Evaluating backup solutions

A buyer's guide to data protection

solarwinds msp

FIVE QUESTIONS EVERY BUYER SHOULD ASK ABOUT BACKUP AND DATA PROTECTION

Businesses are more dependent on their data than ever—and expect that data to be protected, whatever form it takes, and wherever it's stored.

But that's not as easy as it sounds.

Too many rely on a patchwork of older backup solutions that have been cobbled together to deliver the kind of full-scope protection demanded by today's business requirements. In today's data-heavy environment, what's really needed is a comprehensive **data protection solution**.

Not all data protection platforms are created equal, though. By asking these five questions, you can gather the information you need to purchase the data protection product that will best fits your needs:

1. **What types of data does the solution protect?**
2. **What are the options for data recovery?**
3. **How easy is it to use?**
4. **How much does data storage cost?**
5. **How secure is the stored data?**

FACT

BACKUP IS JUST THE BEGINNING

That wasn't always the case. But with more data stored in more places—and so much of it crucial to organizations' daily business—you need to go beyond checking the box of "taking a backup" and also:

- Safeguard data against compromise and loss from user error, malicious attacks and service outages
- Make decisions in awareness of applicable data security, privacy and governance requirements
- Ensure data is available when needed—and immediately recoverable if disaster strikes, with minimum downtime

Q1 WHAT TYPES OF DATA DOES THE SOLUTION PROTECT?

Data protection needs to cover *all* data, not just the files and emails stored on servers and workstations. Comprehensive coverage has become a practical "must-have."

THE GOAL: MANAGE MORE TYPES OF BACKUPS WITH FEWER TOOLS

A true data protection solution should back up and restore data anywhere it's located: on physical and virtual servers, workstations, and in the cloud as part of software-as-a-service applications.

It also needs to protect data across the full range of operating systems and hypervisors, including Windows, Mac, Linux, VMware and Microsoft Hyper-V. If it can't, technicians will likely have to use many different tools to do their job. That can affect the time it takes to complete routine tasks—and to train up new hires. It also increases the risk of human error during critical recovery procedures if technicians are not familiar with how to perform the same tasks across different tools.

A single, comprehensive solution will make technicians more efficient and enable them to respond faster if something goes wrong.

FACT

FREQUENT TASK SWITCHING CAN MAKE TECHNICIANS

40% LESS PRODUCTIVE

Switching between multiple backup products can add hours to a technician's week. Reducing the number of backup products to be supported can bring real productivity benefits — and free up technicians to focus on more valuable, interesting and engaging work.

Source: "The True Cost of "Multi-tasking," Psychology Today. https://www.psychologytoday.com/us/blog/brain-wise/201209/the-true-cost-multi-tasking (Accessed August 2019).

Q2 WHAT ARE THE OPTIONS FOR DATA RECOVERY?

Data protection solutions need to be able to satisfy the full range of restore and recovery scenarios, not just one or two.

THE GOAL: RECOVER DATA ON ANY SCALE

Ideally, a data protection solution will be capable of all forms of restoration and recovery. This isn't always the case with traditional backup products: some focus on file/folder-level recoveries, others on bare-metal restores, others on virtual or continuous recoveries. These products tend to be strong in their area of specialization but may perform poorly in others.

Solutions also differ in recovery speed and scale. Enterprise backup applications built to recover entire IT systems can be tedious to use when recovering single files, while file/folder-level solutions may perform that one-off recovery task quickly but take days or weeks to recover an entire server—downtime most smaller businesses can't afford.

The fullest possible protection and optimal recovery speeds in any scenario require a data protection architecture that can efficiently handle disasters both large and small.

FACT

60%

OF BUSINESSES COULDN'T RECOVER FROM A CATASTROPHIC DATA LOSS

Businesses located in areas prone to floods and hurricanes may have operational needs for file and folder-level recoveries—but should also have the reassurance of full system restores being available if disaster strikes.

Source: "With the Bigger Dangers of Data Loss and Some Statistics, the Value of Backups Is Becoming Prominent," CIO. https://www.cio.com.au/mediareleases/31466/with-the-bigger-dangers-of-data-loss-and-some/ (Accessed August 2019).

Q3 HOW EASY IS IT TO USE?

The easier a data protection solution is to use and manage, the faster and more efficiently technicians can do their jobs—resulting in better, more responsive service.

THE GOAL: TAKE A CLOUD-FIRST, SOFTWARE-BASED APPROACH

Organizations that depend exclusively on proprietary appliance-based backups must be prepared for ongoing upgrade cycles (and costs), especially as data volumes continue to climb. With cloud-first, software-based backups, it's easy to add capacity as needed.

That said, keeping a local copy of backups is always recommended, allowing for recovery at LAN speed whenever possible. That means even with a cloud-first solution, there is still a need for on-premises backup storage. But the decision about which hardware to use should be up to you, not the backup solution vendor.

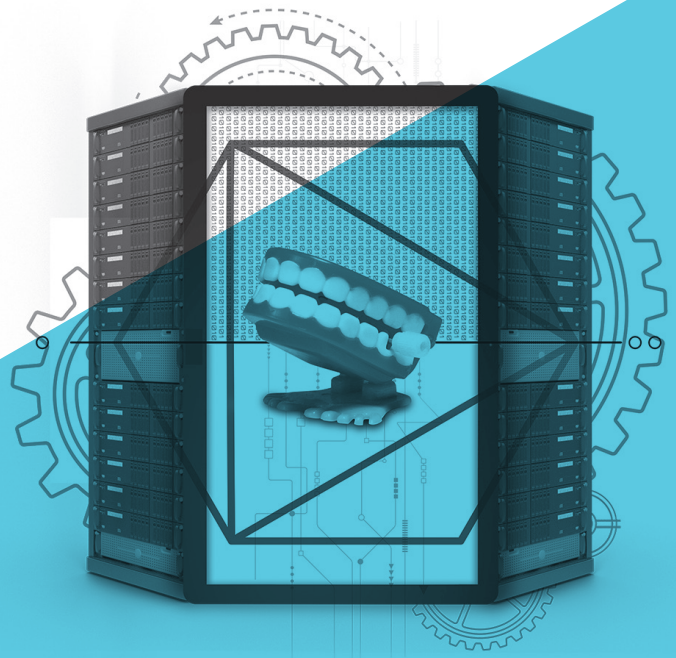
Yet in many cases, backup vendors insist on deploying proprietary appliances, with the backup process entirely dependent upon that appliance. This creates a single point of failure, especially if that appliance is the only way to collect, deduplicate, and compress data that will ultimately be stored in the cloud. In addition, the cost of replacing the appliance (if it gets damaged) or upgrading its capacity (as data grows) can be quite high, often with the additional factors of technician travel and on-site work time. And during the swap-out downtime, numerous backups can be missed.

FACT

A SINGLE, MULTI-TENANT DASHBOARD CAN SIGNIFICANTLY ACCELERATE TECHNICIANS' WORK

When technicians can view *all* customers across multiple environments from a single screen, they can check the backup status of every server and workstation at a glance and drill down into issues for resolution with one click. This kind of console can be hosted on a dedicated server (which will need ongoing maintenance and VPN access) or can be web-based for access from any device in any location.

Bandwidth consumption is an additional issue to consider. With backup solutions that aggregate data locally and then batch-push it to the cloud, the network can get bogged down, affecting other business traffic. In an ideal cloud-first scenario, each device backs up directly to the cloud, minimizing the bandwidth burden.



Q4 WHAT ARE THE DATA STORAGE COSTS?

Those who work with small- and medium-sized businesses know price matters. As part of the evaluation process, it's important to look for predictable pricing options without hidden costs.

THE GOAL: FIND A PRICING MODEL THAT WORKS FOR THE BUSINESS

There are two primary ways you'll be asked to pay for data protection. The first involves billing based on the volume of data you want to protect (often called "selected size" backup). In this scenario, if you have a 100 Gb server to protect, you need a license that covers 100 Gb of data storage. This means that unless the amount of data being protected changes, your bill won't change, even as restore points and archived data grow over time.

Another model is to bill you according to the amount of space the data actually takes up in the vendor's cloud storage. Because your backup data is deduplicated and compressed, you will likely initially use less than 100 Gb of cloud storage, so it will look like a good deal. However, as time goes on and the number of backups, archives, and recovery points increases (likely beyond the original 100 Gb), your cloud storage costs will rise as well. While this method may seem more appealing at first, it is ultimately less predictable than pricing based on selected size and can bring problems down the road.

There's no right or wrong model in this case beyond what works best for your business in the long term.

FACT

CLOUD STORAGE COSTS ARE NOT ALWAYS INCLUDED IN THE SOLUTION PRICE

Some vendors provide the software for backups, but not the local data storage hardware or remote cloud storage. This is often positioned as giving the freedom to choose any cloud provider but, for you, it means negotiating an additional contract, multiple invoices, and multiple points of contact if something goes wrong. Some vendors may try to hide the fact that cloud storage is not included in their base price. Be sure you understand what you're buying—and what else you'll have to buy to get a full data protection solution.

Q5 HOW SECURE IS THE STORED DATA?

The security and integrity of the data being protected needs to be a top priority, especially in the face of increasingly complex cyberattacks and more stringent regulations about where data can and cannot be stored.

THE GOAL: LET CUSTOMERS CHOOSE WHERE TO KEEP THEIR DATA

If a company is based in the United States or Canada, it will probably want its data to stay in its home country, largely to speed up recovery times. Organizations in Europe that are subject to the General Data Protection Regulation (GDPR) absolutely *need* to keep their data local—otherwise, they'll face stiff financial penalties.

The best backup vendor for far-flung locations would be able to provide cloud storage from your choice of data centers all over the world. That way, you can choose where you'd like your data to be stored and be confident that data locality requirements are being met.

FACT

DATA CENTERS SHOULD HAVE BOTH
PHYSICAL AND DIGITAL
SECURITY MEASURES

Any data centers where your backups will be stored should not only have high-strength encryption for data in transit and at rest but also uninterruptable power supplies, on-site and video surveillance, biometric access controls, the latest firewalls and intrusion prevention systems, and other measures to mitigate security risks and prevent data loss.

HOW DO DIFFERENT BACKUP VENDORS STACK UP?

There are a lot of cloud-based backup and data protection solutions to choose from. G2.com's user reviews from real customers provide an objective ranking based on multiple criteria to help buyers compare and evaluate the options.

G2 rates products algorithmically based on data sourced from product reviews shared by G2 users as well as data aggregated from various online sources and social networks. It then uses that data to calculate satisfaction and market presence scores and, finally, an overall G2 ranking.

	# of Reviews	Satisfaction	Market Presence	G2 Score
SolarWinds Backup	108	88	91	89
Backblaze	33	83	73	78
Code42	95	87	66	77
Carbonite	65	68	86	77
Veeam	27	69	83	76
Acronis True Image	16	72	76	74
Mozy	14	70	74	72
Druva inSync	12	67	43	55
SSD Nodes	13	76	7	41
Sync.com	12	52	11	31

Source: G2 Small Business Grid Report for Online Backup, Spring 2019.

WHY DOES SOLARWINDS BACKUP TOP THE LIST?

SolarWinds Backup is the top-ranked online backup solution for small- and medium-sized businesses on G2.com. It is a modern, cloud-first backup solution that is robust enough to handle data of all types and sizes, and supports all recovery types—from single deleted files to entire systems.

SOLARWINDS BACKUP PROVIDES:

- A multi-tenant dashboard to easily check backup status, schedule jobs and recover data across all locations and data sources.
- Fast backups and rapid restores thanks to built-in deduplication and compression.
- Private cloud storage at one of 30+ data centers around the world—included in the price with no hidden costs.
- The option to keep local copies of customers' backups using the storage hardware of their choosing.
- AES 256-bit encryption before the data is sent to the cloud—and it's never unencrypted until it is recovered.
- Multiple recovery options, including bare metal, physical-to-virtual and virtual-to-virtual.

"It's quick and easy to install and configure. Saves me time and thus saves me money. It's reliable and cost-effective compared to other cloud backup software."

–CEO of a small managed IT service provider

STRENGTHEN YOUR DATA PROTECTION TODAY

With a cloud-first approach and unified management console, SolarWinds Backup checks all the boxes for what a data protection solution needs to provide. Try SolarWinds Backup with a free 30-day trial.

TRY IT FREE

Visit www.solarwindsmsp.com/products/backup to learn more.

© 2019 SolarWinds MSP Canada ULC and SolarWinds MSP UK Ltd. All rights reserved.