rubrik

EBOOK

5 Things Your Legacy Backup Vendor Won't Tell You

Why legacy backup won't protect you from a cyberattack —and what you should be doing instead.

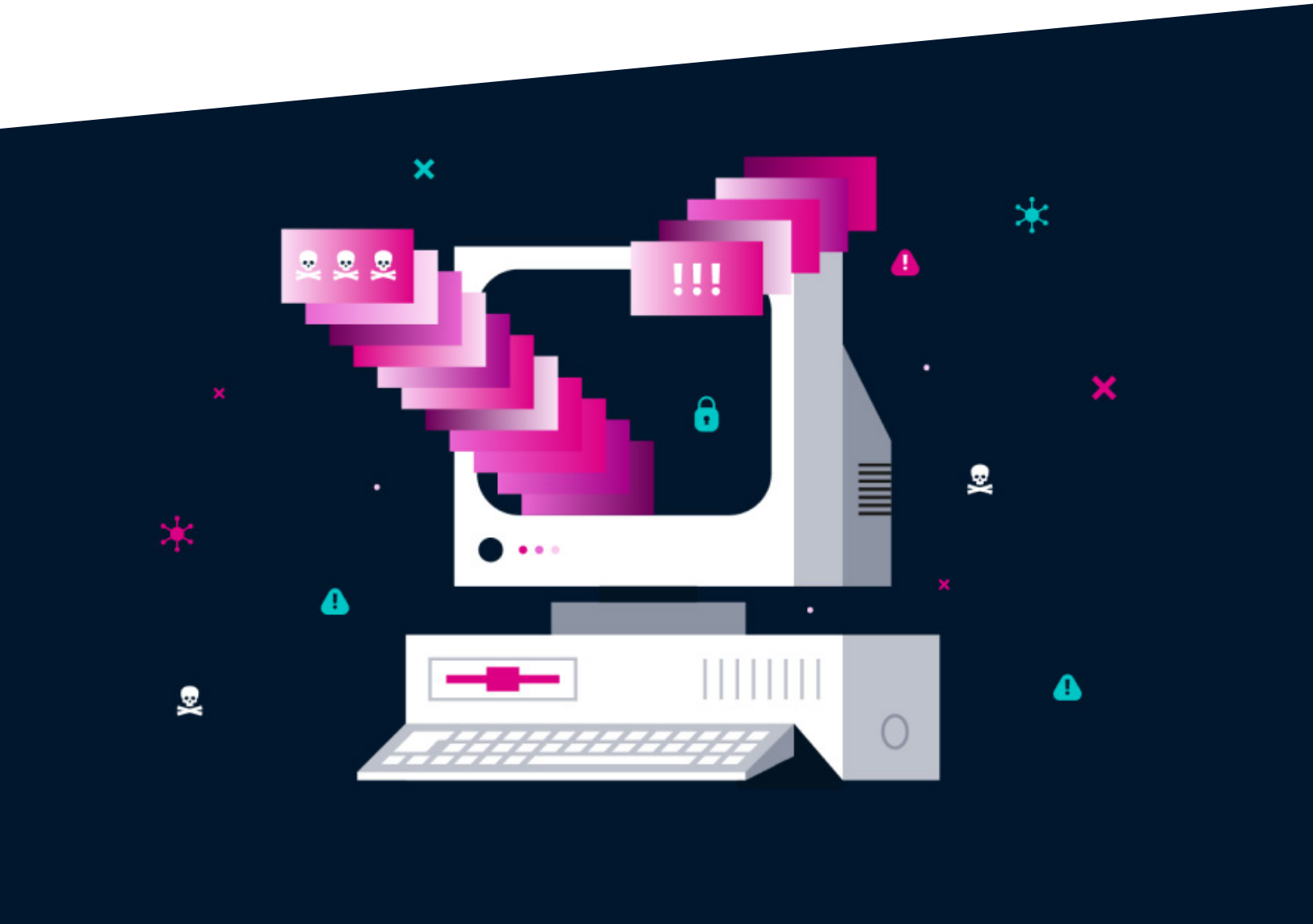


TABLE OF CONTENTS

CYBERATTACKS ARE ON THE RISE

Cyberattacks are now so prevalent that it's not a question of whether your infrastructure will be targeted, **but when**.

And a successful attack can be disastrous to your business:

- **Business impact:** 93% of organizations that dealt with a cyberattack last year suffered some level of negative business impact as a result, ranging from operational disruptions to reputational damage
- **Revenue loss:** Cyberattacks can lead to financial losses due to operational disruptions, ransom demands, or the theft of sensitive financial information
- **IT and security team fallout:** Cyberattacks can result in widespread effects to organizations and their IT and security teams, including leadership changes, loss of trust, and increased anxiety
- **Fines and other penalties:** Successful cyberattacks can lead to the exposure of sensitive data, which may result in legal penalties, regulatory fines, and reputational damage

With the odds of a cyberattack so high and the potential business impact potentially severe, you need a strategic plan that limits the damage and helps you recover quickly.

CAN YOUR DATA SURVIVE A CYBERATTACK?

For most organizations, legacy backup is the last line of defense. And while that's great for rebuilding your environment from scratch after a natural disaster—like a lightning strike, earthquake, or tidal wave—it's not enough to help you recover from a cyberattack.

But your legacy backup vendor won't tell you that.

Protecting your data with a legacy backup solution is like trying to clean up toxic waste with a feather duster. Today's cybercriminals are too organized and too sophisticated for you to trust anything other than a data security solution specially designed for cyber resilience.

Let's look at five more things your legacy backup vendor won't tell you about protecting your data from a cyberattack.

GLOSSARY OF TERMS

Cyber Recovery: The ability to quickly return to business as usual within hours or days of a cyberattack (not weeks or months).

Cyber Posture: Efforts made to reduce cyber risk by gaining visibility into your sensitive data, analyzing access activity, and proactively enabling least-privileged controls.

Cyber Resilience: The ability to withstand and quickly recover from a cyberattack. Complete cyber resilience requires both cyber posture and cyber recovery.

1 YOUR BACKUP SYSTEM IS A TARGET

Most organizations use legacy backup solutions as their last-resort cybersecurity option. But these backups are far from a safe haven. Today's cybercriminals now specifically target legacy backups to disable them as a safeguard against attack.

Here's the uncomfortable truth: **"90% external organizations reported malicious actors tried to impact data backups during a cyberattack."**

What makes legacy backups such an attractive target?

- **Obsolete security:** Your legacy backup solution may not have the orchestration tools necessary to collect and manage data from various siloed sources—including cloud instances. It may also lack the data observability features that monitor the health and performance of your data and create audit trails that may reveal the root causes of data anomalies.

  Indeed the very platform your legacy backup is built on may lack basic security features such as multi-factor authentication, role-based access control, and more.

- **Open technologies:** Legacy backup systems may use open storage protocols that can expose data to unauthorized access and manipulation by hackers. This can be particularly problematic when coupled with other security weaknesses, such as the absence of multi-factor authentication.

- **No insight:** Legacy backup systems often lack the analytics and real-time visibility into at-risk data, obscuring the extent and details of a breach.

Even though many vendors today claim to offer a "modern" backup solution, they often rely on insecure, legacy architecture. By targeting the backup, an attacker can exploit vulnerabilities in these systems to gain unauthorized access to sensitive data and threaten the viability of an organization.

Clearly, relying on legacy backup as a defense in today's rapidly evolving threat landscape is not a winning strategy. **Indeed, it can have grave consequences.**

››› PRO TIP

The only way to protect your vital business data is with a cyber resilience solution that makes your data indestructible, helps you spot threats, and facilitates speedy recoveries.

2 YOUR BACKUP HAS MULTIPLE SECURITY FAIL POINTS

Legacy backups often sacrifice robust security features in the name of convenience. Some were designed in an era when"disaster recovery" meant only restoring operations after a natural disaster—not a cyberattack. As a result, your legacy backup may be an easy target for attackers who are looking for vulnerabilities to exploit.

In other words: You may sleep well at night, thinking your data is safe because you have a backup. But that backup data is itself vulnerable to ransomware, malware, and data breaches.

Often, legacy backup solutions run on operating systems that need to be maintained, use software that needs to be patched,and contain databases that need care. That usually means technical staff must take specific action to reinforce the security of your backup. Much of this work is manual—and often, the team that maintains the server operating system is different from the one responsible for security. As a result, legacy backups may not be regularly updated or maintained, leaving them open to cybercriminals looking to exploit known vulnerabilities.

Legacy backup solutions also often lack automation or intuitive user controls, which makes these systems vulnerable to human error. For instance, it's not unheard of for staff to accidentally delete or overwrite critical data or fail to properly secure backups, leaving them susceptible to unauthorized access.

Additionally, legacy backup systems often use open storage protocols that lack the sophisticated encryption and authentication mechanisms needed to protect sensitive data.

Brent

"

The rise in successful ransomware attacks—notably against Hackney Council (practically our neighbors) and Redcar & Cleveland Borough Council—was the catalyst for moving this up our priority list and refreshing our environment sooner.

Kevin Ginn
Brent Council's Head of Operations

- Legacy solution could not guarantee peace-of-mind
- New Rubrik solution has built-in ransomware recovery
- **100%** security compliance
- **50%** time savings

Indeed, something as basic as multi-factor authentication may be totally absent from your legacy backup security practices. And since many legacy backup systems store data in unencrypted databases, a successful attack can reveal unprotected passwords to your critical systems—handing over "the keys to the kingdom" and granting malicious actors free reign over your entire infrastructure.

In this nightmare scenario, your backup itself can be used as a beachhead—turning the very system you rely on to protect you into a weapon against you.

››› PRO TIP

Your backup solution must be built for cyber resilience. It must be zero trust by design, architected with air gapping, use secure protocols, and support native immutability, data encryption, role-based access controls, and multi-factor authentication.

WABASH™

"

The backup software solutions we were using were outdated, required multiple patches, frequent firmware updates, and hands-on management of day-to-day backup jobs.

- **60% TCO savings** by eliminating licensing and consolidating storage
- **RTO reduced** from 45 minutes to seconds with no performance compromise
- Higher frequency backups **improve RPO** for less SQL and Exchange downtime

3 YOUR BACKUP WON'T HELP YOU SPOT AN ATTACK

Most legacy backup systems fail to provide critical insights or visibility into the sensitive data on your network—such as customer records that contain personally identifiable information or financial data within transaction records.

Legacy backup also lacks the ability to quickly determine what data has been affected during an attack. This means you may have to spend valuable time figuring out what exactly happened to your most sensitive data, all while responding to an incident in progress. Meanwhile, cybercriminals could continue to wreak havoc within your systems.

Here are the top three areas where legacy backups fall short during an attack:

- **Incomplete view of data:** Legacy backup systems often have limited visibility into stored data. So when a threat arises, your security team may struggle to find your most sensitive data. And if you haven't made the effort to identify your most critical and sensitive data in advance, you may lack a complete understanding of the business impact of an attack. Also, legacy backups without auto-protect policies may not capture all the data needed to fully restore a system. Attackers can exploit this by deleting files that are critical to performing a recovery.
- **No threat hunting capabilities:** The best place to find a cyberattack is within your backup system, where your security team can run expedited hunts for threats without any impact on production systems. Without effective threat hunting tools, your security team won't be able to find the source of the attack, nor ascertain which data has been tampered with or deleted.
- **Slow recovery times:** The more data you store in your legacy backup, the longer it will take to do a full restore of all enterprise data. Without the tools to determine the scope of an attack (and understand what data has been affected) you will not be able to restore critical data in a targeted, surgical way. Waiting for a full enterprise recovery prevents you from bringing unaffected systems back online quickly.

The inability to effectively monitor your own data puts you in a highly vulnerable position and significantly hinders your ability to quickly and accurately assess risks and remediate threats.

And every second you lose to ignorance is a second longer that attackers have to steal valuable data and potentially bring down your business.

››› PRO TIP

A modern backup solution must be engineered for cyber resilience. Cyber posture capabilities must be built in so your security team can easily identify threats to sensitive enterprise data in your backup instance—minimizing impact on mission-critical production systems. Cyber recovery capabilities must be able to quickly restore targeted systems, limiting a cyberattack's impact on business operations.

4 YOUR BACKUP MAY ALSO BE INFECTED

Remember we said that today's cybercriminals are increasingly targeting legacy backups? That means your backup, far from being a pristine copy of your data, could very well be **"patient zero."**

When a system is first infected, there's a period of time before your IT and security teams become aware of the intrusion, called "dwell time."

During that time, backups are running as normal—and malware is being backed up along with the rest of your company's data. If you restore from an infected backup, you're copying the malware right back to your production environment.

Imagine this: You spend hours (or possibly even days) cleaning your production system to remove all traces of malware, not realizing your backup is infected as well. If you don't know when the initial infection took place, you risk restoring with an infected backup and repeating the whole cycle all over again. As a result,you're forced to go even further back, wasting valuable time with every failed attempt to find a clean backup.

An attacker can also use the dwell time before they're discovered to target the backup itself, encrypting data so you can't restore even if you wanted to. What then?

Game over.

››› PRO TIP

Your cyber recovery solution must prevent malware reinfection and support digital forensics by analyzing the history of data for indicators of compromise to identify the initial point, scope, and time of infection.

AMERICAN FAMILY INSURANCE®

"

Threat Hunting for AmFam has been a game changer. It allows our security teams to look for specific malware or zero-day vulnerabilities across our entire ecosystem.

Nate Brooks
Technology Services Manager, AmFam

- **Consolidated** 13 backup vendors into one secure solution
- **Single view** of resiliency status and security footprint
- **13 million** customers protected
- Recovery time reduced from **days to hours**

carhartt

“

We work hard to ward off intruders but we have to operate on the assumption that they will find a way in.

Michael Karasienski
Cloud Platforms Manager, Carhartt

- **Malware found** in legacy backup tools
- Moved to a single solution for **cloud and on-premises**
- **600+** workloads migrated
- **50%+** monthly cost savings

5 YOUR BACKUP IS SLOW—YOUR RECOVERY MAY BE SLOWER

Backing up your data using legacy solutions can be slow and laborious. This is especially true if you're backing up a large amount of data that's constantly changing. For instance, if your business takes online payments, that transaction information is often stored in databases that can grow exponentially. Backing up all that data can cause your critical systems to slow to a crawl—or worse, crash completely.

Another factor that can cause problems is the lack of automation and orchestration. Legacy systems often require manual intervention to initiate backups and restorations. Because they're manual, these interventions can be time consuming and error-prone. They also don't allow you to simulate and test your recovery, so you're often left in the dark as to how long recovery would take if needed—or even if you could recover at all.

Plus, should the worst happen and you need to recover after an attack, legacy systems often force you to restore the entire system—potentially petabytes worth of data—instead of just the data you need. Recovering massive amounts of data you don't need to recover is a potentially massive time sink during a process **in which every minute counts**.

And again, legacy systems don't provide an easy way to ensure that the restored data is free of malware. So even if you manage to get your systems up and running again quickly, your environment could contain a ticking time bomb—and you could be dealing with the fallout for months.

When you're working to recover from a cyberattack, that's time you don't have.

››› PRO TIP

Make sure your cyber recovery helps you bounce back from an attack as quickly as possible with automation that limits manual processes, cyber recovery simulation that allows you test and validate your recovery plans, and the ability to restore only the data you need.

SLCC
SOUTH LOUISIANA COMMUNITY COLLEGE

“

Without Rubrik backups, recovery could have taken weeks. Thanks to Rubrik's immutable backups, **this breach was simply an inconvenience** for the two hours that we were rebooting backups.

Nick Pitre
Director of IT at South Louisiana Community College (SLCC)

- 100% recovery within **2 hours**
- **Zero** data lost
- **$0** paid in ransom

“

Our clients want to know they are partnering with a trustworthy and secure firm. Rubrik is our insurance policy for our data. **How do you quantify that peace of mind? It is priceless.**

PAYETTE

“

News never stops, and we cannot allow cyber threats to slow us down. **Rubrik gives us peace of mind knowing our data is protected and available**, which allows us to focus on our commitment to be the premier source of news that informs our readers and empowers communities to thrive.

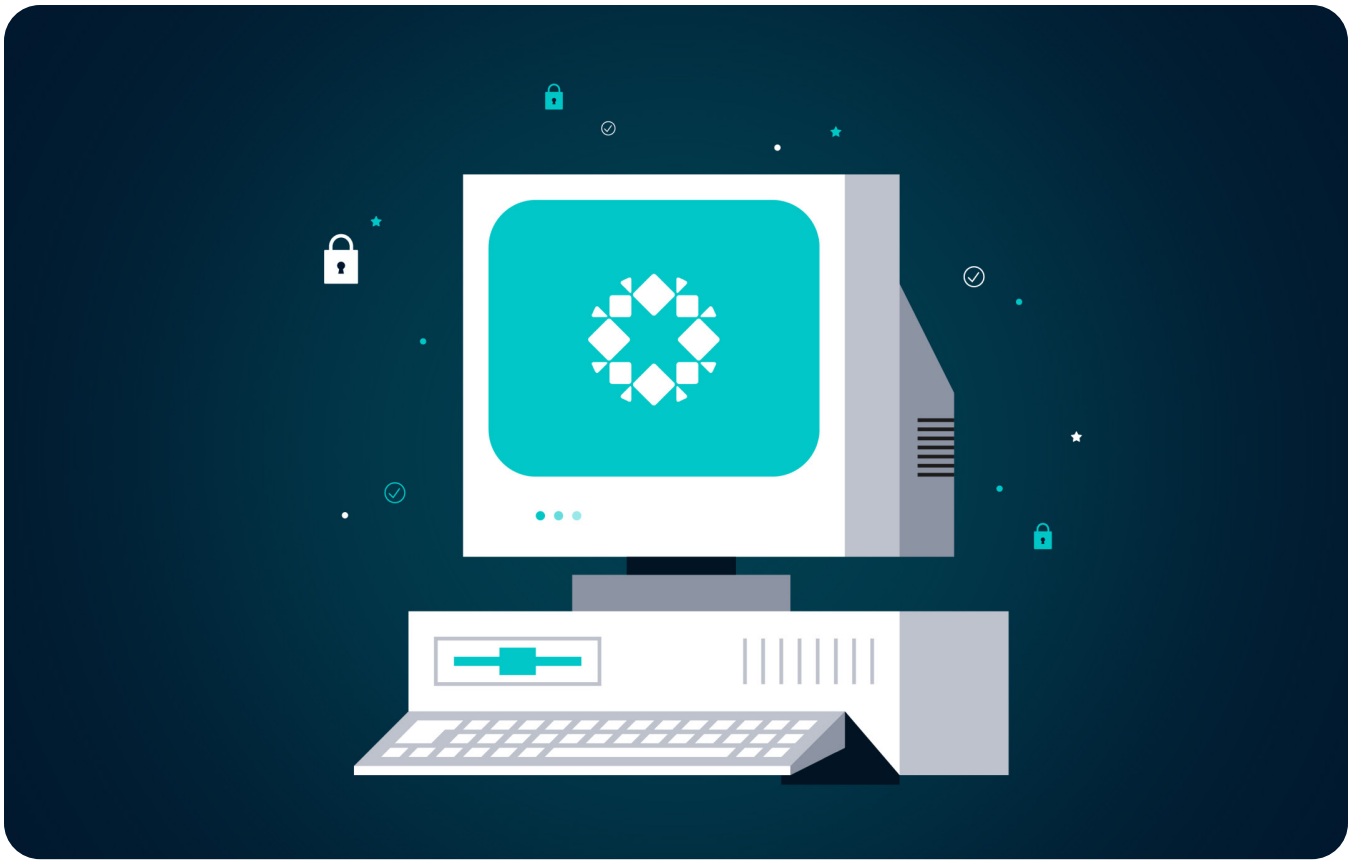
GANNETT

DON'T TRUST YOUR DATA WITH ANYTHING BUT RUBRIK SECURITY CLOUD

Your legacy backup vendor won t tell you these things—so whats a modern security professional to do?

Its time to ditch legacy backup and get a cyber resilience solution that ll keep your data safe and available,help you spot data risks and threats sooner, and allow you to recover your data—faster, safer, and with more confidence.

Rubrik Security Clouds zero trust approach keeps bad actors out, monitors for threats, and recovers your data as fast as possible. Plus, it makes protecting your data easier through automation and incremental forever backups that have minimal impact on system performance. So you can be confident in your ability to stay up-and-running, no matter what, without having to spend time doing a seemingly endless amount of manual work.



Rubrik delivers four unique benefits to your organization that legacy backup solutions simply can't:

- **Data Protection:** Ensure data integrity and availability with automated, air-gapped, immutable, and access-controlled backups designed to withstand cyberattacks, malicious insiders, and operational disruptions
- **Data Threat Analysis:** Continuously monitor for threats to your data, including ransomware, data destruction, and indicators of compromise
- **Data Security Posture:** Proactively identify and monitor sensitive data exposure (including user access analysis) and use intelligent insights to mitigate risks to this data
- **Cyber Recovery:** Quickly return to business as usual within hours or days, not weeks or months. Automated recovery orchestration and system quarantining enable you to contain threats and rapidly recover your apps, files, or objects while avoiding malware reinfection

Don't wait until a cyberattack takes down your business to realize that legacy backup has failed you. Switch to a data security solution designed for cyber recovery—one that inspires confidence that your data is safe and recoverable. Rubrik keeps your data safe, helps you spot threats, and facilitates speedy recoveries.

Don't bet your business on legacy backups. Get a true cyber resilience solution before it's too late.

Learn more here.