metallic™

7 Tips to Safeguard Your Company's Data

Avoid common data loss mistakes and outsmart ransomware

Introduction

Anyone who works in IT will tell you, losing data is no joke. Ransomware and malware attacks are on the rise, but that's not the only risk. Far too often, a company thinks data is backed up – when it's really not.

The good news? There are simple ways to safeguard your organization. To help you protect your company (and get a good night's sleep), our experts share seven common reasons companies lose data – often because it was never really protected in the first place – plus tips to help you avoid the same.

64%

of IT pros surveyed report failing to recover data over the past year.[1]

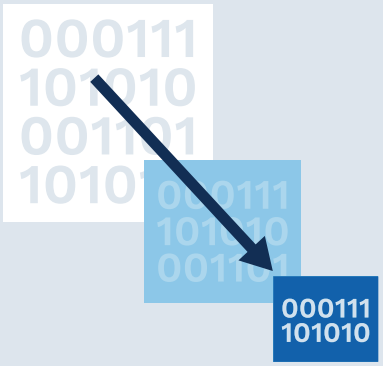
1 You're a slave to bandwidth

You know the drill: The backup is running and taking forever to complete. It's slowing systems down, so you're asked to stop the backup and run it later. It's a vicious cycle. Between your data center and your smaller offices or endpoints, getting backups to complete can be slow and painful, leaving data unprotected.

76%

of IT pros surveyed agree they experience bandwidth constraints during backup.[2]

TIP #1



Backup and recovery solutions with advanced deduplication and compression technology can reduce the size of the data before it's sent across the network. This means your backups can complete, even if you're bandwidth-challenged. If you're running a legacy backup product, this is one big reason to modernize your solution. **As you do your research, select a provider with proven network optimization as part of the underlying technology. Try the product to see if it actually delivers on the promise of bandwidth optimization before you make a purchase.**

2 No air gap, and now you're paralyzed

You've been hit by ransomware – now what? Getting your data back can be a nightmare, particularly if your backup systems are part of the compromised infrastructure. This is where companies need an air gap between the systems they are protecting and the systems they intend to recover from, meaning their backup systems or services are physically and logically separate from the impacted systems.

84%

of organizations have suffered a malicious attack within the past 12 months.[3]

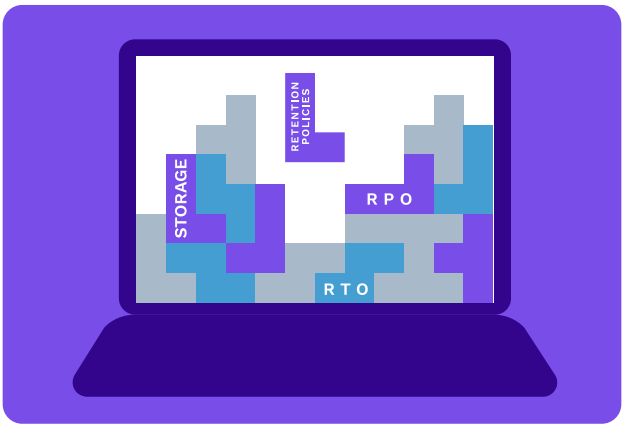
TIP #2

By running SaaS backup and recovery with the backup service hosted in the cloud, you can create secondary data copies in resilient cloud storage. This way, your backups will be ready to access, even if ransomware hits. **Consider a SaaS backup and recovery solution to protect both on-premises and cloud data.**

3 Fail to plan, plan to fail

Just as the foundation is the most important part of a house, your backup plan configuration is the most important factor in being able to recover data. Companies frequently put the wrong backup plan in place, particularly as IT admins are doing many jobs, often without the luxury of a dedicated backup expert on staff. When setting up your backup, you need to use the right RPO, RTO, storage and retention policies in order to recover what you need.

For example, there is a difference when planning between VM and SQL backups in terms of how frequently to back up. It's far too easy to end up making a wrong decision or forgetting a link in the chain – like that secondary cloud copy.



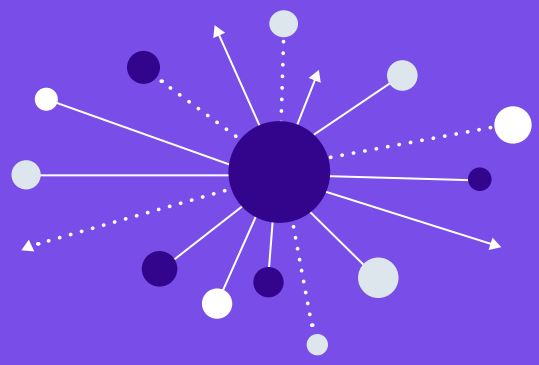
TIP #3

To take the guesswork out of configuring your backups, leverage professional services or use a smart configuration wizard within a product. **Just be sure to seek best practices guidance when setting your policies.**

4 Paying for bad decisions of the past

While the right configurations will save you money by optimizing storage, the wrong decisions can cost you. Whether it was your younger self (we've all been there) or a predecessor, someone made retention decisions years ago that have you facing massive storage costs today.

Now you're under pressure to lower storage costs, and it's on you to clean up this mess of data. Many IT admins are forced to make decisions without partnership from the broader business and inadvertently delete the wrong thing.



Data will grow at a 40% to 50% CAGR through 2025; the volume of data stored more than doubles every three years.[4]

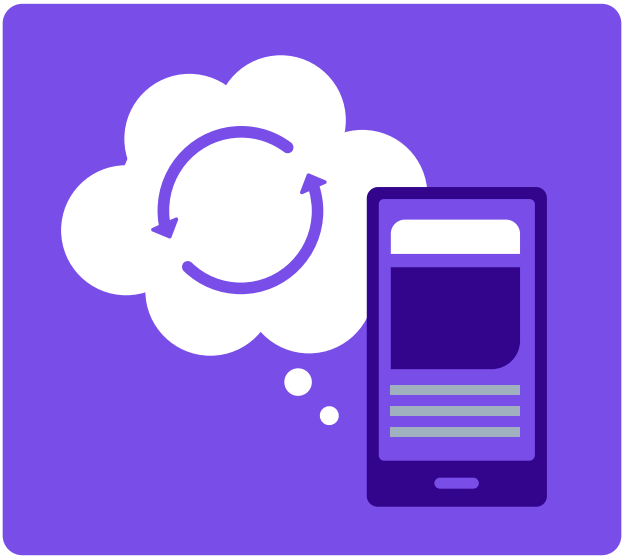
TIP #4

Work with the business owner of each application to select the backup parameters in line with compliance regulations and best practices. This way, you'll avoid creating a costly liability that can come back to bite you. **In addition, when selecting a backup solution, make sure it indexes data so it's quick and easy to find at the granular level, for when you need to clean house.**

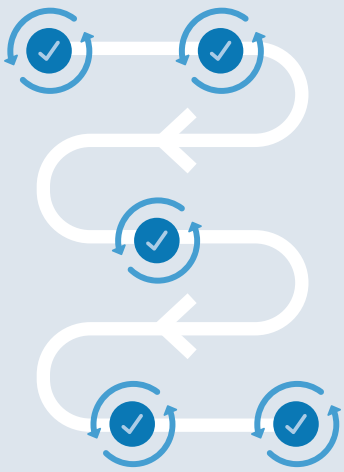
5 New apps, but backup was an afterthought

In the rush to roll out new applications, backup can often be an afterthought. You've seen it: Your company rolls out an application, you have a new data type to protect, and you realize your current backup solution won't cover it.

For example, many companies may not realize that while implementing Office 365, Microsoft's focus is on high availability, not long-term backup and retention. Office 365 customers would need to leverage a purpose-built solution for feature backup and recovery, and for enabling Office 365 content to be managed and searched with the rest of the company's data.



TIP #5



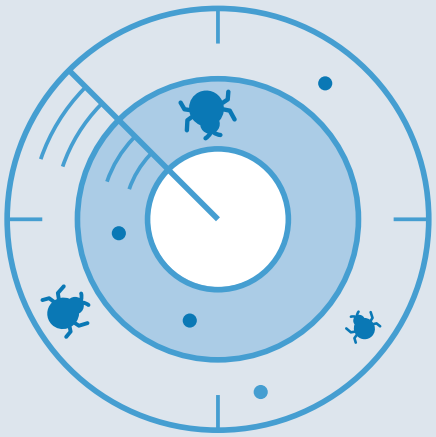
Make backup and recovery part of the planning process for all new applications your organization is considering, even those managed within lines of business. **In addition, select a backup and recovery solution with breadth of coverage so you won't be scrambling for separate new solutions to protect the latest flavor of file or database servers, VMs, endpoints and Office 365 data.**

6 With ransomware, you snooze, you lose (your data)

Companies often have safeguards against ransomware but may not be aware that their backup solution can be the last defense, even after an attack has taken place. When ransomware hits, early detection is very important. It allows a company to mount defenses quickly, contain the spread of ransomware and avoid additional data loss. Smart backup solutions can use machine learning to identify patterns, and alert you to suspicious activity, which can indicate an attack.

The other side of avoiding data loss from ransomware is being able to get it back. Once you have been alerted to ransomware, you need to be able to easily find and recover what you need from among the mountain of data in your secondary storage.

TIP #6



Stay alert to unusual activity detected by your backup solution. Make sure your backup provider offers anomaly detection powered by machine learning, granular recovery capabilities and global index to let you find and restore what you need as quickly as possible. **Select a backup provider that includes both anomaly detection and data indexing for granular recovery.**

7 You've under-engineered your backup solution, now you're not cloud ready

Data is growing like wildfire, and in IT we feel the pain of making sure it's secure and available. Companies are facing quickly growing data sets and evolving technology, and if they aren't ready to handle more data, more users and diversified environments, their backups will slow down or stop working altogether. Companies need to stay protected as they migrate data and applications to the cloud, or pursue multicloud strategies. And if you're running on-premises backup and recovery, you'll need to stay ahead of the game by adding infrastructure as your data grows, which takes time and planning.

90%

of organizations expect to use the cloud for at least a portion of their data protection strategy.[5]

TIP #7

If your backup service is managed in the cloud, you won't have to worry about rightsizing your infrastructure because the backup system is elastic. It shrinks or grows as your needs do and is easy to put in place. **Consider a SaaS backup and recovery solution to protect both on-premises and cloud workloads.**

At Metallic, our engineers and product team have decades of combined experience protecting customer data. When it comes to backup and recovery, we've seen it all – the good, the bad and the ugly.

We understand backup is not something you want to worry about – which is why we've designed Metallic™ enterprise-grade backup and recovery with the simplicity of SaaS. Our cloud-based data protection solution comes with underlying technology from industry-leader Commvault and best practices baked in. Metallic offerings help you ensure your backups are running fast and reliably, and your data is there when you need it. Any company can be up and running with simple, powerful backup and recovery in as little as 15 minutes.

Check out Metallic with a free 45-day trial today

Sources:

1,2 Hanover Research Paper, Sponsored by Commvault, Backup & Recovery Challenges and Trends, November 2019

3,4,5 IDC White Paper, sponsored by Commvault, SaaS Backup and Recovery: Simplified Data Protection without Compromise, September 2019