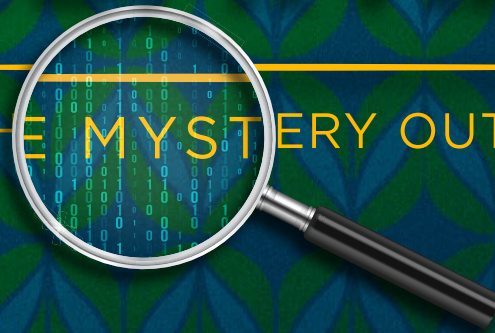


WHO'S COMPROMISING THE COMPANY?

TAKING THE MYSTERY OUT OF BCDR



CONTENTS

Setting the Stage.....	02
Keeping Tabs On All the Threats: How the BCDR Landscape Has Changed.....	03
What a Modern BCDR Plan Looks Like.....	06
Rubrik and Microsoft Are On the Case.....	13
The Case of the Payette Cyber Breach.....	18
Wrapping Things Up.....	20
Resources.....	21

SETTING THE STAGE

A data center is taken out by an earthquake or flood. A head of technology leaves and locks out key systems. Hackers break into an environment and hold your data hostage.

Companies like yours confront worst-case scenarios every day. If you don't have a good Business Continuity Disaster Recovery (BCDR) plan in place, you can lose millions in revenue. Your reputation can suffer. You can even go out of business.

The goal of this ebook is to help you avoid all that with a BCDR plan that ensures you:

- > Have control of your data at all times
- > Stay poised for recovery in case of a breach
- > Achieve strong organizational security
- > Quickly return to business as usual if you do get hit.

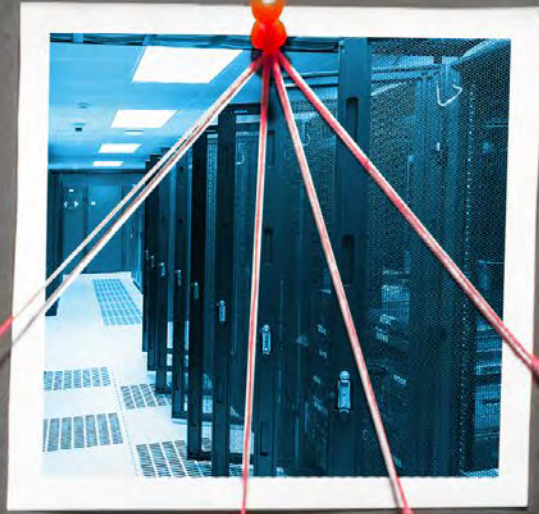
We start with an overview of the steps we at Rubrik put in place for our own BCDR plan. Our recommendations cover both traditional and new threats, and apply wherever data lives — on prem, in the cloud, or a mix. Next, we'll look at what to consider, the why behind certain initiatives, and some questions that will help you figure out how to get things done. Then we'll show how Rubrik and Microsoft can help you meet your own data security challenges. It's what works for us, and we hope you find it useful as you create your own plan.

Let's get started.



KEEPING TABS ON ALL THE THREATS

How the BCDR Landscape Has Changed





A SERIOUS THREAT CAN COME FROM ANYWHERE

Business continuity management has been around for decades, becoming more sophisticated as we've all become more dependent on technology. For a long time, good BCDR plans only had to focus on events like a natural disaster, market volatility, or a disgruntled (or absentminded) employee. Savvy companies set up procedures that would mitigate damage and get them up and running quickly. They were ready if disaster struck.

In today's business environment, you no longer have the luxury of that mindset. Because with malware, ransomware, and other cybercrime added to the traditional challenges, it's no longer a question of if your data will be compromised, but when.

Rubrik Zero Lab's [survey of 1,600 IT and Security leaders](#) found that cyber-attacks are becoming more serious and more frequent. On the right column, survey respondents (who are some of the most senior personnel in their companies) dealt with significant issues in the last year:

98% reported that a cyberattack reached their level of awareness

On average, they were made aware of attacks **47 times**

52% suffered a data breach

51% dealt with ransomware



All of this is in addition to other security challenges such as:



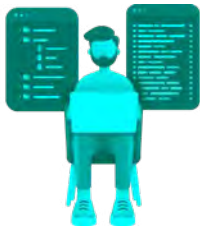
Remote Workers



Access Control



Ai-Powered Attacks



Insider Threats



Phishing

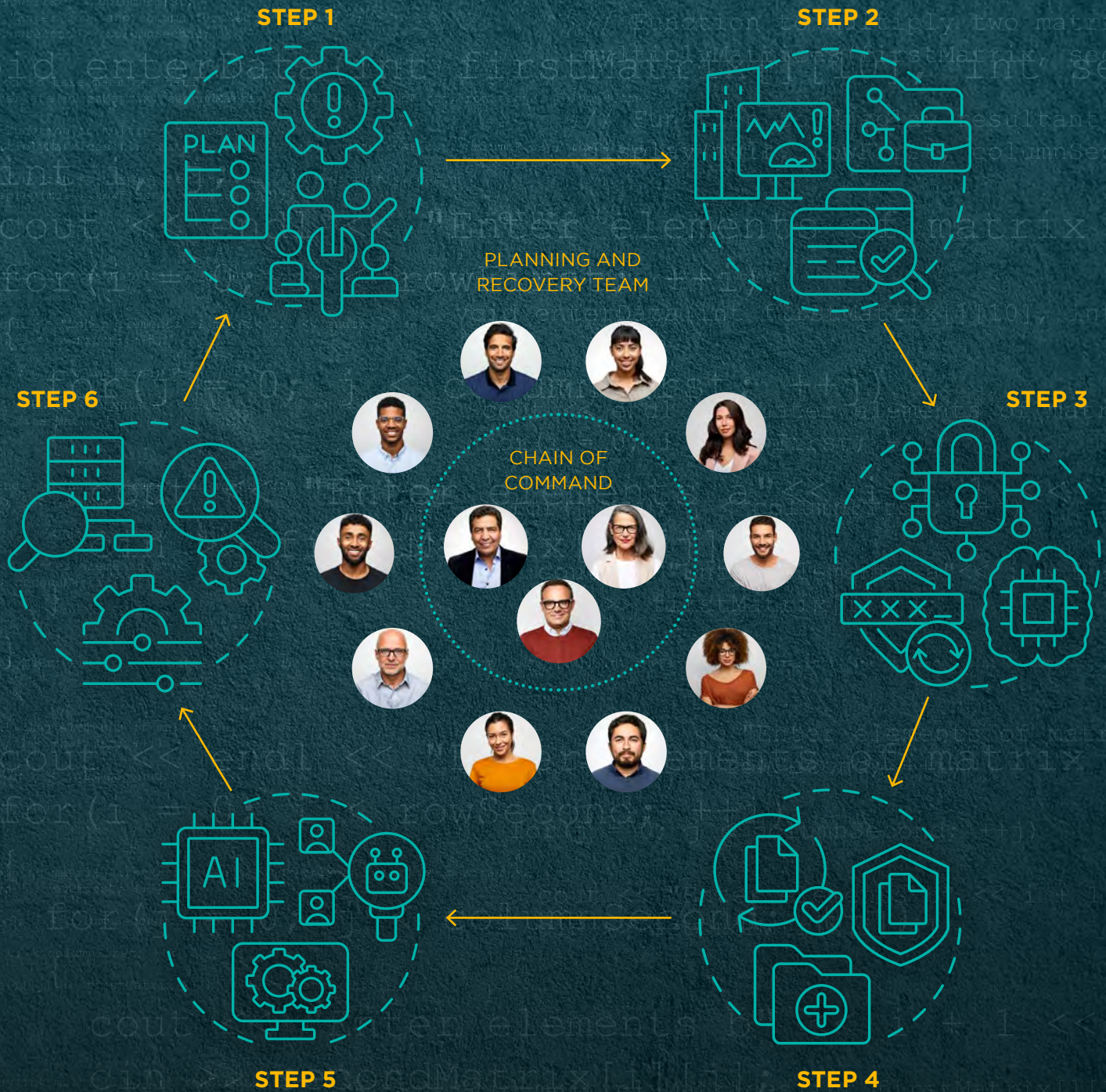


Vandalism

WHAT WE KNOW

Cybercrime is the number one reason for companies needing data recovery today.

WHAT A MODERN BCDR PLAN LOOKS LIKE



It may be elementary, but we'll say it anyway:
The time to build a modern BCDR plan is before you need it.

Your plan must guard against four very real risks: reputational, regulatory, legal, and financial. Ultimately, your goals should be to build resilience in your organization and safeguard the interests of your key stakeholders, whether they're internal or external.

At Rubrik, we developed steps to help us form our own recovery playbook:



Basically, it boils down to **people, process, and technology**. Let's go through the reasoning for each of these and see what key questions you can ask to flesh out your own plan.

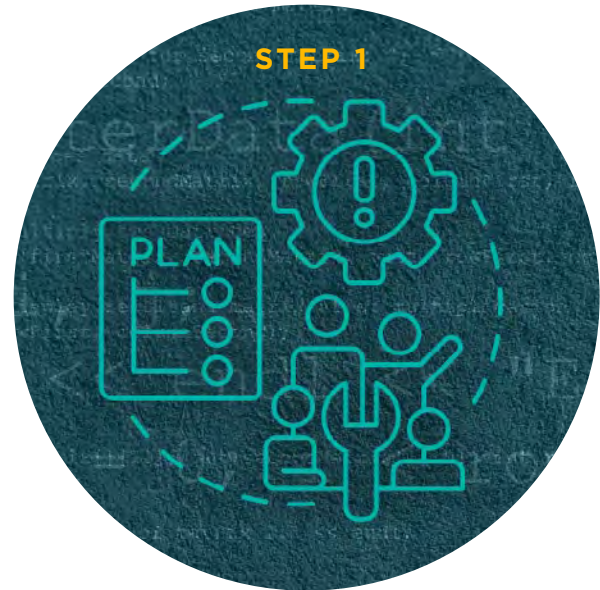


Establish a Planning and Recovery Team

Disasters aren't tidy, and they don't respect business hours. They can happen on the weekend, 2am, holidays, your birthday...really, any time. You don't want to be left scrambling to figure out who should be doing what while your business is offline or under attack.

Whether you have a crisis response team in place or need to build one from scratch, it's critical to set expectations:

- **Who are the key teams and individuals?** It might not be all hands on deck, but you'll need input and participation from across your organization (including folks you might not have thought of, such as Legal).
- **What is the chain of command?** In time of crisis, the person who makes the final decisions should be available and responsive.
- **What is each team member's responsibility?** Who does what, when, and in consultation with whom?
- **What are the methods and procedures for communications amongst the team?** It's a three-day weekend and your app is down – how do you get in touch with the right people?
- **What kind of internal reporting is necessary (outside the team), and who is responsible for it?** Are there any people outside the immediate recovery team who need to be updated on a regular basis?



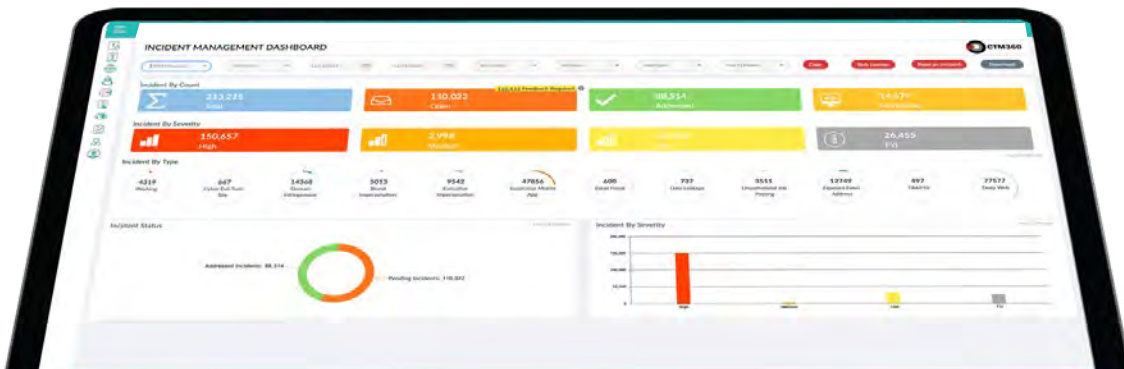
Understanding these details beforehand will help ensure a smooth response and recovery when time is tight and stress levels are high.



Perform a Business Impact Assessment

Not all threats are created equal. A hacker holding all of your customer data for ransom, for example, could be much more serious than a partial server failure. A business impact assessment will help you set expectations for level of effort and recovery.

- **What level of severity will potential threats have on your business?** At Rubrik, we classify them as low, medium, or high, depending on scope and scale.
- **What are your recovery time objectives (RTO) and recovery point objectives (RPO) for threats?** How quickly should your app be available after it's down, and how much data can you afford to lose?



In a disaster, clarity is key. When your team has benchmarks, they'll have a clear goal to strive toward in a chaotic time.



Identify and Protect Critical Systems and Data

Here's where we get to the real meat of your plan, especially in a cybercrime scenario... keeping the bad guys out in the first place and preparing to get up and running quickly.

You'll want to establish protection – especially Zero Trust security – at every potential point of vulnerability: perimeter, network, endpoint, application, and data. And you'll want to know exactly what to do if there's a breach or failure.

- **Which apps, systems, and data are critical?** What, exactly, do you need to protect and restore in the first place?
- **Where can data go?** If you need to rollover to a different environment, where do you have capacity?
- **What is the proper order to restore systems?** What, if any, are the dependencies in the environment that need to be taken into account?

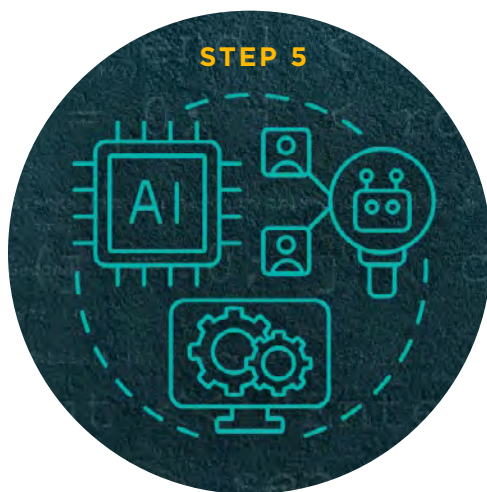


In the next chapter, we'll go more in depth about how Rubrik and Microsoft can help you with this step, which is one of your most important challenges.



Document Policies and Procedures

Once you've thought through your plan – established a team, run an impact assessment, and identified critical systems and data – it's time to document the process. Write it down and make it accessible within your organization so the right people know exactly where to go and what to do when the time comes. You'll be happy you have a structure to follow when time is of the essence.



Put Resources In Place

Now that you know what to do, you have to make it possible to do it. You've likely discovered some gaps – areas where you need resources to put your plan into action.

- **Do you have the right people to implement the plan?** You'll need people with the right skillsets – and enough of them to do it quickly.
- **Do you have the technology you need?** Security, failsafes, rollover options... you'll need a variety of tools, and the middle of a disaster is not the best time to go scrambling for them.



It's a good idea to build these considerations into your budget and acquire them as soon as possible. The cost of downtime (in both revenue and reputation) could far outstrip the funds you'll need to adequately prepare for disaster.



Test and Update Plan Regularly

Even the best plan can have weaknesses; you'll want to know yours before a hacker figures it out. At Rubrik, we test our BCDR plan at least quarterly. And we update it as new threats and trends emerge, or with what we've learned from a threat that's hit us. This kind of regular challenge helps keep us on our toes and makes sure our plan isn't gathering dust (and becoming irrelevant in the process). And we've made it possible for you to do this easily.



With our [Cyber Recovery](#) tool, you can create, test, and validate whether your recovery plan works, so you're prepared to meet your recovery SLAs.

In essence: Trust, but verify.



Now that you have our recommendations for building a strong BCDR plan, let's look more in depth at how you can protect your critical data with Rubrik and Microsoft.



RUBRIK AND MICROSOFT ARE ON THE CASE

EVIDENCE



JANITOR
ACCESS LEVEL:
FULL



CYBERCRIMES



At Rubrik, we address companies' most pressing data challenges: rapid recovery from ransomware, automation of data operations, and the transition of data to the cloud.

Together, Rubrik and Microsoft add even more value, providing Zero Trust data protection for hybrid cloud environments spanning data center, edge, and cloud, including Microsoft 365. Here are just some of the benefits you'll see when you have the power of Rubrik and Microsoft working together for you.



We Save You Money

If you were to piece together your own data protection and recovery mix, you'd easily need at least ten to 15 different tools to cover everything we do. In addition to the cost of the tools themselves, you'd have the management costs for your team to keep multiple products up and running (and working together smoothly). We offer one holistic solution for multiple challenges. That just seems simpler (and more cost effective), no?



We Save You Time

When your app is down or your data is held hostage, time is of the essence. We get you up and running quickly, with features like management simplicity via policy-driven automation; fast recovery with instant access, from on-prem to Azure; and native protection of your virtual workloads and SaaS applications running on Azure. You'll see near-zero RTOs, self-service automation at scale, and accelerated cloud adoption.

Rubrik Adds Value to Microsoft Azure and M365

With Rubrik and Microsoft working together, you have a powerful tool for detecting and fighting hackers and other threats to your environment.


In Azure and M365, Rubrik:

- Provides monitoring and investigation
- Alerts to anomalies in the data
- Alerts for malware hitting the environment
- Provides snapshots to enable forensics:
 - When did malware hit?
 - What data was affected?
 - What's the last known clean copy?
- Prevents malware reinfection



We Deliver Best-In-Class Technology

First-class technology and security are at our core. With Microsoft, you have a smart, well-developed, time-tested platform you can trust. Add Rubrik's monitoring and investigation, malware and data anomaly alerts, forensic snapshots, and reinfection prevention for Azure and M365, and you can be confident you have the tools you need to prevent and address data breaches. Plus, we're constantly analyzing new threats and updating our technology so you're protected in the future, as well.



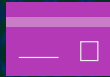
**Zero Trust
Data Protection**

Data Available
with ZT Architecture



**Ransomware
Investigation**

Discover Data
Anomalies with ML



**Sensitive Data
Discovery**

Classify Data and
Assess Exfiltration Risk




**Incident
Containment**

Discover Point of
Malware Infection



**Orchestrated
Application Recovery**

Recover Apps & Data
with Guide Workflows



Cloud Vault

Logically air-gapped
archive built on Azure



We Make Your Life Easier

You're likely already doing business with Microsoft, and Rubrik intelligence is an easy extension of all that Microsoft goodness. Our partnership enables us to architect a solution that makes the most sense for your business. That means data protection and recovery are easier to adopt, easier to integrate, and easier to scale. And who couldn't use a little more easy in their lives, especially in a crisis situation?

Whether you're adopting the cloud to improve security, scalability, and remote management, or keeping your data on prem, Rubrik and Microsoft have the solution you need for end-to-end data management and protection of your enterprise applications, including backup and disaster recovery and data security.

With our solution, mission-critical applications such as SAP, SQL, Oracle, VMware, as well as enterprise NAS workloads, can tightly integrate protection and automation with Azure – a critical part of your digital transformation. Together, we can help you address your data protection and recovery needs while saving you time, resources, and headaches.

Rubrik and Microsoft Solve For:



THE CASE OF THE PAYETTE CYBER BREACH



THE PLACE

Payette is an award-winning architecture firm with a mission to create buildings of purpose: life learning, discovery, and healing. Payette's architects have shaped all kinds of buildings, from cutting-edge 5.5 million-square-foot science centers to world-changing hospitals across the globe.



THE CONTACT

Dan Gallivan, Director of IT for Payette: "Once I got to the office and started to bring the system back up, I realized this wasn't just a standard power outage. We were under attack."



THE CRIME

One early Saturday morning, Dan got a call that systems were down. He soon learned, however, that Payette was under attack.

A hacker had compromised an admin account and waited until after hours to initiate his attack, encrypting and corrupting 50TB of Dell EMC Isilon data. Windows servers and network data shares were also compromised.

THE OUTCOME

Luckily, the Payette team had already segmented data, using Rubrik CloudOn to migrate VMs to Azure and Rubrik CloudOut to deploy and build their Azure infrastructure. This meant:

- Critical systems were online in less than 24 hours
- Payette thwarted the cyber attack before the hacker could demand ransom
- 100% recovery within one week
- Zero data lost
- Microsoft 365 and Azure stayed resilient against cyber threats

Uncover more details on the Payette case [here](#).

WRAPPING THINGS UP

Today, more than ever, you need a robust, modern BCDR plan that can meet the challenges of today's business environment.

We recommend:

- > A **Planning and Recovery Team** to manage crises
- > A **Business Impact Assessment** to set expectations for response and recovery
- > **Protection** for your critical systems and data
- > Detailed and accessible **documentation** of your plan's policies and procedures
- > Adequate **resources** – both people and technology – to address crises
- > A regular cadence for **testing** your plan and **updating** when necessary

With cutting-edge technology, unified tools, and a team who's always on the lookout for the next threat, Rubrik and Microsoft have the solutions you need to protect and recover your data living on Azure and 365.

If you'd like to learn more about Rubrik's superior solutions for data protection and our proven approach to formulating and executing a modern BCDR plan, contact one of our BCDR experts at **1-844-478-2745** or **BCDR@rubrik.com**.

Never compromise your company again.



FOR HELP WITH YOUR OWN SOLUTION

This ebook is partially derived from ActualTech Media webinars [[Part 1](#), [Part 2](#)] featuring Rubrik Global Field CSO and CISO John Murphy and Microsoft Principal Product Manager Karl Rautenstrauch, as well as the [Rubrik on Rubrik BCDR](#) webinar featuring Rubrik CIO and Chief Data Officer Ajay Sabhlok.

For more information on Rubrik capabilities with Microsoft, visit our [Azure](#) and [365](#) pages and [our 365 solution overview](#).

To review an independent evaluation of Rubrik's capabilities, download the analyst report [Gartner® Critical Capabilities for Enterprise Backup and Recovery Software Solutions](#).

For more in-depth information on how to address disasters and build a BCDR plan, visit the following:

- > [Business Continuity Institute](#)
- > [Disaster Recovery Institute International](#)
- > [Institute for Business Continuity Training](#)

THE RUBRIK + MICROSOFT PARTNERSHIP

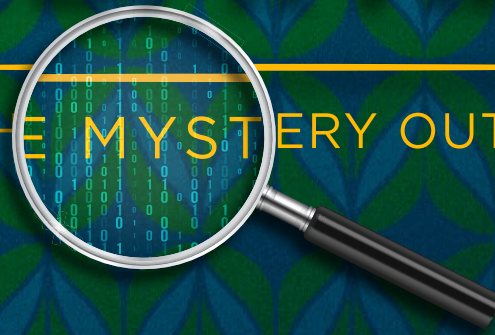
As the number one partner to Microsoft, Rubrik has pioneered cutting-edge technology built on zero trust principles that secures the entire data lifecycle. As one of the most trusted brand in the world, Microsoft brings reliable, complementary technology that works on proven platforms.

Together, we deliver an integrated BCDR solution that stands up to modern cyber threats. Our custom, scalable solution ensures you retain control of your data, wherever it lives. It's the solid foundation you need to build strong organizational security, stay poised for a rapid recovery, and quickly return to business as usual.



WHO'S COMPROMISING THE COMPANY?

TAKING THE MYSTERY OUT OF BCDR



 rubrik +  Microsoft

