rubrik | Microsoft

The New Business Continuity: Enhancing BCDR with Zero Trust Data Security

Abstract

When work no longer has any boundaries, how do you know what to protect?

This complicates business continuity and disaster recovery (BCDR) planning, which requires companies to identify risks and critical business resources, put risk mitigation plans in place, and prepare backups. The Zero Trust framework offers a new way to approach BCDR. For this new framework to stick—without impacting business operations and employee experiences—organizations will need the right data protection platform.

Over 30 percent of employees currently work remotely while 60 percent work in hybrid environments.[1]

Chapter One

The New Challenges Facing BCDR

"If you know your enemy, and you know yourself, then you need not fear the result of a hundred battles."

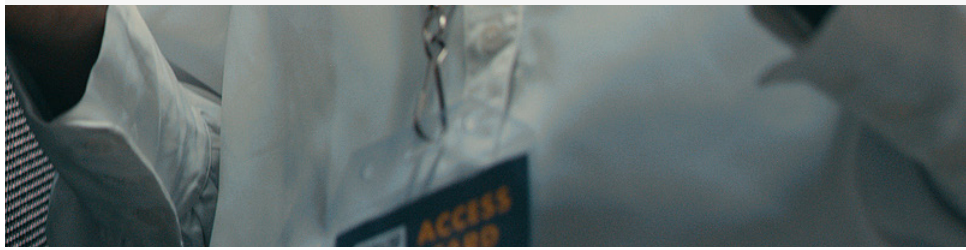
When Sun Tzu wrote those words, he may not have had business continuity and disaster recovery in mind, but they certainly apply. Today, cyberattacks and business interruptions are not a matter of if, or even when—they're a matter of how many.

Globally, both individuals and organizations are facing those "hundred battles" the famous military strategist spoke of.

Most organizations are aware of their vulnerabilities, including cyber attackers, human error, system malfunctions, and natural disasters. What's a little harder to pin down is the right defense strategy and protective mechanisms. An effective BCDR plan calls for sharp awareness of critical systems, potential vulnerabilities and attack vectors, and what steps to take to restore normal business operations after a disruption. If there is an adverse event, it's crucial to identify what has happened, where it's happened, and the scope of the damage—quickly.

Without this information, organizations are forced to restore entire systems, losing perfectly good data that was never affected. But above all, they wind up wasting precious time—in some cases days or weeks—restoring their systems.

Unplanned downtime costs businesses 35 percent more per minute than planned downtime.[2] It also chips away at brand reputation.



Enterprises are generating data at a rapid pace

But it's not just money that companies wind up losing.

The amount of time it takes to restore compromised data turns an inconvenient interruption into an existential threat.

This need to protect data presents one of the biggest challenges facing modern business continuity and disaster recovery planning. Traditionally, companies have used tape archives for their long-term backup needs because tape is easy to store, dependable (one can't really "hack" it), and low cost. But tape storage cannot keep pace with the rate of data being generated. By 2025, enterprises are projected to produce 181 zettabytes of data yearly. That's up from 5 zettabytes in 2011.[4] Not only is it difficult to capture data at this rate using tape storage, it's difficult to restore it quickly in the event of an attack.

The two biggest challenges of unplanned downtime are lost revenue (53 percent) and data recovery (49 percent).[3]

Ransomware has a new target: backups

Even if companies do manage to back up their data at a rapid enough pace using traditional methods, cyber attackers have identified a new target: the backups themselves. The traditional M.O. of a cyber attacker is to gain access to an organization's data, encrypt the data, and then demand payment to decrypt it. Organizations that regularly backup their data simply restore from the backups and move on without paying a cent. Attackers have since caught onto this and now target both primary data sources and backups, so that organizations have no choice but to pay.

More data from more places and no perimeter

Further complicating modern business continuity and disaster recovery is the death of the perimeter. For decades, employees logged into company-issued devices on company property. IT teams put up a firewall and assumed that everything within the firewall was trustworthy. This isn't a viable approach with cloud computing, bring-your-own-device policies, and hybrid or remote working arrangements. And contrary to popular belief, VPNs are not the cure-all some believe them to be. VPNs were designed for a pre-cloud era, and often have difficulty keeping up with changing business requirements. Moreover, VPNs assume that the person accessing this "tunnelled" connection to the network is trustworthy. If a malicious user—or a benevolent user with an infected device—gains access to the network using a VPN, they can infect the entire system.

Fortunately, a new approach to organizational network security—the Zero Trust Framework—offers a solution.

The rapid proliferation of data, the increase in attacks on backups, and the shift to hybrid and remote work all present new challenges that modern BCDR teams must address.

Chapter Two

The Emergence of the Zero Trust Security Framework

If you work in cybersecurity, then you're familiar with the castle-and-moat approach to security. You're probably also aware that this approach is getting harder and harder to use as business needs change.

It takes a lot of effort to gain access, but once you're in, you're in, with the freedom to roam the palace grounds. But what do you do when you have to protect a million tiny castles that all have tunnel access into the main castle? Drawing a misshapen circle around all of these satellite locations would be difficult, especially if these spots are all over the world.

With the castle-and-moat method, organizations invest the majority of resources into protecting the perimeter with firewalls, intrusion detection systems, etc.

The alternative is a Zero Trust Security Framework. The Zero Trust Security Framework teaches organizations to trust no one, even if they're inside the network. Everyone is subject to a "trust nothing, verify everything" response. **The principles of the Zero Trust Security Framework are to:**[5]

- **Verify explicitly:** Security decisions are made based on all available data points such as identity, location, device health, data classification, anomalies, etc. Authentication is required and identities of users and services are continuously tested.
- **Use least privileged access:** Just-in-time and just-enough access is given, so people have the access they need to do their jobs and nothing more.
- **Assume a breach:** All access is treated as if it's a potential breach, meaning the potential damage zone is minimized using micro-segmentation, continuous monitoring, end-to-end encryption, and automated threat detection and response.

In practice, this means that organizations must be able to:[6]

- **Secure access:** Verify if a user or service is using Multi-Factor Authentication (MFA), for example through a combination of a password and a trusted device such as a phone or hardware key (or something inherent to the user such as a fingerprint).
- **Determine authorization:** Ensure users and services only have the access necessary to do their jobs so that an attacker wouldn't have the kind of administrative access that gives them the ability to do anything within the system.
- **Create immutable backups:** Organizations must be able to create immutable backups that can't be changed or encrypted by malicious actors.
- **Establish a logical air gap:** Physical air gaps (a separation between two systems) provide an effective safety buffer, but they cannot keep up with modern business needs. What's needed is a new, "logical air gap" that achieves the same objectives as a physical air gap.

Of course, if you work in cybersecurity, you know that implementing this approach is easier said than done. Traditional cybersecurity tools are more labor-intensive than people know. If enterprises want to implement a Zero Trust approach, protect their data, and avoid eroding the user experience, they need a platform that provides the tools, the abstraction, and the user interface to support security professionals.

Chapter Three

Bridging Data Security with Hybrid Work Environments

81%

Eighty-one percent of organizations have at least one application running in the cloud.[7]

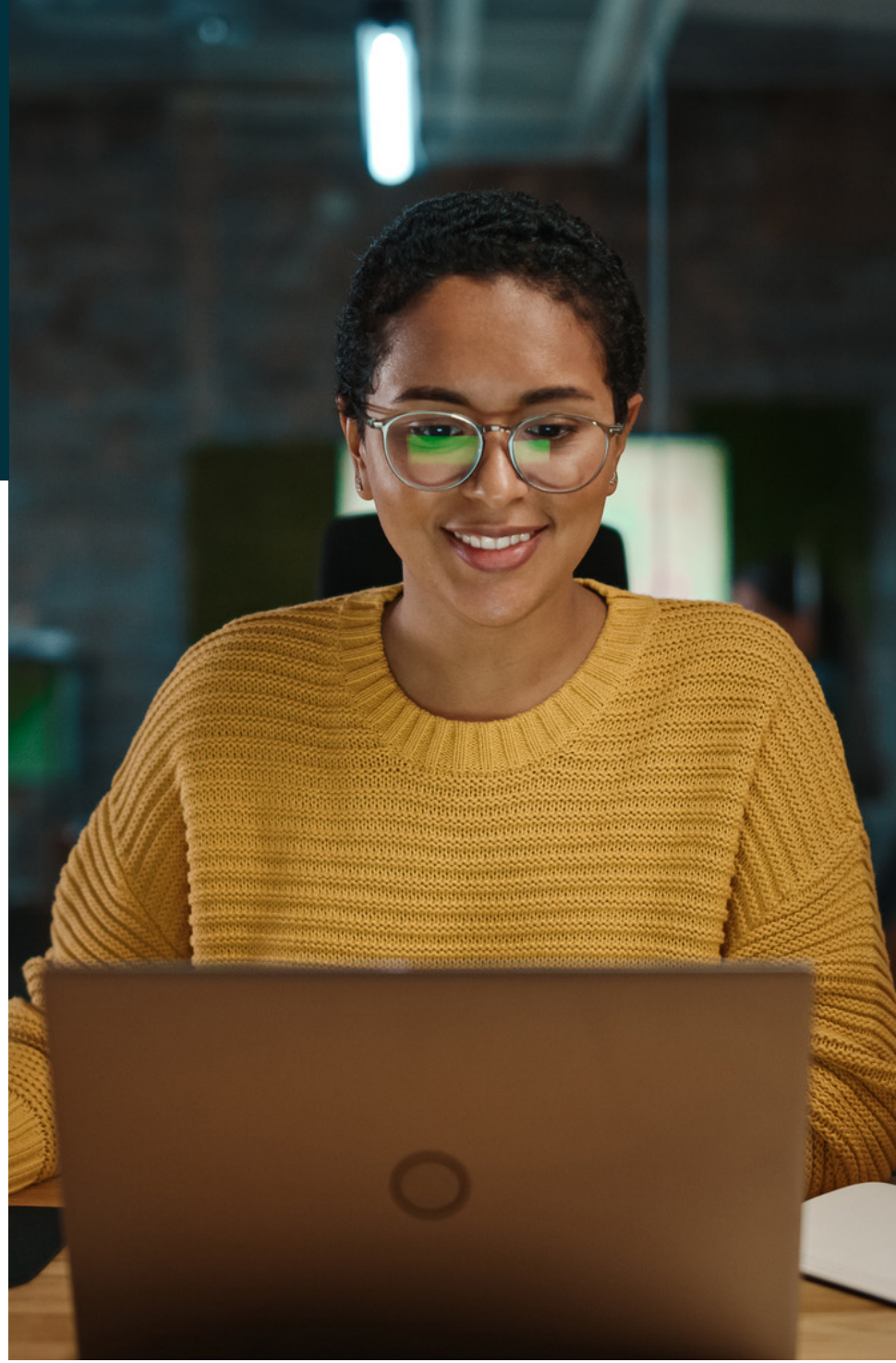
20%

Microsoft Azure has a 20 percent share of the global cloud market.[8]

+145 million

And there are over 145 million daily active users of Microsoft Teams.[9]

With so many organizations relying on Microsoft for their cloud computing needs, there's a need for a solution that seamlessly integrates with Microsoft services and delivers a reliable data backup solution while supporting a Zero Trust architecture.



You can extend Zero Trust into your Azure environment by using Rubrik Zero Trust Data Protection to:

- Ensure full data protection for virtual machines running in Azure
- Ensure full data protection for storage volumes via Azure Managed Disks
- Guarantee immutable long-term archiving using API-driven integration between Rubrik and Azure storage services
- Protect Microsoft 365 environments by creating a logical air gap for Microsoft data that is located outside of your Microsoft 365 account

Rubrik, the Zero Trust Data Security™ Company, delivers data security and operational resilience for enterprises. Rubrik's big idea is to provide data security and data protection on a single platform, including Zero Trust Data Protection, ransomware investigation, incident containment, sensitive data discovery, and orchestrated application recovery. This means data is ready at all times, so you can recover what you need and avoid paying a ransom. Because when you secure your data, you secure your applications, and you secure your business.

Here's how Rubrik Zero Trust Data Security™—a data management and cyber resilience platform—protects Azure environments.

Native multi-factor authentication (MFA)

All users are assumed to be unsafe until proven trustworthy, so they go through Rubrik-native MFA. While this MFA solution offers time-based one-time passwords, Rubrik has adopted SAML 2.0, so it can seamlessly integrate with Azure Active Directory, creating a centralized user-friendly solution that is easy for IT to manage. Azure AD provides a number of MFA options including SMA, voice, and an authenticator app.

Providing least privileged access

Your user's in, but that doesn't mean they get the run of the place. Now that they've been authenticated, it's time to ensure they only get access to what they absolutely need to do their work. They're authorized using Rubrik fine-grained Role Based Access Control (RBAC). This meets two key objectives:

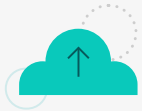
1. Ensuring least privileged access
2. Ensuring users can quickly access the resources they need

Enterprises can use RBAC to create predefined or custom roles that determine what a user has the right to access. This can also be easily aligned with predefined roles that have already been created in Azure.

Extending data immutability into Azure

Your employees, customers, and vendors are generating data at breakneck speed, so you need a way to back up that data as fast as it's created. Rubrik Zero Trust Data Protection stores information in a secure, immutable format that can't be changed once it's been ingested. As it's stored, it's broken up into chunks called patch files. An algorithm creates a data fingerprint that's applied to each patch file, and that fingerprint must be verified any time data is read from the backup to ensure that it is unaltered.

Rubrik securely transfers the data to Azure Blob Storage to create a readily available yet immutable offsite copy of each enterprise's data. This protection is also available for cloud-native workloads running on Azure when using Rubrik Cloud-native protection. This means that enterprises can have a rock-solid backup for traditional, on-premises, and cloud-based workloads.



Whenever organizations have to archive data from the Azure cloud environment, Rubrik integrates directly with the native immutability features of Azure Blob storage.

Establishing a logical air gap

In the past, companies backed up files on tape and then stored them off site, creating what's known as an air gap. While secure, the physical nature of tape storage makes it difficult for backup efforts to scale. **Rubrik grants all the benefits of a "logical air gap". This logical air gap is created through:**

- **Authentication:** Both the system's graphical user interface (GUI) and command line interface (CLI) are secured using multi-factor authentication, meaning attackers can't gain access to backups even if they have compromised credentials.
- **Authorization:** Access is granted with fine grained, role-based access control, meaning users can't move laterally within the system and access more resources than necessary.
- **Audit logging:** There's an audit trail whenever any changes are made that can be monitored locally or shipped to a log analysis tool.
- **SLA Retention Lock:** Organizations can prevent unauthorized reduction in data retention so that data is always ready to be recovered using Rubrik SLA Retention Lock.

Rubrik supports a core set of technologies that set it apart from legacy backup solutions:

- **Immutable data platform:** No external or internal operation can modify data once ingested. Data managed by Rubrik is never available in a Write state to the client, so it can never be overwritten. This means that even if infected data is ingested by Rubrik, it can't infect clean files and folders.
- **Declarative policy engine:** Rubrik makes it simple for organizations to carry out data protection activities. With the Rubrik declarative SLA policy engine, simple input fields set RPO, retention period, archive target, and replication target.
- **Threat engine:** Organizations get a full perspective of what's going on in a given workload thanks to machine learning that analyses each backup snapshot's metadata. Rubrik detects anomalies, analyzes threats, and helps accelerate recovery in the event of an adverse event.
- **Secure API-first architecture:** Rubrik has an API-Driven Architecture. If something can be done through the Rubrik user interface, it can be done through an API secured by role-based access and OAuth 2.0 Bearer tokens.

Today's organizations need business continuity and disaster recovery plans that evolve with the threats they face. This means creating a nimble, flexible method of monitoring and detecting threats to a distributed work environment. It also means preparing for the *when*, not *if* of cyberattacks. This means protecting critical information in the event of an attack with a system that creates an immutable backup of data both at rest and in flight.

Still unconvinced? Rubrik offers a warranty of up to $5 million for customers who can't recover Rubrik-protected data after a ransomware attack. The warranty now includes Rubrik Cloud Vault, a fully managed, secure, and isolated cloud vault service built on Microsoft Azure. Through the integration with Microsoft Azure, Rubrik Cloud Vault simplifies air-gapping of critical data and provides end-to-end data immutability to ensure data is not compromised, corrupted, or maliciously deleted. With Rubrik Cloud Vault, customers are better equipped to recover their data as cyberattacks continue to increase in volume and sophistication. Learn more about why we're willing to put our money where our mouth is.

Learn more about the Rubrik Ransomware Recovery Warranty and Rubrik Cloud Vault

References

1 What is your workplace's stance on remote work?
https://www.statista.com/statistics/1111290/workplace-stance-on-remote-work/

2 The Real Costs of Planned and Unplanned Downtime.
https://www.ibm.com/downloads/cas/L57KW7ND

3 The Real Costs of Planned and Unplanned Downtime.
https://www.ibm.com/downloads/cas/L57KW7ND

4 Volume of data/information created, captured, copied, and consumed worldwide from 2010 to 2025.
https://www.statista.com/statistics/871513/worldwide-data-created/

5 Evolving Zero Trust: How real-world deployments and attacks are shaping the future of Zero Trust strategies:
https://www.microsoft.com/en-us/security/business/zero-trust

6 Zero Trust strategies:
https://www.microsoft.com/en-us/security/business/zero-trust

7 32% Of IT Budgets Will Be Dedicated To The Cloud By 2021
https://www.forbes.com/sites/louiscolumbus/2020/08/02/32-of-it-budgets-will-be-dedicated-to-the-cloud-by-2021/?sh=384b9af15fe3

8 Microsoft Azure – Statistics & Facts
https://www.statista.com/topics/8031/microsoft-azure/#dossierKeyfigures

9 Microsoft Teams usage jumps to 145 million daily active users
https://www.theverge.com/2021/4/27/22406472/microsoft-teams-145-million-daily-active-users-stats