rubrik

Database Threats: Preventing the Worst With Zero Trust Data Management

Christopher Wolff

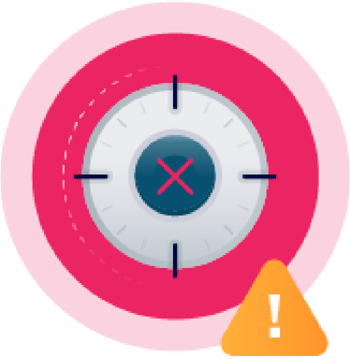
Database Solutions Architect

Today's Agenda

1. What's the problem?
2. Is there a solution?
3. How do we address it?

What’s the Problem?

You’ve been hacked or you don’t realize you’ve been hacked!



Defense-in-depth isn’t enough

Humans are not infallible!

Is There a Solution?

Security at the
point of data

Zero Trust throughout
the data lifecycle

Implement mitigation
plans to minimize impact

Proactive Mitigation

Preventing the worst from happening

What can we do *BEFORE* an attack?

Focus efforts in the following areas:

- Infrastructure
- Authentication
- Privileges
- Data Lifecycle
- Application Usage

Infrastructure

What can we do before an attack?

BIOS Firmware

- Often forgotten about
- Patch low level exploits

OS Platform

- Red Team vs. Blue Team
- Bug bounty programs
- Security updates keep OS hardened

Hypervisor

- Additional point of entry □ contain their own set of exploits

DB Platform

- Security updates
- Normal monthly updates
- Specific to database platform

Authentication

What can we do before an attack?

MFA

- Something you know
- Something you have
- Something you are

Password Storage

- Never in plain text
- Hash passwords

Password Policy

- Length > Complexity
- Breached Password List
- Consider not doing periodic resets

Token/Certificates

- Do not hardcode
- Treat like a password
- Expire tokens
- Use HTTPS

Auth0 Blog
NIST Password Guidelines

DZone Blog
Managing API Access Tokens

Auth0 Blog
Token Best Practices

rubrik

Privileges

What can we do before an attack?

Excessive Privileges

- Minimal permission
- Elevated access
- Ability to change data
- Admin or root access

Abuse of Privileges

- Rogue admin
- Grandfathered access
- Privileges revoked

Abandoned Privileges

- Users still active
- Users have left company

Data Lifecycle

What can we do before an attack?

Knowing Where Data Lives

- How many copies
- Stored in multiple places
- Copies of tables
- Sensitive data
- Flat files
- Spreadsheets

Storage Media Exposure

- Access to database files
- Access to backup files
- Access to delete data
- Physical access to storage

Data Placement

- Internal used data near externally used data

Application Usage

What can we do before an attack?

Data Masking

- Row level security + masking
- Clear text

Database Injection

- Elevated permissions
- Direct queries to the database

Auditing

- Usage auditing helps with forensics
- Work with auditors

Insurance Policy

How do we hedge our bets?

- Proactive mitigation can’t prevent everything
- We need a safety net against human error!

Human error is unavoidable

How do we hedge our bets?

Recovery Strategy, Not a Backup Strategy

- What are you trying to recover from?
- “0” data loss
  - Show them the bill
  - What data loss can be accepted

Backup Testing

- Does it meet your business requirements?
- 1 and done is not good enough
- Pull backup from storage
- Don’t overlook BMR

Zero Trust Data Security

Rubrik for Database

Consolidate database protection into one platform

Get time back with automated discovery and protection

Deliver near-zero RTOs while keeping DBAs in control

Support secondary users with self-service clones

> It’s a huge relief for us knowing that our most critical database is protected with Rubrik.

Adam Monnery
Head of Information and Communications Technology,
Museum of London

MUSEUM OF LONDON

> We chose Rubrik for its automated management of Oracle databases and its ability to greatly reduce our RTOs.

Edward Poll
Head of IT Infrastructure,
Cranfield University

Cranfield University

rubrik

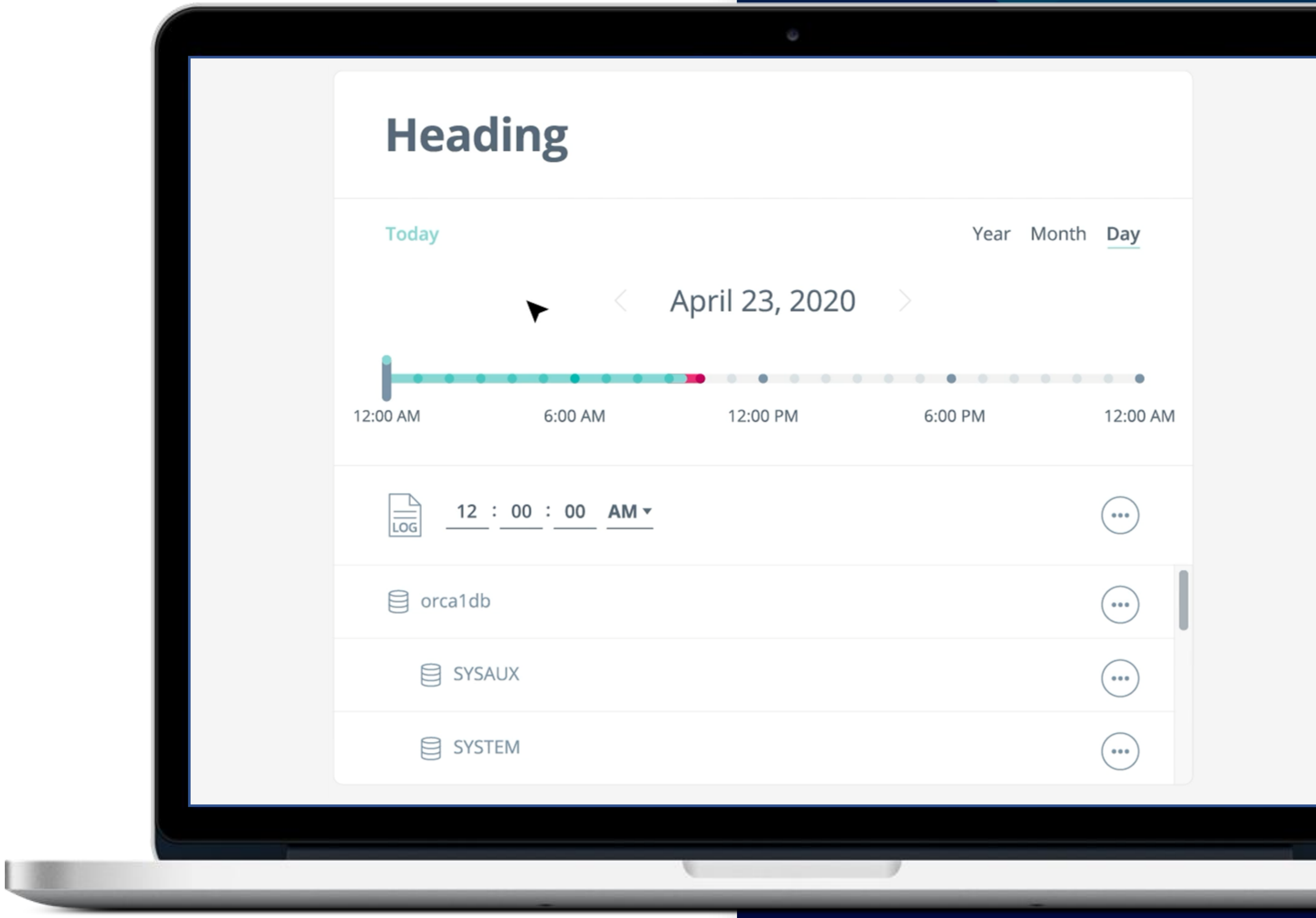
Designed for Recovery

Rubrik for Database

Enable near-zero RTOs without the need for added storage

Flexible recovery options to keep DBAs in control

Ensure backups are valid and recoverable

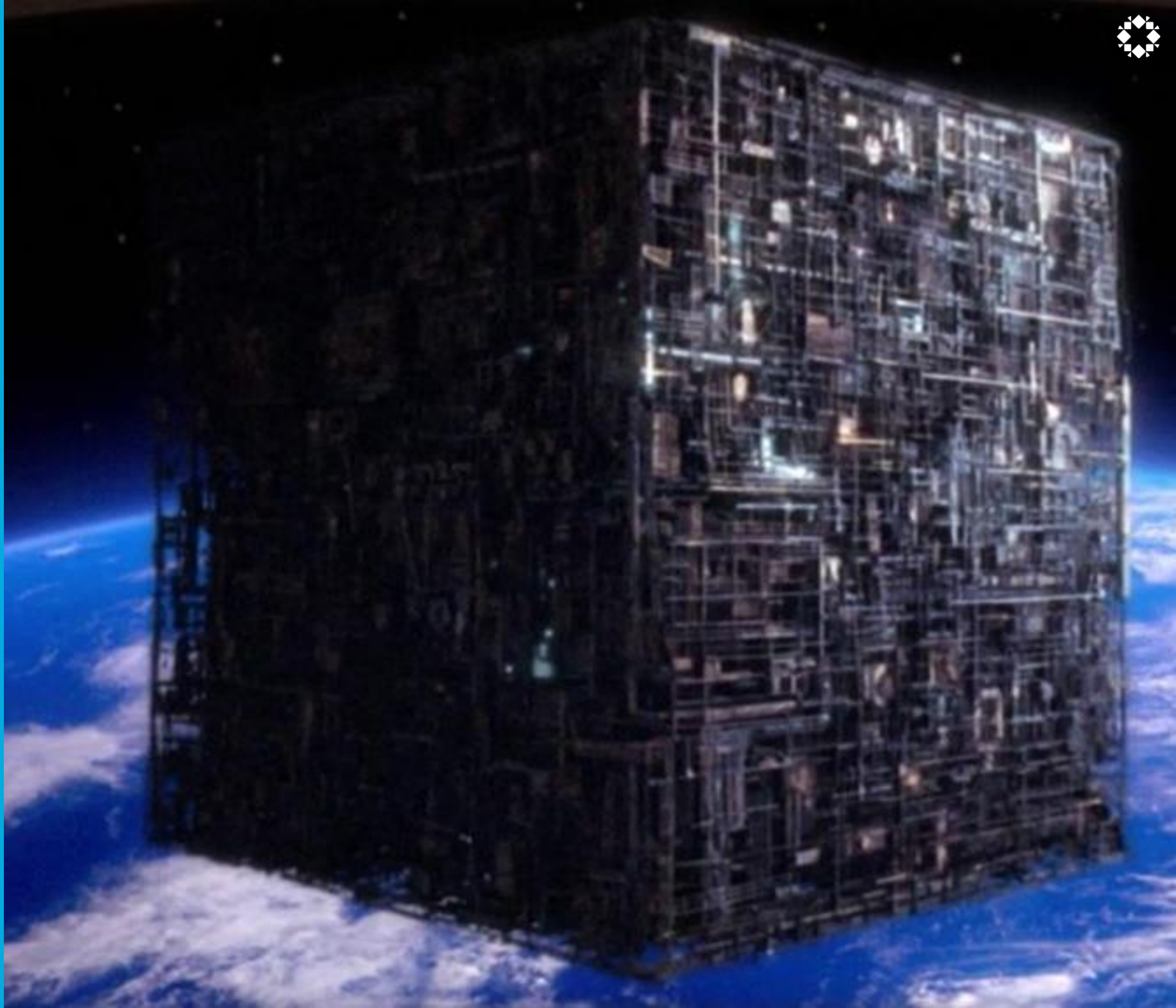


rubrik

Reactive Mitigation

Dealing with the worst happening

Resistance is futile…



Stop...breath...stay calm...think before acting

Dealing with the worst happening

Affected Assets

- What’s good?
- Blast Radius
- Recovery Steps
- Targeted Recovery

Recovery Plan

- Run books
- Recovery times
- Recovery isolation

Recovery Tools

- Clean backups?

Stopping Operations

- Stop operational tasks
- Don’t backup
- Don’t delete

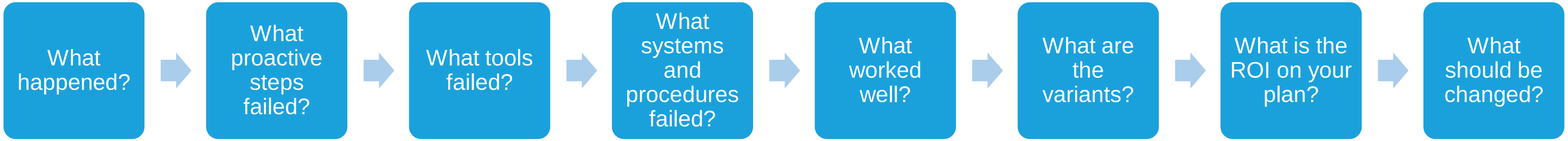
Communication

- Does everyone know the recovery options?

rubrik

Postmortem

Dealing with the worst happening



What happened?

What proactive steps failed?

What tools failed?

What systems and procedures failed?

What worked well?

What are the variants?

What is the ROI on your plan?

What should be changed?

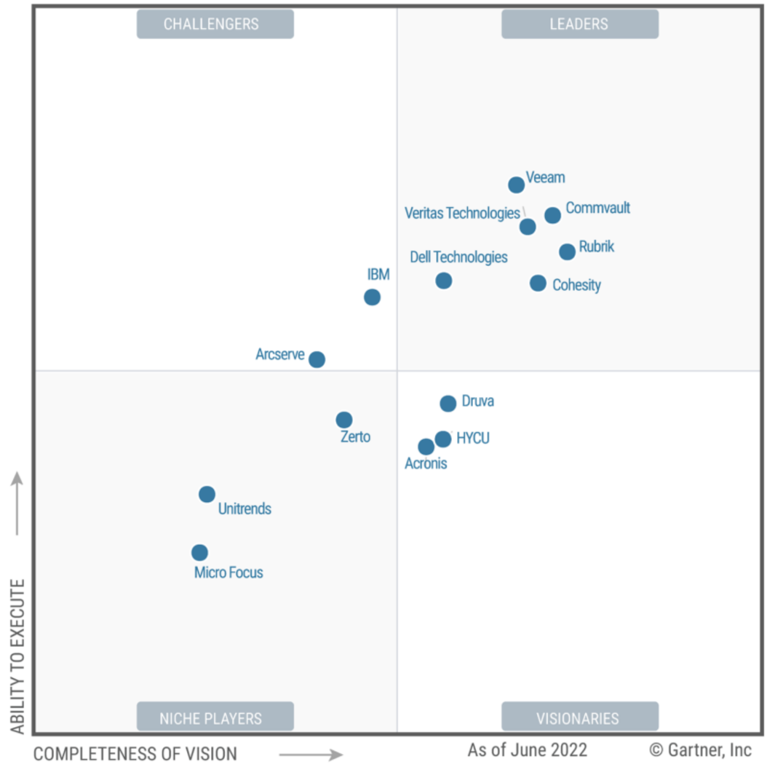
Key Takeaways

1. Work with your security teams
2. You can’t prevent every risk!
3. Plan, Prepare, Practice!

Leader for the third year in a row

Rubrik achieved the furthest overall position in Completeness of Vision

Figure 1: Magic Quadrant for Enterprise Backup and Recovery Software Solutions



Source: Gartner (July 2022)

> Protecting hybrid, SaaS and multicloud environments, preparing for ransomware attacks, and the need to simplify backup and data management are forcing I&O leaders to rearchitect their backup infrastructure and explore other solutions.

Gartner

Source: Gartner, Magic Quadrant for Enterprise Data Center Backup and Recovery Solutions. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

Resources & Next Steps

Some info to get you started

Let's Get Started

- Register for Virtual Demos: Learn about Rubrik Products and Solutions
- Attend Virtual Camp Rubrik: Get firsthand look at Rubrik
- Take a Savings Assessment: Get your custom report and see why people switched

General Resources

- **eBook:** An Ultimate Guide to Rapid Ransomware Recovery and Cyber Resiliency
- **eBook:** Modern Data Protection for Databases
- **eBook:** Top 20 Questions to Ask When Modernizing Your Backup

rubrik | Zero Trust Data Management™

Thank you.