Srihari Pakalapati

Trader Interactive

Ransomware Readiness: Backup and Recovery in the Cloud

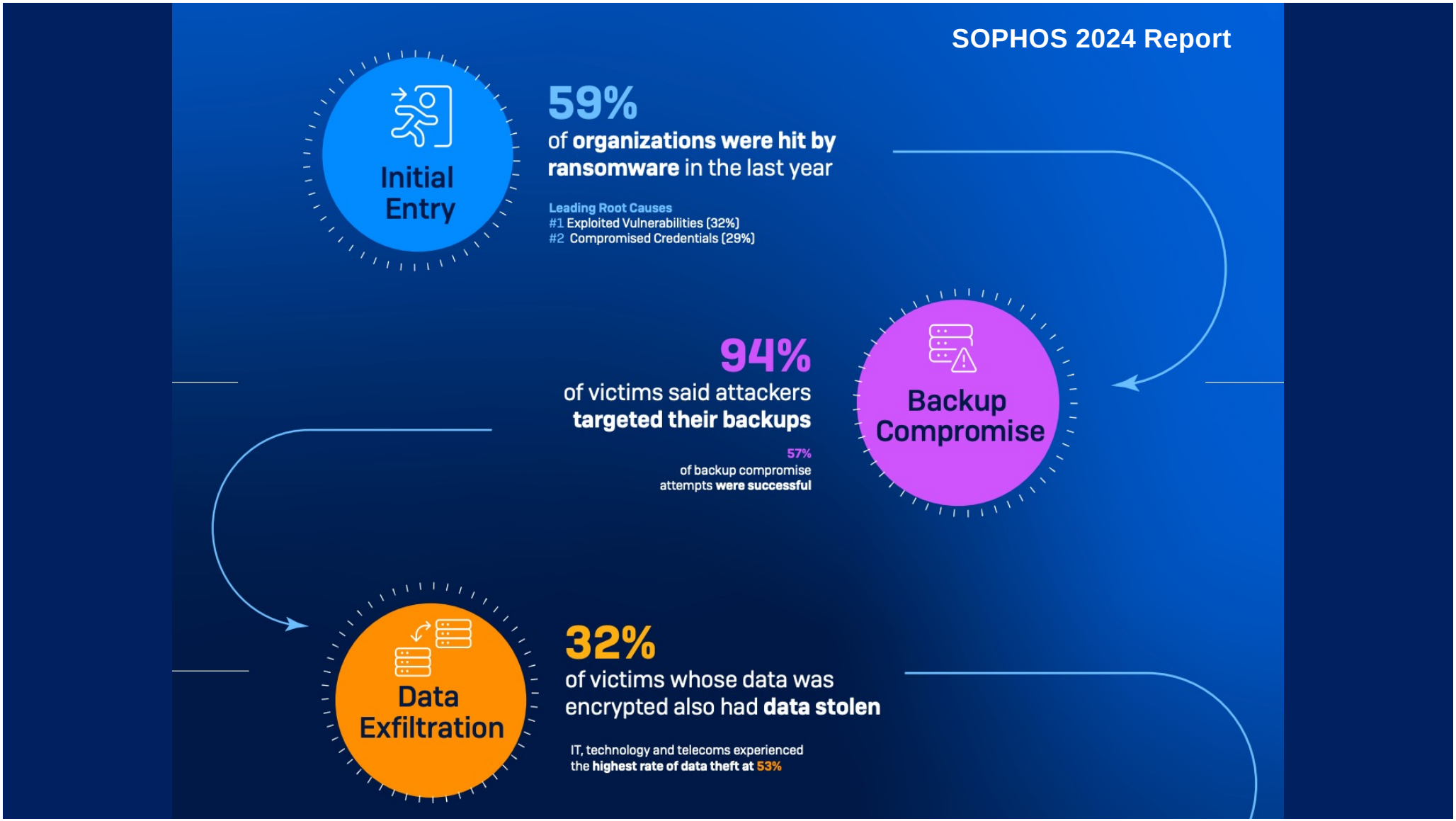
Conf42 Site Reliability Engineering (SRE)
April 17 2025 • Online

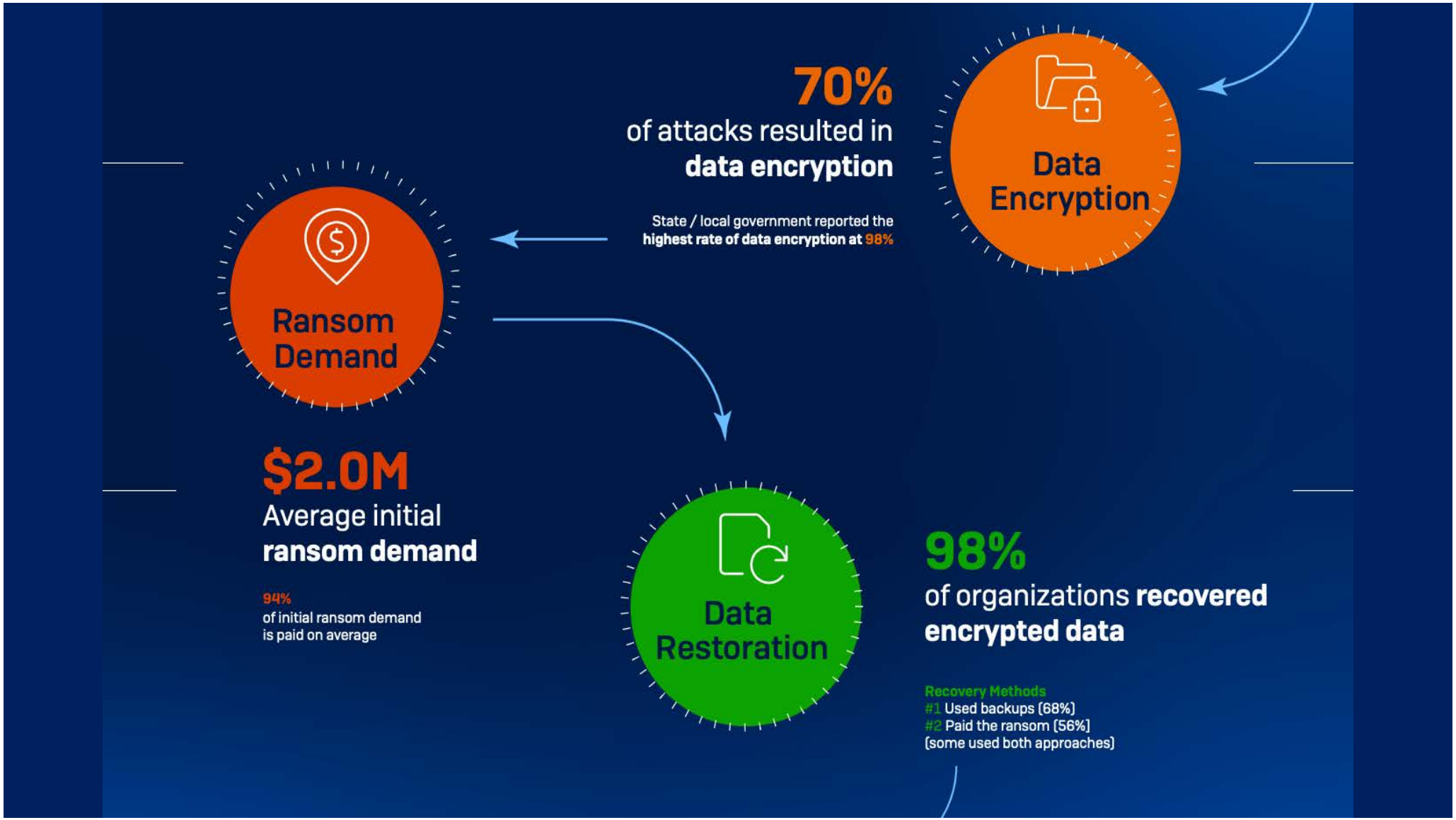
CONF42

What is ransomware?


Ooops, your files have been encrypted!
English
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
Payment will be raised on
Time Left
02:23:30:20
Your files will be lost on
Time Left
06:23:30:20
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin
ACCEPTED HERE
Send $300 worth of bitcoin to this address:
13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94
Copy
Check Payment
Decrypt

SOPHOS 2024 Report



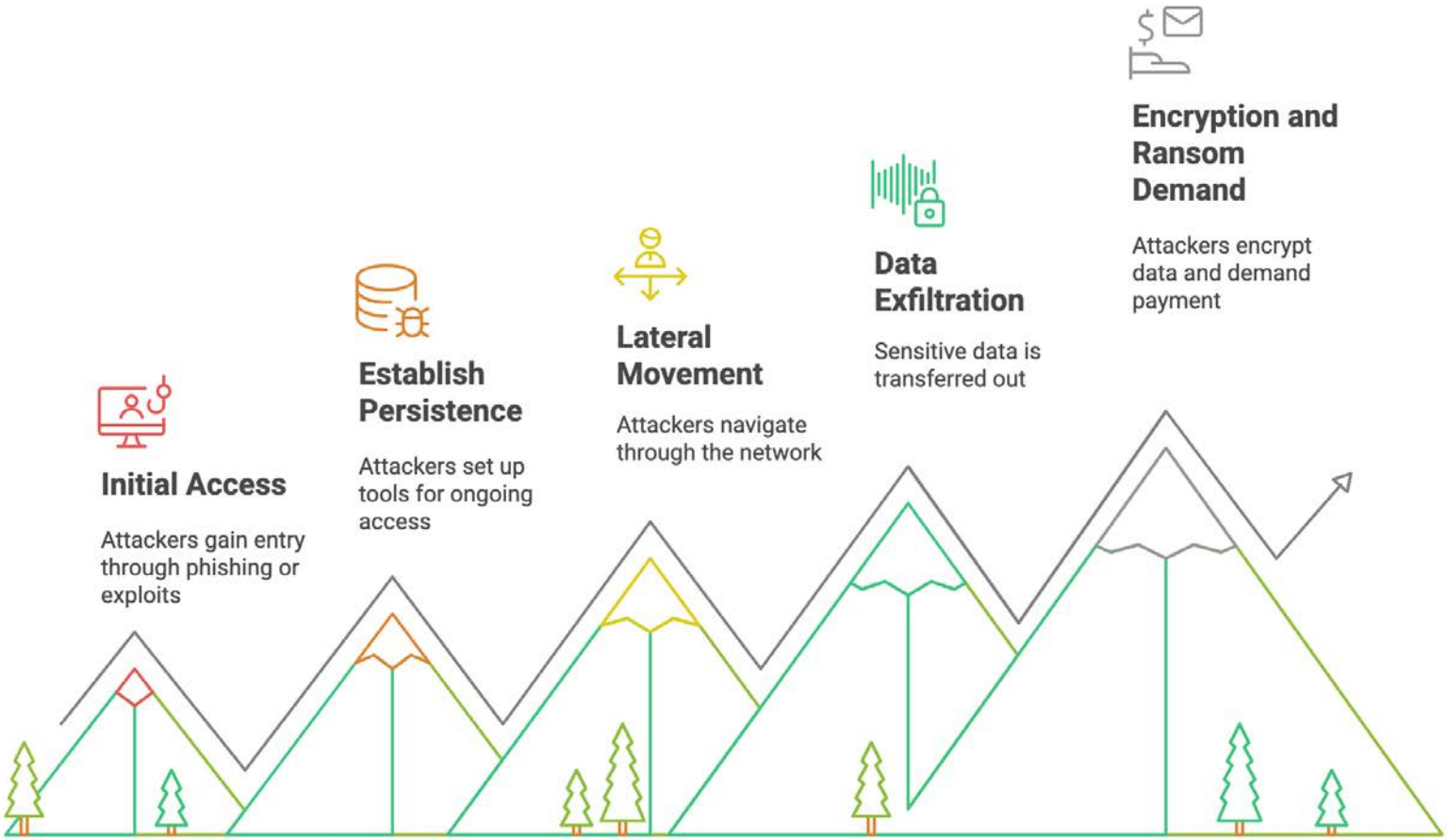

70%
of attacks resulted in
data encryption
State / local government reported the
highest rate of data encryption at 98%
Data Encryption
Ransom Demand
$2.0M
Average initial
ransom demand
94%
of initial ransom demand
is paid on average
Data Restoration
98%
of organizations recovered
encrypted data
Recovery Methods
#1 Used backups (68%)
#2 Paid the ransom (56%)
(some used both approaches)

$2.73M

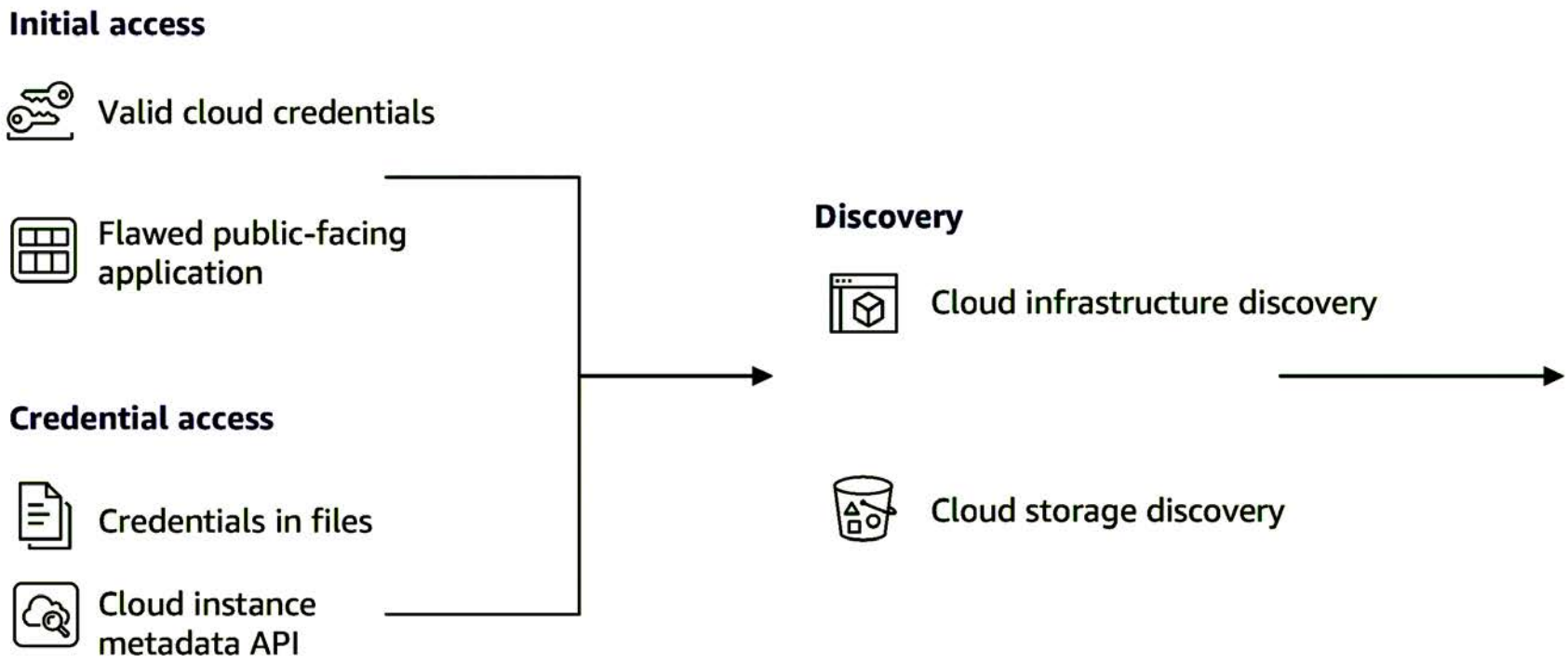
Average recovery cost (excl. ransom payment)

34%
of organizations **took more than a month** to recover

Ransomware Landscape



Event chain


Initial access
Valid cloud credentials
Flawed public-facing application
Credential access
Credentials in files
Cloud instance metadata API
Discovery
Cloud infrastructure discovery
Cloud storage discovery

Event chain

		Impact
→	Data destruction	Object deletion Snapshot deletion
→	Data exfiltration	Snapshot sharing Object download
→	Data encryption	Database tables File system

Attack Scenarios

Data Encryption

Attackers lock down critical files.

System Disruption

Operational systems are rendered unusable.

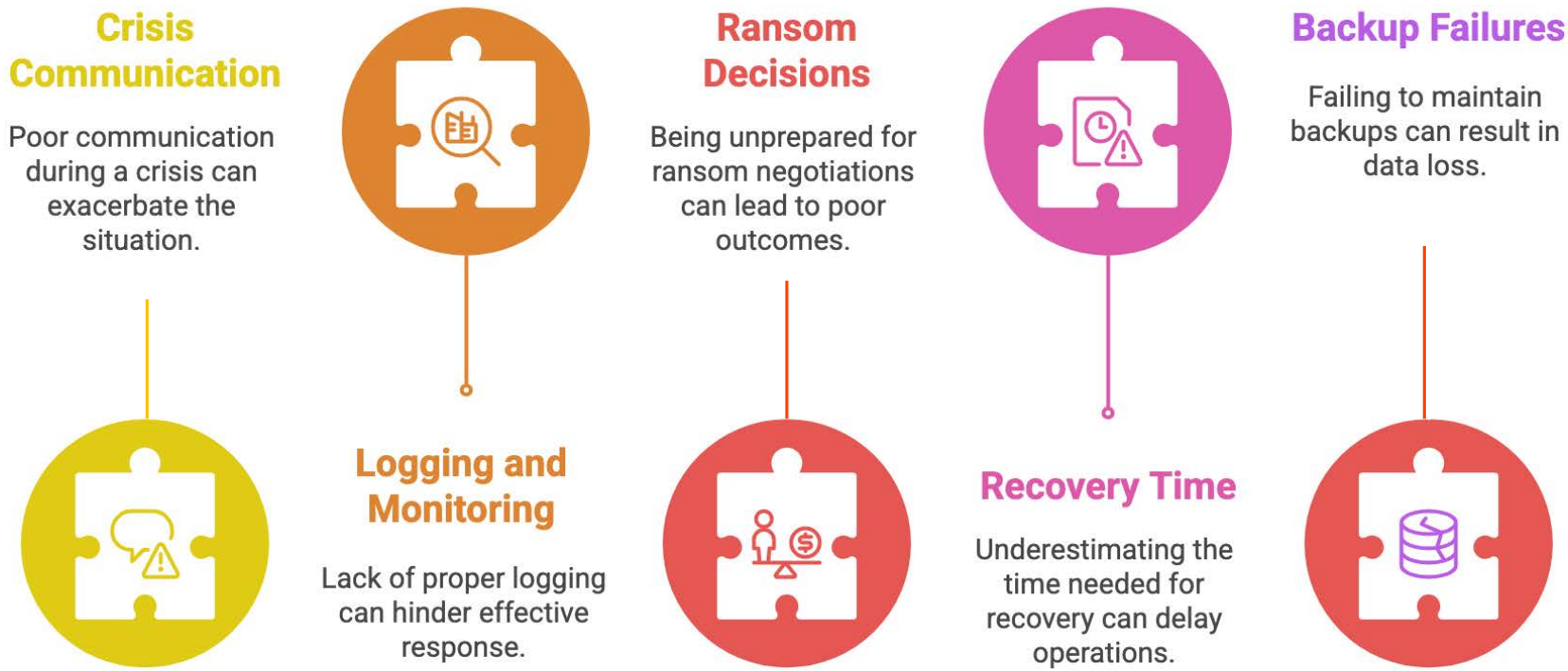
Data Exfiltration

Sensitive data is stolen before encryption.

Extortion Demands

Payment deadlines are enforced with threats of public data leaks.

Common pitfalls in Ransomware Response



How to Optimize Recovery Strategy?

Determining your recovery objectives: RPO & RTO

How much data can you afford to recreate or lose?

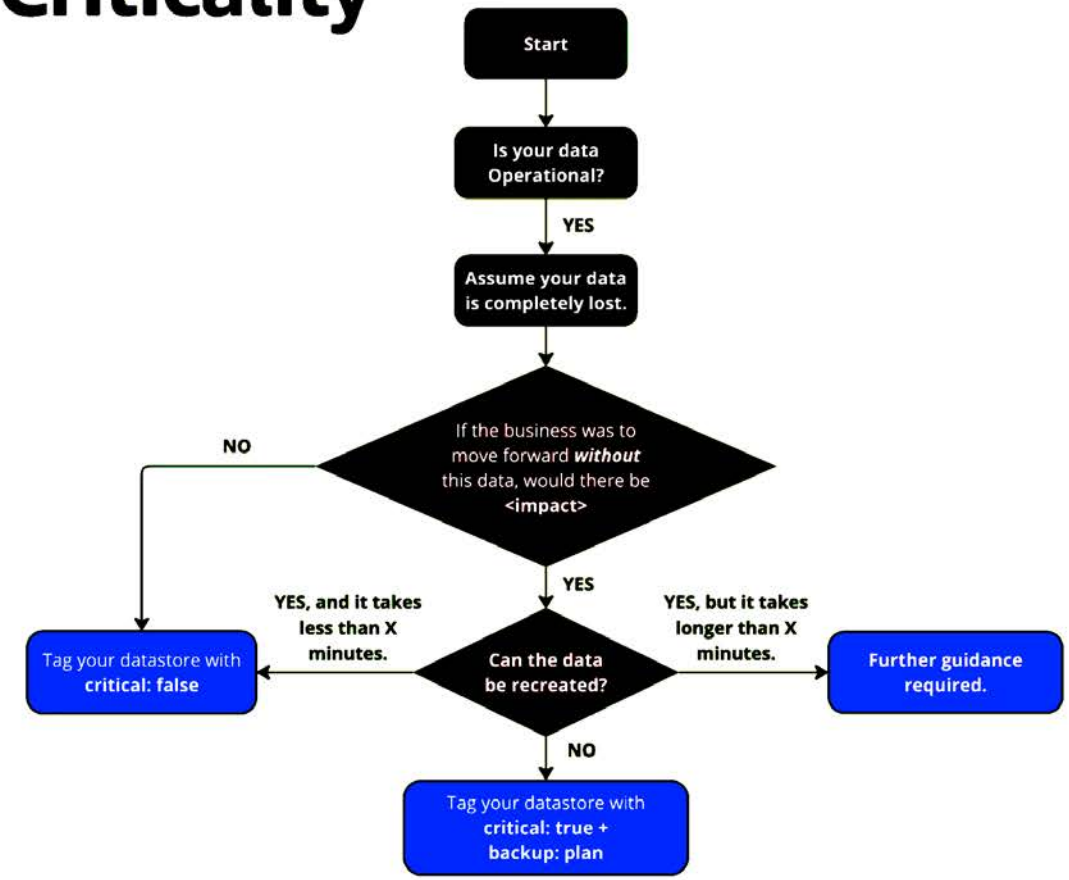
How quickly must you recover? What is the cost of downtime?

Discovery, Ownership + Criticality

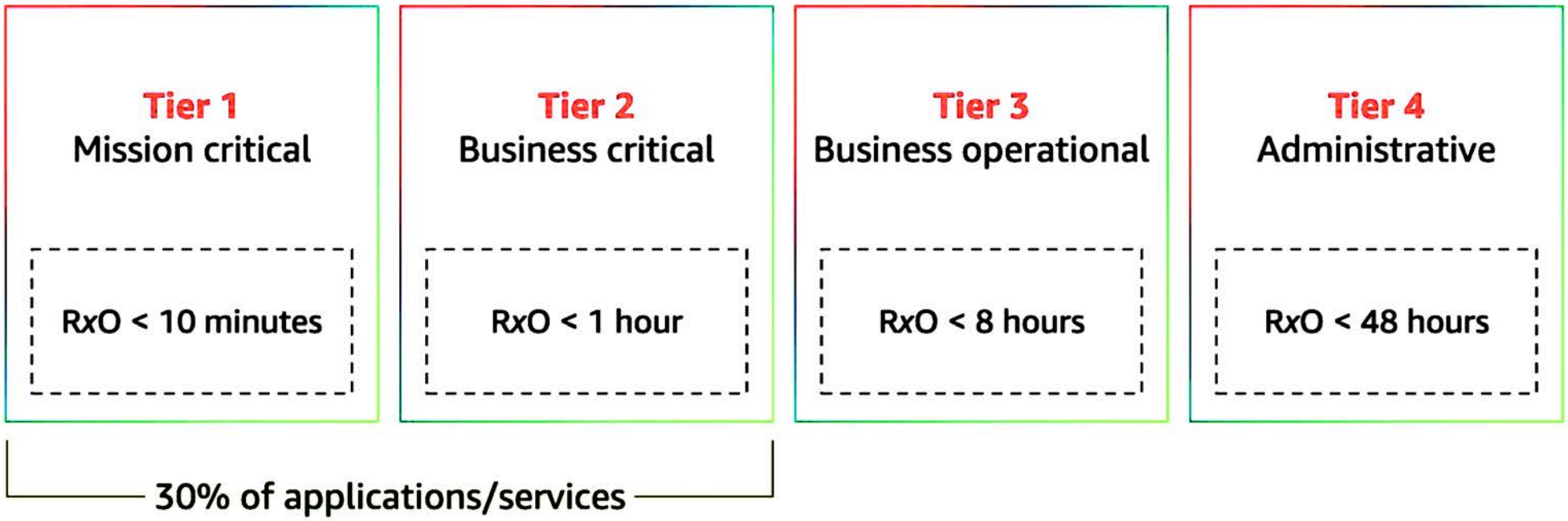
Understand
what type of data you have,
who owns it,
and if it is critical for your business.

What does critical mean?

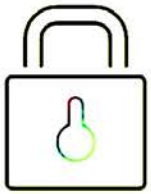
Does it impact Customer?
Does it impact Business Revenue?



Different tiers, different RPO and RTO



Building your resilience strategy



Backup

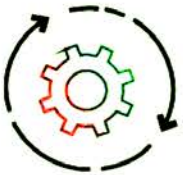
Making copies of data to restore it in case of loss or corruption

RPO:	Hours
RTO:	Hours
Cost:	$

Disaster recovery

Returning to operations within specific targets in cases of highly impactful failures

RPO:	Seconds
RTO:	Minutes
Cost:	$$



High availability

Resistance to common failures through design and operational mechanisms

RPO:	Seconds
RTO:	Near real-time
Cost:	$$$

The 3-2-1-1-0 Backup Rule

Air-Gapped Vaults: The Key to Secure Backups

Immutable Security

Ensures data integrity and compliance through unchangeable security measures.

Enhanced Encryption

Utilizes service-owned keys for superior protection against vulnerabilities.

Simplified Sharing

Facilitates easy and secure data sharing across accounts and organizations.

Flexible Recovery

Supports rapid data recovery and forensic analysis across different environments.

Advanced Backup & Ransomware Recovery Architecture

Implement local backup vault for operational backup

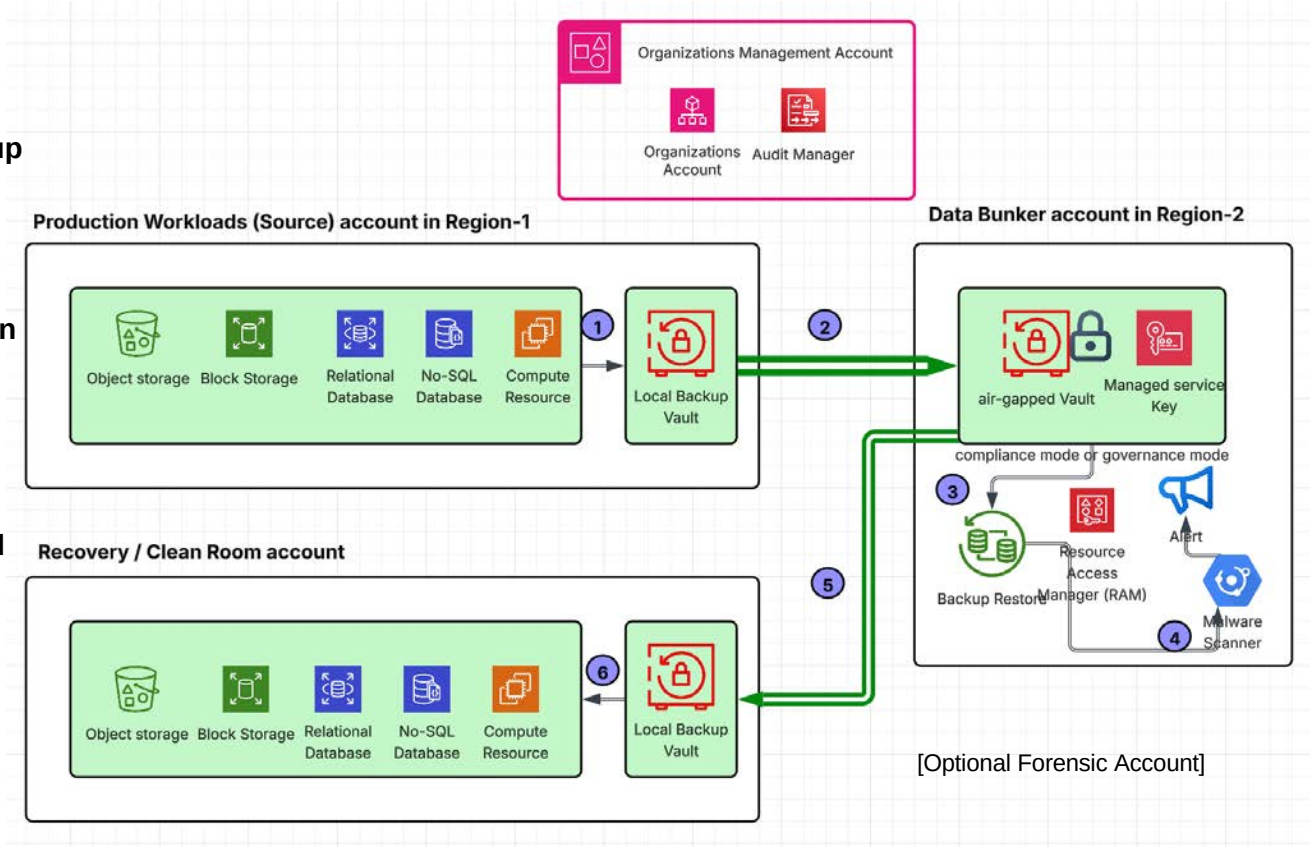
Air-gapped vaults in dedicated accounts, storing immutable Backups

Cross-Region vault architecture provides protection against Regional disruptions

Perform Restore Testing along with error-free & Data integrity scan before actual recovery

Clean Room for data validation from the air-gapped Vault shared with RAM

Automate backup testing with workflows that cleanup resources after successful validations.



Restore testing

Backup Restore Testing (RT) can assess recoverability of business data against data loss events and prove the recovery posture for compliance using custom-defined restore testing plans.

The growth in ransomware makes this even more important, as a tested, clean, air-gapped backup might be the only way to restart the business after an attack.

Assess recoverability of business data against data loss events

Customers can test recovery readiness to prepare for data loss events and to measure duration times for restore jobs

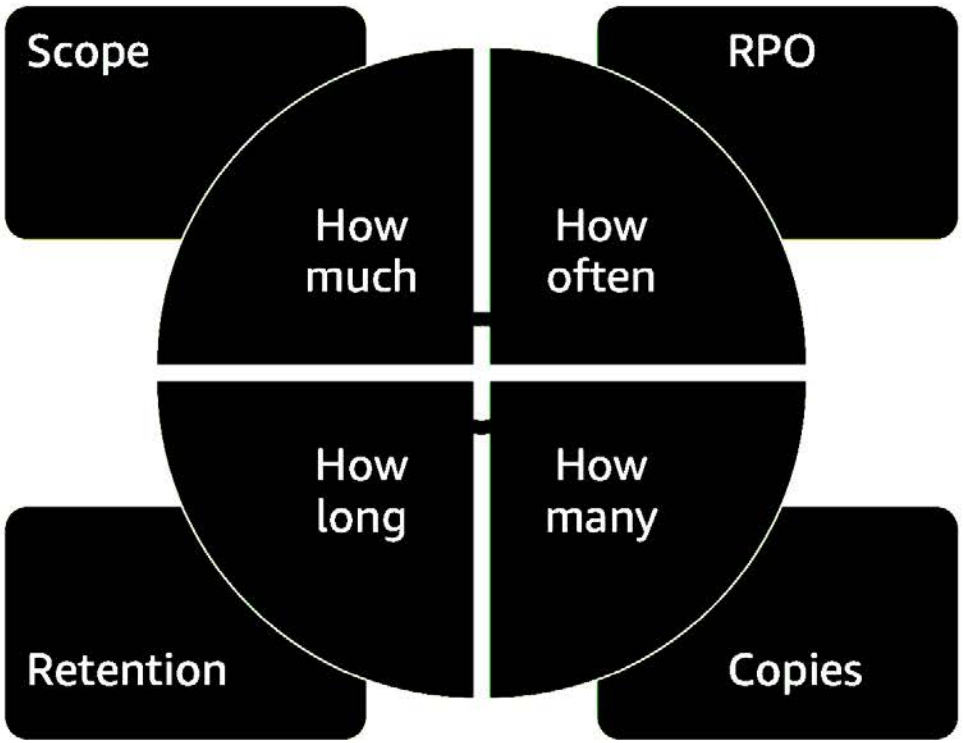
Report on recovery readiness to meet compliance and audit requirements

Use Backup Audit Manager (BAM) Restore Job reports to report on Restore Times

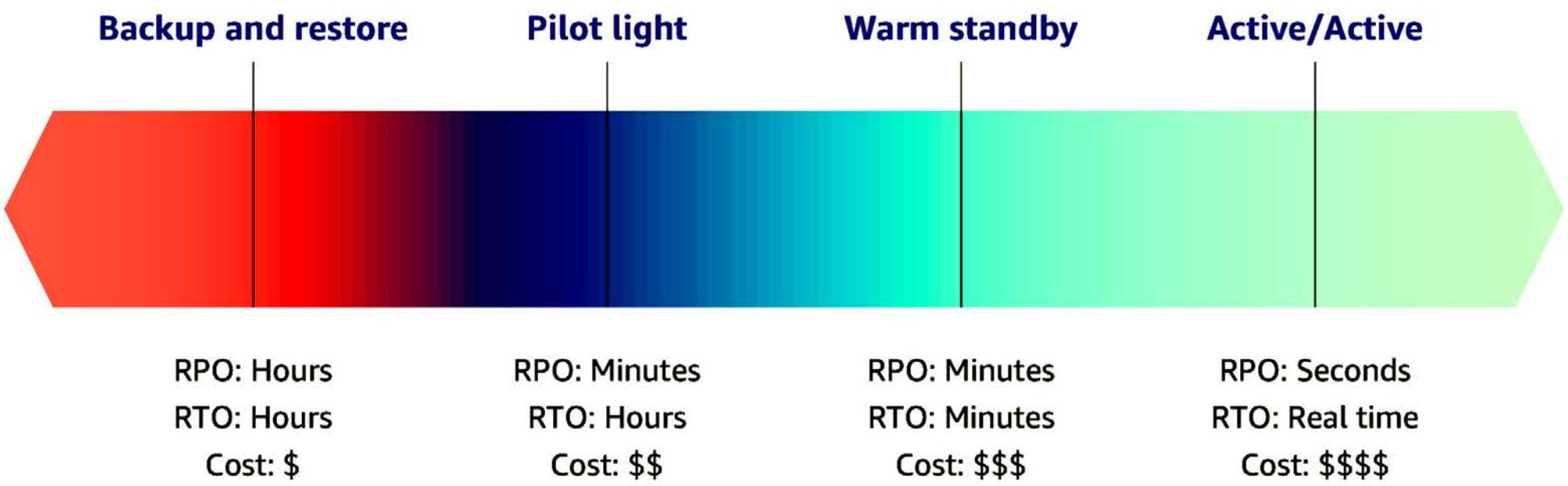
Setup restore testing plans to schedule test restores, and automatically clean-up all tested resources

This feature will perform automated and periodic restore tests of supported resources that have been backed up

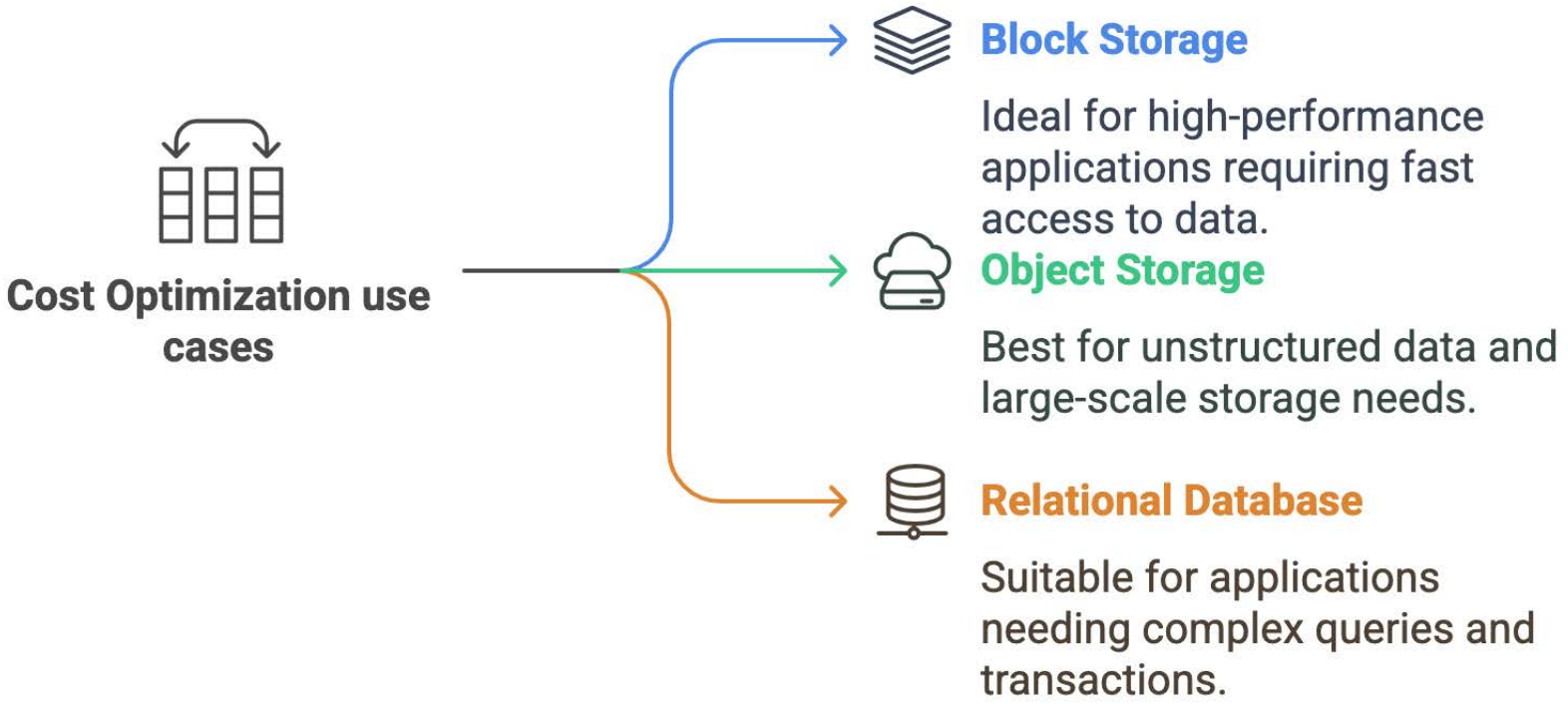
What factors impact cost?



Data resilience options in the cloud



Cost Optimization Use Cases



Cost Optimization Best Practices

Block Storage Snapshots

Manage change rate and growth

Object Storage Backups

Use continuous backups and retention

RDS Backups

Leverage free backups and manage costs

Ransomware Response Plan

Key Takeaways

It's not a matter of if, but when. The threat landscape continues to evolve, with attacks becoming more sophisticated and damaging.

But only if backups are properly protected, tested, and recoverable. Adopting the 3-2-1-1-0 rule, zero-trust ransomware architecture & immutable backups provides a solid foundation for ransomware resilience.

Untested backups often fail when needed most. Regular testing is essential to ensure your recovery capabilities are functional. (Often Overlooked)

Organizations with documented and practiced response plans recover faster and experience less financial impact.

Incident response requires cross-functional collaboration Respective teams must work together during an incident.