rubrik | Zero Trust Data Security™

# Zero Trust Culture Drives Cyber Resilient Missions

**August 25, 2025**

**Travis Rosiek, Public Sector CTO**

# Today's agenda

1. Introduction
2. Cyber Risk
3. Mission Risk
4. Data/Cyber Resilience
5. Cyber Recovery
6. Q&A

# Introduction

## Travis Rosiek

With over 20 years of experience in the security industry, Travis is a highly accomplished cybersecurity leader and innovator having led both commercial product companies and U.S. government programs. His unique understanding of the cybersecurity challenges that organizations face and skills to build cybersecurity-related capabilities have helped countless organizations innovate and become more proactive in their approach to cybersecurity resiliency initiatives.

# Cyber Risk =

# Threat * Vulnerability * Impact * Likelihood

# Mission Risk =

# Threat * Vulnerability * Impact * Likelihood

# Adversarial Threat Tiers

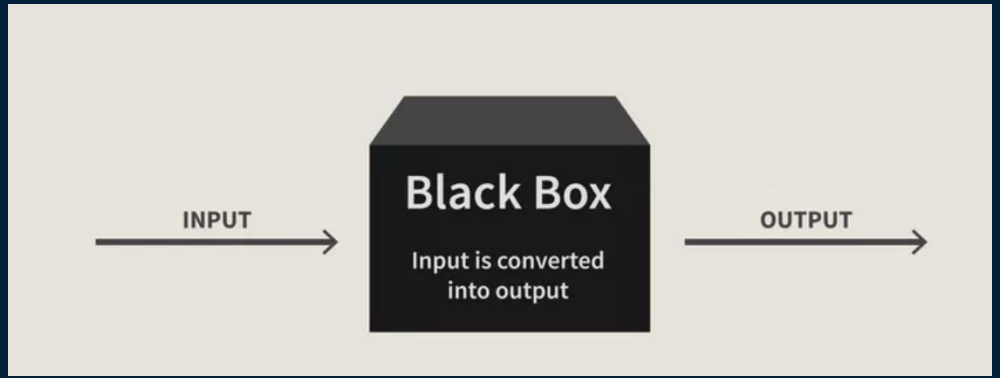
| | |
|---|---|
|  | **ATT 5 – Extreme:** (e.g., **Russia SVR, APT-29**). Uses a range of initial exploitation techniques that vary in sophistication, coupled with 'stealthy' intrusion tradecraft to cause denial, degradation, deception, disruption, and destruction of mission capabilities. Uses custom tools, compromised accounts, and system misconfiguration to blend in with normal/unmonitored traffic to move undetected in victim networks. Demonstrated capability to target cloud resources and supply chain (e.g., SolarWinds). |
|  | **ATT 4 – Advanced:** (e.g., **Russia GRU, APT-28; China APT-41**). Conducts complex, long-term cyber attack operations combining multiple intelligence sources to obtain access to high-value networks. After gaining access, combines well known TTPs to move laterally, evade defenses and collect additional info. Uses tools to conduct widespread, distributed and anonymized 'brute force' access to cloud services. Develops detailed target technical knowledge for more damaging attacks. |
|  | **ATT 3 – Moderate:** Sophisticated, persistent, and well-resourced adversaries at nation-state level. Capable of advanced cyber tradecraft to use publicly available tools, develop/use customized malware, and acquire access to some ATT-4/ATT-5 tools to stealthily implant malware/vulnerabilities, conduct wide-ranging intelligence collection operations, gain access to more isolated networks, and in some cases, create limited effects against defense critical infrastructure networks. |
|  | **ATT 2 – Limited:** Capable of limited advanced cyber tradecraft using publicly available and customized tools to exploit known and unknown vulnerabilities. Able to identify -- and target-for espionage or attack -- easily accessible unencrypted networks running common operating systems using publicly available tools. Possesses some limited strategic planning. |
|  | **ATT 1 – Nascent:** Little-to-no organized cyber capabilities, with no knowledge of a network's underlying systems beyond publicly connected open-source information. Willing to exploit known vulnerabilities. |

# Software Supply Chain Attacks

**Destructive Malware**

- SolarWinds
- NotPetya
- CC Cleaner
- Log4J type of attacks
- Ransomware - Motive

**WHY?**




Implicitly Trust?

# ORGANIZATIONS HAD A RECORD-SETTING NUMBER OF ISSUES TO TACKLE LAST YEAR

Vulnerabilities are not a perfect exposure measure, but they do provide a solid view on the scope and scale of inherited risk from vendors.

2022 was a record-setting vulnerability year

**25,083**
vulnerabilities discovered

2023 set a new record, a 16% increase over the previous record:

**29,065**
vulnerabilities discovered

2024 set a new record, a 37% increase over the previous record:

**40,063**
vulnerabilities discovered

# We are Data Hoarders

Data is growing at 7x pace over next 5 years

Too much data in too many places without enough visibility

Data is oxygen, you don't think about it until it's gone–and then its your only thought

**Your Mission requires Data**

# Impact

## Rob Joyce
## “It’s clear, their intent is destructive"

# Likelihood

## Ron Ross

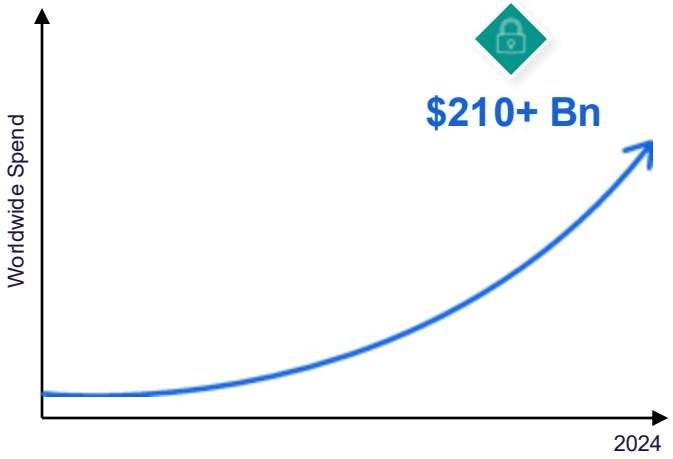
## “It’s not a 1 in 100 or 1 in 10 chance of happening, it’s going to happen.”

**Plenty of focus on**
**Attack Prevention.**

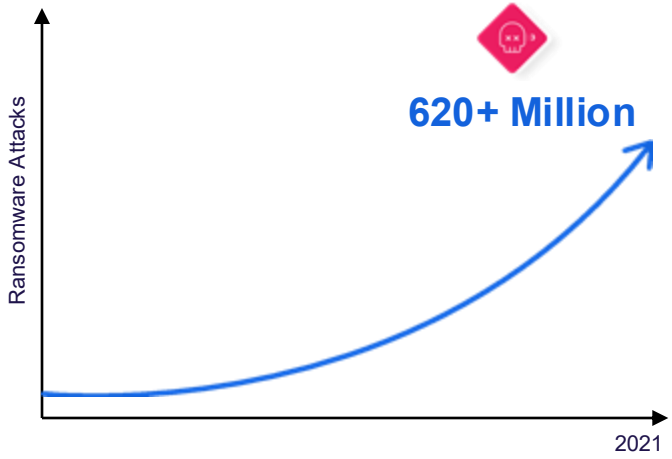
**Not enough on**
**Cyber Recovery.**

# Despite High Security Spend, Attacks Continue Unabated

## Worldwide Security Spend is Up[1]




## Ransomware Still on a Tear[2]




1. Gartner Forecast: Information Security and Risk Management, Worldwide, 2022-2028, 1Q24 Update, March 2024.
2. Mid-Year Update: 2022 SonicWall Cyber Threat Report: Global Ransomware Attacks in 2021.

# CYBERCRIMINALS ARE HIP TO THE BACKUP GAME AND ROUTINELY TARGET BACKUPS

Attackers almost universally attempted to remove backup and recovery options from defenders. External organizations that reported a successful attack observed:

Backups compliance: copies in different locations

**96%**

Attackers tried to affect the backups in 96% of these attacks.

**74%**

And were at least partially successful in 74% of those attempts.

i.e. not able to recover -> attacked

Cyber Insurance Companies – requiring immutable and tested backups to get insurance

# Are you Prepared for a Cyber Typhoon?

- Backup != Cyber Recovery
- RTO and RPO times for your mission?
- Have you tested your backups? @ Scale?

- Does your DCO team know what your backup capability is?
- Is cyber recovery part of your cyber exercises?
- Do you have your IR and CR procedures printed out and updated?

# Mission Systems are Compliant

USG Readiness

Typhoons are Coming

# Cyber Resilience with Urgency


THE SECRETARY OF THE NAVY
WASHINGTON DC 20350-1000

September 30, 2024

MEMORANDUM FOR CHIEF OF NAVAL OPERATIONS
DEPARTMENT OF THE NAVY CHIEF INFORMATION OFFICER
DEPARTMENT OF THE NAVY PRINCIPAL CYBER ADVISOR

SUBJECT: Mission Assurance of Digital Infrastructure

The mission capability of our forces is critically dependent on general purpose digital infrastructure. Cyber risks are especially significant across all phases of a high-end conflict with near peer adversaries. I am encouraged by the Navy's focus on developing a shared understanding of the risks to mission assurance from cyber threats and vulnerabilities. Substantial improvements to Navy cyber doctrine, organization, operations, training and technology employment that yield cyber resilient platforms is fundamental to maintaining the advantage in the maritime domain.

# Cyber Space: Early Warning Signs (It's time to prepare or Evacuate)

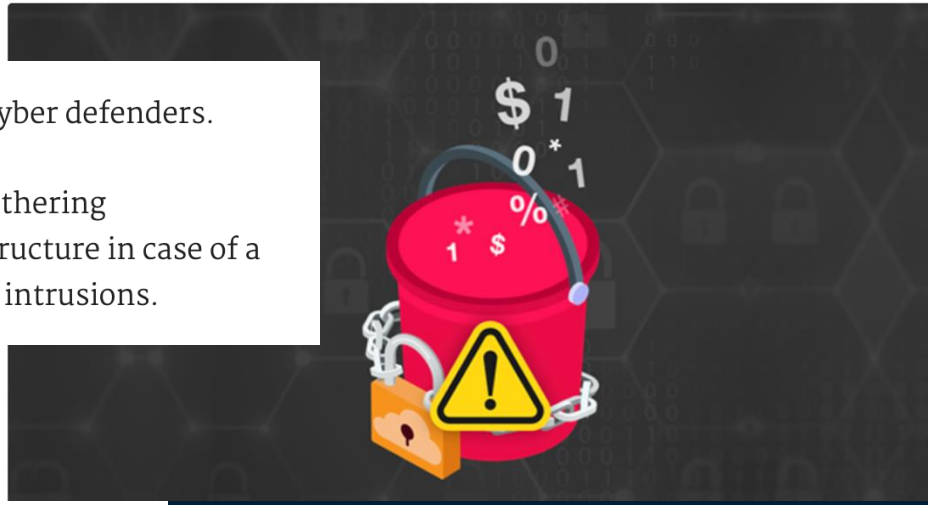
## US National Guard unit 'extensively' hacked by Salt Typhoon in 2024

Salt Typhoon has emerged as one of the top concerns of American cyber defenders.

US officials allege that the hacking group is doing more than just gathering intelligence; it is prepositioning itself to paralyse US critical infrastructure in case of a conflict with China. Beijing has repeatedly denied being behind the intrusions.

## SANS Institute Warns of Novel Cloud-Native Ransomware Attacks

Mar 17, 2025 The Hacker News



DEFENSESCOOP Topics Events Podcasts Vi

CYBER

## Hegseth calls on DOD CIO to protect tech supply chain from influence of China

The order comes after an eye-opening investigation revealed Microsoft had been relying on China-based engineers to support DOD cloud computing systems.

rubrik

# It’s Time to Stop Hitting Snooze!

## China Is Winning the Cyberwar

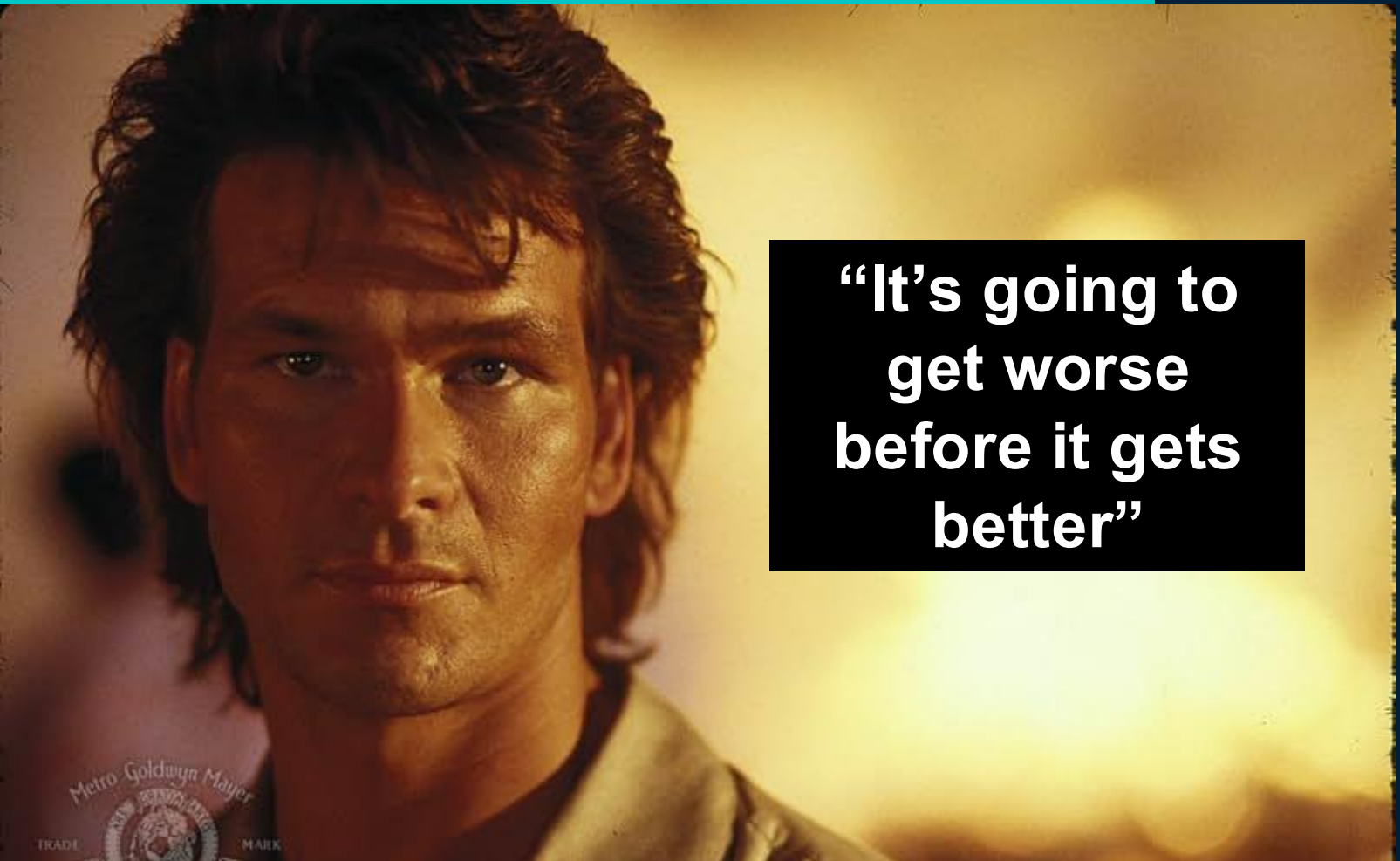
*America Needs a New Strategy of Deterrence*

ANNE NEUBERGER

September/October 2025

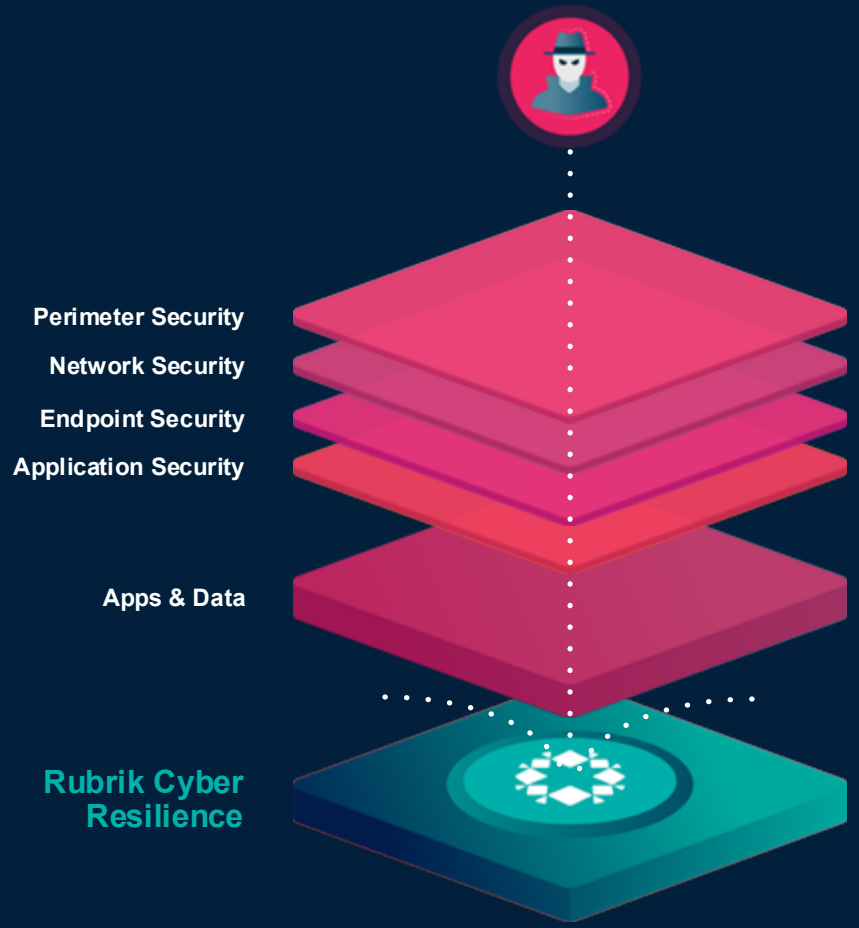
*Published on August 13, 2025*

# What Next?


“It’s going to get worse before it gets better”
Metro Goldwyn Mayer
TRADE
MARK

# Zero Trust: Assume Breach!

# Can You Recover From A Cyber Attack Within 24 Hours?



# Mission Resilience

# Security Guidance

## Assume Breach


Executive Order 14028

CISA Zero Trust Maturity Model v2.0


DoD Zero Trust Reference Architecture v2.0

DoD Zero Trust Strategy v1.0

CJCSM Cyber Survivability Endorsement

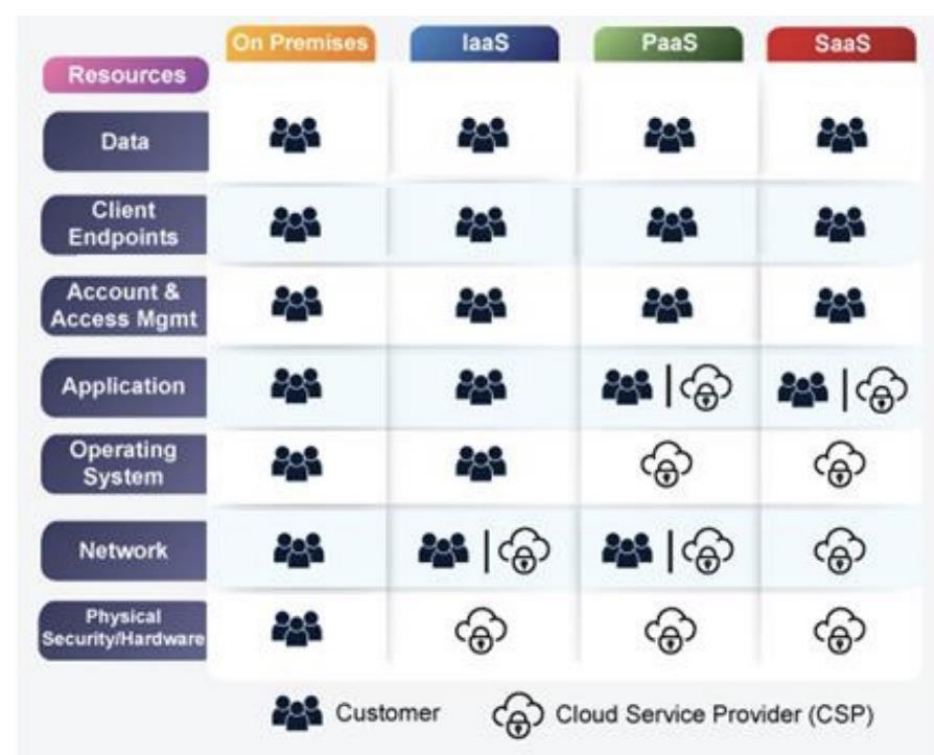

NIST AI Risk Management Framework

Building Cyber Resilient Systems

CSF 2.0

# Responsibility Model

## NSA Uphold the Shared Responsibility Model




"Customers are responsible for data stored in the cloud."

"Actively Hunt for Intrusions in the Cloud."

# Cyber Resilience

## NIST SP 800-160v2R1 Developing Cyber-Resilient Systems

### Cyber Resiliency Goals:

**Anticipate**

**Withstand**

**Recover**

**Adapt**

**Data Resilience is a foundational building block**

"Our infrastructure needs to have operational resilience, functional resilience, that even in the face of degradation, even if their systems are under attack, they can continue to deliver the vital functions."

**Brandon Wales**
CISA

# Why is the Cyber Survivability Endorsement needed?

- Lack of Cybersecurity and Cyber Resiliency metrics
- Limited by compliance requirements – the ceiling
- RMF is necessary but not sufficient to achieve and maintain an operationally relevant cyber risk posture
- Cybersecurity Supply Chain Risk – Cyber SCRM

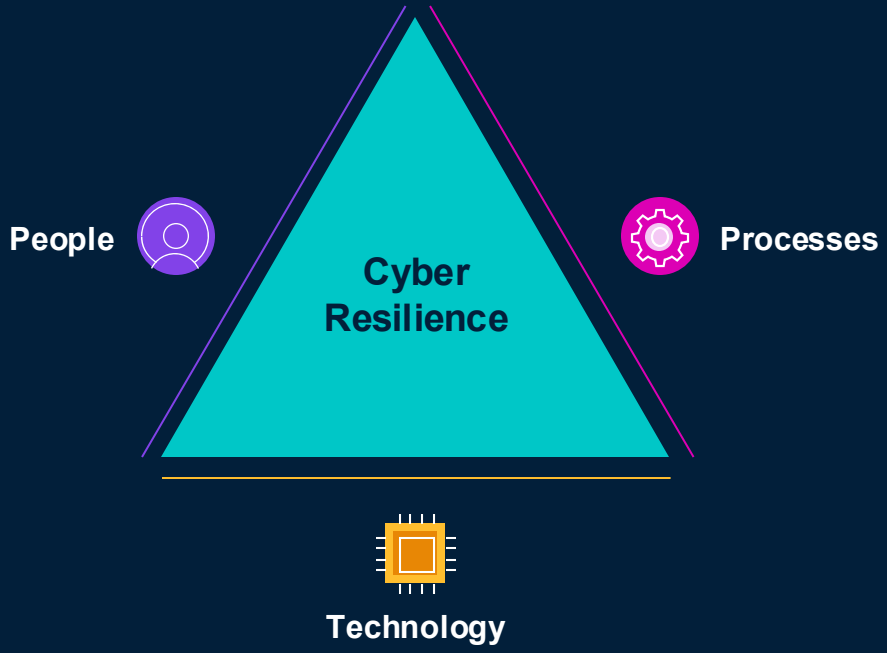
# CSA-09 Recover System Capabilities

Cyber Survivability Attributes (CSA)

- (U) “After a cyber-event, the system shall be capable of being restored to full functionality from a trusted source; at a minimum, being restored to partial mission capability, between mission cycles or within xx hours [specified by sponsor], to fight another day. System recovery shall prioritize cyber operational resiliency functions.”

# Zero Trust Architecture

## Making it work

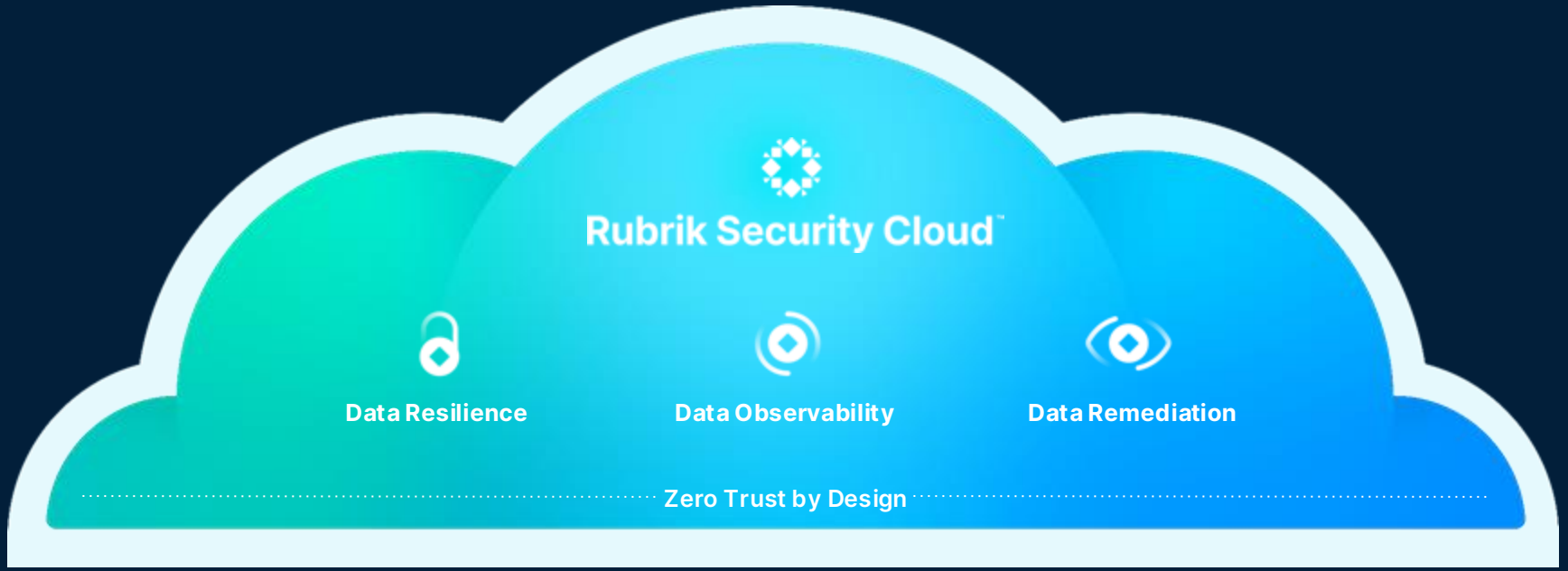



"We must ensure cyber attacks have limited impact, quick recovery and minimal disruption."

**Rob Joyce**

Former NSA Cybersecurity Director

# Last Line of Defense



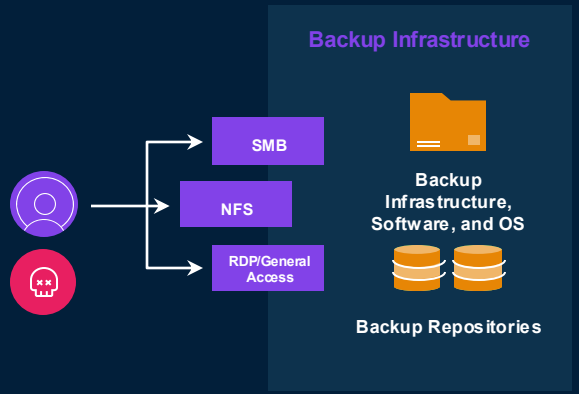
# Zero Trust Principles

## Trust nothing. Always verify.

- Network Security
- Identity and Authentication
- Principle of Least Privilege
- Tamper Prevention
- Observability

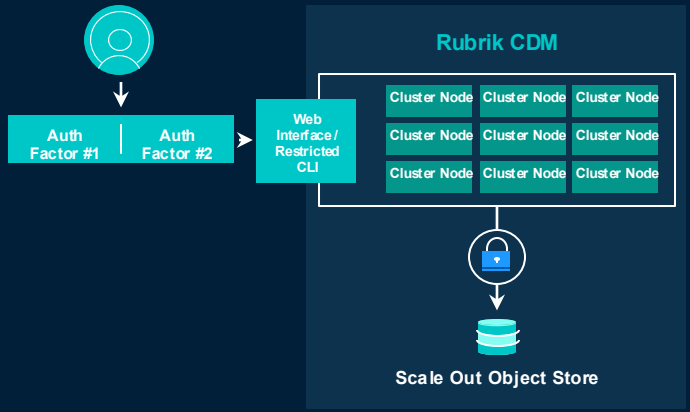
### Traditional Backup

- Native data copies remotely accessible to network + attack




### Rubrik

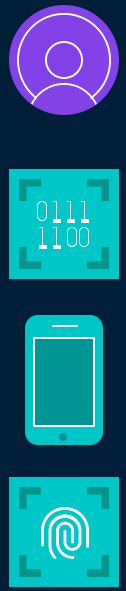
- Native backup data is not openly accessible on the network



# Zero Trust Principles

## Trust nothing. Always verify.

- Network Security
- Identity and Authentication
- Principle of Least Privilege
- **Tamper Prevention**
- Observability




**1**

Authorized Rubrik user gains access to system with MFA

**2**

Attempts to modify an SLA Policy in the system

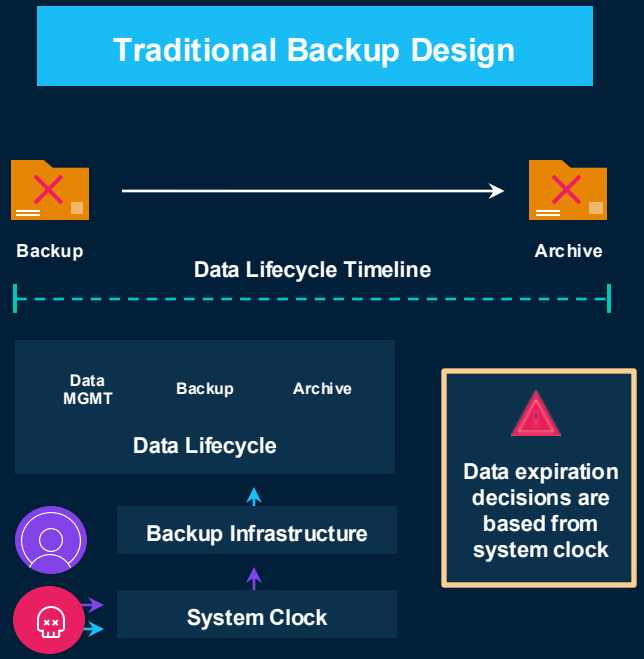

**3**

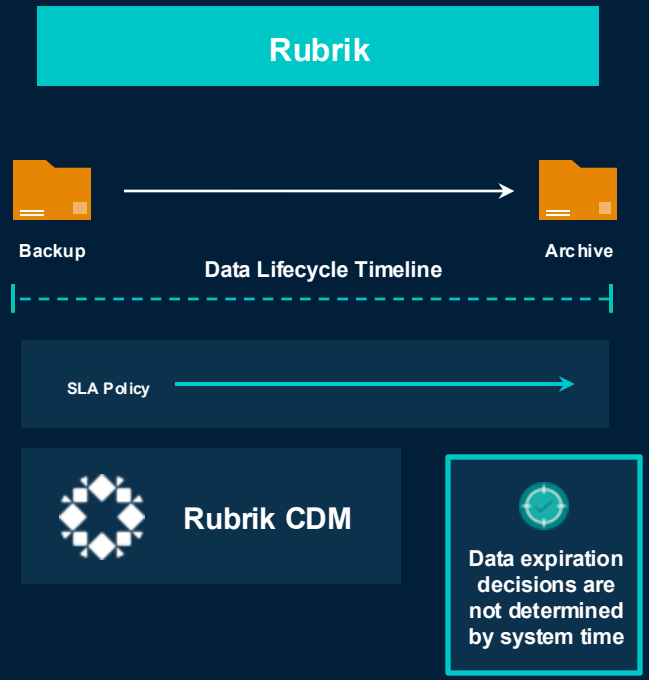
Rubrik SLA Retention Lock prohibits actions without support intervention and a 2-person validation

# Zero Trust Principles

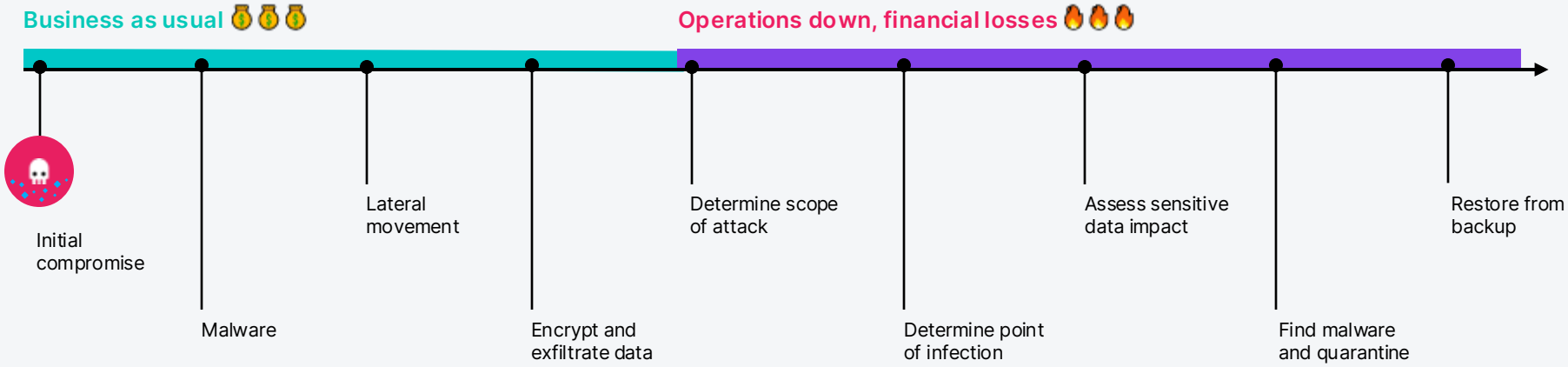
## Trust nothing. Always verify.

- Network Security
- Identity and Authentication
- Principle of Least Privilege
- Tamper Prevention
- Observability



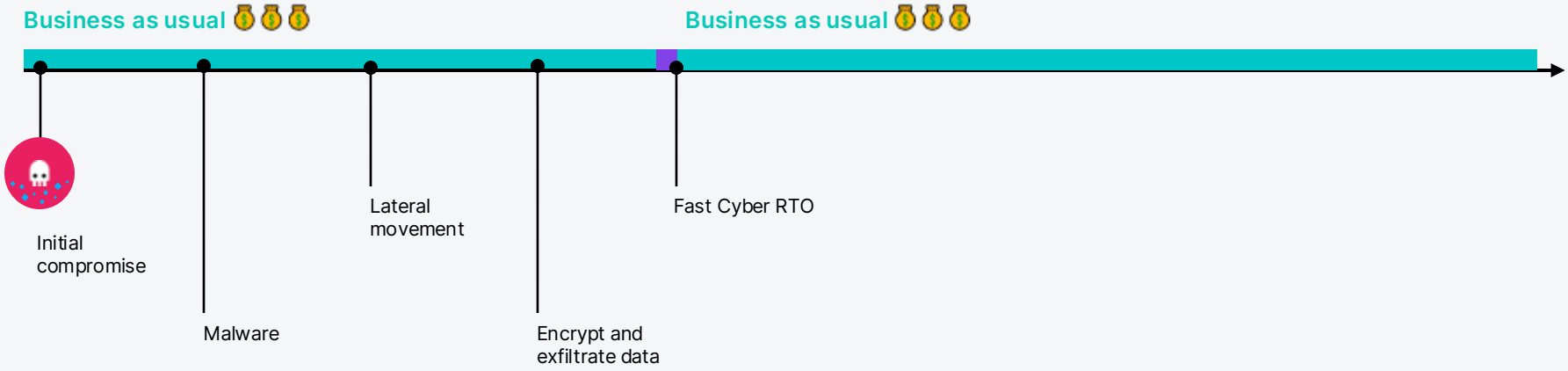



# Before Rubrik



# No wonder when you're breached, you're down for weeks.

# After Rubrik

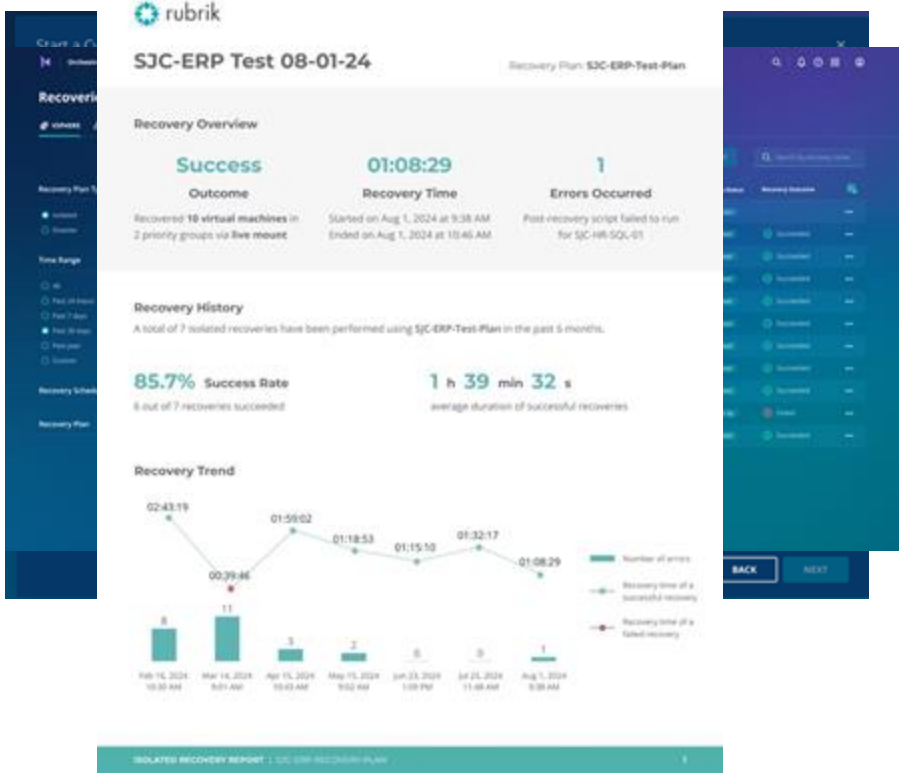


# Plan, Test, and Validate Cyber Recoveries

Plan and automate your disaster recovery, isolated recovery, and in-place recovery processes.

Regularly test the success of your recovery plans through manual and automated test runs.

Monitor recovery progress and download on-demand recovery performance reports.



# Cost Savings/Efficiencies

- Storage tier usage
- Single Pane - reduction of swivel chair management
- Hybrid cloud and multi-cloud friendly
- Reduced O&M by > 70%
- Can achieve TCO savings
- Rapid Cyber RTOs < 24 hours

Reduce Cloud storage costs up to 30%

# The Time to Act is Now: Proactively Protect Your Mission & Data

- Cyber and Data Resilience is Critical
- Keep the mission/data safe despite a cyber attack
- Test Your Backups
- Recovery - Speed of Trust, Speed of Decision Making
- Be Proactive – Go beyond compliance, cyber threat actors are banking on you only being compliant and reactive
- Data Integrity is key to Trustworthy AI
- Cyber Exercise Planning

**May not be able to recover when it Matters Most!**


# Thank you!

## Q&A

Travis.Rosiek@rubrik.com
www.rubrik.com