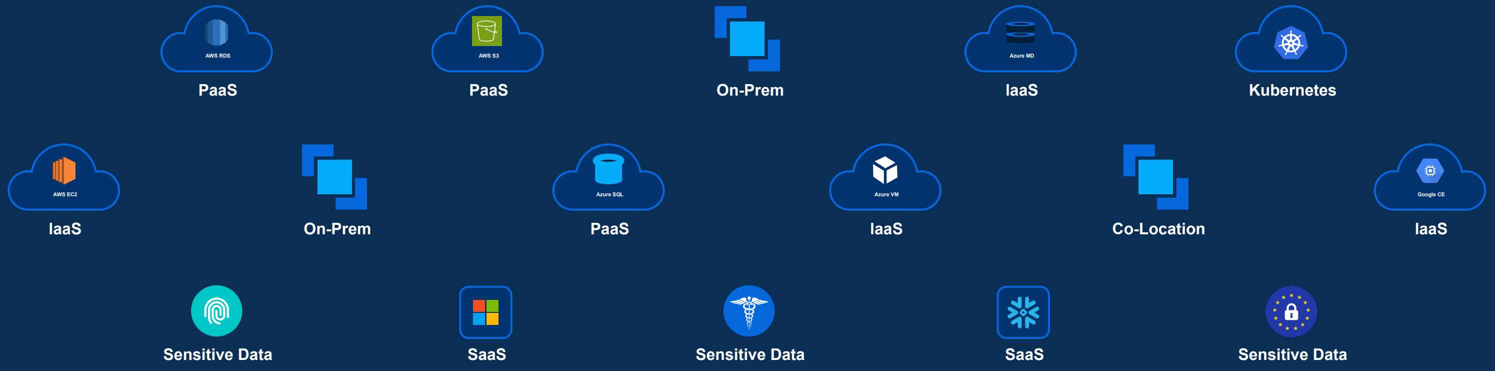
Cloud Cyber Resilience

Cloud Snapshots ≠ Cyber Recovery

Almási Zsolt - CLICO

Your Cloud’s Complexity is Your Biggest Vulnerability

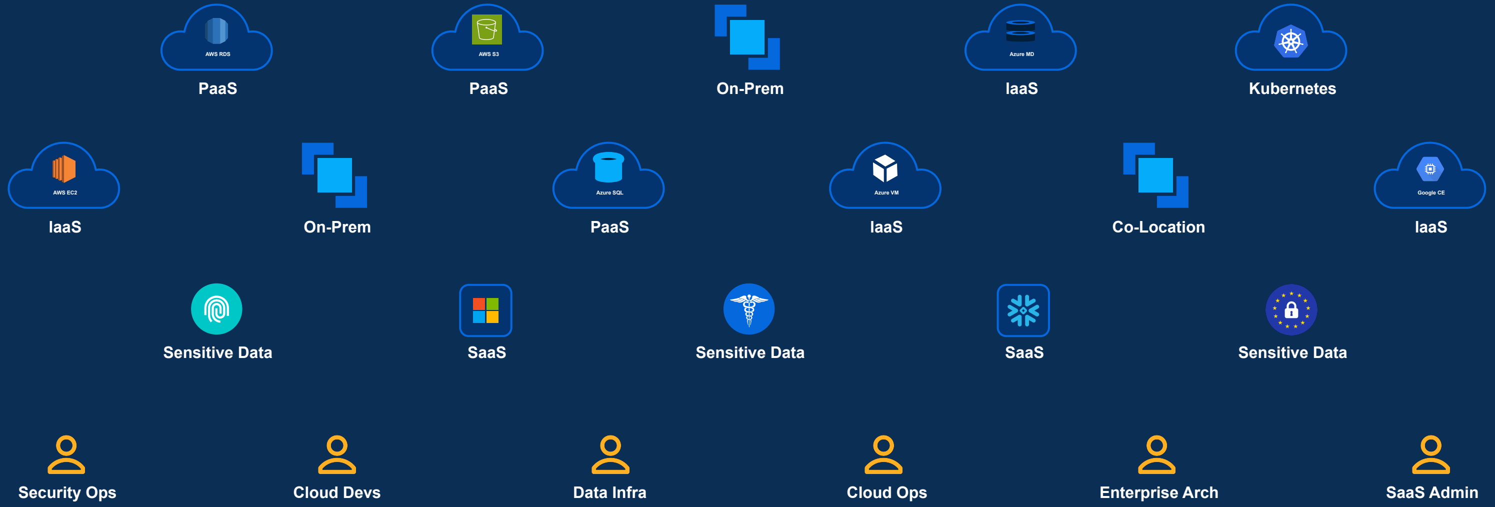


PaaS PaaS On-Prem IaaS Kubernetes

IaaS On-Prem PaaS IaaS Co-Location IaaS

Sensitive Data SaaS Sensitive Data SaaS Sensitive Data

Your Cloud’s Complexity is Your Biggest Vulnerability



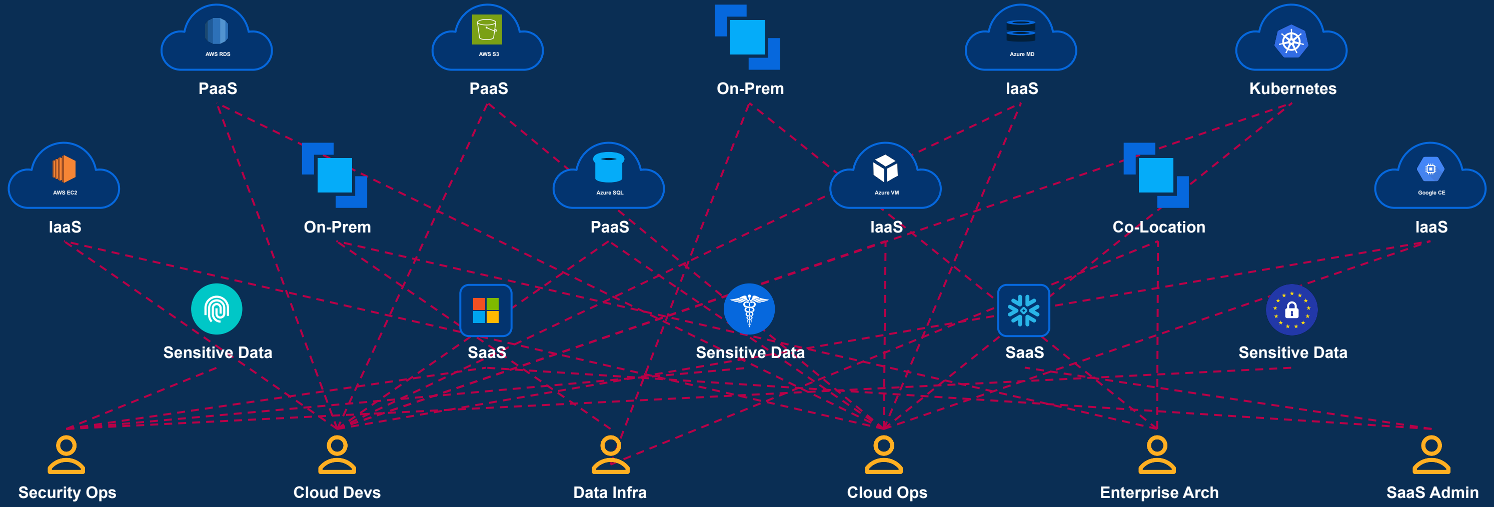
PaaS PaaS On-Prem IaaS Kubernetes

IaaS On-Prem PaaS IaaS Co-Location IaaS

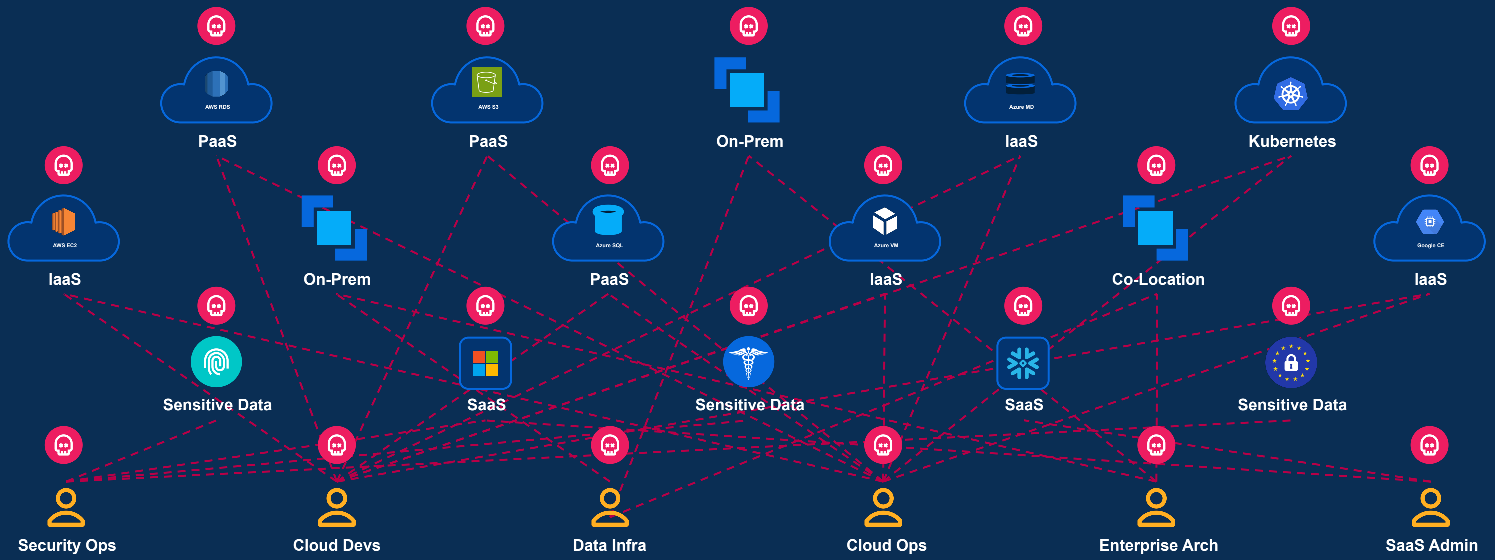
Sensitive Data SaaS Sensitive Data SaaS Sensitive Data

Security Ops Cloud Devs Data Infra Cloud Ops Enterprise Arch SaaS Admin

Your Cloud’s Complexity is Your Biggest Vulnerability



And it’s Under Siege



PaaS

PaaS

On-Prem

IaaS

Kubernetes

IaaS

On-Prem

PaaS

IaaS

Co-Location

IaaS

Sensitive Data

SaaS

Sensitive Data

SaaS

Sensitive Data

Security Ops

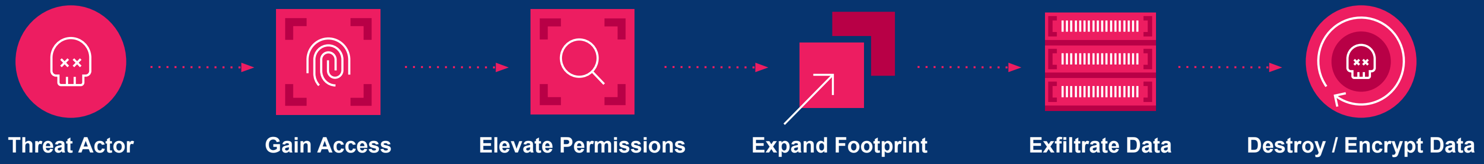
Cloud Devs

Data Infra

Cloud Ops

Enterprise Arch

SaaS Admin



Threat Actor

Gain Access

Elevate Permissions

Expand Footprint

Exfiltrate Data

Destroy / Encrypt Data

When your cloud is breached, how long will your business be down?

Cloud Snapshots ≠ Cyber Recovery

AWS S3
PaaS
On-Prem
Azure MD
IaaS
Kubernetes
On-Prem
Azure SQL
PaaS
Azure VM
IaaS
Co-Location
Google CE
IaaS
SaaS
Sensitive Data
SaaS
Sensitive Data
Cloud Devs
Data Infra
Cloud Ops
Enterprise Arch
SaaS Admin

Deal with Zero Day Attacks ✗

Cloud Snapshots ≠ Cyber Recovery

Deal with
Zero Day Attacks

✗

Find & Quarantine
Malware

✗

Cloud Snapshots ≠ Cyber Recovery

Deal with
Zero Day Attacks

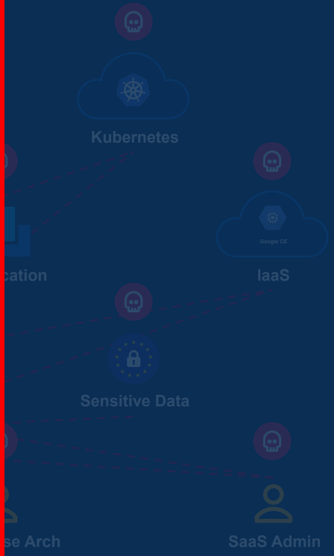
✗

Find & Quarantine
Malware

✗

Assess Sensitive
Data Impact

✗



Cloud Snapshots ≠ Cyber Recovery

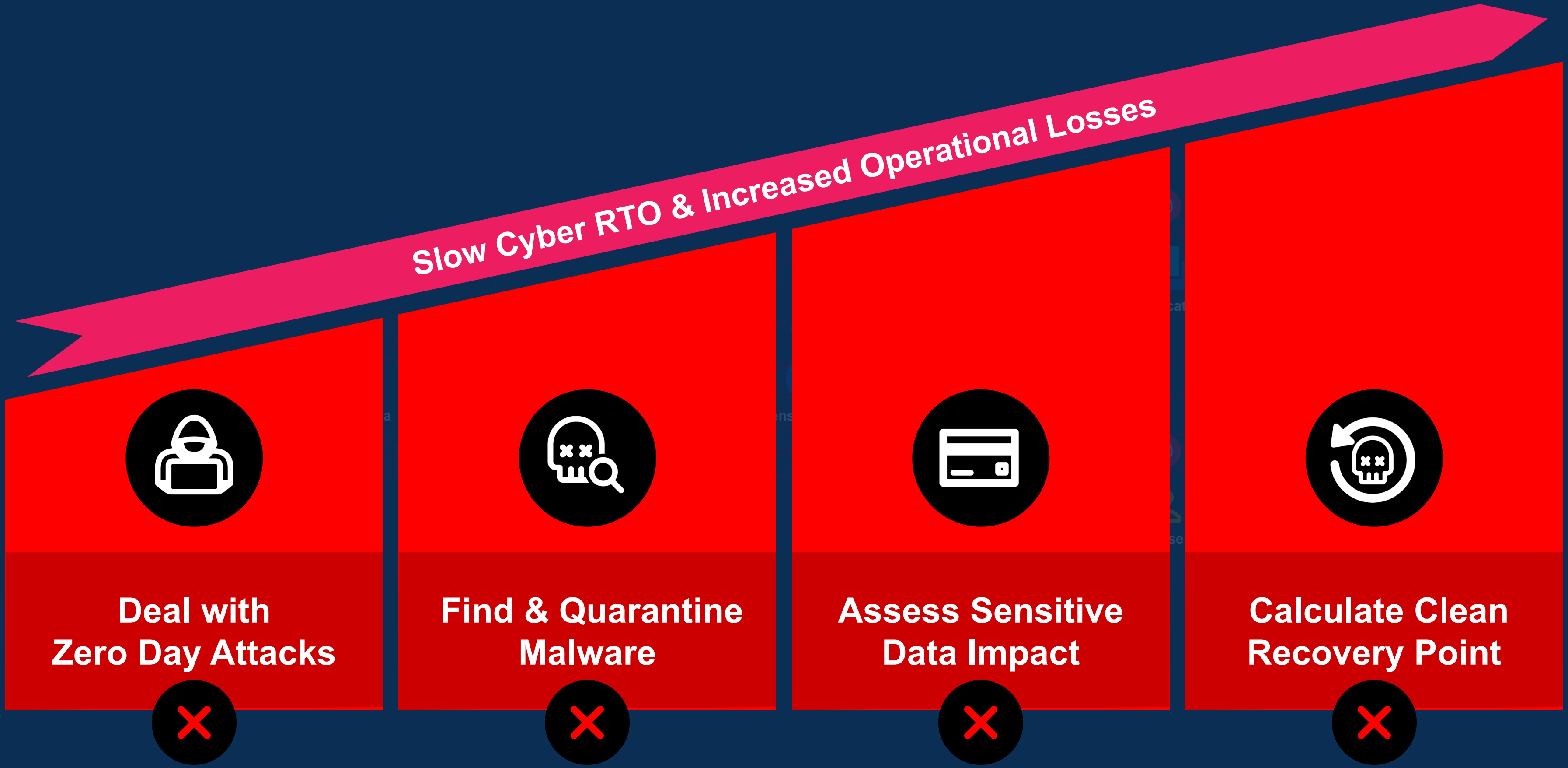
Deal with
Zero Day Attacks
✗

Find & Quarantine
Malware
✗

Assess Sensitive
Data Impact
✗

Calculate Clean
Recovery Point
✗

Cloud Snapshots ≠ Cyber Recovery



Slow Cyber RTO & Increased Operational Losses

Deal with Zero Day Attacks ✗

Find & Quarantine Malware ✗

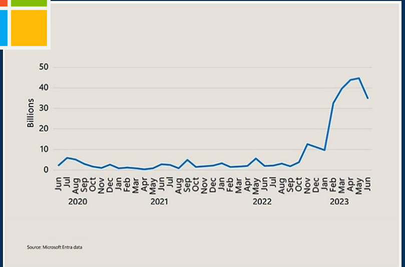
Assess Sensitive Data Impact ✗

Calculate Clean Recovery Point ✗

No wonder when your cloud is breached, you're down for **weeks.**

Impact of recent attacks and relevance for every Company

Microsoft Digital Defense Report 2025



Source: Microsoft Entra data

Telemetry sources: Microsoft Defender for Endpoint, Microsoft Defender for Cloud Apps, Microsoft Defender for Identity, Microsoft Defender for Office 365, Azure AD Identity Protection, Microsoft Defender Threat Intelligence

- **A rise in disruptive attack campaigns.** There has been an 87% increase in campaigns aimed at disrupting customer environments through ransomware, mass deletion, or other destructive actions.
- **An escalation in credential theft and data exfiltration attempts.** Credential and access key theft attempts are up 23%. Attempts to extract sensitive data from storage accounts and databases increased by 58%.

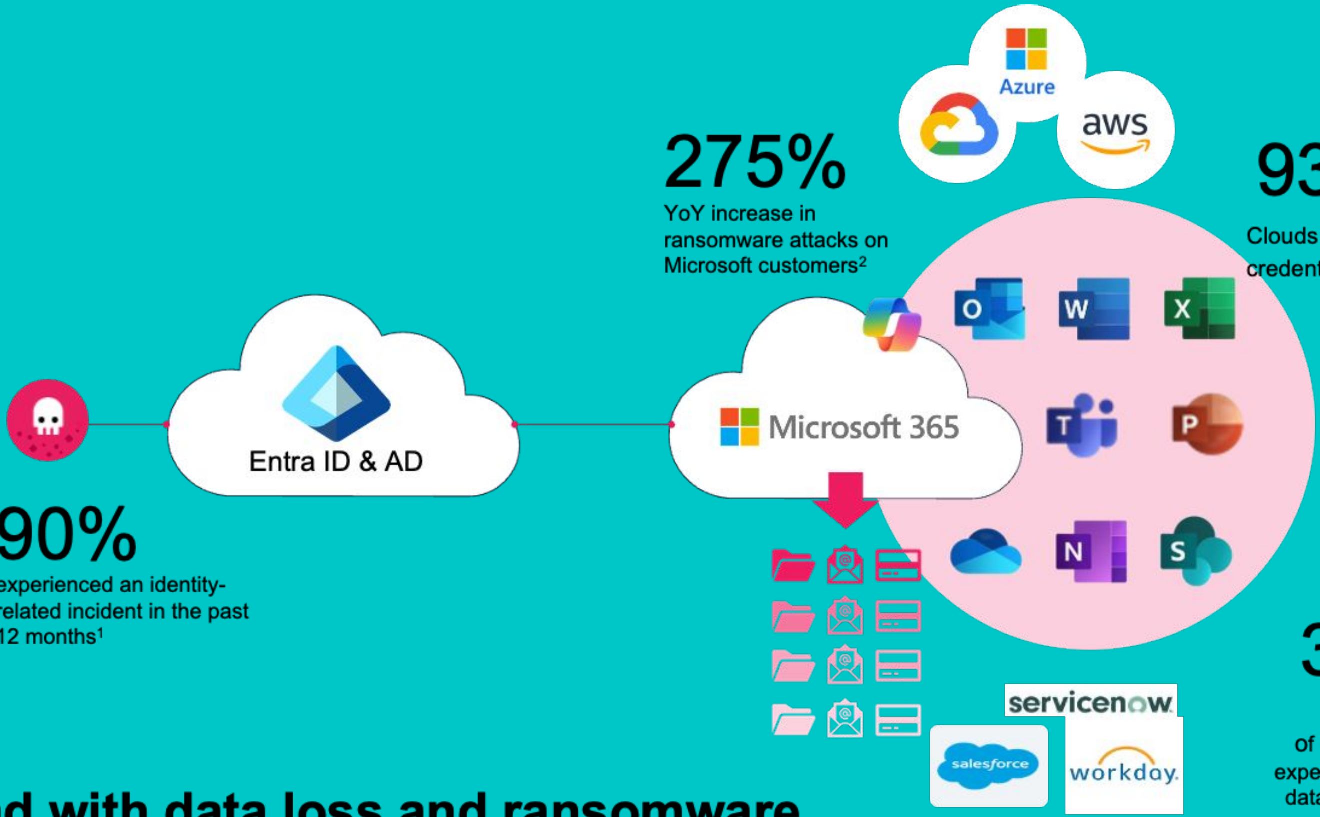
- **600 M identity attacks/day up 10×**
- **4,000 attacks per second** on average
- **87%** increase in attack campaigns

- **Cloud workloads = prime target** (token theft, SaaS lateral moves)
- **Identity now the #1 entry vector** in manufacturing & retail incidents

	Manufacturing	Retail	Healthcare
What Happened?	Likely identity-led. AD + ERP affected **Full production halt**	Help-desk / MFA reset / AD dump / Azure infiltration based on misconfiguration, M365 compromise **Full retail business stop**	Identity + on-prem + cloud compromise -> Commvault backups deleted **Disconnection of core transaction services**
Business Impact	**$6.8 M/day losses, bankruptcy warnings & thousands of job lay-offs in supply chain** Multi-week outage	**£300 M profit hit, £1.2B reduction in company value** 4 months e-commerce offline; warehouse planning, all communication, hiring, and digital payments down	**$2.9 B total impact** National disruption, sensitive data exfiltrated (but not identified which ones), regulatory fines, CEO stepped down
Why it Matters for You	Mirrors OT/IT supply-chain exposure. One identity-led intrusion can idle factories and ripple to suppliers, similar to your operating model.	Retail-like order flows exist in aftermarket spares; an identity breach can stall e-commerce & POS-like portals, stop customer and internal communication, hit service revenue and customer trust.	Shows how platform centralization (e.g., global ERP/PLM/CRM) can become single points of failure affecting cash flow & customer deliveries.

Public disclosures (Jaguar Land Rover 2025, M&S 2025, UnitedHealth 2024).

We see that attacks start with identity compromise



90%

experienced an identity-related incident in the past 12 months[1]

275%

YoY increase in ransomware attacks on Microsoft customers[2]

93% of

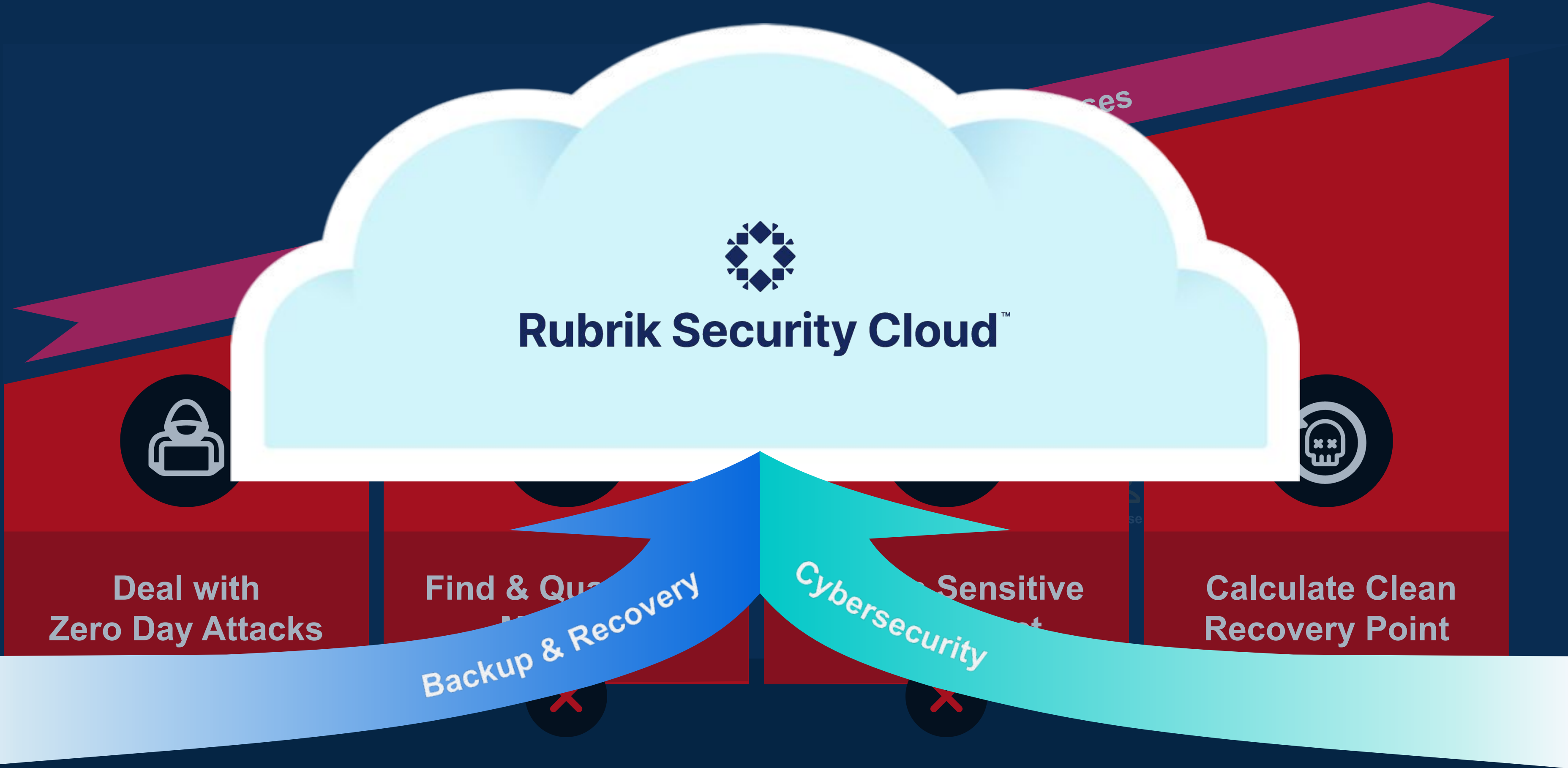
Clouds tenants face credential compromised

31%

of organizations experienced a SaaS data breach in the past year

They end with data loss and ransomware.

Introducing Rubrik Security Cloud



One Platform for Cyber Resilience Across Data + Identity

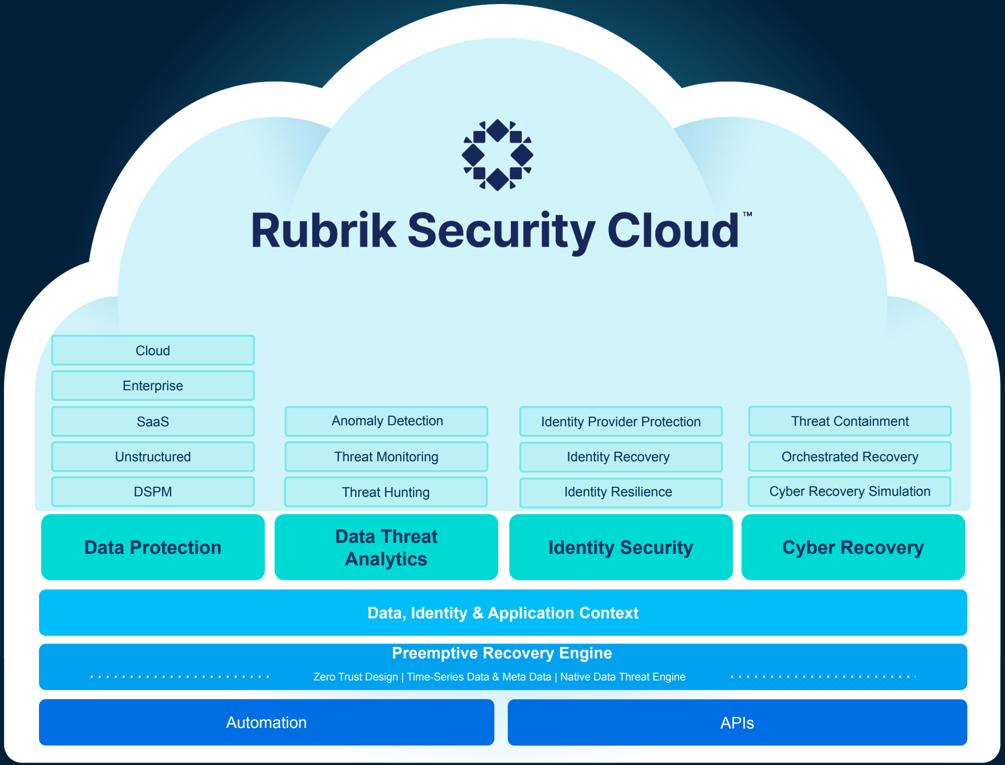
Enterprise
On-premises

Cloud

SaaS

Unstructured Data

Identity Providers



CYBER INTEGRATIONS

Palo Alto Networks

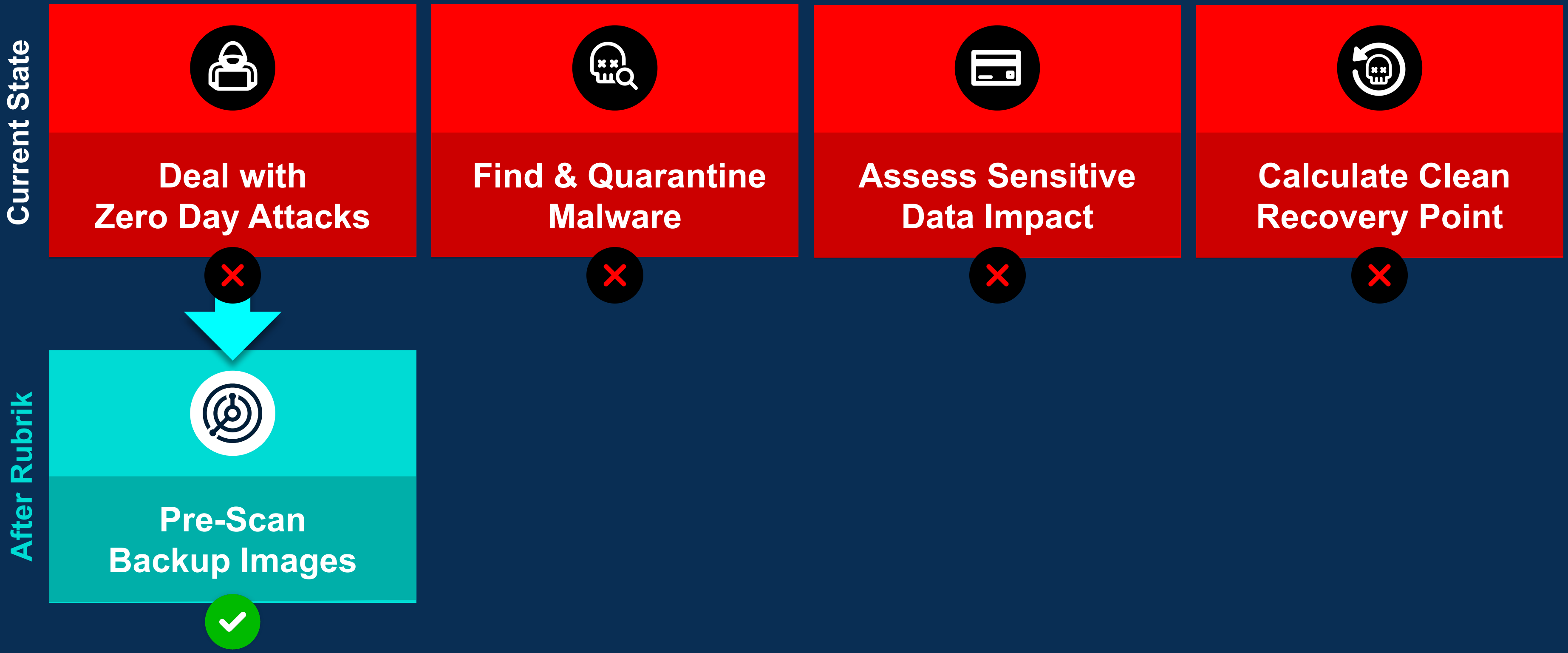
Zscaler

CrowdStrike

Splunk/Cisco

Mandiant

Pre-Calculated Clean Recovery



Current State

Deal with Zero Day Attacks ✗

Find & Quarantine Malware ✗

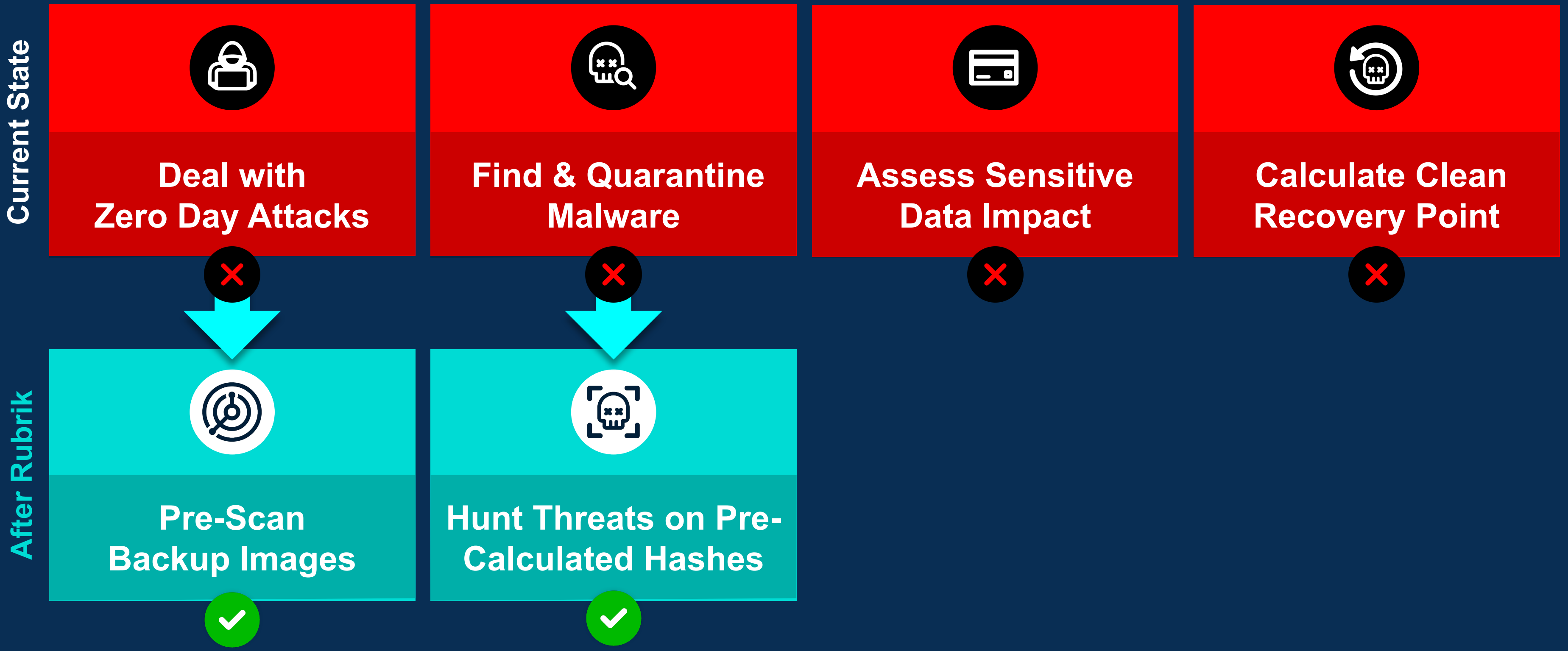
Assess Sensitive Data Impact ✗

Calculate Clean Recovery Point ✗

After Rubrik

Pre-Scan Backup Images ✓

Pre-Calculated Clean Recovery



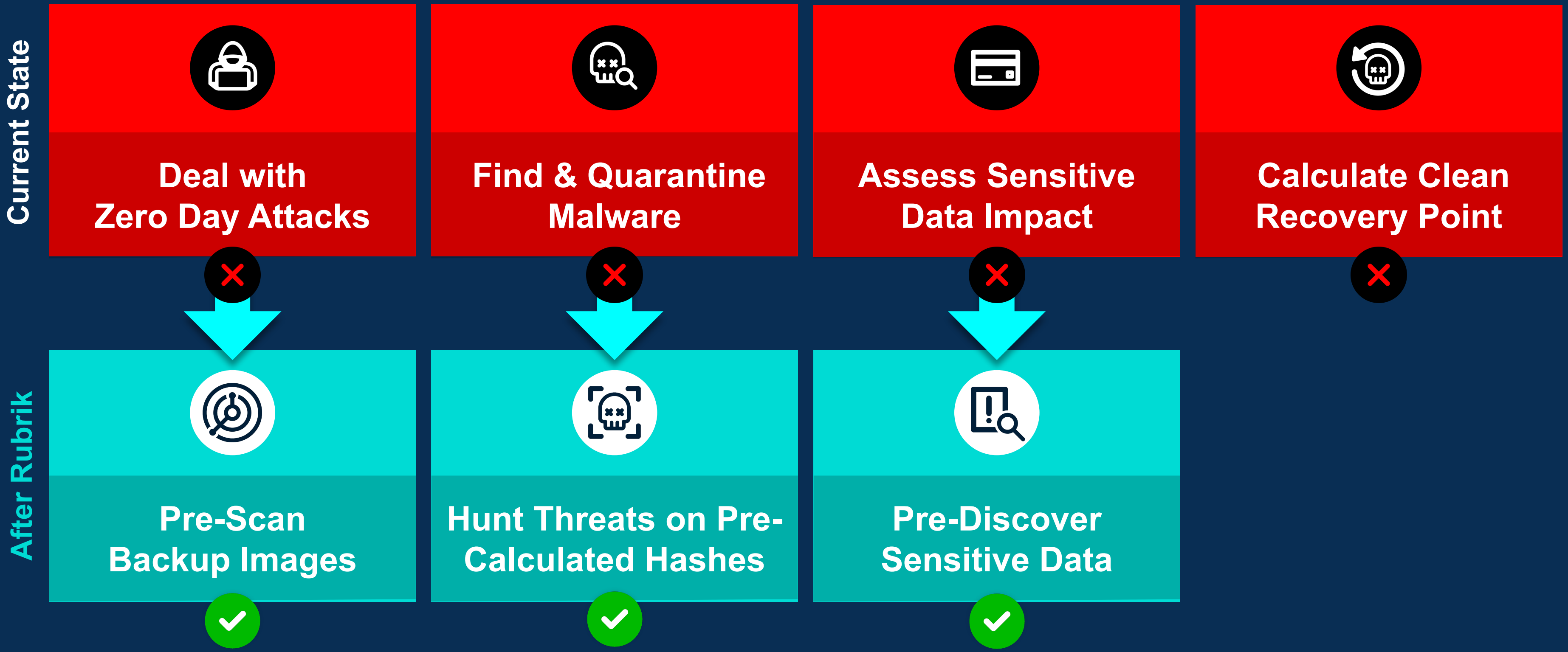
Current State

- Deal with Zero Day Attacks ✗
- Find & Quarantine Malware ✗
- Assess Sensitive Data Impact ✗
- Calculate Clean Recovery Point ✗

After Rubrik

- Pre-Scan Backup Images ✓
- Hunt Threats on Pre-Calculated Hashes ✓

Pre-Calculated Clean Recovery



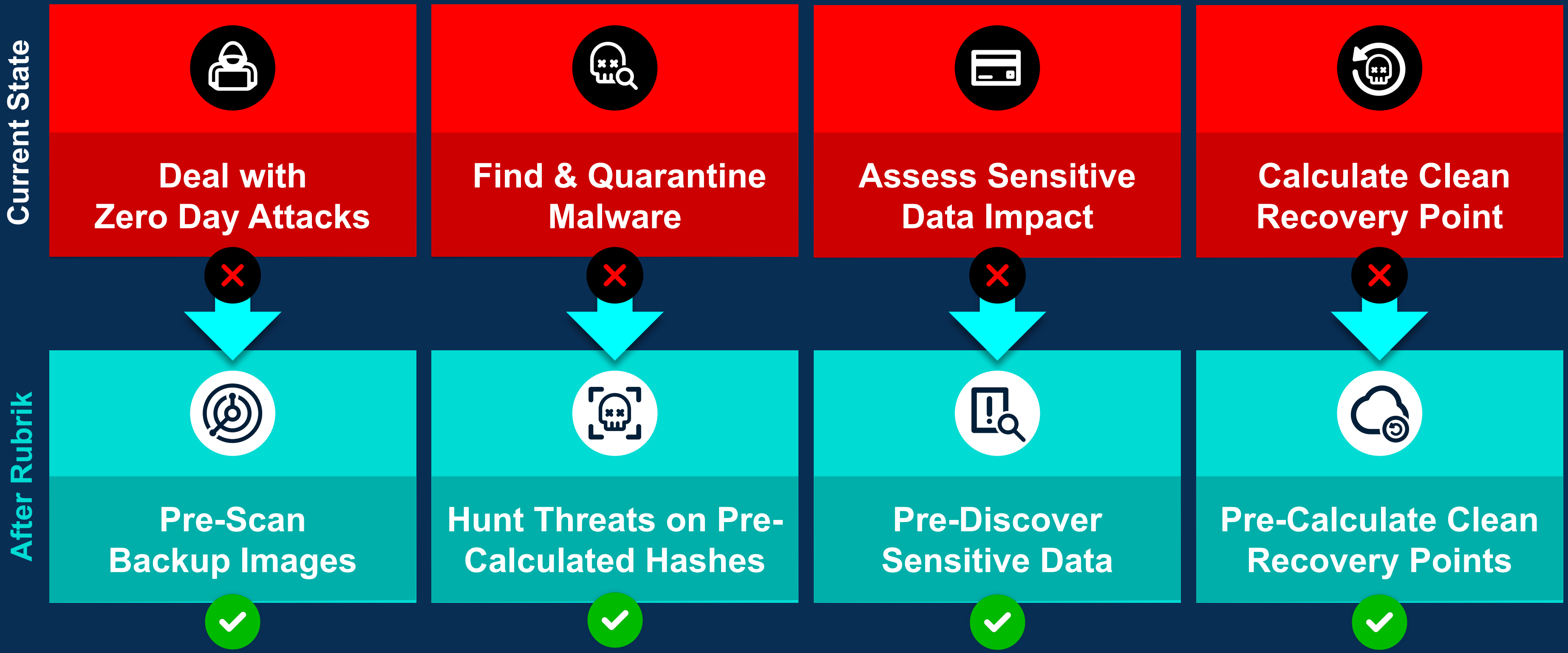
Current State

- Deal with Zero Day Attacks ✗
- Find & Quarantine Malware ✗
- Assess Sensitive Data Impact ✗
- Calculate Clean Recovery Point ✗

After Rubrik

- Pre-Scan Backup Images ✓
- Hunt Threats on Pre-Calculated Hashes ✓
- Pre-Discover Sensitive Data ✓

Pre-Calculated Clean Recovery



Current State	Deal with Zero Day Attacks ✗	Find & Quarantine Malware ✗	Assess Sensitive Data Impact ✗	Calculate Clean Recovery Point ✗
After Rubrik	Pre-Scan Backup Images ✓	Hunt Threats on Pre-Calculated Hashes ✓	Pre-Discover Sensitive Data ✓	Pre-Calculate Clean Recovery Points ✓

Up to 100x Faster Recovery

No clean room required.

Cloud Backup Posture Risk Management

Problem: Lack of visibility into cloud data increases risk & costs

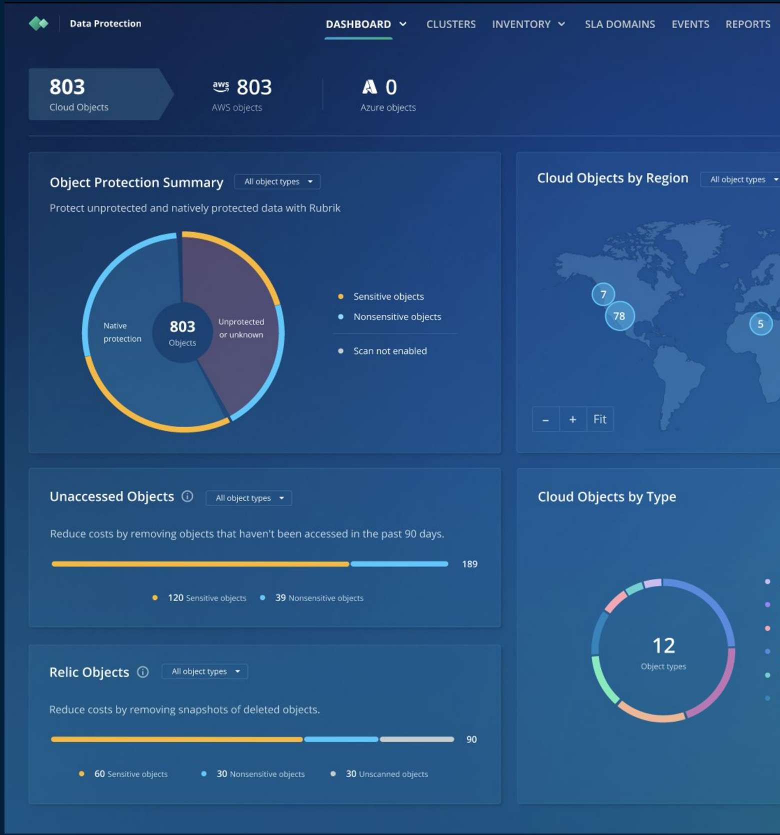
- Cloud data sprawl makes it difficult for IT and security teams to understand where all the cloud data lives and whether that data is properly protected

Solution: Visibility into backup status, sensitive data, and more, included in all Cloud licenses

- Find and protect unprotected critical data to reduce risk
- Shift backup to Rubrik to achieve backup cost savings
- Remove stale data (not accessed in >90 days) or orphaned data, reducing risk and cost

Why Rubrik?

- Achieving this level of visibility would require implementation of additional tools; get this embedded in what you've already bought
- Easy to continuously monitor cost savings and risk reduction capabilities



Protect unprotected and natively protected data with Rubrik

Reduce costs by removing objects that haven't been accessed in the past 90 days.

Reduce costs by removing snapshots of deleted objects.

Comprehensive Data Protection for cloud

aws

AWS EC2, AWS EBS, AWS DynamoDB, AWS RDS, AWS Aurora, AWS S3, AWS EFS, AWS FSx, AWS EKS, VMware Cloud on AWS (VMC), SQL Server, Oracle, SAP HANA, MongoDB

Microsoft Azure

Azure VM, Managed Disk, Blob, Azure SQL, Azure Kubernetes Service (AKS), Azure Files, Microsoft 365, Entra ID, Azure NetApp Files, SQL Server, Azure VMware Solution (AVS), Oracle, SAP HANA, MongoDB

Google Cloud

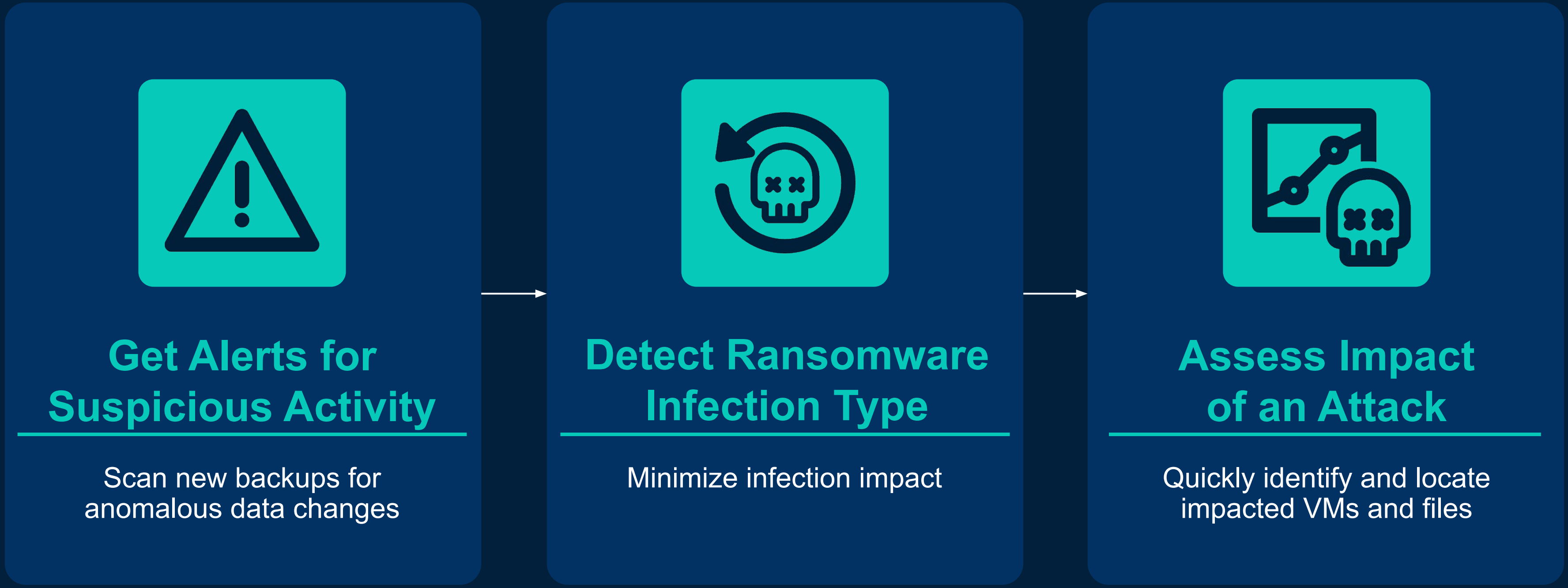
GCE VM, Persistent Disks, Google Cloud VMware Engine (GCVE), SQL Server, Oracle, SAP HANA, MongoDB

ORACLE CLOUD

Oracle DB on VM, Oracle Cloud VMware Solution (OCVS)

Rubrik Anomaly Detection

Detect Ransomware in Backup Data to Respond Quickly



Get Alerts for Suspicious Activity

Scan new backups for anomalous data changes

Detect Ransomware Infection Type

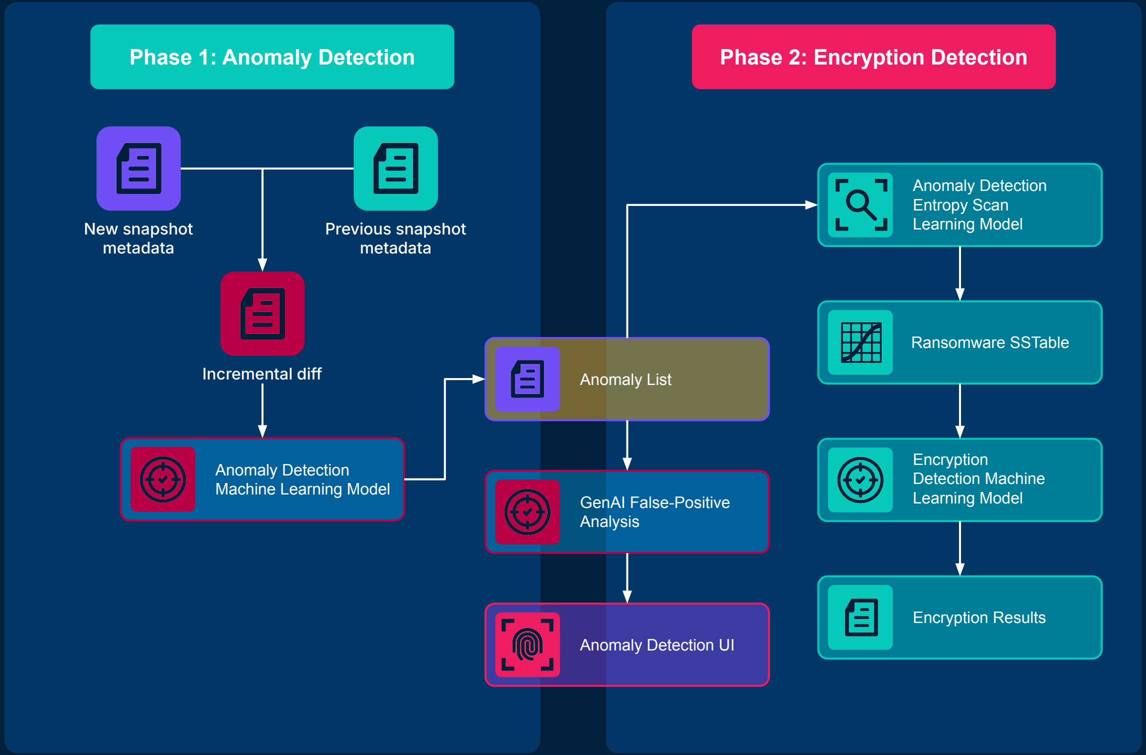
Minimize infection impact

Assess Impact of an Attack

Quickly identify and locate impacted VMs and files

How It Works

1. Metadata for a new snapshot is generated and compared to the previous snapshot to generate diff
2. Diff is fed to ML Model to detect Anomalies
3. List of Anomalies is generated
4. Check for non-malicious anomalies with GenAI
5. Anomalies sent to UI
6. Detected Anomalies are analyzed for encryption
7. Encryption stats are saved within SSTable file
8. Files are fed to ML model to prevent false positives
9. Model outputs likelihood of encryption on file

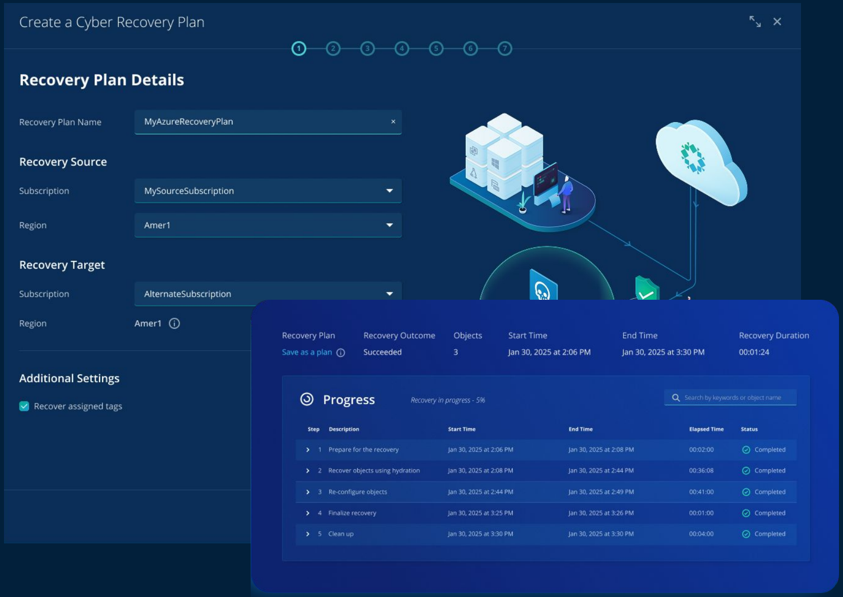


Phase 1: Anomaly Detection
New snapshot metadata
Previous snapshot metadata
Incremental diff
Anomaly Detection Machine Learning Model
Anomaly List
GenAI False-Positive Analysis
Anomaly Detection UI
Phase 2: Encryption Detection
Anomaly Detection Entropy Scan Learning Model
Ransomware SSTable
Encryption Detection Machine Learning Model
Encryption Results

Cloud: GA for Azure VM, AWS EC2; Upcoming for Azure SQL

Orchestrated Recovery

Customer Challenge		Rubrik Solution
Customers lack repeatable and validated recovery plans, owing to operational complexity and manual effort in testing. Lack of historical data also limits process improvement and auditability	**P**REPARE	Rubrik enables customers to **create and test recovery plans** in isolated environments, without impacting production, as well as provides **comprehensive reporting** for compliance and refinements
During an attack, customers struggle with finding IOC-free clean backup for recovery, relying on guesswork or 3rd party tools, thereby risking reinfection and increasing downtime	**R**ESPOND	Rubrik provides **integrated threat hunting and anomaly detection** enabling quick and easy identification of clean-point-of recovery to execute pre-validated recovery plans
During recovery, customers juggle manual, slow and error-prone processes across recovery and incident response, inflating business downtime and jep[ordizing RTOs	**O**RCHESTRATE	Rubrik enables **orchestration of pre-validated recovery plans** with just a few clicks, as well as, **ad- hoc cyber recovery** for scenarios not covered by pre-defined plans, expediting complex workflows



Create a Cyber Recovery Plan

Recovery Plan Details

Recovery Plan Name: MyAzureRecoveryPlan

Recovery Source

Subscription: MySourceSubscription

Region: Amer1

Recovery Target

Subscription: AlternateSubscription

Region: Amer1

Additional Settings

☑ Recover assigned tags

Recovery Plan	Recovery Outcome	Objects	Start Time	End Time	Recovery Duration
Save as a plan	Succeeded	3	Jan 30, 2025 at 2:06 PM	Jan 30, 2025 at 3:30 PM	00:01:24

Progress

Recovery in progress - 5%

Search by keywords or object name

Step	Description	Start Time	End Time	Elapsed Time	Status
1	Prepare for the recovery	Jan 30, 2025 at 2:06 PM	Jan 30, 2025 at 2:08 PM	00:02:00	✓ Completed
2	Recover objects using hydration	Jan 30, 2025 at 2:08 PM	Jan 30, 2025 at 2:44 PM	00:36:08	✓ Completed
3	Re-configure objects	Jan 30, 2025 at 2:44 PM	Jan 30, 2025 at 2:49 PM	00:41:00	✓ Completed
4	Finalize recovery	Jan 30, 2025 at 3:25 PM	Jan 30, 2025 at 3:26 PM	00:01:00	✓ Completed
5	Clean up	Jan 30, 2025 at 3:30 PM	Jan 30, 2025 at 3:30 PM	00:04:00	✓ Completed

Customer Benefits

Confident & Clean Recovery: Recover from cyber attack confidently and reliably without risking reinfection with battle-tested recovery plans and easy identification of clean-point-of-recovery

Reduced Downtime & Operational Burden: Minimize disruption and streamline efforts during critical post-recovery period with integrated threat hunting and recovery orchestration

Compliance & Governance Adherence: Satisfy regulatory mandates and demonstrate recoverability to leadership and compliance auditors through comprehensive reporting

Orchestrated Recovery: How it Works

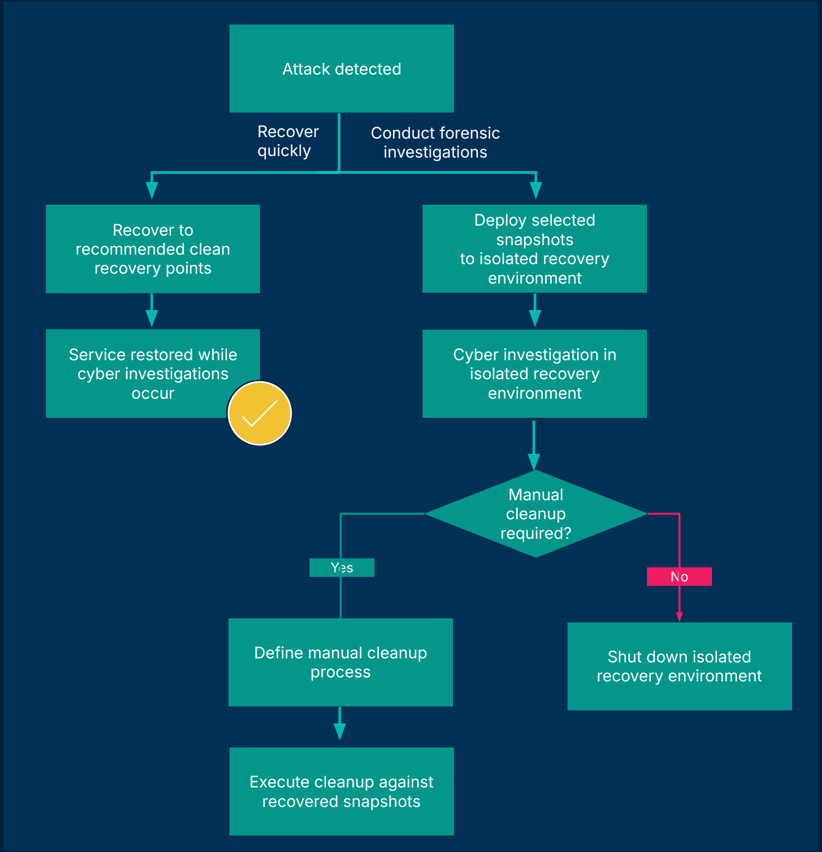
1. Create recovery plans defining, destination subscription, vNet for IRE, boot order priority

2. Confirm and save recovery plan for future use

3. During recovery, start by using IoC-free snapshots from completed threat hunts or anomaly detection results. Restore critical business systems the first time using non-anomalous and non-quarantined recovery point filters to reduce reinfection risk

4. Mount snapshot for IRE for conducting forensics in parallel with recovery or to further
 Validate snapshot (before recovery)

5. Monitor recovery progress and conduct automated cleanup actions. Generate ad-hoc recovery reports on historical performance and outcomes


Attack detected
Recover quickly
Conduct forensic investigations
Recover to recommended clean recovery points
Deploy selected snapshots to isolated recovery environment
Service restored while cyber investigations occur
Cyber investigation in isolated recovery environment
Manual cleanup required?
Yes
No
Define manual cleanup process
Shut down isolated recovery environment
Execute cleanup against recovered snapshots

GA Date: Jan 3 2025
Cloud: Azure, AWS

Retention Lock

The Customer Challenge

Malicious actors can manipulate backup policies and **shorten retention period of backups**, even to 0 days!

This results in backups expiring before they should, leaving a customer **vulnerable to data loss** and **compliance breaches**.

The Rubrik Solution

A comparable security feature to native cloud backup solutions like AWS Backup Vault Lock and Azure Backup Retention Lock. Rubrik can now **lock retention of backups to prevent unintended changes**.

Rubrik differentiates with a **simplified configuration process**, and advanced security layers such as **DSPM** and **air-gapped backups** for added protection from cyber threats.

Customer Benefits

Enhanced Security - Strengthen security posture with extended immutability capabilities, protecting against ransomware, accidental deletion, or malicious deletion events.
More Control - Gain granular control with retention settings for different types of cloud data.
Reduced Risk - Minimize the risk of data loss from policy conflicts, human error, or bad actors with locked SLA retention settings that cannot be disabled, deleted, or reduced, even by an Admin.

Retention Lock and Quorum Authorization

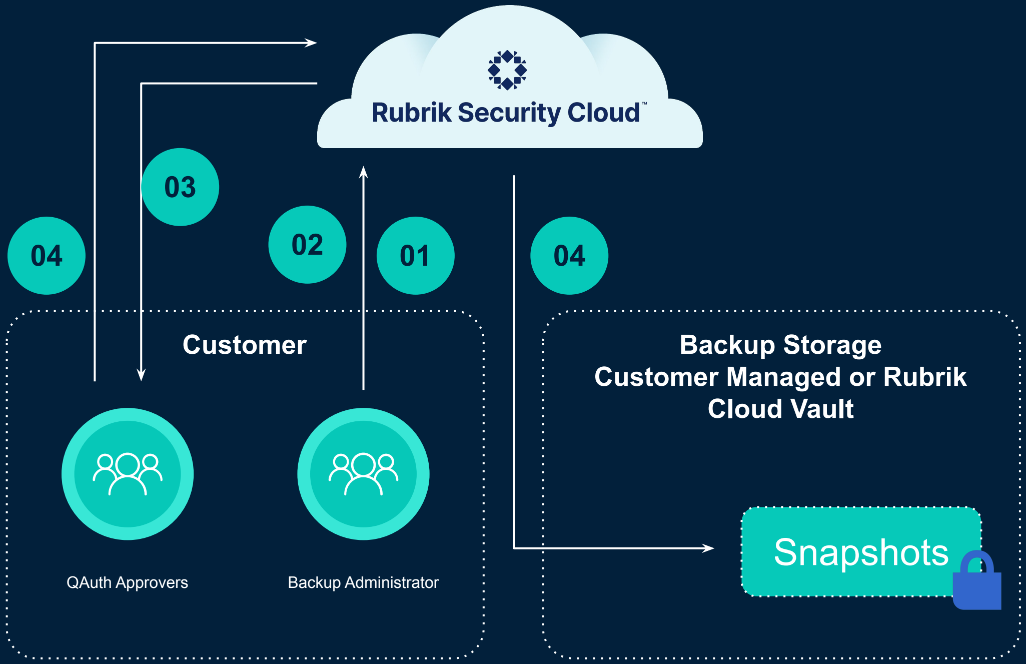
How it Works

01 Customer creates retention locked SLA. Snapshots are now locked to their assigned expiration date

02 Customer makes request to configure SLA in such a way that calls for early expiry and/or delete a Retention Locked snapshot

03 Action is blocked and held in queue. Quorum Authorization request is sent

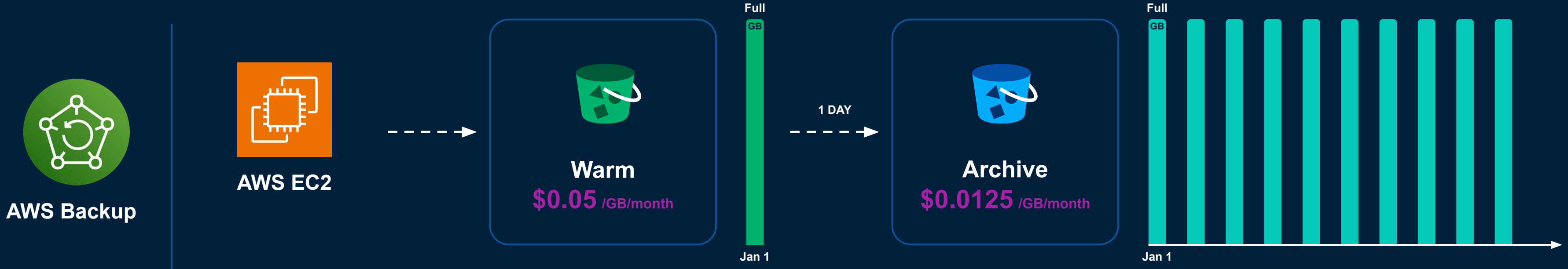
04 Quorum approver(s) log in and either approve or deny the request



Additional Value of Rubrik Security Cloud

AWS Backup	Added Value	Rubrik
Stores backups in a "warm" storage tier (e.g. $0.05 GB/Month)	**Lower TCO**	Compresses backup data and can archive immediately to S3 IA (e.g. $0.0125 GB/Month)
Is focused on protecting AWS data	**Unify Multi / Hybrid Cloud Protection, Visibility, and Governance**	Delivers complete cyber resilience across on-prem, cloud, and SaaS in one platform
Separates administration of backup and restore for each AWS account and region	**Simplify Administration of Multiple AWS Accounts and regions**	Provides a single place to manage AWS workloads across all AWS accounts and regions
Performs full restores of EC2 and EBS Cannot see or backup DBs inside VMs Cannot auto recover to another account	**Gain Critical Backup & Recovery Features**	Can search and recover individual files, objects, and folders Integrates with DBs so can backup DBs inside VMs
Does not scan backup data for security threats	**Enable Data Threat Analytics**	Evaluates the impact of cyberattacks and continuously monitors for suspicious activity, detecting over privileged users, and proactively identifies sensitive data exposure

Why is Rubrik More Cost Efficient than AWS Backup for EC2?

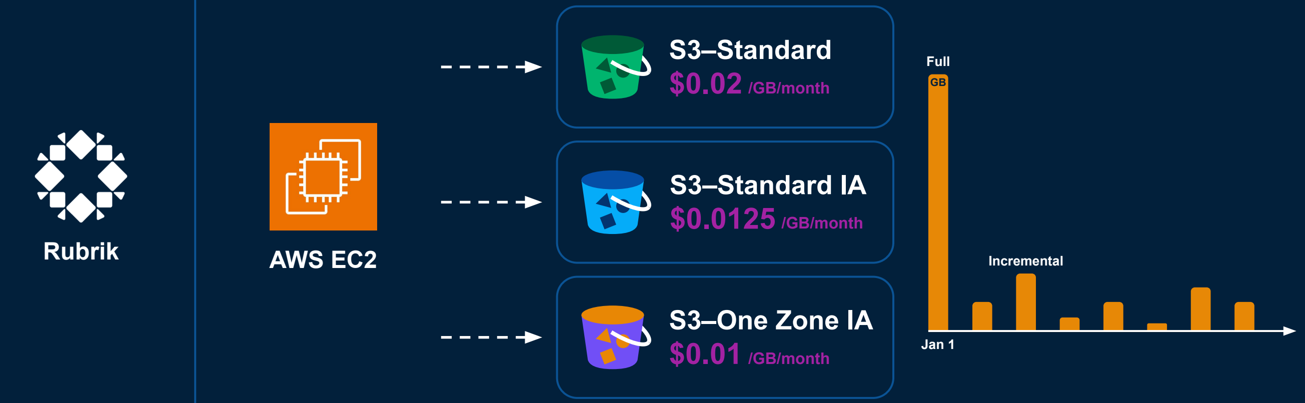


AWS Backup

AWS EC2

Warm
$0.05 /GB/month

Archive
$0.0125 /GB/month



Rubrik

AWS EC2

S3–Standard
$0.02 /GB/month

S3–Standard IA
$0.0125 /GB/month

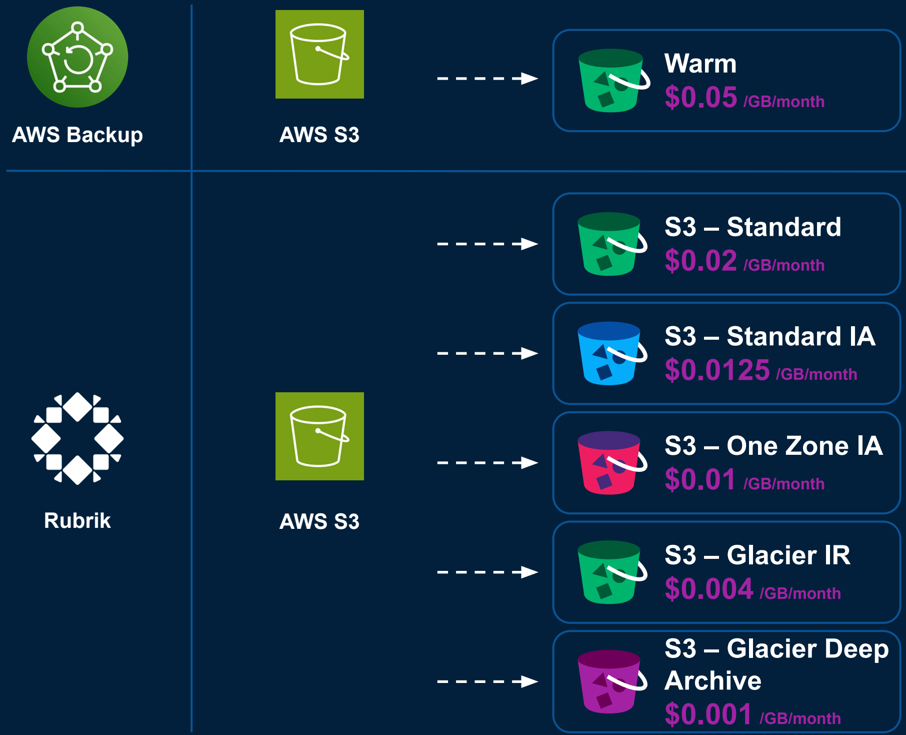
S3–One Zone IA
$0.01 /GB/month

AWS Backup stores a full backup copy in Warm and can only store full backups in Archive. AWS Backup also requires a min 90 day retention in Archive tier.

Rubrik can archive immediately and can store incremental backups. Rubrik does not have a min retention.

*US West, Oregon

Why is Rubrik More Cost Efficient than AWS Backup for S3?



AWS Backup

AWS S3

Warm
$0.05 /GB/month

AWS Backup can only store S3 backup data in Warm storage

Rubrik

AWS S3

S3 – Standard
$0.02 /GB/month

S3 – Standard IA
$0.0125 /GB/month

S3 – One Zone IA
$0.01 /GB/month

S3 – Glacier IR
$0.004 /GB/month

S3 – Glacier Deep Archive
$0.001 /GB/month

Rubrik can store S3 backup data across multiple S3 tiers, depending on cost and RTO requirements

*US West, Oregon

Interested in more ?

rubrik@clico.hu

Bugár Zoltán
Product Manager @ CLICO

Christian Putz
RSM Eastern Europe @ RUBRIK

Almási Zsolt
Sr. System Engineer @ CLICO

Jürgen Kaus
Security Consultant @ RUBRIK