the GORILLA GUIDE® to...

SECOND EDITION

Cyber Resilience for Databases

A Key Element of Your Database Protection Strategy

LARRY MILLER

POWERED BY ActualTech MEDIA

the GORILLA GUIDE® to...

Cyber Resilience for Databases

A Key Element of Your Database Protection Strategy

By Larry Miller

POWERED BY ActualTech MEDIA

www.actualtechmedia.com

PUBLISHER'S ACKNOWLEDGEMENTS

DIRECTOR OF CONTENT DELIVERY

Wendy Hernandez

CREATIVE DIRECTOR

Olivia Thomson

SENIOR DIRECTOR OF CONTENT

Katie Mohr

WITH SPECIAL CONTRIBUTIONS FROM RUBRIK

Amanda O'Callaghan
CORPORATE MARKETING

Justin Ruiz
PRODUCT MARKETING

ABOUT THE AUTHOR

Larry Miller has worked in information technology in various industries for more than 25 years and served as a Chief Petty Officer in the U.S. Navy. He earned his MBA in Supply Chain Management at Indiana University. He has written more than 200 books on numerous technology and security topics.

ENTERING THE JUNGLE

CALLOUTS USED IN THIS BOOK

SCHOOL HOUSE

In this callout, you'll gain insight into topics that may be outside the main subject but are still important.

FOOD FOR THOUGHT

This is a special place where you can learn a bit more about ancillary topics presented in the book.

BRIGHT IDEA

When we have a great thought, we express them through a series of grunts in the Bright Idea section.

DEEP DIVE

Takes you into the deep, dark depths of a particular topic.

EXECUTIVE CORNER

Discusses items of strategic interest to business leaders.

DEFINITION

Defines a word, phrase, or concept.

GPS

We'll help you navigate your knowledge to the right place.

KNOWLEDGE CHECK

Tests your knowledge of what you've read.

WATCH OUT!

Make sure you read this so you don't make a critical error!

PAY ATTENTION

We want to make sure you see this!

TIP

A helpful piece of advice based on what you've read.

INTRODUCTION

From budgeting and inventory tracking to order fulfillment, maintenance, and more, modern enterprises depend on the data in their databases for many critical operations. But protecting databases has become an increasingly difficult job due to several important trends:

- **Database growth.** The amount of data, and the number and types of databases, that organizations manage continues to grow at an exponential rate.
- **Evolving threat landscape.** Cybercriminals are getting more sophisticated in how they: 1) find and exploit vulnerabilities, 2) operationalize attacks, 3) use social engineering to deceive their victims. As a result, organizations face a high likelihood of being attacked and possibly breached.
- **Limitations of traditional backups.** The last line of defense in database protection is a robust backup and recovery strategy. However, traditional backup and recovery solutions often fall short when it comes to protecting modern database environments.

This guide explores the challenges that organizations must address to protect their enterprise databases and introduces solutions to help you ensure the resilience of these critical assets in the face of cyberattacks, operational failures, and other database risks.

CHAPTER 1

Today's Database Environments

Organizations rely on their databases for everything from simple business processes to advanced innovations and digital transformation. Because this data is so essential, organizations can't afford to be without their databases—even for brief periods of time. In this chapter, you explore the challenges of databases and database protection.

The Growing Size, Number, Types, and Complexity of Databases

As the importance of data has grown, so has the amount of data and the number and types of databases each organization manages. Statista forecasts that the volume of data created, captured, copied, and consumed worldwide will grow from an estimated 120 zettabytes in 2023 to more than 180 zettabytes by 2025. As much as 20% of this digital data universe will consist of structured data in databases according to IDC, and Gartner Inc. estimates that the database market grew by more than 14 percent to $91 billion dollars in 2022.

In addition to their size and volume, databases have also become more complex in the last decade with the adoption of open-source NoSQL databases, such as Cassandra and MongoDB, and the broad adoption of cloud technologies, like data lakes and database-as-a-service (DBaaS) managed databases. In an earlier era, nearly all applications relied on proprietary relational databases. In most cases, these databases came from one of the big three vendors: IBM, Microsoft, or Oracle. Today, open-source databases dominate the market. In its 2023 Survey Report, database consulting firm Percona found that many respondents leverage multiple database types in their organizations, including MySQL (53%) and PostgreSQL (47%), followed by Oracle (43%), Microsoft SQL Server (30%), MariaDB (24%), and IBM DB2 (23%).

The resources needed to manage these different databases have also increased. Most database administrators (DBAs)—the primary group of people responsible for ensuring the performance and general availability of an organization's databases—specialize in a specific database engine. So, when development teams introduce new data stores in an unfamiliar database, DBAs often lack the expertise to manage and back up the data in line with the best practices for that database. For example, a SQL Server DBA may struggle initially to understand how to deploy, manage, and support a MongoDB database.

While Infrastructure-as-a-Service (IaaS) workloads are more common between cloud providers, Platform-as-a-Service (PaaS) offerings (such as DBaaS) can have very different backup and restore options, even within the same cloud. This often leads to a myriad of operational approaches and procedures that can confound even the best DBAs.

Cyberattacks Continue to Wreak Havoc

As if managing an ever-changing database landscape weren't enough, organizations also have to worry about protecting their data against attacks. A recent report by Rubrik Zero Labs demonstrates just how vulnerable organizations are despite heavy investments in infrastructure and perimeter security. The survey of more than 1,600 IT and security leaders revealed that over half (53%) of organizations experienced a material loss of sensitive information in the last year, with about one out of every six organizations (16%) experiencing multiple losses in 2022.

Ransomware is a particularly insidious threat. During a ransomware attack, the threat actor typically encrypts files on one or more servers, then demands that the organization pay a ransom in order to regain access to their data. And ransomware attacks are more common than you might think. Gartner reports that 75% of organizations will face a ransomware attack by 2025.

There's a reason ransomware attacks are so pervasive: Threat actors have been incredibly successful at extorting ransoms. Beyond simply encrypting data, attackers are also increasingly practicing "double extortion," in which they threaten to publish an organization's sensitive data unless another payment is made. Cybercriminals have also moved into the software and services business with Ransomware-as-a-Service (RaaS) offerings. The growth of RaaS has democratized cybercrime by enabling threat actors with less technical expertise to conduct ransomware attacks that are built or managed by others.

Organizations that decide to pay a ransom to get their data back do so at their own risk. Even if an organization pays the ransom, it still might not get its data back. In fact, only 42% of organizations that paid were able to recover all their systems and information, and 80% of organizations that paid the ransom were subsequently hit with another ransom demand, according to the Cybereason study Ransomware: The True Cost to the Business. Additionally, paying a ransom likely finances future ransomware attacks and may lead a victim organization afoul of the U.S. Federal Bureau of Investigation (FBI) and the U.S. Department of Treasury's Office of Foreign Assets Control (OFAC). Thus, organizations should consult with both law enforcement and legal counsel before making the decision to pay a ransom demand.

Backups: Your Last (and Best) Defense Against Cybercrime and Other Database Threats

Digital data—including financial, intellectual property, and customers' private information, among others—has become the lifeblood of many modern organizations. Protecting this data from insider threats, operational failures, and cyberattacks must be a key goal for every organization. To achieve that goal and ensure business continuity organizations must have a robust data backup and recovery strategy. Remember, you can't restore your critical data if you don't have a good backup.

But because the data and threat landscapes have changed so much, traditional backup methods don't provide the reliable safety net they once did. For one thing, backup and recovery processes are now often carried out by separate teams, each with their own processes and tools. These silos often limit teams' ability to perform critical tasks quickly. For another, traditional backup and recovery approaches were designed around how to respond to large scale disasters, such as earthquakes and floods. Today, organizations use backup and recovery practices for everything from accidental deletions to providing copies of databases to development teams. Yet, today's teams are limited by processes and tools built for traditional recovery use cases. Finally, cybercriminals have caught on to the fact that organizations use backups to recover their data and now target backups directly, in addition to the production environments of their victims, to impede or entirely derail an organization's data recovery efforts.

According to a 2023 Rubrik Zero Labs report, nine out of ten organizations reported malicious actors attempted to access data backups during a cyberattack, and 73% were partially successful.

CHAPTER 2

Recognizing Limitations in Traditional Database Protection Approaches

Database protection requires DBAs to ensure their organization's critical databases are secure (protected from cyberthreats), resilient (always up, running, and available), backed up (according to predetermined service-level agreements, or SLAs), and able to be recovered quickly (to meet recovery time objectives, or RTOs). In this chapter, you examine legacy database protection approaches and their limitations.

Yesterday's Backup Strategies Can't Protect Your Databases Against Modern Threats

As the number and types of databases managed by an organization grows, environments become more dynamic, and cybercriminals get more sophisticated, it becomes exponentially more difficult to ensure your critical databases are protected from threats, such as SQL injection attacks and the FARGO ransomware family which targets vulnerable Microsoft SQL servers.

But protecting your databases isn't enough. Cybercriminals recognize that backups are a critical component of enterprise business continuity and disaster recovery plans, particularly for ransomware recovery. As a result, attackers now directly target backups to limit their victims' recovery options. Thus, your backups need to be protected like any other critical data in your organization.

Unfortunately, legacy database protection solutions—typically comprised of loosely coupled backup hardware, software, and secondary storage systems—can expose a large and vulnerable attack surface for cybercriminals to exploit. Organizations need to take a holistic approach which addresses people, process, and technology challenges to protect their production and backup data and achieve cyber resilience in their critical databases.

When New Databases Cannot Be Easily Assimilated, Resilience Is Futile

Adding a new database to the backup schedule using legacy data protection methods is a time-consuming, multi-step, error-prone manual process. Each new backup job has to be created using native scripting, which not only requires writing the script (or modifying an existing one), but also installing it on the server and scheduling it to run—for instance, using cron on Linux or the SQL Server Agent job scheduler.

Backup jobs are typically configured by a backup administrator who has to work with a storage administrator to identify a storage target with enough capacity. Then, the backup administrator needs to coordinate backup schedules to make sure that too many backups aren't running at the same time, potentially creating bottlenecks on servers, storage, and/or networks.

All these manual steps are time consuming and potentially open the door for configuration errors and other issues including:

- **Unprotected or under-protected databases**
- **Prolonged backups that can negatively impact production systems**
- **Failed backups that put critical data and recoveries at risk**
- **Extended troubleshooting to identify and remediate problems**

At best, these mistakes can cost organizations many hours of lost productivity. At worst, an overlooked yet critical database could be hit with ransomware and bring business operations to a halt.

Your Data Has Changed, but Backup Processes Haven't

The way you use data has likely changed significantly over recent years, but you may still be managing your critical database backups using processes that date back to a bygone era. Legacy backup tools and processes were designed at a time when applications and databases were a lot less complex than they are today—and data volumes were nowhere near the size and scale of modern databases that span on-premises, cloud, hybrid, and multi-cloud environments.

Due to their complexity, database backups are frequently excluded from the centralized backup infrastructure within an organization. Instead, DBAs often back up databases to online storage like a file share, which then gets backed up as part of the centralized backup process. While this process may meet the needs of both database and backup teams, it also increases the level of risk in the process.

In many cases, database backups are stored on the same storage subsystem as the production database, which means if there is a major storage failure, critical data could be lost.

Additionally, when backups are managed in isolation by the database team, the broader backup system will have limited or no visibility into the database backup process. It won't have a catalog of backups or be able to quickly identify failed backup jobs. Only the database team will know what backups were successfully completed, when they were completed, and the intricate details of how they were done for each individual database across different database servers and platforms.

Finally, legacy backup tools often lack the robust capabilities required for modern databases, such as the ability to automatically discover and protect new databases, holistically manage different types of databases, and create immutable copies of data (that is, backups that cannot be modified, deleted, or otherwise altered) by default.

Managing the Long Road to Recovery with Legacy Tools and Processes

Anytime a database goes down, it's an emergency. Modern enterprises typically employ multiple strategies to achieve cyber resilience for their critical databases, including high availability, database mirroring, data replication, and more. But should these methods fail, organizations rely on their backups to get their databases up and running again. Database downtime has a direct impact on an organization's bottom line, so time is of the essence when it comes to database recovery. DBAs and backup administrators need to work together quickly to get the database working again as soon as possible.

Unfortunately, restoring databases using legacy processes and solutions can be just as time-consuming, if not more so, than backing them up.

Backup administrators and DBAs often perform their individual responsibilities using tools and processes that the other group has limited—if not zero—access to. These siloes help the various team members make the best use of their skills, but also lead to costly delays during recovery scenarios.

Typically, DBAs are dependent on backup administrators and storage teams to provide the right backup and the necessary storage to perform the restore. Coordinating across different teams using different tools takes time. If the files aren't online, the process can take even longer.

In addition, many legacy recovery methods require entire workloads to be recovered, even if only specific datasets are actually needed. If a legacy recovery tool can't recover just the data that's needed, the recovery teams lose valuable time copying over data that might not need to be recovered.

Database backups are unique among backup infrastructure, because of the need for point-in-time recovery to ensure database resilience. This capability is typically provided by a combination of full database backups and backups of the transaction logs. After restoring a database, the transaction logs can be replayed, allowing the database to be recovered to a specific transaction to minimize data loss and ensure atomicity, consistency, isolation, and durability (ACID) properties in database operations.

These factors combined can lead to missed RTOs, lost revenue, and reputation damage for the organization. Given the critical nature of database applications, DBAs often leverage other tools to ensure high availability of critical databases. But should a DBA be forced to restore from a backup, these hurdles can exacerbate a crisis.

DBAs also regularly perform a lot of other time-consuming tasks using backup data and recovery methods. For example, it's very common for application teams to request "refreshes" of lower tier systems (such as development, QA, or testing) with data from production databases. For smaller databases, this is a relatively trivial operation, but it can also be prone to mistakes. For example, the DBA can accidentally restore to the wrong target environment and overwrite production data. For larger databases, such as a multi-terabyte database, fulfilling these requests requires a lot of manual effort when using legacy tools and processes.

CHAPTER 3

What Should Database Protection Look Like Today?

The ever-growing scale and sophistication of cyber threats requires organizations to maintain constant vigilance and proactively manage the security posture of their critical databases—including backups—across their data center and cloud environments. In this chapter, you learn what modern database protection is, how it complements your database security goals, and how it can bolster your organization's cyber resilience.

Defining Your Requirements

A modern, secure-by-design database protection strategy should help organizations:

- **Keep databases secure and available** with air-gapped, immutable, access-controlled backups that can be easily replicated and archived to multiple locations.
- **Automate database protection** by automatically discovering and dynamically securing databases across the enterprise and in the cloud.

- **Backup and access data faster** leveraging modern techniques like parallelization, only backing up data that has changed, and making recovered data rapidly available.
- **Reduce complexity** in database protection with global management that provides ease-of-use and self-service access.
- **Recover what they need, when they need it** with the flexibility to rapidly restore only specific data at a granular level, or entire workloads en masse.

Rubrik for Databases: The Solution Your DBAs Have Been Looking For

There is a database protection solution that checks all those boxes. Rubrik for Databases delivers all the key capabilities and features of a modern database protection solution, ensuring that your critical databases and data are protected from data loss, cyberattacks, and operational failures by providing the ability to recover data quickly and surgically across on-premises and cloud databases (see **TABLE 1**).

Rubrik for Databases unifies backup, replication, archival, and recovery in a single, converged software platform designed to protect *all* of your databases. So, for instance, in the event your organization gets hit with a ransomware attack, your teams will be able to work from a single pane of glass to manage the recovery effort. They will also have peace of mind in knowing that your databases are protected with air gapped and immutable backups, allowing for fast restores and minimal downtime.

REQUIREMENT	RUBRIK'S APPROACH	WHAT YOU CAN DO
Keep databases secure and available	Zero trust by design; Immutable, air-gapped, and access-controlled backups	Keep your databases safe and readily available
Automate database protection	Global policy driven automation	Discover your databases as they're created and protect them by automatically applying custom policies
Backup and access data faster	Incremental forever backups and live mount	Reduce your backup windows and access data quickly
Reduce complexity	Global catalog management and control	Centralize your database protection to simplify management at scale
Recover what you need, when you need it	Flexible recovery	Quickly and easily recover entire databases, or only the data you need

TABLE 1: Rubrik for Databases key capabilities and features

Plus, with Rubrik for Databases, DBAs no longer have to deal with painful scripting and local job schedules on each of their database servers. Instead, databases are discovered and protected automatically as they get created. Advanced capabilities—like parallelization

and mounting—help you reduce backup windows and access data quickly. And flexible recovery options help you recover entire databases or only the data you need.

Rubrik for Databases is modern database protection for the modern era. Don't settle for anything less when it comes to ensuring cyber resilience for your organization.

MORE EFFICIENT OPERATIONS

This guide has provided a look at the ins and outs of database protection, including backup and recovery. The way IT does business has radically changed, and understanding those changes is imperative. Database growth and complexity has made protecting databases more challenging than ever. And data loss, cyberattacks (including ransomware), and operational failures are all existential threats to modern databases.

Rubrik for Databases addresses these challenges, providing protection across data estates, flexible recovery options, and a central control plane for all your backup and recovery operations. This means more efficient operations and the peace of mind that comes with knowing your organization's backups are secure and ready when needed.

To get started modernizing database protection for your organization, check out Rubrik Explore.

ABOUT RUBRIK

Rubrik is a cybersecurity company and our mission is to secure the world's data. We pioneered Zero Trust Data Security™ to help organizations achieve business resilience against cyberattacks, malicious insiders, and operational disruptions. Rubrik Security Cloud, built with a Zero Trust design and powered by machine learning, delivers complete cyber resilience in a single platform across enterprise, cloud, and SaaS. Our platform automates data policy management and enforcement, safeguards sensitive data, delivers data threat analytics and response, and orchestrates rapid cyber and operational recovery.

ABOUT ACTUALTECH MEDIA

ActualTech Media, a Future company, is a B2B tech marketing company that connects enterprise IT vendors with IT buyers through innovative lead generation programs and compelling custom content services.

ActualTech Media's team speaks to the enterprise IT audience because we've been the enterprise IT audience.

Our leadership team is stacked with former CIOs, IT managers, architects, subject matter experts and marketing professionals that help our clients spend less time explaining what their technology does and more time creating strategies that drive results.

If you're an IT marketer and you'd like your own custom Gorilla Guide® title for your company, please visit actualtechmedia.com.