tierpoint

SECUR-SERV

Future OPS 2025

Disaster Recovery

An update…

Mike Sander

Sr. Solutions Engineer – TierPoint – Omaha

How Has Disaster Recovery Evolved?

BEFORE

A few critical apps

9-5 interactions with customers

Business could run on paper

Tolerance for downtime

NOW

All apps are important

Customers expect a 24/7 experience

Applications are the business

Image is everything

Complex compliance requirements

Increase in Cyber Breaches

Critical Challenges of Business Availability

Evolving Threat Landscape

85% had at least one ransomware attack last year
93% of attacks attempted to destroy backup data
75% of backup repositories were affected

Data Availability, Protection & Recovery

93% suffered data-related disruptions
85% recognize an availability gap
76% experiencing a protection gap

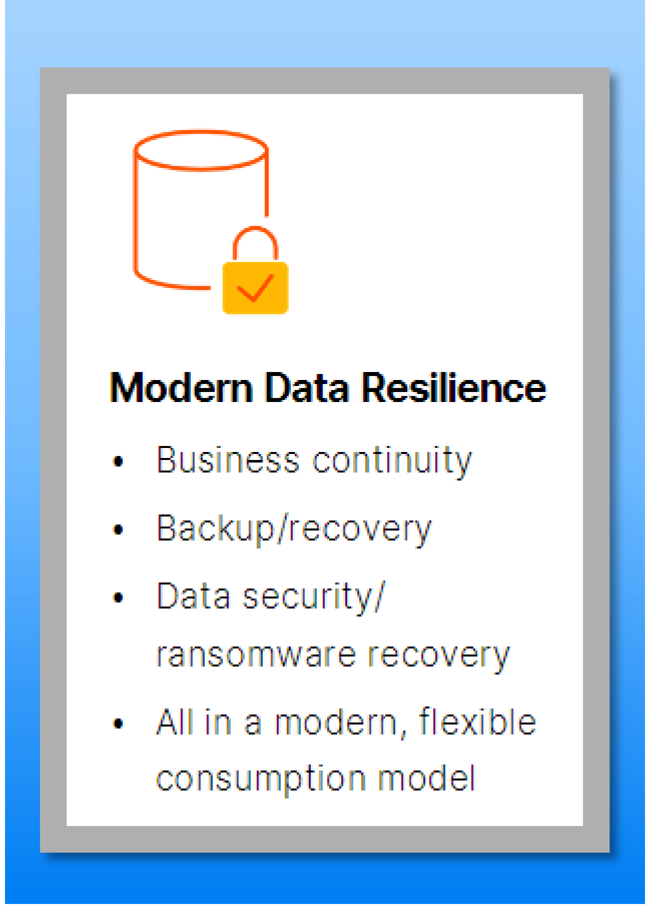
IT Modernization, Complexity & Compliance

92% increasing data protection budgets
70% cloud environments now employ managed AI services
74% will use cloud powered services by 2025

The Need for Rapid, Reliable Recovery

Success requires expanding data protection efforts to focus on fast and reliable recovery, including:

- **Detection:** Rapidly identifying and responding to anomalies and security intrusions
- **Protection:** Creating and maintaining clean, **immutable** copies of essential data
- **Recovery:** Quickly getting essential data and applications back into the hands of the business



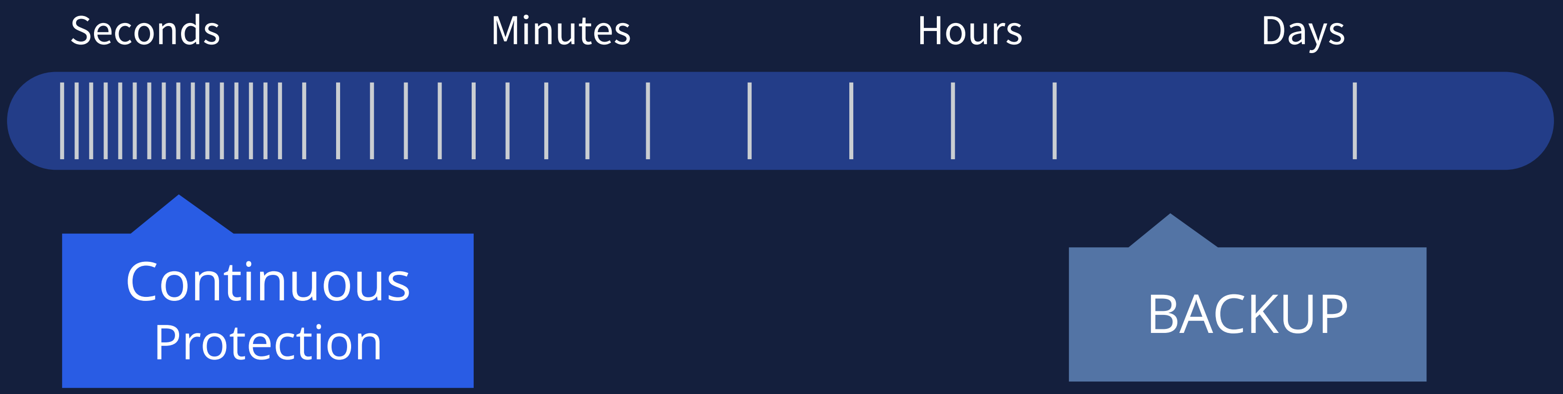
Modern Data Resilience

- Business continuity
- Backup/recovery
- Data security/ ransomware recovery
- All in a modern, flexible consumption model

REPLICATE AND DETECT
ISOLATE AND LOCK
TEST AND RECOVER

Continuous Protection and Layered Detection

Detect at the point of encryption, not just after backing up



Seconds

Minutes

Hours

Days

Continuous Protection

BACKUP

Continuous Data Protection = Lower RPO and RTO

Real-time Detection = Lower MTTI and MTTC

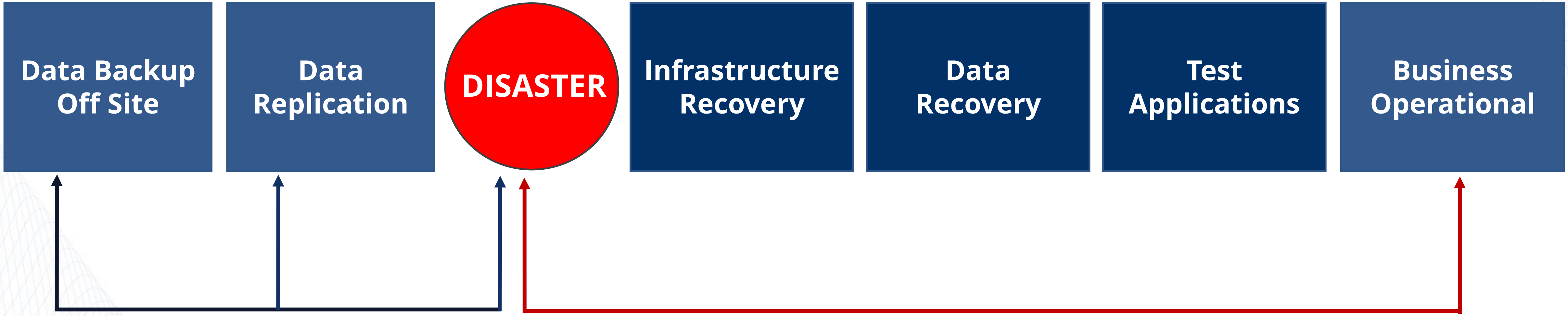
Recovery Timeline

BUSINESS CONTINUITY

A plan encompassing people, processes, procedures and systems to ensure mission-critical functions can resume during and after a crisis

DISASTER RECOVERY

Specific steps taken to get mission-critical systems and data back up and running as quickly as possible. A key part of a strong business continuity plan



Data Backup Off Site

Data Replication

DISASTER

Infrastructure Recovery

Data Recovery

Test Applications

Business Operational

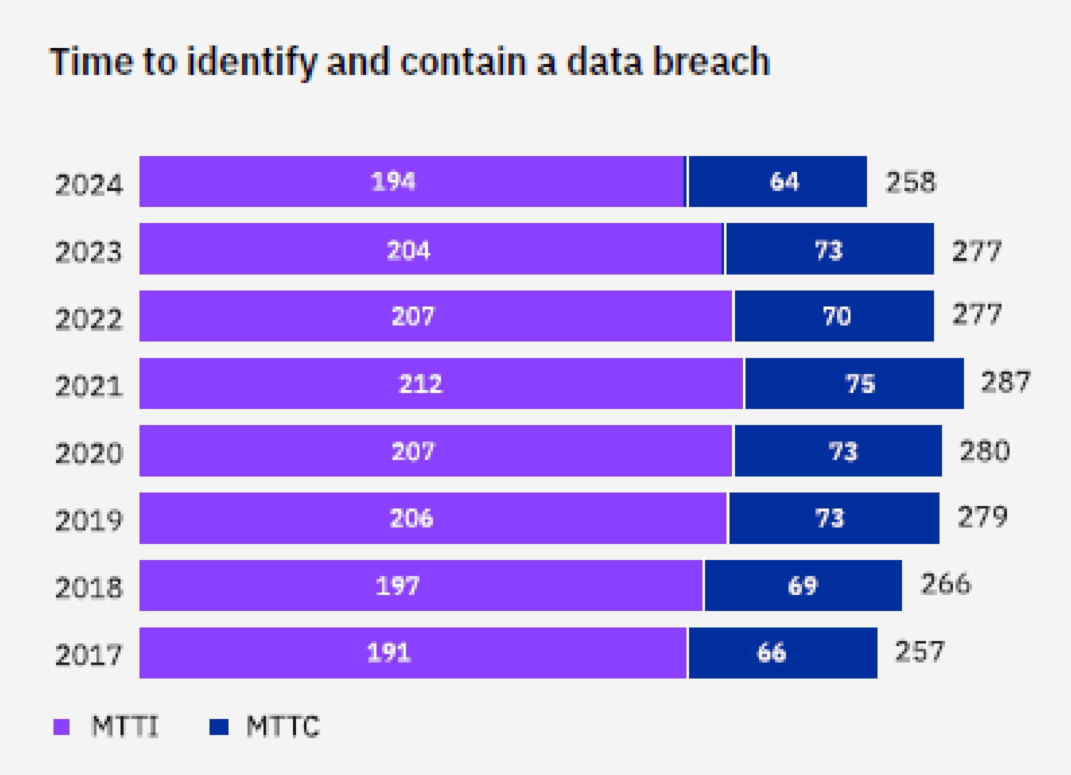
Recovery Point Objective (RPO)

Recovery Time Objective (RTO)

RPO = how much data can you afford to lose?

RTO = how long can you be down?

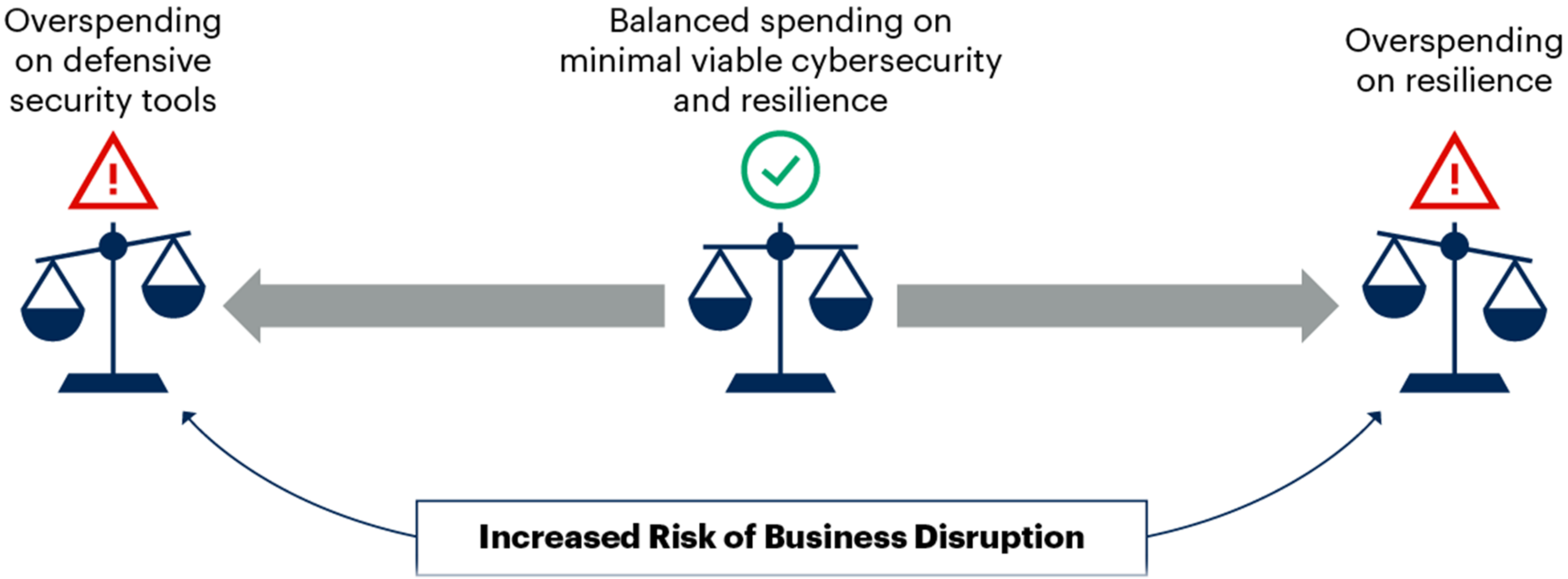
Some Global Data



Time to identify and contain a data breach

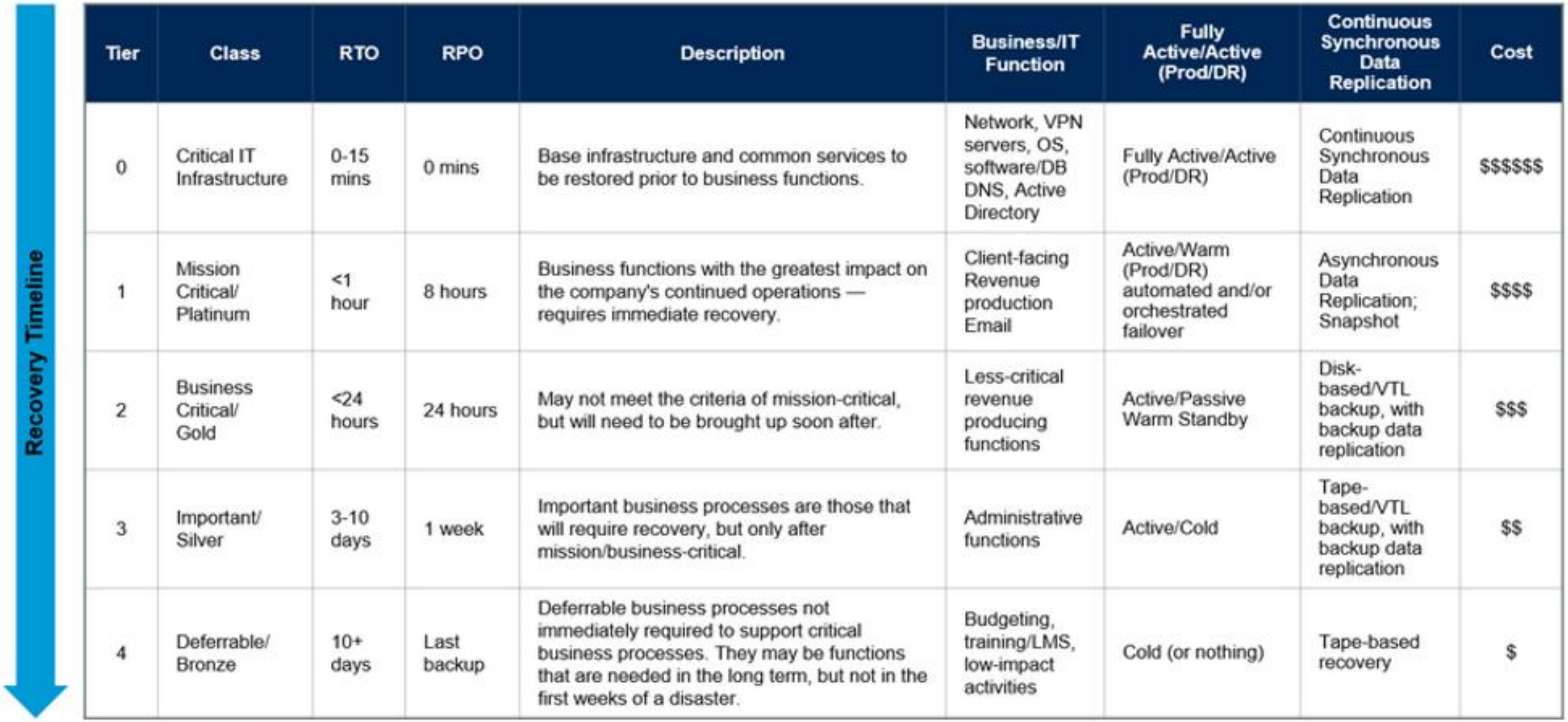
Source – IBM Cost of a Data Breach Report 2024

Maintain a Balanced Approach with Defense and Resilience


Overspending on defensive security tools
Balanced spending on minimal viable cybersecurity and resilience
Overspending on resilience
Increased Risk of Business Disruption

© TierPoint

Strategic Approach to Recovery Tiering



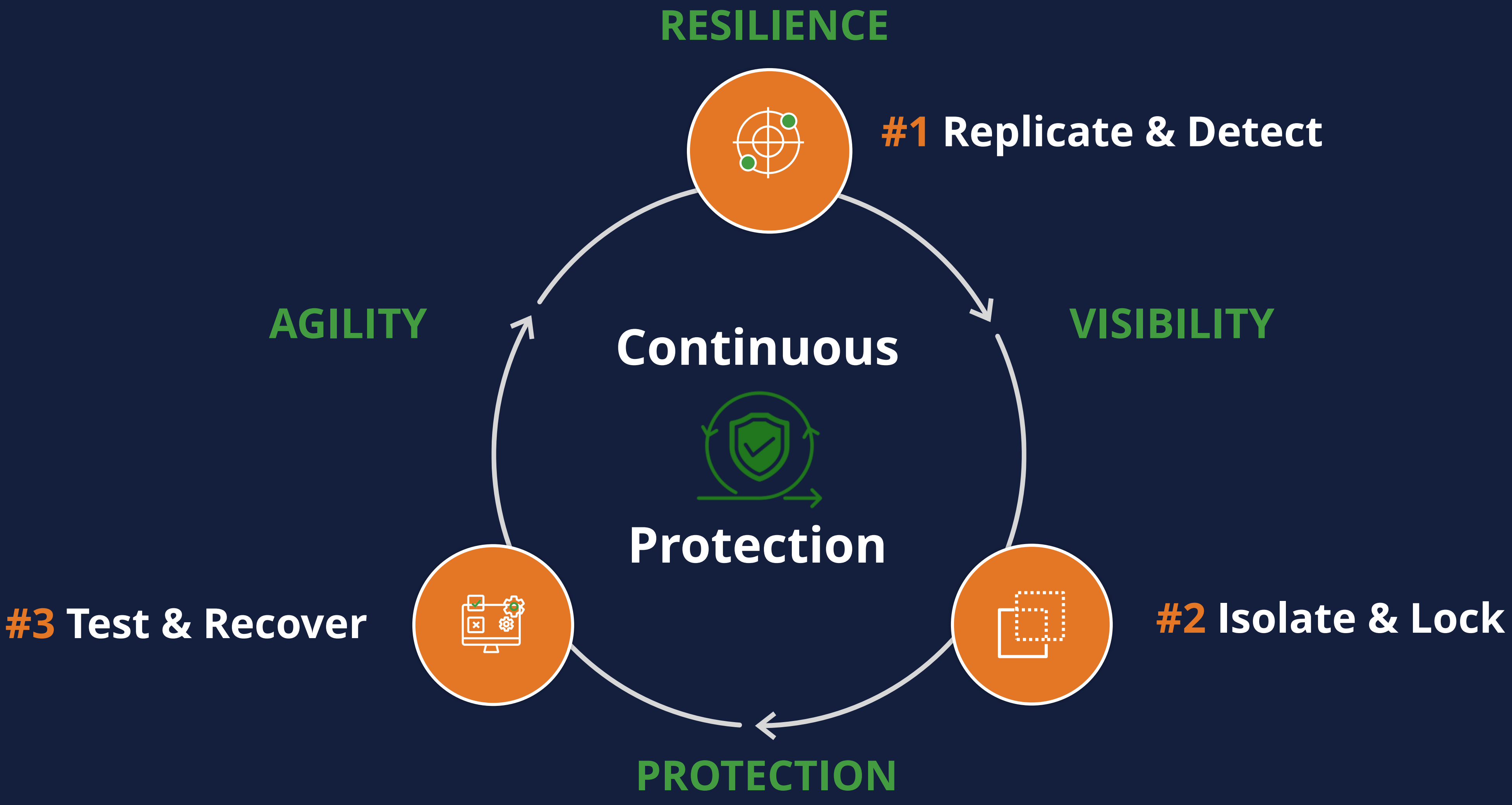
Recovery Timeline

Tier	Class	RTO	RPO	Description	Business/IT Function	Fully Active/Active (Prod/DR)	Continuous Synchronous Data Replication	Cost
0	Critical IT Infrastructure	0-15 mins	0 mins	Base infrastructure and common services to be restored prior to business functions.	Network, VPN servers, OS, software/DB DNS, Active Directory	Fully Active/Active (Prod/DR)	Continuous Synchronous Data Replication	$$$$$$
1	Mission Critical/ Platinum	<1 hour	8 hours	Business functions with the greatest impact on the company's continued operations — requires immediate recovery.	Client-facing Revenue production Email	Active/Warm (Prod/DR) automated and/or orchestrated failover	Asynchronous Data Replication; Snapshot	$$$$
2	Business Critical/ Gold	<24 hours	24 hours	May not meet the criteria of mission-critical, but will need to be brought up soon after.	Less-critical revenue producing functions	Active/Passive Warm Standby	Disk-based/VTL backup, with backup data replication	$$$
3	Important/ Silver	3-10 days	1 week	Important business processes are those that will require recovery, but only after mission/business-critical.	Administrative functions	Active/Cold	Tape-based/VTL backup, with backup data replication	$$
4	Deferrable/ Bronze	10+ days	Last backup	Deferrable business processes not immediately required to support critical business processes. They may be functions that are needed in the long term, but not in the first weeks of a disaster.	Budgeting, training/LMS, low-impact activities	Cold (or nothing)	Tape-based recovery	$

Source: Gartner (February 2020)
ID: 465090_C

Gartner

Resilience with Data Protection



RESILIENCE

#1 Replicate & Detect

VISIBILITY

#2 Isolate & Lock

PROTECTION

#3 Test & Recover

AGILITY

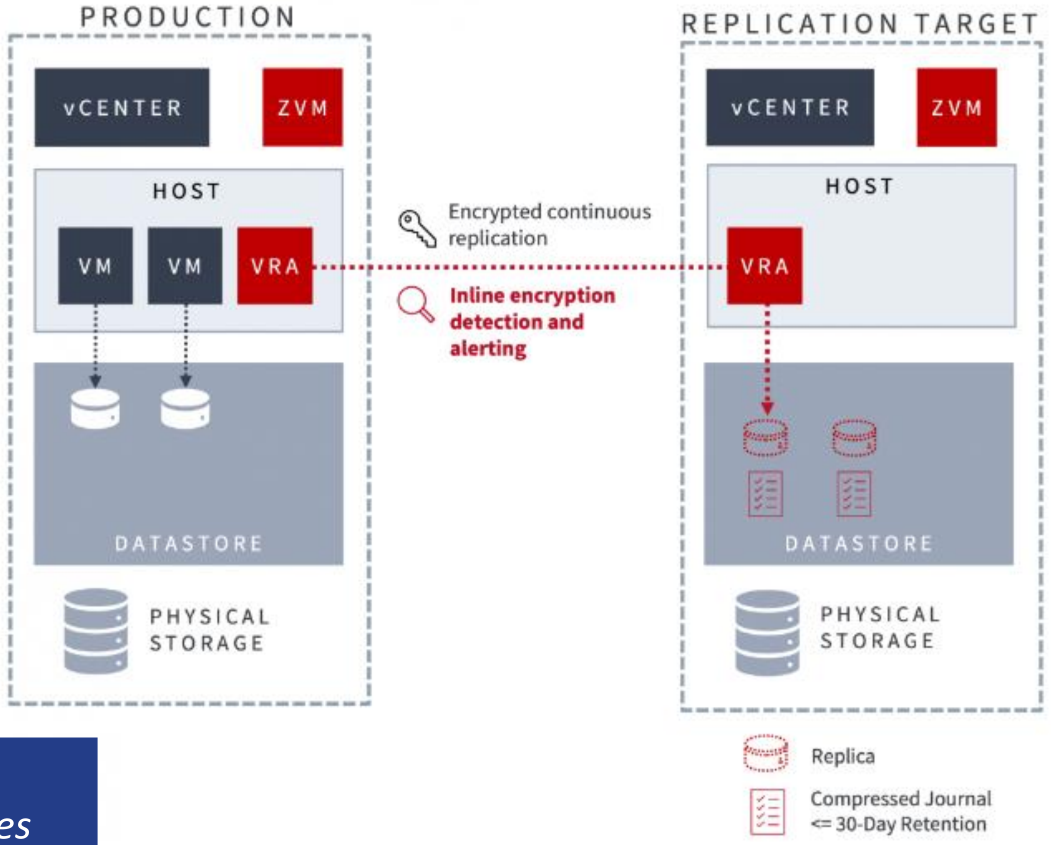
Continuous Protection

© TierPoint

Real-time Encryption Detection for Ransomware

How it works

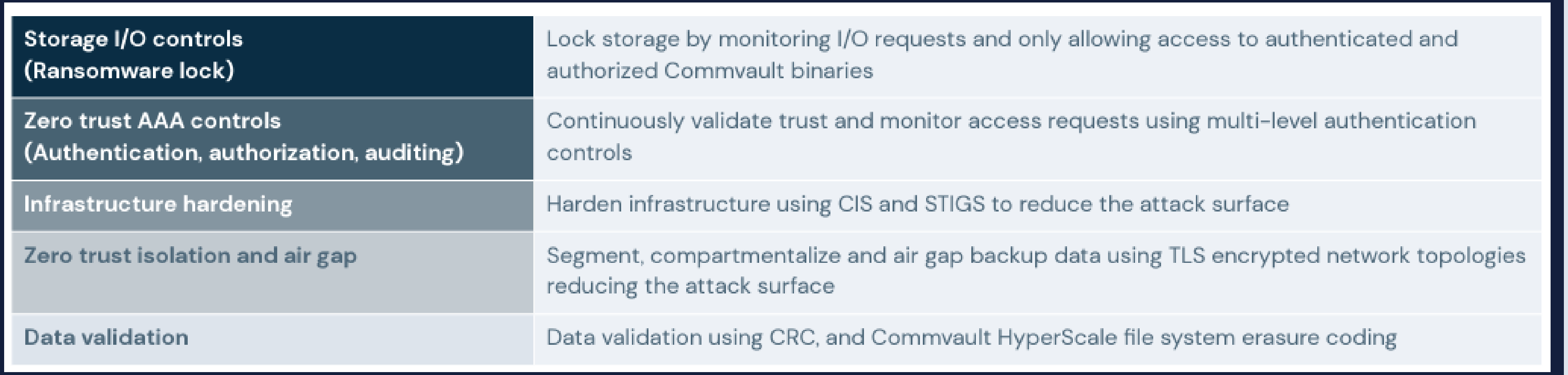
1. Zerto's Encryption Analyzer monitors VMs' write activities in real-time.
2. An alert is triggered upon detecting abnormal encryption patterns.
3. Checkpoints in the Zerto journal aid in identifying recovery points before and after anomalies.
4. The process involves grading suspicion levels (1: low, 2: high).
5. Two tagged checkpoints are generated: one marking detection and another as a safe restoration point.
6. Users can manage recovery or dismiss alerts based on investigation results.



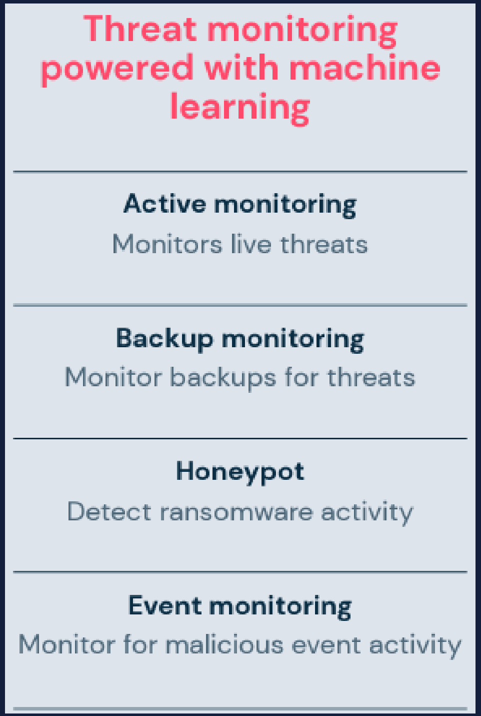
> *"Zerto's real-time encryption detection puts us in a much stronger position to both identify and mitigate ransomware attacks. This gives us confidence that we can proactively meet the risks presented by ransomware."*
> *– Network admin at manufacturing customer*

Commvault’s Immutable Infrastructure Architecture

Employs a multi-layered approach (five layers) to ensure data is safe



Storage I/O controls (Ransomware lock)	Lock storage by monitoring I/O requests and only allowing access to authenticated and authorized Commvault binaries
Zero trust AAA controls (Authentication, authorization, auditing)	Continuously validate trust and monitor access requests using multi-level authentication controls
Infrastructure hardening	Harden infrastructure using CIS and STIGS to reduce the attack surface
Zero trust isolation and air gap	Segment, compartmentalize and air gap backup data using TLS encrypted network topologies reducing the attack surface
Data validation	Data validation using CRC, and Commvault HyperScale file system erasure coding



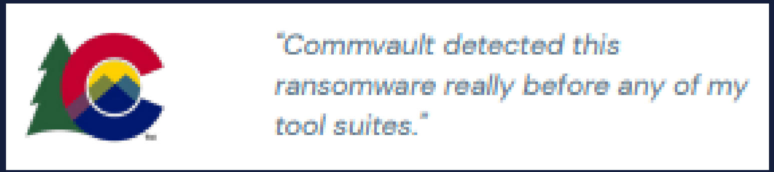
Threat monitoring powered with machine learning

Active monitoring
Monitors live threats

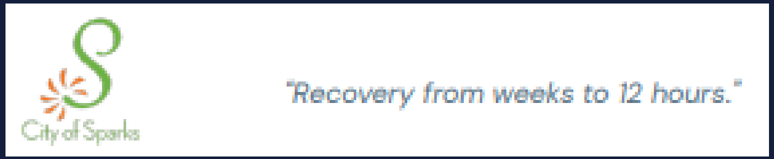
Backup monitoring
Monitor backups for threats

Honeypot
Detect ransomware activity

Event monitoring
Monitor for malicious event activity



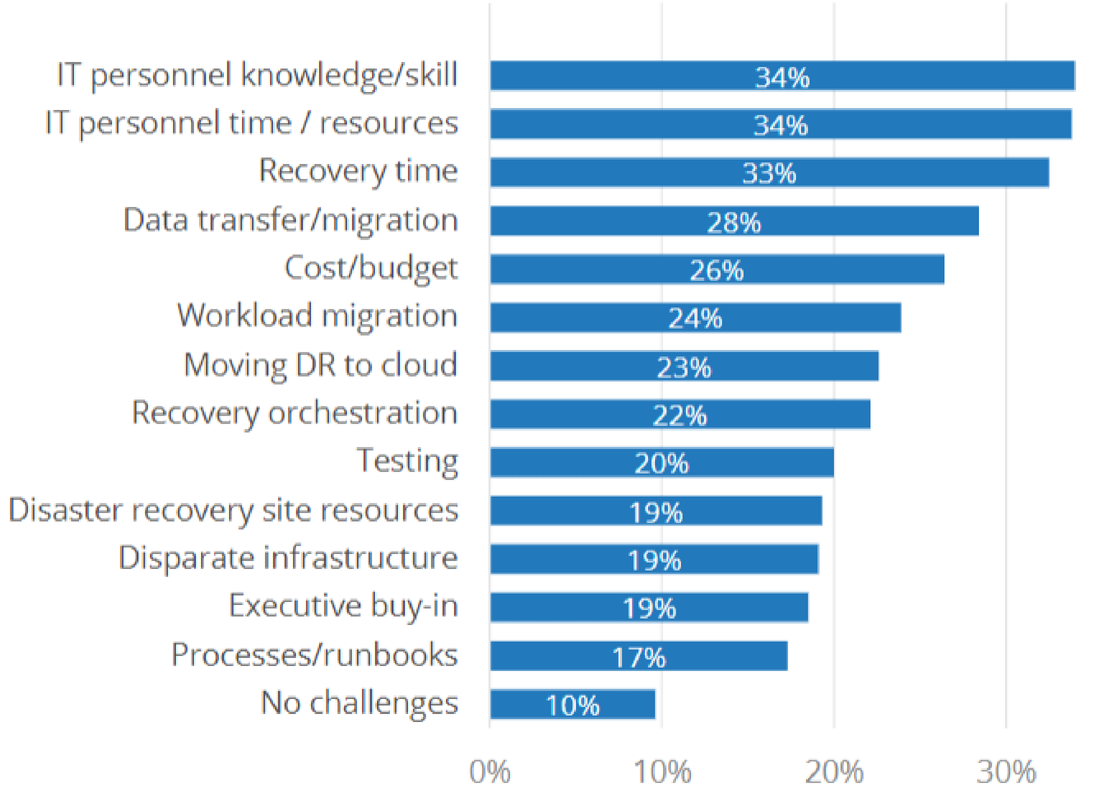
"Commvault detected this ransomware really before any of my tool suites."


City of Sparks

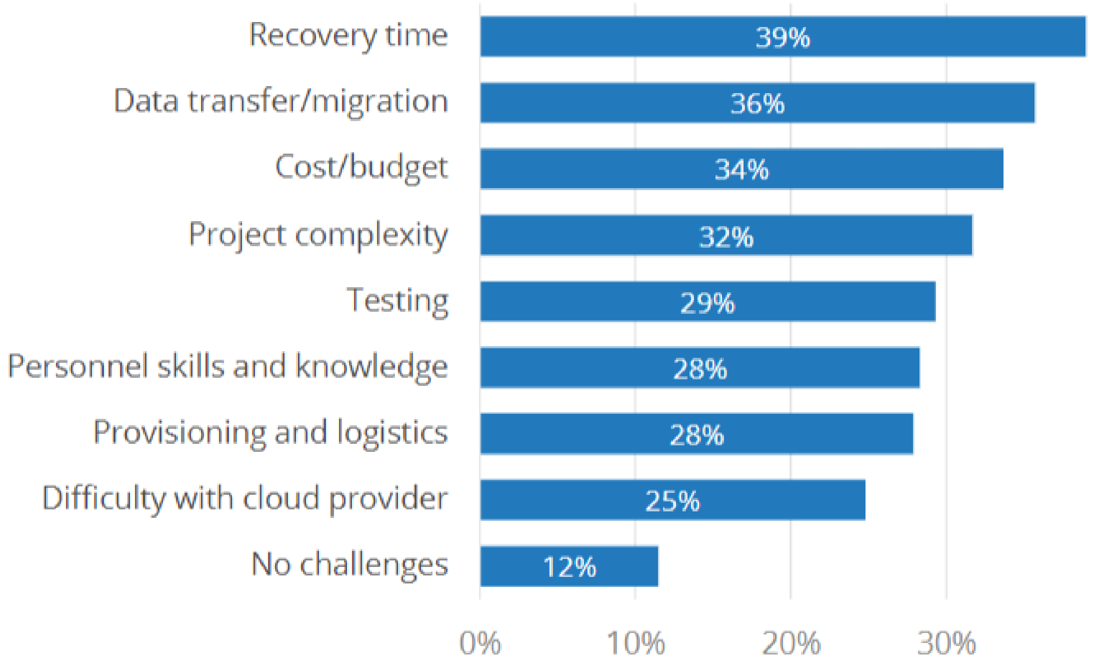
"Recovery from weeks to 12 hours."

Biggest Disaster Recovery Challenges

IT personnel skills is the #1 challenge for DR overall.



Recovery time is the #1 for DR in the cloud.



TierPoint DRaaS Strategy

Primary Site

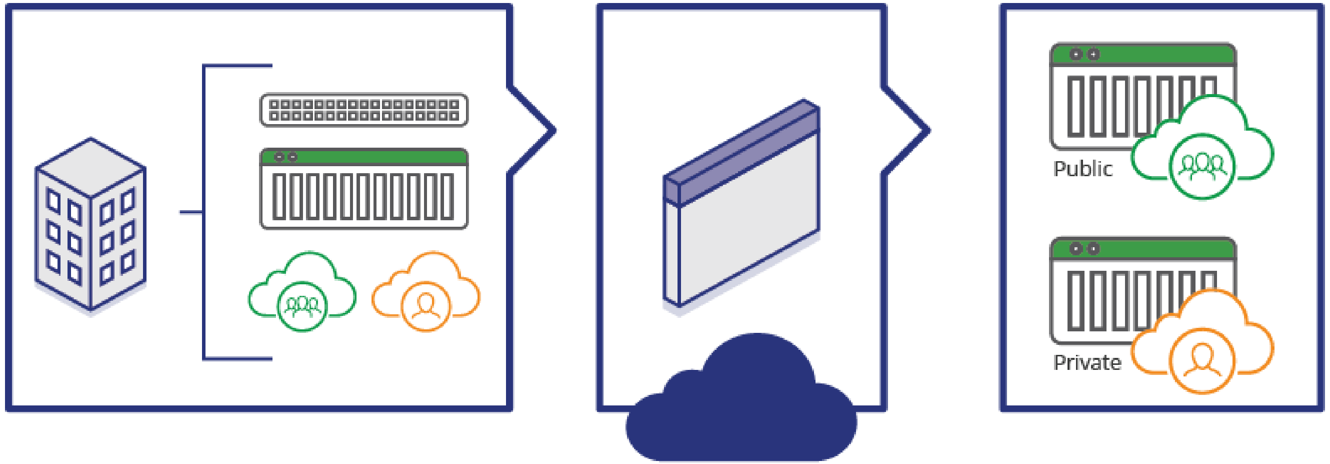
TierPoint protects systems at the customer premise, in the TierPoint Data Center and/or Public/Private Cloud.

Replication to Cloud

Data and applications are replicated to the cloud.

Recovery Site

Protected servers, applications and data are ready and available in minutes

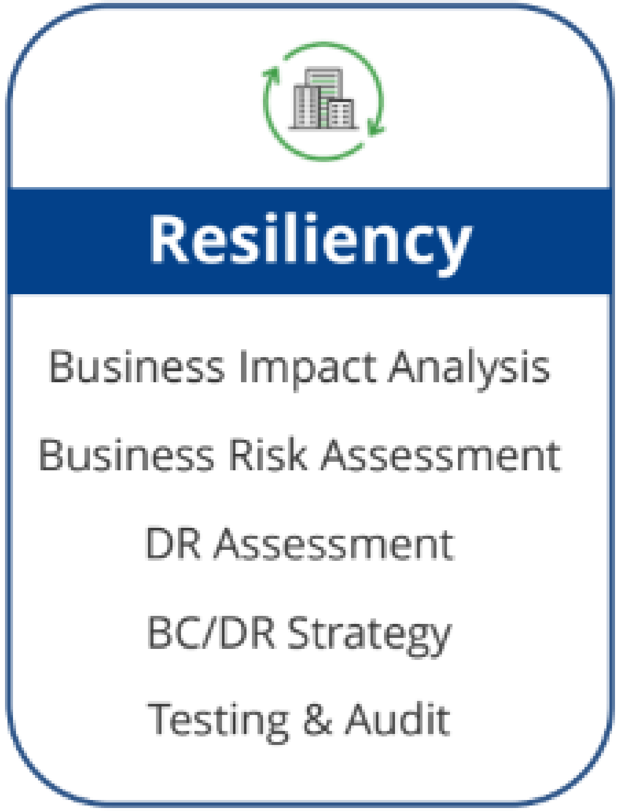


Core Offerings:

- Cloud to cloud recovery to managed infrastructure
  - Zerto
  - ASR
  - SRM
- IBM recovery services; iSeries/Unix/Mainframe, AIX Recovery

Zerto vmware ZPX CLOUD Tectrade A CSI GROUP COMPANY CloudFirst

Professional Services



Resiliency

Business Impact Analysis

Business Risk Assessment

DR Assessment

BC/DR Strategy

Testing & Audit

TierPoint Catalog

Cloud Services

- Public Cloud
- Private Cloud
- Multitenant Cloud
- Cloud Connectivity
- Hybrid Cloud

Security Services

- XDR
- Firewall
- AV
- MFA
- Compliance

Storage

- Shared
- Dedicated
- Healthcare Imaging

Disaster Recovery

- Cloud-based DRaaS
- Backup as a Service

Data Center Services

- Colocation; Standard & High-Density
- Remote Hands
- Network Services
- Business Continuity Seating

Managed Services

- Microsoft 365
- OS & Database Management
- IBM Power & Mainframe
- Help Desk Services

Advisory/Consulting

- Cloud, Security, and Business Continuity Consulting
- Advanced Public Cloud Services including App Modernization, Data & Analytics, and DevOps

Key Technology Partners

aws COMMVAULT DELL Technologies FORTINET PLATINUM PARTNER Microsoft PURESTORAGE vmware by Broadcom Zerto a Hewlett Packard Enterprise company