IBM STORAGE FOR DATA RESILIENCE

Hrvoje Stanilovic
IBM FlashSystem and Business Development Leader, NCEE
hrvoje.stanilovic@hr.ibm.com

- Regulations
- Business impacts
- What does bad look like?
- Steps to resilience
- What does good look like?

Regulations

Operational Resilience Regulations

- Risk to Economy
- NIS2: CEOs or legal representatives can be suspended
- DORA: Act allows for criminal penalties to be imposed on management
- UK Bank fined £48.65m for operational resilience failings
- New standard for best practice

Business impacts

Business impacts of cyber attacks

$5m

Est. average annual cost of a Cyber Attack in 2024

2.5x

increase in attacks

25%

share of malicious attacks that rendered systems inoperable

23

days, average recovery after a ransomware attack

57%

of organizations raised their product or services prices due to a breach

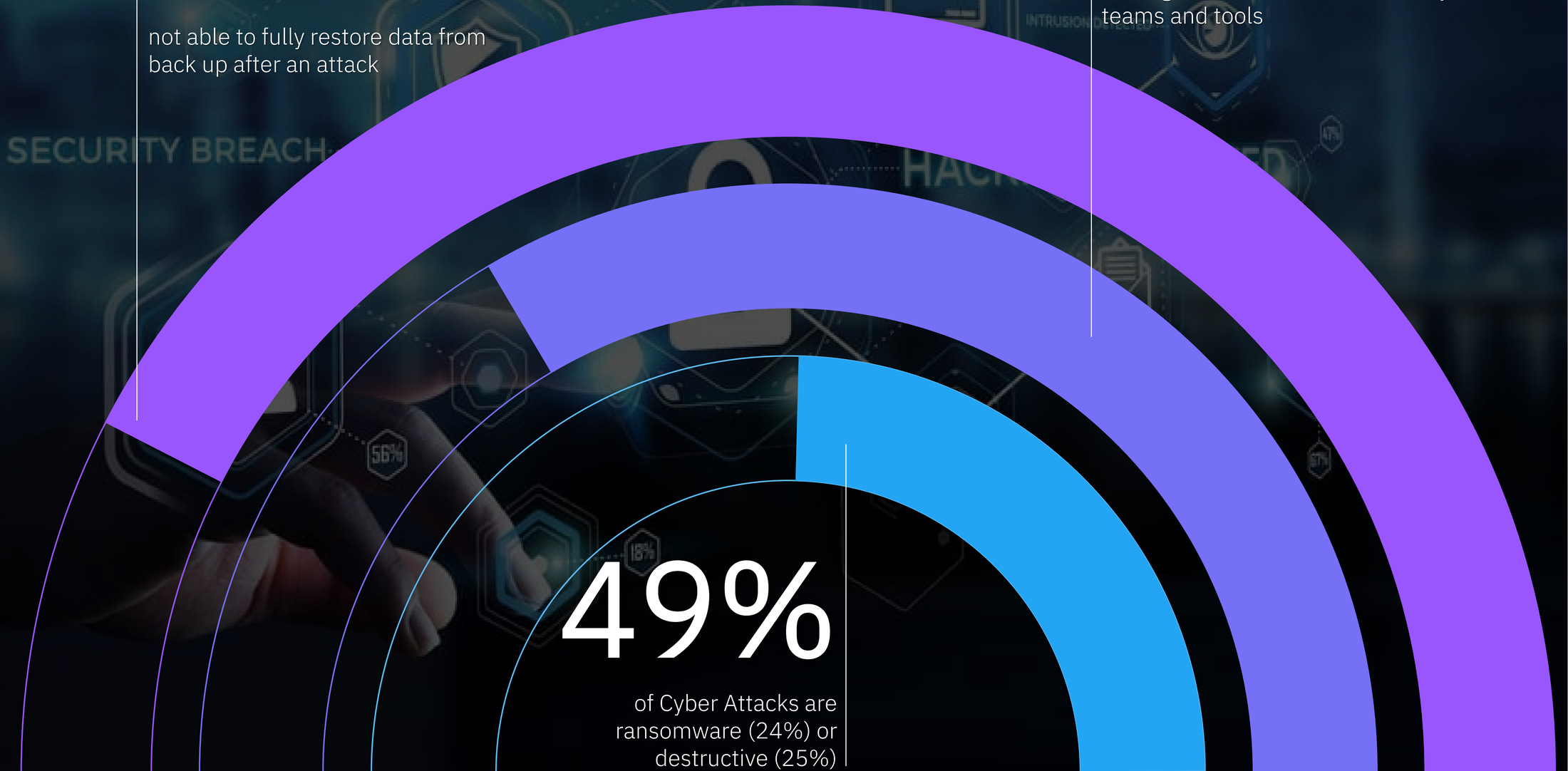
Data is Under threat

85%

not able to fully restore data from back up after an attack

66%

of breaches were not identified by the organization's internal security teams and tools



49%

of Cyber Attacks are ransomware (24%) or destructive (25%)

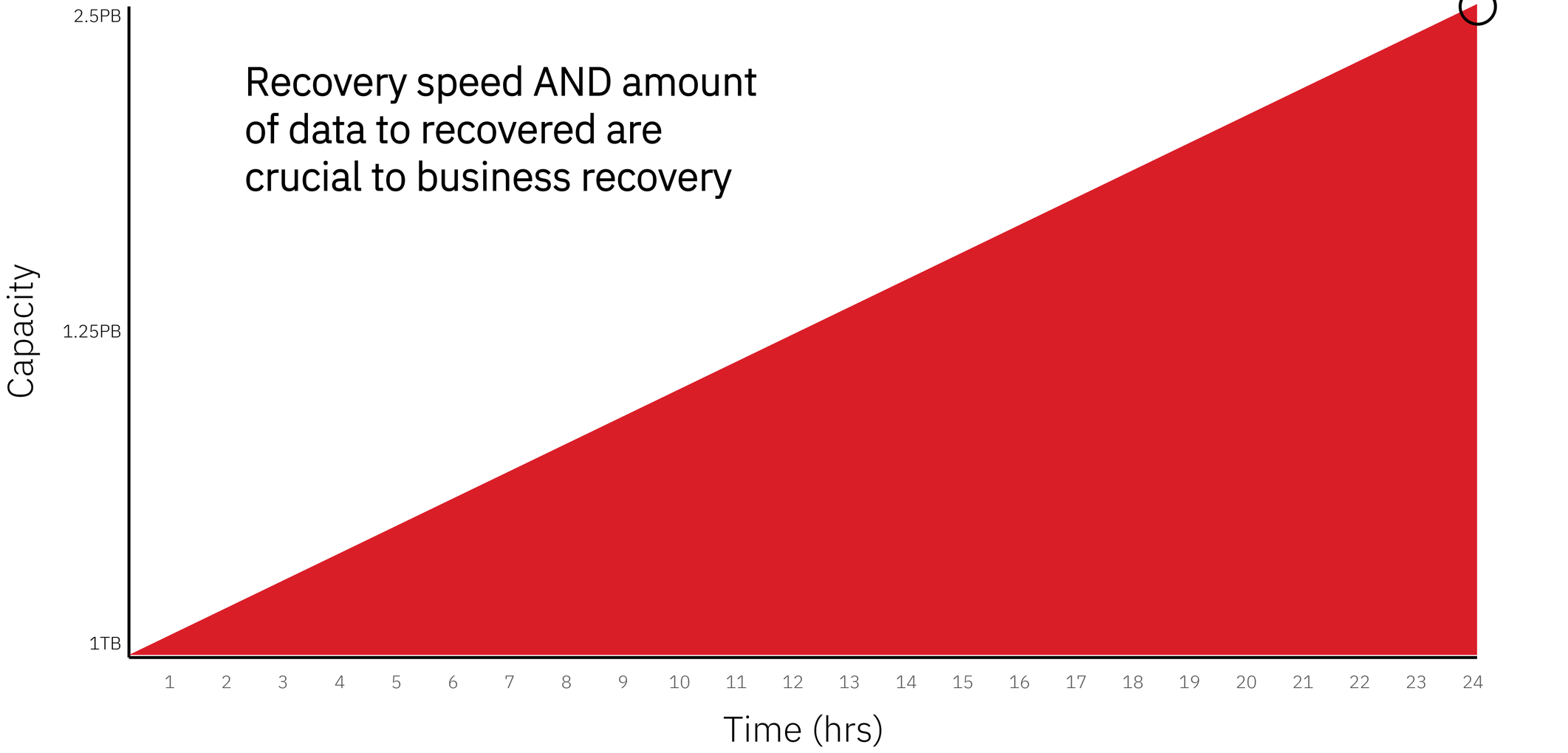
What does bad look like?

Is your business resilient?

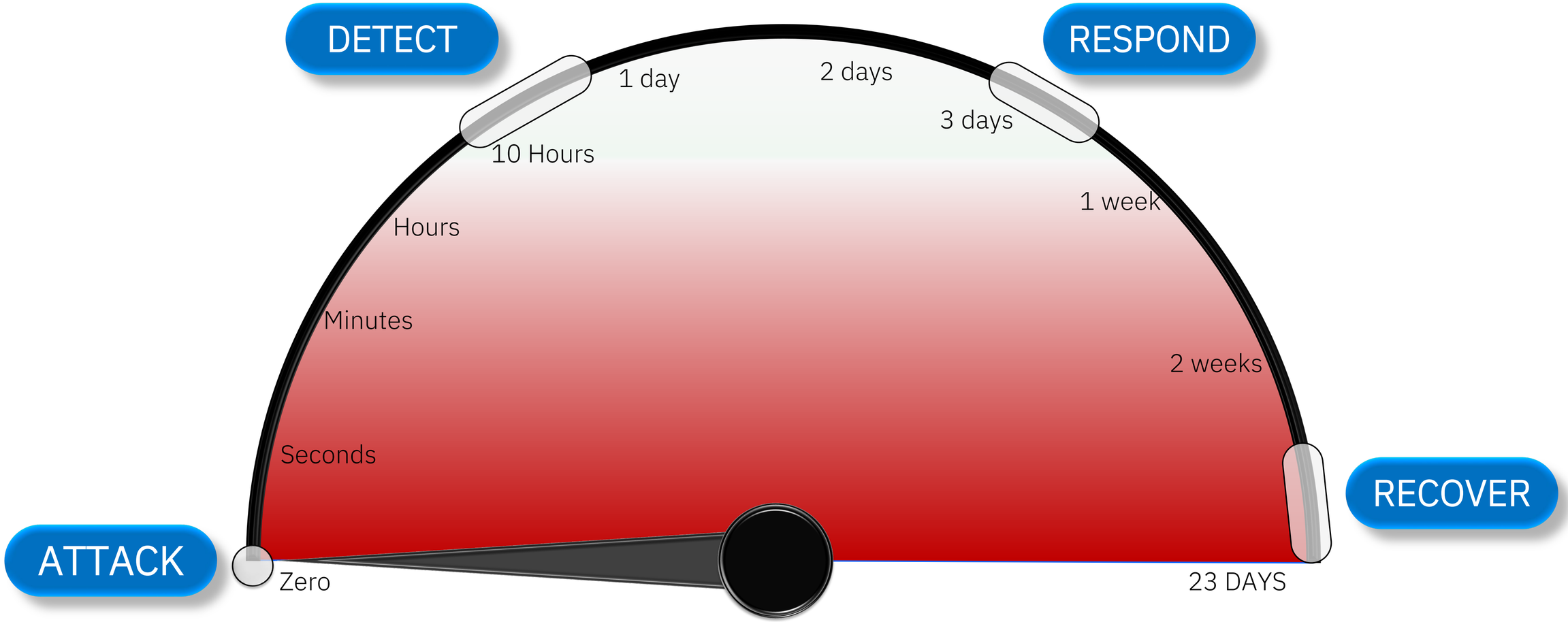
Predict attacks Cyber-attack prevention Respond to cyber-attacks	Minimize/eliminate downtime Protect from infrastructure failures Avoid data loss from disasters	Secure data copies Active and Dormant threat scanning Business recovery

IBM Cyber Resiliency Assessment Tool (CRAT)
Understand your blind spots

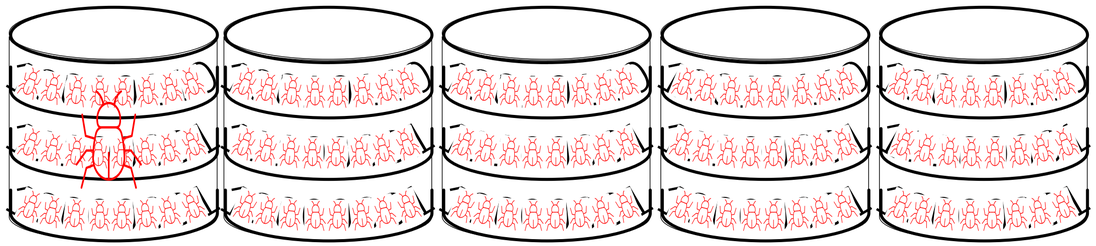
Data Encryption/Destruction over time



Impact timeline

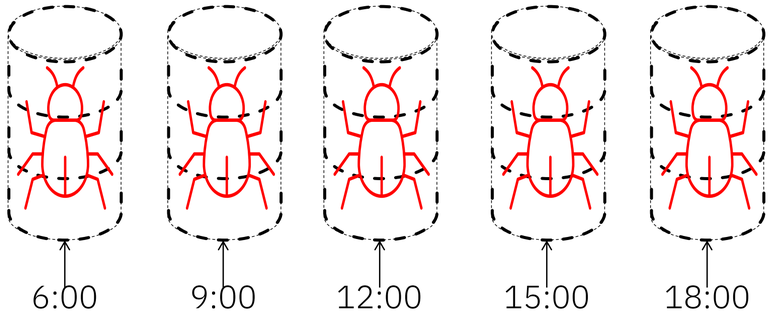


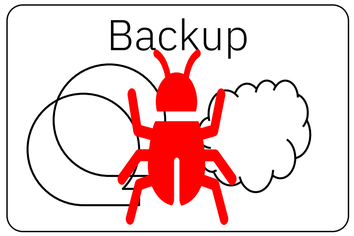
Production workloads



All production workloads stopped and corrupt

Snapshots

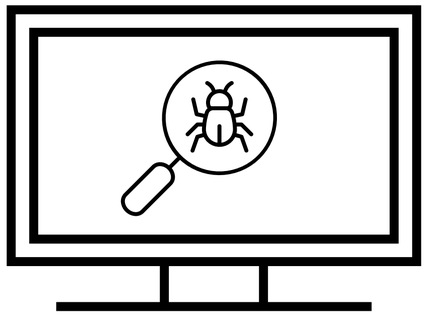




Nothing to recover from

Without Data Resilience

Cyber Security



Steps to resilience

Steps to Data Resilience

SECURITY & DATA PROTECTION

01

Predict, prevent, and respond
SOC Integration
Protect from infrastructure failures and Natural disasters

IMMUTABILITY

02

Recoverable data points
Incorruptible, data can not be deleted

DISCOVERY

03

Find active threats
Find & prevent dormant threats

RECOVERY

04

Rapid operational recovery in seconds, minutes, hours
Avoid paying ransoms

AUTOMATION

05

Simplified operations plus ability to test and prove recoverability
Integration between Cyber Security & Cyber Resiliency

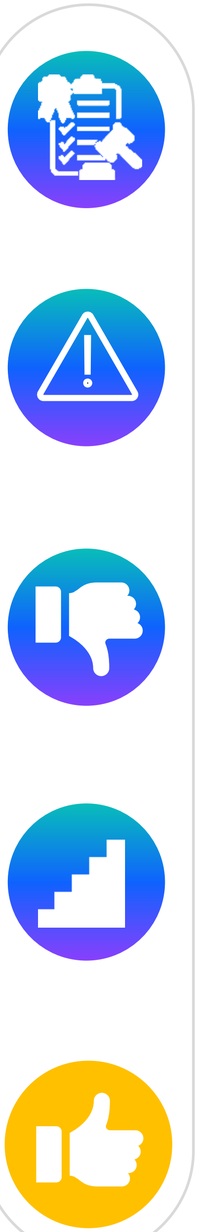
Operational resilience priorities

Minimum Viable Company

Workloads that are making the business money every second of the day

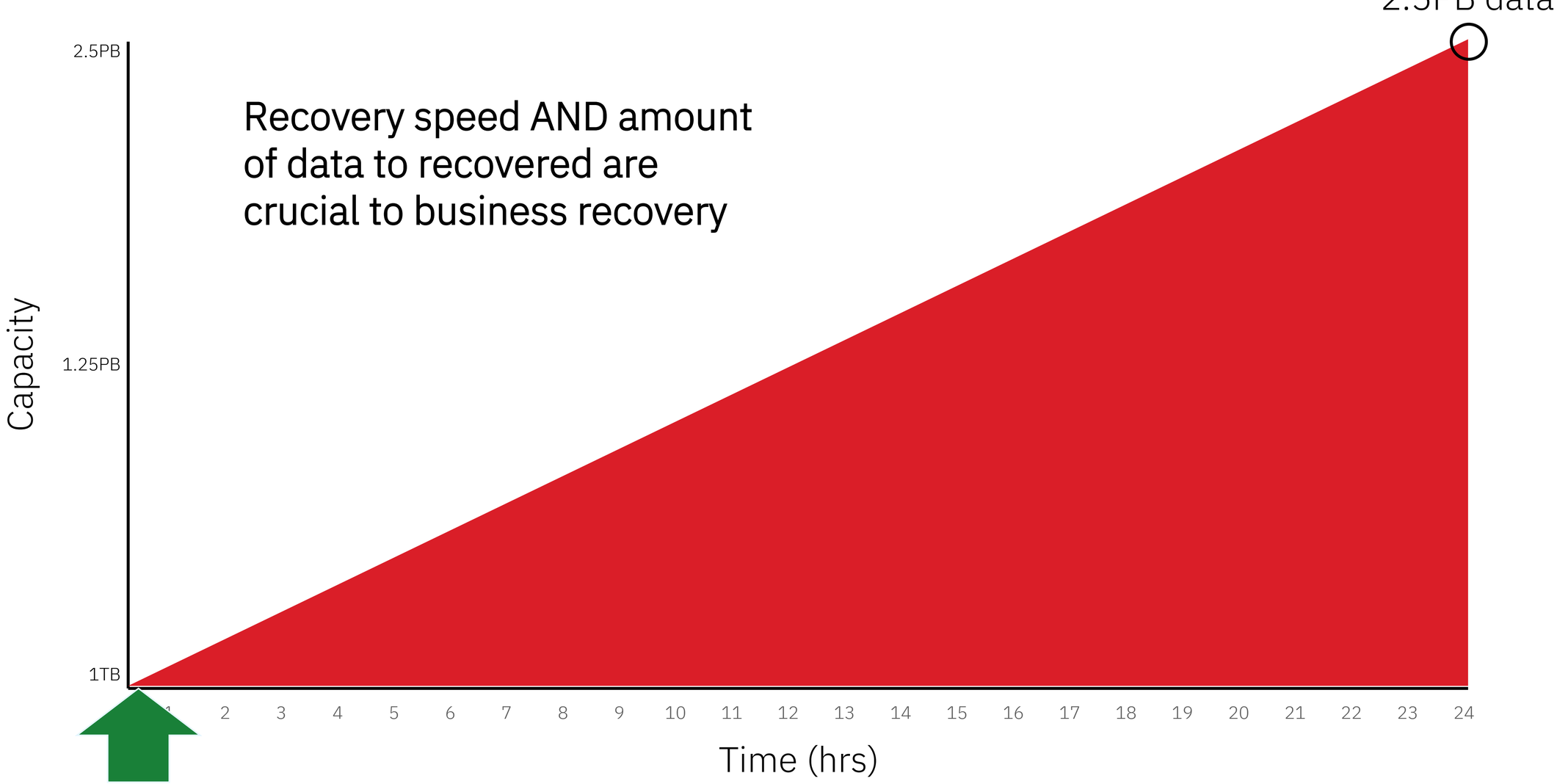
Full Company Recovery

All workloads including non-critical workloads for back-office etc.



What does good look like?

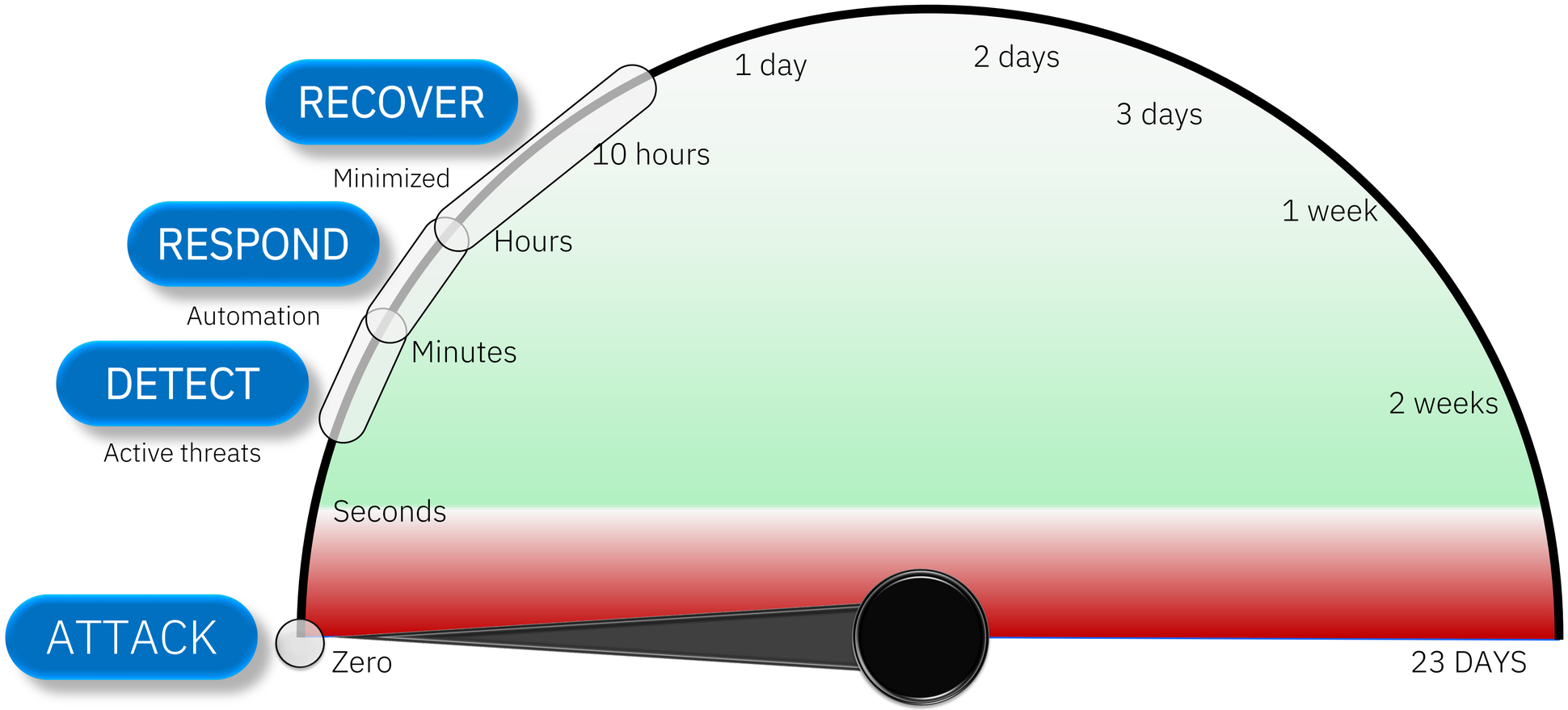
Data Encryption/Destruction over time



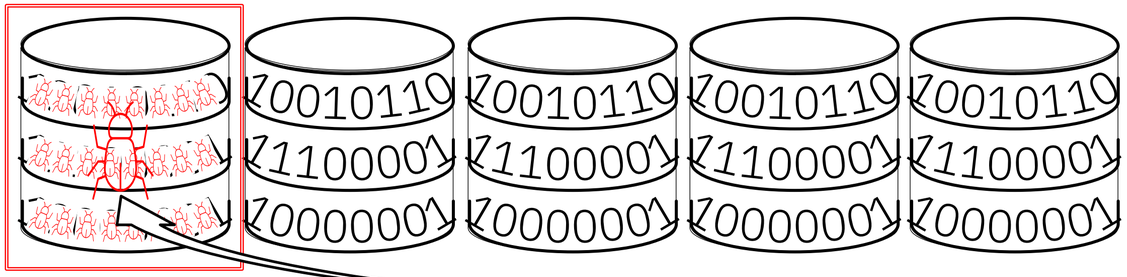
What if you knew the problem here?
Discover in <1 min,
only 1.7TB impacted

1.7TB will recover MUCH faster than 2.5PB

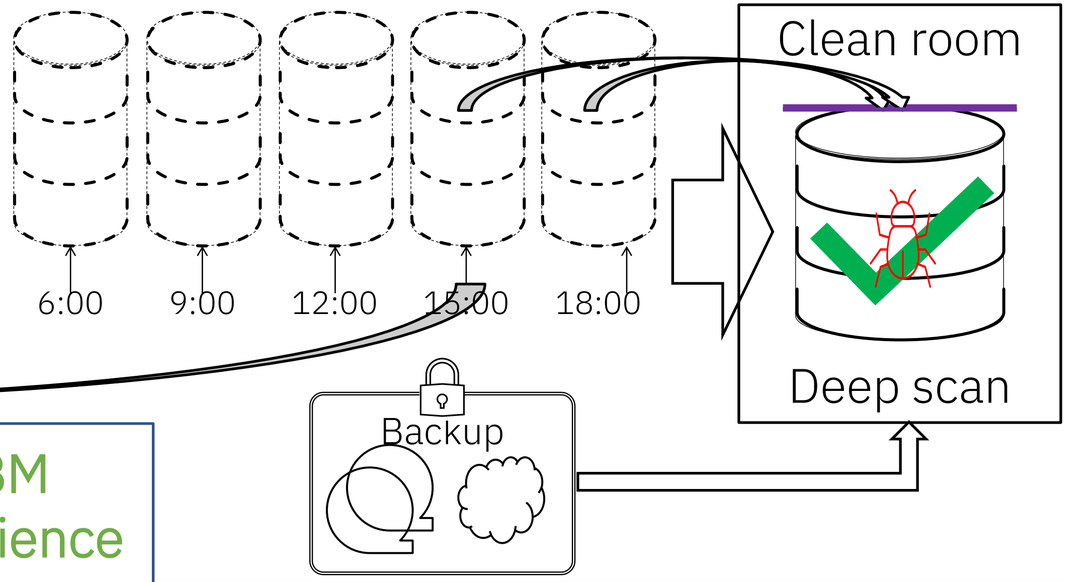
Prevent and minimize operational impacts



Production workloads



Secure immutable copies discovery scanning and clean room

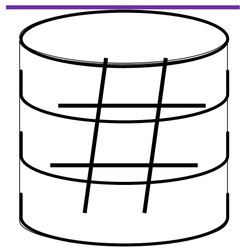


Disruption minimised rapid recovery

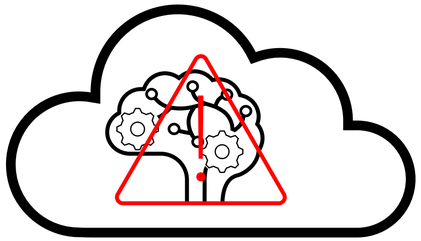
With IBM Data Resilience

Minimum Viable Company

Inline Data Corruption detection

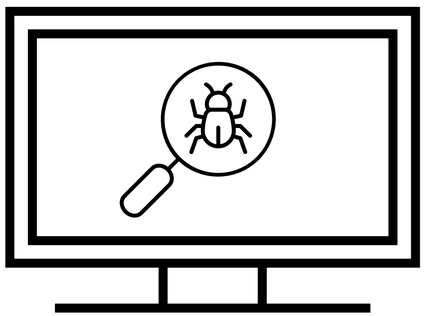


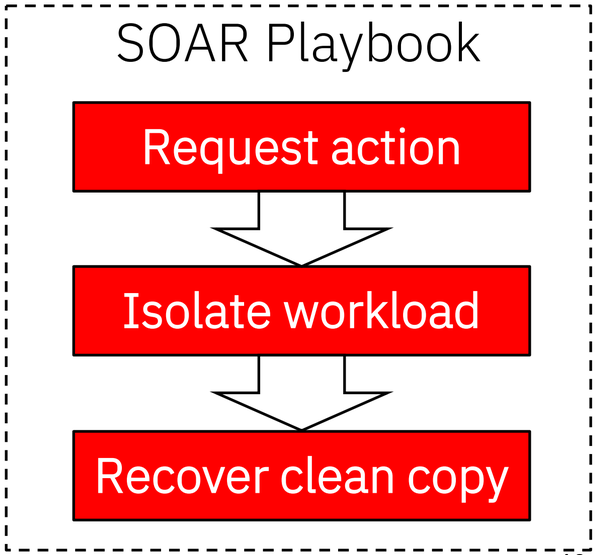
Metadata



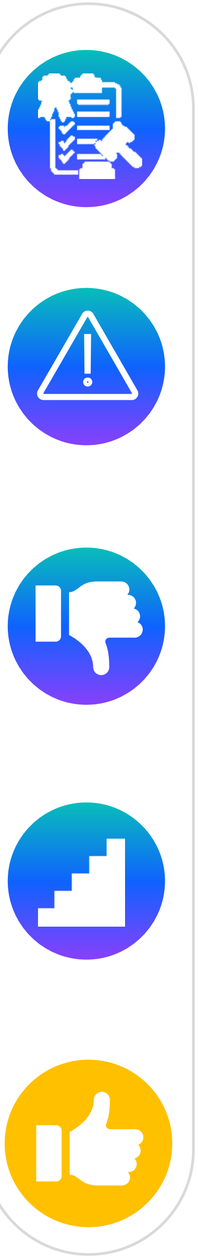
Machine Learning corruption detection

QRadar SOAR





Impact prevention & Recovery from Attacks



IBM Storage FlashSystem

Active threat Detection *Minimize Impact*

Detect in Seconds VM & Volume

Secure Copy *Assured Recovery*

On Array

Dormant threat detection *Prevention*

1 to many/ day

Recovery *Biz Impact Mitigation*

Vols in secs

Scan on recovery

Pre-attack performance

Automation & Threat Index *Simplicity*

IBM Storage Defender

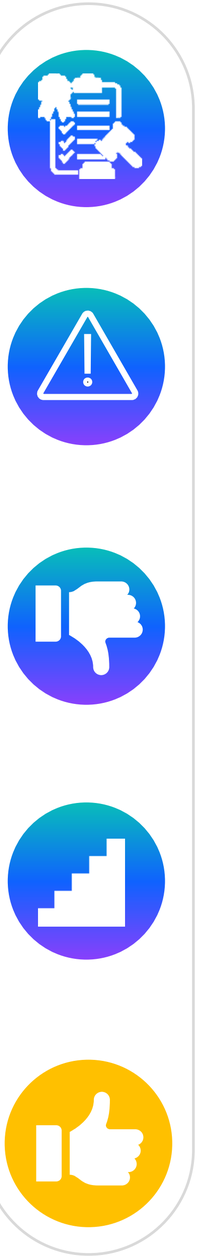
Biz recovery in mins to hrs

Security Tools Integration *Simplicity*

Consolidated Alerts

Increased Threat Intelligence

Impact prevention & Recovery from Attacks



IBM Defender Data Protect

Active threat Detection *Minimize Impact*	Secure Copy *Assured Recovery*	Dormant threat detection *Prevention*	Recovery *Biz Impact Mitigation*	Automation & Threat Index *Simplicity*	Security Tools Integration *Simplicity*
				IBM Storage Defender	
Detect in Seconds VM	On secondary	After backup + Repeated cycle	Instant Mass Restore k's of VMs Perf. compromise until vMotion	Biz recovery in hours	Consolidated Alerts Increased Threat Intelligence

Impact prevention & Recovery from Attacks

	Active threat Detection *Minimize Impact*	Secure Copy *Assured Recovery*	Dormant threat detection *Prevention*	Recovery *Biz Impact Mitigation*	Automation & Threat Index *Simplicity*	Security Tools Integration *Simplicity*
NON-IBM	After backup/ none	Copy On Secondary (not all secure)	Once after backup	Hours to weeks (instant up to 25VM's, 100's unavailable for hrs/days) Perf. compromise until restored to primary (hrs/days)	Biz recovery in days to weeks	Consolidated Alerts

Impact prevention & Recovery from Attacks

	Active threat Detection *Minimize Impact*	Secure Copy *Assured Recovery*	Dormant threat detection *Prevention*	Recovery *Biz Impact Mitigation*	Automation & Threat Index *Simplicity* (IBM Storage Defender)	Security Tools Integration *Simplicity*
IBM Storage FlashSystem	Detect in Seconds VM & Volume	On Array	1 to many/ day	Vols in secs Scan on recovery Pre-attack performance	Biz recovery in mins to hrs	Consolidated Alerts Increased Threat Intelligence
IBM Defender Data Protect	Detect in Seconds VM	On secondary	After backup + Repeated cycle	Instant Mass Restore k's of VMs Perf. compromise until vMotion	Biz recovery in hours	Consolidated Alerts Increased Threat Intelligence
NON-IBM	After backup/ none	Copy On Secondary (not all secure)	Once after backup	Hours to weeks (instant up to 25VM's, 100's unavailable for hrs/days) Perf. compromise until restored to primary (hrs/days)	Biz recovery in days to weeks	Consolidated Alerts with some