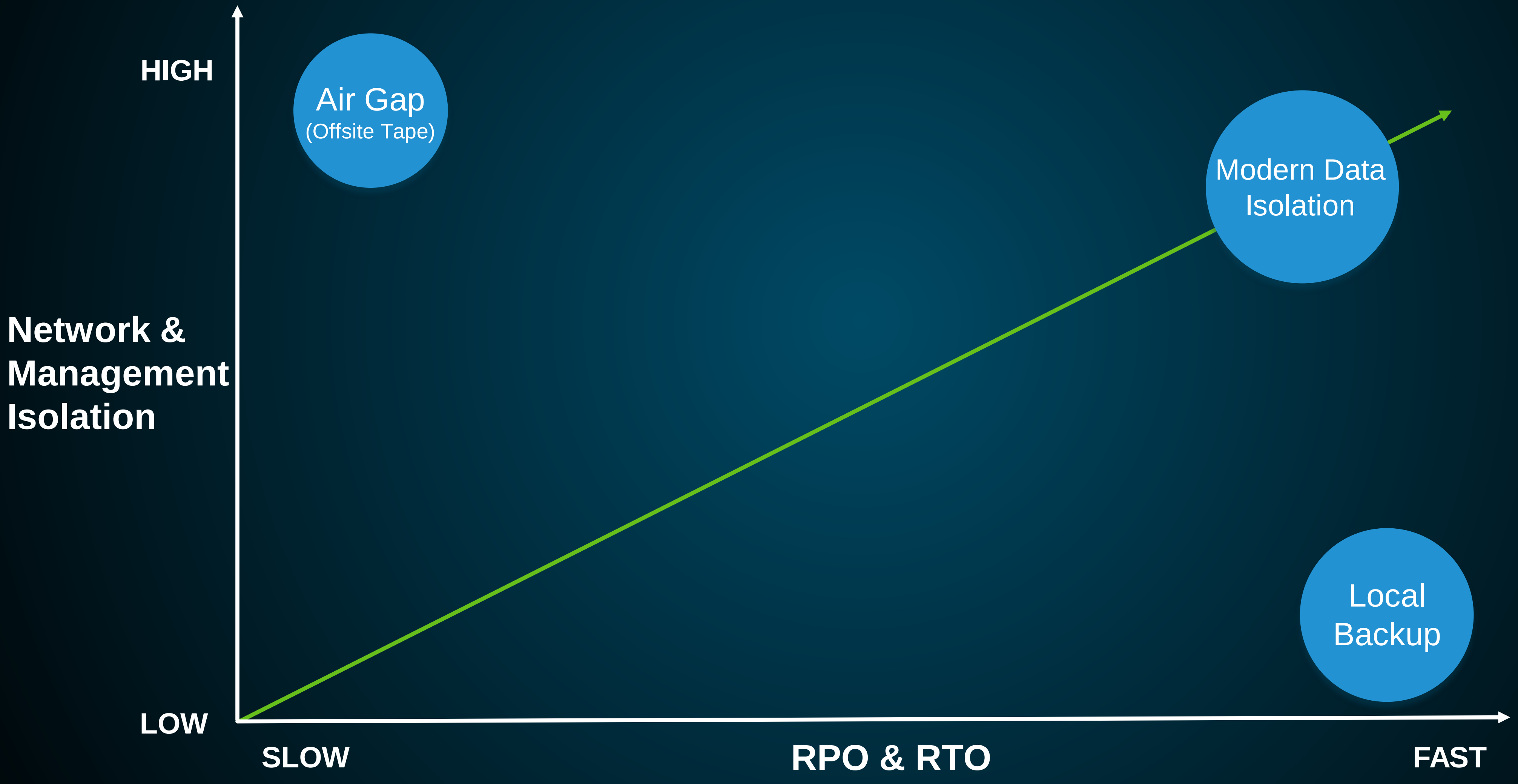
Replication

1

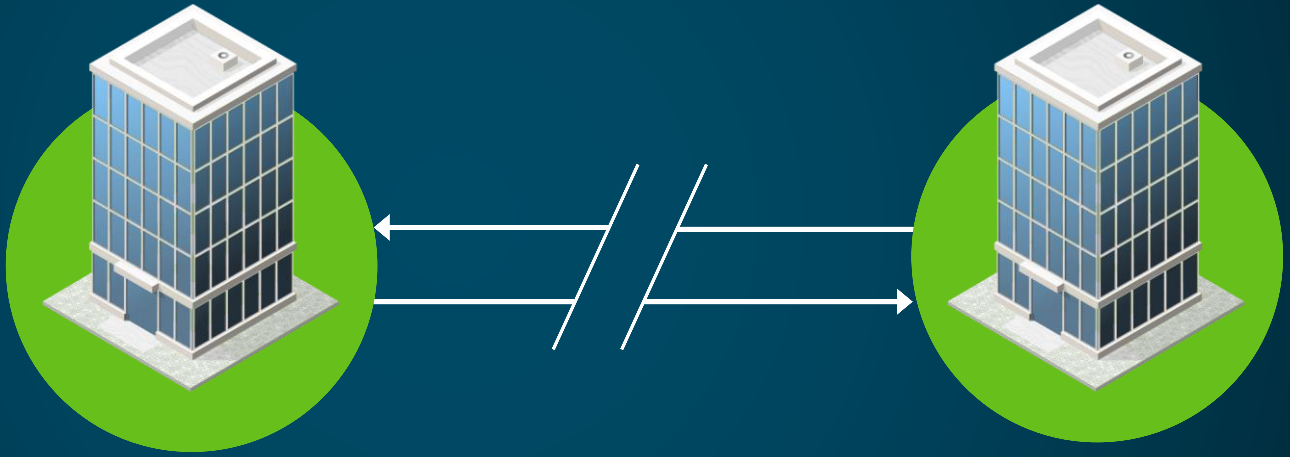
Copy in an off-site location

Archive

Balancing Security and Agility

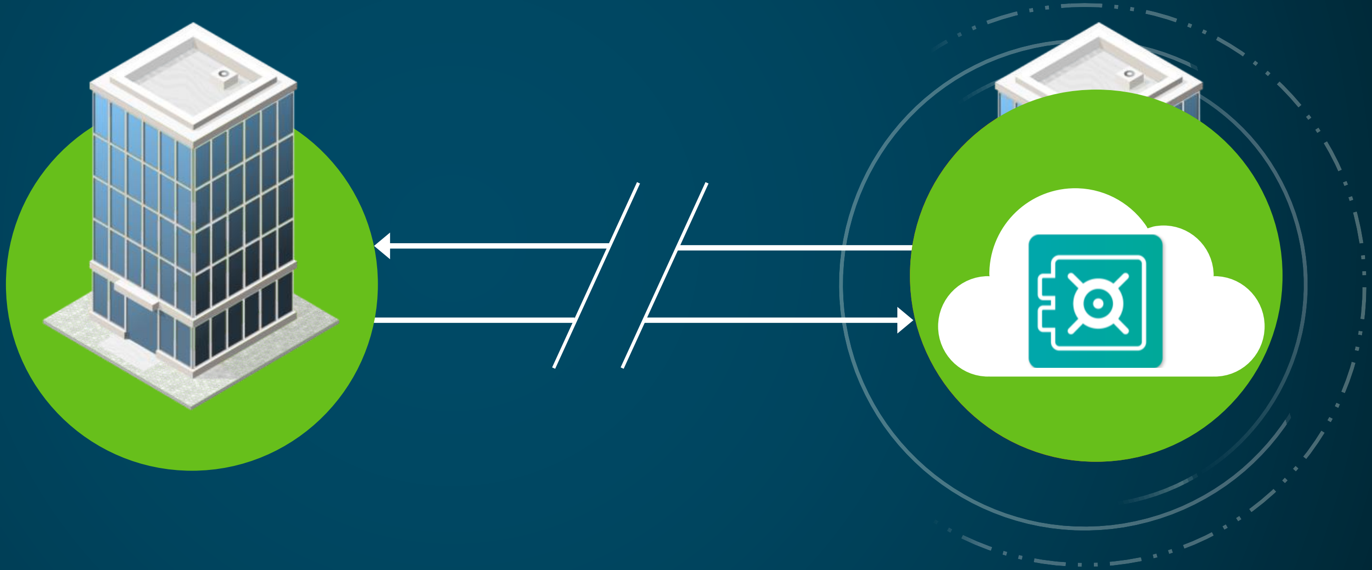


Isolation via a Self Managed Vault



COHESITY

Isolation built for the Cloud Era



Cohesity FortKnox Features & Benefits

Isolated Vault

- Virtually Air-gapped Data Copy
- Management Isolation
- Network Isolation

Controlled Access

- Short-lived token based authentication
- RBAC to limit access to vault data & policies
- Multi-Factor Authentication
- Quorum Controlled Recovery

DataLock

- Immutable Snapshot
- Irrevocable DataLock using AWS ObjectLock

Data Security

- Data-At-Rest & Data-In-Flight Encryption

Ransomware Protection

- Machine Driven Intelligence to identify a clean copy of data
- Anomaly Detection & Reporting

Flexible Recovery

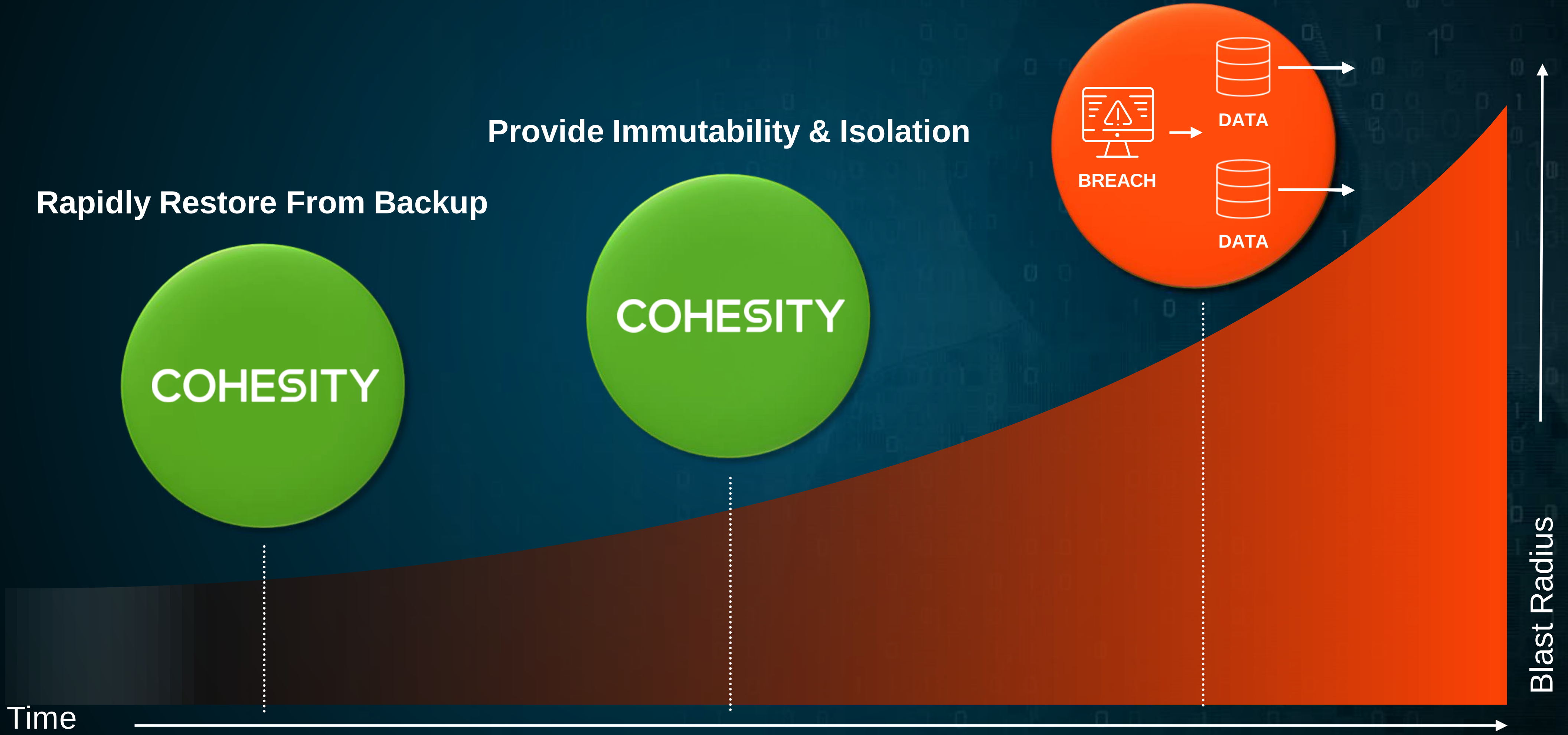
- Global search & Recover
- Granular Recovery
- Recover to Original/Alternate Location

Minimizing the Blast Radius of Ransomware

Converge Data Security & Governance

Provide Immutability & Isolation

Rapidly Restore From Backup



Data Security and Data Governance MUST Converge

Data Security

Who has access
to sensitive data?

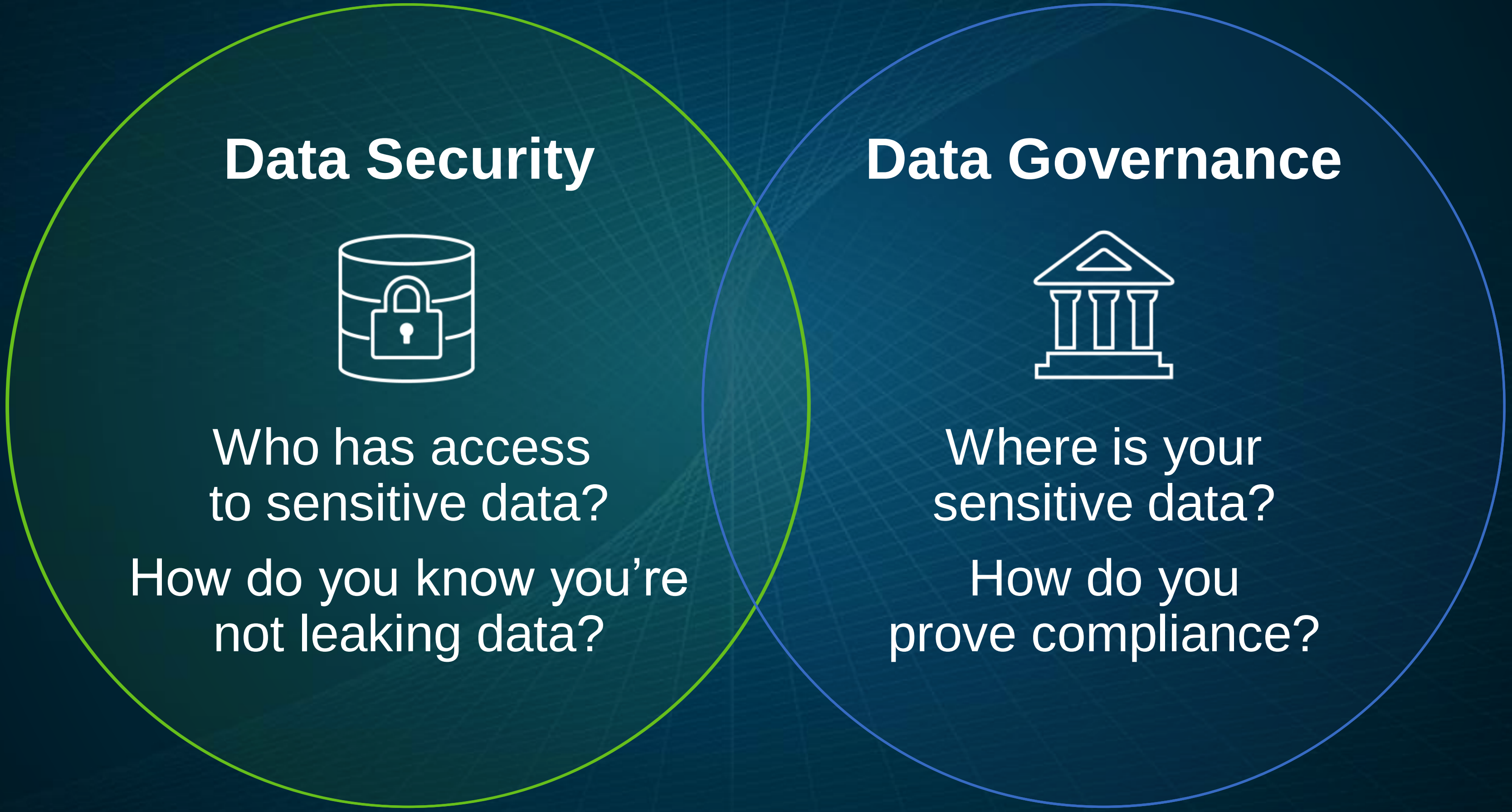
How do you know you’re
not leaking data?

Data Governance

Where is your
sensitive data?

How do you
prove compliance?

Data Security and Data Governance MUST Converge



Data Security

Who has access
to sensitive data?

How do you know you’re
not leaking data?

Data Governance

Where is your
sensitive data?

How do you
prove compliance?

COHESITY

Introducing Cohesity DataHawk

Reduce your risk profile by providing actionable insights and safeguarding data from evolving threats

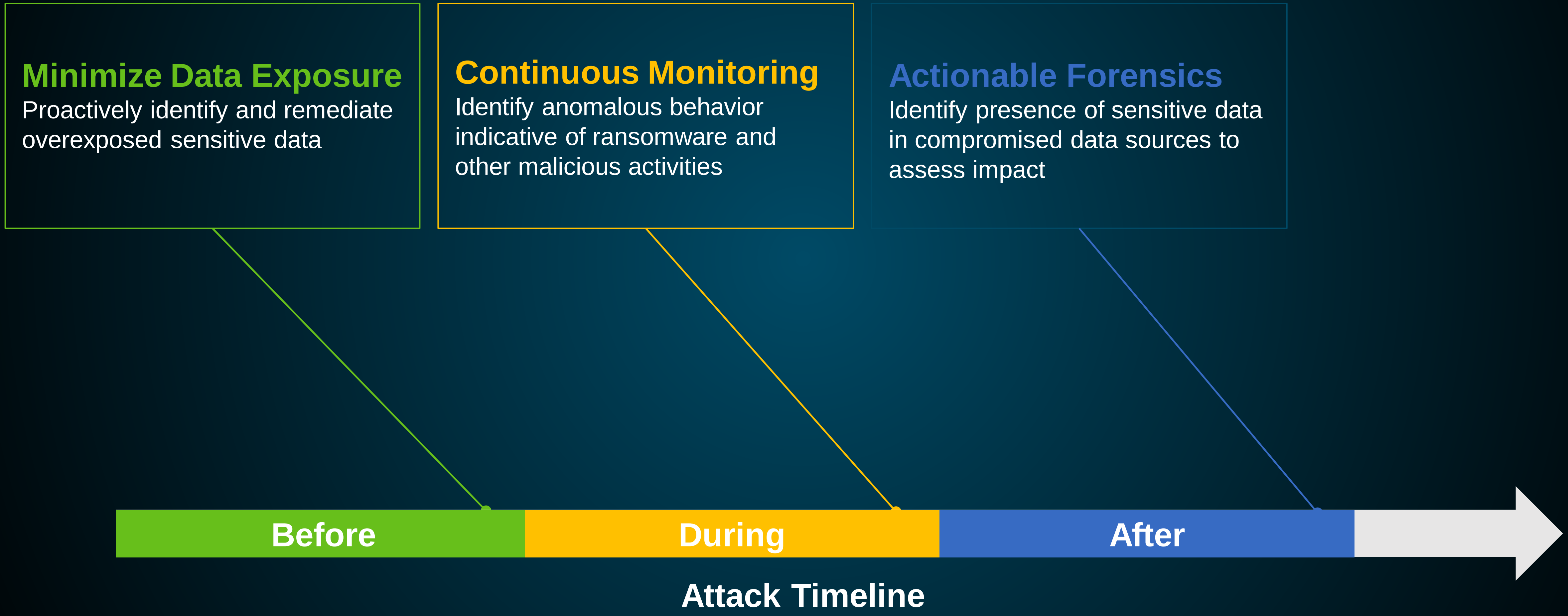
From the
Unknowns

Ransomware
Malware
Uninvited
External Threats

From
Known Elements

Rogue Employees
Unintended
Data Exposure
Prove Compliance

Data Insights across an Attack



Minimize Data Exposure
Proactively identify and remediate overexposed sensitive data

Continuous Monitoring
Identify anomalous behavior indicative of ransomware and other malicious activities

Actionable Forensics
Identify presence of sensitive data in compromised data sources to assess impact

Attack Timeline

Summary

- Modern backup is **no longer optional** as the last line of defense to ransomware
- **Backup alone is not sufficient** to address the newest variants of ransomware
- A **comprehensive data security** approach requires data isolation and shifting left
- As you shift to **hybrid and multi-cloud**, we meet you where you are
- A unified platform will **simplify** your operations reducing skills demand

COHESITY

Thank You